IAEA-TECDOC-1983

IAEA TECDOC SERIES

IAEA-TECDOC-1983

Risk Aggregation for Nuclear Installations

IAEA
International Atomic Energy Agency

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available at the IAEA Internet site

www.iaea.org/resources/safety-standards

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

RISK AGGREGATION FOR NUCLEAR INSTALLATIONS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA-TECDOC-1983

RISK AGGREGATION FOR NUCLEAR INSTALLATIONS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

COPYRIGHT NOTICE

For further information on this publication, please contact:

Safety Assessment Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
December 2021

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Risk aggregation for nuclear installations / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1983 | Includes bibliographical references.
Identifiers: IAEAL 21-01452 | ISBN 978-92-0-135421-1 (paperback : alk. paper) | ISBN 978-92-0-134921-7 (pdf)
Subjects: LCSH: Nuclear facilities — Risk assessment. | Nuclear power plants — Risk assessment. | Nuclear facilities — Safety measures.

FOREWORD

Results of probabilistic safety assessments (PSAs) serve as input for risk informed decision making. Understanding the complete risk profile of nuclear installations is therefore essential for the prioritization and effectiveness of safety related decisions. Many uses of PSAs (such as demonstrating compliance with probabilistic safety goals or criteria) require full scope PSAs, which involve a comprehensive list of initiating events, hazards and all plant operational modes for a given PSA level.

A full scope PSA implies the aggregation of risks across contributions made by various elements. Several PSA studies in Member States have shown that there typically are significant differences among the elements of PSAs (for instance hazards and operational modes) in terms of how realistic they are. This heterogeneity among various PSA elements could impact the understanding of risk profiles and consequently affect the decision making process. Risk aggregation is therefore an important factor in the decision making process and may include risk aggregation from multiple sources of radioactivity on a nuclear installation site. Therefore, activities in this area have been conducted in parallel with IAEA activities in the area of multi-unit PSA.

This publication describes practices and challenges in Member States related to risk aggregation for various hazards and operational states and takes into account all sources of potential radioactive releases at nuclear installation sites. The publication also includes practical examples of risk aggregation and information on the use of aggregated risk results to support the decision making process.

The IAEA is grateful to those who helped prepare this publication for their valuable contributions. The IAEA officer responsible for this publication was S. Poghosyan of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

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

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

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The role of probabilistic methods in safety analysis is highlighted by Requirement 15 of IAEA Safety Standards Series No. GSR Part 4, Safety Assessment for Facilities and Activities [1]. Paragraph 4.55 of GSR Part 4 [1] states:

> "The objectives of a probabilistic safety analysis are to determine all significant contributing factors to the radiation risks arising from a facility or activity, and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where these have been defined… It constitutes a conceptual and mathematical tool for deriving numerical estimates of risk. The probabilistic approach uses realistic assumptions whenever possible and provides a framework for addressing many of the uncertainties explicitly."

The statement above precisely highlights the importance of understanding the complete risk profile arising from a facility or activity, and provides the numerical risk estimates which includes the consideration of uncertainties.

Eventually, the results of probabilistic safety assessment (PSA) will serve as an input for the risk informed decision making (RIDM) process and understanding the complete risk profile is essential to the prioritization and effectiveness of the safety related decisions. Certain uses of PSAs (e.g. use of PSA to demonstrate compliance with existing probabilistic safety goals or criteria), require a full scope PSA involving a comprehensive list of initiating events and hazards and all plant operational modes, or a limited scope implemented for specific safety criteria or goals. Paragraph 2.2 of SSG-3 [2] states:

> "… in order to use the PSA results for the verification of compliance with existing safety goals or criteria, a full scope PSA involving a comprehensive list of initiating events and hazards and all plant operational modes should be performed unless the safety goals or criteria are formulated to specify a PSA of limited scope, or alternative approaches are used to demonstrate that the risk from those initiating events and hazards and operational modes that are not in the model does not threaten compliance with the safety goals or criteria."

The full scope PSA implies that the risk needs to be aggregated from various risk contributors for the considered nuclear installation. Risk aggregation is the process of creating a combined representation of the risk across the various contributors.

There may be significant differences among PSA elements (e.g. hazards and operational modes) in terms of level of detail, resolution, inherent conservatism or even maturity of individual technology elements needed for various supporting analyses. Such heterogeneity among different elements translates into different levels of realism in assumptions, bounding assessments and treatment of uncertainties. Certain hazards could be, for example, modelled in great detail and with more realistic assumptions, whereas other hazards may be treated with bounding assessment, conservative assumptions and/or lower resolution. If not properly understood and addressed, this heterogeneity among various PSA elements could lead to a skewed representation of the final risk profile and consequently affect the decision making process. The heterogeneity of different risk contributors needs therefore to be taken into account

during the risk aggregation process in both the generation of the aggregated risk profile, and in the communication of this critical information to the decision makers.

For example, a classical single unit PSA may include multiple operational states and different hazard groups impacting the unit. If required by the application, risk aggregation can then be expanded to a multi source level, where risk from different sources of radioactivity on a site will be addressed. Radioactive sources can include multiple reactor units, spent fuel pools, fuel dry storage or other installations which might be operating at the site. The computational and analytical challenges can increase significantly in the level of complexity and resources needed, and, therefore, it is important to consider what is the needed level of detail (hence, requiring an understanding of the different level of details in each additional PSA modelling aspects). At the single unit level, different hazard or plant operating states may be addressed with different levels of details; at a multi source level, the process of risk aggregation may even include a different definition of undesired end state (e.g. fuel damage, core damage) and of success/failure along with the associated success criteria, which may be unique for distinct nuclear installation.

The relevance of a more complete understanding of the aggregated risk estimate obviously depends on the application. Different applications requiring risk informed decisions may focus on different risk metrics. Some of the risk metrics might be more applicable to a site level point of view. Aggregation of risk on a multi source level may be the objective for the understanding of the overall risk of radioactive release and/or health effects for a given site containing various nuclear installations under a full scope PSA.

Appropriate communication between multiple stakeholders (e.g. regulatory body, utilities, public) is critical when dealing with risk aggregation. For example, uncertainty information is an important part of the understanding of PSA results and further decision making process when dealing with heterogeneous PSA outputs. Therefore, risk aggregation will need to consider how decision making may be impacted by the propagation and representation of uncertainties in quantitative results.

During the development of this publication several consultancy meetings have been conducted and a large technical meeting was organized with involvement of 45 participants from 24 IAEA Member States. The feedback from the discussions have been continuously shared with the IAEA project on multiunit PSA and disseminated among the topical international working groups (such as the working group on risk assessment, WGRISK, at the Organisation for Economic Cooperation and Development's Nuclear Energy Agency, OECD/NEA).

1.2. OBJECTIVES

The objective of this publication is to describe the practices and challenges in Member States related to risk aggregation for various hazards, various operational states, and taking into account all sources of potential radioactive releases at the nuclear installation site. This publication provides a methodology and technical basis on risk aggregation and identifies the good practices available in IAEA Member States.

Requirements for risk aggregation in the national legal and regulatory framework differ among Member States. The specifics of how risk aggregation is done in different Member States would be impacted by different requirements, e.g. safety goals established for specific risk metrics. Therefore, the information provided in this publication could be used by multiple stakeholders (regulatory body, utilities, public) in different regulatory contexts that will drive different requirements to perform aggregation of various risk contributors for nuclear installations.

1.3. SCOPE

The scope of this publication includes consideration of risk assessment for various aspects covering the following elements:

— Various possible hazards, namely: internal initiating events caused by random component failures or human errors, internal hazards (e.g. internal fires and floods), and external hazards (both natural and human induced);
— Various operational states of nuclear installations;
— Various sources of radioactivity for nuclear installations on the site (e.g. reactor units, spent fuel pools, fuel dry storage).

The basic underlying assumption of this publication is that the process of risk aggregation is implemented after the risk metrics are quantified for various risk contributors, considering the recommendations and requirements to PSA presented in IAEA Safety Standards (e.g. [1]-[3]), and supporting technical publications (e.g. [4]). In addition, this publication also addresses qualitative aspects of risk aggregation and safety related decision making, using the results of risk aggregation.

Although, the need for consideration of the full scope PSA is mentioned above, it needs to be emphasized that the principles reflected in this publication and the importance of risk aggregation are applicable and relevant for the non full scope PSA as well.

This publication is foreseen to be applicable for nuclear installations (not only to nuclear power plants, NPPs). While examples are mainly about NPPs, they are not intended to be limited to only one type of nuclear installation, as all the principles reflected in this publication can be equally considered for risk aggregation for non NPP installations. Where appropriate, specific examples related to non NPP installations (if available) have been introduced (e.g. for research reactors or other installations such as facilities for storage of radioactive waste on site).

1.4. STRUCTURE

Section 2 provides the general approach of risk aggregation by presenting the discussion of the quantitative and qualitative aspects of risk aggregation. Section 3 defines the methodology and different approaches for risk aggregation and presents the practice in IAEA Member States aimed at illustrating the risk aggregation process for the following areas: various sources of radioactivity, various hazards, and various plant operational states. Section 4 addresses the relationship between risk aggregation and decision making processes. Section 5 presents the details on communicating the risk information from the perspective of various stakeholders. Section 6 provides a brief discussion on the open issues and challenges in the area of risk aggregation. Section 7 provides the list of terms and definitions widely used in the publication related to risk aggregation. Appendix I presents the mathematical foundation for the methodology of risk aggregation described in Section 2. Appendix II describes the illustrative example of risk aggregation for different hazards. Appendix III presents the challenges expected for certain PSA applications in terms of risk aggregation results. Appendix IV provides examples of the risk communication from the perspective of various stakeholders. Annexes contain descriptions of Member States' practices related to risk aggregation and the use of aggregated risk results in RIDM process.

2. GENERAL APPROACH FOR RISK AGGREGATION

As indicated in the IAEA Safety Glossary [5], the term 'risk' has multiple meanings. This publication uses definition (1) from the IAEA Safety Glossary [5]:

> "A multiattribute quantity expressing hazard, danger or chance of harmful or injurious consequences associated with exposures or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences."

In mathematical terms, this definition can be expressed generally as a set of triplets, $R = \{\langle S_i|p_i|X_i\rangle\}$ [6], where S_i is an identification or description of a scenario i, p_i is the probability of that scenario and X_i is a measure of the consequence of the scenario. The concept of risk is sometimes also considered to include uncertainty in the probabilities p_i of the scenarios. It is important to note that there can be uncertainties in the consequences of a scenario, as well as in the probability. Simply put, this definition of risk answers (1) What can go wrong? (2) How likely is it? and (3) What are the consequences?

In this way, it can be seen that this concept of risk includes qualitative as well as quantitative aspects. In particular, it includes the description of potential scenarios and a characterization of uncertainty. Thus, the process of risk aggregation is not limited to the arithmetic summation of quantitative estimates of risk metrics. Rather, following the dictionary definition of 'aggregation,' it involves the general collection and gathering into a whole of qualitative and quantitative risk information. The purpose of this aggregation is to form a combined representation of risk supporting risk characterization[1] [7] and risk informed decision making (RIDM).[2]

This section provides an overview discussion of a high level approach to risk aggregation that is consistent with good practices in Member States. Section 2.1 identifies different risk metrics that might be used in support of risk informed applications[3]. Section 2.2 discusses, in general terms, how estimates (including quantified uncertainties) of these metrics can be mathematically developed from estimates for different risk contributors (See Appendix I for a detailed mathematical basis). Section 2.3 discusses what additional quantitative and qualitative information can be used to create a combined representation of risk. Practical complexities in the application of the methods described in Sections 2.2 and 2.3 are discussed in Section 3.

2.1. RISK METRICS

Numerous risk metrics are used in Member State for RIDM applications. These metrics, many of which are institutionalized through safety goals, standards, and criteria, include (see Appendix I of Ref, [4], SSG-3 [2], SSG-4 [3], Refs [8] and [9]):

---

[1] Per the U.S. National Research Council, 'risk characterization' involves the translation of information in a risk assessment into a form useable by a risk manager, individual decision maker, or the public [7].

[2] As discussed in [11] risk aggregation is also important for non decision oriented uses of risk information, such as the development of risk understanding and risk communication.

[3] This includes any type of risk informed application and is not limited to risk informed applications related to regulatory decision making.

— Metrics related to the frequency or probability of an undesired end state (e.g. core damage frequency — CDF, large early release frequency — LERF, fuel damage frequency — FDF, release category frequency — RCF, core damage probability —CDP)[4];
— Metrics related to the conditional probability of undesired end states, given a specified condition (e.g. conditional core damage probability — CCDP, conditional containment failure probability — CCFP, conditional fuel damage probability — CFDP);
— Metrics related to changes in end state frequency or probability (e.g. change in core damage frequency — ΔCDF) or conditional accident probability (e.g. incremental conditional core damage probability — ICCDP);
— Metrics related to scenario consequences (e.g. probability distributions for health effects, mean values of such effects).

It is important to note that not all risk metrics for a given level of analysis can be aggregated. For example, it may not be meaningful or correct to aggregate CCDP across all radiological sources; CCDPs and CFDPs, which represent different end states; or consequence metrics with significantly different timing characteristics. Analogous risk measures can be used in analyses for multiple sources of radioactivity (see Section 3.2 for more detailed discussion).

In the context of RIDM, these risk measures are typically used in comparisons with established criteria. As a more complicated example, probability distributions for accident consequences, which quantify the aleatory uncertainty in these consequences, can be compared against limit lines. This concept is exemplified by a 1967 reactor siting proposal by Farmer (see Fig. 1) [10], which shows intervals of accidental releases of ^{131}I as a function of an equivalent ground level release of ^{131}I.[5]

In the cases of both event based (e.g. binary states such as core damage) and consequence based metrics (e.g. metrics with a continuous value such as dose), the PSAs used to estimate these metrics are subject to uncertainties. Therefore, situations can exist where it is uncertain whether or not established criteria has been met. Guidance for addressing such situations can be found in the IAEA-TECDOC-1909 [11] and NUREG-1855 [12].

For the purposes of this publication, it is important to recognize that the metrics used in practical RIDM are aggregated quantities (i.e. aggregated across various radiological sources, hazards, and plant operating states). Section 2.2 provides a general discussion of the quantitative combination of risk metrics (including uncertainties). Section 2.3 provides a discussion of additional risk information needed for RIDM beyond quantified results for risk metrics. Section 4 discusses the relationship between the risk aggregation aspects addressed in this publication and the RIDM process.

[4] Appendix I discusses the relationship between accident frequencies and probabilities. For the purposes of this publication, the distinction is particularly important when aggregating risk across plant operating states.
[5] Although the mean value is typically used for decision making, it is also important to note that the full aleatory distribution provides additional useful information that can help decision makers separately consider events/scenarios with differing combinations of likelihood and consequence but have the same expected value of risk (as computed using Definition (2) of 'risk' in the IAEA Safety Glossary).

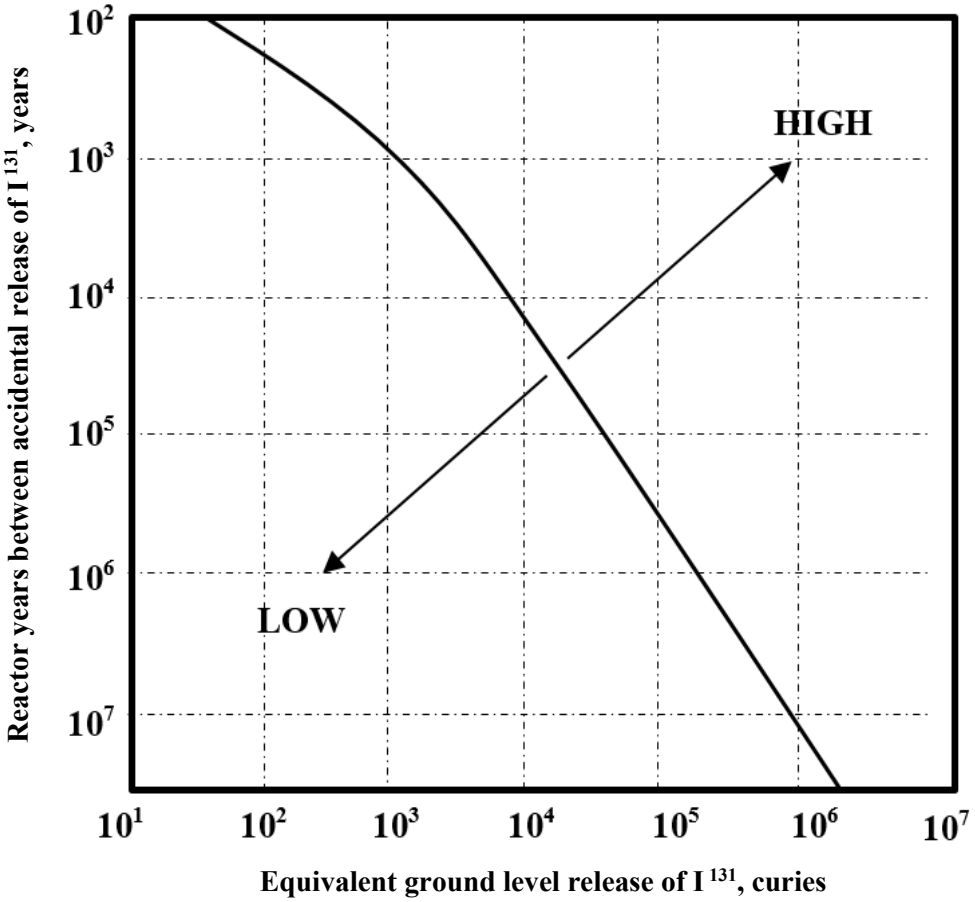


FIG. 1. Proposed frequency consequence limit line for siting applications.

2.2. QUANTITATIVE ASPECTS OF RISK AGGREGATION

While the mathematical operations related to quantitative risk aggregation may be relatively straightforward, there are several important aspects of the aggregation process to consider when generating results. Three major assumptions underlying the mathematical framework of current PSA models are:

— Assumption 1: random (i.e. aleatory) events occurring over time (e.g. initiating events, runtime failures) are typically modelled as Poisson processes;
— Assumption 2: random events occurring in response to demands (e.g. failures to change state on demand, initiating events occurring in response to manipulations or tests fixed in time) are typically modelled as Bernoulli processes[6];
— Assumption 3: The accident scenarios in the PSA models are typically modelled as being stochastically independent.[7]

[6] Both the Poisson process and the Bernoulli ('coin flip') process are memoryless — the probability of a future event does not depend on past history.
[7] Note that this assumption applies at the accident scenario (i.e. scenario) level where an accident scenario consists of an initiating event followed by subsequent events that represent the success or failure of plant equipment or operator actions (i.e. a cut set). Within scenario dependencies (e.g. altered failure probabilities due to scenario specific conditions) are treated within the scenario model.

Given these three assumptions, the following well known properties of quantitative risk aggregation can be derived (see Appendix I for details):

— Property I: the occurrence of an accident scenario is a Poisson process. The frequency of this process[8] (i.e. the scenario frequency) is the product of the initiating event frequency and the probabilities of subsequent events (conditioned, as appropriate, on preceding events in the scenario).
— Property II: The occurrence of an undesired end state (e.g. core damage) is also a Poisson process. The associated total frequency of that end state is the sum of the frequencies of the scenarios leading to that end state.
— Property III: For a specified consequence measure, the total probability distribution quantifying the aleatory uncertainty in that measure is the weighted sum of the contributions from all scenarios in the PSA model.
— Property IV: The mean total frequency of an event based end state is the sum of the mean frequencies of the scenarios leading to that end state regardless of the underlying distribution of the individual scenarios. Similarly, the mean total value of a consequence based end state is the weighted sum of the mean contributions from all scenarios.

The remainder of this section provides a discussion of a general mathematical framework for developing combined quantitative risk results and the associated quantified uncertainties; how that mathematical framework applies to PSA; and general conclusions and observations to consider when combining quantitative risk results and uncertainties to serve as input to the RIDM process.

The general mathematical framework described herein relates to the aggregation of quantitative risk results in cases where the result for a given risk metric is described by the mean value of the associated full probability distribution function. Furthermore, it is assumed that the results for a risk metric from different analyses (e.g. different radiological sources, hazards, and operating states) are stochastically independent. It is mathematically correct to add the means to obtain the combined quantitative result. Regarding uncertainties, the distribution of the combined result may be calculated analytically (e.g. via the convolution integral) or numerically (e.g. numerical sampling methods) for stochastically independent PSA inputs. Other cases that involve quantitative aggregation of different statistical measures or point estimates are discussed briefly at the end of this section. The following are some general points about uncertainties that are important to consider when aggregating quantitative risk results. Since the PSA input parameter values are subject to epistemic (i.e. state of knowledge) uncertainty, the resulting accident scenario (see Property I above) and end state frequencies (see Property II above) are also epistemically uncertain.

In principle, the distribution for the end state frequency (see Property II above) due to input parameter uncertainties can be computed using the convolution integral if the PSA input parameters are epistemically independent (i.e. there are no state of knowledge dependencies). In practice, sampling based approaches (e.g. direct Monte Carlo, Latin hypercube sampling) are typically used to ‘propagate’ the input parameter uncertainties. Adjustments to account for epistemic dependencies (i.e. state of knowledge dependencies) can be made using conventional

[8] Recall that the Poisson process is characterized by a single parameter, called the frequency. This does not imply that Poisson events occur regularly in time. See Appendix I for more information.

PSA software tools[9]. It is important to note that the resulting end state frequency distribution typically does not reflect model uncertainties. By definition, a model uncertainty is an uncertainty related to some aspect of a PSA model that can be represented by any one of several different modelling approaches; none of which is more clearly appropriate/correct than the other.Additional information on model uncertainty can be found in NUREG-1855 [12].

While the individual contribution of a specific hazard may include larger uncertainty, the summation of various contributors can result in a narrower distribution around the sum of frequencies if one hazard has a significantly higher absolute value (e.g. adding a frequency of 1E-7/year to 1E-4/year will result in 1.001E-4/year, which is essentially 1E-4/year for practical purposes). Although the relative uncertainties in individual risk contributors may be very large, the relatively uncertainties in the sum can be comparatively small. Fig. 2 provides an illustration of this effect for a plant specific PSA, as adapted from [13]. This figure was derived from assumed lognormal distributions for the individual contributors (as shown) and the aggregated sum was obtained via Monte Carlo simulation where the equivalent normal distributions are plotted since this makes visualization easier (note: the distributions appear normal in this scale but the actual distributions are non normal, as they usually are in PSA models). In other words, the x-axis is scaled in order to better compare the individual contributors and the aggregated result. It is also important to note that the aggregated result has a quasi-lognormal distribution. Regardless of the magnitude of uncertainty in the model inputs, or of the degree of epistemic dependence between inputs, the mean values of frequencies and consequences are still additive.

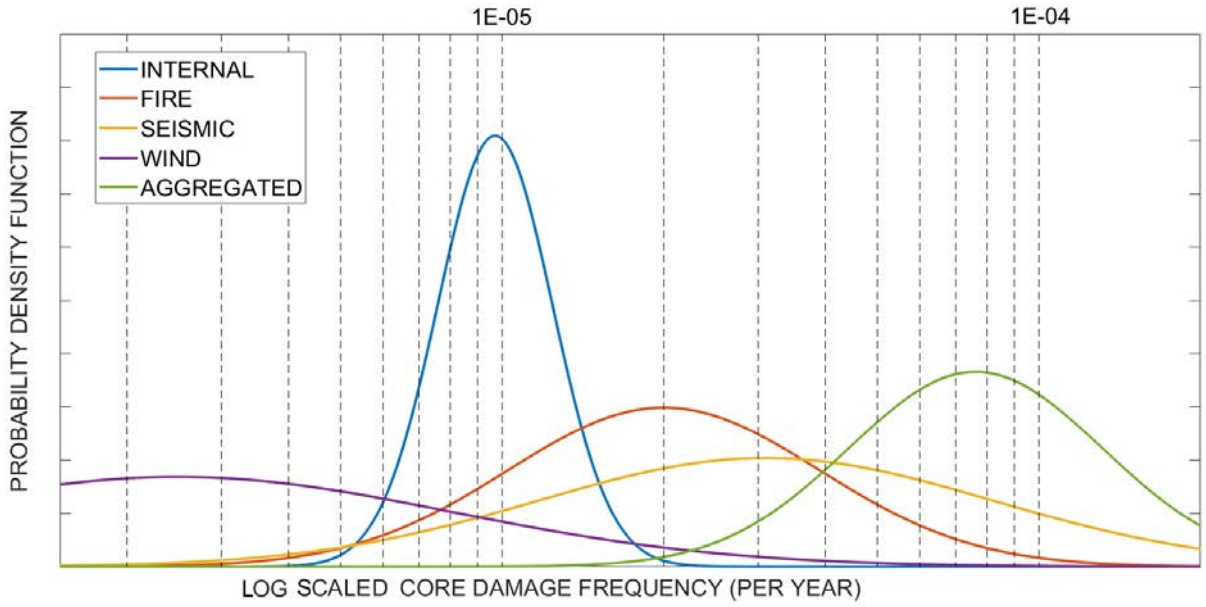


FIG. 2. Uncertainties in major contributor CDFs and total CDF from a plant specific PSA plotted in an adjusted scale for ease of visualization.

The following are some conclusions and considerations that result from the aggregation of quantitative risk results. For most practical applications, the annual probability of events can be reasonably estimated using a Poisson model with a time based average of the at power and low

[9] It is important to recognize that the existence of epistemic dependencies between scenarios affects epistemic uncertainty propagation calculations, but does not affect the fundamental additivity of scenario frequencies (which characterize the aleatory uncertainties in the occurrence of the different scenarios).

power/shutdown event frequencies. Of course, the average event frequency can deviate significantly from instantaneous event frequency at any given point in time.

For the purposes of this publication, which focuses on risk aggregation across radiological sources, hazards, and operating states, the usefulness of the sums of conditional risk metrics (e.g. CCDPs or CFDPs) across these aspects of a PSA will be dependent on the intended application. For example, when looking at the conditional risk metrics associated with the occurrence of different hypothetical initiating events in a prospective analysis, interpretation and appropriate use of the sum can be challenging because of the differing conditions associated with these events. On the other hand, the sum can be useful for retrospective event analyses. One ongoing application involves the summation of CCDPs associated with accident precursors [14]. Here, the sum is not meant to represent an alternative estimator of the total core damage frequency of an operating fleet of reactors, but it is considered to be a useful index. As another example, the summation of CCDPs for fire initiated operational events has been used to provide one piece of evidence in an evaluation of fire PSA maturity and realism [15]. As with the accident precursor example, the sum was not proposed as an alternative means for generating fire CDF estimates suitable for RIDM.

Difference based metrics (e.g. ΔCDF) and importance measures are derived from baseline metrics (e.g. CDF) evaluated under different conditions. Quantitative assessments of the uncertainties in these derived metrics need to recognize the epistemic dependencies between baseline metric estimates and difference based metrics (e.g. due to the appearance of many of the same parameters in the pre- and post change estimates of the basic metric).[10]

Some importance measures are additive while others may not be additive. For example, the risk achievement worth for a system can be greater than the sum of the individual risk achievement worth for the components in that system, as discussed in [16]. However, for importance measures that are additive, it may be necessary to disaggregate the results to gain a better understanding of the meaning of the aggregated result. This topic is discussed further in Section 5 and 6.

In cases where models for some of the contributors to a total risk metric are overly conservative, the derived metrics might actually be overly non-conservative (i.e. if an overly conservative result dominates, then other more realistic inputs may appear as less important, when this may not actually represent the risk profile of nuclear installation). This topic is further discussed in Section 4.

As with any computational process, meaningful input is needed to produce meaningful output. Thus, if the epistemic distributions for input parameters do not reasonably represent the state of knowledge concerning those parameters, or if PSA models for certain contributors are biased such that the distributions for the frequency and consequences of those contributors are likely biased, the propagation of uncertainties through the PSA model may not result in a distribution that adequately represents the state of knowledge with respect to the risk metrics of interest. Similarly, in such cases, the sum of mean values across scenarios/contributors may not provide a reasonable estimate of the total mean value.

[10] In principle, estimates of ratio based importance measures that use mean values for the base metric are only point estimates. A full uncertainty propagation would have to be done to derive the mean value of the importance measure.

When combining a risk metric mean value with a point estimate, it is generally acceptable to add these two different types of results; however, the meaning and implications of the combined result needs to be well understood and documented. This is particularly important given that the point estimate may be very different from the associated mean value (e.g. adding together a mean value and a conservative point estimate from a scoping assessment). In such cases, the analyst may need to apply engineering judgement to provide a characterization or recognize the implications of adding a point estimate on the overall characterization of uncertainty.

2.3. QUALITATIVE ASPECTS OF RISK AGGREGATION

Risk aggregation implies combining quantitative risk results and qualitative risk insights to develop a more complete and broader understanding of the overall risk that would not otherwise be conveyed by combining quantitative risk results alone. A process of integrating qualitative risk aspects generally includes:

— Identifying the role and impact of risk aggregation for the given risk informed application;
— Identifying important factors contributors to the decision;
— Identifying sources of uncertainty important to the decision;
— Documenting on risk aggregation for the decision consideration.

Probabilistic safety assessment used for regulatory decision making needs to be as realistic as practicable; however, conservative modelling choices and assumptions are generally used in order to focus analytical resources on the most important aspects. It is important to recognize that employing any conservatisms or non-conservatisms, can bias the results, which will have different impacts on the decision depending on the risk informed application. See Refs [12] and [17] for additional discussion on conservative bias. As such, the impacts of important conservative modelling choices in a PSA (i.e. those that can potentially influence the decision) for the specific application needs to be clearly understood and communicated. Conservatisms in PSAs can generally be described in terms of degree of realism and the level of detail in a PSA.

The concept of PSA realism addresses the degree to which an analysis represents the technical and organizational system relevant to the decision under consideration. For example, a PSA system model that is based on plant specific failure data will be more realistic than the same model that is based on generic industry wide failure data (although the use of generic data may be suitable to the specific application). It is important to recognize that PSA realism also relates to the extent to which uncertainties are explicitly considered in the model. Closely related to PSA realism is PSA level of detail, which is the degree of fidelity employed in the development of a given model. For example, a system that is modelled at the functional level has a lower level of detail than the same system which is modelled down to the component level. The impact of greater level of detail in terms of realism as well as the increased need and availability of data needs to be considered (e.g. is more detail needed, can it be practically modelled, is data available) [15].

Related to the concept of PSA realism is the concept of PSA maturity, which addresses the relative state of development of a technical discipline. Judging the maturity of a technical field is a subjective matter, being dependent on the judgment of the assessor. The characteristics that are considered to be indicators of maturity of an analysis technology are:

— Current state of development of the technology;
— Level of analysis possible;

— How the analysis technology is applied in practice;
— Number of experienced practitioners using the technology;
— Use of the technology in support of practical decision making.

Reference [15] also point out that the analytical technology (i.e. methods, models, tools, and data) of a less mature discipline could, but need not, produce unrealistic analysis results. Conversely, a more mature discipline could, for practical reasons, employ technology with known weaknesses, only requiring that the weaknesses be understood and appropriately addressed in the decision making process. Also it needs to be highlighted that the practitioners of a less mature discipline might intentionally use conservative (and potentially unrealistic) assumptions in an attempt to compensate for weaknesses in the current state of knowledge [15].

Another qualitative risk aspect that is generally important to understand is the use and interpretation of the mean value. As discussed in NUREG-2201 [18], the mean value is a mathematical quantity that, although precisely defined and typically easily computed, it does not have as intuitive of a meaning as some other parameters such as the median (i.e. the middle of the distribution) or the mode (i.e. the most likely value of a distribution). However, in addition to being a clearly defined quantity that is easily computed, the mean value is still useful in decision making as it is a scalar (i.e. a single value) that can be easily compared with simple criteria that allows decision makers to make informed decisions without needing to consider the full results of a detailed uncertainty analysis. Also, because it is computed using the entire probability distribution, the mean value provides some reflection of the uncertainty quantified by that distribution.[11] Further, in formal theories of decision making, it can be shown that the mean value is the theoretically appropriate metric to use under certain conditions. It needs to be noted though that it is nonetheless important to understand the meaning of a given mean value from an analysis, particularly in cases where the mean value may be representative of extreme portions of the associated distribution.

Depending on the risk informed application under consideration, other qualitative risk aspects that may be important include analysis of PSA insights, such as a qualitative inspection of minimal cut sets to help inform an assessment of the level of defence in depth or the reliability of digital instrumentation and control systems [19], [20]. Additionally, providing context for the decision such as historical precedent for similar risk informed decisions can be useful complementary information. It needs to be noted that, with some adaptation to specific applications, the general concepts in this section can be applied also to non NPP nuclear installations. For example, if a quantitative risk assessment is developed for a research reactor (i.e. PSA for research reactor) or if a high level waste nuclear repository is assessed using a probabilistic approach (e.g. a performance assessment), while the terminology and methods may differ from NPPs, the aggregation of quantitative risk information and the need to understand the risk profile is equally applicable at a high level.

To summarize, it needs to be highlighted that the specific qualitative risk aspects needed for risk aggregation are dependent on the role of risk in a particular risk informed application as well as a Member State's regulatory framework. The aggregation of qualitative and quantitative risk insights is discussed in more detail in Section 4 highlighting also the relationship of the risk aggregation to the process of decision making.

[11] Note that the median is not affected by the length of distribution tails (i.e. the possibility of large deviations from the distribution center), and the mode, in most practical situations, represents only one point on the distribution.

3. AGGREGATION OF VARIOUS RISK CONTRIBUTORS

Prior to the individual discussion of issues relating to multi source, multiple hazards, and various plant operating states it is important to highlight some high level insights from past experience with risk aggregation to reinforce the fact that:

— Dealing with risk aggregation is not a new issue for PSA modelling or application;
— Whether risk aggregation is needed or not, it is application specific and its benefits depend on the quality of the underlying PSA model.

3.1. HISTORICAL BACKGROUND

There are various references that have highlighted the experience and evolution of PSA modelling in various Member States (see Ref. [21]–[25]). As stated above, the goal here is not to repeat a detailed discussion of historical aspects but highlight important high level insights for risk aggregation.

A foundational effort on using PSA for nuclear safety aspects published in 1975, the Reactor Safety Study (also known as WASH-1400) [22], provided the basic PSA technology framework that is still in use today. Effectively, WASH-1400 showed how various accident sequences and release categories could be aggregated, using the common nomenclature still applied to most PSA models. WASH-1400 represented a milestone in demonstrating how PSA can provide a quantitative approach to estimate and present the risk in a useful form. In effect, by highlighting how less severe events than those defined under design bases accidents could drive risk, WASH-1400 depicts a strong case for a more complete understanding of the risk profile, as discussed in Section 1 and 2 in this publication.

In line with internal events WASH-1400 attempted to estimate the contribution from internal fire and external events, by applying the simplified methods that mostly resulted in the conclusion that these posed small risk contributions when compared to internal events [21]. Similarly, the treatment of Level 2 PSA aspects in WASH-1400 is considered outdated by current standards and the study was focused on radiological releases from reactor core accidents. However, the overall framework and several of the terms traditionally used in PSA today were established and applied in WASH-1400.

Later additional PSA studies worldwide highlighted that the contribution of external events may not be as low as WASH-1400 had indicated and that their individual quantitative results would be site specific. In addition to external events, the extension and adaptation of the PSA framework to the consideration of plant risk from multiple plant operating states (i.e. low power and/or shutdown, LPSD) also became the focus of more concentrated efforts (see [26] and [27]).

In 1986, the US NRC published another seminal study, NUREG-1150 [23], as essentially an update to WASH-1400 with significant advances in multiple areas. This publication assessed the risk from severe accidents at five commercial nuclear power plants in the United States of America at a time where PSA methods were shifting from theoretical to actual implementation in regulatory issues. NUREG-1150 provided a more comprehensive framework for the development and quantification of Level 1, 2, and 3 PSA methods and techniques; including what it defined as ‘risk integration’ of the overall results and insights (as well as a more detailed uncertainty analyses). While internal fire and seismic risk contributors were considered quantitatively, other external events were assessed with bounding analyses and screened out based on low frequency estimates (shutdown risk was not addressed). The enhanced level of detail and realism added to NUREG-1150, in comparison with WASH-1400, was indicated as

a main benefit to the integrated nature of the approach (essentially, risk aggregation), especially in terms of providing guidance to decision making and where resources to improve nuclear safety is to be allocated (without the need for great precision in PSA results). In many ways, NUREG-1150 still represents the current state of the art of full scope PSA issues for the United States of America, as no specific regulatory requirement for such models exists for the large number of reactors currently in operation (despite extensive present use of PSA Level 1 in both licensing and oversight aspects). This will be eventually supplanted once the US NRC completes its most recent effort to update NUREG-1150 insights [24].

Since NUREG-1150 has been issued, multiple individual areas of PSA modelling and development continued expanding. A specific, significant effort was undertaken in the mid-1990s in the United States of America, the individual plant examination (IPE) and individual plant examination of external events (IPEEE) submittals as a response to the US NRC's Generic Letter 88-20, 'Individual plant examination for severe accident vulnerabilities' [25]. Unlike NUREG-1150 (which was a US NRC product), the results from multiple external events from various the United States of America licensee submittals were aggregated and compared to internal events CDF quantitative results in many cases, despite a recognized variation in the level of detail and realism included in the various hazards. This included a more detailed seismic contribution treatment for specific plants, semi quantitative screening methods for internal fire, and various bounding assessments for other external events. NUREG-1742 recognized that not all contributors were treated equally and/or used PSA techniques to quantitatively derive results. One of the objectives of the IPE/IPEEE programme was to obtain a qualitative understanding of the overall likelihood of core damage and fission product releases; with the careful consideration that simplifying assumptions and approximations employed in the analyses may limit quantification insights to general indicators of risk, and is not to be viewed as being well established (although some cases were deemed to apply more rigorous, realistic numerical estimation methods).

3.1.1. Integrated model vs separate models

With the occurrence of the Fukushima Daiichi accident in March 2011, a renewed interest in the characterization of plant risks from various hazards, plant operating states, and radiation sources ensued (among other insights obtained from posterior investigations of the event [28]). In addition, the wider use of PSA technology worldwide means that the principles mentioned in IAEA-TECDOC-1909 [11] and INSAG-25 [29] have increased in importance, i.e. using risk assessment in making safety decisions relating to nuclear installations. Hence, while some form of risk aggregation has been taking place in nuclear power plant risk assessment in the past, the issue of integrating the individual parts of specific risk informed modelling efforts (various hazards, different plant operating states, and multiple sources of radioactivity) will continue to gain importance. The fact that some components of the risk model (or their integration of probabilistic and deterministic aspects) is evolving, is not to be seen as a limitation of risk methods. Instead, this is a natural progression of a more complete overall risk profile. On the other hand, it needs to be recognized that the development of an integrated, full scope PSA model that incorporates highly detailed all hazards, all modes, and all PSA Levels poses resources and technical challenges. Scope and technical limitations imply that this will most likely continue to result in areas where a specific contributor may be treated in a less complete way across the multiple dimensions identified above, inducing PSA heterogeneity which is discussed next.

The term 'integrated' means a model in which individual risk contributors (e.g. internal events versus internal fire) are coupled into a single PSA model (assuming the risk software used

allows for such a model to be built and solved). In this case, any potential interactions between contributors (e.g. seismic induced fires, floods) would have been addressed either explicitly or by screening approaches such that the integration of individual contributors (e.g. fire and seismic) would provide a full risk profile of these hazards.

For the total risk T^R at a certain level (considering different PSA levels) the risk aggregation may be related to multiple dimensions, where the objective is to incorporate as many of these multiple dimensions as possible. For the general or global aggregation of all risk contributors to the total risk T^R the following example and notation may be used:

$$T^R=G(U_i(H_j(S_k))) \quad (1)$$

where G represents the function of general or global aggregation.

This means that in an integrated risk model with risk contributors from separate models or dimensions (where indices i, j, k expresses the specific or cumulative number of considered alternatives in different dimensions), the risk from each unit U_i is aggregated after the aggregation each hazard H_j and from each plant operational state S_k (i.e. all modes are aggregated first, with all hazards next, and, finally, all units).

A separated model, unlike an integrated model, would have each contributor calculated in a separate logic structure where the results are aggregated at the total risk level for that contributor. For example, for a single unit, at power Level 1 internal events, fire, and seismic PSA models built and quantified separately (not including other sources), $G(U_i(H_j(S_k)))$ could be collapsed into $G(U_1(H_j))$, with i = 1, 2, 3 as follows $G(U_1) = CDF_{INTERNAL} + CDF_{FIRE} + CDF_{SEISMIC}$. Similar to the integrated model, potential interactions between contributors such as seismic induced fires, for this example, would have been addressed either explicitly or by screening approaches to estimate the additional contribution of $CDF_{SEISMIC\text{-}FIRE}$, as needed. Note that these separate models may not immediately produce additional integrated results such as combined minimal cutsets and importance measures in an integrated approach. Despite the complexities and given the current computer power capabilities use of integrated PSA models is preferable for risk aggregation and for providing adequate input for the decision making process.

3.1.2. Heterogeneity in the models

In this context the heterogeneity is understood as a measure of the difference in level of realism and maturity among different analysis areas (e.g. hazards, plant operational states) which may have implications for both the quantitative and the qualitative aspects of interpreting aggregated PSA results.

As mentioned in the brief historical overview above, understanding the contribution from multiple challenges to nuclear installation safety has been a long standing goal with regards to nuclear safety. As PSA methodologies and implementation evolved for the last decades, progress on additional modelling and quantification of various phenomena and applications expanded, albeit at different levels of detail and implementation. The reasons for this heterogeneous level of development are varied and can range from an initial rudimentary understanding of the potential risk of a particular hazard to the level of regulatory policy and requirements driving the use of PSA. Understandably, Member States with extensive experience with PSA will have undergone some of the evolutionary process in developing a more inclusive and integrated PSA, while others will benefit from the lessons learned from the wider international experience as they begin to implement and apply the RIDM infrastructure

needed. In either case, the interest in achieving a balanced, realistic, and well integrated model is to be a common goal and addressing risk aggregation is an important component in achieving this objective.

As discussed in Section 2, heterogeneity is defined here as some measure of the difference in level of realism and maturity among different analysis areas (e.g. hazards, plant operational states) which may have implications for both the quantitative and the qualitative aspects of interpreting aggregated PSA results (see Section 2.3). For example:

— Modelling of seismic contributors in PSA has evolved significantly over the last three decades. A seismic PSA that meets current good practices and standards may or may not be available with respect to a PSA standard compliant model, peer reviewed against current requirements;
— Risk-informed applications in some Member States may rely on bounding assessments intended to show that at least two independent trains of safe shutdown equipment would remain available with or without quantification via the estimation of the ground motion capacity of individual components.

Some of these issues may not be easily quantified (i.e. it may not be as simple as assigning a wider uncertainty distribution as questions on the representativeness of the single total output may even raise whether the point estimate represents a mean or a more bounding percentile). Even assessing the impact of heterogeneity in a qualitative manner may not be straight forward as this may depend on the level of detail needed for the specific decision for which the PSA results are being used (the higher the implications of the decision, the higher the need for results that do not have wild variation in terms of heterogeneity). The fundamental issue is that: some heterogeneity will always exist in PSA modelling as it is not possible nor desirable to treat every risk contributor to an artificial high level of quality. In this respect, understanding the individual components of PSA, their heterogeneity, and how it affects decision making is more important for assessing the confidence in the PSA output than obtaining the quantitative results themselves.

3.2. GENERAL STEPS OF RISK AGGREGATION

The discussion presented in this section is focused on general aspects of risk aggregation approaches for quantitative risk assessment (i.e. mainly on quantitative PSA part) that follows standard guidance and good practices with respect to the technical adequacy of PSA model development. In this sense, results and risk insights from PSA models that meet international safety standards and good practices (e.g. [1]–[3]), as well as any applicable individual Member States standard (e.g. [4]), are expected to be available prior to considering risk aggregation aspects.

As such, the following sections will discuss some general aspects of current practices that provide insights in the consideration of integrating risk information from the specific contributors: multi source, multiple hazards, and various plant operating states. The intent is to highlight some of the insights and approaches obtained from specific experiences, in light of the above discussion in prior sections that will be elaborated further in the following sections.

It needs to be noted that the interrelationship between each of these contributors is also acknowledged. The consideration may or may not include variously affected multiple sources of radioactivity (e.g. a natural hazard induced event that impacts multiple units in various

operating/shutdown modes while also impacting non reactor sources of potential radiation releases).

As it was mentioned above the total risk T^R could be represented as $G(U_i(H_j(S_k)))$, the risk aggregated risk across multiple dimensions. While this implies that the full scope PSA will have a large number of risk contributors that need to be considered for a more integrated risk profile (which may or may not be risk significant), in this publication they are discussed in three separate subsections (3.2 – 3.4) with respect to:

— Radiological sources (reactor core, spent fuel pool, dry fuel storage);
— Various hazards (entire spectrum of internal events, internal and external hazards);
— Operational states (full power operation, low power, shutdown, start up and other operating states).

Considering the variety of PSA models and their development approaches (separate, joined) and possible heterogeneity with respect to the level of realism, types and degree of approximations, and treatment of uncertainties (e.g. full quantification of uncertainty, using only point estimates) for the different contributors and risk measures, the following steps could be distinguished to generalize the workflow for risk aggregation in case of integrated or separate models. These three steps (phases or stages) are shown in Fig. 3. below and are listed and discussed shortly as follows:

— Step 1. Risk quantification in PSA models. This step implies that the total (aggregated) risk induced by all risk contributors that are incorporated in a common PSA models need to be quantified.
— Step 2. Aggregation of results and their uncertainties, if they are available. This step may include the following substeps:
    - Aggregation of results, having distributions which reflect uncertainties;
    - Aggregation of results expressed only by point estimates.
— Step 3. Representation and interpretation of results. Within this step both quantitative and qualitative aspects of risk aggregation need to be presented (see Section 2.3.).

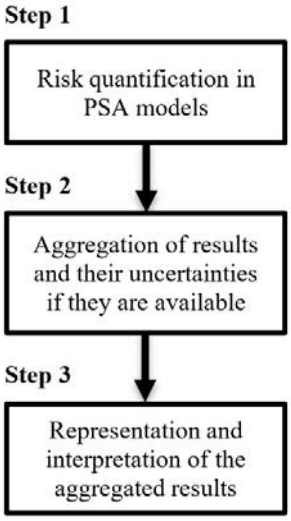


FIG. 3. General workflow for risk aggregation.

It is necessary to highlight that above mentioned Steps are valid both for integrated and separated PSA models, however for integrated model, Steps 1 and 2 are lumped in one single step.

3.3. MULTI SOURCE RISKS

Multi source is a general term encompassing nuclear installations [5], uses of all sources of ionizing radiation, all radioactive waste management activities, transport of radioactive material and any other practice or circumstances in which individuals may be exposed to radiation from naturally occurring or artificial sources. In the context of multi source considerations, the risk aggregation implies the combined representation of risks coming from different sources of radioactivity available at the site (e.g. reactor units, spent fuel pools, dry fuel storage and others). This is important in terms of addressing whether, for specific hazards, the aggregated multi source risk value exceeds criteria established for a site level (e.g. dose limits), which might not be identified under single unit assumptions.

As mentioned in Section 2.2, single unit risk metrics (e.g. CDF, LERF) may not be sufficient for all risk aggregation purposes and, therefore, additional risk metrics are needed. The IAEA Safety Reports [30] and [31] and the ASAMPSA_E publications [32] and [33] defines several risk metrics to complement the traditional PSA metrics that are associated with single unit PSAs. The summary and applicability of the proposed risk metrics is presented in Table 1.

TABLE 1. SUMMARY AND APPLICABILITY OF RISK METRICS[12]

PSA SCOPE / **RISK METRICS**	**Single unit[13]**			**Multi source (in single site)**		
	L1	L2	L3	L1	L2	L3
Core Damage Frequency (CDF) [14]	+					
Large [Early] Release Frequency (L[E]RF)		+				
Site Core Damage Frequency (SCDF)				+		
Single Unit Core Damage Frequency (SUCDF)	+			+		
Multiunit Core Damage Frequency (MUCDF)				+		
Site Fuel Damage Frequency (SFDF)				+		
Single Source Fuel Damage Frequency (SSFDF)[15]				+		
Multi source Fuel Damage Frequency (MSFDF)				+		
Instantaneous severe accident frequency (ISAF)[16]				+		
Single Unit Release Category Frequency (SURCF)[17]		+				
Multi-Unit Large [Early] Release Frequency (MUL[E]RF)					+	
Site Large [Early] Release Frequency (SL[E]RF)					+	
Site Release Category Frequency (SRCF)					+	
Site Very Large Release Frequency (SVLRF)[18] [32] and [33]		+			+	
Complementary Cumulative Distribution Function (CCDF)			+			
Site Complementary Cumulative Distribution Function (SCCDF)						+

[12] Definitions of the multi-unit and site level risk metrics can be found in [30], [31], [32] and [33]. It needs to be noted that the risk metrics presented in Table 1 are overlaping and their selection depends on the intent of the PSA.
[13] Single unit in this context refers to the nuclear reactor only, relevant metrics do not cover sources of radioactivity other than reactor core such as the spent fuel pool and other radiological sources.
[14] In some Member States (e.g. Russian Federation), severe accident frequency is used as the risk metrics for fuel damage in reactor core and corresponding spent fuel pool and other fuel locations related to that particular reactor.
[15] the frequency per site year of an accident involving fuel damage from a single source on a multi-unit site
[16] ISAF – the frequency per reactor year of severe accident (reactor core, SFP, DS), calculated on the assumption that the state of the nuclear power plant at a given time will be unchanged during the year. (see details in Annex III)
[17] SURCF – the frequency per site year of each distinct release category for a Level 2 SUPSA given a release from one and only one reactor on mutli-unit site.
[18] SVLRF need to be used by defining a very large release threshold, for which there is no harmonized approach available. As an example, it might be considered to set the threshold to 500 PBq I-131 (or equivalent) based on [35] (see page 17).

It needs to be noted that there is no single approach or method available that applicable to all RIDM applications. For example, in order to understand the development of the total site risk estimate, a site with three sources of radioactivity can be considered: Unit 1, Unit 2, and a SFP [34]. In this case, there are seven possible outcomes that involve release from one or more units, as listed below:

— Single source outcomes: (1) undesired end state at Unit 1 only, (2) undesired end state at Unit 2 only, (3) undesired end state at SFP only;
— Dual source outcomes: (4) undesired end state at Unit 1 and Unit 2 only (i.e. no undesired end state in SFP), (5) undesired end state at Unit 1 and SFP only (i.e. no undesired end state in Unit 2), (6) undesired end state at Unit 2 and SFP only (i.e. no undesired end state in Unit 1);
— Triple source outcomes: (7) undesired end state at Unit 1 and Unit 2 and SFP.

The various outcomes can be depicted on a Venn diagram presented in Fig. 4 [34].

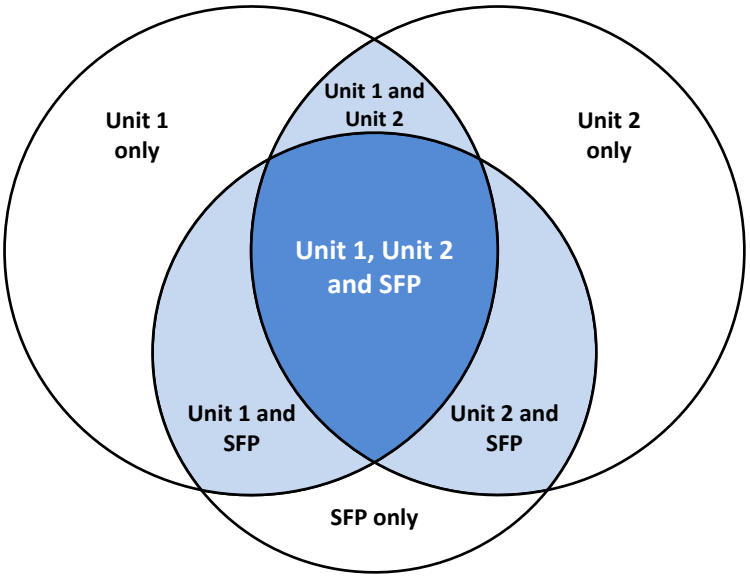


FIG. 4. Diagram depicting multi source accidents.

With each event being assumed as disjunctive, the total probability of having an undesired end state at the site is the sum of the probabilities of all these terms. In general, for a site that has n sources the number of outcomes that involve exactly k out of n sources is:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{2}$$

For a site with n sources, $2^n - 1$ disjunctive events need to be considered if all possible combinations need to be explicitly determined for calculating a site risk measure. For sites with many sources this will be an incentive for more conservative and bounding approaches instead of a rigorous investigation of all potential interdependencies [34].

3.3.1. Integrated vs separated model

Traditional PSA models typically consider each reactor separately when multiple reactors are located in the same site. Multi source risk aggregation using separate PSA models for different sources may not be always practical. When attempting to aggregate risk on the basis of single-

source PSA models, care needs to be taken to justify that all of the important dependencies, interactions and qualitative considerations are properly addressed and the scenarios affecting (at least partially) various sources are not double counted. Omitting some of the dependencies and interactions could lead to the over- or underestimation of the multi source risk profile, which is the main output from risk aggregation to the decision makers. Despite the fact that there is a limited experience in the field of multi source PSA, there are different approaches on integration of individual PSA models.

The approach proposed in [30] implies direct combination of accident sequence models for different units, which is illustrated for the example of a station blackout (SBO) scenario for two identical units (see Fig. 5).

Another approach is used by US NRC in Level 3 PSA project for Vogtle NPP [36]. This approach implies constructing multi source PSA model as a large fault tree, starting with the top level 'AND' gate combining end states for selected radiological sources (see Fig. 6). Mid level 'OR' gates combine selected accident scenarios for each selected radiological source. The bottom level AND gates combine basic events for each selected accident scenario for each selected radiological source.

Three approaches have been proposed for use by IAEA/NSNI project on MUPSA [31]. For instance the hybrid approach proposed in [31] implies transformation of the accident sequences with undesired end states (e.g. core damage) to the fault trees, which could be later used as references for function events in the multi source event tree for the whole site. Similar approach has been applied for the pilot MUPSA study for the Paks NPP, Hungary [37] (the conceptual approach is presented in Fig. 7).

The advantage of the approach IAEA MUPSA method is that it accounts for moderate complexity while allowing the risk analyst to cover two or more sources of radioactivity in an integrated PSA model. The dependencies and interactions between the sources considered need to be covered in the level of fault trees connected to the master event tree. The approach could lead to challenges in terms of long computational time and need for the simplification of the fault trees. The main efforts within this approach are expected to be spent on converting event trees to fault trees and addressing the dependencies (e.g. common cause failures, CCFs) in the level of fault trees. The other challenge related to this method could be the size of the integrated model, which could create obstacles for effective use of PSA software.

It needs to be noted that, for non NPP installations; the sources of radioactive releases may be different. Understanding the release path and the accident scenarios that deal with such applications may not involve reactor cores in full power operation and, therefore, the availability of the radioactive material and the types of relevant hazards, accident scenarios, and releases may require different methods and tools. However, if Member State regulations require an integrated understanding of the overall risk profile of such installations (where multiple releases are possible); then a similar logic to the one discussed above may apply.

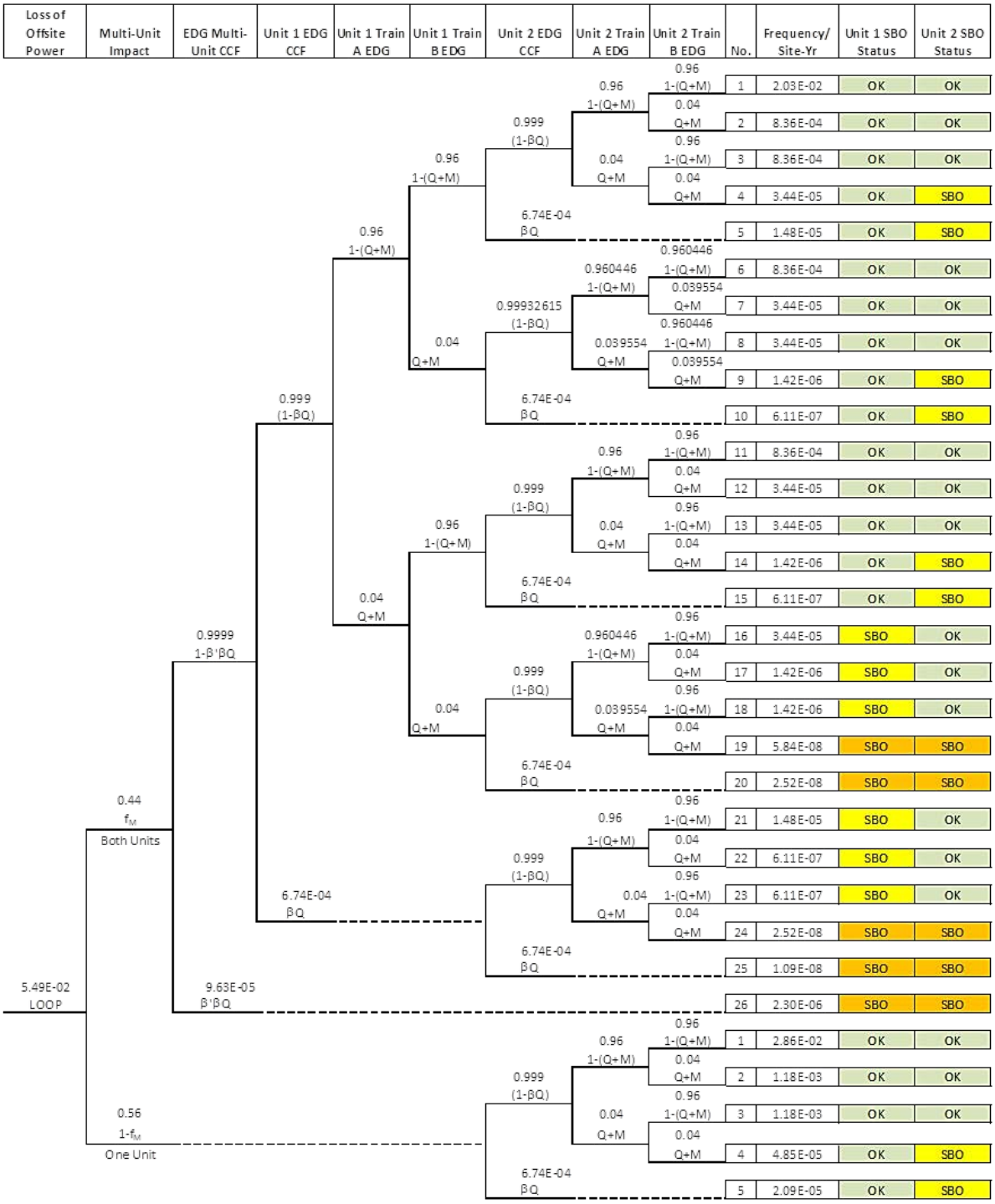


FIG. 5. Event tree for multiunit loss of offsite power and station blackout.

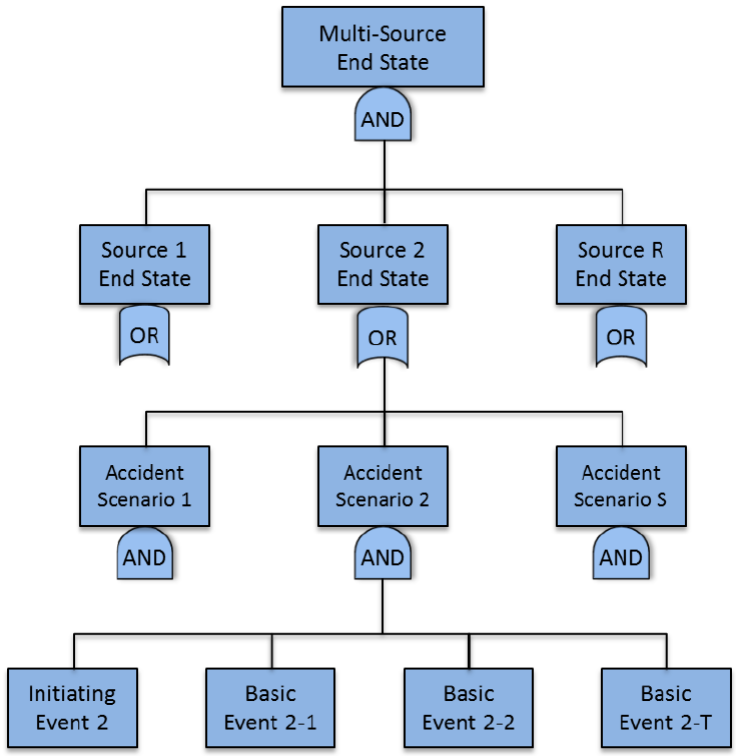


FIG. 6. The concept of using large fault tree for construction of multi source PSA model.

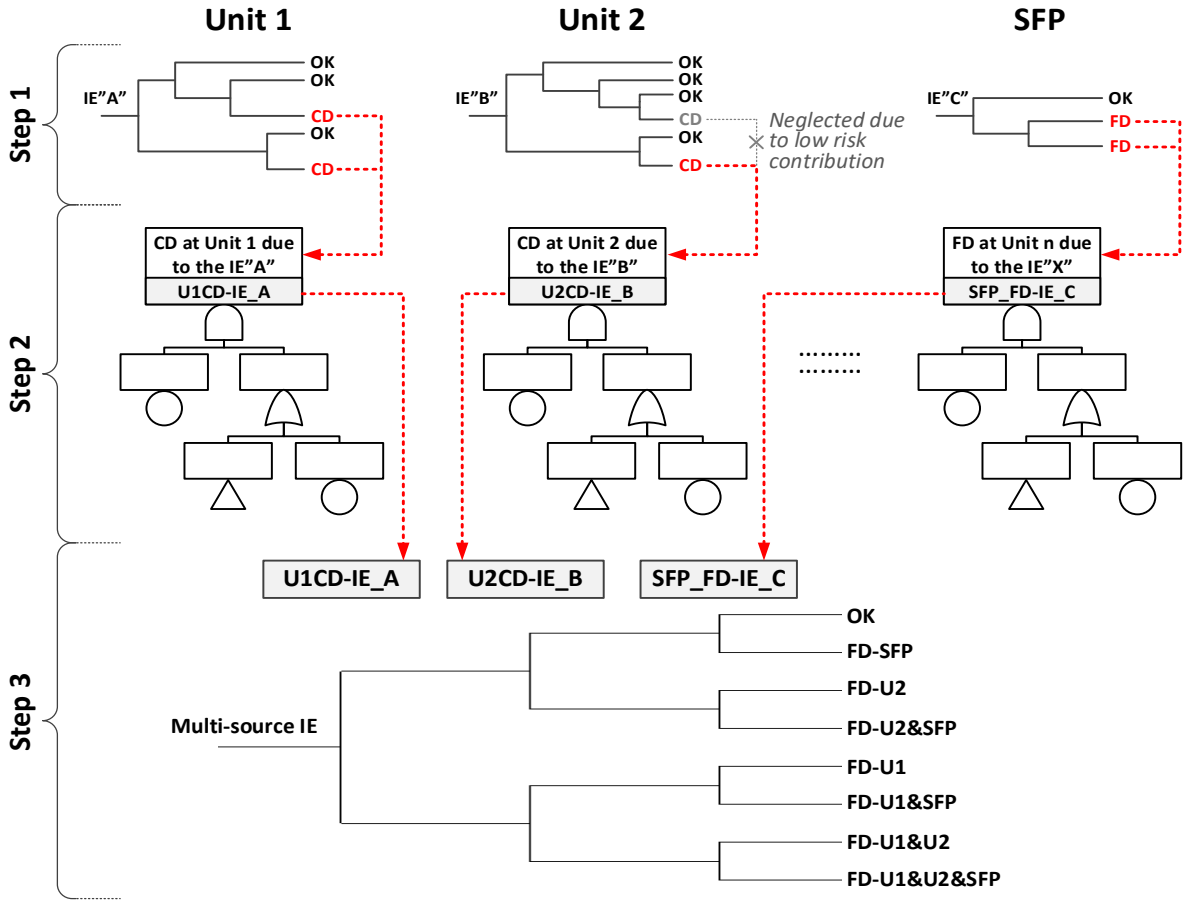


FIG. 7. The concept of hybrid approach.

3.3.2. Heterogeneity in the models

As it was stated above, the prerequisites of multi source PSA are PSAs of individual nuclear installations (reactor unit, SFP, DS). However, the level of detail and scope of the individual models are often very different in nature (see an example on Fig. 8 [38]). In addition, it needs to be mentioned that the specific sources could be in principle screened out from further analysis based on defined and well justified criteria (e.g. connected with the radioactive release levels).

Another obstacle in this context for risk aggregation is the fact that different installations have different success / failure criteria as well as different definition of undesired end state. For instance, reactor core damage is frequently defined in connection with the maximum cladding temperature of 1200°C, whereas fuel damage in the SFP is usually postulated in case of fuel uncover and or mechanical fuel damage due to the inappropriate fuel handling. Therefore, aggregation can be performed more directly on the releases (Level 2 PSA) and the consequences (Level 3 PSA) but may be less meaningful or incorrect for Level 1 PSA metrics.

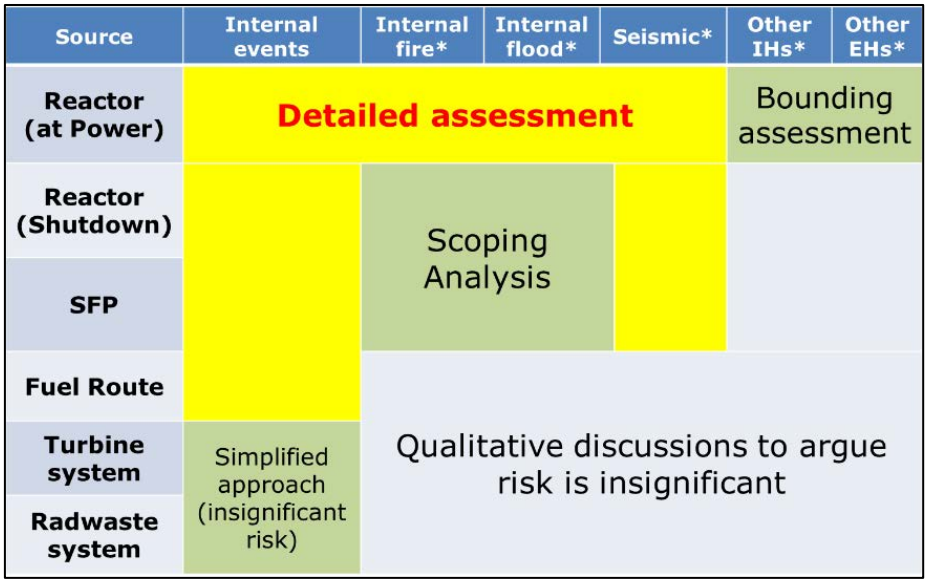


FIG. 8. Scope of UK Advanced BWR PSA during the GDA phase.

Thus, even if aggregation is performed for different installations having different definition of undesired end state, the above mentioned qualitative features of aggregated risk need to be communicated to the decision maker for further consideration (see Section 4 for more details).

3.4. RISKS FROM VARIOUS HAZARDS

The IAEA Safety Glossary [5] defines hazard as the potential for harm or other detriment, especially for radiation risks; a factor or condition that might operate against safety. 'Hazard group' refers to a collection of hazards that are assessed in the PSA using a common approach, methods, and data, while a 'hazard' is the specific phenomenon that puts the plant at risk. The SSG-3 [2] and IAEA-TECDOC-1804 [4] provide the concept of 'hazard' phenomenon, where the 'hazard event' is defined as an occurrence of the phenomenon of a specific severity that could potentially result in the initiating event. In this context, SSG-3 [2] states:

> "An initiating event is an event that could lead directly to core damage (e.g. reactor vessel rupture) or that challenges normal operation and which requires successful mitigation using safety or non safety systems to prevent core damage".

In addition to this definition, which is limited for NPPs, Thus, the 'hazard event' is considered to be a cause of an initiating event representing the effect it has on the nuclear installation [4]. The term 'hazard' will be used in the remainder of this section to discuss these concepts with respect to risk aggregation. In addition, this section discusses risk aggregation aspects related to hazard events or hazard groups that includes internal events.

3.4.1. Integrated vs separated model

The Level 1 PSA model for internal events is usually the starting basis for developing PSA models for other hazards. Consequently, the availability (or development) of the Level 1 PSA model for internal events is a prerequisite for developing other portions of the PSA model (e.g. internal fire, internal flooding, external events). However, the different hazard groups are generally quantified separately, i.e. individual PSA results are usually constructed as individual models or model parts and its outputs are evaluated separately (e.g. risk metrics, minimal cut set lists, importance measures). As discussed earlier, the PSA team may follow the individual stand alone hazard modelling approach or choose to develop an integrated PSA model. Such an integral model incorporates all the different hazard groups and quantifies risk results under a single model. Various reasons can motivate the decision on using separate PSA models, such as the evolution of PSA development and implementation in a specific Member State (as discussed in section 3.1), feasibility of quantification using a single analysis PSA software tool (which can require significant pre- and/or post processing, typical for several initiating events other than internal events), and the difficulties in managing and extracting meaningful results from a large size integrated PSA model.

With respect to risk aggregation for different hazards, integrated PSA models have meaningful implementation and quantification advantages over separate PSA models for risk aggregation purposes.

If all the hazard groups are modelled within an integrated PSA model, the harmonization of the logic structure and reliability data of all components for the various hazards may be better coordinated than in individual hazard stand alone models. Also, modifications, refinements or upgrades made in any part of the PSA model are applied automatically to all relevant hazard groups. However, integrated PSA models may become overly complex if not implemented properly, which. Additionally, a large integrated model's quantification may take a considerable amount of time.

There are also specific analysis methods and associated algorithms that may not be implemented in contemporary PSA software so that a single analysis tool can be applied commonly for all the hazard groups. For example, convolution of hazard curves and fragility curves need to be performed for an adequate analysis of most external hazards, although not all PSA software packages may necessarily have this capability, especially if one intends to use the continuous hazard and fragility functions for the whole hazard intensity range, as opposed to using a coarse partitioning.

In contrast to integrated PSA models, it is easier to keep the size of the separate models which makes it easier for managing and quantifying the model within a PSA software tool. Also, the limitations of a PSA software package can be overcome by developing pre- or post processing tools to enable the use of some special analysis methods exemplified earlier (i.e. the convolution of continuous hazard curves with continuous fragility curves). On the other hand, a modification that has general implications (e.g. update of the component reliability data using recent plant specific data) may require multiple, repetitive manual changes in each stand alone PSA model

(which increases the use of resources and creates the possibility of introducing errors) unless they can be automated in some form.

If an integrated PSA model is developed for all the hazard groups, and model quantification is feasible for all hazards within the boundaries of the applied analysis tool, risk aggregation, including the associated uncertainty analysis, can be performed adequately and directly by applying the same PSA software package used for risk assessment without a need for further efforts to be spent on obtaining aggregated results. This is highly beneficial in case of risk applications requiring many calculations or online calculations (e.g. risk monitor). Aggregation can be completed by collecting and collectively quantifying all those relevant accident sequences the risk is intended to be aggregated for.

Individual PSA models can also be used to obtain appropriate aggregated results. The use of separate PSA models for the different hazards also requires a dedicated tool for aggregating the results, depending on what PSA outputs are being used. For example, when calculating the overall risk results separately (e.g. CDF from internal events and multiple hazards) different probability distributions need to be aggregated in an appropriate manner (e.g. via Monte Carlo sampling). In this case, the distributions are typically added probabilistically, which may require a post processing action. This approach is different form the analysis of more detailed PSA model outputs such as minimal cut set lists, unless a special post processing tool is developed and used that is capable of aggregation based on the use of the minimal cut sets with their frequencies, as opposed to handling merely the distribution functions. Consequently, when the distribution functions representing of the different hazard groups are summed without taking into account the minimal cut sets that contribute to the risk measure in question, the outputs associated with specific inputs (e.g. component failures that contribute to more than one hazard) may result in inaccuracies[19]. This may cause some (but usually not serious) imprecision in the uncertainties of the results. On the contrary, the use of an integrated PSA model enables uncertainty analyses so that all hazards are considered simultaneously, and the probabilities of random component failures that appear in the PSA models of different hazard groups are taken into account in an appropriate manner.

3.4.2. Heterogeneity in the models

There can be significant differences in the supporting analyses performed and modelling assumptions made in the development of accident sequence models for different groups of hazards. Varying levels of realism may be introduced, as well as approximations generally present in deterministic analysis (e.g. in thermal hydraulic models, structural reliability analysis, modelling of complex natural physical phenomena), data assessment, and expert judgments used within the risk assessment for the different types of hazards, resulting in various possible impacts to the aggregated results as a function of the extent and magnitude of these potential biases. The reasons for this are manifold and are not discussed further in this publication (for details see [17]). It needs to be noted that this heterogeneity in hazard assessment is an inherent aspect of integrating different phenomena and plant responses and is not to be viewed negatively (i.e. homogeneity may not be feasible nor something that needs to be always imposed or strived for). In fact, the extent and level of approximations may provide sufficient confidence in the results where no additional refinements are needed. For example:

[19] According to NUREG-1855, it is important to consider the state of knowledge correlation between events, i.e. for a failure parameter the same value needs to be taken into account in all minimal cut set in every uncertainty calculation. This cannot be ensured when only distribution functions are aggregated mathematically.

— The risk contribution due to a specific hazard group is sufficiently low such that additional refinements would be too resource intensive to alter the risk insights that could be obtained from the model, i.e.:
  - Either because they do not change the overall risk aggregation significantly nor provide additional insights into plant behaviour, or
  - Because there is not a sufficiently mature methodology available such that additional short term efforts will not produce better refinement);
— In some cases, only the quantification of point estimates may be feasible by applying a conservative assessment without quantitatively describing the uncertainties in the risk measure in question (e.g. bounding assessment for some newly introduced hazards such as water intake blockage induced by industrial oil releases).

Although uncertainty assessment is usually performed for most of the hazards, the quantification of the uncertainty parameters for some hazards may be limited or simplistic (e.g. appropriate data is unavailable). In summary, risk needs to be well understood when making decisions based on risk aggregation results. Taking into account the facts that stand alone PSA models may be applied, and risk assessments show substantial heterogeneity with respect to the level of realism, types and degree of approximations, and treatment of uncertainties for the different hazard groups, some practical steps are needed for aggregating risk from different hazards. These steps are shown schematically in Fig. 9 and are discussed briefly below.

3.4.2.1.Step 1. Risk quantification in PSA models.

Risk aggregation for different hazards begins with the quantification of the total (aggregated) risk induced by all the hazards that are incorporated in a common PSA model and uncertainty assessment had been performed thereto[20]:
— This analysis needs to be performed for PSA model representing the different hazard groups (could be an integrated PSA model or for each separate model if the integral model is not available)[21];
— Risk summation can be completed by collecting and jointly quantifying all relevant accident sequences within each PSA model;
— Quantification of the collected accident sequences needs to ensure mathematically correct calculations of importance and sensitivity measures as well as uncertainties relevant to the hazard group as a whole (similar to the quantification of individual hazard groups);
— When propagating uncertainty using individual stand alone PSA models, a set of probability distributions for each hazard group for the risk measures considered will be obtained and steps 2A and 2B needs to be performed next;
— If an integrated PSA model is developed for all the hazard groups, and model quantification is feasible within the PSA software tool for all hazards aggregated, then the results (including the associated uncertainty analysis) are immediately available without the need for performing Steps 2A and 2B.

[20] It is important to assure the compatibility of the models (level of details, having the same plant condition reflected).
[21] As it was already stated above, the mentioned steps are valid both for integrated and separated PSA models, however for integrated model, Steps 1, 2A and 2B are implemented automatically typically using the computer software where the PSA model is constructed. Thus, from this perspective the application of integral models is preferable.

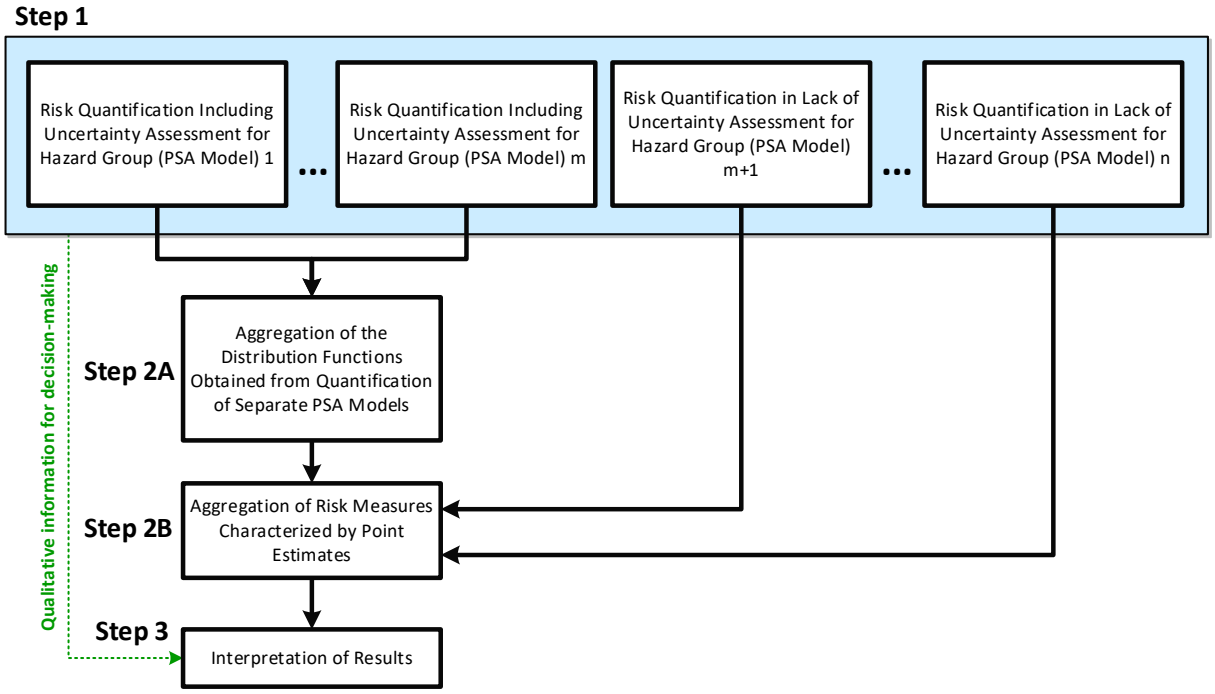


FIG. 9. The process of risk aggregation of various hazards.

3.4.2.2.Step 2A. Aggregation of the distribution functions obtained from quantification of separate PSA Models

In the next step of the risk aggregation process for different hazards, the distribution functions obtained in Step 1 for the hazard groups assessed in separate PSA models need to be summed up using the methodology described in Section 2. A dedicated software tool capable of aggregating the different distribution functions may be needed to perform this step (e.g. via Monte Carlo simulation) unless the PSA software used has this capability. It is again noted that the aggregation of the results from the individual stand alone PSA models numerically may not account for the impact on the minimal cut set logic which may or may not influence the overall results by not handling correctly the probabilities of random component failures that have some meaningful contribution to the risk induced by more than one hazard. This limitation could be overcome by developing and using a special post processing tool that is capable of aggregation based on the use of the minimal cut sets including their frequencies rather than just handling distribution functions.

In summary, the result of this step of aggregation is a single numerical result with an associated uncertainty distribution that reflects the aggregated risk for those hazard groups explicitly modelled.

3.4.2.3.Step 2B. Aggregation of risk measures characterized by point estimates

This step includes aggregation of point estimates to the distribution function computed in Step 2A from those hazards or hazard groups that have not been subject to quantitative uncertainty analysis in PSA. Point estimates are typically conservative (bounding) values but could be the result of best estimate assessments as well. Adding these point estimates shifts the results via simple addition but will not incorporate the individual uncertainty information and its subsequent impact to the uncertainty distribution of the overall aggregated risk result.

This method (i.e. shifting the distribution function) results in mathematically correct risk estimates only if the point estimates represent mean values (without having uncertainties). If the point estimates do not represent mean values, the expectation is that they are bounding If the impact is limited (i.e. orders of magnitude lower than other dominant hazards), then the resulting contribution to risk aggregation will be limited. Otherwise, it may be more prudent to consider whether a bounding estimate is particularly appropriate to capture the overall risk profile for that specific hazard.

Consequently, shifting the distribution function in this manner is seen sufficiently justified, more importantly, it is in line with the approach to sum risk results from individual hazards. In addition, if a common PSA model incorporates hazards lacking quantitative uncertainty assessment as well as hazards with quantitative uncertainty assessment, this shift may be done in Step 1 by collecting and jointly quantifying accident sequences related to both categories of hazards. Another approach could be to introduce an uncertainty distribution for the risk estimate relevant to the hazard characterized by only a point estimate originally, and sum the newly introduced distribution function with the results obtained from Step 2A (in a same manner as presented in Step 2A). However, choosing a probability distribution to introduce an uncertainty characterization in a point estimate value needs to have sufficient technical bases (i.e. introducing arbitrary distributions will ultimately not improve the uncertainty characterization).

3.4.2.4.Step 3. Interpretation of results

The distribution function representing aggregated risk from all the hazard groups can be developed by performing Steps 1 to 2B. However, it is essential to understand and document the expected heterogeneity in the aggregated assessment and in the results for the different hazard groups in an appropriate level of detail and depth (e.g. commensurate with the potential impact to the overall risk aggregated results). Most importantly, the degree of realism as well as the assessment of uncertainties (e.g. comprehensive or limited, qualitative and/or quantitative) is to be considered for each hazard group.

The assumption of independence is often applicable for single hazards, however, this assumption may not be appropriate when modelling combinations of hazards (e.g. a seismic model and a fire model, as opposed to a seismically induced fire model). The approach to ensuring the independence of a combined hazard model from the single hazard models that are incorporated within the combination is dependent on the hazard assessment technique, but is generally a complex task (see Section 6 on challenges in risk aggregation).

For example, assume that event logic models are developed for high wind, extreme rainfall, and a combination of both. The aggregation of the risk measures from these three initiators needs to account whether they are mutually exclusive initiators or not. In this example the hazard curve considered in the high wind PSA needs to reflect the occurrence frequency of high wind events without any rain. Similarly, the PSA on extreme rainfall needs to take into account the event frequency of heavy rain without strong wind, and lastly the model for the combined hazards would cover the frequencies both hazards occurring simultaneously. Theoretically, use of multivariate hazard functions (hazard surfaces) could yield more detailed results in which marginal distributions for the different hazards would represent single hazard situations, but the use of such an approach is beyond state of the art at present.

A note needs to be made on the aggregation of importance measures assessed for the different hazards. If a single integrated PSA model is developed for all the hazard groups, calculation of importance and sensitivity measures is feasible using the applied PSA software tool. A short

discussion is presented in Section 6 under challenges on approaches applicable to aggregating importance measures without the use of the underlying lists of minimal cut set (i.e. by using pre- or post processing tools), that also addresses the issue of feasibility as well as challenges and difficulties in performing aggregation for the different measures.

Finally, it needs to be noted that non NPP applications will most likely need to address the impact of multiple hazards. For example, fuel cycle facilities need to address hazards initiating internally (within plant operations), as well as externally (e.g. seismic, high winds, external flooding). While the types of accident scenarios and releases may be different than NPP operations, the aggregated risk (if required by RIDM application and/or Member State regulations) may need to be considered.

3.5. RISKS ASSOCIATED WITH VARIOUS OPERATIONAL STATES

Plant operational state (POS) for the purpose of PSA is defined as a plant configuration during which plant conditions do not significantly change (and activities that impact risk are relatively similar). The different POS modelled in a PSA are intended to cover the entire spectrum of plant operation in PSA to ensure its completeness when assessing risk for multiple POSs. The aggregated risk profile can be incomplete and distorted if specific POSs and associated configurations defined in plant technical specifications or specific plant outages are incorrectly translated into the risk assessment [4]. It is noted that site level (overall) POSs are not addressed in this Section, since the risk aggregation aspects are the same for single unit and for multiunit POSs, and the POS identification for multiunit PSAs is not in the scope of this study.

The key differences between different POSs relate to the activities being performed and the plant's ability to prevent an undesired end state. Those differences could be related to, for instance, the availability of safety features (including level of redundancy), success criteria, effectiveness of barriers, operator actions and other aspects.

A POS can be a steady state POS (e.g. full power, low power, hot standby, cold shutdown while on residual heat removal cooling) or can represent a transition phase between steady states. Each POS implies specific duration, plant configuration and safety challenges, that has direct impact on the aggregated risk value for this particular POS. Hence, different POSs could have very much different risk contribution (see Fig. 10).

The frequency and duration of POSs need to be determined based on relevant plant specific records (such as operating profile, trip history, outage plans, maintenance records, logbooks) and the frequency of forced/unplanned outages and/or power reductions (see attribute OS-C01 in [4]). In the context of risk aggregation, the treatment of the frequency and duration of POSs needs to be done carefully in order to avoid potential double counting. This could be especially challenging for the forced/unplanned outages and/or power reductions.

3.5.1. Integrated vs separated PSA models

The methodologies available at Members States indicates different approaches to plant specific full scope PSA model for different POSs. The usual practice is to begin with a detailed full power internal events model, then supplement it with the wider spectrum of internal and external hazards. Typically, POSs other than full power operation are included only after the first or second step are taken, (usually first for internal initiating events and then supplemented by a wider spectrum of internal and external hazards). Eventually, the PSA models could be integrated in one model or kept as separate models for different POSs (usually separate model

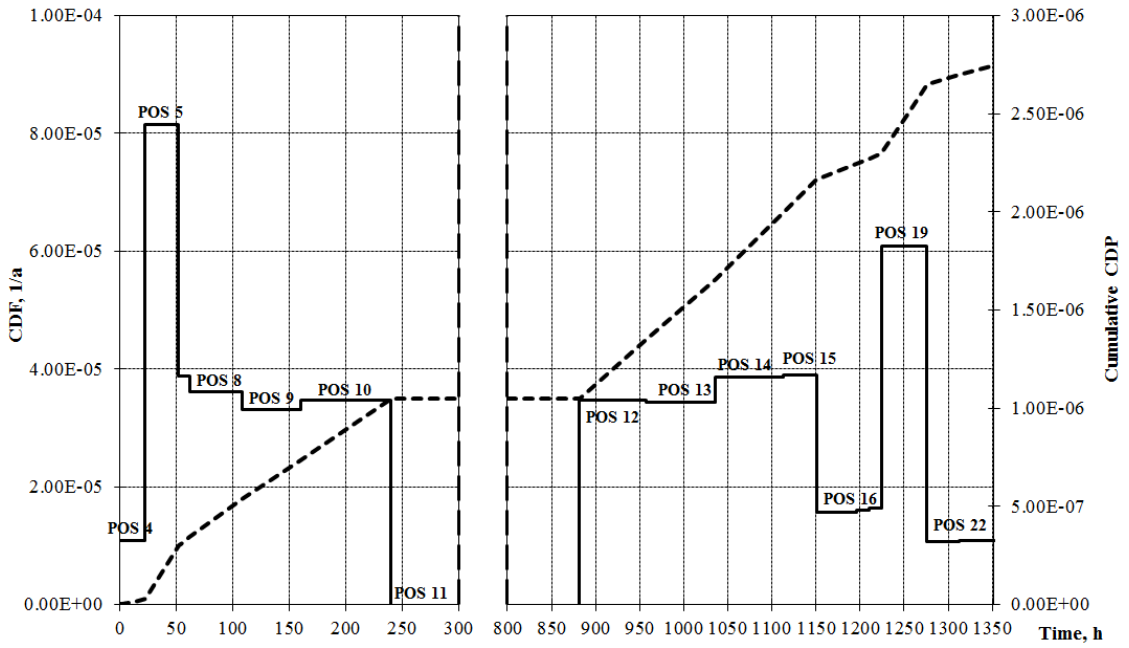


FIG. 10. Illustration of risk in different POSs modelled in low power and shutdown PSA.

for full power and separate one covering low power and shutdown modes). Either way the overall concept of aggregation of various risk contributors in terms of different POSs is the following (for Level 1 PSA):

$$CDF(total) = \sum_{i=POS1}^{POSx} \omega_i CDF_i, \text{ given that } \sum_{i=POS1}^{POSx} \omega_i = 1 \quad (3)$$

where

ωi – the relative duration of POS_i;

CDF_i - core damage frequency (expressed in unit: 1/calendar year) associated with POS_i (including consideration of entire spectrum of hazards);

x – total number of POSs considered in the PSA.

In the context of risk aggregation, the advantages and disadvantages of integrated vs separate PSA models for different POSs are very much in line with the ones described in Section 3.3. Eventually, the integrated PSA models for different POSs provide meaningful implementation and quantification advantages over separate PSA models for risk aggregation purposes (i.e. easier keeping consistency among the POS modelling, avoiding duplication of certain parts of the model for all POSs, automatic generation of aggregated results). Thus, integrated PSA model for different POSs provide the possibility for a more comprehensive uncertainty analysis than the one performed separately. At the same time separate PSA models for different POSs could still be used to obtain appropriate aggregated results. However, risk aggregation that uses separate PSA models need to be done considering possible overlaps and dependencies in order to ensure sufficient delineation between distinct POSs for risk characterization purposes. If the definition of POS groups and determination of the frequency and duration of POSs are implemented in a proper way, independence for different POSs needs to be suitable for the aggregation of mean values and uncertainties of the undesired end state parameter (e.g. CDF, LERF). As for hazards, the issues connected with the aggregation of importance measures could still remain unresolved (see further discussion in Section 6).

3.5.2. Heterogeneity in the models

Since stand alone PSA models may be applied, and risk assessments may involve considerable heterogeneity regarding the level of realism, types and degree of approximations, as well as the treatment of uncertainties in analysing different plant operational states, some practical steps are needed for aggregating risk metrics for POSs. The steps are presented schematically in Fig. 11 and are discussed below in some more detail. It is noted that these steps show substantial similarities to the steps proposed for aggregation of risk from different hazards (see Section 3.3), except for a preparatory step to be taken in risk aggregations for POSs. Moreover, in contrast to Fig. 9, Fig. 11 represents not only the generalized case (i.e. separate PSA models available for the different POSs, some with and others without uncertainty assessment at the same time, illustrated by the subsection with Hazard Groups *k*+1 to *m* in Fig. 11), but it separately shows the applicability of the approach if:

— All the PSA models for the different POSs include uncertainty assessment (Hazards Group 1 to *k*);
— Only point estimates are available (Hazard Groups m+1 to n).

The reason for introducing the latter two cases are the principles described in Section 3.1 on first aggregating risk from the different POSs for each hazard separately and subsequently performing aggregation of risk induced by the different hazards. Accordingly, Fig. 11 represents the cases yielding risk measures on hazard groups for all operating states that includes uncertainty assessment (see Hazard Groups 1 to *m* on Fig. 9 and Fig. 11) as well as those that do not include quantitative uncertainty assessment (see Hazard Groups *m*+1 to *n* on Fig. 9 and Fig. 11). This creates a link between Fig. 9 and Fig. 11.

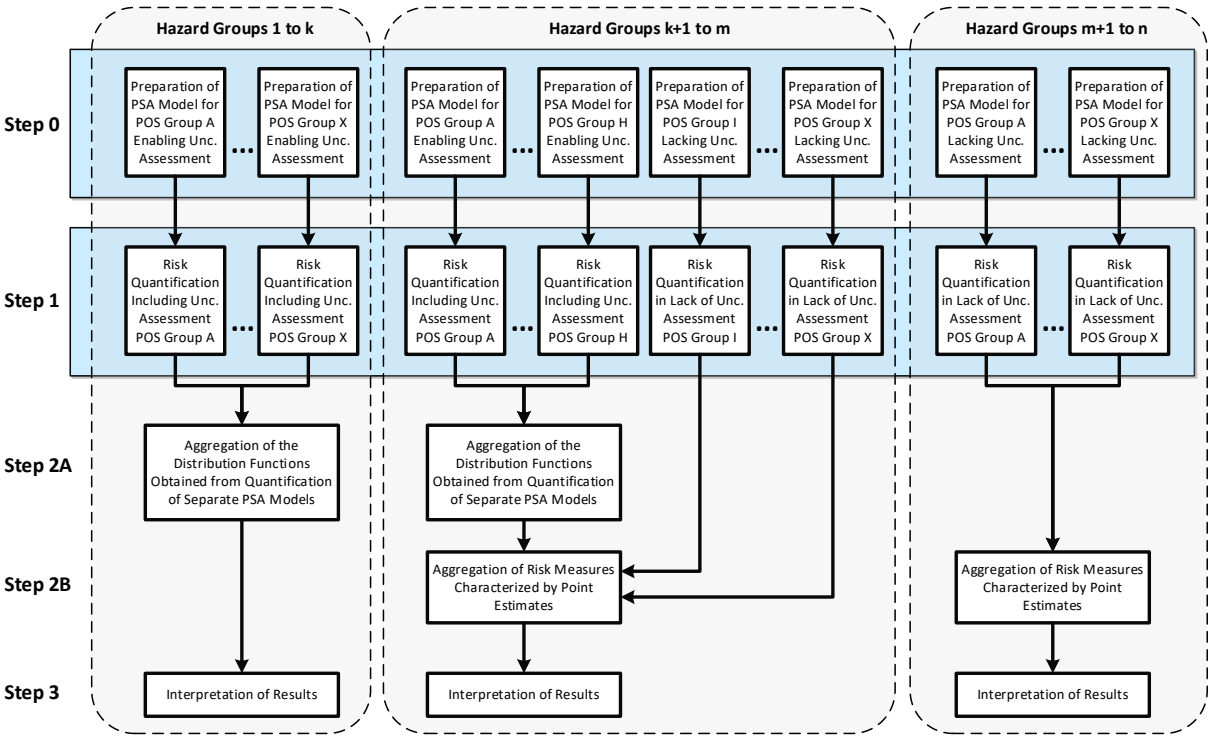


FIG. 11. The process of risk aggregation of various hazards and POSs.

The steps of the proposed approach applicable to risk aggregation for different POSs are as follows below.

3.5.2.1. Step 0. Preparation of the separate PSA models to enable aggregation

As mentioned earlier in this section, risk aggregation for the different POSs is performed by assessing the weighted sum of the risk measure in question for all POSs, where the weights represent the relative annual duration of each POS. Consequently, as a preparatory step to enabling risk aggregation, the annual relative POS durations need to be given in the models.

3.5.2.2.Step 1. Risk quantification in separate PSA models

After the preparation of the separate PSA models for the different POSs, quantification of the total (aggregated) risk representing all the POSs that are incorporated in a common PSA model needs to be performed. This analysis needs to be performed for each and every separate PSA model representing the POS groups, if a fully integrated PSA model is not available. The tasks to be completed and the discussion presented in Step 1 of the approach on hazard risk aggregation (see Section 3.3) are equally applicable to risk aggregation for POSs.

3.5.2.3.Step 2A. Aggregation of the distribution functions obtained from quantification of separate PSA models

In the next step of the risk aggregation for different POSs, the distribution functions obtained in Step 1 for the POS groups assessed in separate PSA models need to be summed using the methodology described in Section 2 (see Step 2A of the approach on hazard risk aggregation in Section 3.3 for details).

3.5.2.4. Step 2B. Aggregation of risk measures characterized by point estimates

This step includes aggregation of point estimates to the distribution function computed in Step 1 from those POSs that have not been subject to quantitative uncertainty analysis in PSA. The discussion related to Step 2B of the approach on hazard risk aggregation as given in Section 3.3 is also relevant to POS risk aggregation.

3.5.2.5.Step 3. Interpretation of results

The risk for all POSs within a hazard group can be aggregated by performing Steps 0 to 2B resulting in aggregate yearly average frequency (or annual probability) as a risk measure. However, it is also essential to describe and discuss the heterogeneity in the assessment and in the results for the different POSs in an appropriate level of detail and depth. Moreover, it is also advisable to show the risk contribution from the different POSs as well as the instantaneous frequency of the risk measure in question in each POS, including at least full power operation and also all low power and shutdown states in total. The reasons for differences and similarities in the risk figures based on the insights from the PSA need to be discussed.

Figure 10 shows an illustration of the change in risk over POSs as well as time. Note that in POS 11 all the fuel assemblies are unloaded and stored in the spent fuel pool, so the risk related to this time period is assessed in the spent fuel pool PSA that is not indicated in the figure. The duration of POS 11 is quite long compared to other POSs (~650 hours). Since the frequency of core damage (in the reactor vessel) is zero and the cumulative core damage probability does not change in this POS, only the beginning and the end of this POS is indicated in the example.

It needs to be noted that aggregated risk estimate (either an uncertainty distribution or a point estimate) usually reflects an average measure of risk over several years rather than the cumulative risk of a certain year. The reasons for this are manifold:

— There may be different kinds of outages over the years (e.g. fully or partially unloaded core) that need to be considered in the POS definitions, POS durations and in the associated PSA models;
— The fuel cycle length can differ from 12 months, hence the POS durations normalized for a year can differ from the actual POS durations too.

It is highlighted, that within this step the interpretation of results is limited to risk aggregation over the different POSs for each and every hazard, and does not cover the overall (fully aggregated) risk, so it is only a small portion of the latter. The purpose of interpreting the results for risk aggregated over the different POSs for each hazard in the manner described hereby is to gain some insights into the results of risk aggregation for the different POSs (to enable comparison of POS level risk values), and to facilitate the interpretation of result for the overall aggregated risk that covers all POSs, hazards (or even sources) too.

As for hazards, the above steps do not cover the aggregation of importance measures assessed for the different POSs. Short discussion on the open issues and challenges to aggregating importance measures is provided in Section 6.

While the focus of the different POSs discussion is on NPPs, it needs to be noted that the high level concept can be extended to non NPP nuclear installations, considering the different operational modes applicable to those installations. It is expected that fuel cycle and storage facilities may not have the diversity of POSs exhibited by NPPs or the need to assess risks for all operational modes. However, recognizing that changes in operation during the lifetime of non NPP installations may incur different risk levels (e.g. during fuel loading operations versus permanent closure or decontamination) may require similar consideration on how this may impact risk insights.

4. RISK AGGREGATION IN DECISION MAKING PROCESS

This section will briefly discuss the role of risk aggregation within the RIDM process in general. As discussed in Refs [11] and [29], the integration of deterministic and probabilistic analyses to support design, safety evaluation and operations is increasing; to the extent that a balance between all the supporting information needs to be encouraged through the use of a structured and transparent RIDM process when applied to nuclear installation safety. In addition, the decision maker needs to consider both quantitative and qualitative aspects when using risk results within the RIDM process.

As stated in INSAG-25, quantitative and qualitative aspects are equally important and need to be considered holistically; which is particularly important when considering risk aggregation issues in the integrated risk informed decision making (IRIDM) framework described in Refs [29] and [11] (see Fig. 12 for key elements of IRIDM). The objective of this section is not to repeat the overarching discussions on the intent, structure, and purpose of IRIDM but to highlight the relationship with risk aggregation issues as discussed in this publication. To the extent that IRIDM may be considering issues related to multi hazards, multi operational states, and multi source (or combination thereof), some of the aspects of risk aggregation discussed in this publication will be relevant to the decision making process.

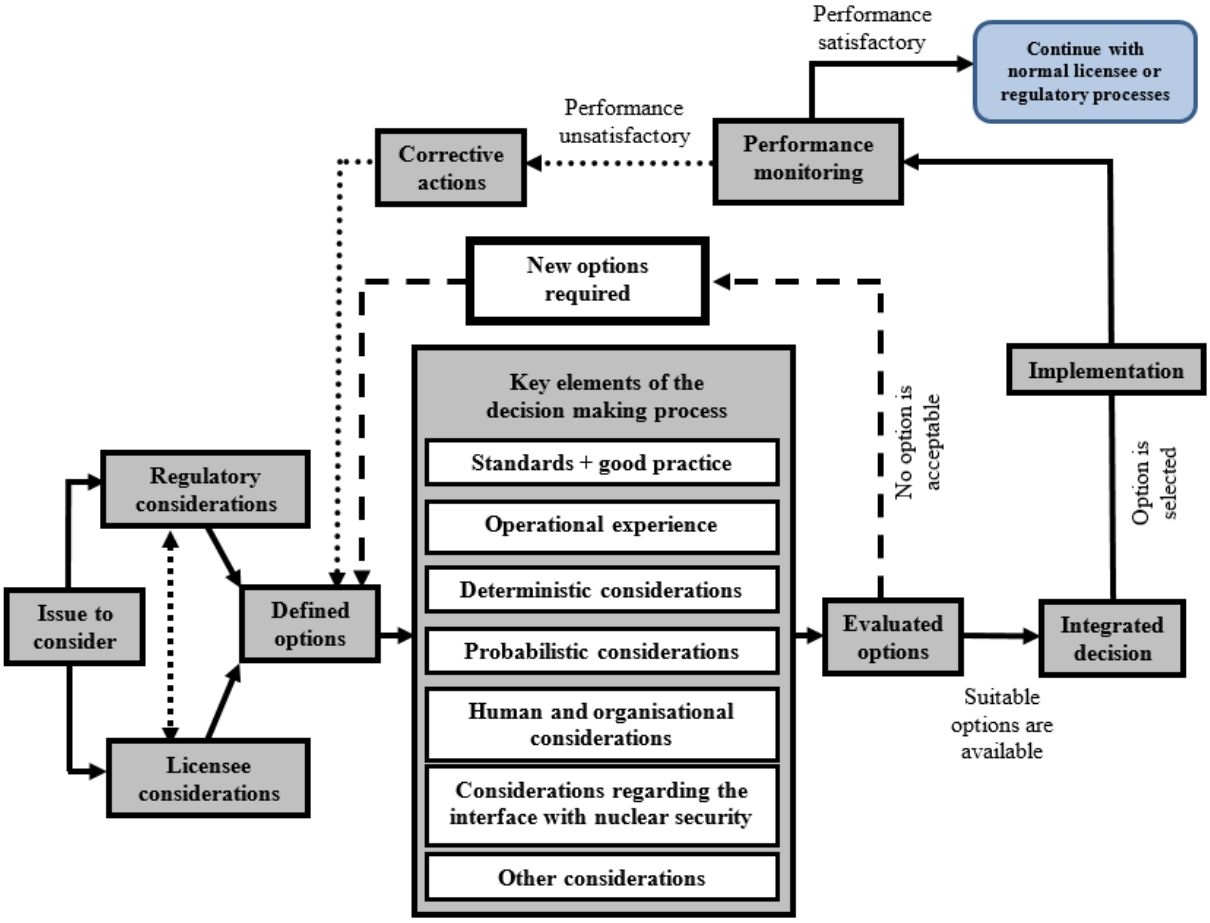


FIG. 12. Key elements of the integrated risk informed decision making process.

4.1. RISK INFORMED DECISION MAKING FRAMEWORK IN MEMBER STATES

The integration of deterministic and probabilistic considerations in the decision making is widely applied in many Member States and implies application of information on results of deterministic analysis and aggregated risk profiles for proper decision making (relevant examples are presented below and in Annex III).

A similar structured process to that in Ref. [29] is presented in Ref. [39]. In this publication, the use of PSA modelling for comparison with regulatory guidelines is expected to include a full scope assessment (e.g. multiple hazards, multiple operating states). However, it also recognizes that many PSAs are not full scope and PSA information of less than full scope may be acceptable as long as an understanding of the robustness of the assessment of the individual contributors and the impacts of uncertainty is included. In addition, Ref. [39] provides explicit risk criteria on the risk metrics used for determining the acceptability of plant licensing bases changes using risk informed approaches (e.g. see Figures 13 and 14).

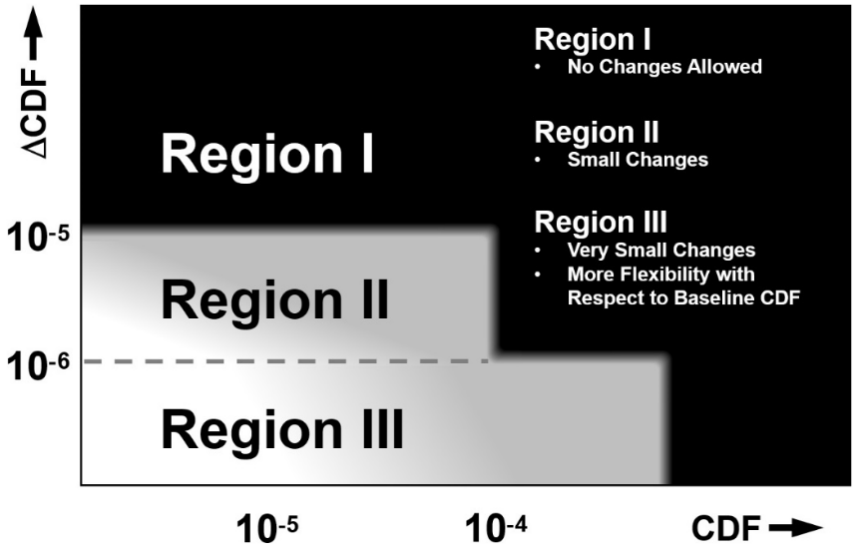


FIG. 13. US NRC regulatory guide 1.174 [39] acceptance guidelines for CDF.

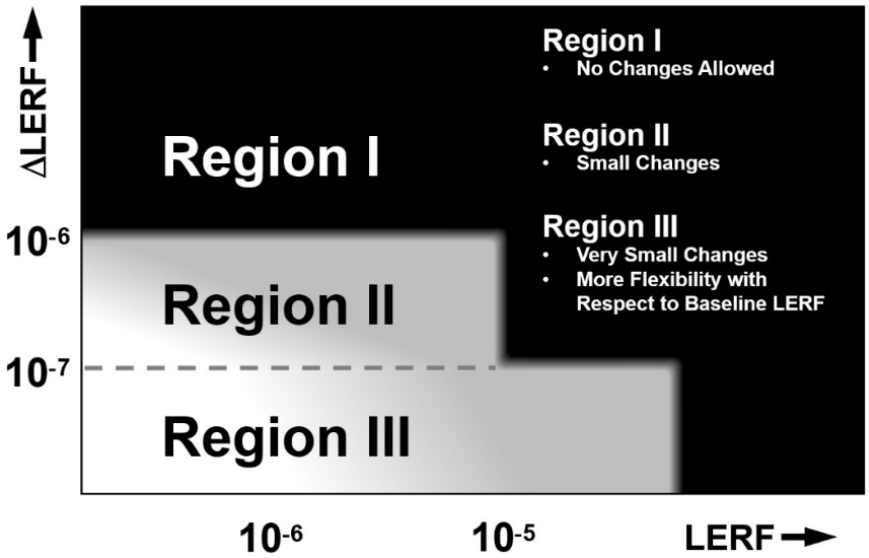


FIG. 14. US NRC regulatory guide 1.174 [39] acceptance guidelines for LERF.

A similar concept of risk acceptability is also represented in the regulatory guidelines on risk informed decision making in Russian Federation (see Fig. 15) [40]. The areas presented in Fig. 15 represent correspondingly: Area I — unacceptable risk, Area II — conditionally acceptable risk and Area III — acceptable risk. The concept of areas on Fig. 15 is similar with the concept of regions provided in Fig. 13, however it contains certain conceptual differences (e.g. Area I and Area III do not have any common boundaries).

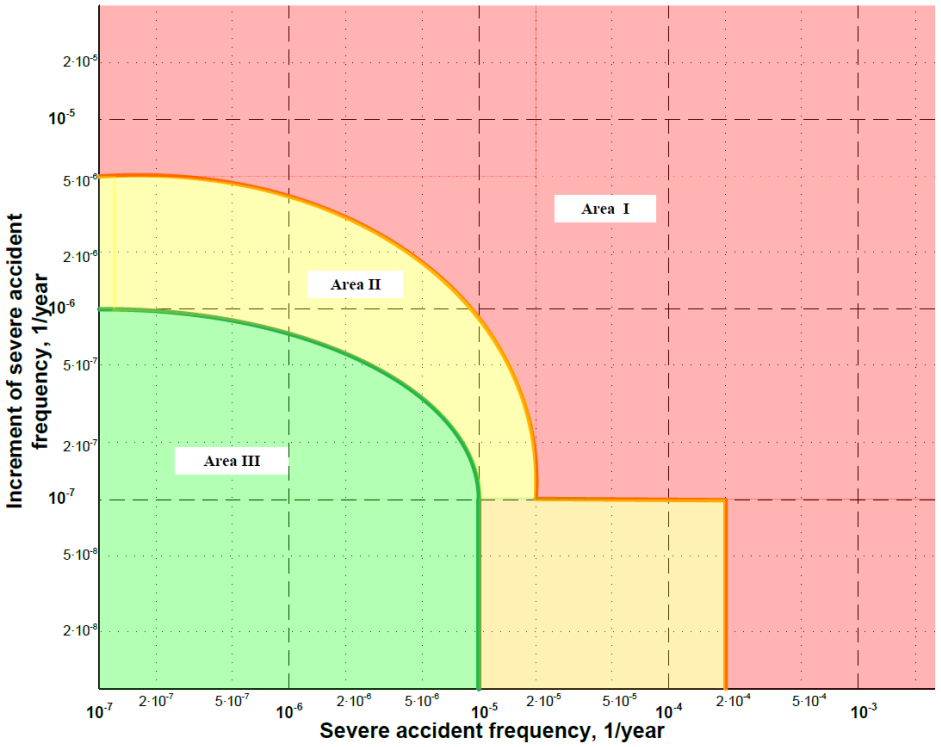


FIG. 15. Diagram of assessment of risk acceptability for a severe accident.

It is important to note that above mentioned concepts are also applied for large (early) release frequency and designed to reflect the risk acceptability limits for a single unit (multi source risk is not explicitly covered). More details on this approach are presented in Annex III.

Another approach to considering risk information using different metrics is highlighted in Fig. 16, based on the regulatory framework by the United Kingdom's Office of Nuclear Regulation (ONR), as described in ONR's 'Safety Assessment Principles for Nuclear Facilities', Revision 0, 2014 [41]. As part of the basis for ONR's regulatory judgements and recommendations when undertaking technical assessments of nuclear site licensees' safety submissions, several numerical targets are used in terms of potential consequences. Specific numerical targets consider different aspects such as location of the exposed person (e.g. on site, off site), from an individual accident frequency versus total accident frequency, individual fatality versus 100 fatalities, among others. In this case, the RIDM approach is based on a frequency consequence relationship (similar to what was presented in Figs 1 and 19 but with specific thresholds as shown in Fig. 16 on an installation basis (i.e. Target 8 as described in [41]). Targets associated with PSA outputs require some form of aggregation in the UK, but to different levels.

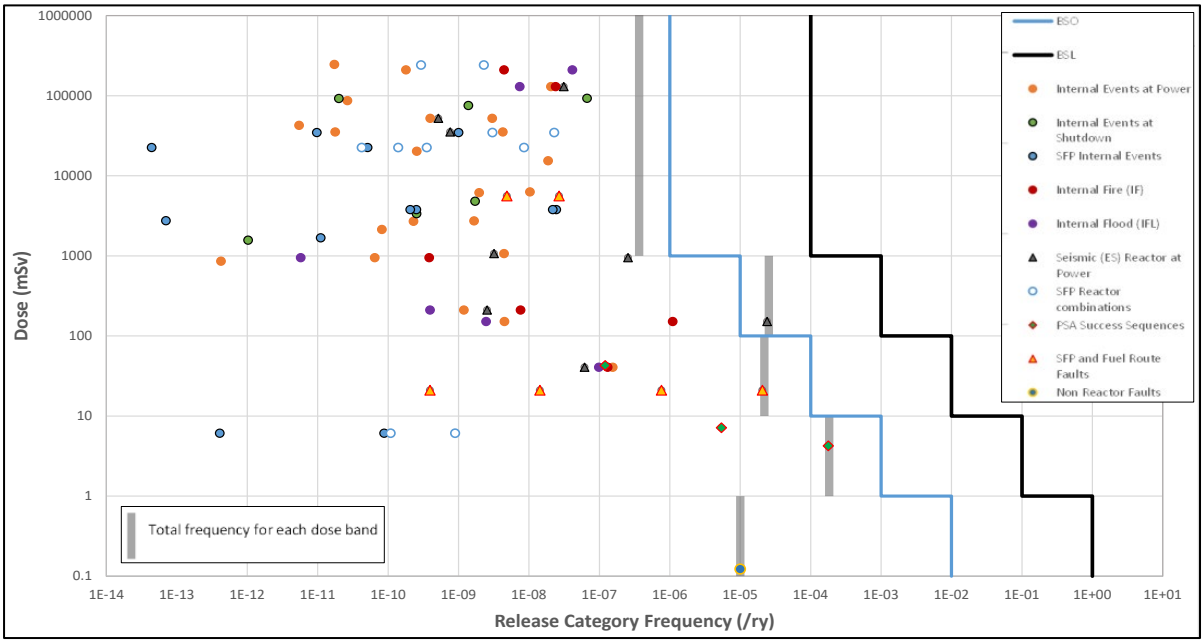


FIG. 16. Example of assessment of compliance to basic safety limits (BSL) and basic safety objectives (BSO) used in UK.

Another example is included in guidance published by the Nuclear Regulatory Authority of Argentina (Autoridad Regulatoria Nuclear, ARN) in Ref. [42]. This publication describes risk criteria associated with accidents at NPPs, as shown in Fig. 17 (left). In this figure, duplicated from Figure 1 in Ref. [42], the x-axis shows effective dose (Sv) and the y-axis represents the annualized probability of accident sequences as an overall risk curve for protection of the public against NPP accidents. The orange portion represents areas where the risk of radiological exposure is acceptably low, while the white areas are equivalent to Region III in Figs 13 and 14, and Area I in Fig. 15 (i.e. regions of unacceptable risk). The figure on the right shows the comparisons with the basic safety limits (BSL) and basic safety objectives (BSO) from the UK's ONR (see Fig. 16).

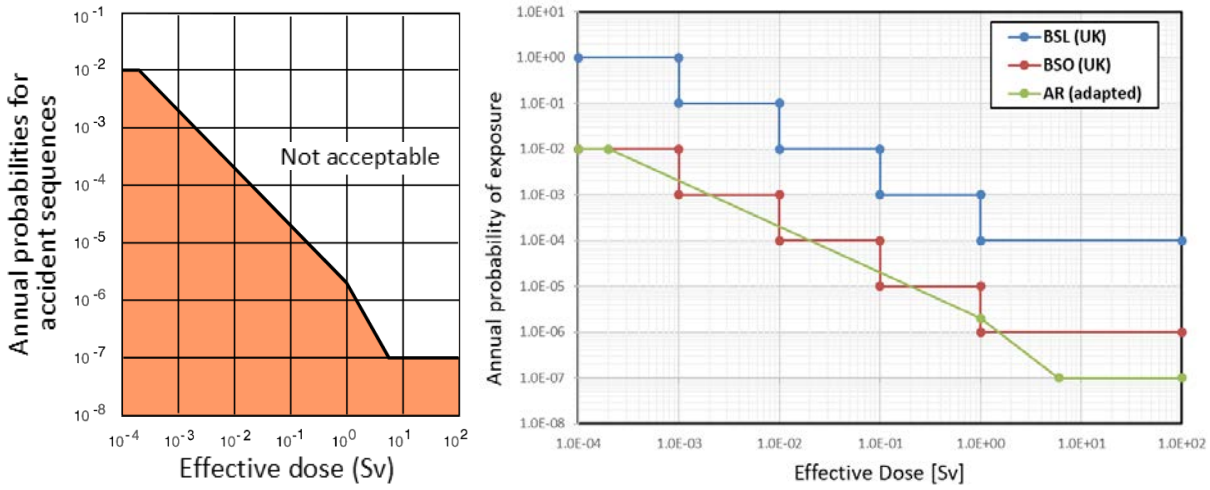


FIG. 17. Risk criteria for effective dose and annual probability of accident sequences by ARN, Argentina (left) and comparison with UK BSL and BSO (right).

With regards to the treatment of uncertainty in the decision making process, Ref. [12], which is directly referenced in Ref. [39], addresses risk aggregation further. Reference [12] states that the addition of independent hazards and plant operating states is mathematically correct (as shown in Appendix I), but that the varying level of PSA detail is to be considered when combining different PSA models for decision making purposes. Furthermore, Ref. [12] recognizes that lower contributors from different PSA models may be modelled only to the level of detail sufficient to prove they are not important to the results. This is important when including external hazards and LPSD PSAs, for example, as they may have significantly higher levels of conservative bias [12]. In addition, the type of RIDM application is also an important consideration, to the extent that risk aggregation may be a more or less important issue depending on the specific application details. Further details on issues such as dealing with cases where the PSA results challenge regulatory guidelines, as well as documentation aspects, are provided. For example, see Fig. 18 on the overarching process used in Ref. [12] for the treatment of uncertainty in PSA for RIDM.

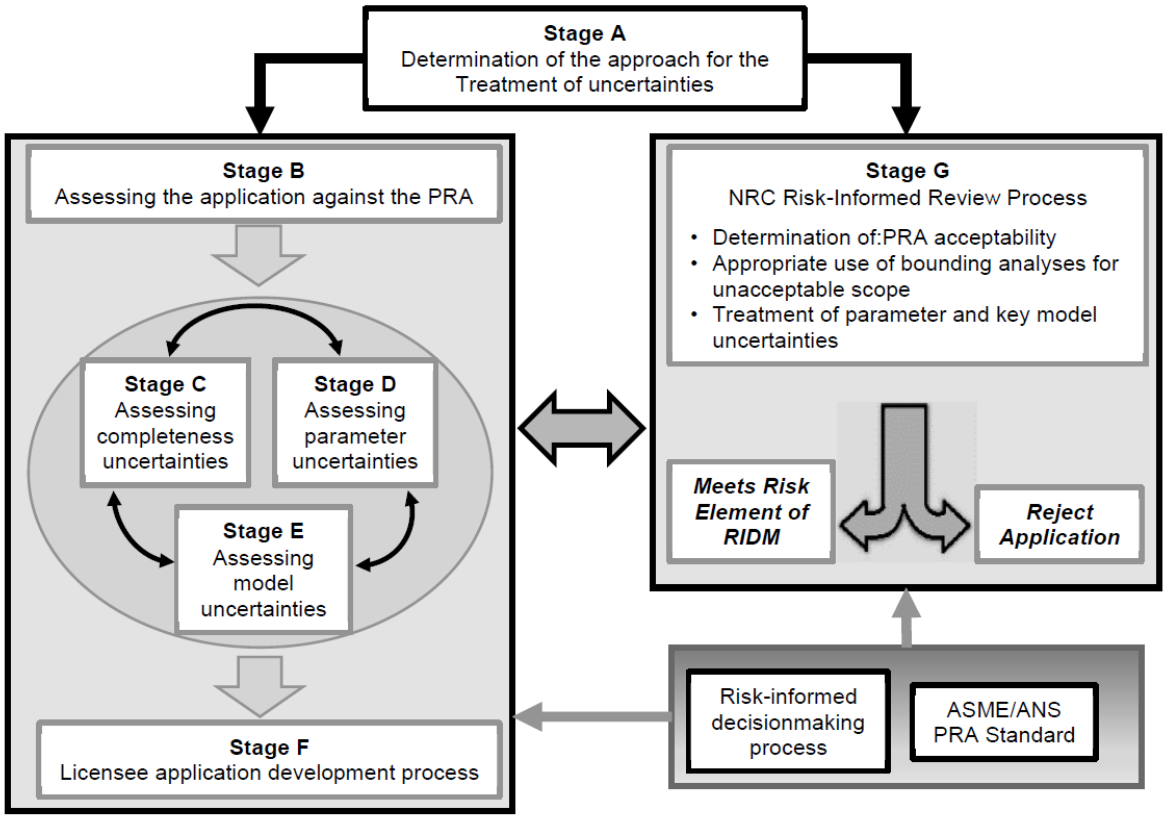


FIG. 18. Example of the process for the PSA treatment of uncertainties in risk informed decision making from Ref. [12].

A prior publication by the US NRC [43] suggested a frequency-consequence curve for a proposed technology neutral framework for licensing advanced reactors as shown in Fig. 19, although this is now being modified for non light water reactor applications.

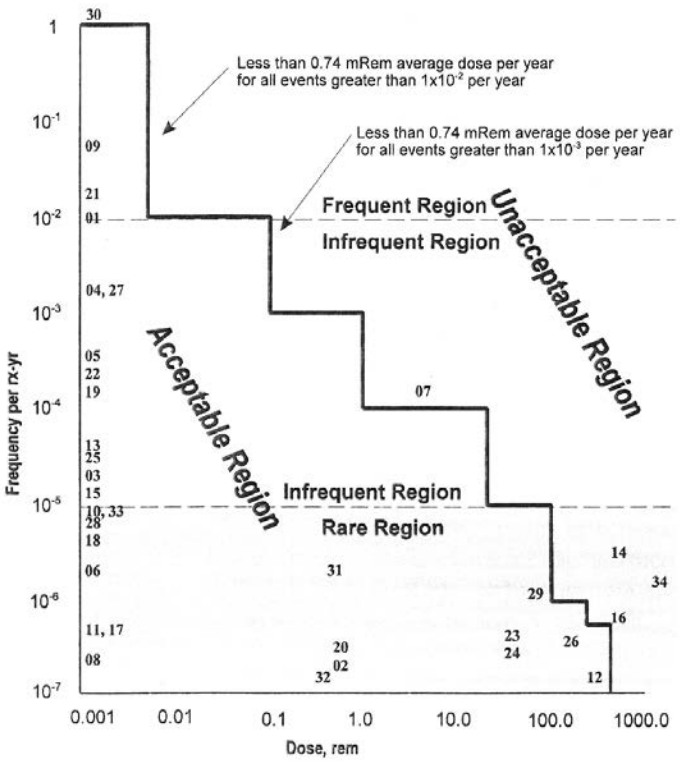


FIG. 19. Example of the frequency consequence limit line for licensing basis event selection from Ref. [43].

Additional activities on the topic of RIDM were discussed on two publications by the US Electric Power Research Institute (EPRI) [17], [44]; both directly focused on the issue of risk aggregation for RIDM. In effect, the most recent publication [17], identifies the issue of risk aggregation as the process of combining all relevant risk information from various contributors to provide an overall characterization of risk for use in RIDM (i.e. risk aggregation is considered directly embedded in the context of RIDM). This is in line with statements in [39] and [12], with a focus on moving beyond mathematical summation to a more deeply informed understanding of the aggregated risk given:

1) Differing levels of maturity of various hazards in PSA modelling;
2) Approximations made to facilitate the PSA model development;
3) Nature and magnitude of associated uncertainties.

4.2. RISK AGGREGATION TO SUPPORT DECISION MAKING PROCESS

The structured decision making process that balances probabilistic and deterministic information needs to be guided by core principles to ensure consistency and transparency. Broadly speaking, these principles address the need to assess not just the quantitative risk results and the robustness of the probabilistic analyses, but also to consider key deterministic concepts in nuclear safety, such as defence in depth and safety margin. By doing so, risk aggregation is less focused on pure mathematical addition of risk results and more about the aggregation of risk insights [41]. As shown in Fig. 20, the process described in Ref. [17] suggests a well-structured and integrated approach to the treatment of risk aggregation in general; this includes establishing the role of the PSA with regards to support in the RIDM being considered, assessment of the PSA baseline model for performing a RIDM assessment, consideration of the risk metrics to be used, and additional refinements needed. In addition, characterizing sources of uncertainty and documentation of RIDM are intrinsic steps in the process.

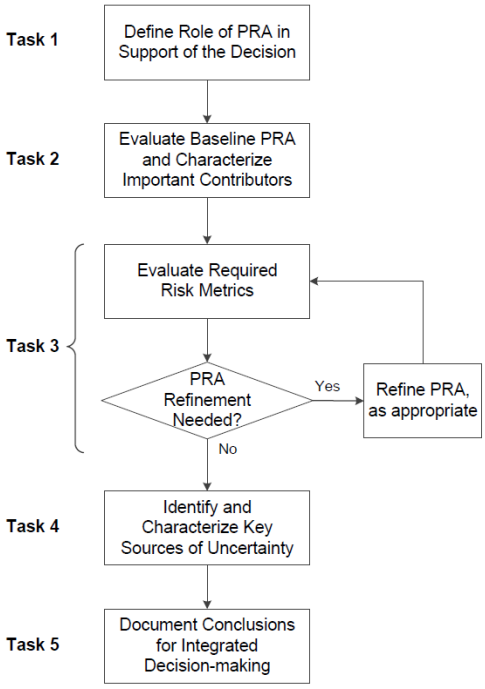


FIG. 20. EPRI's proposed process for aggregation to support RIDM.

As discussed in Refs [17] and [44], if risk aggregation is treated as only a matter of simple addition without considering the effect of potentially uncertain or conservatively biased inputs, then an overall biased result can be obtained (either conservative or non-conservative). The increased complexity of PSA models implies that fully determining the effect of all biases in a quantitative manner may be very difficult, again requiring a strong link between the IRIDM structure and its core principles. In addition, the need for risk aggregation itself is an important consideration in IRIDM depending on the specific application of PSA, the risk results needed, risk metrics to be measured against, and purpose of the assessment. It is discussed next in more detail.

Many Member States have established overarching safety goals for the operation of NPPs, including associated quantitative risk goals and processes for dealing with risk informed decision making aspects [45]. In this context, risk aggregation may play a central role, as addressing specific quantitative risk goals may depend on having a combined picture of the risk profile of various hazards through PSA modelling. While this publication assumes that the need to aggregate risk exists, it is recognized that, more broadly, if an individual Member State regulatory regime allows for individual hazards to be assessed separately, then risk aggregation may need to be treated differently. In addition, in other risk informed applications, the need to aggregate all hazards may be less important and/or impact the IRIDM process differently than when comparing baseline PSA results alone (e.g. baseline CDF and LERF). Hence, it is important to establish the role and impact of risk aggregation a priori depending on the characteristics of available risk informed processes, where PSA is expected to provide specific outputs for decision making. An example of the types of risk informed processes that may be considered, beyond demonstrating that an overarching safety goal has been met, are discussed in [17]. These may involve PSA input to specific regulations (e.g. allowing risk informed maintenance activities), allowing for licensing bases changes (i.e. where the change in risk becomes an additional risk metric to consider), comparing design alternatives, and assessing the impact of operational events or regulatory oversight activities, to name a few. By evaluating the need for detailed risk aggregation in advance, the level of detail and PSA modelling needed for individual PSA components can be scoped and planned accordingly.

Once the specific role of risk aggregation is identified, the impact of the varying level of realism in the PSA model may provide insights as to how the IRIDM process needs to be implemented in terms of areas of increased focus and/or integration with deterministic concepts such as defence in depth. For example, if the focus of the PSA is on relative risk ranking rather than baseline metrics, then importance measures may not be passive of simple additive mathematic treatment and may need to be weighted via a specific approach.

In addition, if various models are integrated from varying individual PSA applications (e.g. internal events and natural hazards), overly conservative/non-conservative assumptions may mask the real importance of contributors by unduly raising the risk importance measure of specific failures at the expense of others (i.e. in essence, providing a potentially misleading set of risk insights for decision making). In this case, IRIDM considerations may need to focus more closely on the implications of such assumptions, which may be less of a concern for direct baseline comparisons where it can be more easily demonstrated that the PSA modelling credibly supports the conclusion that a safety goal is not exceeded. In the case where this conclusion is not as easily achievable (or for situations where the level of granularity goes deeper than a single metric comparison, e.g. relative risk ranking), the focus in IRIDM is to be on identifying the important contributors first (meaning those that have the greatest role in the decision at hand). This would be followed by the decomposition of the results by hazard group, significant accident sequences or cut sets, and eventually reaching the level of significant basic events.

Once those PSA risk insights are available, along with the level of robustness, detail, and technical bases; a decision can be made whether further refinement in the PSA is needed (or if the issue is of sufficient realism where actual design/modifications need to be entertained, along with the associated impact and cost benefits). Finally, identifying and documenting sources of uncertainty (especially model uncertainty) would still be needed (as discussed in more detail in Refs [12], [46], [47]).

The benefit of a structured IRIDM process in this context would be to ensure (1) the availability of the relevant information, (2) an understanding of the impacts of the individual and aggregated PSA modelling, (3) communication of the important risk insights within and across organizations, and (4) the documentation of a solid technical bases for a decision that accounts for a balance between probabilistic and deterministic considerations in a more objective manner. For example, Fig. 21 shows a proposed approach to characterize the impacts on defence in depth (DID) on changes regarding a specific RIDM application.

By establishing the identified change with respect to specific areas known to potentially impact DID (e.g. common cause failures, barrier integrity) the decision maker can assess how much the PSA can provide a robust input into the decision making process or whether the balance is to be focused on more qualitative approach. An approach for defence in depth is discussed in IAEA's safety report No. 46 [48] that can support in making such decisions. Due to the hazard specific nature of such concepts and multiple possible interpretations of how qualitative concepts can be evaluated, a detailed descriptive guidance is neither considered to be within the scope of this publication, nor would it be useful or sufficiently complete to satisfy all possible issues that may arise for aggregation purposes.

It needs to be noted that this is simply a proposed structured approach, so the entire process of considering how the PSA can support RIDM and what aspects may need refinement (or additional deterministic consideration) is subject to a systematic, well documented search for potential aspects that may impact the final decision.

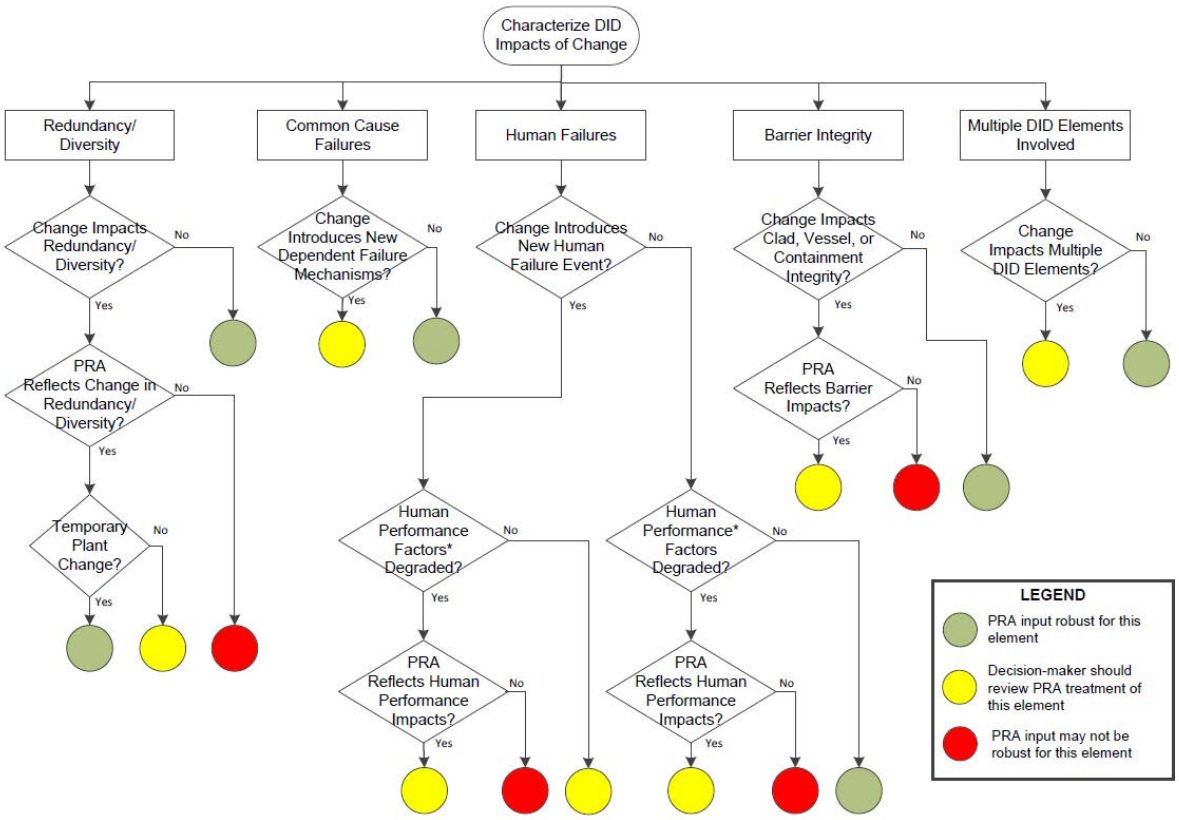


FIG. 21. US EPRI's Process for evaluating defence in depth implications in RIDM.

As far as documentation provided for the benefit of decision makers, risk aggregation has a strong need for appropriate risk communication. The main elements of the information to be communicated are [17]:

— Quantitative numerical results (individual and aggregated);
— Comparison with respect to acceptance guidelines of the relevant risk metrics;
— Information on the sources of uncertainty and the reasonableness of any alternate assumptions (via either uncertainty analyses and/or sensitivities).

It is necessary to highlight the importance of the communication task, which may need to be tailored to the individual audience, their context and role within IRIDM, and the importance of the decision being made; as well as the extent of PSA modelling involved. More details about risk communication are provided in Section 5.

In summary, addressing the risk from all significant contributors is expected to continue to be an essential part of IRIDM for various risk informed applications. The extent to which risk aggregation plays a role in the decision to be made and how to properly disposition issues associated with the individual PSA components is a key component of the process. As discussed above, risk aggregation needs to be considered more than just the numerical addition of mean values of piece parts of PSA (which is mathematically correct when dealing with independent models). In this context, the core benefit of PSA becomes more meaningful and valuable when using a structured IRIDM process that highlights areas of uncertainty and potential alternatives, as well as quantitative and qualitative considerations. It needs to be noted that there are challenges for various PSA applications in terms of use of aggregated risk results. The summary of these kind of challenges for various categories of PSA applications are provided in Appendix III.

5. COMMUNICATING RISK INFORMATION

As it was described in Section 4, the risk communication task is critical for the effective risk informed decision making and needs to be tailored for specific context. The need for risk communication arises in various contexts and is focused on accurate understanding of risks and. As Ref. [11] notes:

> "The outcome of decision making in relation to complex facilities and situations is often difficult to explain to stakeholders who may feel that their concerns are being excluded from consideration. A well-documented IRIDM process can assist in communicating how the decision has been made, the factors considered and the significance of each factor in the final decision. Whilst other stakeholders may wish to include additional factors, or to put different emphasis on the factors considered, the framework of IRIDM is expected to allow a more structured and mature discussion thus facilitating communication. One of the important features of IRIDM process is traceability of any decision made."

Although these comments are made in the context of IRIDM, they apply equally to the characterization of risks, including the various aspects of aggregating risks. The three primary considerations are:

1) What is the purpose of communicating risk information?
2) What is the information that needs to be conveyed?
3) How can the information be most effectively characterized?

Each of these considerations depends on the parties involved in the communication process. Communication may need to take place:

— ***Between the risk analysis team and decision makers***. This entails ensuring that management of nuclear installation understands the perspective provided by the aggregated risk with regard to the overall level of safety for the nuclear installation and the aspects of the design and operation that contribute most to risk in order to aid in making informed decisions.

— ***Among the staff***. Staff need practical information regarding the systems and components determined to be important. This information can help them to be especially alert when engaged in operations or maintenance activities involving these systems or components. The information can also be used to address spatial considerations, such as clearly demarking important fire areas in which combustible materials are not to be stored. Special considerations come into play with respect to personnel responsible for configuration risk management during various operating states.

— ***Between the operating organization and the regulatory body***. The nature of the information communicated between the operating organization and the regulatory body varies from country to country. In general, these communications focus on risks relative to any formal metrics that may be in place in the respective countries. At a minimum, most regulatory authorities require estimates of risks as supplements to deterministic safety assessments for periodic safety reviews or other actions. Where more formal risk informed processes are in place, these processes typically define the types of information that needs to be communicated.

— ***Between the operating organization or the regulatory body and the public***. Communicating pertinent aspects based on detailed technical information to the public presents particular challenges. In some countries, the public may be sceptical of any risk

information presented by either the operating organization or the regulatory body. Moreover, putting into a proper perspective risks when the frequencies of serious accidents may be very low, but the consequences may be relatively high is difficult. Risk information that may be relevant might include that needed to provide a proper view of the safety of a proposed or operating nuclear installation, or to explain the significance of an operational occurrence or regulatory finding.

5.1. COMMUNICATING WITH THE MANAGEMENT OF THE NUCLEAR INSTALLATION

Risk information, including aggregated characterizations of risk, may need to be communicated to decision makers within the operating organization for a variety of reasons. These reasons most often include situations in which:

— Decision makers seek to use risk insights to provide additional assurance that the nuclear installation is being operated in a safe manner;
— Results and insights from a new or updated PSA have identified important new risk contributors that may merit attention and action;
— Risk implications may provide context for the significance of operational occurrences;
— In a risk informed regulatory environment, management needs to decide whether to pursue formal risk informed applications and approve any related submittals to the regulator.

The extent to which aggregated risk characterizations are useful in a decision making process varies among these situations. In the case of using risk information as a supplement in judging the overall level of the safety of the nuclear installation, as full a picture of risk as possible is desirable. That is, it can be misleading to communicate only a portion of the risk profile without in some manner acknowledging the role of other potential contributors. That is not to say that the risk needs to be quantified for every possible hazard for the information to be of use to decision makers. To be most effective, this picture needs to include an appropriate representation of uncertainty and a fair assessment of the adequacy or shortcomings of the underlying PSA itself.

Providing extensive quantitative results can, in some cases, make effective communication challenging; detailed probability distributions such as those presented in Appendix II, for example, may be of limited use to decision makers. Thus, the information to be communicated in this context includes the following:

— The overall mean estimates for relevant risk measures (CDF, LRF, LERF, or others) and a comparison to any applicable criteria. These criteria may be those imposed by the regulator or may be internal goals set by the operating organization;
— A breakdown of the aggregated risk according to the contributing hazards, systems, components, human failure events, and other elements;
— An indication of the uncertainty in the overall estimates of risk and of the various contributors;
— A description of qualitative factors that may need to be taken into account in using the risk results. These may include known areas of heterogeneity (e.g. conservatism or non-conservatism) that are not explicitly accounted for or the impacts of assumptions that may have a significant impact on the PSA;

— Recommendations for any safety improvements to the nuclear installation (design, procedures, or operating practices) that might merit consideration and an assessment of the value of these changes in terms of the resulting impacts on the risk measures.

Appendix IV provides examples of ways in which aggregated risk information may be presented to the management of nuclear installation to support the first two items listed above. On occasion, an operating occurrence or condition at the nuclear installation may raise questions about the significance of some aspect of the design or operating practices. The risk metrics used in communicating this information might depend on the nature of the occurrence or condition at the nuclear installation. If the occurrence entails an initiating event with some complicating factors, it may be desirable to address the conditional core damage probability (CCDP) for that condition, compared to the CCDP for the initiating event using the baseline PSA model. That provides a direct indication of the margin to core damage in probabilistic terms. If the occurrence entails discovery of an extended unavailability for important equipment, it may be useful to calculate the CCDP as well as the absolute and relative increases in CDF as points of comparison to the baseline risk.

Irrespective of the nature of the occurrence, the information that is to be communicated needs to include a clear, concise summary of:

— The impacts of the SSC failures or conditions or Human Failure Events that gave rise to the increase in CDF;
— The remaining features that functioned or that were available to prevent core damage.

Examples of communicating information of this type are provided in Appendix IV.

Finally, with respect to communications relating to formal risk informed submittals that management may need to consider for approval and submittal to a regulatory authority, the format and content of the information to be provided will depend on the specific nature of the application and will often be specified through regulatory interactions. The principles presented in this section, however, need to be relevant. These include presenting technical information in a clear and straightforward manner that can be understood by persons who are not experts in PSA technology, together with qualitative information that characterizes the significance of various aspects of the results in the context of available engineering features and operating practices.

5.2. COMMUNICATING WITH THE STAFF OF THE NUCLEAR INSTALLATION

Communicating with the staff represents an important aspect of effective risk management. In this case, it is usually the practical insights that can be drawn from the aggregated risk results that are of value, rather than the overall risk estimates themselves. These insights may be obtained from reviewing importance measures and by examining other aspects of the risk profile.

In some nuclear installations, personnel are routinely apprised of important risk results and insights, most commonly through posters and other visual displays. Some nuclear installations display very high level information derived from aggregate risk estimates. These displays may be present at the security portals, so that they reach all employees as they report to work. Similar displays may be found at other strategic locations on the site. They may take a variety of forms, including video displays or other types of sign boards (an example is provided in Appendix IV).

Many installations also use a somewhat more extensive display to communicate important results and insights from the risk assessment to a broad spectrum of the staff, often in the form of a poster. This display captures a variety of aspects that could be of value, including:

— Ranking of the systems according to their importance to risk (without necessarily indicating the numerical importance and with limited reference to technical PSA terms). Such a ranking can help to focus the attention of personnel who needs to interact with systems during maintenance, testing, and routine operations. It can be particularly valuable to point out the impact on risk when a portion of a system is removed from service;
— Listing of areas especially important with respect to fire (or internal flooding). This listing can be useful when planning work activities such as welding (for example, provisions may be made for a special watch in such areas when welding is taking place) and to identify locations where storage of flammable materials needs to be avoided altogether;
— Summary of the operator actions that play a significant role in the risk profile.

More detailed information may be of use in operator training programs. The PSA results can help to identify operator actions whose reliability has the most impact on risk. Communicating an understanding of these actions through operator training programs can assist to effectively prepare operators for the types of challenges that may be most important from a risk perspective. The selection of operator actions to communicate can be made largely on the basis of importance measures. For example: Fussell-Vesely importance, which could help to identify operator actions for which improvements in operator performance would have the biggest impact on reducing risk, and risk achievement worth (or risk increase factor) which could identify those actions for which it would be especially important to maintain high reliability.

It is not necessary to attempt to communicate the actual importance measures; these measures are not generally of direct value or interest to operators. This information is of use in identifying the actions to be communicated to the operators. Although the numerical importance measures may not be relevant, the PSA team needs to provide qualitative information that provides a context for the nature of the actions and why they are important. This will often be obvious to experienced operators, but on some occasions the results may not be intuitive and will require some explanation. An example of a listing that might be assembled is provided in Appendix IV.

More extensive communication of technical information is most often needed for the purpose of the configuration risk management (CRM). Results of the PSA are often used directly on a virtually continuous basis to assess the level of safety of the nuclear installation and to plan and manage testing and maintenance activities. This CRM process may be employed during power operation but also during shutdown and transitional states. The nature of the communication will depend on the specific process in place and the group tasked with performing the assessments. The CRM could be performed by the PSA team or by the work planning organization. While personnel in that organization will not necessarily have a detailed knowledge of the PSA models, they will be familiar with the CRM tools, including how to designate equipment as out of service, how to account for the relevant conditions at the nuclear installation, and how to interpret the results. In most cases, this will be sufficient for an effective CRM process. At times, however, a configuration may be conceived that is not well reflected in the PSA models due to assumptions or simplifications that have been made in developing the models. In this application of the PSA, the primary communication entails ensuring that the PSA staff has provided the most relevant models to the organization performing the CRM assessment and is available to respond to questions that may arise in unusual situations. The CRM assessment team needs to also communicate the results of its assessments to the PSA staff

on a routine basis to ensure that any anomalies or assessments beyond the PSA's capabilities are noted and addressed.

5.3. COMMUNICATING WITH THE REGULATORY AUTHORITY

As noted above, the needs for communicating specific types of risk information varies among countries according to the extent to which regulatory authority use such information. Irrespective of the specific types of regulatory interactions, however, the critical aspects that typically require effective communication include:

— Understanding of the overall (aggregated) risk, as appropriate;
— Description of the relative risk contributors (including a characterization of the level of realism and detail represented by the estimations);
— Representation of uncertainties;
— Identification of specific elements of the risk informed decisions to be made.

In the case of communicating with regulatory authorities, it is reasonable to expect that the regulatory authority have staff members familiar in detail with risk concepts and relevant technical details, and typically these staff members are responsible to relate relevant results and conclusions to decision makers within the regulatory authority. In some cases, the communication of aggregated risk information needs to conform to the manner in which decision criteria are formulated. This is the case, for example, with respect to the approaches summarized in Annex III. Other possible types of tools for communicating with regulators are outlined in Appendix IV.

5.4. COMMUNICATING WITH THE PUBLIC

There are occasions when it is useful to communicate risk information to the public. This might be the case when for example a new NPP is being proposed, when changes to a licence for an existing nuclear installation are being considered, or to put into context some aspect of operating experience.

The nature of such communications heavily depends on the national legislative framework and on the type of information that needs to be conveyed, to the extent that it is not possible to provide useful detailed guidance in this context. Irrespective of the specific information or approach to communication, however, a major challenge is to communicate effectively in a clear and straightforward manner but in a form that can be understood by persons without extensive technical backgrounds. Often, a focus on qualitative factors is most useful. In some specific cases, it may also be useful to present the risk information relative to other risks that are more familiar.

6. CHALLENGES IN RISK AGGREGATION

The information provided in previous Sections represents the good practice available in IAEA Member States related to the topic of aggregation of various risk contributors for nuclear installations. As indicated previously, some challenges and open issues related to risk aggregation have been identified:

— **Aggregation of risks for different type of installations.** As it was highlighted before, different installations might have different failure criteria as well as a different definition of undesired end states, which could create obstacles for risk aggregation. The typical example is aggregation of risks of reactor core damage with the fuel damage in the Spent

Fuel Pool. The undesired end state in case of reactor core is usually linked with the maximum cladding temperature, whereas the fuel damage in Spent Fuel Pools can be defined in terms of fuel uncovering and / or mechanical damage of fuel. While the high level concepts discussed in previous sections may apply, the specific details on how these applications are to consider risk aggregation will vary from the NPP based approach. Such details are not discussed in this publication.

— **Aggregating risks for combined/correlated hazards.** This issue is related to aggregation of risks coming from individual hazards and combined/correlated of hazards. When models are developed independently, they may partially overlap in the quantification of specific initiators. For example, loss of offsite power (LOOP) frequency used for the internal events models, includes in some cases plant centred LOOP, grid centred LOOP and weather related LOOP (often due to natural hazards). When the external hazards model is developed, the LOOP contribution could partially overlap with the frequency used in the internal events assessments. Similar partial overlap can exist between a seismic PSA and an external flooding PSA (e.g. due to seismically induced tsunami or dam failure). Normally, a seismic PSA needs to include the effect of the tsunami, or of the seismic induced dam failure, if the tsunami is generated by the same seismic event impacting the site, or if the dam is located in close proximity of the plant. Seismic induced failures of dams far away from the plant are normally screened from the scope of an external flooding PSA, which addresses the impact of the water reaching the site (not otherwise impacted by the seismic event). Similarly, tsunami generated by seismic events far away from the site are within the scope of an external flooding evaluation. The determination of how far away a dam (or the source of a tsunami) needs to be for it to be excluded from further assessment in the PSA, is currently a technological limitation.

— **Aggregation of risk importance and sensitivity measures (in case of separate models).** This issue is related to aggregation of risk importance measures and sensitivity measures obtained using separate PSA models. The aggregation of these measures is necessary in order to understand the overall importance of the given component and sensitivity of the results towards the parameters used for further decision making. Some risk importance measures could be aggregated using the information on proportional risk contribution coming from each hazard. Then, the expression for the aggregated risk importance measure of fractional contribution (FC_{TOTAL}) might be presented as follows:

$$FC_{AGG} = \sum_{i=1}^{n} FC_i \frac{CDF_i}{CDF_{TOTAL}} \quad (4)$$

Thus, for example, if for a given component the fractional contribution equals FC_{SEIS}=0.1 for seismic hazard and FC_{INT}=0.4 for Internal events and given the fact that contribution from seismic hazard is 80% of total CDF and contribution of internal events is 20% of it, then aggregated fractional contribution could be calculated as FC_{AGG} = 0.8x0.1 + 0.4x0.2 = 0.16.

— **Resource issues.** Both for separate and integrated models, the quantification of a large model (or the combination of results from multiple models) is challenging. For example, it is a known issue that some external hazard models (e.g. seismic PSAs) present challenges in the quantification process, mainly due to the failure of the rare events approximation. Because of this reason, very high truncation limits may need to be used for efficiencies in the quantification or pruning of the model may be needed. When

integrating models, the quantification and maintenance of the models may become an issue.

— **Large uncertainties / heterogeneity.** This issue is related to aggregation of risk coming from various contributors when one (or a subset) of them has point estimate/mean value and uncertainty distribution significantly higher than others. In such cases, aggregated risk is dominated by this single contributor (or few contributors) and can mask insights important for RIDM. This challenge is more typical for new designs with very low CDF (in the range of 1.E-7 1/a) where the highest contribution to risk may come from natural hazards (e.g. seismic). Figure 22 below illustrates the issue where the aggregated risk is completely determined by one contributor having the greatest uncertainty and mean value (in this case seismic).

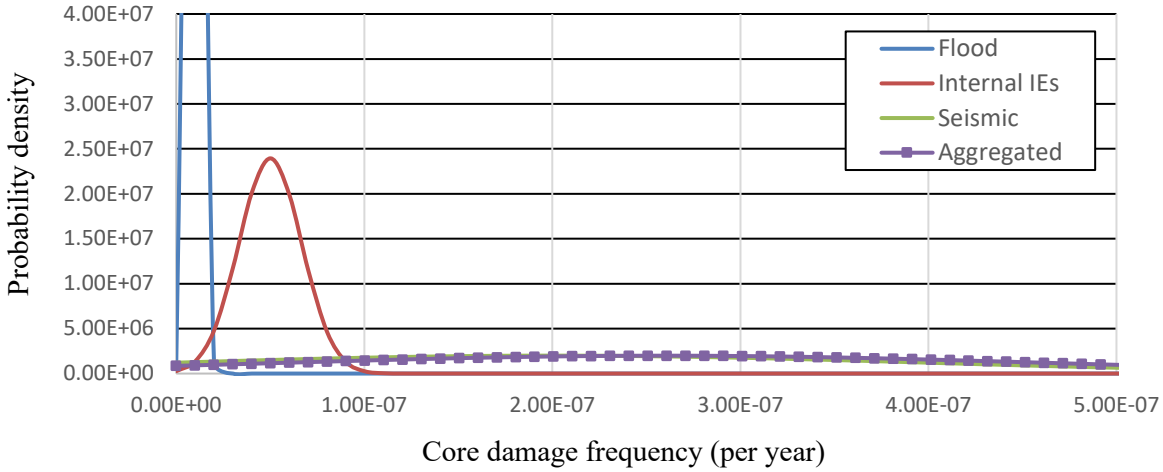


FIG. 22. Example of aggregated risk in the context of high uncertainty of one of risk contributors.

While mechanics of aggregation of different risk contributors are not different from those discussed in Section 2 and Appendix I, the main challenge may be to provide a clear understanding of what this masking may imply for decision making.

APPENDIX I. MATHEMATICAL FOUNDATION FOR RISK AGGREGATION

As it was mentioned above in Section 2.2, three major assumptions underlying the mathematical framework of current PSA models are:

- Assumption 1: Random (i.e. aleatory) events occurring over time (e.g. initiating events, runtime failures) are typically modelled as Poisson processes;
- Assumption 2: Random events occurring in response to demands (e.g. failures to change state on demand, initiating events occurring in response to manipulations or tests fixed in time) are typically modelled as Bernoulli processes;
- Assumption 3: The accident scenarios in the PSA models are typically modelled as being stochastically independent.

Given these assumptions, the following well known properties of quantitative risk aggregation can be derived (see Section 2.2 for details):

— Property I: the occurrence of an accident scenario is a Poisson process.
— Property II: the occurrence of an undesired end state (e.g. core damage) is a Poisson process.
— Property III: For a specified consequence measure, the total probability distribution quantifying the aleatory uncertainty in that measure is the weighted sum of the contributions from all scenarios in the PSA model.
— Property IV: The mean total frequency of an event based end state is the sum of the mean frequencies of the scenarios leading to that end state regardless of the underlying distribution of the individual scenarios. Similarly, the mean total value of a consequence based end state is the weighted sum of the mean contributions from all scenarios.

This appendix outlines the mathematical foundation for the quantitative aggregation properties listed above. Figure 23 shows a simple event tree[22] used as an example throughout this appendix. This event tree provides a concrete means of illustrating the PSA quantification process.

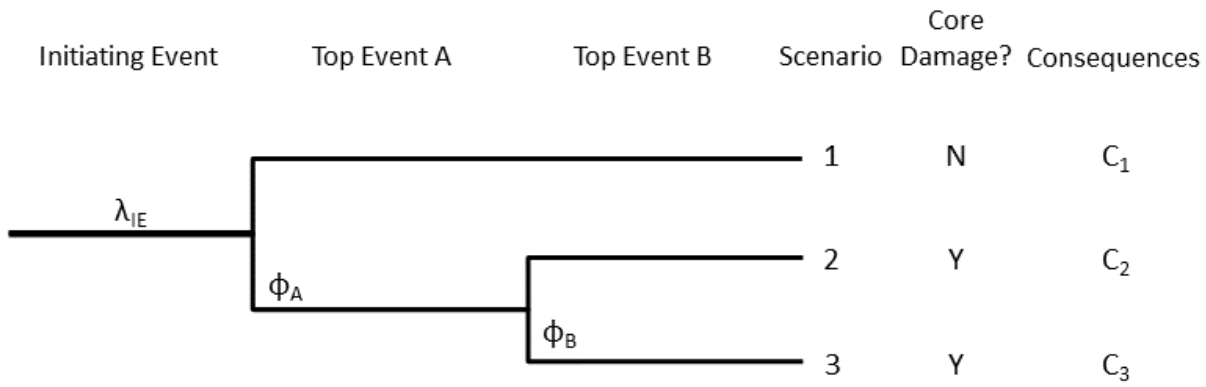


FIG. 23. Example Event Tree.

The initiating event frequency is denoted by λ_{IE} and the branching probabilities are denoted by the ϕ's. These probabilities are, in the most general case, path dependent (i.e. they are

[22] In practical terms, Top Events A and B could be interpreted as representing highly simplified representations of systems and actions that prevent core damage (i.e. Level 1 PSA) and systems and actions that mitigate the releases from a core damage event (i.e. Level 2 PSA), respectively.

conditioned upon preceding events in the event tree) and thereby account for aleatory dependencies in the scenario. The scenario dependent consequences (Ci), which can represent Level 2 metrics (e.g. source term characteristics) or Level 3 metrics (e.g. public health effects) are aleatory variables. In general, the Ci are vector valued quantities; however, to simplify the discussion, they are treated as scalars in this appendix to limit discussions of multivariate probability distributions. Treating the Ci as vectors would increase the complexity of the mathematical notation but would not change the fundamental results of interest to this publication.

I.1. ASSUMPTIONS

This section provides a detailed discussion of the three major assumptions listed above.

I.1.1. Assumption 1 — random events occurring over time

Random events occurring over time (e.g. initiating events, runtime failures) can be reasonably modelled as Poisson processes. Thus, the probability of observing N such events in a specified time interval (0, τ) is given by the Poisson distribution:

$$P_N(n) = P\{N\ events\ in\ (0,\tau)|\lambda\} = \frac{(\lambda\tau)^n}{n!}e^{-\lambda\tau} \quad (5)$$

where λ, the single parameter characterizing the distribution, is the frequency of the process.

The parameter λ has units of inverse time and is called the frequency of the process. Since specifying this parameter completely characterizes the Poisson distribution, the left hand side of Eq. (5) is often written as a conditional probability: $P\{N = n\ events\ in\ (0,\tau)|\lambda\}$.

Poisson processes are 'memoryless' and the probability of observing N = n events in the time interval (0, τ) is independent of the number of events observed prior to that interval. Eq. (5) can actually be derived from more formal mathematical statements of the memoryless property. Epistemic uncertainties in the value of the estimated frequency, λ, are typically characterized with continuous probability distributions, which can be updated using a Bayesian approach.

From Eq. (5), it can be seen that the probability of observing no events in (0, τ) is $e^{-\lambda\tau}$. Thus, the probability of observing one or more events in that time interval is $1 - e^{-\lambda\tau}$. The mean ('expected') number of events in the time interval (0, τ) is equal to λτ.[23]

Let T be a random variable representing the time of the first occurrence of an event generated by a Poisson process with characteristic frequency λ. (For example, T can represent the failure time of a running component.) It can be shown that T is exponentially distributed, also with characteristic frequency λ. The cumulative distribution function and probability density function for T are, respectively

$$F_T(t) = P\{T \le t\} = 1 - e^{-\lambda t} \cong \lambda t\ when\ \lambda t < 0.1 \quad (6)$$

$$f_T(t) = \lim_{dt\to 0}\frac{P\{t\le T<t+dt\}}{dt} = \lambda e^{-\lambda t} \quad (7)$$

[23] In this appendix, as in the literature, the terms 'mean value,' 'average value,' and 'expected value' refer to the same concept: the mathematical expectation of the variable. This is discussed further in later portions of this appendix.

From Eq. (6), it can be seen that shorter occurrence times are more likely than longer ones, i.e. Poisson process events are not regularly spaced in time. A representative time trace of events, developed from a random sample of exponentially distributed event times, actually shows clusters, as illustrated in Fig. 24. As per the assumption of a memoryless process, the likelihood of a future event is unaffected by the past. For example, it is not unreasonable for two 100-year floods to occur within a few years of each other or that a 100-year period may elapse without the occurrence of at least one 100-year flood.

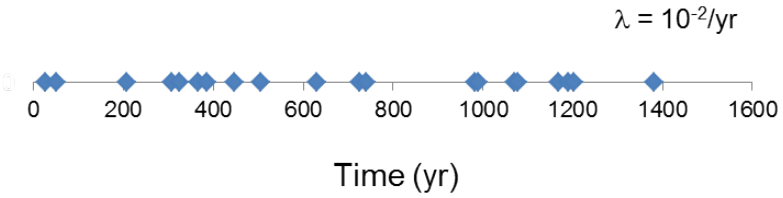


FIG 24. Example time trace for a Poisson process.

I.1.2. Assumption 2 — random events occurring in response to demands

Random events occurring in response to demands (e.g. failures to change state on demand, initiating events occurring in response to manipulations or tests fixed in time) can be reasonably modelled as Bernoulli ('coin flip') processes. Thus, the probability of the random variable N being equal to n such events in a specified number of trials (demands), m, is given by the binomial distribution:

$$B_N(n) = P\{N = n \text{ events in } M \text{ trials}\} = \frac{m!}{n!(m-n)!}\phi^n(1-\phi)^{m-n} \quad (8)$$

The parameter ϕ is dimensionless and is called the event probability for a single trial. Since specifying this parameter completely characterizes the binomial distribution, the left hand side of Eq. (8) is often written as a conditional probability: $P\{N = n \text{ events in } m|\phi\}$.

The parameter ϕ quantifies the likelihood of a particular outcome of a random trial, i.e. it measures aleatory uncertainty. To emphasize this point, especially in the case of event trees such as shown in Fig. 23, it sometimes is called a 'split fraction' or a 'conditional split fraction.' Epistemic uncertainties in the value of ϕ are typically characterized with continuous probability distributions, which can be updated using a Bayesian approach.

Bernoulli processes are 'memoryless' — the probability of observing N = n events in a set of m trials is independent of the number of events observed prior to those trials. (Eq. (8) can be derived from more formal mathematical statements of the memoryless property). It needs to be noted that the mean number of events in m trials is equal to ϕm.

I.1.3. Assumption 3 — accident scenarios in PSA models

Accident scenarios in the PSA models can be reasonably modelled as being stochastically independent. This assumption applies specifically to dependencies between scenarios in the PSA model. The appropriate treatment of dependencies within scenarios is critical to the PSA.

The existence of common event types in different accident scenarios does not necessarily imply stochastic dependencies between the scenarios. For example, Scenarios 2 and 3 in Fig. 23 both involve the same initiating event type (e.g. an earthquake of magnitude X) and the failure of

the system specified by Top Event A, but represent two separate occurrences.[24] Stochastic dependencies could arise if the actual events (e.g. the earthquakes) are correlated, but this is counter to Assumptions (A) and (B) above. This can be treated by dynamic PSA, where time dependence is considered.

One potential source of intra scenario stochastic dependency involves situations where components are unavailable (e.g. due to maintenance) for an extended period of time. In such situations, the relevant basic event can be shared between scenarios. For example, the period of unavailability for a component may be long enough such that more than one initiating event could reasonably occur during that period. However, in most practical PSA applications, it can be expected that the degree of intra scenario dependency is small.

Stochastic dependencies can also exist for scenarios triggered by separate, but correlated hazards (e.g. external flooding and high winds due to same storm). From a general PSA modelling standpoint, it appears that such situations are best treated as single scenarios with multiple, correlated hazards. However, the practical assessment of such combined hazard scenarios is an area of ongoing research.

I.2. ACCIDENT SCENARIO OCCURRENCES

Let λ represent the frequency of events generated by a Poisson process, and ϕ represent the fraction of times an event is actually counted (so the fraction of times an occurring event is ignored is $1 - \phi$). It can be shown that the number of counted events is governed by a Poisson process with frequency $\lambda\phi$.[25] Therefore, generalizing to an event tree scenario, applying Assumptions 1 and 2 mention in Section I.1 the occurrence of a given accident scenario is a Poisson processes with frequency equal to the product of the initiating event frequency and the probabilities of subsequent events (for success or failure, conditioned as appropriate on preceding events) defined by the scenario (see Property I).

For example, in the case of Fig. 23, the occurrence of Scenario-2 type events is governed by Eq. (4), with frequency $\lambda_2 = \lambda_{IE}\phi_A(1 - \phi_B)$. Note that Property I applies to sequence level cut sets (i.e. the result obtained after linking fault trees for the event tree top events).

I.3. END STATE FREQUENCIES

Consider a situation where a final state (e.g. end state) may be reached from an initial state by a number of independent Poisson processes related to various initiating events and so called 'competing risks'[26], as illustrated by the multiple paths in Fig. 25.

---

[24] Accident scenarios can be viewed as random events in time. If the occurrence of one scenario does not affect the likelihood of occurrence of subsequent scenarios, the scenarios are stochastically independent. (Of course, this is an idealization, as the actual occurrence of a major accident can lead to significant changes in the industry.)

[25] Such a partial counting process is sometimes called a 'filtered Poisson' process.

[26] This situation is a simple version of the so called 'competing risks' problem, where the term 'risk' is used in the sense of a hazard.

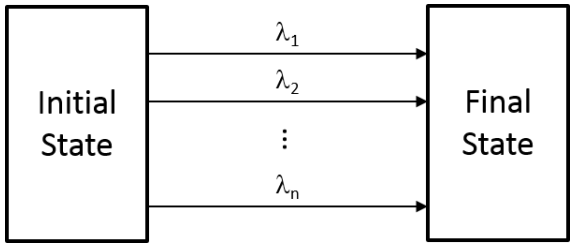


FIG. 25. Competing risks model.

Noting that the path transition times from the initial to the final state are random, for any given trial, the transition from initial to final state occurs along the quickest transition for that trial. Thus, the overall transition time is the minimum of the path transition times. It can be shown relatively easily that the overall transition from the initial state to the final state is governed by a Poisson process with frequency equal to the sum of the individual transition frequencies. Applying this result to PSA models, the occurrence of a specified end state is a Poisson process with frequency equal to the sum of the frequencies of the scenarios leading to that end state.

In the event tree of Fig. 23, for example, the occurrence of core damage is a Poisson process with frequency $\lambda_{CD} = \lambda_2 + \lambda_3$.

I.4 END STATE PROBABILITIES

In situations where the plant's nominal operating condition remains constant over the time interval of interest, the probability of transitioning to a particular end state (e.g. core damage) in that time interval is given by Eq. 6 and dictated by Property II.

In cases where the plant changes condition (e.g. as it progresses through various plant operational states during an outage), determination of the end state probability is straightforward (at least in principle).

Consider a situation where at a defined point in the time interval of interest, the system changes from one plant operational state (i.e. mode) to another (see Fig. 26).[27]

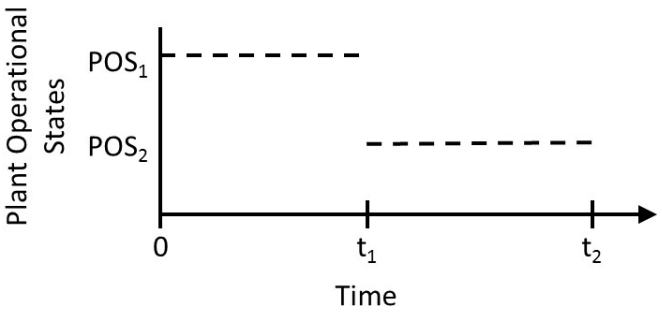


FIG. 26. Phased mission example.

Assuming that end state transitions are final (i.e. achieving the end state precludes any subsequent transitions), the probability of an end state transition over the total interval $[0, t_2]$ is approximately the sum of individual transition probabilities for the two phases.

[27] Analyses of such situations are sometimes called 'phased mission' analyses.

In this example, assuming for simplicity that the event tree structure remains constant over the two phases and using the approximation from Eq. (6),

$$P\{T_{CD} \leq t_2\} = \left[1 - e^{-\left(\lambda_2^{(POS_1)} + \lambda_3^{(POS_1)}\right)t_1}\right] + e^{-\left(\lambda_2^{(POS_1)} + \lambda_3^{(POS_1)}\right)t_1}\left[1 - e^{-\left(\lambda_2^{(POS_2)} + \lambda_3^{(POS_2)}\right)(t_2 - t_1)}\right]$$

$$\cong \left[\lambda_2^{(POS_1)} + \lambda_3^{(POS_1)}\right] t_1 + \left[\lambda_2^{(POS_2)} + \lambda_3^{(POS_2)}\right](t_2 - t_1) \quad (9)$$

for typical values of initiating event frequencies and top event probabilities, and where the superscript '(POS_j)' indicates the appropriate plant operational state.

Akin to the point raised in I.1.3, notably there could be cases where a prolonged equipment outage during the first phase could carry over into the second phase, thereby introducing a dependency between the phases. In principle, such cases can be treated through appropriate conditioning of the probability of core damage during the second phase. In practice, the numerical effects of such dependencies are expected to be small.

I.5. CONSEQUENCE PROBABILITIES

The preceding sections deal with binary consequence measures — the occurrence or non occurrence of specified end states. For more general consequence measures (e.g. the amount of radiological material released, the number of public health effects), the magnitudes of which are values of scenario dependent random variables, the approach to aggregation is straightforward in principle but can be somewhat complicated from a computational point of view.

Consider the consequences from scenario i, whose magnitude is denoted by the random variable C_i. The aleatory uncertainty in the set of consequences for n scenarios, $\underline{C} = \{C_1, C_2, \ldots, C_n\}$, is characterized by a joint probability distribution. For example, if n = 2, $\underline{C} = \{C_1, C_2\}$ and the joint probability density function is defined by

$$f_{C_1,C_2}(x,y) = \lim_{dx,dy \to 0} \frac{P\{(x \leq C_1 < x+dx) AND (y \leq C_2 < y+dy)\}}{dxdy} \quad (10)$$

As it was stated above, for a specified consequence measure, the total probability distribution quantifying the aleatory uncertainty in that measure is the weighted sum of the contributions from all scenarios in the PSA model. The mean value of the consequence measure is the sum of the mean values of the contributions.

The weighted sum of the contributions to a consequence measure is the sum of the products of the likelihood of occurrence of a given accident scenario, p_i, and the distribution of the resulting consequences, $f_{C_i}(c)$, where c is some specified level of consequence. In the case of our simple example in Fig. 23, assuming that the consequences from non core damage scenarios are negligible, and assuming that the C_i are positively valued, the probability density function of the total consequence is given by

$$f_{C_T}(c) = \sum_{i=1}^{n} p_i \cdot f_{C_i}(c) \quad (11)$$

Aleatory uncertainties in the consequences for a given scenario are explicitly treated for Level 3 PSA, but are typically neglected in Level 2 PSA[28].

I.6. UNCERTAINTIES AND MEAN VALUES

The preceding discussions are focused on the treatment of aleatory uncertainties. However, the results hold even when there are epistemic uncertainties in the scenario frequencies and consequences and, therefore, in the end state frequencies and total consequences. The following discussion addresses the computation of mean values and other important characteristics (e.g. distribution percentiles) characterizing these epistemic uncertainties.

The notation $\pi(\bullet)$ is used to refer to the joint probability density function characterizing epistemic uncertainties. This is in contrast to the notation $f(\bullet)$, used earlier to refer to the joint probability density function (i.e. the joint distribution) characterizing aleatory uncertainties.

Although the concepts of aleatory and epistemic uncertainties are distinct, both $\pi(\bullet)$ and $f(\bullet)$ are probability distributions and are subject to the same mathematical laws of probability. Thus, many of the following results are mathematically identical to results presented previously with regard to frequency and probability estimates.

In principle, this section's discussion applies to all PSA levels. However, it needs to be noted that although the modelling conventions for addressing aleatory and epistemic uncertainties are well established and routinely implemented for Level 1 PSA, they are still a matter of discussion for the severe accident analysis portion of Level 2 PSA. For Level 3 PSA, epistemic uncertainties associated with environmental transport, population exposure, and ultimate effects are often acknowledged and treated with sensitivity studies, but typically are not treated with a full probabilistic analysis.

I.6.1. End state frequencies and probabilities

The mean ('expected value') frequency/probability of an end state is the sum of the mean frequencies/probabilities for the scenarios leading to that end state. Let $g(\underline{\lambda})$ be the sum of the λ_i:

$$g(\underline{\lambda}) = \sum_{i=1}^{n} \lambda_i \tag{12}$$

$$E\left[g(\underline{\lambda})\right] = \sum_{i=1}^{n} E[\lambda_i] \tag{13}$$

It is important to note that this relation holds regardless of the distributional form of the joint distribution for $\underline{\lambda}$ and, therefore, regardless of the shape of the marginal distribution for each λ_i and the degree of (epistemic) dependency between the λ_i. A similar result holds for the sum of end state probabilities (e.g. when summing over different operational states over the course of a refuelling cycle).

$E[\lambda_i]$, the mean value of the scenario frequency λ_i, is the product of the mean values of the scenario parameters (initiating event frequencies, probabilities of subsequent events) if, as is usually the case, those parameters are assumed to be epistemically independent (i.e. there are

[28] The latter generally attempt to define scenarios in a manner to account for major sources of aleatory uncertainty, and then use deterministic models to estimate the consequences for these scenarios.)

no state of knowledge dependencies). Thus, for Scenario 2 in Fig. 23, the mean value of the scenario frequency is given by $E[\lambda_2] = E[\lambda_{IE}]E[\phi_A](1-E[\phi_B])$ if the parameters λ_{IE}, ϕ_A, and ϕ_{B1} are epistemically independent. If the parameters (or a subset of the parameters) are completely dependent, methods such as those described in NUREG-1855 [12] can be applied. Both the completely independent and completely dependent cases are treated by typical PSA software tools. Situations involving partial epistemic dependency require no analytical developments, but will require the assessment and quantification of such dependencies, and the development of appropriate simulations and software algorithms to propagate the dependencies through the PSA model.

The mean is defined without any reference to the 'centre' of the joint distribution for $\underline{X}$. For example, for many PSA parameters of practical interest, the mean value of a parameter can correspond to a very high percentile for that parameter. The lack of correspondence between the mean value and the distribution median or mode needs to be kept in mind when considering the meaning of an aggregated result (as discussed in Section 2.3).

In practice, the mean value of the end state frequency can be developed from a 'point estimate' calculation performed using the mean values of the contributing scenario frequencies, as shown by Eq. (13), or from a sampling based calculation where input parameter uncertainties are propagated through the PSA model using Monte Carlo or other sampling techniques.

It needs to be noted that the epistemic probability distribution for the frequency/probability of an end state is the probabilistic sum of the distributions for the contributing frequencies/probabilities. The problem of aggregating epistemic distributions for end state frequencies/probabilities has the same mathematical characteristics as the problem of aggregating aleatory distributions for consequences (discussed in Section I.5). Thus, for example, the epistemic distribution for the core damage frequency in our simple example of Fig. 23 is computed using the joint epistemic distribution for λ_2 and λ_3:

$$\pi_{\lambda_{CD}}(\lambda) = \int_0^{\lambda} \pi_{\lambda_2,\lambda_3}(x, \lambda - x)dx \tag{14}$$

In practice, the distributions for the end state frequencies/probabilities are typically developed using Monte Carlo or other sampling techniques. This facilitates the treatment of epistemic dependencies between scenarios (e.g. due to shared model parameters).

I.6.2. End state consequences

The mean consequence is the weighted sum of the mean contributions from all scenarios. This property holds for the total consequence when averaged over all aleatory and epistemic uncertainties.

Using the event tree of Fig. 23 as an example, assume that the non core damage scenarios (Scenarios 1) have negligible consequences. Further assume that the aleatory distributions $f_{C_i}(\bullet)$ for the scenario consequences C_2 and C_3 are characterized by parametric distributions with characteristic values $\underline{\theta}_2$ and $\underline{\theta}_3$[29]. The expected value of C_T is given by

[29] For example, if the distribution for C2 is lognormal, $\underline{\theta}_2$ is a two parameter vector.

$$E[C_T] = \int_{All\ \underline{\theta}_3} \int_{All\ \underline{\theta}_2} \left(E\left[C_2|\underline{\theta}_2\right] + E\left[C_3|\underline{\theta}_3\right]\right) \pi_{\underline{\Theta}_2,\underline{\Theta}_3}\left(\underline{\theta}_2, \underline{\theta}_3\right) d\underline{\theta}_2 d\underline{\theta}_3$$
$$= E[C_2] + E[C_3] \quad (15)$$

where $\pi_{\underline{\Theta}_2,\underline{\Theta}_3}\left(\underline{\theta}_2, \underline{\theta}_3\right)$ is the joint density function for $\underline{\theta}_2$ and $\underline{\theta}_3$ and

$$E\left[C_i|\underline{\theta}_i\right] = \int_0^\infty c \cdot f_{C_i}\left(c|\underline{\theta}_i\right) dc \quad (16)$$

$$= \sum_{i=1}^n p_i\, E[C_i] \quad (17)$$

The average aleatory distribution for the total consequence C_T can be developed in a similar manner.

$$E[f_c\left(c|\underline{\theta}\right)] = \int f_C\left(c|\underline{\theta}\right) \pi_{\underline{\theta}}\left(\underline{\theta}\right) d\underline{\theta} = \int \sum p_i\, f_{c_i}\left(c|\underline{\theta}_i\right) \pi_{\underline{\theta}}\left(\underline{\theta}\right) d\underline{\theta} \quad (18)$$

where $\underline{\theta} = \{\underline{\theta}_1, \underline{\theta}_2, ..., \underline{\theta}_n\}$. In principle, the above results can be readily generalized for more complicated problems. In practice, the average aleatory distribution is typically estimated using sampling based methods.

APPENDIX II. EXAMPLE OF RISK AGGREGATION FOR DIFFERENT HAZARDS

This appendix discusses how risk aggregation results could be obtained and displayed in the context of decision making, assuming the specific case of an individual PSA model for a site that has developed detailed analyses for multiple individual hazards.

It needs to be noted that, while based on actual plant results in some cases, the material presented here is for illustration purposes, as opposed to a prescriptive approach on how risk aggregation needs to be done. Given the variability in design, operations, site specific hazards, modelling approaches, and IRIDM frameworks, these examples are also not meant to indicate a specific risk profile that would be expected for all nuclear power plants.

In addition, the example focuses on a single metric (i.e. core damage frequency, CDF) but could be replicated for other metrics; assuming the underlying modelling has been correctly performed. Discussion of whole site PSA, MUPSA, and LPSD examples are also not included, as this discussion is not intended to be exhaustive, although similar illustrations could be represented here for these cases (assuming metrics are appropriately aggregated, as discussed in the main text).

Finally, it needs to be noted that this discussion follows a similar example on risk aggregation performed in 1980 for the Indian Point nuclear power plant in the state of New York, in the United States of America (titled the 'Indian point probabilistic safety study' or IPPSS) [13]. This early PSA study was one of several seminal efforts within the nuclear power plant industry to perform an in-depth safety review of the design and operations of nuclear installation for the purposes of addressing concerns about safety. It used the state of the art knowledge of PSA methods and tools at the time (which has significantly evolved since then) but it represented a significantly detailed study with presentation of details that included frequencies and consequences of specific accident scenarios as well as the presentation of a large amount of risk results and information. This effort was subject of several discussions and additional activities [49], but it also provides an early example of risk aggregation that is still relevant for the current, more widespread use of nuclear reactor PSA and risk information in general.

In particular, it needs to be noted that IPPSS provided aggregated risk results (including uncertainty information) for individual and multiple hazards to include the frequency of core melt, source terms, releases, and consequences for individual reactors as well as accidents assumed to involve both Unit 2 and Unit 3. While the specific results are not necessarily relevant to current reactors (or to the Indian Point reactors themselves, still in operation); the overall approach can be replicated using modern PSA models. For example, the CDF results are replicated in Fig. 27 from [13], the total aggregated frequency is shown for the hazards considered in IPPSS (i.e. internal events, internal fire, high winds, and seismic).

Again, while the actual results or the ranking of the individual hazards is not important here, the overall approach highlights the assembly of individual contributors and their associated uncertainty characterization in a single total aggregated result. As discussed in Section 3, whether the PSA modelling approach includes separate individual models or an integrated single PSA model (for hazards, multi-units, and/or multi sources), if the integration has been properly performed either in advance or in post processing, a similar depiction of the results as shown in Fig. 27 can be performed.

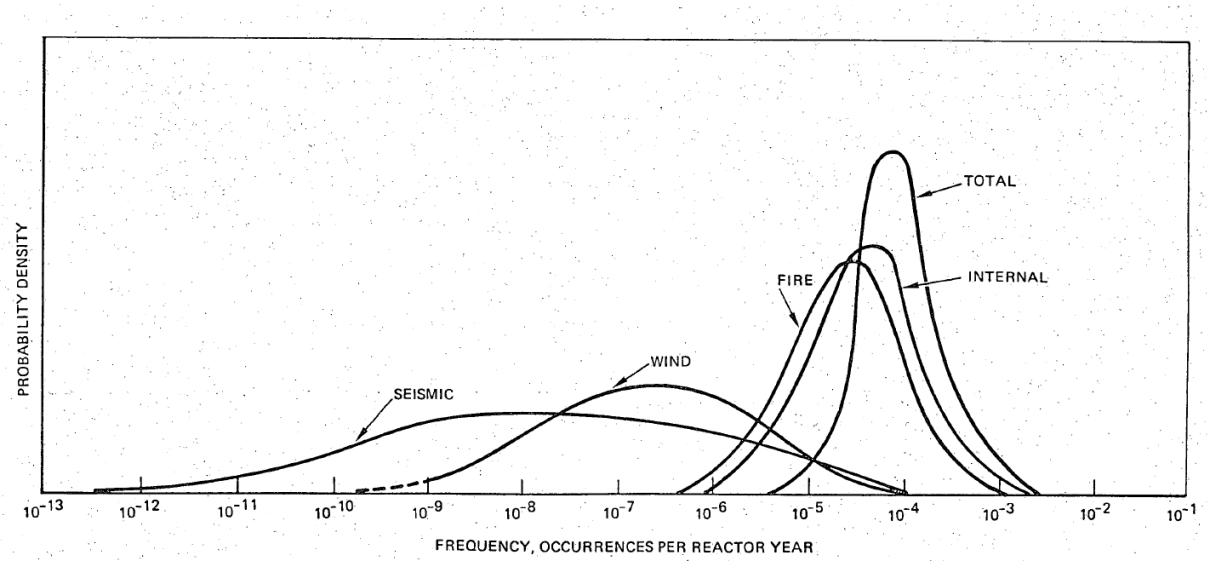


FIG. 27. IPPSS core melt frequency results for various hazards for Indian Point Unit 3.

Hence, it is important to understand how the structure can be derived and presented here. As discussed in Appendix I, Section I.6.1, the scenario frequency λ_i can be treated as a random variable with mean expressed as $\mu_i = E[\lambda_i]$, and standard deviation σ derived from $\sigma_i^2 = E[\lambda_i^2] - (E[\lambda_i])^2$. The mean of the sum of multiple λ_i is the sum of the mean of the individual λ_i for various scenarios/hazards. As stated in Annex I, this holds regardless of the distributional form of the underlying λ_i contributors.

However, it needs to be noted that metrics such as CDF and LRF/LERF are derived from the frequency distributions of multiple accident sequence scenarios which, in turn, are a function of cutsets with large combinations of summation and multiplication of basic events (random variables themselves). Hence, the resulting uncertainty characterization of λ_i as a frequency in nuclear PSAs is more often approximated as quasi lognormal distributions (as the multiplication of random variables tends towards a lognormal distribution which overwhelms the summation tendency towards a lognormal distribution).

In addition, the underlying result for a hazard will be subject to state of knowledge correlation (SOKC) effects, as mentioned in Appendix I, such that the uncertainty propagation through cutsets will be impacted by common uncertainty data in basic event models (i.e. basic events that appear in multiple cutsets modelled with the same mean and uncertainty distribution). This will result in the potential for some distortion in the individual λ_i mean derived from point estimates that could underestimate the actual mean. This is a well known effect in PSA modelling that is usually dependent on the level of dependency in the results (which can range from limited to significant). As stated in NUREG-1855 [12] and other publications, the influence or importance of the SOKC on the value of the risk metrics will vary from case to case. Typically, this effect will be limited in specific hazard models or accident scenarios and, if it can be demonstrated that the effect will be minimal, approximated point estimates results will not exhibit significant distortions [50] (however, it needs to not be assumed a priori).

— To complete the discussion in Fig. 27, it needs to also be clearly understood that the figure displays the probability density functions that correspond to the μ_i, σ_i, and the distributional form of individual λ_i in the following way: The x-axis displays the

frequency of core met (per reactor year) in a lognormal scale such that the base of 10 indices are clearly visualized.

— The actual distributions shown represent the transformed normal distribution space such that, if an actual lognormal distribution were assumed to represent an individual λi then it would appear as an exact normal distribution in the transformed space. In other words, the plotted distributions are $\Lambda i = \log(\lambda i)$, where Λi is the lognormal transform of λi (i.e. which has the effect of usually turning skewed distributions into a more centralized representation).

— Since this is a probability density function plot, the y-axis will show the weighted scale of the density functions magnitude that would result in the area under each curve to integrate to 1 (an intrinsic property of probability density functions). These values tend to be rather large and are not relevant for practical discussion purposes (so they were omitted in the IPPSS plots).

While the first and third statements are self explanatory, the second one bears additional discussion to clarify potential misperceptions: no actual change in the distributional form of λ_i is taking place here (i.e. it is not being suggested here that λ_i needs to have a normal distribution). The transformed normal space is used for ease of visualization purposes, since plotting the actual distributions (which, again, tend to exhibit quasi lognormal characteristics in PSA) will result in highly distorted curves which will not aid in communicating the result (most likely, a major reason the IPPSS presented the results in this manner).

Figure 28 replicates in approximate manner the format and results shown in Fig. 27. While the actual PSA model and detailed cutset results are not available, the distribution form for individual λ_i are approximated as lognormal distribution functions with estimated μ_i, σ_i in order to obtain a similar representation. It needs to be noted that, maybe due to SOKC issues and/or the approach used to perform the Monte Carlo simulation in IPPSS, the distributions in Fig. 27 may not exactly follow lognormal distributions, but the replicated results are sufficiently similar. As stated above, since the actual distributions for the individual λ_i are lognormal, they are shown in their normal equivalent distribution in Fig. 28 for visualization purposes, as discussed above.

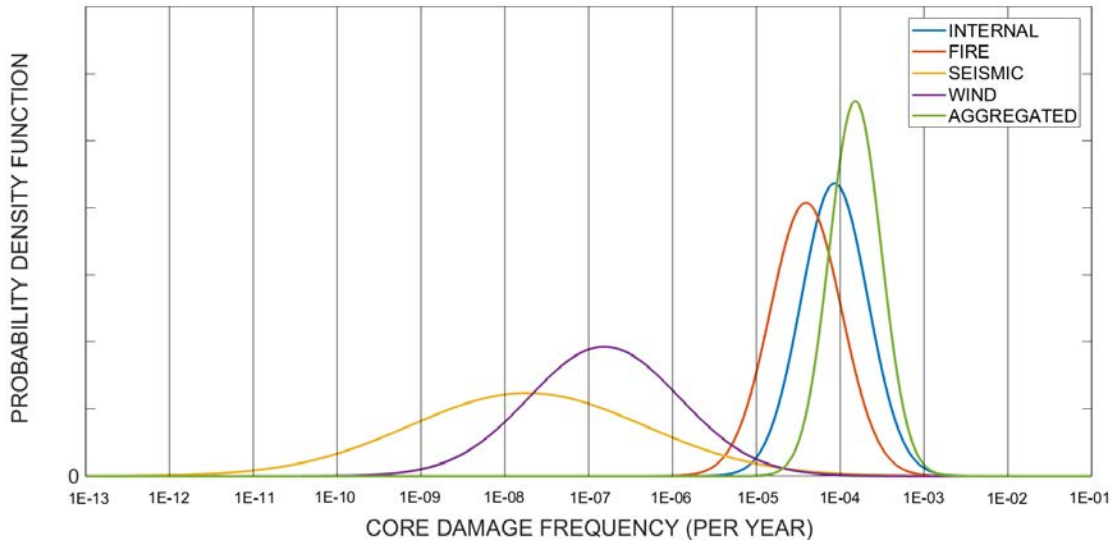


FIG. 28. Replicated IPPSS core melt frequency plot using estimated lognormal distributions plotted in the equivalent normal space.

An illustrated example with actual numerical results, based on the previous discussion, can be performed in a simplified manner using typical outputs from a current PSA model for multiple hazards. Assume the following results for CDF are shown in Table 2.

TABLE 2. RESULTS FOR EXAMPLE 1: RISK AGGREGATION ACROSS MULTIPLE HAZARDS

Hazard	95th Percentile	Mean	Median	5th Percentile	Error Factor	Standard Deviation
Internal	7.3E-05	5.0E-05	4.9E-05	3.2E-05	1.5	1.3E-05
Fire	3.2E-05	2.0E-05	1.9E-05	1.1E-05	1.7	6.6E-06
Seismic	3.0E-05	1.4E-05	1.2E-05	4.8E-06	2.5	8.4E-06
Wind	1.3E-05	7.0E-06	6.4E-06	3.2E-06	2.0	3.1E-06
Aggregated	1.2E-04	9.1E-05	8.9E-05	6.7E-05	1.4	1.7E-05

Typically, these distributions will be close to lognormal, as mentioned above; but the actual output may deviate from an exact lognormal fit. If available, the output of the Monte Carlo propagation can be used directly and a better fit with another distribution or even an empirical distribution that fits the data more closely can be used. These examples are not supposed to imply a lognormal distribution is to be always used or that this is the expected distribution function for all data from a PSA model. Instead, for simplicity purposes, lognormal distributions are developed for each hazard which closely match the information above (i.e. assuming the μ_i, σ_i values are given by the information above under a lognormal model). Fig. 29 shows the corresponding individual λ_i, as well as the aggregated total λ_T.

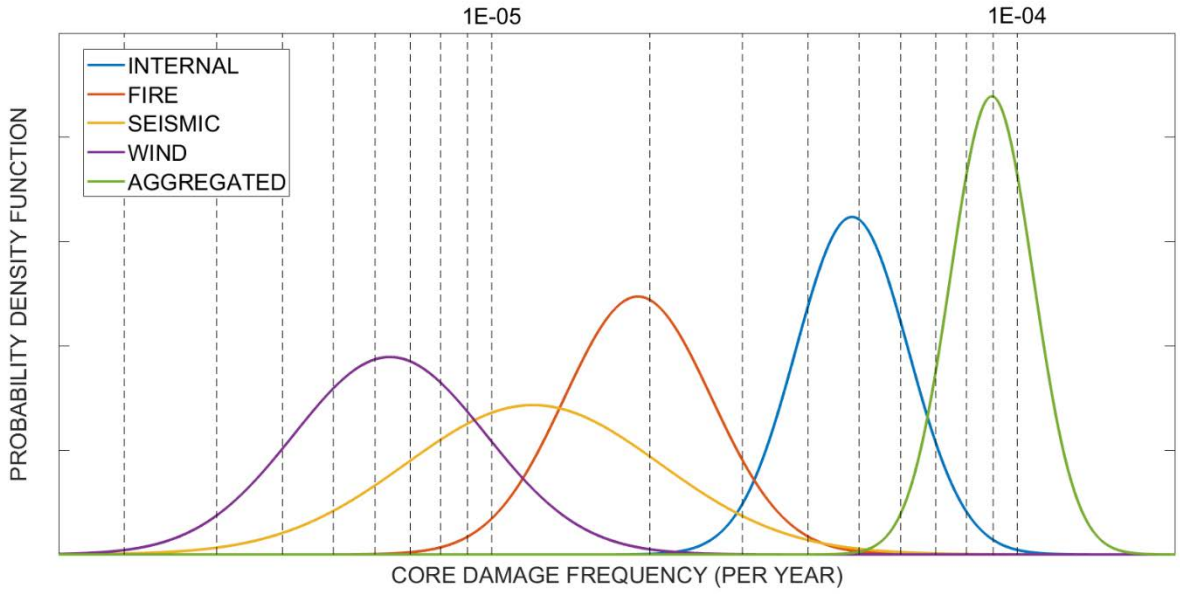


FIG. 29. Example 1 for the individual hazard CDF distributions and aggregated CDF based on the values presented in Table 2.

Notably, since the results are derived from numerical values rather than propagated output distributions, the aggregated total λ_T was obtained via Monte Carlo simulation of the summation of each distribution, where $E(\lambda_T)$ is calculated using Eq. (13) and the resulting aggregated distribution form is quasi-lognormal as shown in Fig. 30 for the μ_T, σ_T corresponding to the aggregated results in Table 2.

An important aspect to note here is that while the error factor (EF) shown for the fitted lognormal distributions is lower for λ_T than for the individual λ_i, this does not mean the resulting aggregated distribution is less uncertain than the individual λ_i (which would violate the expected effect on the standard deviation of the distribution that is the sum of individual distributions, based on first principles). In fact, the resulting distribution form for λ_T has a higher standard deviation. The error factor values are shown here since they are commonly used to represent the spread of lognormal distributions as a ration of the 5th or 95th percentiles to the median value, but the standard deviation results could have been displayed instead.

As stated previously, different PSA models will reflect a variation across different plants for various risk contributors. Another example is shown here to illustrate and reinforce that the focus of this appendix is on aggregating and displaying the results, not on what 'correct' or 'appropriate' PSA values for CDF has to look like. Example 2 is based on another set of individual PSA results as shown in Table 3. Unlike Table 3, the individual λ_i error factor values (and therefore, standard deviations) are significantly larger (i.e. with more spread around the mean, median) to showcase the impact of different aggregated individual contributors. Figure 30 shows the corresponding individual λ_i, as well as the aggregated total λ_T for Example 2.

TABLE 3. RESULTS FOR EXAMPLE 2: RISK AGGREGATION ACROSS MULTIPLE HAZARDS WITH WIDER UNCERTAINTY DISTRIBUTION CHARACTERISTICS FOR SPECIFIC INPUTS

Hazard	95th Percentile	Mean	Median	5th Percentile	Error Factor	Standard Deviation
Internal	1.5E-05	1.0E-05	9.7E-06	6.5E-06	1.5	2.5E-06
Fire	6.0E-05	2.5E-05	2.0E-05	6.7E-06	3.0	1.9E-05
Seismic	1.6E-04	5.0E-05	3.1E-05	6.2E-06	5.0	6.4E-05
Wind	1.7E-05	5.0E-06	2.5E-06	3.5E-07	7.0	8.7E-06
Aggregated	2.0E-04	9.0E-05	7.3E-05	3.4E-05	2.8	6.7E-05

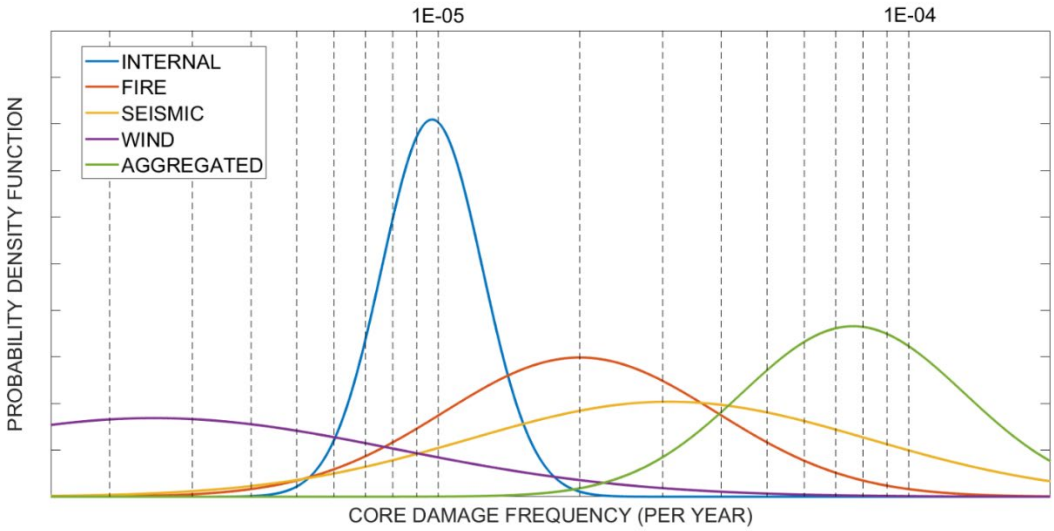


FIG. 30. Example 2 for the individual hazard CDF distributions and aggregated CDF based on the values presented in Table 3.

As one can see, the aggregated result is impacted by the increased uncertainty in some of the inputs (especially external hazards such as seismic and high winds, which would be indeed expected) by resulting in a wider distribution for λ_T, albeit still following a quasi-lognormal distribution.

The illustrated examples presented here represent only one approach to visualizing the result. Many other plots and visual aids can be used and several PSA software packages can produce graphic results. In addition, an integrated PSA model as discussed in Section 3, can be capable of directly producing an aggregated distribution that accounts for dependencies in the different hazards, as well as producing uncertainty characterization for λ_T and all λ_i. The summed λ_i approach may work when distortions due to SOKC and other effects are shown to not be significant and are not be assumed in advance, although this may provide a useful approximation when separate PSA models are used. As always, producing PSA results for risk aggregation purposes is only one step in a RIDM framework, where the underlying technical adequacy of the assumptions, other engineering aspects, and an overall decision making framework also need to be considered.

APPENDIX III. CHALLENGES OF PSA APPLICATIONS IN TERMS OF RISK AGGREGATION

Table 4 below presents the challenges expected for certain PSA applications in terms of risk aggregation. The PSA application categories and areas of PSA applications are adapted from IAEA-TECDOC-1804 [4]. The challenges are described in 3 categories: challenges related to the completeness, conservatism and uncertainties in the aggregated risk results.

TABLE 4. CHALLENGES EXPECTED FOR CERTAIN PSA APPLICATIONS IN TERMS OF RISK AGGREGATION

PSA Application Category	Area of PSA Application	Challenges in terms of risk aggregation
1. Safety assessment	1.1 Assessment of the overall plant safety 1.2 Periodic safety review 1.3 Analysis of the degree of defence in depth and safety margin against beyond design basis site hazards, including correlated site hazards	**Completeness** - Lack of completeness underestimates risk contribution from omitted elements (e.g. hazards, operating states or sources) **Conservatism** - Intentionally or forced conservatism or bounding assessments overestimate the risk. - Immature methods have the tendency to result in conservative estimates - The existence of a dominating risk element does not challenge the assessment of safety but can challenge the analysis of the defence in depth and safety margin as it may be related to non actionable elements (e.g. uncertainties of rare natural hazards) **Uncertainties** - Parametric uncertainties are not normally used for comparison with regulatory thresholds and therefore only play a role in the development of mean values - Epistemic uncertainties normally not included in the comparison with regulatory thresholds and only addressed via sensitivities.
2. Design evaluation	2.1 Application of PSA to support decisions made during the NPP design (plant under design) 2.2 Licensing of design 2.3 Optimization of protection against hazard events (e.g. fires, floods) and common cause failures, including consideration of correlated site hazards and hazard induced fires and floods	**Completeness** - Lack of completeness underestimates risk contribution from omitted elements (e.g. hazards, operating states or sources) **Conservatism** - Intentionally or forced conservatism or bounding assessments overestimate the risk. - Immature methods have the tendency to result in conservative estimates - The existence of a dominating risk element does not challenge the assessment of safety but can challenge the analysis of the defence in depth and safety margin as it may be related to

PSA Application Category	Area of PSA Application	Challenges in terms of risk aggregation
	2.4 Establishment of equipment reliability targets for manufactories 2.5 Identification of R&D which are necessary to support the design 2.6 Development operator procedures and training programs and support for Human Factors Engineering	non actionable elements (e.g. uncertainties of rare natural hazards) **Uncertainties** - Parametric uncertainties are not normally used for comparison with regulatory thresholds and therefore only play a role in the development of mean values - Epistemic uncertainties normally not included in the comparison with regulatory thresholds and only addressed via sensitivities.
3. NPP operation	3.1 NPP maintenance 3.2 Accident mitigation and emergency planning 3.3 Personnel training 3.4 Risk based configuration control (e.g. Exemptions to TS, Risk Monitors)	**Completeness** - Lack of completeness misses to identify components targeted for optimized maintenance. - Emergency planning is potentially more sensitive to aggregation of different sources into a Level 3 PSA aggregation - Total risk metrics (normally based on both total CDF/LERF and ΔCDF/ΔLERF) are potentially impacted by completeness of risk aggregation. **Conservatism** - Intentionally or forced conservatism or bounding assessments results in focusing on different set of components. - If one risk element is dominant and is not sensitive to operator actions, there is a risk of an artificially lowered importance of operator actions to be targeted with refined procedures or focused training - ΔCDF/ΔLERF may be artificially minimized if a conservative assessment is performed. **Uncertainties** - Uncertainties not normally consequential in identification of important components (risk importance measures are based on mean value)
4. Permanent changes to the operating plant	4.1 Plant changes 4.2 Technical specification changes (including surveillance test and ISI) 4.3 Establishment of graded QA programme for SSC	**Completeness** - Lack of completeness underestimates risk contribution from omitted elements (e.g. hazards, operating states or sources) - Total risk metrics (normally based on both total CDF/LERF and ΔCDF/ΔLERF) are potentially impacted by completeness of risk aggregation. - When importance measures are used as metric, they may ned to be corrected because of the challenge by aggregation of multiple hazards models. Importance measures are challenged

PSA Application Category	Area of PSA Application	Challenges in terms of risk aggregation
	4.4 Risk informed special site protection measures (e.g. fire, flood protection)	by combination of hazards, especially for hazards with high probabilities, which challenge the quantification and accuracy of the measures due to limitation in the rare events approximation validity. **Conservatism** - Intentionally or forced conservatism or bounding assessments overestimate the risk. - Immature methods have the tendency to result in conservative estimates - The existence of a dominating risk element does not challenge the assessment of safety but can challenge the analysis of the defence in depth and safety margin as it may be related to non actionable elements (e.g. uncertainties of rare natural hazards) **Uncertainties** - Parametric uncertainties are not normally used for comparison with regulatory thresholds and therefore only play a role in the development of mean values - Epistemic uncertainties normally not included in the comparison with regulatory thresholds and only addressed via sensitivities.
5. Oversight activities	5.1 Performance monitoring (e.g. planning inspections) 5.2 Performance assessment (evaluation of inspection findings, analysis of operational experience)	**Completeness** - As oversight activities are largely based on numerical risk thresholds, missing hazards or plant operating space impacts the definition of the acceptance thresholds. **Conservatism** - Conservative risk estimates may be translated in conservative and difficult to achieve risk thresholds. **Uncertainties** - Epistemic uncertainties normally not included in the comparison with regulatory thresholds and only addressed via sensitivities. - Lack of explicit sensitivities on epistemic uncertainties may miss to point to area more worth of performance monitoring because of limited dataset or agreed upon methods.
6. Evaluation of safety issues	6.1 Risk evaluation (e.g. corrective measures, ranking safety issues) 6.2 Regulatory decisions (long term and short term)	**Completeness** - Lack of completeness underestimates risk contribution from omitted elements (e.g. hazards, operating states or sources) **Conservatism**

PSA Application Category	Area of PSA Application	Challenges in terms of risk aggregation
		- Intentionally or forced conservatism or bounding assessments overestimate the risk. - Immature methods have the tendency to result in conservative estimates - The existence of a dominating risk element does not challenge the assessment of safety but can challenge the analysis of the defence in depth and safety margin as it may be related to non actionable elements (e.g. uncertainties of rare natural hazards) **Uncertainties** - Parametric uncertainties are not normally used for comparison with regulatory thresholds and therefore only play a role in the development of mean values - Epistemic uncertainties normally not included in the comparison with regulatory thresholds and only addressed via sensitivities

APPENDIX IV. EXAMPLES FOR RISK COMMUNICATION

This appendix provides examples relevant to the various types of communication discussed in Section 5.

IV.1 EXAMPLES OF RISK COMMINICATION WITH THE MANAGEMENT OF NUCLEAR INSTALLATION

As noted in Section 5.1, different types of information regarding aggregated risk estimates may need to be communicated from the PSA team to the management responsible for making decisions (see also [51]).

With regard to using risk information as an additional check on the overall level of NPP safety, a depiction such as that shown in Fig. 31 may be useful. This figure conveys the overall CDF as well the CDF for a range of contributing hazards. This information can be organized in different ways, such as by operating state, by single- vs. multi-unit risk. This particular depiction provides an indication of the uncertainty associated with the risk for each hazard as well as additional information relevant to understanding how meaningful the estimates are. If there is a specific acceptance criterion, this can be displayed as a point of comparison as well. Note that the information is presented in a manner that does not require an in depth understanding of probability distributions. The intent of this sort of depiction is to convey a sense of the uncertainty associated with the overall risk and the individual contributors without focusing on the numbers.

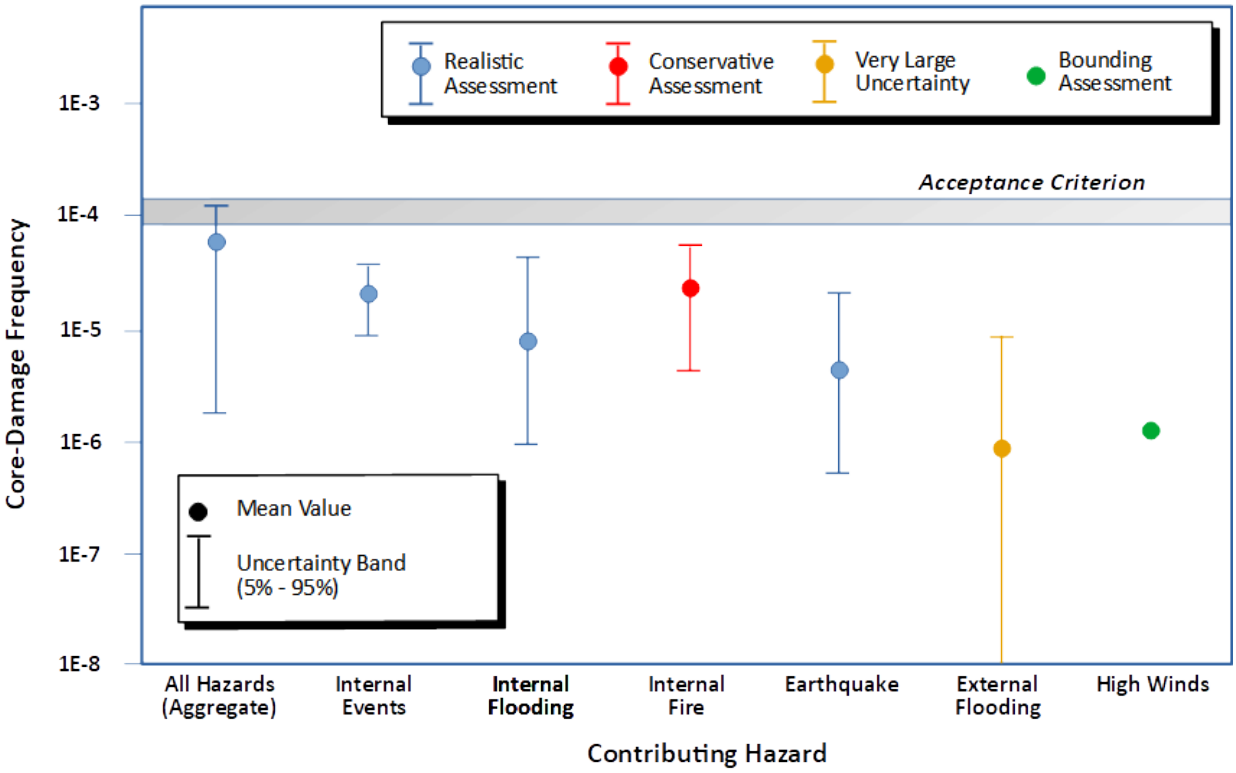


FIG. 31. Example illustration of overall risk and contributing hazards.

Section 5.1 also addresses the potential need to communicate information regarding significant new contributors to risk that may merit consideration regarding changes to the plant. As an example of such a communication, suppose a newly completed fire PSA has determined that a significant contributor to the frequency of core damage is due to a fire that could disable power

to both trains of the primary means of supplying suction to the auxiliary feedwater pumps after the initial inventory in the condensate storage tank is depleted. The information that would be of use to decision makers at the plant would include

— The relative contribution of this scenario to the aggregated risk;
— The relative contribution of this scenario to the fire CDF;
— Options that might be effective in addressing this risk contributor;
— The relative benefits and costs of each of the options.

A simple way to communicate some of this information in a format that is coming into increasing use among plant managers is via a 'heat map'. A 'heat map' can display a variety of types of information in a manner that makes different aspects easy to compare. A very simple example that might be applied in communicating the information about this potential fire scenario is shown in Fig. 32.

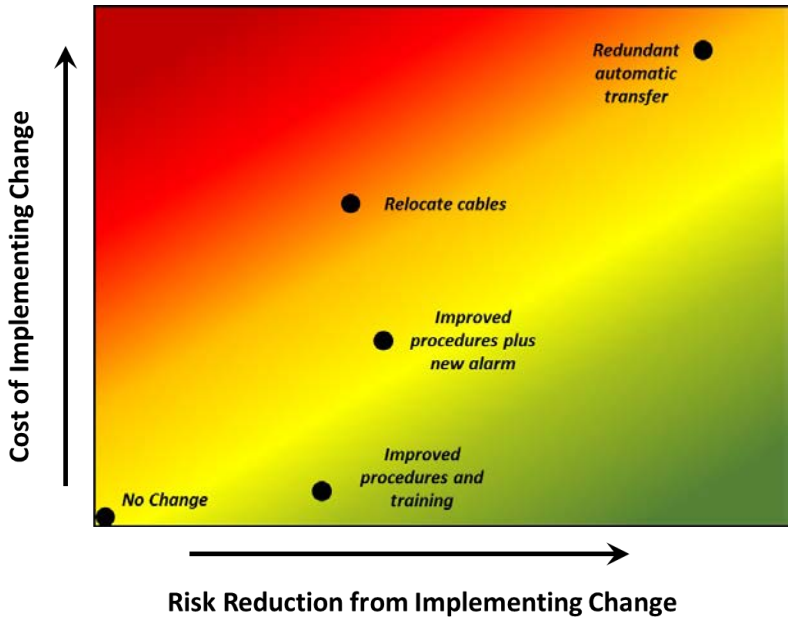


FIG. 32. Example of a 'heat map' for considering actions to address a significant risk contributor.

While this example might relate important information relatively quickly, it would require substantially more explanation to be of maximum use. For example, the 'heat map' does not provide a context for the risk contributor with respect to the aggregated risk, or even to the risk of fire. These contributions can be readily illustrated using such tools as pie or bar charts.

Even when the context for the contribution of this fire scenario is better established, it might be necessary to describe the elements in the 'heat map' more explicitly. An example of such a description is provided in Table 5. As the decision process proceeds, more specific estimates of the benefits in terms of risk reduction and the relative costs can be provided for consideration.

Another potential need for communication with plant management discussed in Section 5 may arise when there is a need to develop a risk informed context for an event or condition at the plant. This context may be important in determining whether some change to the plant is warranted to reduce the potential for or significance of such an occurrence in the future. For example, an occurrence in which there is a loss of the main condenser at a BWR (causing a reactor trip and closure of the main steam isolation valves) during a time when the reactor core

isolation cooling (RCIC) pump is out of service. The initiating event in this case is an infrequent, but not rare, occurrence. The most valuable insights may be obtained by calculating the CCDP given the occurrence of main steamline isolation for both the baseline PSA and for the situation in which RCIC is unavailable.

TABLE 5. EXAMPLE EXPLANATION OF ELEMENTS IN 'HEAT MAP' ON FIG. 32

Option for Addressing Risk Contributor	Risk Benefit and Other Considerations	Relative Cost of Implementation
No action	No reduction in risk	No cost
Revise procedures and training to prepare operators better to perform local manual actions to align suction supply	Small to moderate reduction in risk associated with this scenario. Increased burden on operating staff.	Low cost.
Revise procedures and training and add alarm independent of fire impacts to provide compelling indication of need to transfer suction	Moderate reduction in risk associated with this scenario. Increased burden on operating staff.	Low to moderate cost to install new alarm.
Reroute cables to provide separation that preserves redundancy under fire conditions	Moderate to large reduction in risk for this scenario. Better conformance with design philosophy for the plant.	Moderate cost to reroute cables.
Install new supply line independent of existing lines.	Essentially eliminates risk associated with this scenario.	High cost to install new supply line.

A comparison to the baseline may be presented in a simple format, such as that shown in Fig. 33. This figure illustrates that the increase in CCDP is not negligible, but that there remains a substantial margin afforded by other systems (including using high pressure coolant injection or depressurizing the reactor to permit use of any of several sources of low pressure injection) to prevent core damage. It might also be important to point out the average frequency of this initiating event to provide further context.

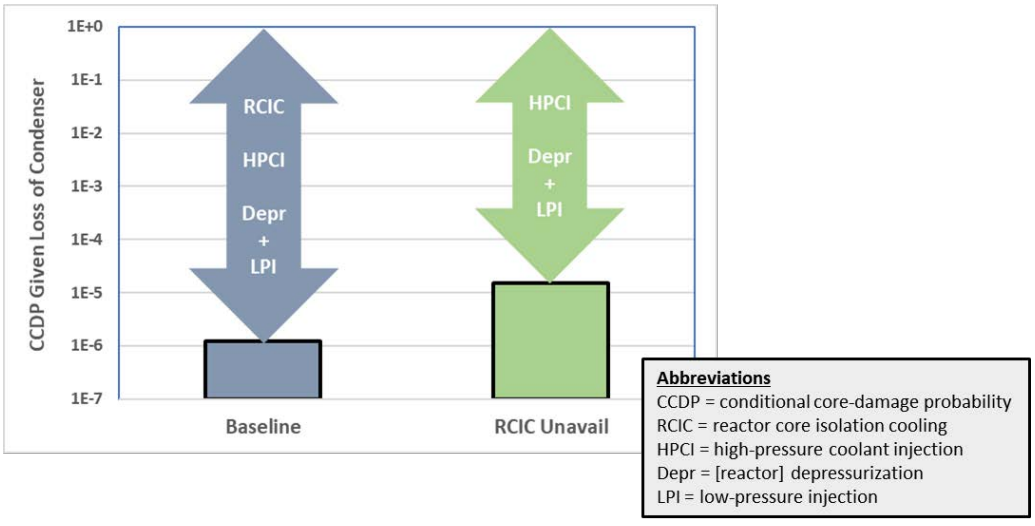


FIG. 33. Comparison of conditional probabilities of core damage given reactor trip with main steam isolation.

Another example might be one in which it is discovered that a piece of standby equipment was in a state for an extended period during which it would have been unable to perform its function if it had been needed. Relating back to the previous example, suppose that it was discovered

that the wrong lubricant had been used for the RCIC pump bearings during maintenance that took place nine months before the discovery. The lubricant might have been adequate to allow the RCIC pump to pass short periodic tests, but the pump would almost certainly have experienced failure if it had needed to run longer than the duration of the tests, as would have been the case in an actual demand. In this case, it may be both the absolute value of the elevated risk compared to the baseline risk that may be of interest (as shown in Fig. 34), as well as the CCDP over the duration of the undesired state of the pump. it may be important to communicate the risk during the period the condition persists relative to the baseline risk.

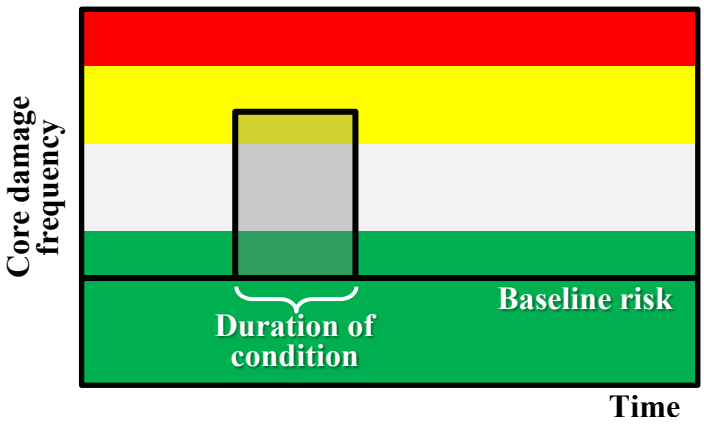


FIG. 34. Example of risk context for condition at plant.

To summarize, in any of these examples, it is important to present the information in a manner that can be readily understood by plant decision makers who may not be very familiar with PSA concepts. Quantitative information derived from aggregated risk estimates needs to be complemented by qualitative summaries of important risk contributors and other relevant considerations.

IV.2 EXAMPLES OF RISK COMMINICATION WITH THE STAFF OF NUCLEAR INSTALLATION

As noted in Section 5.2, there are a number of reasons that risk information might be routinely communicated to the staff. Many plants display high level information derived from aggregate risk estimates. These displays may, for example, be present at the security portals, so that they reach all employees as they report to work. Similar displays may be found at other strategic locations on the site. They may take a variety of forms, including video displays or other types of sign boards. An example is shown in Fig. 35.

FIG. 35. Example for communicating basic plant risk configuration.

In this example, there is no indication of quantitative risk measures (which would not be useful to most staff members), but rather a very brief summary of practical information that may be of value across multiple disciplines (including operations, maintenance, and performance testing). Many plants also use a more extensive display to communicate important results and insights from the risk assessment to a broad spectrum of plant staff. The example of communication of important operator actions is provided in Table 6.

TABLE 6. EXAMPLE COMMUNICATION OF IMPORTANT OPERATOR ACTIONS

Risk Significant Operator Action	Reason for Significance
Shed loads on emergency batteries	Total loss of offsite and on site AC power (station blackout) is an important risk scenario. Timely shedding of DC loads can significantly extend battery life, affording more time to restore AC power.
Make up to the condensate storage tank to provide a sustained suction supply for the auxiliary feedwater pumps	If main feedwater cannot be restored, it may be necessary to continue to use auxiliary feedwater for an extended period of time. Makeup to the condensate storage tank may be needed to support this extended period of operation.
Align auxiliary feedwater to backup suction supply	Under some circumstances involving extended use of auxiliary feedwater (including, for example, following a loss of instrument air), it may not be feasible to make up to the condensate storage tank. Being prepared to switch to the backup supply is very important under those conditions.
Restore feedwater flow following loss of main feedwater	Manual starting of auxiliary feedwater may be necessary if auto start fails.
Depressurize steam generators and provide flow from condensate pumps	Following a loss of main feedwater, it can be important to use the condensate pumps as a source of supply to the steam generators. This may require that the steam generators be depressurized below the shutoff head of the condensate pumps.
Trip reactor coolant pumps following loss of seal cooling	In the event of a loss of seal cooling (both seal injection and cooling of thermal barriers), it is important to trip the reactor coolant pumps to avoid severe damage to the pump seals and consequential high rates of leakage from the reactor coolant system. This is particularly important for situations in which the loss of seal cooling is the result of loss of component cooling water, since the high head safety injection pumps needed to respond to the loss of reactor coolant would be unavailable due to lack of bearing cooling.
Isolate recirculation lines for high head safety injection following switchover to sump recirculation	For small LOCAs that involve difficulty in cooling down and depressurizing the reactor coolant system, it may be necessary to switch suction for high head safety injection to the containment emergency sump. When that happens, it is particularly important to isolate pump recirculation lines to prevent diverting some sump water back to the refueling water storage tank and to maximize flow to the reactor coolant system.

IV.3 EXAMPLES OF RISK COMMINICATION WITH REGULATORY AUTHORITIES

In the case of communicating with regulatory authorities, it is reasonable to expect that the agency will have staff familiar enough with risk concepts to understand technical details, and that these staff members will have the responsibility to relate relevant results and conclusions

to decision makers within their agency. Thus, for example, a plot of aggregated risk and the contributing hazards such as that shown in Figures 31 and 33 can be useful.

Another set of examples is shown in Fig. 36. These three example cases illustrate three different types of risk outcomes relative to the regulatory threshold or limit that might be in place. In these examples, the threshold is depicted by a broad, shaded line, rather than a distinct point. This is consistent with concepts such as those from US NRC regulatory guide 1.174, as discussed in Section 4.

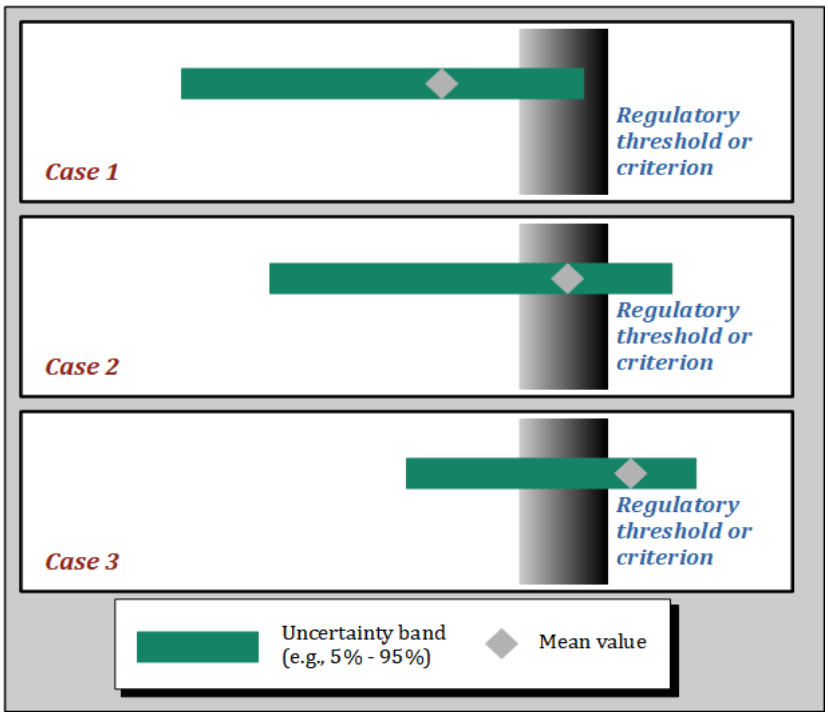


FIG. 36. Examples illustrating risk relative to regulatory criteria.

The intent of these examples is to show that communications regarding whether or not aggregated risks satisfy regulatory thresholds is often not a simple matter. The discussion will need to include not only how the relevant point estimate (in most cases, the mean risk) compares to the threshold, but also the implications of uncertainties. The plant operator will need to be able to explain the impact of uncertainties in a qualitative sense, which may include an assessment of the degree of belief in the PSA models themselves. A complement to the depictions in Fig. 36 is provided in Fig. 37.

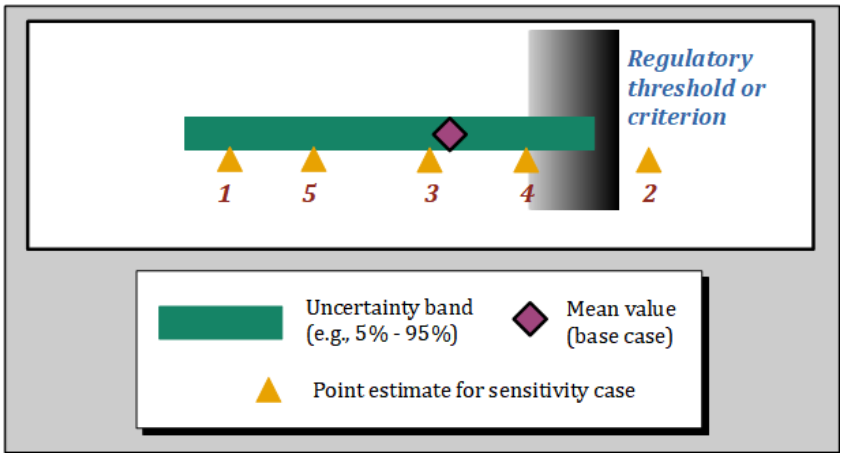


FIG. 37. Examples illustrating results of sensitivity studies relative to regulatory criteria.

In this case, the focus is on communicating the implications of various sensitivity cases that may be relevant to the decision at hand.In all of these cases, the graphic summaries will clearly require substantial written explanations to provide an adequate understanding.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010). (a revision of this publication is in preparation)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-4, IAEA, Vienna (2010). (a revision of this publication is in preparation)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA-TECDOC-1804, IAEA, Vienna (2016).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (), 2018 Edition, IAEA, Vienna, (2019).

[6] KAPLAN, S., B.J. GARRICK, On the quantitative definition of risk, Risk Analysis, **1**, 11–37 (1981).

[7] NATIONAL RESEARCH COUNCIL, Understanding Risk: Informing Decisions in a Democratic Society, Paul C. Stern and Harvey V. Fineberg, Editors; Committee on Risk Characterization, Washington, DC (1996).

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

[9] Working Material: Output of the IAEA Technical Meeting on Level 3 Probabilistic Safety Assessment, IAEA Headquarters, Vienna (July 2-6, 2012).

[10] FARMER, F.R., Reactor safety and siting: a proposed risk criterion, Nuclear Safety, **8**, 539-548 (1967).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on Performing Integrated Risk Informed Decision Making, IAEA-TECDOC-1909, IAEA, Vienna (2020).

[12] US NUCLEAR REGULATORY COMMISSION, Guidance on the Treatment of Uncertainties Associated with PRAs in Risk informed Decision-making, NUREG-1855, Rev. 1, Washington, DC (2017).

[13] CONSOLIDATED EDISON CO. AND NEW YORK STATE POWER AUTHORITY, Indian Point Probabilistic Safety Study, New York (1980).

[14] SIU, N., COYNE, K., NAKOSKI, J., HUNTER, C., "Accidents, near misses, and probabilistic analysis: on the use of CCDPs in enterprise risk management," in Proceedings of ANS International Topical Meeting on Probabilistic Safety Assessment (PSA 2017), Pittsburgh, PA, September 24-28, (2017).

[15] SIU, N., COYNE, K., MELLY, N., Fire PRA Maturity and Realism: A Technical Evaluation, US Nuclear Regulatory Commission, Washington, DC (2017).

[16] SIU, N., KELLY, D.L., "On the use of importance measures for prioritizing systems, structures, and components," Proceedings of 5th International Topical Meeting on

Nuclear Thermal Hydraulics, Operations, and Safety (NUTHOS-5), Beijing, China, April 14-18, (1997), pp. L.4-1 - L.4-6.

[17] ELECTRIC POWER RESEARCH INSTITUTE, An Approach to Risk Aggregation for Risk informed Decision-making, EPRI 3002003116, Palo Alto, CA (2015).

[18] U.S. NUCLEAR REGULATORY COMMISSION, Probabilistic Risk Assessment and Regulatory Decision-making: Some Frequently Asked Questions, NUREG-2201, Washington, DC (2017).

[19] NUCLEAR ENERGY INSTITUTE, Guidance for Addressing Digital Common Cause Failure, NEI 16-16, Draft 1, Washington, DC (2016).

[20] ELECTRIC POWER RESEARCH INSTITUTE, Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems, EPRI 3002005326, Palo Alto, CA (2016).

[21] KELLER, K., MODARRES, M., A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen, Reliability Engineering and System Safety 89 (2005).

[22] US NUCLEAR REGULATORY COMMISSION, Reactor Safety Study, WASH-1400, NUREG-75/014, Washington, DC (1975).

[23] US NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, Washington, DC (1986).

[24] US NUCLEAR REGULATORY COMMISSION, Full Scope Site Level 3 PRA Project Communication Plan, Washington, DC (2016).

[25] US NUCLEAR REGULATORY COMMISSION, Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, Generic Letter 88-20, Supplement 4, Washington, DC (1991).

[26] US NUCLEAR REGULATORY COMMISSION, Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1, NUREG/CR-6144, Washington, DC (1995).

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic safety assessments of nuclear power plants for low power and shutdown modes, IAEA-TECDOC-1144, IAEA, Vienna (2000).

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, The Fukushima Daiichi Accident, Report by the IAEA Director General, IAEA, Vienna (2015).

[29] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for an Integrated Risk Informed Decision Making Process, INSAG-25, IAEA, Vienna (2011).

[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units, Safety Reports Series No. 96, IAEA, Vienna (2019).

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Multi-unit Probabilistic Safety Assessment, Safety Reports Series No. 110, IAEA, Vienna (in publication).

[32] WIELENBERG, A., LÖFFLER, H. et al., Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA, ASAMPSA_E, Technical report ASAMPSA_E/WP30/D30.7/2017-31 volume 2, (2017).

[33] WIELENBERG, A., HASNAOUI, C. et al., Risk Metrics and Measures for an Extended PSA, ASAMPSA_E: Advanced Safety Assessment Methodologies: extended PSA. Technical report ASAMPSA_E/ WP 30 / D30.7 / 2017-31 volume 3 (2017).

[34] STUTZKE M., “Scoping Estimates of Multiunit Accident Risk”, in Probabilistic Safety Assessment and Management PSAM 12, Honolulu, Hawaii, (June 2014).

[35] INTERNATIONAL ATOMIC ENERGY AGENCY, INES - The International Nuclear and Radiological Event Scale User's Manual, 2008 Edition, IAEA, Vienna (2013).

[36] US NUCLEAR REGULATORY COMMISSION, Technical Analysis Approach Plan for Level 3 PRA Project (Rev 0a, Working Draft), (2013) https://www.nrc.gov/docs/ML1311/ML13112A444.pdf

[37] BAREITH, A. at al., "A Pilot Study on Developing a Site Risk Model", in 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), www.psam13.org, Seoul, Republic of Korea, 2-7 October, (2016).

[38] LI, J.Y., MILLER, G., HENNEKE, D., Safety Demonstration of GEH Advanced Nuclear Power Plant Designs: A summary of Risk Results and Benefits of Risk informed Regulatory Initiatives, International Conference on Topical Issues in Nuclear Installation Safety, IAEA, Vienna, 6–9 June (2017).

[39] US NUCLEAR REGULATORY COMMISSION, An Approach for Using Probabilistic Risk Assessment in Risk informed Decisions on Plant specific Changes to the Licensing Basis, Regulatory Guide 1.174, Revision 2, Washington, DC (2011).

[40] Lankin, M. "Preparation of Risk-Informed Decision for NPP: Evaluation of Risk Acceptability and the Level of Decision Influence on Defence-in-Depth." Proceedings of the 2012 20th International Conference on Nuclear Engineering and the ASME 2012 Power Conference. Vol. 4., pp. 215-220, Anaheim, California, USA. July 30–August 3, 2012 (2012)

[41] OFFICE FOR NUCLEAR REGULATION, Safety Assessment Principles for Nuclear Facilities, Revision 0, UK, (2014).

[42] AUTORIDAD REGULATORIA NUCLEAR, Criterios radiológicos relativos a accidentes en reactores nucleares de potencia (AR 3.1.3), Argentina (2002).

[43] US NUCLEAR REGULATORY COMMISSION, Feasibility Study for a Risk Informed and Performance based Regulatory Structure for Future Plant Licensing, NUREG-1860, Washington, DC (2007).

[44] ELECTRIC POWER RESEARCH INSTITUTE, Aggregation of Quantitative Risk Assessment Results – Comparing and Manipulating Risk Metrics, EPRI 1010068, Palo Alto, CA (2005).

[45] INTERNATIONAL ATOMIC ENERGY AGENCY, Hierarchical Structure of Safety Goals for Nuclear Installations, IAEA-TECDOC-1874, IAEA, Vienna (2019).

[46] ELECTRIC POWER RESEARCH INSTITUTE, Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments, EPRI 1016737, Palo Alto, CA (2008).

[47] ELECTRIC POWER RESEARCH INSTITUTE, Practical Guidance on the Use of PRA in Risk informed Applications with a Focus on the Treatment of Uncertainty, EPRI 1026511, Palo Alto, CA (2012).

[48] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Reports Series No 46, Assessment of Defence in Depth for Nuclear Power Plants, IAEA, Vienna (2005).

[49] US NUCLEAR REGULATORY COMMISSION, Review and Evaluation of the Indian Point Probabilistic Safety Study, NUREG/CR-2934, Washington, DC (1982).

[50] LLOYD, M., et al., "Simple method to account for the state of knowledge correlation", in Probabilistic Safety Assessment Conference (PSA 2017), Pittsburgh, PA, September 24-28 (2017).

[51] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT NUCLEAR ENERGY AGENCY, Towards a Shared Understanding of Radiological Risks, NEA No. 7554, OECD Publications, Paris, France (2021).

ANNEXES: COLLECTION OF MEMBER STATES EXPERIENCES

The following annexes provide a collection of certain Member States' experiences in the area of risk aggregation, use of aggregated risk in decision making and risk communication. The summary of experiences presented in the annexes have been prepared from the original material as submitted by the contributors and have not been modified or edited by the staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily reflect the views of the IAEA or its Member States.

ANNEX I. PILOT OF THE EPRI RISK AGGREGATION FRAMEWORK FOR RISK INFORMED DECISION MAKING

Section 4 of this publication discusses the relationship between risk aggregation and RIDM and describes a framework for risk aggregation developed by EPRI [I–1]. The Pressurized Water Reactor Owners Group (PWROG) leveraged two plant PSAs to pilot the EPRI framework [I-2], which is summarized in this annex. Ongoing risk informed applications in place at the pilot plants were used to test the effect of using aggregated risk information from multiple hazards to guide the decision making associated with pursuing plant changes or measuring risk with the main objective of evaluating whether aggregated risk information would have yielded different insights (and therefore led to different decisions).

The two pilot plants have different backgrounds and boundary conditions with respect to PSA model heterogeneity, namely difference in which hazards are explicitly modelled, use of qualitatively addressed and/or screened approaches, status and vintage of the underlying PSA model(s) and associated peer reviews. The two pilot plants also have a different suite of available risk informed applications that represent a good spectrum of the operating fleet of NPPs operating in US.

It has been observed that while adding explicit modelling of hazard specific risk reduces the completeness uncertainty associated with the plant PSA, it also increases the cumulative estimated risk, raising it closer to the regulatory thresholds associated with risk informed applications in the United States of America regulatory framework [I–3]. An additional objective of this pilot application was to be able to better characterize the plant risk profile as the main risk metrics (i.e. CDF, LERF) approach or even slightly exceed the regulatory thresholds of 1E-4/yr and 1E-05/yr for total plant CDF and LERF respectively. Note that existing guidance clearly states that exceeding such thresholds does not prevent risk informed applications but increases the burden of the plant for defending the appropriateness of the requested licence change.

The EPRI framework can be summarized in five major tasks (see Section 4, Fig. 18), which were exercised for six distinct applications at the two pilot plants. Such applications included:

— Risk informed oversight activities (i.e. addressing the risk significance of an inspection finding);
— Risk informed Completion Time (RICT);
— Risk informed management of maintenance risk;
— Evaluation of Critical Human Action (CHA) using a risk informed approach.

Task 1: Define role of PSA

The initial work related to Task 1 of [I–1] is the identification of the applications to be used for the pilot activity, which will be developed further in Tasks 2 through 5. For each of the applications selected for this pilot activity, the role of PSA is already clearly understood in the United States of America industry.

PILOT PLANT 1

Task 2: Characterize important contributors to risk

Task 2 evaluated the baseline PSA and characterized important risk contributors for the individual PSA models. This task focused on understanding the dominant contributors of the risk metrics used in the applications being considered, i.e. CDF and LERF (see Table I–1). This task began with the existing PSA models and results. For Pilot 1, note that tornado and external flood were screened from the need for explicit PSA analysis. The seismic PSA values shown were developed in support of US NRC Generic Issue (GI) 199 and therefore represent a simplified estimate of seismic CDF; no explicit seismic LERF evaluation exists in the GI-199 evaluation, so seismic LERF was conservatively assumed to equal CDF.

TABLE I–1. CDF/LERF RESULTS BY HAZARD GROUP

Hazard Group	Mean CDF (/yr)	% Contribution	Mean LERF (/yr)	% Contribution
Internal Fire	5.47E-05	67%	5.85E-06	41%
Internal Events	1.78E-05	22%	9.52E-07	7%
Seismic	7.30E-06	9%	7.30E-06	52%
Internal Flood	1.50E-06	2%	4.77E-08	0%
Tornado	Screened	N/A	Screened	N/A
External Flood	Screened	N/A	Screened	N/A
	8.13E-05	**Total**	**1.41E-05**	

** Mean values are assumed to be equal to point estimates for internal fire and seismic PSA while for internal events (including flooding) are determined by propagating parameter uncertainties.*

Note how total CDF is driven by the fire PSA results and how the simplified and conservative seismic estimates are in turn driving the total LERF. Key contributors to risk and uncertainty associated with each model were identified by examining importance measures, reviewing the plant's existing uncertainty analysis, and evaluating open facts and observations from the most recent PSA peer reviews.

For the full power internal events (FPIE) model, the list of potential key uncertainties includes:

a. Common cause failure (CCF), especially in support system initiating events;
b. Interfacing system LOCA IE frequencies;
c. Credit for auxiliary feedwater (AFW) cross tie;
d. Initial plant configuration assumed in the baseline PSA;
e. Induced steam generator tube rupture (SGTR) probabilities;
f. Assumed residual heat removal pumps failure for containment isolation pathway;
g. SGTR events without AFW conservatively assumed LERF after core damage;
h. Time to trip the reactor coolant pumps (RCPs) on loss of seal injection and thermal barrier cooling to protect the shutdown seals (SDSs);
i. Human error probabilities (HEPs).

For the internal flood model, additional key uncertainties include:

a. Internal flood IE frequencies based on generic data;
b. HEPs for manual containment isolation actions.

For the internal fire model, the list of potentially key uncertainties includes:

a. Undeveloped fire base scenarios;
b. Cable routing state of knowledge.

For the seismic portion of the analysis, since the values are based on simplified quantitative estimates only, the analysis is considered generally conservative due to its use of outdated hazard information and generic component fragilities. No additional specific model uncertainties were identified.

The investigation of top contributors and associated uncertainties for each hazard model allowed the characterization of each model in terms of model realism and uncertainty, consistently with the rubric concept presented by EPRI.

Task 3-5 for Plant 1, Example Application: SDP

Application 1 for pilot plant 1 was an analysis for an example calculation supporting the assessment of the risk significance of an inspection finding under a risk informed oversight process (e.g. the significance determination process, SDP, used by the US NRC). The example evaluation addressed the evaluation of the risk significance of the failure of an Emergency Core Cooling System (ECCS) sump recirculation motor operated valve (MOV). During a surveillance, the MOV failed to fully open due to corrosion of the actuator torque switch. While the MOV may have been able to provide sufficient flow in a partially open state, the dual position indication that occurred with the partial failure would have caused the operators to put the corresponding RH pump in 'pull to lock', thus disabling that train of ECCS until the MOV could be locally opened.

The role of the PSA in the SDP calculation is to generate the incremental core damage probability (ICDP) and the incremental large early release probability (ILERP) for the specific issue under consideration, which produced the results shown in Table I–2.

TABLE I–2. SDP RESULTS BY HAZARD GROUP

Metric	ICDP	ILERP
Internal Events	2.02E-06	1.58E-08
Internal Flood	1.27E-08	2.25E-10
Internal Fire	5.79E-05	1.88E-06
Seismic	1.90E-09	Not calculated
Total	**5.99E-05**	**1.90E-06**

Values for the FPIE, flood, and fire hazard groups were calculated directly using the PSA model. The seismic ICDP is provided from work done on a similar analysis, and no ILERP was provided given the very low ICDP associated with the seismic hazard. The basic sum of the hazards puts the evaluation into the Yellow category, driven mostly by the fire PSA ICDP result.

Each of the potential key uncertainties identified above for the base case was then specifically examined for any impact it may have on this specific application. Based on that evaluation, the following potential sources of uncertainty are considered for potential impact on the application

and are discussed with any conservatisms and potential sensitivities that are considered. Some examples are provided here below:

— A new operator action was added to model the MOV recovery, the associated HEP for the recovery action showed a Fussell-Vesely importance measure value (FV) of 0.03 while set at 0.1 in the fire PSA, so it does not appear to be driving the results. However, if conservativisms in the fire PSA (i.e. unmapped cables that are assumed to be failed) are improved, the HEP could become more important. This was categorized as a conservative model assumption.
— The cross tie related to AFW was not credited in the fire PSA. Though it could have a significant effect based on the important sequences, it would not have been creditable in this SDP because of the assumption of loss of main feedwater and less time available to implement the action due to inadequate procedures to allow it to be credited. This was categorized as an irreducible uncertainty because AFW cross tie use was at the time prevented by a regulatory action.
— The SDP analysis conservatively assumes that the components from the other train are susceptible to the same common cause mechanisms. There could be some benefit in relaxing this assumption of CCF between the two trains if the failure mechanism can be shown to not directly impact the other train. Nevertheless, the modelled CCF's FV is only 0.019, so the benefit would be minor. This is categorized as a conservative method;
— A key HEP for the base case is the tripping of the RCPs after loss of seal cooling. This HEP showed a significantly reduced FV, so it does not appear to be a major contributor and is not significantly contributing to the SDP result;
— Spurious operation probabilities appear in some key cutsets, but it is not clear whether these can be justifiably altered because they follow current industry guidance. This is categorized as an irreducible uncertainty;
— Small LOCAs could possibly be mitigated by going to shutdown cooling rather than ECCS recirculation, which is not currently credited. A significant amount of investigation would be needed to determine the necessary operator actions and the availability of the actions during key fire scenarios to apply this to the key cutsets. This is categorized as a simplified method;
— The only other remaining option would be significant investigation and refinement of the fire mapping and modelling work. Given the significant effect of the fires on the newly dominant sequences, this has promise, but the level of effort to enable quantitative changes is beyond the scope of this pilot study. This is categorized as a simplified method.

The final major process decision asks whether or not it is possible to refine the models. This question has a mixed answer. The fire PSA model can be refined in several areas that could impact important scenarios. However, those areas that are more straightforward to refine appear to be unlikely to reduce the calculated results enough to change the decision. A few larger refinements (e.g. fire mapping and modelling) that may have greater potential to affect the decision would require significant resources.

The conclusion is that the computed total ICDP is above 1E-5/year (Yellow) and may be able to be reduced only with significant application of resources. However, there was no indication that risk aggregation has changed or skewed the insights for RIDM purposes.

PILOT PLANT 2

Task 2: Characterize important contributors to risk

In the base case PSA, the hazard groups contribute to CDF for Plant 2 as shown in Table I–3.

TABLE I–3. CDF RESULTS BY HAZARD GROUP

Hazard Group	Mean CDF[1] (/year)	% Contribution
Internal Fire	3.55E-05	36%
Internal Events	2.19E-05	22%
Seismic	2.15E-05	22%
Internal Flood	1.40E-05	14%
Tornado	4.34E-06	4%
External Flood	8/78E-06	1%
Total	**9.81E-05**	

[1] Mean values are assumed to be equal to point estimates.

The important contributors to risk for the applicable hazard groups include:

Internal Fire:
— Fires in the Auxiliary and Turbine Buildings contribute most to CDF risk;
— The dominant fire sequences involve loss of an essential bus;
— Failures to restore secondary side heat removal represent the dominant operator actions;

Internal Events:

— LOCAs contribute the most to CDF. Transients make up the next highest contributing initiator class, followed by SGTRs;
— The failure of the operators to initiate the high pressure recirculation mode of core cooling following a small or medium LOCA is the dominant human error event;

Internal Flood:

— The top risk significant internal flood initiators for CDF involve pipe or tank breaks in the condensate, feedwater or drinking water systems;
— Failures to maintain adequate borated water storage tank level during a flood and to restore secondary side cooling are dominant operator action failures.

Plant 2, Example Application: critical human actions

One of the tested applications for pilot plant 2 is the identification and characterization of the risk significant operator actions, also referred to as CHAs. Since no plant change is involved, the base case PSA models are used to identify the CHAs for the modelled hazard groups. The PSA is used to provide the identification and characterization of CHAs. This information, along with deterministic considerations such as defence in depth and safety margin, may be used as inputs to decision makers.

Risk achievement worth is selected as the importance measure of interest, which identified the CHAs that can result in the largest risk increases if they fail to be performed. A composite RAW importance value greater than 2.0 is typically used to identify CHAs. The composite RAW

values are obtained using a weighted average based on the percent contribution of each hazard group to the overall CDF from Table I–3.

The same process discussed for pilot plant 1 was used to review important assumptions and associated uncertainty and judge the realism and uncertainty associated to each hazard model for the specific application. The final result of the assessment is the Rubric shown in Table I-4, which also shows the operator actions with a composite RAW greater than 2.0. Note that the characterization of CHAs changes when the RAW criterion of RAW>2.0 is used in the aggregated perspective because of the dominance of fire PSA result lower the importance of operator actions that may be risk significant for other hazards.

The pilot plant recognized this possible masking of insights. Recognizing that hazard group contributions to overall CDF are not known with absolute precision, a hazard group RAW value of 4.0 is also used to identify candidate CHAs. For a hazard group whose 'true' contribution to overall CDF is 50%, a basic event with a hazard group RAW of 4.0 would have a composite RAW of 2.0. One specific operator action was characterized as CHA based on application of this second criterion.

TABLE I–4. EXAMPLE OF MODIFIED RUBRIC

Purpose

Characterize the critical human actions (CHAs) included in the base case PSA models. The identified CHAs are used by the plant to prioritize training for operators and for improved understanding of human action risk contributors.

Risk Information

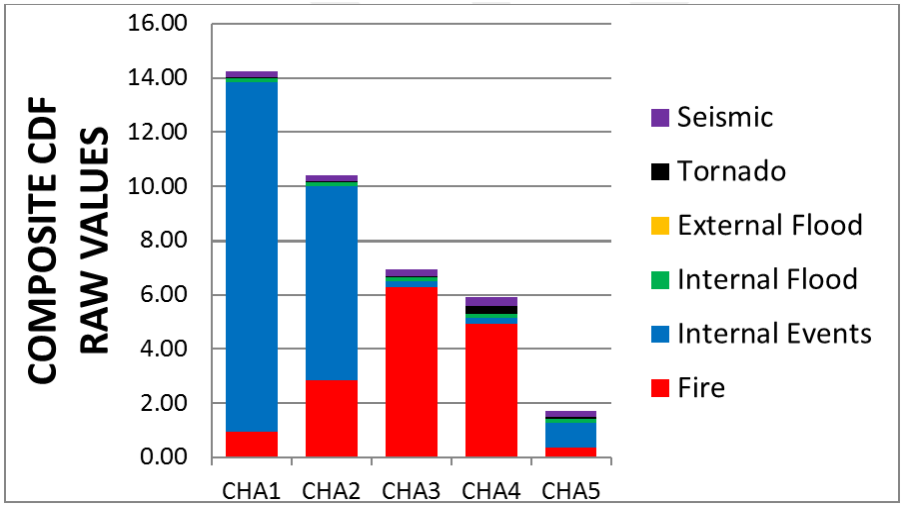
CHA	Description	Core damage frequency (CDF) Risk achievement worth (RAW) by hazard group						Composite RAW
		Fire	Internal Events	Internal Flood	External Flood	Tornado	Seismic	
1	Operators fail to initiate high pressure recirculation	2.6	57.7	1.0	1.0	1.0	1.0	14.2
2	Operators fail to throttle high pressure injection flow following initiating event	4.8	31.9	1.0	1.0	1.0	1.0	10.4
3	Operators fail to trip the RCPs in time to prevent RCP seal failure	17.3	1.0	1.0	1.0	1.0	1.1	6.9
4	Operators fail to deploy to the standby shutdown facility	13.6	1.0	1.0	1.0	6.6	1.5	5.9
5	Operator fails to refill BWST following a SGTR	1.0	4.11	1.0	1.0	1.0	1.0	1.7

Parametric uncertainty

- The mean frequency associated with each hazard group is used to determine its contribution to CDF.

Modelling uncertainty

- Conservative methods are used in portions of the fire analysis when such approaches are judged to have minimal impacts on the base case results. For example, detailed circuit failure analysis was only performed on those scenarios that otherwise would have been high risk contributors. Similarly, components whose cable routing or other information are not readily available are assumed to be failed in all fire areas.
- For CHAs 3 and 4, fire sequences are especially risk



significant. Further refinement of the fire analysis associated with these sequences may be desired.
- Based on more recent information, the seismic hazard curve is significantly more challenging than is currently modelled. However, more detailed fragility analysis may offset the risk increase associated with an update to the hazard curve.

Completeness uncertainty
- All relevant site hazards for full power operation are considered.

Risk Information – Model Realism and Uncertainty

Hazard Group	Modelling	Uncertainty
Seismic	REALISTIC	HIGH
Tornado	CONSERVATIVE	MODERATE
External Flood	REALISTIC	MODERATE
Internal Flood	CONSERVATIVE	MODERATE
Internal Events	REALISTIC	LOW
Fire	CONSERVATIVE	MODERATE

Defence in depth Characterization

For this application, there is no change in plant design or operation. Thus, there are no defence in depth implications.

Safety Margin Characterization

For this application, there is no change in plant design or operation. Thus, there are no plant design safety margin implications.

Performance Monitoring

Performance monitoring is not performed for an importance measure evaluation. Thus, this element is not applicable for this application.

Integrated Decision making Inputs

Risk	Defence in depth	Safety Margins	Performance Monitoring
Composite RAW > 2.0 for four CHAs *Hazard Group RAW > 4.0 for one additional CHA*	*No impacts* PSA	*No impacts* PSA	*Not applicable* PSA

Conclusions:

Five human actions are risk significant for the integrated plant model:

Conclusions

Both pilot plants identified cases where the insights are different depending on whether the risk information is considered on a single hazard basis or as an aggregate.

The process of characterizing the uncertainties associated with individual risk hazard led to a more evident explanation of how, at least in one case, an overly conservative approach to LERF estimate (for an external hazard) could lead to an overly restrictive decision. This reinforced the conclusion that the risk from the different hazards needs to be contextualized and characterized based on the identified uncertainties. An appropriate characterization of the uncertainties associated with the different hazard specific risks that are aggregated together ensures that decision making can consider when regulatory thresholds are crossed on the basis of simplified and conservative approaches, but also when the aggregated risk, while still under the regulatory threshold, becomes close to crossing them, granting therefore additional scrutiny and evaluation.

Note that both pilot plants refined the rubric associated with the base case and the applications in a way that more explicitly shows the quantitative uncertainty associated with the risk measures. One of the challenges identified by the pilot plants was that multiple models of records are used for different hazards and sometimes even between the base case results and the documented uncertainty evaluations; this results in challenges associated with producing an up to date uncertainty evaluation. Most notably, there was a perceived confusion on the characterization of the PSA and its way of measuring other aspects of the risk informed framework. In the version of the rubric presented by the pilot plants, a clearer differentiation was made between whether a specific application is indeed impacting one of the pillars of the risk informed approach (e.g. defence in depth) and how the PSA can (or cannot) measure such impact. The rubrics have therefore been modified to provide a visual representation (i.e. a box within a box, as seen in Table I–4) of the resolution of a PSA, so that the decision maker can ascertain the degree to rely on the quantitative information provided by the PSA itself.

In general, one of the main conclusions of this work is that a robust and well thought uncertainty analysis is key to appropriately characterize the contribution of multiple hazards. Uncertainty characterization also has to be consistent among the hazards and in the context of the specific application, otherwise it may not really uncover critical aspects in the uncertain understanding of the risk information that is being used for decision making purposes.

REFERENCES

[I–1] ELECTRIC POWER RESEARCH INSTITUTE, An Approach to Risk Aggregation for Risk informed Decision making, EPRI 3002003116, Palo Alto, CA (2015).

[I–2] BOYER R., THORNSBURY E., LEVINSON, S., MAIOLI A., “Multi-Hazard Risk Aggregation in Support of Risk informed Decision Making”, in Proceedings of ANS International Topical Meeting on Probabilistic Safety Assessment (PSA 2017), Pittsburgh, PA, September 24–28, (2017).

[I-3] US NUCLEAR REGULATORY COMMISSION, An Approach for Using Probabilistic Risk Assessment in Risk informed Decisions on Plant specific Changes to the Licensing Basis, Regulatory Guide 1.174, Revision 2, Washington, DC (2011).

ANNEX II. APPROACHES FOR RISK AGGREGATION IN CANADA

II–1. INTRODUCTION

This annex describes the risk aggregation approaches used by the Canadian licensees for the characterization of the whole site risk which encompasses the contributions and impacts of the different internal and external hazards on the potential radioactive sources at the site considering their different plant operating states.

Risk aggregation refers to the process whereby risk metrics (i.e. SCDF, LRF) calculated using PSA for various hazards, plant states, and multiple units (in case of a site of multiple units), are combined together to generate a value for the site as a whole.

II–2. CNSC REGULATORY REQUIREMENTS ON PSA

The CNSC evaluates how well licensees meet regulatory requirements and CNSC expectations for the performance of programs in 14 safety and control areas (SCAs) that are grouped according to their functional areas: management; facility and equipment; core control processes.

The 'safety analysis' is one of the 14 defined SCAs, and this is defined as a systematic evaluation of the potential hazards associated with the conduct of a proposed activity or facility and considers the effectiveness of preventive measures and strategies in reducing the effects of such hazards.

The probabilistic safety assessment (PSA) is one specific area under the 'safety analysis' SCA. The PSA is used as a complement to the deterministic approaches in order to address plant safety concerns. The information derived from the PSA is used in conjunction with other safety aspects such as such as the defence in depth, the safety margins, and the regulatory requirements. The safety goals form part of the licensing basis to identify design improvements to enhance safety and to ensure that the likelihood of accidents with serious radiological consequences is extremely low. However, the safety goals are not the sole basis for regulatory decisions.

The specific regulatory requirements on PSA are included the CNSC regulatory document REGDOC-2.4.2, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants [II–1][30]. This regulatory document sets out the requirements of the CNSC with respect to the PSA, and reflects the lessons learned from the Fukushima nuclear event of March 2011. Regulatory document REGDOC 2.4.2 explicitly requires the consideration in the PSA of the following:

— Multiunit impacts (if applicable);
— Radioactive sources other than the reactors, such as the Irradiated Fuel bay (known as the spent fuel pool);
— At power and shutdown states, and other expected plant operating states;
— Potential combination of hazards.

[30] The full list of regulatory document series can be found on the CNSC's website (http://www.nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/index.cfm).

Furthermore, and as part of the Public Information and Disclosure, REGDOC 2.4.2 requires that a summary of the results and assumptions of PSA are to be made available to interested stakeholders.

REGDOC-2.4.2 requires the licensees to seek CNSC acceptance of the PSA methodology prior to the conduct of the PSA. This provides confidence that the PSA is developed following the accepted methodology and international state of practice. The regulatory review provides confidence that the accuracy of the technical content and the information derived from the PSA are adequate to support regulatory decisions.

II–3. TECHNICAL AND REGULATORY CONSIDERATIONS FOR RISK AGGREGATION

The development of a whole site PSA requires addressing the regulatory and technical challenges related the risk aggregation at the unit level (aggregation across all hazards, and POS) as well as the risk aggregation at the site level (across all radioactive sources at the site, with due consideration of inter source interactions). The various regulatory and technical considerations include:

II-3.1 Risk dilemma: 'Total risk' vs 'Single risk'

If risk is presented by 'single risks', then there is no adequate appreciation of the implications of this information on the total risk of the activity. On the other hand, if risk is given as a (total risk) piece of information, then the information on the details will be missing, and from a decision making standpoint, no tangible action can be taken unless additional information is available. Also considering the very specific CANDU multiple units design, the risk significance and the importance of shared systems are already captured in the per unit PSA. Therefore, the additional insights expected to be gained from the development of a whole site PSA may prove to be limited.

II-3.2 Lack of site based safety goals

The current safety goals defined in the licensees' licensing basis, and the safety goals as defined in the CNSC regulatory document REGDOC 2.5.2 'Design of reactor facilities: Nuclear Power Plants', are established on a per reactor per year basis, in accordance with the international practice, specifically the IAEA Safety Series No 75-INSAG-3 (1988), Basic Safety Principles for Nuclear Power Plants [II–2], which was updated in 1999 as INSAG-12 [II–3]. The per unit LRF safety goal (Frequency of a release higher than 1E+14 Bq of Cesium-137 to be less than 1E-5/year) was used by OPG as the basis for the comparison against the safety goals.

II-3.3 Lack of international experience and guidance on the development of whole site PSA

The general expectation from a whole site PSA is to calculate the integrated risk taking into account inter unit interactions and human interactions. The PSA practitioners are still facing technical challenges related to the development of a consensus approach and methodology. Therefore, it is internationally accepted that time is needed for building a state of practice before any regulatory requirements on whole site PSA can be made.

II-3.4 Lack of international experience and guidance on risk aggregation at the site level

In the current international practice, the PSAs are developed on a per unit and per hazard basis with differences in level of realism, level of detail in modelling, and uncertainty treatment. This

variety and heterogeneity in the per hazard PSA models are recognized as a challenge for risk aggregation and for the interpretation of the aggregated result. Regulatory Document REGDOC 2.5.2 'Design of Nuclear Facilities: NPPs' [II–4] provides some guidance on risk aggregation, but this is limited to risk aggregation at the unit level, given that the safety goals are established on per unit basis. The general guidance provided in REGDOC 2.5.2 includes the following:

— Calculations of the safety goals include all internal and external events;
— Aggregation of risk metrics through simple addition might not be appropriate;
— If the aggregated total exceed the safety goals, conclusions are not to be derived from the aggregated total until the scope of the conservative bias in the other hazards is investigated.

II-3.5 Differences in the PSAs' level of realism, level of detail in modelling, and uncertainty treatment

Regulatory document REGDOC 2.4.2 requires that the level of detail of the PSA needs to be consistent with the intended uses of the PSA. Regulatory document REGDOC 2.4.2 also allows the use of a graded approach, commensurate with risk, when applying the requirements and guidance contained in this regulatory document. As an example, for the assessment of the risks from radioactive sources outside the reactor core, as well as for the assessment of the risks from internal and external hazards, the licensees may (with the agreement of persons authorized by the Commission) choose an alternate analysis method (other than PSA) to conduct the assessment. Therefore, the PSAs developed as part of the licensees' compliance with REGDOC 2.4.2 may not be readily extendable to a Whole site PSA. Examples includes:

— Not all hazards are assessed through the PSA. Licensees have conducted a thorough and systematic screening process based on the impact, distance, and the frequency of the hazards to screen out those internal and external hazards that do not contribute to the total risk. The hazard identification and screening process generally follows that described in IAEA Specific Safety Guide SSG-3 [II–5] and in ASME/ANS RA-Sb-2013 [II–6].
— Full scope PSA is not conducted for all the assessed hazards:
    - Level 1 and Level 2 Outage PSA for internal fires, internal floods, high winds, and seismic PSA are not developed with the rationale that the accident progression is slower when the plant is in outage, giving more time for operator action; and the time at risk while the plant is in outage is small compared to the time the plant is at power.
    - Level 2 PSA is not fully developed for the Internal Events outage PSA under the rationale that the risk at this configuration is very low.
    - Limited Level 2 PSA is developed for the Seismic and High Wind PSA given that these are common mode events that affect all the units at the station. Level 2 containment failure probability is estimated based on the limiting fragility of the containment systems.
    - Some PSAs for external events are developed using alternative methods, as allowed by REGDOC 2.4.2. These PSA models cannot be directly integrated in the Whole site PSA model, and their results are not readily usable for risk aggregation. Examples include:
        - The use of scenario based PSA, such as in the case of fire and flood PSA;
        - The use of the PSA based SMA in lieu of the seismic PSA.
    - Uncertainty analysis is not performed for all hazards' PSAs. In these cases, the CDF and LRF mean values are not available for a meaningful risk aggregation, and uncertainty propagation.

II-3.6 Risk significance and importance measures of the integrated whole site PSA model

The identification of systems important to safety is derived in part through the use of PSA importance measures (Fussell-Vesely and risk achievement worth) as required by REGDOC 2.6.1 [II–7] 'Reliability Program for Nuclear Power Plants'. The technical challenge consists of which importance measure do we use during the process of systems identification (those derives through separate models, or those obtained from the integrated model). The other issue that can be encountered in the case of the development of an integrated PSA is the potential for masking the risk contributors.

II–4. RISK AGGREGATION APPROACH FOR THE PICKERING MULTIUNIT CANDU STATION

The characterization of the whole site risk for the Pickering Nuclear Generating Station was completed in December 2017, following to the request from the Commission, during the 2013 Pickering relicensing hearings. The Commission requested Ontario Power Generation (OPG) to provide a whole site PSA or a methodology for a whole site PSA, specific to the Pickering NGS site.

It is worth highlighting that although the current CANDU PSAs are conducted on a unit reactor basis, the effects and contributions from adjacent units at multiunit stations are fully accounted for in the calculated PSA results. As an example:

— Level 1 PSA includes the consideration of common mode events affecting all units concurrently (e.g. loss of off site power, loss of service water, seismic event), as well as the contributions from adjacent units (e.g. steam line breaks in adjacent units).
— Level 2 PSA identifies a specific plant damage state (PDS) for multiunit sequences.

OPG followed the CANDU Owners Group (COG**)** approach. The Pickering whole site risk characterization is performed through careful risk aggregation, where the per unit based PSA results are extrapolated to quantify site based risk metrics for a given hazard type. For the aggregation across the units at the Pickering station, the minimal cutsets for the reference unit are interrogated to identify single, two, and four unit sequences. This segregation of the minimal cutsets is an important step prior to the risk aggregation to avoid double (multiple) counting of accidents sequences in the aggregated result. For example:

— Cutsets containing initiating events that affect only the reference unit, e.g. a loss of reactor power control, are designated as single unit sequences;
— Cutsets containing initiating events that might affect more than one unit but contain unit specific mitigating system failures are designated as single unit sequences;
— Cutsets containing initiating events that might affect more than one unit and contain only failures of common mitigating system are designated as multiunit sequences;
— Cutsets initiated by a seismic event that contain only seismically induced failures of mitigating systems are designated as multiunit sequences.

For the aggregation across hazards, OPG approach used the simple summation.

Regarding the aggregation of LRF results, some simplified approaches are used to estimate the LRF for the cases where a full Level 2 was not performed (internal flood, Seismic, and high wind PSA). Large release frequency in this case was estimated conservatively using the results of the level 1 PSA as shown if Fig. II-1 below:

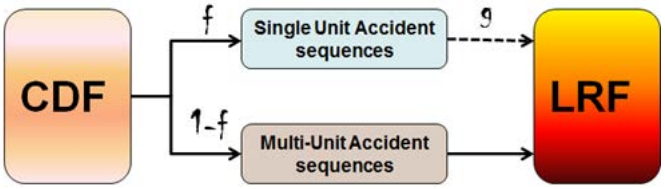


FIG. II–1. LRF estimation from the CDF.

Note: Fractions 'f' and 'g' are derived from site specific PSA

Figure II–2 below illustrates the risk aggregation approach adopted by OPG.

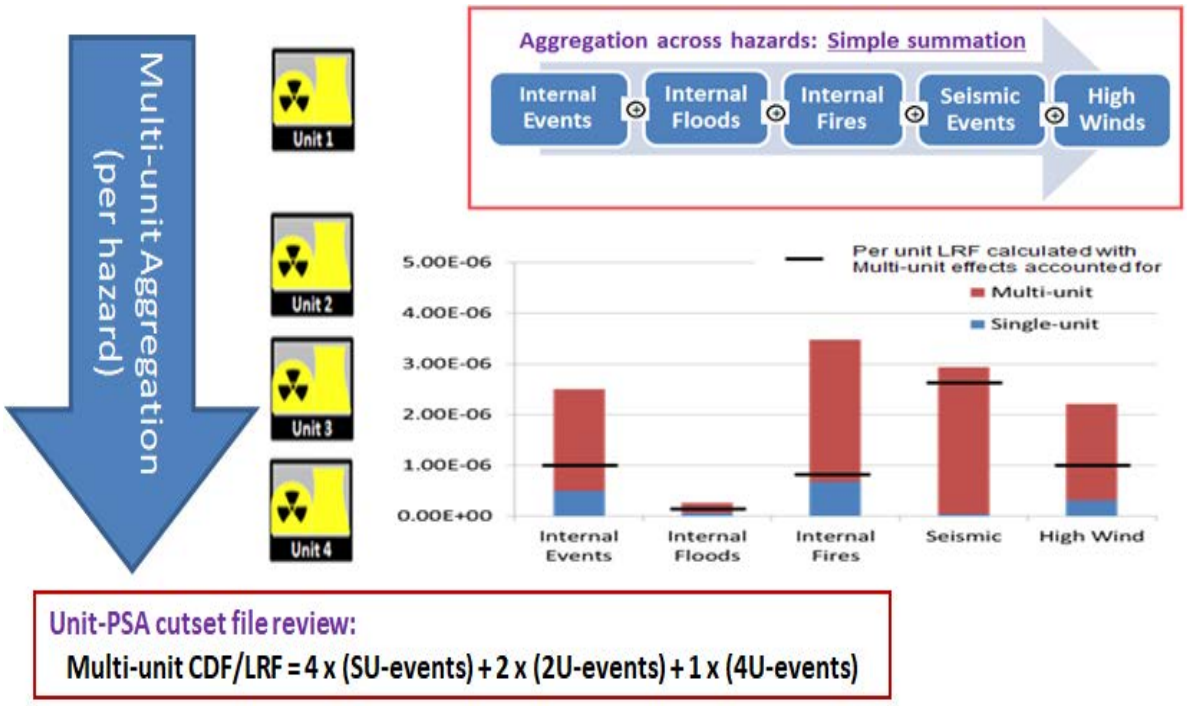


FIG. II–2. Risk aggregation approach.

Simple summation is also used to aggregate the results from Pickering A and Pickering B stations.

II-4.1 Consideration of other plant operating states

The current single unit PSAs are developed for at Power, and guaranteed shutdown (GSS) plant operating states (POS). The identification and selection of other POSs is performed based on time at risk following the COG guidelines, and the overall conclusion is that the risk associated with these identified other POSs is low, or these POSs can be covered by the 100% full power and GSS PSAs for Pickering NGS.

II-4.2 Consideration of other radioactive sources

OPG followed COG general approach for source identification and screening. This approach is acceptable per REGDOC 2.4.2 which allows the use of alternate analysis methods of radioactive sources other than the reactor cores. Various non reactor sources of radioactivity were screened out as being insignificant risk sources at Pickering, with the exception of the

irradiated fuel bays (IFB) and the used fuel dry storage facility. A risk assessment of IFBs, and the used fuel dry storage facility has been conducted, and the overall conclusion is that the risk associated with these sources is low.

II–5. RISK AGGREGATION APPROACH FOR THE POINT LEPREAU GENERATING STATION

The Point Lepreau Nuclear Generating Station consists of a single CANDU nuclear reactor located on the northern shore of the bay of Fundy, having a net capacity of 660 MW (705 MW gross). The spent fuel bays are located adjacent to the reactor building.

The PSA developed for Point Lepreau Nuclear Generating Station considered all hazards to which the plant may be susceptible including internal hazards (that is, internal equipment failures, internal fires and internal floods) and for seismic events (i.e. external hazard). All other external hazard and combinations of hazards have been screened out from further detailed analysis using PSA.

Two methods were used for the characterization of the site risk:

— Use of existing specific hazard groups PSA results with simple summation where appropriate;
— Development of a master PSA models for full power; shutdown with PHT depressurized and full; shutdown with PHT drained.

II-5.1 Risk aggregation using the separate PSA models results

For the aggregation across hazards, simple summation is used where appropriate. For the aggregation across the plant operating states, simple summation of the at power PSA results with shutdown PSA results is not appropriate because the plant cannot simultaneously be in both plant states at the same time.

II-5.2 Development of a master model

An integrated master model file is built for both the SCDF and LRF for full power and shutdown state. The SCDF/LRF master model includes the top 99% sequences from each of the Level 1/Level 2 internal events, internal flood, internal fire and seismic events results.
Given that internal fire and internal flood PSAs are developed on a scenario based and CCDP/CCFP calculation, XInit software is used to inject fire and flood initiator beside the affected basic events (following XInit rules).
Results obtained with the ‘master model’ are lower than ‘simple aggregate results’.

II-5.3 Consideration of other radioactive sources

Fuelling machine accidents on and off reactor, are already considered as part of the internal events PSA. Fuel storage accidents: analysis shows that the time for the bay water to boil, or for the top row of bundles to become uncovered are too long, and the contribution to LRF is negligible.

II–6. CONCLUSION

Whole site risk characterization for the Pickering site is performed through a careful use of risk aggregation. The aggregation on a per hazard basis across all unit is conducted through the cutset interrogation to segregate single unit and multiunit events to avoid the double (or multiple

counting) of accident sequences. The final aggregation across hazards is performed using the simple summation. The Canadian practice for multiunit CANDU plants showed that more comprehensive characterization of multiunit PSA is gained, however more detailed technical insights are best gleaned from the per unit PSAs, on a hazard by hazard basis.

The assessment of the contributions to risk from the different hazards' groups, for the Point Lepreau station, is performed using two approaches. The first approach consists of simple summation of separate PSA results where appropriate. The second approach is the development of a master PSA model which integrates all hazards.

It is, however, acknowledged that the international community is still working for the development of guidance regarding risk aggregation.

REFERENCES

[II–1] CANADIAN NUCLEAR SAFETY COMMISSION, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, regulatory document REGDOC-2.4.2 (2014).

[II–2] INTERNATIONAL ATOMIC ENERGY AGENCY, INSAG Series, Basic Safety Principles for Nuclear Power Plants, IAEA Safety Series No 75-INSAG-3 (1988).

[II–3] INTERNATIONAL ATOMIC ENERGY AGENCY, INSAG Series, Basic Safety Principles for Nuclear Power Plants, IAEA Safety Series No 75-INSAG-3 Rev 1 INSAG-12, Vienna (1999).

[II–4] CANADIAN NUCLEAR SAFETY COMMISSION, Physical Design, Design of Reactor Facilities: Nuclear Power Plants, regulatory document REGDOC-2.5.2, Ottawa, ON, Canada (2014).

[II–5] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010). (a revision of this publication is in preparation)

[II–6] AMERICAN SOCIETY FOR MECHANICAL ENGINEERS, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sb-2013, (2017).

[II–7] CANADIAN NUCLEAR SAFETY COMMISSION, Reliability Program for Nuclear Power Plants, regulatory document REGDOC-2.6.1, Ottawa, ON, Canada (2017).

ANNEX III. REGULATORY PERSPECTIVES ON RISK AGGREGATION AND RIDM IN THE RUSSIAN FEDERATION

III–1. BACKGROUND

A general consensus has been reached in the international community that it is necessary to jointly engage both deterministic considerations and risk assessments (see, for example, section 3 [III–1]) when addressing fundamental principles and requirements of nuclear safety. Paragraph 5.8 of IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities. [III–2] states that:

> "The results of the safety assessment have to be used to make decisions in an integrated, risk informed approach, by means of which the results and insights from the deterministic and probabilistic assessments and any other requirements are combined in making decisions on safety matters in relation to the facility or activity".

Rostechnadzor, the Russian Federation regulatory body, approved a document [III–3], in which it is stated that it expects organizations responsible for operating NPPs to make an effort to apply risk informed approaches in decision making regarding NPP safety aspects. In addition, Rostechnadzor intends to actively introduce risk informed approaches in its own activity and to develop a regulatory base in this field.

One of the practical steps in this direction was the development of regulatory guideline RB-101-16 [III–4], which presents a framework for risk informed decision making. The guidance in RB-101-16 is aimed operators, plant designers, and regulatory staff and are to be applied in making and evaluating decisions, influencing NPP safety, such as changes in plant safe operating conditions, introducing modifications into safety-relevant systems and components, design and operational documentation and other modifications, which modify may affect NPP operating procedures. Finally, RB-101-16 contains recommendations on content, structure and application of research using RIDM.

III–2. METHODS OF DECISION MAKING

RB-101-16 [III-4] states that the following aspects need to be taken into consideration in making a decision, influencing NPP safety:

— Whether implementation of a decision observes the norms and regulations in the field of nuclear energy use;
— Operating experience for a corresponding NPP unit and similar units;
— Current level of scientific and engineering knowledge;
— Influence of decision on defence in depth and its elements;
— Acceptability of risk connected with the implementation of the decision.

According to RB-101-16 [III–4], a decision is considered acceptable if it does not lead to the violation of regulatory norms and regulations, its acceptability is not contradicted by the existing operational experience, it is in line with modern scientific and technical views, risk associated with the decision and its impact on defence in depth are evaluated as acceptable. The general structure of RIDM in RB-101-16 [III-4] is shown in Fig. III–1.

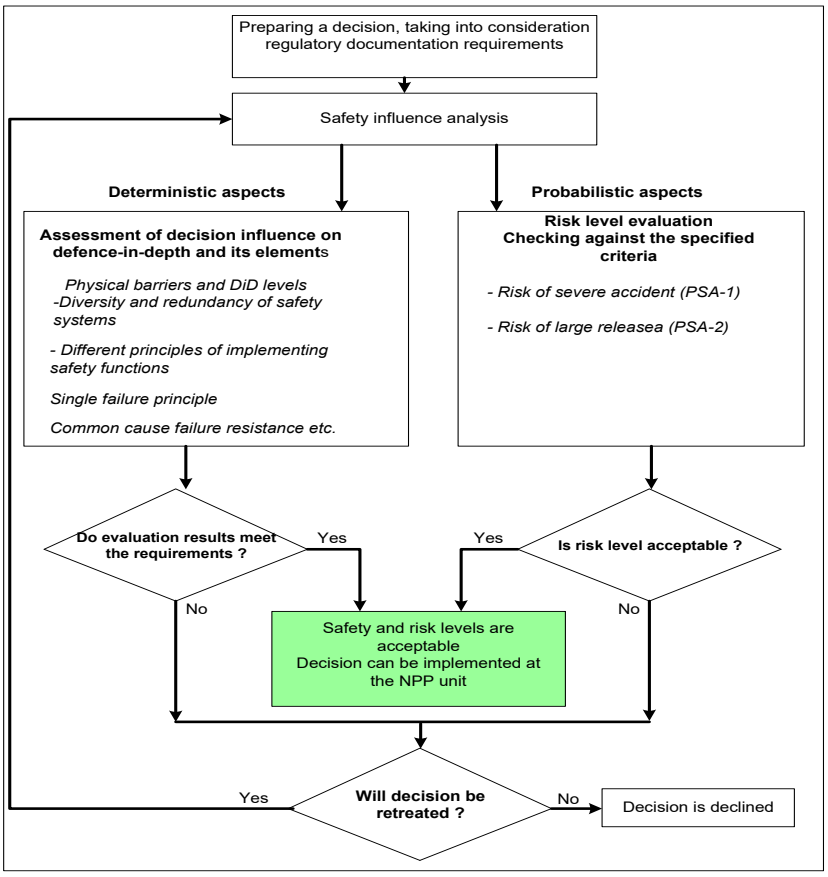


FIG. III–1. The general structure of RIDM as described in RB-101-16.

III–3. ASSESSMENT OF RISK ACCEPTABILITY

According to RB-101-16, the assessment of risk acceptability is to be performed using probabilistic analysis that meets the quality requirements stated in [III–3, III–5, III–6]. If needed, this may require updating an existing PSA model.

The decision flowchart for accounting risk acceptability in RB-101-16 is shown in Fig III–2. It consists of the following main activities:

— Validation of how well the existing probabilistic assessment of the decision under consideration represents the factors influencing safety; including its completeness. Modification of the PSA model if necessary;
— Calculating risk measures connected with the implementation of the decision;
— Assessment of risk acceptability for decision implementation given the available results for the risk metrics considered.

Probabilistic targets specified in the Russian Federation regulations in NP-001-15 [III–7] were taken as a starting point in the risk acceptability assessment approach. The first of them refers to the frequency of severe accident (if limited to the reactor core, the said frequency equals core damage frequency) with a numerical target of 10^{-5} 1/year, and the second one refers to the large emission frequency metric with a numerical target of 10^{-7} /year.

In addition, the approach takes into account such risk metrics as base severe accident frequency (SAF) and increase of SAF as a result of implementing a specific decision (along with its equivalent metrics for LRF and increase in LRF), as well as the instantaneous value of SAF. Based on the combination of values of the abovementioned metrics and according to the

developed approach, risk numerical results can be binned as falling into one of the three zones: acceptable risk (green zone), unacceptable risk (red zone) or to the zone of conditionally acceptable risk (yellow zone). Limits of the zones were chosen taking into consideration the following principles:

— If target values, established in the national regulatory documents, have not been met (unless there is a risk reduction instead of an increase), then the risk results cannot be considered to meet green zone expectations (i.e. acceptable risk);
— Green and red zones cannot have common threshold limit boundaries;
— When target values are exceeded, the yellow zone's upper limit is represented by the line of negligible risk impact31;
— When target values are exceeded considerably, any increase of risk, connected with decision making falls into the red zone;
— When base severe accident frequency or base large release frequency values are decreasing, the margin to the green yellow or yellow red boundary values are increasing.

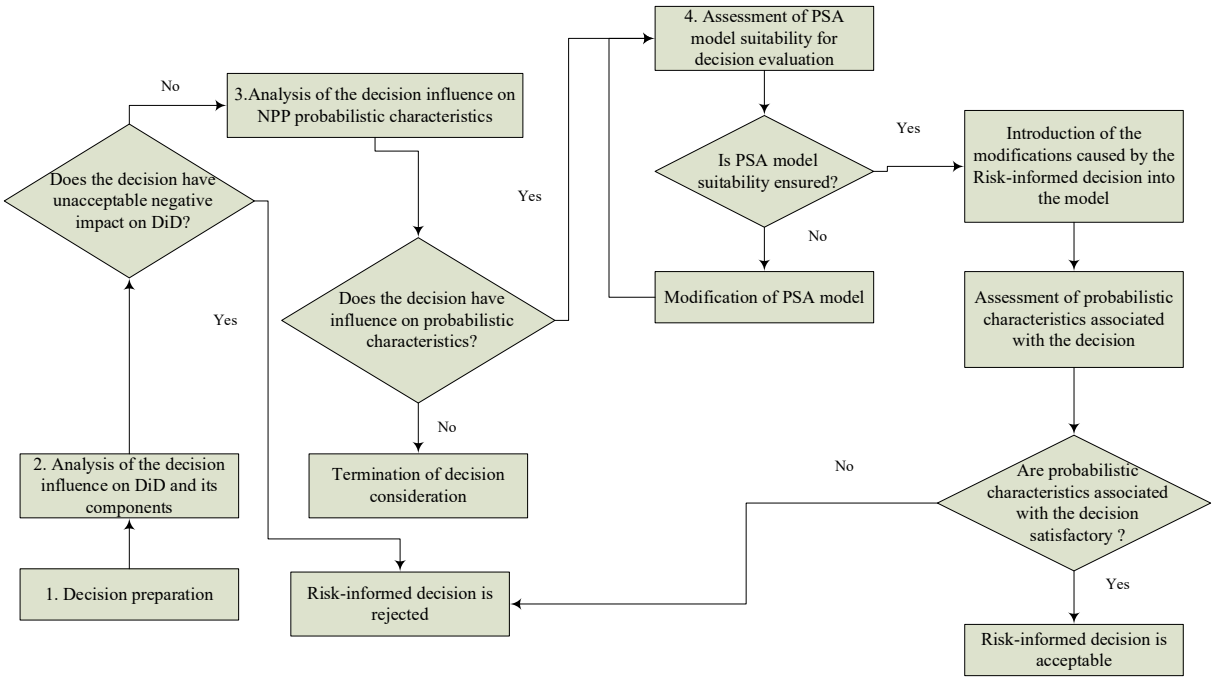


FIG. III–2. Decision flowchart in RB-101-16 for evaluating risk acceptability.

On the basis of the abovementioned considerations, two diagrams of risk acceptability were developed: one is for increment in SAF (see Fig. III–3 below), and the other one is for increment in large emission frequency (see Fig. III–4 below).

Their application can be demonstrated on the example of the first diagram. If the implementation of the decision under consideration leads to a decrease in the frequency of severe accident or to a numerical increase falling into Area III, then decision risk is considered to be acceptable.

If the implementation of the decision falls into Area II, the risk is considered to be acceptable on the condition that compensatory measures be considered for severe accident frequency

[31] It is assumed that the level of negligible risk in terms of severe accident frequency can be defined to be equivalent to a numerical threshold of 10^{-7} 1/year.

reduction. The implementation of the decision and compensatory measures need to show their impact to be associated with the intended application area they impact (i.e. those aspects of plant safety the implementation decision impact). The cumulative effect of risk changes in the implementation of previous risk informed decisions need to also be taken into consideration.

If decision implementation leads to an increase in the total probability of severe accidents and its value is in Area I, then risk of decision implementation is classified as unacceptable.

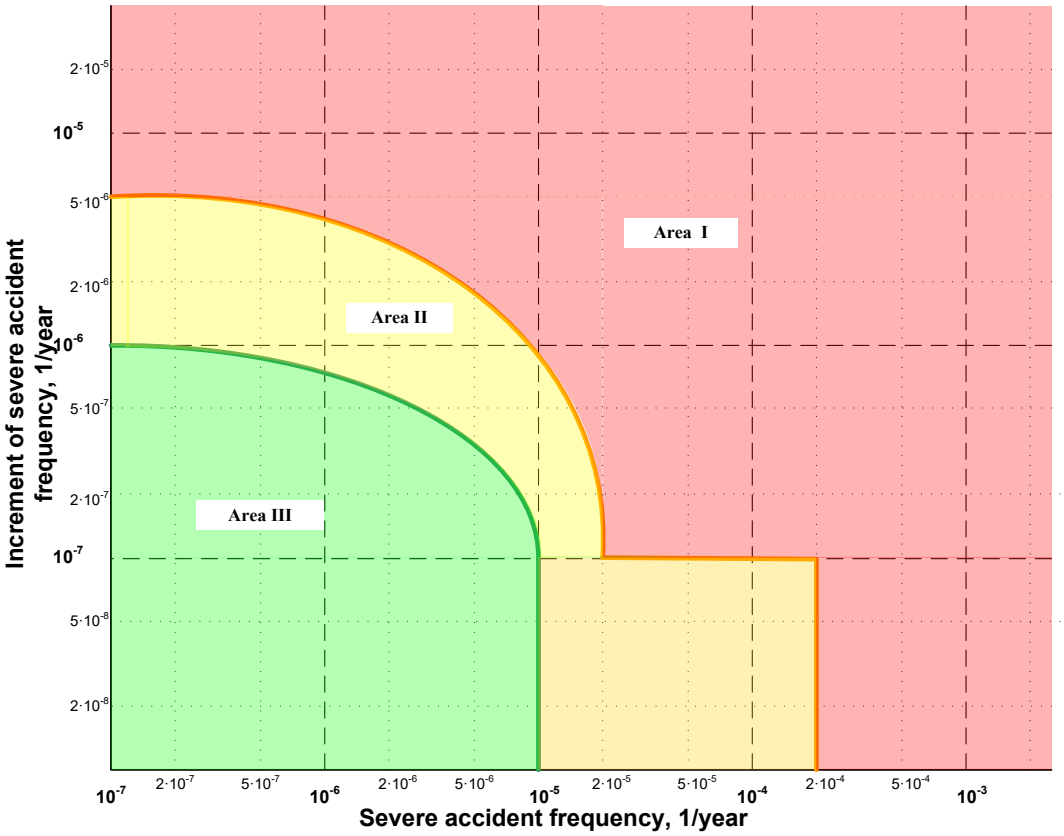


FIG. III–3. Diagram of assessment of risk acceptability for a severe accident risk measures.

Similar rules are applied to reading diagram of Fig. III–4, which represents large release frequency and its increment.

Apart from the above, there is a rule stating that irrespective of risk acceptability assessment results according to diagrams of Fig. III–3 and Fig. III–4, risk is classified as unacceptable if decision implementation leads to increase in *instantaneous* value of total frequency for severe accident of over 10^{-3} 1/year[32].

Assessment is performed using point SAF values, instantaneous value of SAF and LRF. If using 95 percentile results of the numerical results for the metrics involved, instead of mean point values leads to a different conclusion regarding risk acceptability with uncertainty aspects included, then this sensitivity insight would indicate that additional attention needs to be given to the decision under consideration.

[32] This allows to screen out short duration, but, nevertheless, dangerous changes in plant configuration.

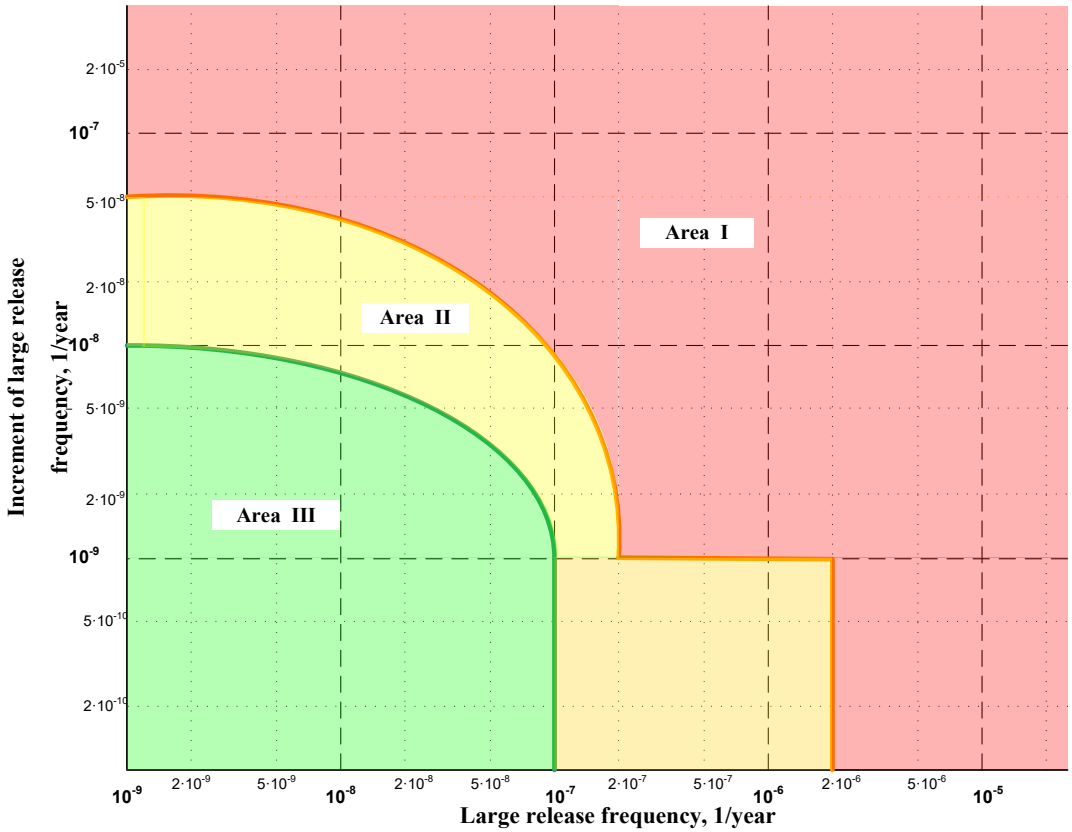


FIG. III–4. Diagram of risk acceptability for large release measures.

III–4. ASSESSMENT OF ACCEPTABILITY OF DECISION INFLUENCE ON DEFENCE IN DEPTH

While a probabilistic approach represents a valid tool for the assessment of nuclear safety, it is important to recognize limitations that may impact its input to decision making [III–8]. This is why deterministic considerations need to also be taken into account in a RIDM approach. RB-101-16 [III–4] explains that systematically addressing the influence on defence in depth is to be carried out. On the basis of the IAEA's safety reports series No. 46 [III–9], RB-101-16 provides a nomenclature of threats to plant defence in depth and threat mechanisms (the complete nomenclature contains about 60 different threats to defence in depth and about 150 corresponding threat mechanisms). An extract from RB-101-16 is given in Table III–1.

These threat mechanisms to defence in depth, according to RB-101-16, need to be analysed systematically. If the threat mechanism exists, the decision needs to consider whether it leads to an increased DiD vulnerability.

Conclusions about absence of negative influence of the implemented decision on defence in depth are to be confirmed separately for each mechanism. If negative influence of the implemented decision on defence in depth has been established, such influence may be recognized as acceptable if sufficient proof is given that the following conditions are observed: physical barriers and their protection measures remain adequately operational, there are no significant changes in probability of abnormal operation (including accidents) occurring and the plant maintains it full capacity of eliminating and mitigating effects of abnormal operation (including accidents).

TABLE III–1. RB-101-16 NOMENCLATURE OF THREATS TO DEFENCE IN DEPTH AND MECHANISMS OF THEIR IMPLEMENTATION

No	DiD level	Safety functions affected	Threats for DiD	Mechanisms	Provisions for withstanding
1	First level	All	Natural factors at site affecting the plant	1.1 Site seismology is adverse for earthquakes, stability of plant structures 1.2 Site hydrology is adverse for external flooding 1.3 Site hydrology is adverse for radioactivity proliferation 1.4 Extreme meteorological conditions (wind, high/low temperature	1. Investigation of likelihood of natural events significant for radiological risk 2. Analysis of effects on plant safety 3. Selection of subset of PIEs as design basis 4. Feasibility assessment of possible compensating safety measures 5. Implementation of measures derived from quantified probabilities and safety analysis 6. Inclusion of adequate margin into structural design
			Human activities at site affecting the plant	1.5 Release of toxic and flammable gases 1.6 Aircraft Impact 1.7 Explosions 1.8 Chemical Hazards 1.9 Other Hazards	1. Investigation of likelihood of human induced events, significant for radiological risk 2. Analysis of effects on plant safety 3. Limitations on human activities in the plant vicinity 4. Selection of subset of PIEs as design basis 5. Feasibility assessment of possible compensating safety features 6. Implementation of measures derived from quantified probabilities and safety analysis 7. Inclusion of adequate margin into structural design.
2	…	…	…	…	…
3	…	…	…	…	…

The results of the assessment of the level of changes in DiD vulnerability, caused by the decision under consideration, needs to be presented in a form given in Table III–2 below, as indicated by RB-101-16. The objective of this approach is to perform a systematic analysis of the decision under consideration, which could require sufficient documentation of the assessment of the influence on separate threats to DiD and the associated mechanisms.

TABLE III–2. PRESENTATION OF THE ANALYSES OF THE INFLUENCE ON BEYOND DESIGN BASIS ACCIDENT AND ITS COMPONENTS ON A SPECIFIC DECISION

DiD Threat Mechanism (according to Table III–1)	Negative influence yes/no	Description of negative influence on DiD and its components		Assessment of acceptability (non acceptability) of negative influence on DiD or grounds for absence of negative influence
		Increase of DiD vulnerability	Increase of probability of mechanisms of threats implementation	
1.1 Set seismology is earthquake adverse, there is a threat to stability of constructions and plant elements				
1.2 Site hydrology can challenge the plant				
1.3 Site hydrology is adverse from the point of view of radioactive substances dissemination				

REFERENCES

[III–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Framework of Integrated Risk Informed Decision Making Process. A Report by the International Nuclear Safety Group, INSAG Series, INSAG-25, IAEA, Vienna (2011).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities. IAEA Safety Standards Series No. GSR Part 4 (Rev. 1) IAEA, Vienna (2016).

[III–3] ROSTEKHNADZOR, Application of Probabilistic Safety Analysis and Risk informed approaches for Nuclear Power Plants. Circular., Moscow (2012).

[III–4] ROSTEKHNADZOR, Regulations on Applying Risk informed Methods in Making Regulatory Decisions Concerning NPPs, RB-101-16., Moscow (2016).

[III–5] ROSTEKHNADZOR, General Requirements to Probabilistic Safety Analysis, NP-095-15, Moscow (2016).

[III–6] INTERNATIONAL ATOMIC ENERGY AGENCY, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA-TECDOC-1804, IAEA, Vienna (2016).

[III–7] ROSTEKHNADZOR, General Regulations on Ensuring Safety of Nuclear Power Plants, NP-001-15, Moscow (2016).

[III–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment. A Report by the International Nuclear Safety Advisory Group, INSAG series INSAG-6, IAEA, Vienna (1992).

[III–9] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants. Safety Reports Series No. 46. IAEA, Vienna (2005)

ANNEX IV. RISK AGGREGATION FOR OPERATIONAL MODES IN MULTIUNIT CONTEXT (REPUBLIC OF KOREA)

IV–1. BRIEF DESCRIPTION OF THE SITE

There are four sites with nuclear power plants in the Republic of Korea, and each site has more than six reactor units including various types of reactor designs such as Westinghouse, Framatome, and CANDU, OPR1000, and APR1400 design. The APR 1400 design is the same reactor design as the units under construction in the United Arab Emirates. Table IV–1 shows the status of NPPs in the Republic of Korea.

TABLE IV–1. STATUS OF NPPs IN THE REPUBLIC OF KOREA

Site	Under operation	Under construction	Permanent Shutdown	Reactor Design
Kori/Saeul	6	3 (APR1400)	1 (W/H type)	Westinghouse type (PWR): Kori unit 1 ~ 4 OPR1000 (PWR): Shin-Kori unit 1&2 APR1400 (PWR): Shin-Kori unit 3 ~ 6
Hanul	6	2 (APR1400)	-	Framatome type (PWR): Hanul unit 1&2 OPR1000 (PWR): Hanul unit 3 ~ 6 APR1400 (PWR): Shin-Hanul unit 1&2
Hanbit	6	-	-	Westinghouse type (PWR): Hanbit unit 1&2 OPR1000 (PWR): Hanbit unit 3 ~ 6
Wolsong	6	-	-	CANDU type (PHWR): Wolsong unit 1 ~ 4 OPR1000 (PWR): Shin-Wolsong unit 1&2

Although the Saeul site was differentiated from the Kori site in 2017 for organizational purposes (e.g. staff)., they are considered as being in sufficient close proximity for MUPSA purposes. This presents a technical challenge in terms of gathering and assessing impacts independently between these sites against external hazards (e.g. seismic) at the moment.

As for design characteristics, NPPs in the Republic of Korea do not share systems, structures, and components (SSCs) related with safety functions defined under domestic regulation requirements, similar to Requirement 33 ‘Sharing of safety systems between multiple units of a NPP’ in IAEA SSR-2/1 and 10CFR Appendix A to Part 50 GDC criterion 5 of the US NRC. The only shared system between units, of which dependencies need to be considered in multiunit PSA models, are items not important to safety, such as instrument air systems and alternative AC diesel generators.

IV–2. DESCRIPTION OF THE OPERATIONAL MODES FOR SINGLE UNIT PSA

The first PSA models that have been developed due to the Severe Accident Policy in the Republic of Korea considered only full power operational mode. Expectations for PSA models for Low Power and Shutdown (LPSD) have been limited for new build NPPs only in the Republic of Korea. However, new regulatory requirements on PSA after the Fukushima accident, have indicated that LPSD PSA models need to be developed for all NPPs in the Republic of Korea. Whereas one operational mode is considered to develop PSA models for full power operation, about fifteen operational modes need to be considered for LPSD PSA models based on operating procedures, overhaul (O/H) experiences, and so on. Considering the operational modes for refuelling and symmetric status, nine distinct sets of PSA models can be obtained from the original fifteen:

1) RCS Cooling by using shutdown cooling system;
2) Draining mode for mid loop operation (before opening the exit of pressurizer);
3) Draining mode for mid loop operation (After opening the exit of pressurizer);
4) Mid loop operation (Install nozzle dam on S/G);
5) Filling cavity for refuelling;
6) Draining mode for 2nd mid loop operation;
7) Draining mode for 2nd mid loop operation (Remove nozzle dam on S/G);
8) Refill RCS for start up;
9) RCS heat up mode by using shutdown cooling system.

There has been a need to consider risk aggregation on the operational modes before the new regulatory requirements. Recently, however, an approach to consider an NPP availability factor (e.g. 95%) when the initiating event frequencies are estimated has been considered, based on operating experiences.

IV–3. SELECTION OF CASES (CONFIGURATION ON SITE)

To consider operating modes of all reactor units of a reference site, historical experiences of O/H and the long term plan for the O/H schedules was reviewed. Based on a chosen reference site assuming nine reactor units in operation, it was identified that all nine reactor units are operated on full power operation during only around 40% of a year. During about 50% period of a year, one reactor unit out of nine is in LPSD operating modes, and the duration of two reactor units in LPSD operating modes corresponds to about 10% period of a year. The period of time three reactor units are in LPSD operating modes was found to be negligible. Since the operating mode covering full core offload takes up a large portion of O/H duration, it was determined that the MUPSA models for five kinds of site operating status (SOS) need to be developed. The first SOS represents the operating status of all nine units on full power operation, and the second SOS is for the eight units on full power operation. In this SOS, the unit in O/H is excluded from PSA reactor modelling since all the fuel is stored in the spent fuel pool. Similarly, the third SOS considers only seven units on full power operation out of nine units. And, the fourth SOS considers the operating status when eight units are on full power operation while one unit is in LPSD operating modes. The last SOS corresponds to the operating status when seven units are on full power operation while two units are in O/H. The portions of SOS duration per year are also considered based on operating experience, which are considered in estimating multiunit initiating event frequencies. Table IV–2 shows the SOSs considered to develop MUPSA models and the portion of duration for each SOS.

TABLE IV–2. SITE OPERATING STATUS IN THE REFERENCE SITE

SOS	Description	Portion of a year
SOS 1	All nine units are on full power operation	44.8%
SOS 2	Eight units are on full power operation (Full core offload to Spent Fuel Pool in one Unit)	23.2%
SOS 3	Seven units are on full power operation (Full core offload to Spent Fuel Pool in two units)	4.7%
SOS 4	Eight units are on full power operation & one unit is in O/H	22.7%
SOS 5	Seven units are on full power operation & two units are in O/H	4.6%

One of the most important challenges on MUPSA is the modelling complexity due to the large number of reactor units. In addition, to consider the operating modes of all reactor units, the number of combinations of reactor units drastically increases. Therefore, some simplification in the modelling approach is necessary when considering multiple possible configurations of all the units on site.

To simplify MUPSA models, two approaches were considered. One is to select the representative reactor unit(s) in O/H for SOS 4&5. Although there could be nine cases for SOS 4, and thirty six cases for SOS 5, just one case for SOS 4 and 5 each is considered to develop MUPSA models. The other is to select the representative operational modes of the unit in O/H among the nine modes, described in the previous section. The most conservative operational mode out of nine modes in O/H, with respect to risk impact, would be selected as the representative operational mode. Although the number of sets of MUPSA models increases, the second conservative operational mode could be considered if the results of MUPSA are considered higher than reasonable levels.

IV–4. RISK AGGREGATION RESULTS AND INTERPRETATION

As for risk aggregation over operational modes in MUPSA, the simple sum of mean values is applied at the preliminary quantification stage. It is considered quite acceptable because the same level of multiunit initiating event frequencies with the portion of duration for each SOS and the similar level of CCDP (conditional core damage probability) models are used over all SOS.

As a result, from evaluating CDF for multiunit LOOP, the CDF level of SOS 4 was considered relatively high. So, additional MUPSA models for SOS 4 reflecting the contribution of the second most conservative operational mode are considered for further development. Since the CDF levels of SOS 4 and 5 for seismic events, however, were not significant to the total CDF for seismic events, additional MUPSA models for SOS 4 or 5 are not considered.

ANNEX V. AGGREGATION OF RISKS COMING FROM DIFFERENT HAZARDS AND PLANT OPERATIONAL STATES FOR PAKS NPP (HUNGARY)

The aim of this annex is to briefly summarize how the different risk contributors are aggregated in practice in the PSA for the Paks NPP in Hungary, focusing on Level 1 PSA for different POSs and hazards in particular. This summary is intended to underpin the methodology presented in Sections 3.3 and 3.4 of this publication as a clarification example; hence the focus is put here on some issues similar to the ones addressed in the corresponding parts of the main body of the publication.

V–1. REGULATORY REQUIREMENTS

The high level nuclear safety regulations in Hungary are the nuclear safety codes (NSC), issued as appendices to the Governmental Decree No. 118/2011(VII.11.). The NSC specify PSA related requirements too, with some distinction between operation and new NPPs. A guidance document has also been issued by the Hungarian Atomic Energy Authority related to probabilistic safety assessment of NPPs, that addresses recommendations on the fulfilment of the NSC requirements.

NSC requirements prescribe that with consideration to all planned operating modes and initiating events, the PSA results are to be used to demonstrate that:

— Core damage frequency does not exceed 10-4/a (excluding sabotage);
— Large or early release frequencies do not exceed 10-5/a (excluding sabotage and earthquake), and 10-6/a is to be targeted (by all means of reasonable plant modifications and interventions).

There are no direct requirements or guidance under the Hungarian nuclear safety regulations on how to justify the fulfilment of numerical safety criteria. However, based on the above mentioned requirements, it can be concluded, that the risk calculated for all the POSs and hazards need to be aggregated at least for justifying compliance with nuclear safety criteria.

V–2. SCOPE OF THE PSA

Unit specific Level 1 PSA models and results are available for the four WWER-440/213 type units of the Paks Nuclear Power Plant. The scope of the risk assessment with respect to hazards analysed in the Level 1 PSA can be summarized as follows:

— Internal events (separately for each unit);
— Internal hazards, i.e. internal fire and internal flooding (separately for each unit);
— External hazards (only for unit 3 as a representative unit, but extension to the other three units of NPP Paks is in progress):
  - Earthquakes;
  - Meteorological hazards: high wind, extreme snow, extreme frost;
  - External events endangering water intake from the river Danube.

Different plant operational states (POSs) were defined for the Paks NPP (full power operation is denoted by POS 0, while POS 1 through POS 24 represent for low power and shutdown (LPSD) states). Modelling of unplanned outages is out of the scope of the Paks PSA at present. The same POS definitions are used for all initiating event groups analysed. Risk estimates of each POS have been derived for all initiating event groups, except for assessing risk due to external events endangering water intake from the river Danube. The latter is limited to risk at

full power operation, although analysis of low power and shutdown states is close to completion too.

The existing unit specific PSA models and results for NPP Paks are updated annually in the frame of a living PSA programme. Accordingly, PSA updates including integration of results from further developments in the PSA scope and models can have a significant effect on the methods and possibilities of risk aggregation every year. This is especially important when a new hazard is included in the Paks PSA, or uncertainties are quantified in a specific assessment area. The PSA model for Paks NPP described below is developed using RiskSpectrum PSA software.

V–3. RISK AGGREGATION FOR DIFFERENT POSs AND HAZARDS

Hereby, the step by step risk aggregation process that has been followed in the Paks PSA is summarized. The special features of risk assessment approaches used in Paks PSA in the different analysis areas are also highlighted in the related subsections. Each hazard group is characterized by the applied modelling technique that may be relevant to risk aggregation. Amongst others, the following aspects are addressed to substantiate the risk aggregation process:

— Software tools used;
— Structure of event logic model (especially for external hazards);
— Methods of dealing with POSs;
— Risk quantification and manifestation of the results.

Firstly, risk aggregation for different POSs is presented (Section V–3.1), followed by the description of the approach applied to aggregating risk from different hazards (Section V-3.2). Similar notations are applied here to the ones used in Sections 3.3 and 3.4 in the main body of the publication.

V–3.1 Risk aggregation for different POSs

The framework of aggregating risk from the different POSs for each hazard separately to the Paks NPP in particular is shown schematically in Fig. V-1. It is noted here, that in general, interpretation of results from risk aggregation point of view need to include a discussion and evaluation concerning the heterogeneity in the assessment and in the results for the different POSs. However, according to the developers of the Paks PSA model, the level of realism, the maturity of the assessment, the types and degree of approximations, and the treatment of uncertainties do not differ to such an extent for the different hazards that would necessitate a detailed discussion of these issues. So, this aspect is not addressed specifically for any of the hazards when the interpretation of results is given.

V–3.1.1 Internal events

The RiskSpectrum PSA software was the only tool used for model development and risk quantification for internal events. No pre- or post processing was needed by means of any other tools, except for assessing the frequencies of those pipe ruptures that had to be considered as internal events as opposed to analysing them in the PSA for internal flooding.

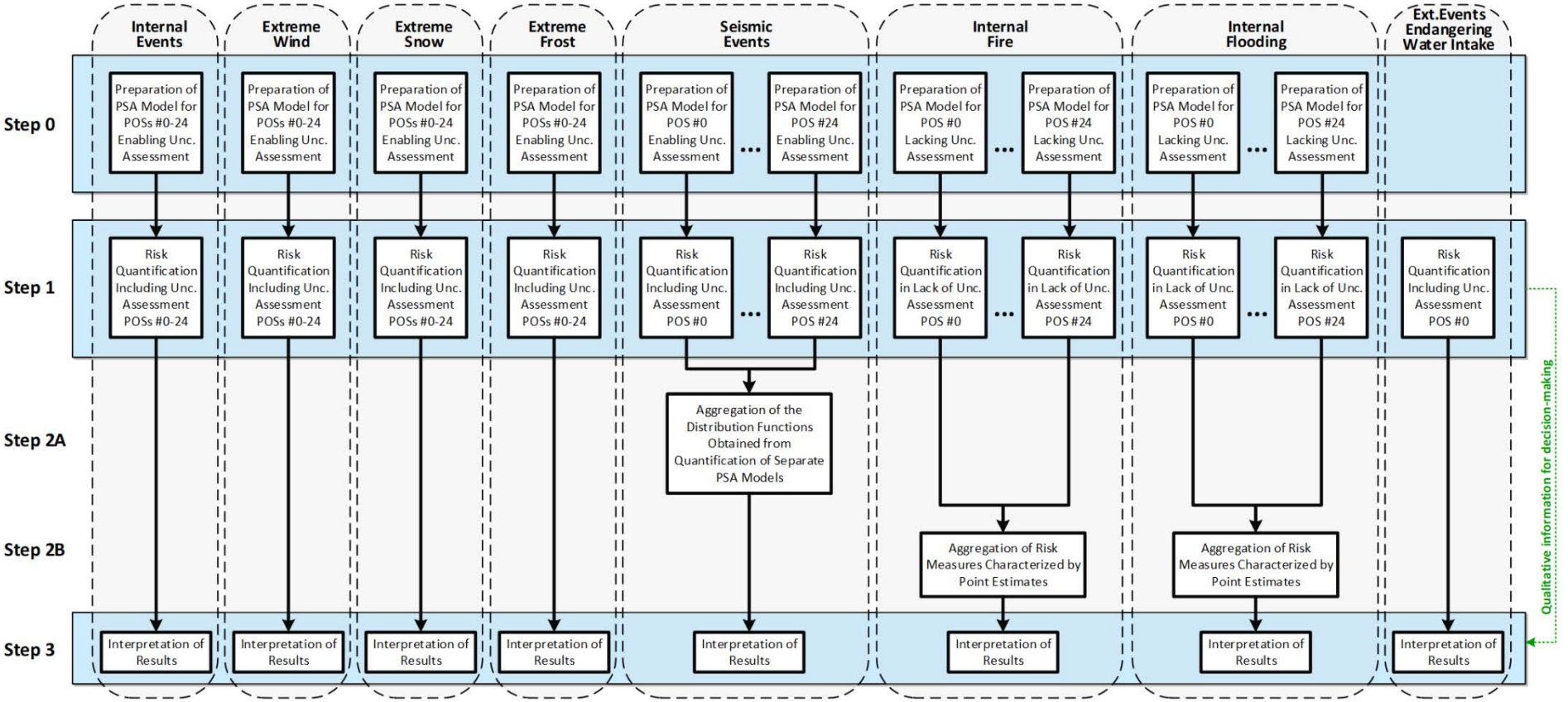


FIG. V–1. The process of risk aggregation of various POSs for the Paks NPP.

The PSA for full power and for LPSD states is integrated in the same PSA model and therefore, internal events PSA can be considered as an integrated model and there is no need to use supplementary tools to quantify risk. This enables a straightforward, relatively simple risk aggregation over the different POSs, as presented below.

V-3.1.1.1 Step 0. Preparation of the internal events PSA model to enable aggregation

The default setting of each initiating event parameter in the internal events PSA model for the Paks NPP corresponds to instantaneous event frequency that is independent of the duration of the POS in which the initiating events are assumed to occur. As this setting does not enable risk aggregation over the different POSs, a special fault tree is used in the PSA model to take the annual relative duration of each POS into account by setting a house event called 'IE_probability' and another house event related to the POS in question (e.g. called 'POS_00' or 'POS_01') to TRUE. This fault tree was put into a separate AND gate with basic events representing internal initiating events in the PSA model.

It is noted that the risk monitor for the Paks NPP is based on the plant (unit) specific PSA models. To enable a simple and accurate use of the PSA models for risk monitoring purposes, some boundary conditions (house events) are set at the level of the so called analysis cases (as opposed to setting them at event tree level in the boundary condition sets of initiating events) where the quantification of different end states for any predefined groups of initiating events are controlled. These boundary conditions are house events related e.g. to different POSs, to some system configuration settings as well as to the unavailability of plant systems or equipment including maintenance of safety system trains. To enable the risk quantification jointly for the different POSs, the boundary conditions sets used at analysis case level need to be temporarily assigned to the relevant initiating event boundary condition sets at event tree level.

V-3.1.1.2 Step 1. Risk Quantification in the internal events PSA model

After completing model preparation described in Step 0, risk aggregation is performed by specifying a dedicated analysis case that collects all internal initiating events in all the POSs. For quantification purposes, the previously mentioned house event called 'IE_probability' has to be set to TRUE in the boundary condition set assigned to the new analysis case. Since an integrated PSA model is available for internal initiating events, and model quantification is feasible within the RiskSpectrum PSA software for all the POSs, the results (including the associated sensitivity, importance and uncertainty analysis) have been obtained by the software run without the need for performing Steps 2A and 2B. It is noted that since uncertainty assessment has been performed for all the POSs for internal initiating events, the notation of 'Hazard Groups 1 to k' in Fig. 11 is applicable to internal events of the Paks PSA.

V-3.1.1.3 Step 2. Interpretation of results

For the purposes of interpreting the PSA results, first the annual core damage probability (yearly average core damage frequency) as an aggregated point estimate for the whole fuel cycle is presented. Secondly, the risk contribution from the different POSs as well as the instantaneous core damage frequency in each POS is shown in various figures and tables (see Figs V–2, V–3 and V–4 as well as Table V–1 as examples).

The reasons for the differences and similarities in the risk figures for the different POSs and POS groups are discussed based on the insights from the PSA. Also, the dominant event sequences and minimal cut sets contributing to the core damage risk from all the POSs are listed and interpreted in detail.

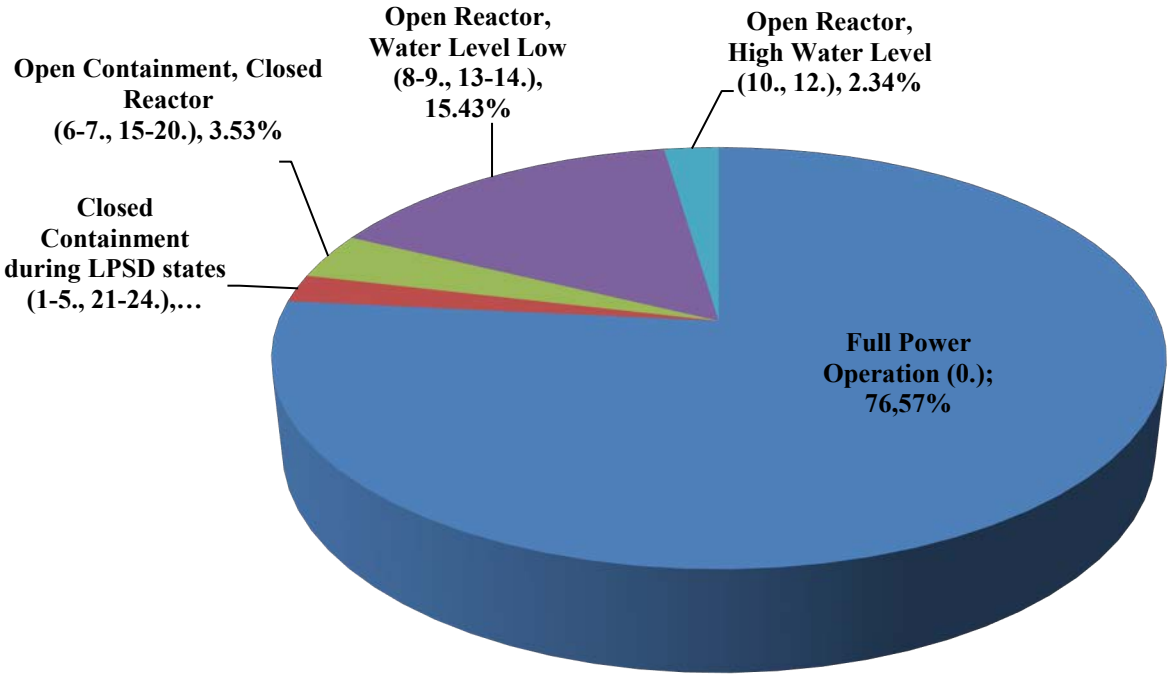


FIG. V–2. Distribution of core damage risk over POS groups.

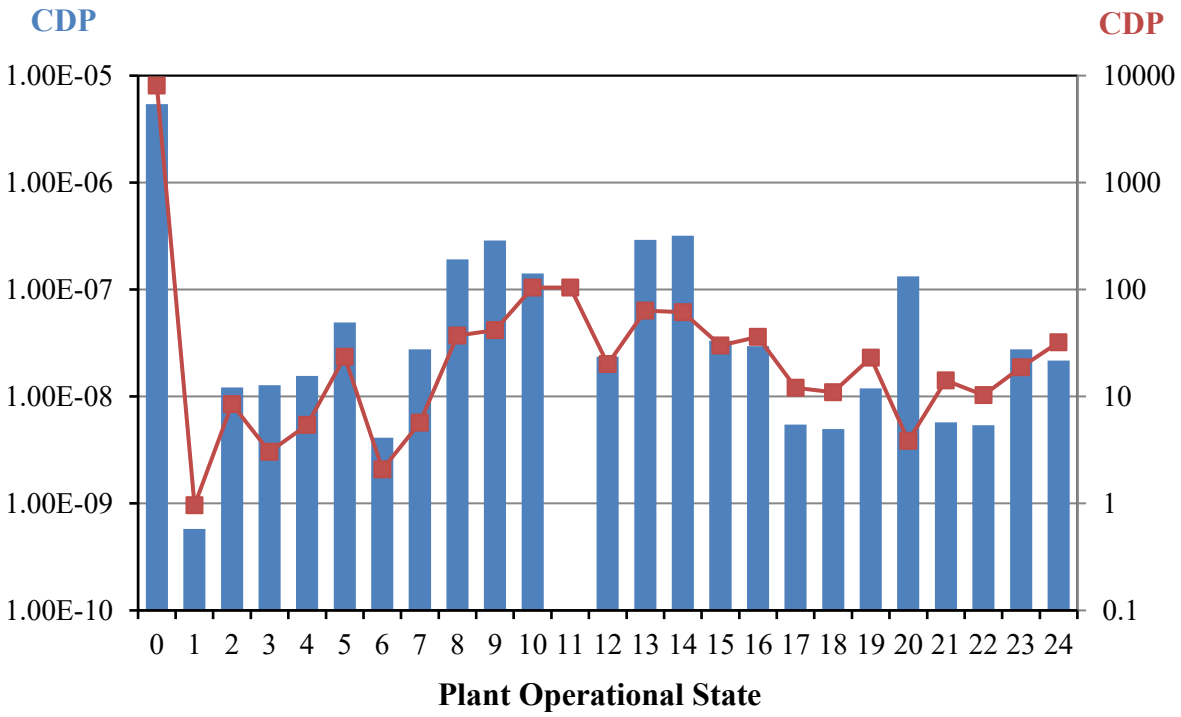


FIG. V–3. Core damage probability (blue bars) and POS duration (red line) for each POS.

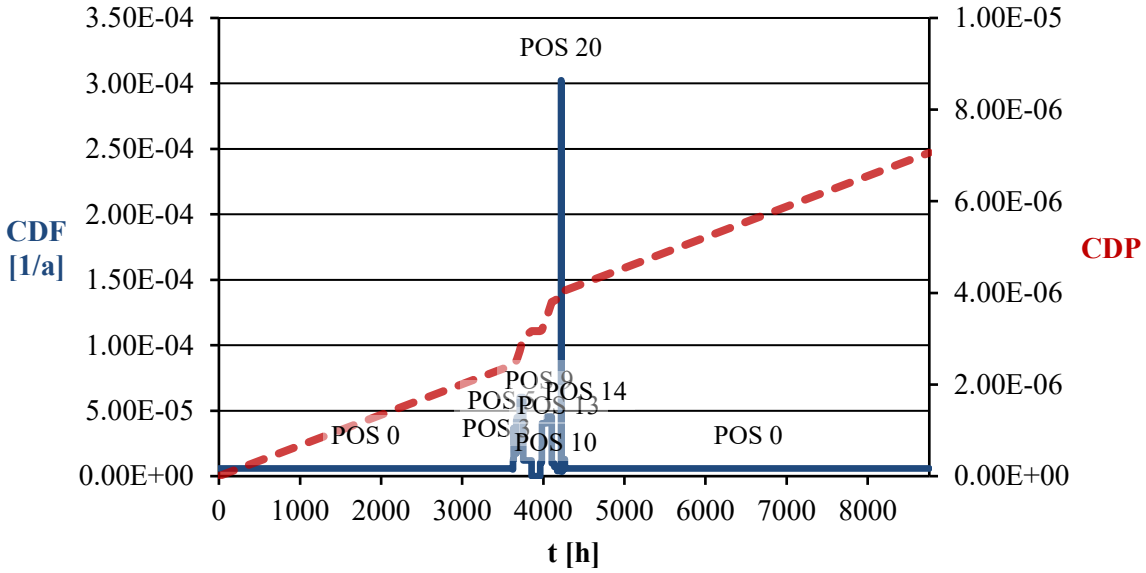


FIG. V–4. Instantaneous core damage frequency (blue line) and cumulative core damage probability (red line) over POSs.

TABLE V–1. CORE DAMAGE RISK IN THE DIFFERENT POSs

POS	CDF, [1/a]	CDP, [-]	CDP, [%]
0	$5.86\ 10^{-6}$	$5.41\ 10^{-6}$	76.57%
1	$5.27\ 10^{-6}$	$5.77\ 10^{-10}$	0.01%
2	$1.25\ 10^{-5}$	$1.21\ 10^{-8}$	0.17%
3	$3.67\ 10^{-5}$	$1.27\ 10^{-8}$	0.18%
4	$2.50\ 10^{-5}$	$1.55\ 10^{-8}$	0.22%
5	$1.82\ 10^{-5}$	$4.91\ 10^{-8}$	0.70%
6	$1.73\ 10^{-5}$	$4.11\ 10^{-9}$	0.06%
7	$4.25\ 10^{-5}$	$2.75\ 10^{-8}$	0.39%
8	$4.50\ 10^{-5}$	$1.91\ 10^{-7}$	2.70%
9	$6.05\ 10^{-5}$	$2.88\ 10^{-7}$	4.08%
10	$1.19\ 10^{-5}$	$1.41\ 10^{-7}$	2.00%
12	$1.02\ 10^{-5}$	$2.35\ 10^{-8}$	0.33%
13	$4.03\ 10^{-5}$	$2.92\ 10^{-7}$	4.13%
14	$4.55\ 10^{-5}$	$3.19\ 10^{-7}$	4.52%
15	$9.70\ 10^{-6}$	$3.32\ 10^{-8}$	0.47%
16	$7.17\ 10^{-6}$	$2.96\ 10^{-8}$	0.42%
17	$3.96\ 10^{-6}$	$5.46\ 10^{-9}$	0.08%
18	$3.96\ 10^{-6}$	$4.95\ 10^{-9}$	0.07%
19	$4.50\ 10^{-6}$	$1.19\ 10^{-8}$	0.17%
20	$3.02\ 10^{-4}$	$1.33\ 10^{-7}$	1.88%
21	$3.54\ 10^{-6}$	$5.72\ 10^{-98}$	0.08%
22	$4.56\ 10^{-6}$	$5.37\ 10^{-9}$	0.08%
23	$1.29\ 10^{-5}$	$2.77\ 10^{-8}$	0.39%
24	$5.92\ 10^{-6}$	$2.17\ 10^{-8}$	0.31%
Total		**$7.06\ 10^{-6}$**	**100.00%**

Besides presenting and interpreting point estimate results, importance and sensitivity measures relevant to all the POSs are also given. The importance and sensitivity measures are to be given for basic events, parameters and for a number of predefined attributes (e.g. human failure events, failure of electrical, I&C, mechanical components).

The uncertainties in the results considering all the POSs are presented as assessed by the RiskSpectrum PSA software using Monte Carlo simulation, and the parameter values of an approximate lognormal distribution function fitted to the simulation data are given. It is again noted, that since model quantification is feasible for internal events within the boundaries of the RiskSpectrum PSA software, aggregation of measures for importance, sensitivity and uncertainty relevant to all POSs could be performed directly by applying this code without a need for further efforts to be spent on obtaining PSA results.

V–3.1.2 Internal hazards

With respect to internal hazards, detailed PSA models were developed for internal fire and internal flood events. In addition, risk due to heavy load drops was quantified as part of the internal events LPSD PSA. The PSA models for internal fire and internal flooding were constructed by making use of a dedicated analysis tool and database called ADRIA. This tool can (1) determine equipment failures induced by the different fire and flood events, and (2) interface with the RiskSpectrum PSA based event sequence model by transferring information on the corresponding fire and flood induced failure events into the model. The minimal cut sets generated for each fire and flood scenario by processing the PSA model using RiskSpectrum PSA are subsequently transferred to ADRIA that quantifies the MCS lists and performs a validity check. The analysis is performed in the same manner for accidents at full power and in LPSD states (using ADRIA and RiskSpectrum PSA jointly).

Concerning flood events, pipe rupture is assumed at each discontinuity in the relevant piping systems, i.e. a failure event (rupture) is assigned to each pipe weld. If a pipe rupture can induce failures in the items important to safety due to jet impingement, pipe whip, compartment flooding by water or steam, spray or any other effects, then the flood event is analysed as an internal hazard. Otherwise, i.e. when no induced failure events can be expected, the initiating event in question is considered and modelled as an internal event. Accordingly, LOCA events as well as ruptures in the secondary side piping systems are included both in the internal events and in the internal flooding PSA as necessary and with an explicit distinction between ruptures without and with consequential equipment failures. The frequencies of the two initiating event categories are determined by comparing the number of potential break locations with and without consequential failures with the total number of break locations.

V-3.1.2.1 Step 0. Preparation of an internal hazards PSA model to enable aggregation

Similarly, to internal initiating events, the default setting of each internal fire or flood event parameter corresponds to the instantaneous event frequency that is independent of the duration of the POS in which the initiating events are assumed to occur. However, to enable risk aggregation over the different POSs the preprocessing module of ADRIA has been prepared to substitute the instantaneous event frequency with event probability calculated by multiplying the instantaneous event frequency and the annual relative POS duration. This model preparation proved to be necessary and sufficient to enable risk aggregation over the different POSs in the internal hazards PSA.

V-3.1.2.2 Step 1. Risk quantification in an internal hazards PSA model

The combined use of the ADRIA and the RiskSpectrum PSA software enables the analysis of each modelled fire and flood event separately, and it yields the minimal cut set lists as well. The post processing module of ADRIA is capable of aggregating the different minimal cut set lists and quantifying them jointly. For instance, if all the MCS lists are determined for each fire event in each POS, the risk over all the POSs due to internal fire is assessed by merging the MCS lists and then quantifying the aggregated list representing the total fire risk.

In the Paks PSA it was assumed that a component will either fail certainly due to fire or flood induced effects, or it will maintain its function (with the corresponding random failure probability) in case of a fire or flood event. So, the failure probability due to an internal hazard is considered to be either 1 or 0. The ADRIA preprocessing tool sets the basic events that are assumed to fail due to a given fire or flood event to TRUE. In this manner, the minimal cut sets generated by RiskSpectrum PSA do not include any of the hazard induced failures. Thus, these failures cannot be taken into account in uncertainty, importance and sensitivity analyses. Since uncertainty, importance and sensitivity analyses could not be performed for the probabilities of fire and flood induced component failures, i.e. for the failure events that actually represent the hazard related effects in the model, it was decided not to do risk quantification other than performing point estimate calculations. Therefore, a limited uncertainty analysis was not performed either by considering uncertainties only in the non hazard related parts of the PSA model (e.g. random failures). It was even considered that mechanistically performing uncertainty, importance and sensitivity analyses by neglecting the effects of hazards induced failures due to the underlying modelling assumption mentioned above could easily give rise to misinterpretation and biased opinion over the PSA results. Consequently, the notation of 'Hazard Groups m+1 to n' in Fig. 11 is applicable to internal hazards of the Paks PSA.

The ADRIA tool is capable of assessing the risk contribution of the different fire compartments, fire ignition sources, flood sources, flooding processes. Since all kinds of calculations referred to above are feasible by using ADRIA and RiskSpectrum PSA in a 'coupled' manner, there is no need to perform Steps 2A and 2B.

V-3.1.2.3 Step 3. Interpretation of results

The point estimate results are interpreted in the same manner as it is given for internal events above. Additionally, the risk contributions of the different fire compartments, fire ignition sources, flood sources and flooding processes are shown in figures (see Fig. V–5. as an example). It is again noted that no uncertainty, classical importance and sensitivity assessment has been performed for internal hazards, so the aggregated results of these measures cannot be presented either[33].

V–3.1.3 Seismic events

The Level 1 seismic PSA was developed in the same PSA model that includes the event logic model for internal events and internal hazards too. For modelling purposes, the whole spectrum

[33] It is noted however, that the sensitivity of the fire and flood PSA results to hazards induced failure events was studied by varying the assumptions made on the occurrence/likelihood of these events, which was particularly useful in conceptualising measures for safety improvements.

of seismic accelerations was subdivided into 7 disjoint accelerations ranges, so for each of the 25 POSs 7 different seismic event trees were delineated in a single PSA model.

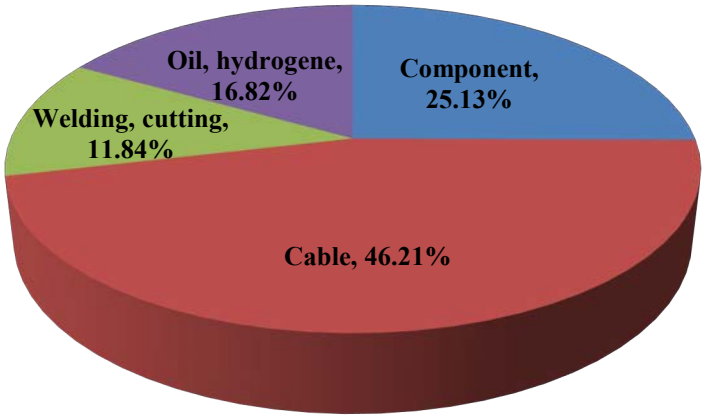


FIG. V–5. Distribution of fire induced core damage risk over fire ignition source groups.

Each seismic event tree starts with a seismic event related to a given acceleration range as initiator, and then it branches off for the different transient initiating failures modelled as event tree headers. A single event tree header was used as the last header after the headers for the seismic induced transient initiating failures. That last header collects the failures of all the mitigation functions and the associated SSCs, i.e. all the core damage event sequences attributable to all the single transient initiating failures. Hence, a simple reading of such a generic event tree structure is that the upper branch represents (as usual) the success of an event tree header (the given transient initiating failure does not occur), while the lower branch represents the failure of the given event tree header (occurrence of the given transient initiating failure). By setting the appropriate boundary condition sets on each event sequence, the last header represents all the mitigation functions and systems for the transients modelled in the corresponding event sequence. Thus, the quantification of 7 event trees is needed in each POS to assess the POS specific seismic induced core damage risk. Seismic accident sequences are modelled in the same manner at full power and at LPSD states by using RiskSpectrum PSA and a dedicated post processing tool jointly.

V-3.1.3.1 Step 0. Preparation of the seismic PSA model to enable aggregation

Similarly, to internal initiating events, the default setting of each seismic initiating event parameter corresponds to the instantaneous event frequency. The dedicated fault tree built for risk aggregation purposes in the internal events PSA (see 'Internal events' part of Section V-3.1 of this annex for details) was put into a separate AND gate with basic events representing seismic initiating events in the PSA model. Also, to enable risk aggregation over the different POSs, boundary conditions sets used on analysis case level need to be temporarily assigned to the relevant seismic initiating event boundary condition sets at the level of seismic event trees as additional house events (see 'Internal events' part of Section V–3.1 of this annex for details).

V-3.1.3.2 Step 1. Risk quantification in the seismic PSA model

Point estimate quantification is performed using mean hazard frequencies for the specified acceleration ranges and mean values of seismic failure fractions that are derived from the fragility analyses for each seismic acceleration range. After completing model preparation specified in Step 0, risk aggregation of point estimate is performed by specifying a dedicated analysis case that collects all seismic initiating events for all acceleration ranges in all the POSs. For quantification purposes, the house event called 'IE_probability' has to be set to TRUE in

the boundary condition set assigned to the analysis case. The RiskSpectrum PSA software was the only tool used for model development and point estimate calculations for all the POSs, so the point estimate results can be made readily available without the need for performing Steps 2A and 2B. However, uncertainty, importance and sensitivity analyses cannot be fully completed by the RiskSpectrum PSA software, only the results (MCS lists, importance and sensitivity measures) of each acceleration range are determined separately in each POS. Hence, Step 2A had also to be performed for aggregating uncertainties (as well as importance and sensitivity measures) for all the acceleration ranges in each POS. It is noted that since uncertainty assessment has been performed for all the POSs for seismic events, the notation of 'Hazard Groups 1 to k' in Fig. 11 is applicable to modelling seismic accident sequences in the Paks PSA.

V-3.1.3.3 Step 2A. Aggregation of the distribution functions obtained from quantification of separate PSA models

Relevant MCS lists in Step 1 were determined for each acceleration range in each POS by using RiskSpectrum. A dedicated code was developed to combine the complete set of seismic hazard curves and the full range of fragility distributions for seismic failures at different confidence levels through a convolution integral to establish true uncertainty distributions for seismic induced failure frequencies. Also, uncertainties in seismic induced failures were combined with uncertainties in human error rates and random equipment failures using Monte Carlo simulation with the dedicated code developed for that purpose. As a preparatory step, 1000 different sets of random numbers are established, and a separate number is assigned in each set to every basic event included in the seismic PSA model.

The minimal cut sets for each acceleration range and each POS (corresponding to 7·24=168 MCS lists in the Paks PSA) are the input parameters of the special purpose code. It then calculates the risk corresponding to each MCS list 1000 times using the prepared sets of random numbers, and it sums up the CDF values from those runs that have been performed with the same set of random numbers. This process leads to the generation of 1000 aggregated risk values that characterize the probability distribution function of the aggregated seismic risk. This approach considers the state of knowledge correlation (SOKC) between events, i.e. the same value is taken into account for a failure parameter in all the minimal cut sets in every round of uncertainty calculations. This cannot be ensured when only the distribution functions are aggregated mathematically.

Although aggregation of importance and sensitivity measures are not covered in the methodology elaborated in Section 3.4 of the main body of this publication, the approach used in the seismic PSA of the Paks NPP is summarized here for reference. The aggregated importance and sensitivity measures are determined by making use of the same special purpose code that is applied for aggregating uncertainties. As input data to such calculations by the dedicated post processing tool, use was made of the importance and sensitivity measures calculated for the different seismic acceleration ranges in every POS by the RiskSpectrum PSA software. The aggregated importance and sensitivity measures have been quantified by using the following formulas:

$$FC(BE^*) = \frac{\sum_{i=1}^{N} FC_i(BE^*) \cdot CDP_i}{CDP} \quad \text{(V–1)}$$

$$RDF(BE^*) = \frac{1}{1-FC(BE^*)} = \frac{CDP}{\sum_{i=1}^{N} \frac{CDP_i}{RDF_i(BE^*)}} \quad \text{(V–2)}$$

$$RIF(BE^*) = \frac{\sum_{i=1}^{N} RIF_i(BE^*) \cdot CDP_i}{CDP} \quad \text{(V–3)}$$

$$SE(BE^*) = \frac{CDP_U(BE^*)}{CDP_L(BE^*)} = \frac{\sum_{i=1}^{N} CDP_{U,i}(BE^*)}{\sum_{i=1}^{N} CDP_{L,i}(BE^*)} \quad \text{(V–4)}$$

where:

$FC(BE^*)$ – fractional contribution of basic event BE^* in relation to the aggregated core damage risk;
$RDF(BE^*)$ – risk decrease factor of basic event BE^* in relation to the aggregated core damage risk;
$RIF(BE^*)$ – risk increase factor of basic event BE^* in relation to the aggregated core damage risk;
$SE(BE^*)$ – sensitivity measure of basic event BE^* in relation to the aggregated core damage risk;
$FC_i(BE^*)$ – fractional contribution of basic event BE^* in relation to the i-th seismic event tree;
$RDF_i(BE^*)$ – risk decrease factor of basic event BE^* in relation to the i-th seismic event tree;
$RIF_i(BE^*)$ – risk increase factor of basic event BE^* in relation to the i-th seismic event tree;
CDP_i – core damage risk (probability) due to the i-th seismic event tree;
CDP – aggregated core damage risk:

$$CDP = \sum_{i=1}^{N} CDP_i \quad \text{(V–5)}$$

$CDP_U(BE^*)$ – upper bound of aggregated core damage risk;

$CDP_L(BE^*)$ – lower bound of aggregated core damage risk;

$CDP_{U,i}(BE^*)$ – upper bound of core damage risk in relation to the i-th seismic event tree;

$CDP_{L,i}(BE^*)$ – lower bound of core damage risk in relation to the i-th seismic event tree;

N – number seismic event trees (number of seismic initiating events equals 7-24).

It has to be noted that these well known formulas are applicable only if the rare event approximation is acceptable, which cannot be ensured for large seismic acceleration that can lead to high seismic failure probabilities.

V-3.1.3.4 Step 3. Interpretation of results

The results are interpreted in the same manner as it is described for internal events in 'Internal events' part of Section V–3.1 of this annex. Additionally, the risk contributions of the different acceleration ranges are shown in various ways too (see Fig. V–6. as an example, where SEIS1 – SEIS7 represent the different seismic acceleration ranges in terms of peak ground acceleration).

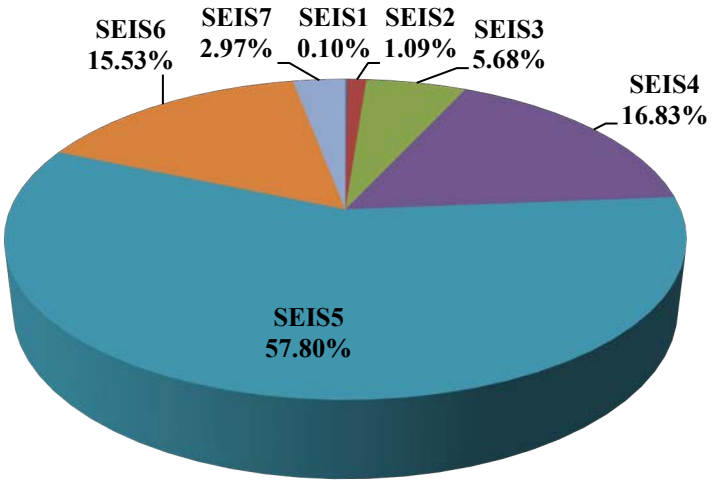


FIG. V–6. Distribution of seismic induced core damage risk over seismic acceleration ranges.

V–3.1.4 Meteorological hazards

A detailed logic model was developed for extreme wind, snow and frost hazards, and therefore core damage risk has been quantified for these meteorological hazards as well. Unlike in seismic PSA, a single event tree was delineated for each meteorological hazard in each POS without binning hazard intensities into different ranges, since continuous hazard and fragility curves are used for the whole range of hazard intensities of interest. Use of continuous hazard and equipment fragility curves enables a convenient treatment of numerous fragility curves with largely varying means and variance during quantification as well as straightforward numerical assessment of uncertainty and sensitivity. A so-called generic event tree was built up for each meteorological hazard in every plant operational state to identify hazard induced core damage sequences. This event tree models both single and multiple hazard induced transients together with the associated consequences on plant and human responses in the same manner as it is presented for 'External hazards' in Section V–3.1 of this annex.

V-3.1.4.1 Step 0. Preparation of a meteorological hazards PSA model to enable aggregation

The preparation of the model was performed in line with the steps described for internal initiating events (see 'Internal events' part of Section V–3.1 of this annex for details) or for seismic events (see 'External Hazards' part of Section V–3.1 of this annex for details).

V-3.1.4.2 Step 1. Risk quantification in an external hazards PSA model

The dominant core damage minimal cut sets of failures induced by meteorological hazards are determined in the first place by using the RiskSpectrum PSA software. In particular, a common PSA model is applied that includes the event logic model for all other hazards too. The dominant minimal cut sets are generated by specifying a dedicated analysis case that collects all initiating events relevant to a specific meteorological hazard in all the POSs. In order to take the relevant POS into account in each MCS, the house event called 'IE_probability' has to be set to TRUE in the boundary condition set assigned to the analysis case.

Since RiskSpectrum PSA is not fully capable of performing the numerical approximation of the convolution integral if for fragility curves a special function other than dual lognormal distribution is used, following the generation of minimal cut sets a separate, stand alone

computer code was applied to determining cut set frequencies, calculating the overall core damage frequency, and performing importance and sensitivity analyses.

The following measures of importance and sensitivity were calculated for the different hazard induced failure events and failure event groups in relation to the cumulative plant risk:

— Fussel-Vesely importance (fractional contribution – FC);
— Risk reduction worth (risk decrease factor – RDF);
— Sensitivity measures (SU, SL, SU/L).

The sensitivity measures were determined by assuming a higher and a lower value of HCLPF (high confidence on low probability of failure) for the failure events in question. These higher and lower values were selected so that they represented one order of magnitude change in the hazard occurrence frequency. Moreover, we assessed the expected decrease in the cumulative annual core damage probability if the HCLPF of those fragility groups that have lower resistance than the design basis of the plant was increased up to the design basis value. The results of these analyses enabled the characterisation of expected risk reduction if certain safety improvements were made. Uncertainty quantification was done by using the same special purpose in house developed code that was developed in support of the seismic PSA (see 'External hazards' part of Section V–3.1 of this annex), but in this case the aggregated minimal cut sets for all the POSs were used as input to the calculations.

Since dedicated computer codes are used for calculating the overall core damage frequency and for performing importance, sensitivity and uncertainty analyses so that these codes directly make use of the minimal cut sets for all the POSs in total, the point estimate results are readily available without the need for performing Steps 2A and 2B. It is noted that since the uncertainty analysis was performed for all the POSs for each meteorological hazard, the notation of 'Hazard groups 1 to k' in Fig. 11 is applicable to modelling each meteorological hazard in the Paks PSA.

V-3.1.4.3 Step 3. Interpretation of results

The results can be interpreted in the same manner as it is presented for internal events in the 'Internal events' part of Section V–3.1 of this annex. However, the presentation of importance and sensitivity measures is limited to hazard induced failure events, in contrast to determining these measures for all random failures in the model too.

the external events PSA for the Paks NPP, Hungary has recently been extended with an analysis of events that can lead to loss of ultimate heat sink due to accidental discharge of dangerous substances into the river Danube. Those substances were considered dangerous in the analysis that can directly or indirectly disable water intake from the river. An event tree was developed for each type of contamination. The 'small event tree – large fault tree' concept was applied during event sequence development. Unlike in the PSA for other external hazards, all event tree headers relate to one of the relevant mitigating actions or system operations, as for internal events. As already mentioned, this assessment is limited to full power operation at present. Therefore, risk aggregation for different POSs has no relevance to this hazard. It is noted that since uncertainty assessment was performed for external events endangering water intake from the river Danube, the notation of 'Hazard Groups 1 to k' in Fig. 11 is applicable to this hazard type in the Paks PSA.

V–3.2 Risk Aggregation for different hazards

The Level 1 PSA model for internal events was used as the basis for developing PSA models for internal and external hazards. The PSA models have been developed in a common RiskSpectrum PSA model for all the analysed initiating events and hazards. However, the joint hazard specific PSA models cannot be considered as a truly integrated PSA model, even if each hazard specific risk assessment makes use of the RiskSpectrum model that was elaborated originally for internal events, since risk quantification cannot be completed by using the very same and single analysis tool that has been applied for model construction, i.e. by the RiskSpectrum PSA software. In this respect risk needs to be aggregated taking into account 'separate' PSA models for hazards or hazard groups. The framework of aggregating risk from different hazards to the Paks NPP in particular is shown schematically in Fig. V–7.

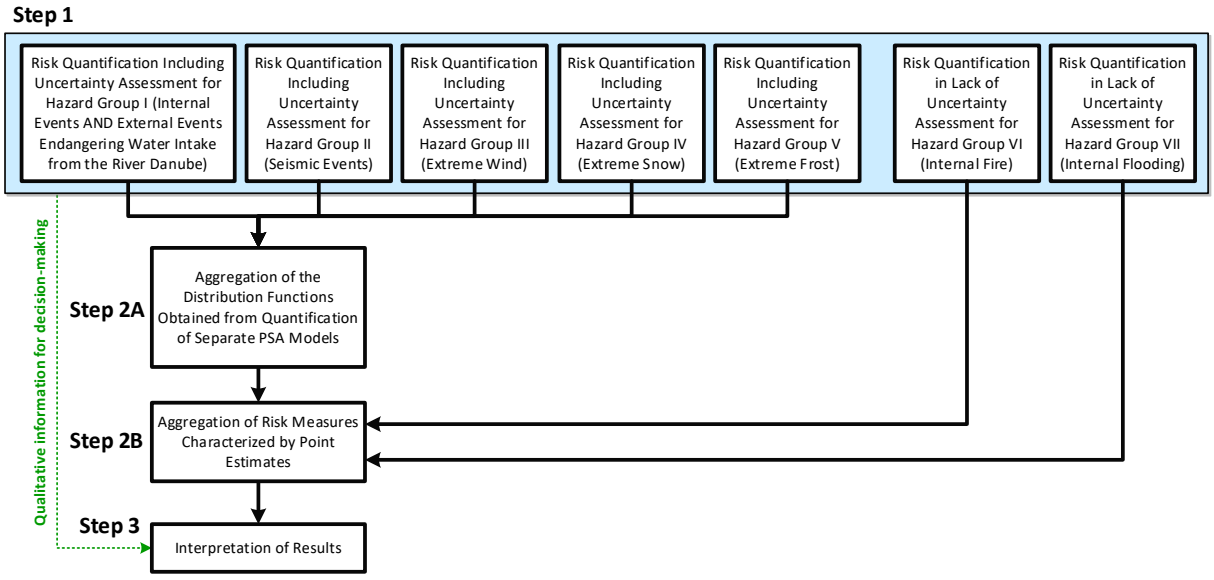


FIG. V–7. The process of risk aggregation of various hazards for the Paks NPP.

V–3.2.1 Step 1. Risk quantification in the separate PSA models

(a) Risk quantification including uncertainty assessment for hazard group I (internal events and external events endangering water intake from the river Danube)

The PSA model for internal events can be considered as an integrated model, since all the POSs are incorporated in one PSA model, and there is no need for any other tool to quantify risk but RiskSpectrum PSA. Moreover, the PSA for external events endangering water intake from the river Danube was developed in the same PSA model that includes the event logic model for internal initiating events too. No pre- or post processing is needed by means of any additional tool for assessing risk due to river contamination hazards, so model development and quantification are performed within the RiskSpectrum PSA software.

After completing model preparation described in Step 0 in the 'Internal events' part of Section V–3.1 of this annex, risk aggregation is performed by specifying a dedicated analysis case that collects all internal initiating events and external events endangering water intake from the river Danube in all the POSs. For quantification purposes, the house event called 'IE_probability' has to be set to TRUE in the boundary condition set assigned to the new analysis case.

(b) Risk quantification including uncertainty assessment for hazard group II (seismic events)

The PSA model for internal events and seismic events cannot be considered as a fully integrated model. Since only the point estimate calculations can be performed using the very same software that has been applied for model development, and a separate analysis tool needs to be used for the purpose of uncertainty assessment. The quantification of seismic risk is described in detail in 'External hazards' part of V–3.1 of this annex, so no further discussion is needed here.

(c) Risk quantification including uncertainty assessment for hazard group III (extreme wind)

The PSA model for internal events and meteorological hazards cannot be considered as a fully integrated model, since the risk from meteorological hazards is quantified separately from the RiskSpectrum PSA software by using a dedicated code developed for this purpose. Moreover, risk quantification is performed separately for the different meteorological hazards by making use of this spreadsheet application. Thus, the different hazards are virtually treated as different hazard groups. The quantification of risk due to meteorological hazards is described in detail in 'External Hazards' part of V–3.1 of this annex, so no further discussion is needed here.

(d) Risk quantification including uncertainty assessment for hazard group IV (Extreme Snow)

See the discussion on extreme wind above.

(e) Risk quantification including uncertainty assessment for hazard group V (Extreme Frost)

See the discussion on extreme wind above.

(f) Risk quantification in lack of uncertainty assessment for hazard group VI (internal fire)

Unit specific PSA models are available for internal fire and internal flood hazards that have been partly developed and quantified with the RiskSpectrum PSA software in the same PSA model that includes the event logic model for internal events too. On the other hand, a dedicated software called ADRIA was developed in support of model development and for pre- and post processing purposes, so the PSA model for internal events and internal hazards cannot be considered as a fully integrated model. Moreover, the internal fire and flood events are quantified separately from each other with ADRIA, so they are also treated as different hazard groups. The quantification of risk due to internal hazards is described in detail in see 'Internal hazards' part of Section V–3.1 of this annex, so no further discussion is needed here.

(g) Risk quantification in lack of uncertainty assessment for hazard group VII (internal flooding).

See the discussion on internal fire above.

V–3.2.2 Step 2A Aggregation of the distribution functions obtained from quantification of separate PSA models

The distribution functions obtained in Step 1 for hazard groups I-V quantified in separate analysis tools are aggregated in this step. A dedicated software tool capable of aggregating the

different distribution functions via Monte Carlo simulation is used. Fig. V–8 shows the distribution functions characterising uncertainties in risk due to internal events AND external events endangering water intake from the river Danube, seismic events, extreme wind, extreme snow, extreme frost, and all hazards in total.

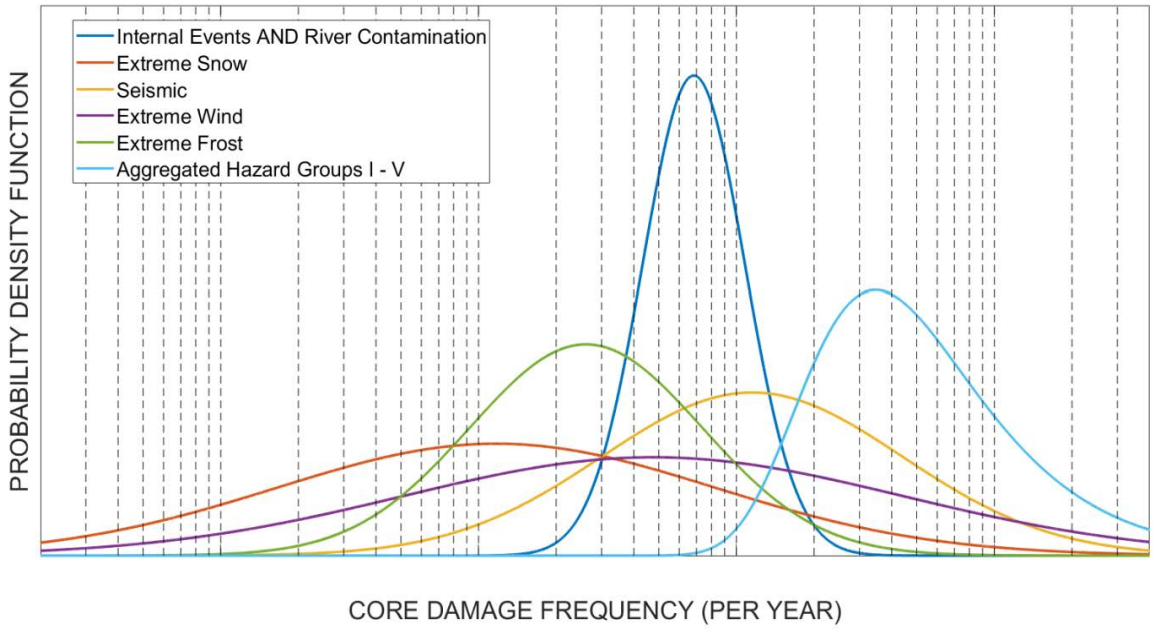


FIG. V–8. Aggregating distribution functions of hazard groups I-V.

V–3.2.3 Step 2B Aggregation of risk measures characterized by point estimates

The aggregated distribution function obtained in Step 2A and the point estimates quantified in Step 1 for internal fire and internal flood events that have not been subject to quantitative uncertainty analysis in PSA are summed up in this step. In practice, the aggregated distribution function was shifted by the point estimates of risk due to internal hazards in total via simple addition (see Fig. V–9).

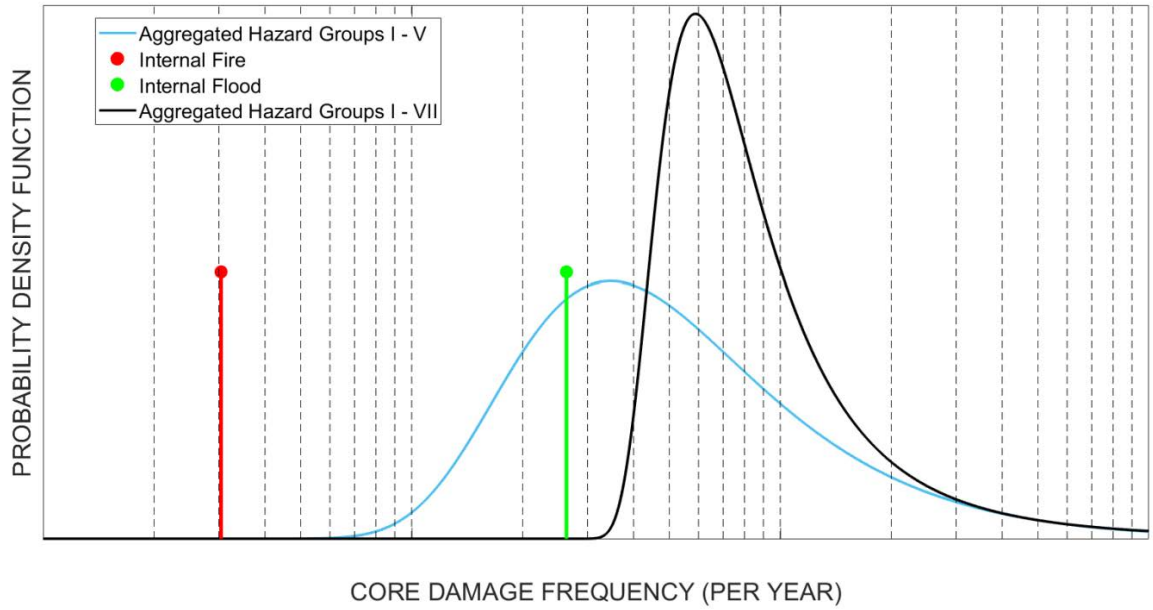


FIG. V–9. Aggregating the distribution function of hazard groups I-V in total and the point estimates of hazard groups VI-VII.

V–3.2.4 Step 3. Interpretation of results

The aggregated risk results due to all hazards and POSs are characterized by a point estimate and by the relevant distribution function representing the effects of uncertainties in the risk estimate (see the aggregated distribution function in Fig. V–9).

Additionally, the contributions of the major hazard groups to the total risk are also presented in a pie chart with an indication of contributions due to full power as well as shutdown risk (see Fig. V–10). It is noted that in Fig. V–10 all external hazards other than earthquake (i.e. meteorological hazards and river contamination) are grouped together as 'other external events'.

Moreover, detailed hazard specific risk results are presented in the same manner as discussed for POSs in Section V–3.1 of this annex. Aggregated importance and sensitivity measures are not derived in the PSA for the Paks plant, all safety enhancement proposals are based on separate hazard specific importance and sensitivity analyses.

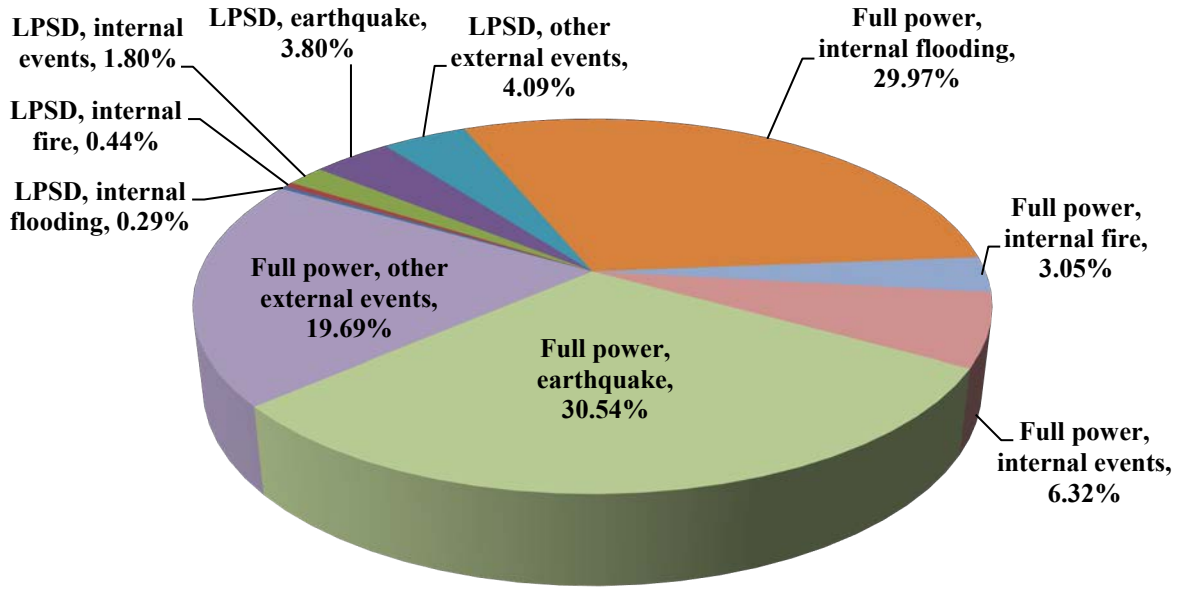


FIG. V–10. Distribution of overall core damage risk over the main hazard types in full power and LPSD operation.

To establish an appropriate basis for decision making with due considerations to the aggregated risk, the heterogeneity in the aggregated assessment and in the results for the different hazard groups are discussed in detail. Over and above the contribution to the overall risk (see Contr. column in Table V–2), information on the following attributes of each hazard is also given in Table V-2 as these are the most important factors in heterogeneity of the aggregated results:

— Characteristics of uncertainty assessment (Uncertainty column in Table V–2);
— Degree of conservatism ('Conserv.' column in Table V–2);
— Limitations of the assessment ('Limit' column in Table V–2).

TABLE V–2. SUMMARY INFORMATION ON RISK AGGREGATION FOR DIFFERENT HAZARDS

#	Hazards	Contr.	Uncertainty	Conserv.	Limit.
1.	Internal events	8.12%	Comprehensive quantitative uncertainty analysis witnessing relatively narrow bounds of uncertainty, short qualitative description of types and sources of uncertainties not quantified	Low	Low
2.	Internal hazards	33.75%	Qualitative	Moderate	Moderate
3.	Earthquake	34.34%	Comprehensive quantitative uncertainty analysis witnessing large uncertainties, short qualitative description of types and sources of uncertainties not quantified	Moderate	Moderate
4.	Meteorological hazards	22.80%	Comprehensive quantitative uncertainty analysis witnessing relatively large bounds of uncertainty, short qualitative description of types and sources of uncertainties not quantified	Moderate	Moderate
5.	External events endangering water intake from the river Danube	0.98%	Limited quantitative uncertainty analysis witnessing relatively narrow bounds of uncertainty, short qualitative description of types and sources of uncertainties not quantified	Moderate	Moderate

V-3.2.4.1 Internal events

The uncertainties in component reliability data, human error rates, initiating event frequencies and any other elements of the PSA model have been described parametrically to the extent found feasible. However, there are some model parameters that do not have uncertainty bounds, e.g. POS durations. The PSA for internal events is always in the focus of PSA update performed annually in the living PSA programme of the plant. A major goal of these updates is to reflect the risk implications of plant modifications of various kinds, such as replacement of equipment, design modifications, changes in plant procedures (e.g. emergency operating procedures), changes in practices in operations or maintenance (some most recent examples being the implementation of a 15 month fuel cycle as opposed to the previous 12 month cycle and introduction of online maintenance). Every 10 years the updates also cover review and update of component reliability data using plant specific data to the greatest extent possible but also looking at improvements in generic databases. Finally, the results of new PSA developments (e.g. extensions in the scope of PSA refinements in modelling details) are also considered in the updates. Hence, a lot of efforts are made in order to keep the internal events PSA up to date, to eliminate unnecessary conservatism and to remove or reduce limitations in the assessment as far as practicable. The internal events PSA of the Paks NPP is considered mature and is regarded as a solid basis for both risk quantification and PSA applications.

V-3.2.4.2 Internal hazards

No quantitative uncertainty analysis has been performed in the internal hazards' PSA of the Paks NPP, hence only point estimates of risk are quantified. It is described in detail under 'Step 1' in 'Internal hazards' part of Section V–3.1 of this annex why it was decided not to perform quantitative uncertainty analysis in the internal hazards' PSA for NPP Paks. For the very same reasons, uncertainties were characterized only qualitatively in the analysis of these hazards. It is also noted that ADRIA is not only an analysis tool supporting the conduct of the internal hazards PSA besides the RiskSpectrum PSA software, but it is also the accredited cable database and cable routing design tool in the Paks NPP. Consequently, the assessment of internal fire and internal flood takes the most up to date information on cable routing and location of components (often modified due to plant modifications) into account. Therefore, the internal hazards PSA can be considered very detailed and adequate from this respect. However, there are also limitations in the analysis. For instance, mostly simplified rules and assessment techniques were applied to determine the impact area of the numerous fire events modelled in the fire PSA, as opposed to performing detailed fire progression and propagation analyses. Likewise, the fire HRA contains several simplifying assumptions too. As a result, some parts of the internal fire and internal flood PSA can be considered reasonably mature and very detailed in some aspects, but it may also be somewhat biased due to the conservatism imposed by the use of simplifying assumptions in other areas of the analysis. The latter is especially relevant to the fire PSA. Refinements in these areas are ongoing or planned in the near future. In summary, the internal hazards PSA of the Paks NPP is considered as a moderately mature risk assessment in comparison to international best practices, although it is noted that the practices of internal hazards PSA continuously evolve internationally, including fire PSA in particular, in order to reduce uncertainties and biases that are present in most of these assessments. The internal hazards PSA for the Paks plant contains conservatisms to a moderate degree as well.

It is noted that the CDF due to internal flooding in full power operation is relatively high for the Paks plant, since a recent reassessment of fire and flood induced structural failures has revealed that the break of a high energy pipeline can cause damage to a brick wall, and the collapse of that wall can lead to the failure of vital plant components. Preparations for eliminating this plant vulnerability by means of strengthening structural supports to the brick wall are ongoing based on a decision of the plant management made in view of the most recent results of the PSA for internal flooding.

V-3.2.4.3 Earthquake

In 2002, when the assessment was first completed, the seismic PSA for the Paks NPP was considered as a detailed, mature assessment reflecting the state of the art at that time. However, the methodology has not been updated since the original analysis, although the models and results have been modified in accordance with the plant changes made. Therefore, some areas of the seismic PSA are considered limited and, presumably, unnecessarily conservative by now. For instance, the correlation between seismic failures is treaded in a simplified manner by assuming complete correlation among failures of components within predefined component groups, and also the seismic HRA relies on significantly simplifying assumptions too. Consequently, the seismic PSA can still be considered well mature in some aspects, however, there are also analysis areas where conservative and simplified approaches have been applied. As mentioned under 'Step 2A' in 'External hazards – seismic events' part of Section V–3.1 of this annex, the complete set of seismic hazard curves and the full range of fragility distributions for seismic failures were combined at different confidence levels through a convolution integral

to develop true uncertainty distributions for seismic induced failure frequencies. Also, uncertainties in seismic induced failures were combined with uncertainties in human error rates and non hazard related equipment failures using Monte Carlo simulation. The seismic PSA of the Paks NPP is considered as a moderately mature risk assessment in comparison to international best practices. Also, the analysis uses conservatisms to a moderate degree too.

V-3.2.4.4 Meteorological hazards

The PSA for meteorological hazards analysed so far for the Paks NPP can be considered as a mature assessment in comparison to the state of the art methods that are available and in use internationally. It needs to be noted however, that the risk due to tornados as well as extreme high and extreme low air temperatures has not been quantified yet, and the assessment is ongoing at present. The current limitations in the scope of the analyses for external hazards also place some boundaries concerning the scope and usefulness of applying the results of the PSA. In addition, the state of the art approaches for assessing risk from meteorological hazards appear less mature and generally more conservative than the internal events PSA, and these features are relevant to the meteorological hazards' PSA for the Paks NPP too. As to uncertainties, a comprehensive quantitative uncertainty assessment was performed in the PSA for meteorological hazards in a similar fashion to the seismic PSA. In summary, the meteorological hazards PSA of the Paks NPP is considered as a moderately mature risk assessment that contains a moderate amount of conservatism too.

V-3.2.4.5 External events endangering water intake from the river Danube

The risk at full power has been assessed till now, the analysis of accidents in LPSD states is ongoing. Loss of ultimate heat sink due to Danube contamination as a PSA initiating event was the subject of probabilistic hazard assessment in this part of the Paks PSA, as opposed to quantifying only the Danube contamination hazard itself. The frequency of the screened in endangering events was determined by a combined use of statistical data analysis and expert judgment as deemed appropriate according to the types of the events. Reliability data relevant to failures independent of Danube contamination were taken from the internal events PSA without any modification. Although the assessment was intended to be best estimate as much as possible, conservative and simplifying assumptions were also needed to be used during hazard assessment. As far as uncertainty assessment is concerned, uncertainties in the initiating event frequencies and in the probabilities of failure to recover the essential service water system following its failure due to riverine events have not been assessed till now due to limitations in applicable data and resources. So, the uncertainty assessment has some limitations in this respect. In summary, this area of the Paks PSA can be considered as moderately mature with a moderate level of conservatism too.

V–4. CURRENT ACTIVITIES AND FUTURE PLANS

The unit specific PSA models and results are annually updated in the living PSA programme for the Paks NPP. In addition, extensions and refinements are ongoing in the PSA for external hazards. The extension of the PSA scope can significantly impact on the aggregated risk estimates. Efforts are being made to determine the risk from tornados, extreme high and extreme low air temperatures as well as river contamination in LPSD situations. The results of these analyses will be used in the near future for risk aggregation purposes, which will influence on estimates of the total risk presented in this annex. Also, refinements in the PSA model (e.g. input data update, fire assessment upgrade) also affect the aggregated risk results that are annually updated in the living PSA programme.

Besides the developments in the unit specific analyses, a study had been conducted to examine the feasibility of developing a site risk model and quantifying site level risk for the four reactor units of the Paks NPP, based primarily on the use of the existing unit specific PSA models. A small scale analysis was subsequently performed for the loss of off site power initiating event to further research the risk modelling and quantification options outlined in the feasibility study. A full scope Level 1 PSA for the Paks site is now in preparation by making use of the achievements of the preparatory analyses performed so far. The assessment needs to provide an estimation of the aggregated risk from the different radiological sources at the site.

It is noted that the current practice at the Paks NPP is to aggregate risk calculated for all the POSs and hazards in order to justify compliance with nuclear safety criteria. However, the application of quantitative PSA results in support of risk informing decisions in relation to operations, maintenance, plant modifications is typically based on a subset of the hazards analysed in PSA. Examples are as follows:

— Risk informed applications relying on the risk monitor of the plant make use of quantitative risk information related to internal events, while the risk from internal as well as external hazards are considered and evaluated in a qualitative manner;
— Safety enhancement proposals are established on the basis of hazard specific assessments, taking into consideration the risk reduction in comparison to the overall risk figures, and the effectiveness of plant modification is evaluated similarly as well.

CONTRIBUTORS TO DRAFTING AND REVIEW

Alzbutas, R.	Lithuanian Energy Institute, Lithuania
Chekin, A.	International Atomic Energy Agency
Ferrante, F.	Electric Power Research Institute, United States of America
Gilbertson, A.	Nuclear Regulatory Commission, United States of America
Jeon, H.	Korea Hydro & Nuclear Power, Republic of Korea
Lankin, M.	RAOS Project Oy, Russian Federation
Lewis, S.R.	Independent consultant, United States of America
Maioli, A.	Westinghouse E.C., United States of America
Minibaev, R.	International Atomic Energy Agency
Poghosyan, S.	International Atomic Energy Agency
Quiroga, D.	Comisión Nacional de Energía Atómica, Argentina
Siklossy, T.	NUBIKI - Nuclear Safety Research Institute, Hungary
Siu, N.	Nuclear Regulatory Commission, United States of America
Yalaoui, S.	Canadian Nuclear Safety Commission

Consultants Meetings

Vienna, Austria: 10–13 April 2017, 20–23 June 2017, 4–7 September 2018

Technical Meeting

Vienna, Austria: 26–29 March 2018

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group

Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

21-03058E

International Atomic Energy Agency
Vienna