Safety Reports Series

No. 96

Technical Approach to Probabilistic Safety Assessment for Multiple Reactor Units

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 on the IAEA Internet site

http://www-ns.iaea.org/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.

TECHNICAL APPROACH TO PROBABILISTIC SAFETY ASSESSMENT FOR MULTIPLE REACTOR UNITS

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
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
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''.

SAFETY REPORTS SERIES No. 96

TECHNICAL APPROACH TO PROBABILISTIC SAFETY ASSESSMENT FOR MULTIPLE REACTOR UNITS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/books

Printed by the IAEA in Austria
May 2019
STI/PUB/1820

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Technical approach to probabilistic safety assessment for multiple reactor units / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2019. | Series: IAEA safety reports series, ISSN 1020–6450 ; no. 96 | Includes bibliographical references.
Identifiers: IAEAL 19-01237 | ISBN 978–92–0–102618–7 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Risk assessment. | Nuclear reactors — Safety measures. | Industrial safety.
Classification: UDC 621.039.58 | STI/PUB/1820

FOREWORD

Current energy demand and the growing difficulty in establishing new sites for nuclear power plants are powerful incentives for the nuclear industry to utilize existing sites to construct new reactor units. Most nuclear power plants contain two or more reactor units, and all nuclear power plants have other radiological sources, such as spent fuel storage and radioactive waste management facilities.

Probabilistic safety assessments (PSAs) have largely been conducted on a single unit basis, treating each unit as completely independent. Acceptance criteria and risk metrics are also applied to single unit evaluations. The accident at the Fukushima Daiichi nuclear power plant, in 2011, highlighted the possibility of multi-unit incidents and the fact that a combination of external hazards can overcome the engineered defence in depth features, leading to severe plant degradation and the unmitigated release of radioactive material to the environment.

The technical approach described in this publication builds on single unit PSAs to identify considerations for multi-unit PSAs, which also include correlated hazards (e.g. high winds and flooding caused by storm surges) that affect single units but are generally not included in a single unit PSA. The events at Fukushima Daiichi demonstrate that these issues are important when characterizing site risk. The technical approach expands on the multi-unit issues explored in earlier publications and combines new methodologies for hazard and risk integration based on a new set of risk metrics.

The IAEA greatly appreciates the contributions of all those who were involved in the drafting and review of this publication. The IAEA officers responsible for this publication were K. Hibino and O. Coman of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

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

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Current energy demands and the growing difficulty in establishing new sites for nuclear power plants are powerful incentives for the nuclear industry to utilize existing sites to construct new reactor units. Most nuclear power plants contain two or more reactor units, and all nuclear power plants have other radiological sources, such as spent fuel storage and radioactive waste management facilities. The reactors and collocated radiological sources typically share a common electrical grid and ultimate heat sink, and in some cases share structures and systems that provide vital safety functions. Each site can be characterized by a set of internal and external hazards that could initiate a sequence of events which go on to challenge vital safety functions and to cause accidents involving one or more units. Internal initiating events are caused by human error and hardware faults. Internal events include internal fires and floods. Examples of external hazards include natural events, such as seismic events, external flooding from tsunamis, river flooding, storm surges, high winds and wind generated missiles, and events caused by humans, such as industrial and transport accidents.

Nuclear reactor accidents initiated by internal and external hazards have been analysed using both deterministic and probabilistic approaches. The focus of the deterministic analyses has mainly been on the successful mitigation of design basis reactor accidents, and the prevention of core damage and other accident conditions. Probabilistic safety assessments (PSAs) have primarily focused on assessing the risks of events involving severe core damage associated with internal initiating events. The comprehensive treatment of external hazards in PSAs has not yet been harmonized across the international community. For example, the treatment of flooding from tsunamis and rivers flooding has been absent in nearly all existing PSAs. In addition, there has only been limited consideration given to accidents involving multiple correlated hazards (e.g. seismically induced fires and floods) as well as accidents involving non-core radiological sources. These limitations are shared by both deterministic and probabilistic safety analyses.

For multi-unit sites, both deterministic and probabilistic safety evaluations have been performed on each reactor unit individually, with the implicit assumption that the collocated reactors and radiological facilities (or sources) are safe while the reactor unit in question is being analysed. In the rare cases in which non-core radiological sources were subjected to a safety evaluation, these were also performed without reference to the possibility that the associated accident sequences might also involve one or more of the reactor units on the site. Only a limited number of PSAs have been performed that address the potential for

accidents involving two or more reactors or radiological sources concurrently. Very few of these consider accidents involving multiple correlated hazards. There have been only limited deterministic safety analyses of multi-unit events. This reveals the lack of guidance on the integrated safety assessment of a site that includes consideration of the potential for accidents involving multiple reactor units and multiple sources of radioactive material concurrently.

The Great East Japan Earthquake, on 11 March 2011, generated ground motion that affected several multi-unit sites at Tokai Daini, Higashi Dori, Onagawa, Fukushima Daiichi and Fukushima Daini. The operating units at these facilities were successfully shut down by the automatic reactor trip systems upon receipt of signals from seismic motion instrumentation and the 'fail safe' design feature of control rod drives that enables passive insertion from the loss of electric power from the seismic event. At Fukushima Daiichi, however, the large tsunami waves caused by the earthquake inundated the site, resulting in plant flooding and significant damage to the on-site electric power systems. This posed a serious challenge to the safety systems of all six units, overpowering the site's defence in depth and severe accident management capabilities [1].

The consequences of the Fukushima Daiichi accident included severe core damage to the three operating reactor units, a containment breach on at least one of the reactors and a large release of radioactive material — the magnitude of which was only exceeded during the Chernobyl accident. Emergency response teams were severely challenged in efforts to prevent even larger releases, as the accident exposed weaknesses in the existing accident management capabilities to cope with a multi-unit accident with extended station blackout conditions [2–4]. Were it not for some units being down for maintenance and refuelling and one emergency diesel generator (EDG) on the site undamaged, the extent of core damage could have extended to all six units, with the potential for even larger releases than those experienced. Heroic actions by the operators and accident management team were instrumental in limiting the damage and delaying the releases to provide the time to evacuate the public near the site, thereby preventing large radiation exposures of the public. Accounting for all issues associated with a multi-unit site accident in a forward thinking site safety assessment is a challenge and faces many technical issues not addressed in earlier safety assessments.

As evidenced by the Fukushima Daiichi accident, multi-unit accidents involve unique challenges for the structures, systems and components (SSCs) that perform safety functions at each facility, and for the humans and infrastructure foreseen (or needed) to operate the facilities and to implement accident management and off-site protective actions. External hazards and combinations of hazards may lead to initiating events and accident sequences on multiple facilities concurrently [1]. An accident involving core damage or release from one facility and the resulting accident management measures may compromise

the capabilities and resources to protect the other facilities on the site. Hence, the probability of preventing and mitigating an accident at one unit cannot be assessed without considering the status of the other units and on-site facilities, including spent fuel storage facilities. In addition, owing to the non-linear dose response model for early health effects (a dose threshold is needed before early health effects would occur), the health effect consequences from concurrent releases from two or more reactor facilities may exceed the linear sum of the consequences from individual reactor accidents. On account of this and that the frequency of an accident on a multi-unit site directly relates to the number of units on the site, the risk metrics of core damage frequency (CDF) and large early release frequency (LERF)[1], which are only meaningful when reactors are assessed one at a time, are not adequate to express the total risk for a multi-unit site. Additional risk metrics are needed to capture fully the integrated risks from multi-unit sites, or even the integrated risks from the multiple radiological sources on single unit sites.

Multi-unit probability safety assessments (MUPSAs) face many technical issues not addressed in earlier safety assessments. The challenge is compounded by a lack of case studies or methodological guidance for MUPSAs. IAEA guidelines on the performance of probabilistic and deterministic safety analysis include the following publications in the IAEA Safety Standards Series:

— SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [5];
— SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants [6];
— NS-G-2.13, Evaluation of Seismic Safety for Existing Nuclear Installations [7].

However, these safety standards do not address multi-unit considerations. To ensure overall site safety, it is important the safety assessment work meet current guidance and standards for technical adequacy and be validated through peer review. To this end, the development of guidelines on site evaluation and external event safety assessment, with an emphasis on multi-unit sites, was taken up in Work Area 8 of the International Seismic Safety Centre extrabudgetary programme and resulted in the development of this publication and two additional Safety Reports:

[1] LERF is defined as the frequency of those accidents leading to significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close population, such that there is a potential for early health effects. There is a related metric known as large release frequency defined as the frequency of an accident involving one or more deaths.

— Safety Reports Series No. 92, Consideration of External Hazards in Probabilistic Safety Assessment for Single Unit and Multi-unit Nuclear Power Plants [8];
— Safety Reports Series No. 94, Approaches to Safety Evaluation of New and Existing Research Reactor Facilities in Relation to External Events [9].

The accident at the Fukushima Daiichi nuclear power plant underlines the importance of expanding the scope of Work Area 8 to include MUPSAs against a comprehensive set of internal and external hazards, including multiple correlated hazards [1]. This publication expands the current PSA process to take account of multi-unit issues.

With respect to the evaluation of external hazards, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities [10], states:

> "4.36A. For sites with multiple facilities or multiple activities, account shall be taken in the safety assessment of the effects of external events on all facilities and activities, including the possibility of concurrent events affecting different facilities and activities, and of the potential hazards presented by each facility or activity to the others.
>
> "4.36B. For facilities on a site that would share resources (whether human resources or material resources) in accident conditions, the safety assessment shall demonstrate that the required safety functions can be fulfilled at each facility in accident conditions."

This means that the integrated effects of an external event on all facilities and activities on the site need to be considered, including the 'domino' effect of hazards at each facility adversely impacting other facilities.

Although general design criteria that provide the basis for most deterministic safety assessments address the sharing of systems at multi-unit sites (e.g. Criterion 5 in Appendix A to Part 50: General Design Criteria for Nuclear Power Plants of 10 CFR 50, Domestic Licensing of Production and Utilization Facilities [11]), deterministic safety analyses of accidents have been exclusively limited to accidental releases from one reactor or facility. However, in light of the safety lessons from the Fukushima Daiichi accident, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [12], states:

> "**Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant**

"**Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.**

"5.63. To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design."

For existing operating nuclear power plants, the sharing of systems usually provides some additional redundancy for each unit; however, such sharing also introduces an increased potential for a multi-unit accident. This sharing of support systems occurs in older plants, and considering lessons learned from the Fukushima Daiichi accident, a multi-unit site evaluation needs to be carried out in an integrated manner rather than evaluating each reactor or facility separately.

The few safety assessments of multi-unit sites which have been conducted include Seabrook Station, United States of America, in the mid-1980s (see Ref. [13]) and more recently plants with Canada deuterium–uranium (CANDU) reactors (see Refs [14, 15]). There have also been some Level 1 PSAs of multi-unit sites that provide information on the frequency of accidents for two reactors concurrently. Beyond these studies, much of what is known today about the risks of multi-unit sites is based on what has been learned through operating experience (see Refs [16, 17]) and the Fukushima Daiichi accident (see Ref. [1]).

1.2. OBJECTIVE

The objective of this publication is to extract insights and lessons learned from existing literature on, and experience of, multi-unit safety assessments to provide guidance on the approach and methods for site evaluation and safety assessment for multi-unit nuclear power plants when establishing an MUPSA on hazards, and the impact of multiple external events. It identifies the technical issues to be addressed in an integrated site PSA and proposes solutions. In line with the current literature, a PSA based approach is used here. However, PSA based approaches need to be supported by engineering analyses (e.g. thermal hydraulic analysis and accident progression analysis), so some recommendations for future deterministic safety assessments that address multi-unit considerations are also included. The intended audience for this publication includes safety assessment practitioners familiar with single unit PSAs for nuclear power plants against a full range of internal and external hazards.

1.3. SCOPE

This publication assumes a pre-existing capability to perform a PSA evaluation for a single reactor unit against a full range of internal and external hazards. It describes a comprehensive approach to performing an MUPSA and provides guidance on implementation, including the impact of multiple internal and external events (e.g. seismically induced tsunamis, fires and floods). Options to perform the PSA to Levels 1–3 are included. The term 'concurrent releases', as used here and especially in reference to the full scope option for a site safety assessment, does not require the releases to occur simultaneously but rather within a time interval short enough that the same person may be exposed to successive radiological releases from two or more reactor units in a multi-unit accident.

This publication includes a definition of the risk metrics that can be used for an MUPSA and suggestions for the development of associated risk acceptance criteria for a multi-unit site. It identifies areas that are in need of further development, including those supporting deterministic safety analyses. The term 'deterministic' is used here to refer to the use of deterministic evaluation models and criteria as documented in safety analysis reports to support success criteria needed for development of the accident sequences (event trees).

This publication includes the consideration of internal hazards for the following reasons:

(a) They are needed to build external hazard models.
(b) Accidents involving releases from two or more reactor units may be caused by internal events and hazards, depending on the site specific hazards and plant design features.
(c) External hazards may induce internal hazards.

Where available, references are made to supporting guides and standards on how specific hazards are treated. Most of these supporting references are limited to the evaluation of a single reactor or facility. This publication defines the differences between a single reactor unit evaluation and an integrated site safety evaluation without repeating the steps needed for a single unit PSA. Hence, basic elements of a single reactor unit external hazards assessment are not repeated here. Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

1.4. STRUCTURE

Section 2 reviews the lessons learned from service experience and completed site safety assessments, and Section 3 provides a summary of the experience with MUPSAs. The steps to prepare the plant and system models for the MUPSA are described in Section 4. These models include the selection of plant operating states, initiating events, accident sequence model development and supporting technical elements. Information is also provided on the use of models for the internal and external hazards that represent important causes of the accident sequences to be included in the site safety assessment. Sections 5–8 address event sequence analysis for several scopes of an MUPSA, including Level 1 where core damage states are resolved (Section 5), Level 2 where release categories are resolved (Section 6), and Level 3 where radiological consequences are determined (Section 8). To support this full scope, it is necessary to develop an appropriate set of mechanistic source terms (Section 7), evaluate the radiological consequences (Section 8), and perform the steps to integrate the frequency and consequence information into an integrated risk assessment (Section 9). The full scope option for the site safety assessment involves a Level 3 PSA of accidents involving each reactor unit as well as accidents involving concurrent releases from two or more reactor units on the site. The interpretation of results and the documentation of the MUPSA are addressed in Section 10. Annex I presents an MUPSA initiating event model, and Annex II outlines the derivation of the seismic common cause parameter for multi-unit seismically induced loss of coolant accidents.

2. LESSONS LEARNED FROM REACTOR SERVICE EXPERIENCE

2.1. FUKUSHIMA DAIICHI ACCIDENT

The sequence of events during the Fukushima Daiichi accident has been reviewed extensively by the IAEA, the National Diet of Japan, the Institute of Nuclear Power Operations (INPO) and the United States Nuclear Regulatory Commission (NRC) [1–4, 18]. A summary of the sequence of events is shown in Fig. 1. In the following subsections, some key lessons learned for performing an MUPSA are discussed. This review of lessons is performed to identify technical issues that need to be addressed in future site safety evaluations.

Date & time	UNIT 1	UNIT 2	UNIT 3	UNIT 4
11 March 2011	Operated at rated output			Under periodical inspection
14:46	**Earthquake**			
	Scram			
	Loss of external AC electricity			
	Automatic activation of emergency diesel generators			
	Start of core cooling by IC system	Start of core cooling by RCIC system	Start of core cooling by RCIC system	
15:37	**Tsunami (peak of waves)**			
	Loss of all electricity		Station blackout	Loss of all electricity
approx. 18:10	Start of reactor core exposure (analysis)			
approx. 18:50	Start of reactor core damage			
12 March				
05:46	Start of freshwater injection			
11:36			Shutdown of RCIC	
12:35			Start of HPCI	
approx. 14:30	Venting			
15:36	Hydrogen explosion at reactor building	Interference with the recovery operation		
19:04	Start of seawater injection			
13 March				
02:42			Shutdown of HPCI	
approx. 09:10			Start of reactor core exposure	
approx. 09:20			Venting	
09:25			Start of freshwater injection	
approx. 10:40			Start of reactor core damage →	Backward flow of H from Unit 3 via SGTS
13:12			Start of seawater injection	
14 March				
11:01			Hydrogen explosion at reactor building	
		Interference with recovery operation ↓		
13:25		Diagnosis of RCIC shutdown		
approx. 17:00		Start of reactor core exposure		
approx. 19:20		Start of reactor core damage		
19:54		Start of seawater injection		
15 March				
approx. 06:00		Damage to suppression chamber, mass discharge of radioactive material		Hydrogen explosion at reactor building

Note: AC — alternating current; HPCI — high pressure coolant injection; IC — isolation cooling; RCIC — reactor core isolation cooling; SGTS — standby gas treatment system.

FIG. 1. Timeline of key events at Fukushima Daiichi Units 1–4. (Reproduced courtesy of National Diet of Japan [2].)

2.1.1. Flood vulnerability

It is clear from reports on the Fukushima Daiichi accident that the plant design had two weaknesses and that if either of them had been identified and fixed prior to the event, there was a significant likelihood that core damage could have been prevented on each of the damaged units. The first weakness was inadequate protection of the site against a tsunami. The second weakness was the location and lack of flood protection for the on-site emergency power system equipment, including diesel generators and switchgear, in the basement of the turbine building, a flood prone area of the plant. Of these unprotected equipment, the most critical was the AC and DC switchgear. Once it had become flood damaged, there was no means of restoring electricity to the AC powered safety systems, even when alternative sources of electricity were brought onto the site, which occurred rather early in the sequence of events.

It is not known what design considerations were given to protect the plant from internal flooding of the turbine building. The critical cause of the station blackout, given the lack of protection of the plant against the tsunami experienced, was the flooding of the turbine building in which the EDGs and safety related switchgear were located. For plants in Japan, it had not been common practice to perform PSAs on internal flooding, seismic events or tsunamis. However, given what is now known, it would appear that if an internal flooding PSA had been performed on Fukushima Daiichi, the following scenario might have occurred:

(a) The CDF due to severe internal flooding of the turbine building would have likely been not lower than 10^{-3} to 10^{-2} per reactor-year, which is the approximate frequency of severe flooding in a turbine building in typical nuclear power plants subjected to an internal flooding PSA. In fact, there have been several such events in the reactor operating experience (see the event at Oconee Nuclear Station, United States of America, discussed in Section 2.1.6). At Fukushima Daiichi, severe flooding in the turbine building would have likely been classified in a PSA as a core damage event owing to the loss of all AC power from the damaged EDGs and switchgear, especially at Units 1 and 2, where both AC and DC electrical switchgear were susceptible to flooding. As discussed more fully in Section 2.1.6, at the Oconee Nuclear Station, the first plant to perform an internal flooding PSA, the initial CDF due to internal flooding of the turbine building was about 10^{-2} per reactor-year. This led to plant modification to prevent damage to critical safety systems (essential service water pumps, in this case) which reduced the CDF to below 10^{-4} per reactor-year.
(b) Given the high CDF to be expected in an internal flooding PSA, the flood vulnerabilities in the location of the unprotected electrical equipment

would have been more fully appreciated, thereby providing an opportunity to fix the problem by relocating the equipment or installing additional flood protection. Although some diesel generators for Fukushima Daiichi Unit 6 were located at elevations less susceptible to tsunami induced flooding, the AC switchgear at Units 1–4 and the DC switchgear at Units 1 and 2 were susceptible to such flooding.

(c) Had the electrical equipment been protected against flooding before the tsunami hit the plant, the occurrence of a station blackout would have been less likely, and core damage at each protected unit would have been prevented.

In 1991, there was an important precursor event involving flooding at Fukushima Daiichi Unit 1 in 1991 (see the discussion in Section 2.1.6). Even though the leak rate from the seawater system was relatively small, a room became flooded that disabled at least one of the two EDGs. If the correct plant modifications had been made to address the vulnerabilities exposed by this event, such as relocating the diesel generators and switchgear or providing more robust protection from turbine building flooding, core damage during the March 2011 earthquake and tsunami could well have been prevented.

A similar scenario can be postulated for the high energy line breaks inside the turbine building. They have a similar frequency as internal flooding and would have also challenged the performance of the on-site power system. A high energy line break inside the turbine building — such as the one that occurred at Mihama, Japan, in 2004, which killed five plant workers — is a 10^{-3} to 10^{-2} per year event. If one had occurred at Fukushima Daiichi, a total loss of on-site AC and DC power could have occurred. A station blackout due to high energy line breaks in the turbine building would also have had a high CDF and would have provided another opportunity to fix this weak design feature that was a critical cause of the accident.

An important insight from a PSA practitioner's review of the Fukushima Daiichi accident is that a good PSA for internal events, combined with prudent decisions to improve the plants to address vulnerabilities found in the PSAs, could have prevented the accident. A good quality internal flooding PSA or high energy line break PSA would have likely yielded a very high CDF, perhaps greater than 10^{-3} per reactor-year on account of the unfortunate selection of location for important safety grade electric power system components. Such high CDF values are generally regarded as an unacceptable risk, and would have provided an opportunity to modify the plant. INPO reports that the Tokyo Electric Power Company (TEPCO) had estimated a frequency of exceeding the tsunami design basis as high as 10^{-2} per year [3, 4].

2.1.2. Seismic and tsunami vulnerability

As throughout the world, nuclear power plants in Japan are protected against design basis earthquake intensities associated with seismic ground motion. If ground acceleration above a set level is registered, systems will take action to bring the plant to a safe shutdown status. The automatic set point for a reactor scram level was set at 135 cm/s^2 (0.14g). The design basis ground motion for both Fukushima plants had been upgraded since 2006 and is now at horizontal 438–489 cm/s^2 (0.45–0.50g) for Fukushima Daiichi. At this level, it is crucial that the reactors retain their safety functions. In 2008, TEPCO upgraded its estimates of design basis earthquake ground motion for Fukushima to 600 cm/s^2 (0.61g).

The recorded data for both plants, which are located about 180 km from the earthquake's epicentre, were approximately 550 cm/s^2 (0.56g) in the foundation of Fukushima Daiichi Unit 2, and the maximum recorded acceleration for Fukushima Daini was 254 cm/s^2 (0.26g). Fukushima Daiichi Units 2, 3 and 5 exceeded their design basis levels by about 20% in the east–west direction, and measurements were made over 130–150 s. All nuclear plants in Japan are built on rock. Ground acceleration on sediments was around 2000 cm/s^2 a few kilometres north of these sites.

According to INPO [3, 4], TEPCO had information that the frequency of a seismic event that exceeded the seismic design basis was in the range of 10^{-6} to 10^{-4} per reactor-year. TEPCO estimated the frequency of a tsunami that exceeded the design basis height of 6 m was on the order of 10^{-2} per year. Unfortunately, this information may not have been adequately considered and the opportunity to manage the risk may have been lost. If the plants had been subjected to the same requirements of performing an individual plant examination of external events (IPEEE) used at the plants at Diablo Canyon and San Onofre, in California, United States of America, they would have been required to perform a seismic PSA owing to the relatively high level of seismic hazard. It is not unreasonable to assume that had a full seismic PSA been performed (even without considering a concurrent tsunami), plant vulnerabilities, such as the lack of protection of the on-site electric power system from flooding, may have been identified. The pipes in the turbine building carrying in sea water were not safety class and would not have been qualified for seismic protection. Hence, the risk of seismically induced flooding might have been identified in a seismic PSA. There are many non-safety-grade piping systems inside a turbine building that would have a low seismic capacity, so flooding of the turbine building and station blackout would have appeared in such a PSA at a high frequency of occurrence, many orders of magnitude higher than CDF estimates for internal events. The reason for making these observations is to clarify the primary motivation for performing an MUPSA — which is to identify vulnerabilities and thereby actively manage the level of risk.

The design basis tsunami height was set at 5.7 m for Fukushima Daiichi and 5.2 m for Fukushima Daini, and the plants were built 10 m and 13 m above sea level, respectively. Tsunami heights coming ashore were more than 14 m above sea level for both plants, and the Fukushima Daiichi turbine halls were submerged by as much as 5 m of sea water until the tsunami subsided. The maximum amplitude of the tsunami was 23 m near the epicentre (180 km from both plants). Over the past hundred years, there have been as many as eight tsunamis in the region with maximum amplitudes at origin above 10 m (some estimated to be much higher). These resulted from earthquakes of magnitudes 7.7–8.4 approximately once every 12 years. The most recent earthquakes in this category occurred in 1983 and 1993 with magnitudes of 7.7, and yielded maximum tsunami heights at origin of 14.5 m and 31 m, respectively [19]. Although there are large uncertainties in predicting tsunami hazard frequencies at a specific site, the general history of tsunamis in the region is sufficient to suggest that tsunamis larger than those protected against at Fukushima Daiichi were a significant risk.

A major question is why the level of protection for tsunamis at the plant was so limited. Nuclear power plants on the west coast of the United States of America, where the tsunami hazard is less severe than in Japan, have greater protection against tsunamis. San Onofre's sea wall protects the plant against tsunamis 10 m above mean sea level. Based on historical data, a tsunami hazard analysis would have predicted that the frequency of a tsunami that exceeded the design basis for Fukushima Daiichi would be on the order of 10^{-3} to 10^{-2} per year, which corroborates TEPCO's estimate according to INPO [3]. If the consequences of a beyond design basis tsunami had been evaluated, the flood vulnerability of the on-site electric power system could have been identified and then fixed.

Prior to the Fukushima Daiichi accident, the Japanese Earthquake Research Committee had been preparing a report on earthquakes and tsunamis off the Pacific coast north-east of Japan in February 2011 and had been planning to release it a few months later in April. The report includes the Committee's analysis of an earthquake of magnitude 8.3, known to have struck the region 1150 years ago when three sections of the seabed shifted at the same instant, triggering very large tsunamis, which flooded large areas of the Miyagi and Fukushima prefectures. INPO [4] reports the tsunami heights to be 9 m, which is only 1 m under the height needed to inundate the Daiichi site and far above the design basis tsunami level. The earthquake on 11 March 2011 had a magnitude of 9.0 and also involved the shifting of multiple sections of seabed. Tsunami waves devastated wide areas of the Miyagi, Iwate and Fukushima prefectures. Hence, it would appear that a tsunami hazard analysis would have predicted that the frequency of a tsunami as severe as that which occurred at Fukushima Daiichi

was on the order of 10^{-3} per year. Evidence available prior to the Fukushima Daiichi accident strongly suggested that there was a high risk of core damage. Unfortunately, sufficient attention had not been given to assess the risks and to review the risk information available to enhance the level of safety protection against both external and internal hazards.

2.1.3. Role of probabilistic safety assessments in support of accident management

The key issues with regard to the quality of the accident management guidelines in place at Fukushima prior to the accident include the following:

(a) Delay in venting the containment;
(b) Too much trust in the assumed battery capacity;
(c) No previous consideration in emergency planning for a simultaneous loss of AC and DC power;
(d) Poor command and control in responsibilities assigned to control room operators;
(e) Conflicting orders from the Government of Japan and TEPCO top management.

Information in the INPO reports [3, 4] suggests that adverse plant conditions would have made it difficult to manage the accident even if improved accident management guidelines had been in place. However, had a quality PSA been performed for even internal events, the likelihood of a station blackout that exceeded the plant battery capacity would have been better appreciated, and much better accident management guidelines could have been developed. In the United States of America, the commitment to performing quality PSAs at the time when accident management procedures were first being developed provided a stronger set of accident management guidelines. The improvements stem from having a more robust set of scenarios defined in the PSA to evaluate the procedures and to conduct emergency training and drills. Operators could learn more about managing a real accident if they could train in scenarios from a quality PSA.

2.1.4. Conclusions about the role of probabilistic safety assessments in accident prevention

When the accident at Three Mile Island, United States of America, occurred in 1979, a PSA had never been performed on pressurized water reactors (PWRs) designed by Babcock and Wilcox, the vendor for Three Mile Island. Even if one

had been performed, it is unlikely that the risk of the accident would have been identified because it was caused by a human error of commission, which remains a challenge for PSAs today. However, the Fukushima Daiichi accident would have been highly predictable in a PSA. If any of the following elements of a full scope PSA had been performed, the poor protection against external and internal hazards could have been identified, the plant design improved and the accident prevented:

— A technically sound PSA of internal flooding;
— A technically sound PSA of high energy line breaks;
— A technically sound seismic PSA including the probability of a concurrent tsunami;
— A technically sound probabilistic analysis of long term loss of off-site power (LOOP) and station blackout.

In addition, a technically sound PSA of internal events could have enabled the development of improved accident management guidelines, such as how to cope with extended station blackout conditions and improved criteria for containment venting.

The conclusion stated above is supported by the head of the Risk Management Task Force, who prepared Ref. [20] and reports that:[2]

> "The Task Force found that the current regulatory system has served the Commission and the public well and it concluded that a sequence of events like that which occurred at Fukushima is unlikely to occur in the United States. As I discussed at the Task Force briefing to the Commission on July 19, 2011, many people have referred to the events at Fukushima as 'unthinkable' and imply that we should strive to protect U.S. plants from events that are of extremely low probability. However, there is growing evidence that the historical record of tsunamis had not been used properly to determine the design basis at Fukushima Daiichi and, consequently, the protection of the plants was not sufficient. The accident was not of extremely low probability, i.e. it was not 'unthinkable'. This observation suggests that we should be mindful of striking a proper balance between confirming the correctness of the design basis and expanding the design basis of U.S. plants."

[2] www.nrc.gov/reading-rm/doc-collections/commission/cvr/2011/2011-0093vtr-ga.pdf

2.1.5. Fukushima Daiichi accident lessons for probabilistic safety assessment: Moving forward

Having examined how PSAs could have either prevented or provided better preparation for an accident, this section explores future PSAs can be improved based on the lessons learned from the Fukushima Daiichi accident. In general, these lessons apply to all current PSAs worldwide.

2.1.5.1. Need to consider the integrated risk of multiple reactor sites

The Fukushima Daiichi accident clearly shows why it is necessary to perform a PSA on integrated risk for sites with two or more reactors. The adverse interactions that resulted from managing reactor cores in six units during the accident management phase would not have been identified in PSAs performed on one reactor at a time. The Fukushima Daiichi accident involved releases from three badly damaged cores and challenges to the spent fuel integrity of the other units. It is not clear how much of the release, if any, occurred from the spent fuel pools, and there is ample evidence to conclude that the vast majority of the release was from the reactor cores at Units 1–3. According to INPO [3, 4], there was no fuel uncover in any of the spent fuel pools and all of the releases were from the damaged cores at Units 1–3. However, the loss of the spent fuel cooling system and damage to the spent fuel pools meant that accident management resources were consumed to provide backup cooling to the spent fuel. These resources competed for those needed to restore core cooling at Units 1–3 and likely amplified the amount of core damage at these units. The lesson from the Fukushima Daiichi accident is that to assess integrated risk, concurrent accidents involving non-core sources of radioactive material (e.g. spent fuel storage) need to be considered. There is clearly no way to identify these issues by performing safety analyses, either deterministic or probabilistic, one reactor or facility at a time. This is probably the most profound lesson from the accident and one of the most difficult to address.

2.1.5.2. Need to address accidents involving multiple hazards

Current PSA guides and standards tend to assume that each hazard (e.g. seismic, fire, flood and internal events) can be evaluated separately in distinct PSA models. This view is strengthened by the way in which the probabilistic risk assessment (PRA) standard [21] of the American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS) is organized in parts with separate requirements for each hazard group. Many users interpret Part 2 of this standard [21] as only being applicable to internal events.

This segregated view of a PSA needs to be revised to consider a more integrated treatment of hazards with due regard to interactions in which different hazards are combined in a single event. The Fukushima Daiichi accident involved a tsunami triggered by a seismic event that led to flooding of the turbine building and a consequential (i.e. causal) station blackout, which could not have been recovered with an external power supply, as is often assumed in station blackout evaluations [1]. Some of the lessons learned from this observation include the following:

(a) More emphasis needs to be placed on identifying the potential for interactions that involve multiple hazards in the enumeration of event sequences in the PSA model and in the quantification of their frequencies. Examples include:
   — Current seismic events and tsunamis for coastal sites;
   — Tsunami induced site inundation and flooding;
   — Seismically induced internal fires and floods;
   — Seismically induced failure of tsunami walls.

(b) Consideration needs to be given to damage to flood and fire barriers caused by severe earthquakes and tsunamis. The procedures for fragility analysis may need to be improved to consider concurrent loads from two or more hazards.

(c) It needs to be emphasized that standards and requirements for PSAs of internal events are also for preparing the PSA model for all events and hazards. It is necessary to add the requirements in Part 2 of Ref. [21] to evaluate the potential for compound hazards and also to add requirements to the hazard specific parts of Ref. [21] to evaluate the potential for one hazard to propagate another.

(d) The evidence for Fukushima Daiichi Units 1 and 2 shows that sequences involving the loss of both AC and DC power need to be considered as dependent events — not independent events. Moreover, accident management for station blackout needs to consider that simply bringing in external power supplies may be insufficient if the critical switchgear is damaged. Hence, PSA models for the loss of electric power need to consider the concurrent loss of AC and DC power, especially at multi-unit sites where parts of the AC and DC systems are shared.

2.1.5.3. Need to consider the impact of multi-unit accident complications and site contamination on human reliability and accident management

Many current PSAs take credit for known and proceduralized operator recovery and accident management actions that could be implemented to recover

the plant from a degraded state or core damage condition. However, as seen at Fukushima Daiichi, once the site becomes contaminated with radioactive material, the capability to implement recovery operations is greatly inhibited. Human reliability analysis does not address this explicitly and this needs to be corrected. A related issue is that the existing PSAs do not address the impact of an event sequence on spent fuel cooling capabilities. Many events modelled in PSAs of internal events, such as loss of service water and loss of electric power, would challenge the capability to maintain spent fuel cooling. This places demands on the emergency operating crews and requires time and personnel that are then not available to support emergency procedures and accident management at the reactor cores. These types of dependency are not modelled very well in existing PSAs, if at all. A related issue is how to treat accident management when the state of the plant and its critical safety parameters are unclear.

2.1.5.4. Clarification on when to apply the 24 hour mission time

It is common practice in PSAs to use a 24 hour mission time to cut-off the consideration of safety system failures over time following an initiating event. The Fukushima Daiichi accident underscores the limitations of cutting off the development of an accident in a PSA model prematurely. The concept behind the 24 hour mission time, as envisioned in its creation in NUREG/CR-2300, PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants [22], is only used when all of the following criteria have been met:

(a) An initiating event has occurred that will enable the plant to restart when the cause of the initiating event has been corrected. This applies to high frequency transients but not to loss of coolant accidents (LOCAs) in which emergency core cooling systems and containment heat removal and spray systems may have to operate for months.
(b) The key plant systems that are supposed to operate following the initiating event successfully perform their safety functions.
(c) All critical safety functions are successfully fulfilled, including systems for reactivity control, core heat removal, reactor coolant system heat removal, coolant inventory control and containment functions.
(d) The items above are achieved for a period of 24 hours, during which plant conditions are stable and do not deteriorate.

A difficult situation is the LOOP leading to a station blackout, which is currently modelled in most PSAs to a mission time for the on-site power system and off-site power recovery of 24 hours. If the on-site power system successfully

operates for 24 hours or until off-site power is recovered, the analysis of core damage probability is normally terminated. This use of the 24 hour mission time needs to be revised and does not need to be applied to any situation in which the LOOP and grid connection continues for more than 24 hours. There have been several instances in the United States of America where the plant lost off-site power for more than 24 hours. One example involved a major regional blackout on 14 August 2003 in the north-east of the United States of America; and another involved a hurricane in Florida when a plant depended on on-site EDGs for almost a week. When the loss of the grid is due to a severe earthquake or tsunami, the mission time for the EDGs certainly needs to be sufficiently long to guarantee off-site power recovery or application of off-site power supplies. Of course, if the on-site switchgear has been damaged, as was the case at Fukushima Daiichi, the recovery of off-site power may not be sufficient to neutralize the accident.

It is necessary to make the distinction between the accident sequence scrutation time (i.e. the time to examine the progression of the accident) and the mission time of the mitigation and support systems. The mission time of the systems should not be confused with a truncation time for the accident sequences. In fact, if for simplification and Boolean reduction reasons a common mission time can be considered for most of the systems (with the implicit assumption that for these systems, the functional redundancies and the longer delays will allow recoveries and repairs in the long term), the accident scrutation time has to be long enough to cover the occurrence of inevitable events in the long term, for example the depletion of the feedwater tank, the switching in recirculation mode of the safety injection and the depletion of diesel fuel reserves.

Even if a common time can be defined for the majority of the accident sequences, it is necessary to take into account events that would occur later or failure modes specific to equipment that is not used in the short term.

2.1.5.5. Limitations of core damage frequency and large early release frequency risk metrics

The use of CDF and LERF risk metrics is only appropriate for accident sequences involving one reactor. They fail to capture the risk of accidents involving two or more reactors or non-reactor sources of radioactive material. A more general set of risk metrics that would apply to all types of accident, such as at Fukushima Daiichi, are those associated with a Level 3 PSA in which the risk of consequences to public health and safety are fully quantified for accident sequences involving any combination of reactor units and radionuclide sources. This issue of risk metrics is explored more fully in Sections 3 and 4.

2.1.5.6. Questionable screening criteria for external hazards in probabilistic safety assessments

A problem identified in earlier PSAs is the attempt to perform risk informed applications with limited scope PSAs. A stronger commitment to performing quality PSAs for a full set of hazards could have prevented the Fukushima Daiichi accident. Questions were raised in Section 2.1.4 about the justification for not protecting the plant against internal and external hazards. This may be due, in part, to an optimistic screening of external hazards in developing the 'deterministic' design basis. It appears that the frequencies of events that would exceed the design basis protection against tsunamis, earthquakes and floods are much more likely than assumed in the design and licensing of the reactor.

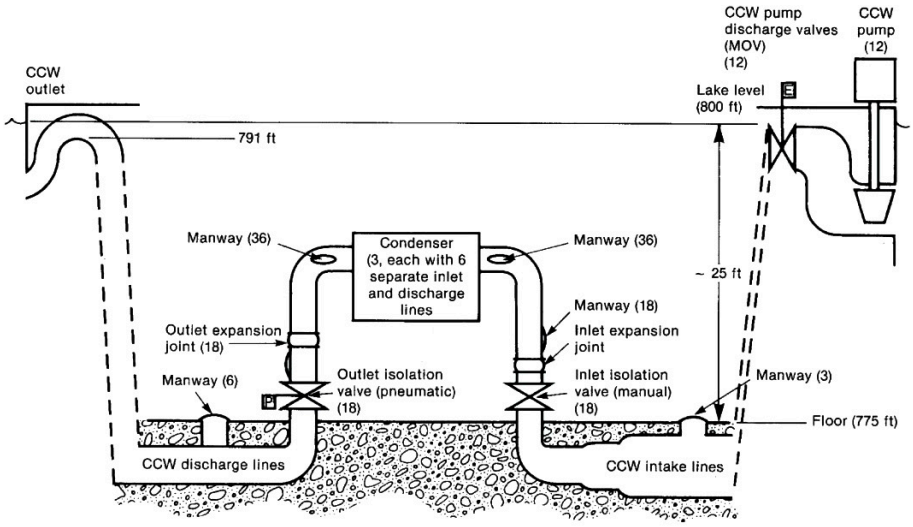
2.1.5.7. Nuclear Regulatory Commission perspectives

At a 2013 conference in Tokyo, Japan, the NRC presented lessons from the Fukushima Daiichi accident and how they help "in identifying where and how we might improve PSA technology and, thereby, future PSAs" [23]. The insights largely reinforce the points raised earlier in this section. The NRC also highlights the need to consider additional feedback loops, such as how delays in evacuation modelled in the Level 3 PSA may interact with accident management (the issue of when to vent the containment), and how screening criteria used in PSAs need to be strengthened to ensure that risk significant events are not overlooked. The investigation was performed to support a Level 3 PSA project on addressing multi-unit risk assessment.

2.1.6. Precursor events at Fukushima Daiichi and Oconee Units 1–3

It is interesting that an INPO report [4] raised the issue of how TEPCO had not considered international operating experience to gain insights into flood vulnerabilities at Fukushima. INPO [4] identified an event in at Le Blayais Nuclear Power Plant, France, it felt provided important lessons that, if heeded, could have led to Fukushima Daiichi plant improvements to address the flood vulnerabilities that were exposed by the accident. It would appear that Fukushima's own service experience provided an opportunity to improve the plant's protection against flooding. However, any improvements that might have been made would have been inadequate to prevent loss of AC and DC power from the tsunami induced flooding.

A more interesting precursor to the Fukushima Daiichi accident is the case at the Oconee Nuclear Station, United States of America, which also experienced a significant flood event in 1976. Oconee followed up with plant improvements



Note: CCW — condenser circulating water; MOV — motor operated valve.

FIG. 2. Oconee turbine building configuration. (Reproduced courtesy of Electric Power Research Institute [24].)

in two stages (see Fig. 2). In the first stage, modifications were ordered by the NRC to improve the plant's protection against internal flooding. The second stage of improvements was a detailed internal flooding PSA — the first time a nuclear power plant in the United States of America had been subjected to one. This is an interesting case study for several reasons:

(a) The precursor event at Oconee was a near miss accident that could have involved core damage at three reactor units that shared a common turbine building where the internal flooding occurred [22]. This is classified as a near miss because the operators were unaware of the flooding until it was too late to prevent critical failures of service water pumps. The critical failures were prevented by luck, namely, the independent recovery of an inverter failure that terminated the flooding (see Fig. 2).

(b) The plant made modifications after the flooding, but it was later determined in the internal flooding PSA that those modifications were insufficient to reduce a high risk of core damage from flooding.

(c) The 1983 Oconee PSA was the first internal flooding PSA in the United States of America. Since then, internal flooding has been included in all PSAs for nuclear power plants in the United States of America. Initially, the CDF from internal flooding was found to be greater than 10^{-3} per reactor-year even after the modifications implemented following operating experience to flooding events. The internal flooding PSA led to additional plant modifications to provide better protection against floods and, as a result, the CDF from internal flooding was reduced to below 10^{-4} per reactor-year.

(d) Had TEPCO and the Nuclear and Industrial Safety Agency considered the flooding at Oconee, which proves that very large floods can occur in the turbine building of any plant, they would have been able to determine that the risk of a severe accident caused by flooding from any cause was unacceptably high.

(e) From 1989, individual plant examinations in the United States of America have been required to identify plant vulnerabilities associated with internal events and internal flooding. Japan also had an individual plant examination programme; but since it appears that floods were not considered in these examinations, the opportunity to identify flood vulnerabilities was not afforded. PSAs in Japan were limited to the treatment of internal events and only recently has a priority been placed on expanding the PSAs to consider a full range of external hazards.

A comparison of the respective treatments of flooding by the operators of Oconee and Fukushima Daiichi is presented in Table 1.

A comparison of flood experiences at Oconee and Fukushima are striking. Both experienced a ‘wake-up call’ that the plants had significant flood vulnerabilities. The Oconee plant was very fortunate to avoid possible core damage of three reactor units; at Fukushima Daiichi, however, three units suffered core damage. At both plants, the steps taken immediately after the initial floods were not sufficient to manage the risks of a flood induced accident. The risk management at Oconee was successful, however, only after a good quality internal flooding PSA was performed several years after the flooding and the first set of modifications. These examples also indicate the primary reason for performing a PSA. It is not to prove that the plant is safe but instead to identify vulnerabilities and to address them to reduce the likelihood of an accident. The costs of performing a PSA cannot be justified unless it is the first step in an effective risk management programme.

TABLE 1. COMPARISON OF INTERNAL FLOODING PRECURSORS AND RISK MANAGEMENT AT OCONEE AND FUKUSHIMA

Evolution of flood evaluation	Oconee	Fukushima Daiichi
Date of flood	October 1976	October 1991
Flood event description	Inverter failure caused air operated valves in the circulating water system to open while the condenser water box was open for cleaning. The turbine building shared by all three reactor units flooded via gravity feed from the lake. The flooding was terminated when inverter failure was recovered prior to operators becoming aware of the flood. Several million litres of water flooded into the building. Safety grade service water pumps in all three units almost flooded which would have resulted in core damage of all three units.	A seawater (circulating water) pipe failed leading to a leak with an estimated leak flow rate of 20 m^3/h into the diesel generator room via a door and penetration for cables, which resulted in a submerged diesel generator.
Design changes in response to flood	A new safe shutdown system was installed and a means of draining the turbine building from a flood was installed.	It is believed that TEPCO took steps to prevent water leakage from basement initiated floods into the diesel generator but it is unknown exactly what was done. It is clear that any design changes were insufficient to protect against flooding starting from outside.
Date of internal flooding PSA	The first internal flooding PSA performed in the United States of America in 1983.	It is not known whether any internal flooding PSA was ever performed. This is doubtful because a large turbine building flood would have likely led to an assessed core damage state due to flooding. Internal flooding PSAs are generally not performed in Japan but are planned for the future.

TABLE 1. COMPARISON OF INTERNAL FLOODING PRECURSORS AND RISK MANAGEMENT AT OCONEE AND FUKUSHIMA (cont.)

Evolution of flood evaluation	Oconee	Fukushima Daiichi
Results of internal flooding PSA	The frequency of a flood causing core damage of all three units was found to be between 10^{-3} and 10^{-2} per reactor-year.	Based on what is now known about the plant design features, it is believed that an internal flooding PSA would have yielded results similar to those at Oconee.
Design changes in response to PSA	Flood protection was added to safety grade service water pumps and flood proof doors were installed to minimize propagation of turbine floods into auxiliary buildings. As a result of design changes, the core damage frequency from internal flooding reduced to below 10^{-5} per reactor-year.	This was a lost opportunity because it appears no flood PSA was ever performed.
Susceptibility to flooding	No known susceptibility.	Susceptibility confirmed by accident.

Note: PSA — probabilistic safety assessment; TEPCO — Tokyo Electric Power Company.

2.2. SEISMIC EVENT AT THE KASHIWAZAKI-KARIWA NUCLEAR POWER PLANT

In a report to the Government of Japan, an IAEA expert mission finds [25]:

"Kashiwazaki-Kariwa nuclear power plant is the biggest nuclear power plant site in the world. It is operated by Tokyo Electric Power Company (TEPCO). The site has seven units with a total of 7965 MW net installed capacity. Five reactors are of BWR type with a net installed capacity of 1067 MW each. Two reactors are of ABWR [advanced boiling water reactor] type with 1315 MW net installed capacity each. The five BWR units entered commercial operation between 1985 and 1994 and the two ABWRs in 1996 and 1997 respectively.

"At the time of the earthquake, four reactors were in operation: Units 2, 3 and 4 (BWRs) and Unit 7 (ABWR). Unit 2 was in start-up condition but was not connected to the grid. The other three reactors were in shutdown conditions for planned outages: Units 1 and 5 (BWRs) and Unit 6 (ABWR).

"A strong earthquake with a moment magnitude of 6.6 (M_{JMA} = 6.8 according to the Japanese Meteorological Agency) occurred at 10:13 h local time on 16 July 2007 with its epicentre about 16 km north of the site of the Kashiwazaki-Kariwa NPP and its hypocentre below the seabed of the Jo-chuetsu area in Niigata prefecture (37°33′ N, 138°37′ E).

"The earthquake caused automatic shutdown of the operating reactors, a fire in the in-house electrical transformer of Unit 3, release of a very limited amount of radioactive material to the sea and the air and damage to non-nuclear structures, systems and components of the plant...."

Although this earthquake caused some damage to non-safety-related SSCs, the design basis earthquake levels were significantly exceeded. Yet, there was no discernible damage to any safety related SSCs, and the fundamental safety functions of reactivity control, core heat removal and confinement of radioactive material were maintained. The lessons learned from this event have been factored into changes to defining the design basis for seismic events worldwide and have been incorporated into the appropriate IAEA safety standards, including IAEA Safety Standards Series No. SSG-9, Seismic Hazards in Site Evaluation for Nuclear Installations [26]. However, since this event did in fact lead to automatic shutdown of the five operating reactors and to some damage of multiple units, it can be classified as an external, multi-unit common cause initiating event (CCIE).

2.3. EXTERNAL FLOODING OF LE BLAYAIS NUCLEAR POWER PLANT

Vial et al. [27] report that:

"On 27 December 1999, a severe storm occurred in the vicinity of the 'Le Blayais' Nuclear Power Plant located on the banks of the Gironde estuary. The severe storm-driven waves coincident, with high water levels in the Gironde estuary exceeded the worst-case scenario considered at the design of the site protection against flooding, resulting in the scram of three out of four units and severe nuclear island flooding. Many underground rooms sheltering safety-related equipment...were flooded, causing the unavailability of all trains of low pressure safety injection and [containment] spray for two of the units. Moreover, the storm conditions also led to partial temporary loss of external power supplies (loss of the auxiliary 225 kV power supplies over the four units, loss of the main grid 400 kV at two units).

.....

"Le Blayais flooding in December 1999 has led Electricité de France and the regulatory authority to re-examine the flood protection of nuclear sites, as detailed in another dedicated paper."

Vial and Rebour [28] identify the following lessons learned from this event and the actions taken to enhance flood protection at nuclear power plants:

"The 'Le Blayais' site flooding has pointed out the possible occurrence of modes of degradation of the safety level affecting simultaneously all the units at a site and has revealed some weaknesses in the site protection against external flooding related to:

- the extreme meteorological conditions considered in the design of the site protection. For the 'Le Blayais' site, high storm-driven waves coincident with high water level in the Gironde estuary had not been initially considered.
- the warning system and its criteria, allowing the anticipation of severe weather (verification of the protection devices, implementation of movable equipment…) and the shutdown of the plants in a timely schedule.
- the site accessibility (blocked roadways), highlighting both the need for additional staff of operating and emergency response personnel prior to the arrival of the severe flooding conditions and the need for an adequate autarchy of the site (water quality and fuel supply…).
- the flooding-related procedures and the on-site emergency organization, considering all the diverse aspects linked to the flooding conditions including:
    - — the accessibility of the equipment located outside of the protected buildings.
    - — the simultaneous impact on several plants, with a potential risk of losing both the external power supplies and the ultimate heat sink.
    - — the isolation of the site and the difficulties to provide rescue staff and equipment.
- the detection of water in the flooded rooms, allowing a quick response of the operating staff for implementing the necessary action, like the implementation of movable pumping devices,
- the faults in electrical isolation, likely to lead to some electrical busbars loss whereas the external grid may be lost due to the severe weather conditions,
- the management of release of the water collected in the flooded facilities."

A key lesson from this event is that the occurrence of external flooding that exceeds the site protection capabilities is not an exceedingly rare event and such events would inherently challenge all of the reactor units and on-site facilities.

2.4. LOSS OF OFF-SITE POWER EXPERIENCE

Service experience with LOOP provides additional insights into the motivations for a site safety evaluation and the challenges it brings. The reason to focus on LOOP is based on the following:

(a) Station blackout initiated by LOOP has often been found to be a risk significant and sometimes risk dominant initiating event in nuclear power plant PSAs. This is important because station blackout renders all AC power driven safety systems unable to perform their safety functions.
(b) LOOP often occurs in a manner that it affects all of the reactors and facilities on the site and hence it can be considered in the MUPSA.
(c) LOOP is a potential consequence of many external hazards such as severe weather, seismic events, external flooding, high winds and transport accidents. It is common practice to assume LOOP in a seismic PSA. LOOP can also result from internal events.

To support an MUPSA, the analysis of LOOP initiating events needs to distinguish between events that challenge individual reactor units independently versus those that impact two or more units on the site concurrently. An example analysis of LOOP initiating event frequencies that addresses this issue is provided in Section 5.2.

2.5. SURVEY OF OPERATIONAL EVENTS IN THE UNITED STATES OF AMERICA

The flood events at Oconee and Fukushima nuclear power plants and the LOOP events occurred in plant operating experience which involved challenges to SSCs in multiple reactor units and facilities on a site. Many other site centred events have occurred that have involved multiple reactor units. Schroer [16] reviews reactor operating experience and identifies many examples at nuclear power plants of events that have the potential for impacting multiple units on the site (see also Ref. [17]). Schroer [16] concludes that all of the nuclear power plant events could be classified into seven categories, one for independent events

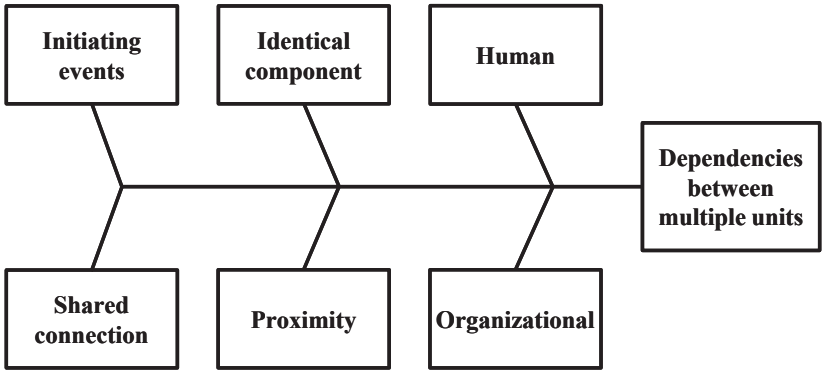


FIG. 3. Multi-unit dependency classification system [16, 17].

localized to a single unit and six for various types of multi-unit dependency (see Fig. 3). Schroer [16] reports:

> "To confirm that the created classification includes all potential events that may link multiple units, all LERs [licensee event reports] that were submitted to the NRC from 2000 through 2011 were evaluated. LERs are submitted to the NRC after plant abnormalities in accordance with guidelines prescribed in 10 CFR 50.73. These LERs discuss the apparent root causes of the events and actions that will be taken by the licensee. It should be noted that LERs include both existing conditions (i.e., latent conditions) that have been found, that is conditions that were discovered before becoming events, and events that have occurred at the plant, that is conditions that were not caught before causing an event. Three-hundred-ninety-one of 4207 total LERs affected multiple units on a site, which amounts to 9% of all LERs submitted between 2000 and 2011. This represents a significant number of multi-unit issues that happen every year; however, 91% of the events belonged to the seventh event classification, independent events."

A breakdown of the multi-unit events into the six categories of Fig. 3 is shown in Fig. 4. The organizational and shared component categories were found to be the most predominant and combine to account for 75% of the observed multi-unit events. The identical component category is common cause failures (CCFs) in identical components across multiple units. CCFs have only been analysed in the context of a single reactor PSA model. Schroer [16] presents strong evidence that dependent failures occur with a relatively high frequency involving multiple units.

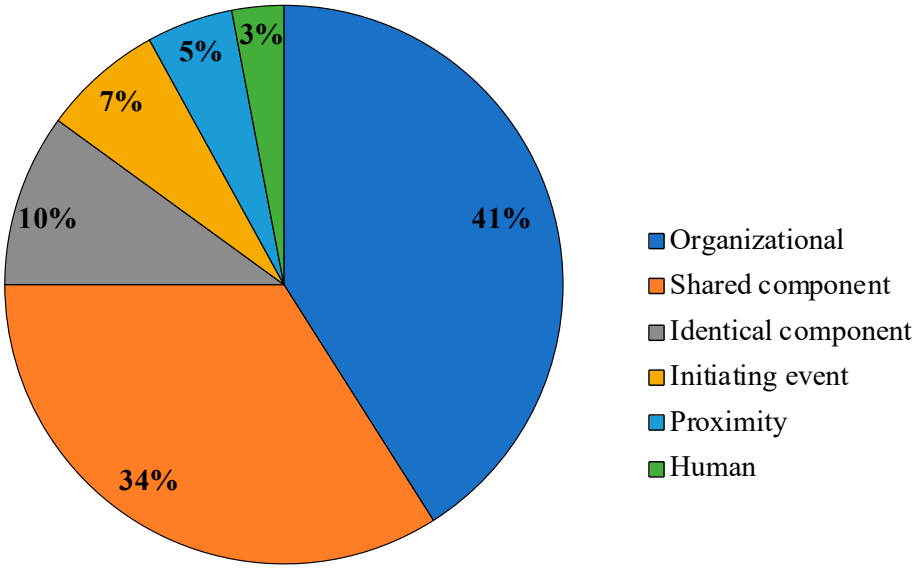


FIG. 4. Breakdown of multi-unit events by dependency classification [16, 17].

An internal fire is another hazard which poses a challenge to sites with multiple reactor units. The infamous Browns Ferry fire in 1975 occurred during construction of Unit 2 while Unit 1 was operating (there are now three units). A candle was used to check for any air leaks which could expose the cable spreading room (situated below the control room) to radioactive material. The flame ignited some cables and the ensuing fire presented a great challenge to the plant operators to extinguish it and to prevent a core damage accident. This is an example of the domino effect of one unit on another (see Ref. [29] for a review of nuclear power plant fires with complex multi-unit interactions). These examples further support the practice of performing MUPSAs.

2.6. INTERNATIONAL REPORTING SYSTEM FOR OPERATING EXPERIENCE

The IAEA and the OECD Nuclear Energy Agency (OECD/NEA) jointly operate the International Reporting System for Operating Experience (IRS) for nuclear power plant incidents (see Ref. [30]). In 2014, the OECD/NEA Committee on Nuclear Regulatory Activities published a report on Fukushima Daiichi nuclear power plant precursor events [31], and in 2007 the Swedish Nuclear Power Inspectorate (SKI) published results of a study of CCIEs using the IRS [32].

3. EXPERIENCE WITH MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENTS

This section summarizes lessons learned from completed PSAs and ongoing PSAs that help to define the technical issues to be addressed in multi-unit and site safety assessments. These include a multi-unit Level 3 PSA completed for Seabrook Station, insights from single unit Level 1 PSAs on a plant with extensive shared structures and systems, PSAs for modular high temperature gas cooled reactors (MHTGRs), and recent MUPSA work that has been completed for multi-unit CANDU reactor plants with shared systems and containment buildings.

3.1. SEABROOK STATION LEVEL 3 PROBABILISTIC SAFETY ASSESSMENT[3]

The earliest example of a safety assessment that addressed the integrated risks of a multi-unit site is that of the original Level 3 PSA carried out on Seabrook Station, comprising two Westinghouse PWR units with large dry containments, and was published in 1983 [13, 33]. Much of what is known today about how to conduct a site safety assessment is based on this work. There is no evidence that any multi-unit Level 3 site safety analyses have been performed since 1983. However, the NRC is performing a Level 3 PSA on a multi-unit site in the United States of America which is expected to consider multi-unit effects [34]. Even though the Seabrook study is rather old, its lessons are still relevant today.

The project called for a state of the art, full scope Level 3 PSA of internal and external hazards, and included accidents initiated from full power, internal and external hazards, such as fires, floods and seismic events, and a site specific model of the emergency plan protective actions. The PSA was subsequently used to address emergency planning issues that had delayed the licensing of that plant. Unique about this PSA was the inclusion of an integrated risk assessment from the operation of both units, including a consideration of multi-unit accidents.

The Seabrook Level 3 PSA began with an assessment of Unit 1, which was the first to be operated. It was done in the usual way by focusing solely on Unit 1 and ignoring Unit 2, which was identical but with a later construction schedule. Hence, the Unit 1 model could be used for Unit 2. All that remained was to complete an integrated risk assessment for the two unit station. As the study did not include an evaluation of the spent fuel pool or other non-reactor sources of

[3] This section is based on Ref. [13] with the permission of the ABS group.

radioactive material (e.g. radioactive waste systems and neutron sources), it was not a complete site risk assessment.

3.1.1. Risk metrics

The first step was to select the appropriate risk metrics. Those selected for the single unit PSA model were CDF, complementary cumulative distribution function (CCDF) curves developed in the Level 3 PSA and the metrics used for the NRC quantitative health objectives (QHOs) based on the risks to individuals living in the vicinity. It is also possible to obtain these results from an LERF. In 1983, however, there were no available risk acceptance criteria for this metric, so it was not emphasized in the results presentation. As is common in PSAs today, single unit accident frequencies and CDFs were based on units of events per reactor-year but this frequency basis had to be modified for the integrated two unit station. Hence, an event frequency per two unit station was adopted for both CDF and CCDF curves. The two unit CDF has contributions from single unit accidents on Units 1 and 2 and accidents involving core damage to both units. Once this frequency basis was selected, it was possible to 'add up' the risk contributions from different components of the risk profile. However, before the risk contributions can be added up, it is necessary to address various dependencies of the type that were defined by Schroer [16].

3.1.2. Integrated risk results

Fleming [33] reports that since the original PSA for Seabrook, there have been a number of updates to support individual plant examinations (including those of external events), and other updates to support ongoing risk informed applications. The CDF results from these recent updates are substantially lower than those developed in Ref. [13], reflecting the results of risk management actions, design changes to improve safety, PSA model improvements, and updates to incorporate more recent generic and plant specific data on equipment failure rates and initiating event frequencies. Since the second unit at Seabrook was cancelled prior to completion of construction, these updates did not include updates to the integrated risk of the two unit station. However, the results of the original PSA offer insights into the relative importance of single unit and multi-unit accidents.

Even though many of the initiating events only challenge a single reactor unit, Fleming [33] reports:

> "There are a variety of initiating events such as certain loss of offsite power events, loss of service water events, and seismic events that lead

to concurrent event sequences on two or more reactor units on a site. The question of multiple concurrent reactor accidents is not one of possibility but rather one of probability. The probability [of a multi-unit accident] is significantly influenced by the use of shared and dependent systems, if this is a factor, as well as common cause failures in redundant systems [at] the multi-unit sites."

The Seabrook PSA results showed that multi-unit accident sequences significantly contributed to site risk even though the sharing of equipment was limited to the sharing of a common electrical grid and ultimate heat sink, conditions common to all nuclear plants with multiple reactor units. Fleming [33] reports:

"Unlike some existing multi-unit sites which have a more integrated and interdependent design of the plant support systems, the multi-unit plant originally designed for Seabrook included two essentially independent reactor units. While each unit had [a dedicated system] of emergency diesel-generators and service water pumps, there was some small degree of shared equipment in the service water and circulating water intake structures and in electrical switchyard."

The major types of dependency that were addressed in the Seabrook two unit station PSA include the following [33]:

- The limited common systems and hardware between the reactor units (e.g. the off-site electric power system and elements of the switchyard);
- Intake structures that supply sea water to cool the service water and circulating water systems shared by both units;
- Some limited capability to cross-tie equipment from one unit to backup failures on the other unit;
- Initiating events reflecting the overlap of the construction schedules for the two units;
- The physical proximity of the two units, separated by some 150 m, to most of the external hazards considered in the PSA (e.g. seismic events and external flooding);
- The potential for CCFs of identical systems or components at different units due to causes other than external hazards (e.g. design errors, environmental stresses or maintenance errors repeated at both units).

The concept of an integrated risk profile for a plant with two reactor units is provided in Fig. 5. This is a site complementary cumulative distribution

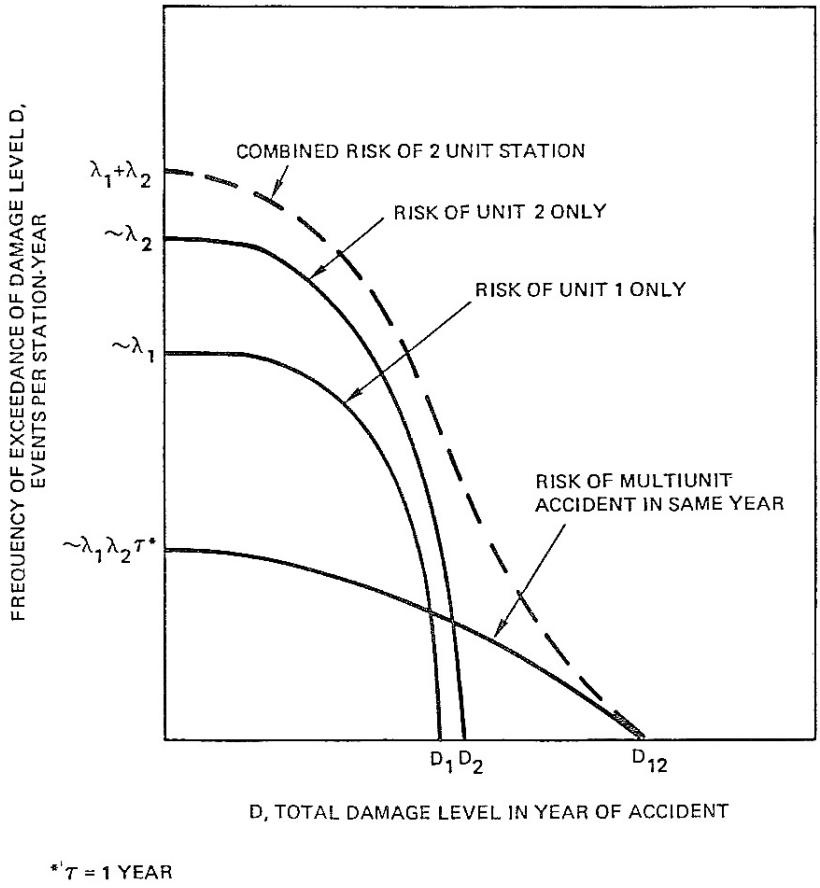


FIG. 5. Concept of two unit integrated risk. (Reproduced courtesy of ABS Group [13].)

function (SCCDF) curve[4] and can be contrasted with a CCDF curve for a single reactor unit that is commonly used in single unit PSAs. The NRC Reactor Safety Study [35] used such CCDF curves to express the results of a single unit PSA, but Fig. 5 expresses the integrated risks for a two unit site. In this figure, each curve represents the sum of the release categories either for a single reactor release or for a multi-unit accident. Fleming [33] reports:

> "Each curve is in turn the sum of a set of curves for different accident sequences grouped into release categories. To produce these curves

[4] Each point on the SCCDF curve represents the frequency (y axis) of an accident whose consequences are at a given damage level or greater (x axis).

uncertainties in the estimation of event sequence frequencies, source terms, and [off-site radiological] consequences are taken into account. Single curves represent mean frequency values."

Figure 5 shows the general case in which each unit has a different risk profile. In the case of Seabrook, however, the individual reactor units were identical. The combined risk of a plant with two reactor units is obtained by adding the contributions from three curves, one for single reactor accidents associated with each of the units and one for the contributions from multi-unit accidents [33]. Each curve in this figure can be further decomposed to show the risk contributions of different initiating events, hazards, accident sequences and accident sequence families, as is done in a single unit PSA.

In comparing the combined risks from both units to that of each unit, two key differences are noted. There is an increased frequency of accident consequences in the high frequency–low consequence end of the accident spectrum due to the increased likelihood of single unit accidents from two reactors. There is also an increased consequence at the low frequency–high consequence end of the accident spectrum due to the contributions from accidents on both units concurrently. These increases are not linear because of dependencies on the frequency side and because the consequences from a dual unit accident may be amplified due to the dose thresholds associated with radiation sickness.

The integrated PSA of the two unit station started by completing a single unit PSA on Unit 1 and then using this information to construct the PSA for Unit 2 and a modelling of accidents that could influence both units concurrently. The PSA for Unit 2 was a rather simple task because both units were designed as identical units. The key challenge was to identify and model accident sequences involving both units, not only from the aspect of defining multi-unit core damage, but also the resulting containment response, mechanistic source terms and off-site radiological consequences.

To define the multi-unit accidents, it it necessary to review the list of initiating events to identify those that would have the potential to impact both units concurrently as well as those that challenge the units independently [33]:

"The list of initiating events from the single unit PRA was divided into three categories: those that would definitely impact both units; those that would impact both units under certain conditions; and those that would be expected to occur independently: The results of this evaluation are shown in Table [2]."

TABLE 2. ANALYSIS OF INITIATING EVENTS FOR INTEGRATED SEABROOK RISK MODEL [13, 33]

Event category	Initiating event
Events impacting both units concurrently	Loss of off-site power Seismic events Tornado and wind External flooding Truck crash into switchyard
Events impacting both units concurrently under certain conditions	Loss of condenser vacuum Loss of service water Turbine missile
Events impacting each unit independently	Loss of coolant accident General transients Loss of component cooling Loss of one DC bus Internal fires Internal flooding Aircraft crash

In the Seabrook study, all LOOP events were assumed to impact both units concurrently, but as discussed in Section 2.4, some LOOP events may only impact a single unit. The split is highly dependent on the nature of the electrical grid and the design of the electric power systems. Hence, the determination of which events impact single or multiple units needs to be addressed on a plant specific basis. It should also be noted that the LOCA indicated in Table 2 is for internal events. The seismic events include scenarios in which the accident is the result of a seismically induced LOCA. In addition, seismic events, high winds, external flooding and truck crashes also involve scenarios with a LOOP.

The next step was to construct an event sequence model for initiating events that challenge both units concurrently [33]:

> "An important aspect of this model is the treatment of common cause failures on redundant components in both units [including CCFs that impact components in different units]. In the case of seismic events, the usual conservative model was applied in which it is assumed that seismic failure of a given component represents the common cause failure of all the similar components using that same fragility curve. In the case of loss of offsite power events and truck crash into the transmission lines, a special model was developed that distinguished between common cause failures

that impact both diesel generator units at one reactor unit, from common cause failures that impact all 4 diesel-generators at the two unit station. In the dataset that was used to derive the diesel generator beta factors[5] a total of 8 common cause events were found to be applicable to the Seabrook design. One of these events was judged to impact all 4 emergency diesel-generators, while the remaining 7 were found to impact two diesel generators on a given unit. Hence, an effort was made to refine the common cause treatment of emergency diesel generators so as not to mask the ability to distinguish between single and multiple reactor accidents."

This refinement in CCF treatment was also extended to motor operated valves with each unit and between different units. Seismically induced CCFs that could cause LOCA on both units were also addressed, as will be explained more fully in Section 5.2.5.

The results from the Level 1 PSA for the two unit station are shown in Table 3. In this table and throughout this publication, CDF refers to the traditional risk metric from a single reactor PSA, whereas site CDF (SCDF) refers to the metric in an MUPSA. Reporting on the SCDF for the two unit station, Fleming finds [33]:

"The results obtained for the calculation of core damage frequency provided some surprising results. It was not expected that multiple reactor accidents would have a significant frequency because the reactor units designed for Seabrook did not have a significant degree of shared systems. The initiating events found to be common to both reactors would be present at essentially any site. Nonetheless the frequency of events involving damage to both reactors was found to be less than an order of magnitude less frequent than the single reactor CDF value."

The conditional probability of a multi-unit accident (CPMA) given core damage to each unit was found to be about 0.14. Fleming [33] reports:

"Due to the relatively high contribution from dual reactor core damage scenarios, the total frequency of core damage at the two unit station was found to [be] significantly less than that found by simply doubling the single reactor CDF result."

---

[5] The beta factor for a redundant component is the fraction of the failure rate associated with CCFs in which two or more redundant components fail owing to a single shared cause in a brief interval of time.

TABLE 3. CORE DAMAGE FREQUENCY RESULTS FROM THE SEABROOK MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT (PSA) [13, 33]

PSA scope	Risk metric	Mean	Frequency unit
Unit 1 only	Single reactor CDF	2.3×10^{-4}	Events per reactor-year
Integrated PSA of Units 1 and 2	Single unit accident (SUCDF)	4.0×10^{-4}	Events per site-year
	Multi-unit accident (MUCDF)	3.2×10^{-5}	
	Total SCDF	4.3×10^{-4}	

Note: CDF — core damage frequency; MUCDF — multi-unit core damage frequency (of multiple reactors); SCDF — site core damage frequency; SUCDF — (site level) single unit core damage frequency.

This is true because doubling the single reactor CDF counts the dual unit accidents reflected in the multi-unit core damage frequency (MUCDF) twice. As shown in Section 3.2, when multi-unit plants have more shared systems, the MUCDF is expected to be a larger fraction of the single unit core damage frequency (SUCDF).

Fleming [33] notes "that when presenting results for an integrated PRA for a multi-reactor site, the frequency basis needs to be defined carefully", so as not to confuse reactor based and site based risk metrics. To enable the proper description of a multi-unit risk assessment [33]:

> "it is not useful to measure frequencies on the traditional reactor year basis. Event sequence frequency results are most conveniently expressed on a per site year basis. Only the events that are assumed to occur on each unit independently, or single unit results, make sense in terms of per reactor year units. To combine all the results, the site year metric is most convenient.
>
> "One of the reasons for the relatively high contributions from dual reactor accidents was the fact that at Seabrook, the single reactor results were dominated by the same list of initiating events that were found to impact both units. Loss of offsite power was the dominant initiating event in the single reactor PRA results. If the single reactor CDF result had been dominated by independent events such as loss of coolant accidents, the relative contribution from dual unit events would have been much less.
>
> "It is also necessary to define what is meant by the term 'core damage frequency' in the context of integrated risk. The frequency of core damage

[SCDF] at the two unit station planned for Seabrook, a value of 4.3×10^{-4} per station year is the frequency of an accident involving damage to one or both cores. There is another metric, which is the frequency of core damage on one and only one core, which has a different value of 4.0×10^{-4} per station year [and the frequency of core damage on both units concurrently has a value of 3.2×10^{-5} per site-year]. Hence the whole concept of surrogate risk metrics for integrated risk needs to be considered very carefully."

Previous efforts to correlate CDF to public health and safety risk was based on the results from single reactor PSAs. However, most nuclear power plants in the United States of America, and worldwide, have two or more reactor units. The major contributions to dual reactor unit CDF (i.e. frequency of an accident involving core damage to both units) are listed in Table 4. Fleming [33] finds the SCDF results "to be dominated by seismic events, although loss of offsite power and external flooding also make significant contributions." The seismic results are influenced by a conservative assumption that was made in the treatment of seismic fragility correlation[6] for identical components on different units [33]: "However, even if this assumption were relaxed, the frequency of dual unit core damage events would still be significant, and certainly too high to be dismissed."

TABLE 4. INITIATING EVENT CONTRIBUTIONS TO MULTI-UNIT CORE DAMAGE FREQUENCY (CDF) [13, 33]

Initiating event	Multi-unit CDF (events per site-year)	Percentage of total (%)
Seismic events	2.8×10^{-5}	86
Loss of off-site power	2.8×10^{-6}	8.6
Truck crash into transmission lines	1.0×10^{-7}	0.31
External flooding	1.6×10^{-6}	5.0
Total	3.2×10^{-5}	100.0

[6] 'Fragility correlation' refers to the modelling of multiple component failures that share the same fragility curve to resolve the probabilities that multiple component failures are CCFs or independent failures (see Annex I for example approaches for estimating and modelling fragility correlation).

These CDF results are based on early PSA technology and reactor performance. In more recent updates of the Seabrook PSA performed for Unit 1 (Unit 2 has since been cancelled), the total SUCDF results, including a recent update of seismic events, fires and floods, indicate a CDF value of around 2×10^{-5} per reactor-year, or about an order of magnitude lower than the values listed in Table 3 [33]. However, most of the reduction in the CDF is from reductions in the single unit parts of the integrated risk assessment completed in 1983. So, while the risk of core damage is much lower, the relative contribution of dual unit events, if that PSA had been carried forward, would not likely be much different and, in fact, could be even higher than it was in 1983.

LOOP induced station blackout is still a dominant contributor and these events have a significant potential for impacting both units. At Seabrook and many other nuclear power plants, a station blackout of one unit is produced by a LOOP and failure of two EDGs. It only takes two more diesel generator failures to have a multi-unit blackout at most sites. Service data show that some CCFs of diesel generators involve failures on multiple units. Hence, despite the age of the Seabrook results, the lessons learned about the importance of multi-unit accidents still need to be heeded.

Figures 6 and 7 present the total integrated risk for the two unit station in the form of CCDF curves and for early fatality risk and latent cancer risk, with subscripts 1 and 2 for single and dual unit releases, respectively [33]:

> "The separate contributions from single reactor accidents and dual unit accidents from each of the dominant release categories are shown. Fortunately, the frequencies of release category S6V2 [(large unscrubbed containment failure and release from both units)] is sufficiently small that it does not make a significant contribution to the overall profile for early fatality risk. However release category S2V2 [(small unscrubbed containment failure or bypass and releases from both units)] does in fact make a significant contribution to the overall early fatality risk profile, and in fact tends to dominate the risk curve in the low frequency–high consequence end of the profile.
>
> "The results for latent cancer fatality risk include a third release category for dual unit events, S3V which involves late containment failures due to over-pressurization and since it is late does not contribute to early health effect risk. The three dual unit release categories combine to dominate the integrated risk curves at exceedance frequencies below about 10^{-7} per station year, while in the higher frequency ranges, the single reactor events dominate."

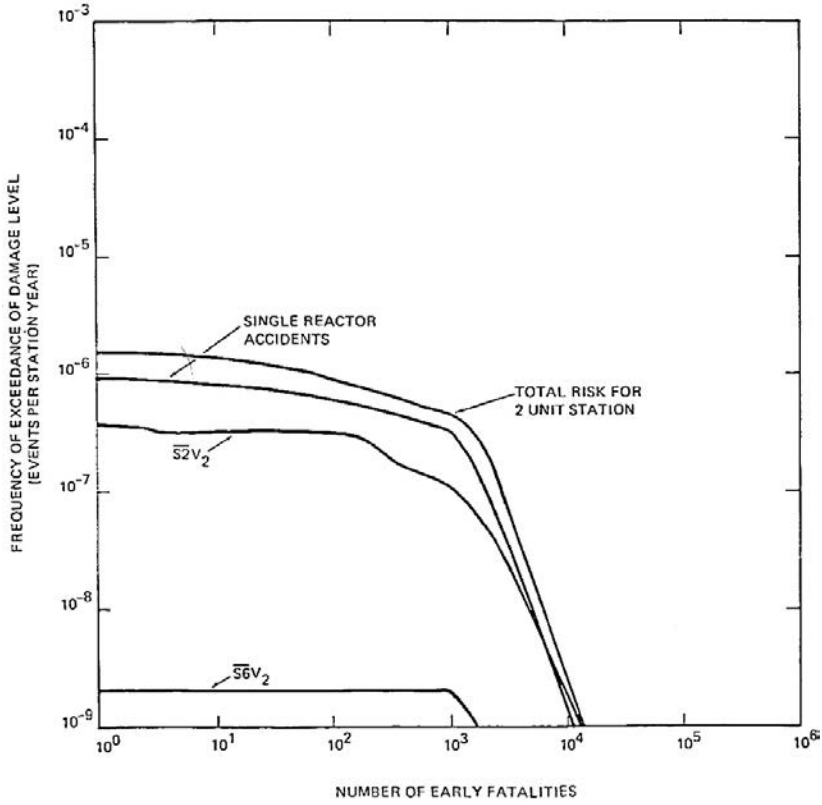


FIG. 6. Risk curve (complementary cumulative distribution function) for early fatalities for the two unit Seabrook Station. (Reproduced courtesy of ABS Group [13].)

In reviewing these results, Fleming [33] offers the following observations and conclusions, which still apply to existing multi-unit sites as well as to future modular reactor plants:

(a) To obtain an integrated risk profile for multiple reactor units, it is not possible to simply manipulate the risk profiles from single unit PSAs.
(b) For an integrated risk assessment of a site with multiple units, the frequency basis is better expressed on a per site-year basis; continuing to express frequencies on a per reactor-year basis is problematic for expressing clearly the contributions from single and multiple reactor accidents.
(c) The CPMA, given that core damage to a specific reactor has occurred, provides a relative risk measure for multi-unit accidents. For Seabrook, the CPMA was estimated to be 0.14.

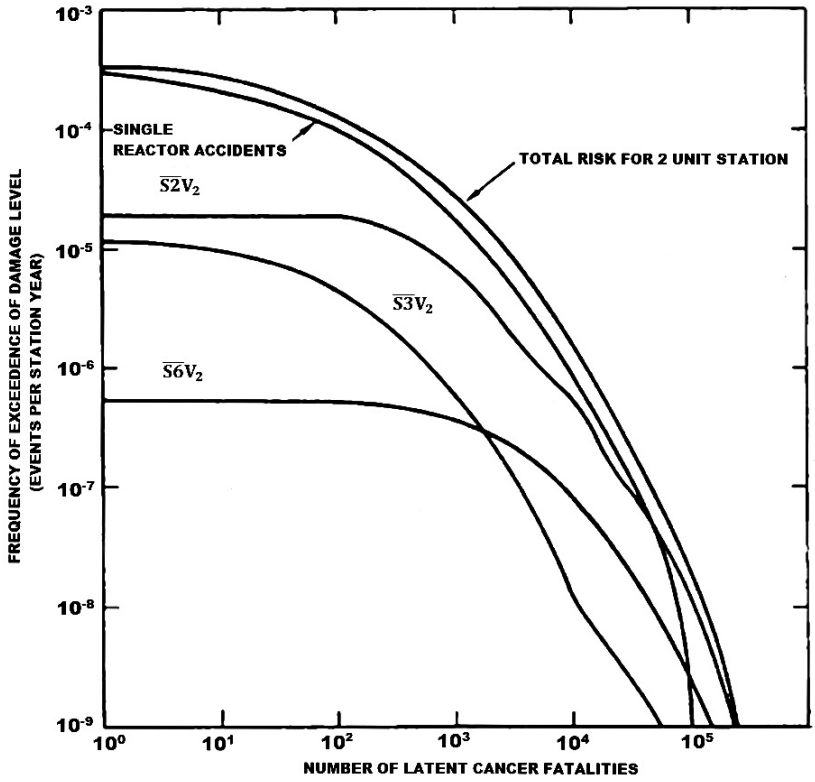


FIG. 7. Risk curve (complementary cumulative distribution function) for latent cancer fatalities for the two unit Seabrook Station. (Reproduced courtesy of ABS Group [13].)

(d) In order to address the risk contributions from multi-unit accidents at Seabrook, only a modest increase in the level of model complexity was required.

(e) The contribution to risk from multi-unit accidents was minimized at Seabrook due to the lack of shared systems. Sharing structures and systems would only increase the relative importance of multi-unit accidents.

(f) Owing to the collective lack of experience in performing MUPSAs, the results developed at Seabrook require careful review and interpretation. The multi-unit risk contribution from seismic events may have been somewhat overstated, owing to some of the modelling simplifications associated with seismic fragility correlations. Much has been learned about PSA modelling since this study was performed. Nonetheless, the conclusion that multiple reactor accidents are significant contributions to risk is viewed as robust.

(g) The evidence presented in this section indicates that the frequency of multiple concurrent reactor accidents on the same site is significant and needs to be taken into account when addressing the integrated risks from a multi-unit site. In the ASME/ANS PRA standard [21], risk significance is defined as an accident sequence that contributes at least 1% to the total risk or a basic event that contributes at least 0.5% to the total risk. Using these criteria, multi-unit accidents can be assumed to be a significant risk unless proven otherwise.

(h) Owing to the non-linear relationships used to predict early health effects from radiological exposures, simple manipulation of single unit PSA risk metrics will not suffice for estimating the site risk. The consequences of a multi-unit release can be much greater than the linear combination of individual reactor consequences because of the dose thresholds needed to produce radiation sickness.

(i) QHOs are best applied to the entire site rather than to single reactor PSA results separately. An MUPSA that addresses all of the reactors on the site should be considered, including the contributions from multiple reactor accidents.

(j) The links that have been established between the surrogate risk metrics of CDF, LERF and the safety goal QHOs are only valid for the case of single reactor sites. These established links are based on a body of work from PSAs that have generally not considered multiple unit accidents and the integrated risks at the site.

3.2. LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT RESULTS FOR PLANTS WITH SHARED SYSTEMS

In the case of Seabrook, the reactor units had minimal shared systems. The data analysis by Schroer [16], discussed in Section 2.5, shows that there other plants with a much greater extent of shared systems — 34% of the multi-unit events were associated with shared components or structures [16, 17].

In the late 1990s, a Level 1 PSA upgrade was performed on two sister plants, each with two 4-loop Westinghouse PWR units with shared structures and systems. One two unit site is near a river and the other is near a lake. Both plants have similar shared structures for safety related systems and components for systems such as emergency and non-safety service water, component cooling water, fire protection and electrical power. The Level 1 PSA models developed for both sites were quite complex; to model the risk at each reactor unit, both units' equipment was modelled to capture all of the shared equipment dependencies. Even though there was no requirement to do so, the PSA models were constructed

in such a manner that scenarios involving core damage to both units at each site could easily be identified. In processing the results, the relative contributions of single unit and dual unit core damage were identified. It is important to note that this was done primarily out of curiosity. There were no requirements at that time to analyse multi-unit accidents in PSAs. In addition, the PSA applications that were being supported only required the traditional, single reactor type of PSA.

In a PSA update performed to support a risk informed evaluation of a proposed technical specification change for the EDGs, the Level 1 PSA results were developed for both units at this two unit site. The results for the normal single reactor risk metrics of CDF and LERF for the two units at one of these sites are shown in Table 5 for the base case and for each EDG out of service.

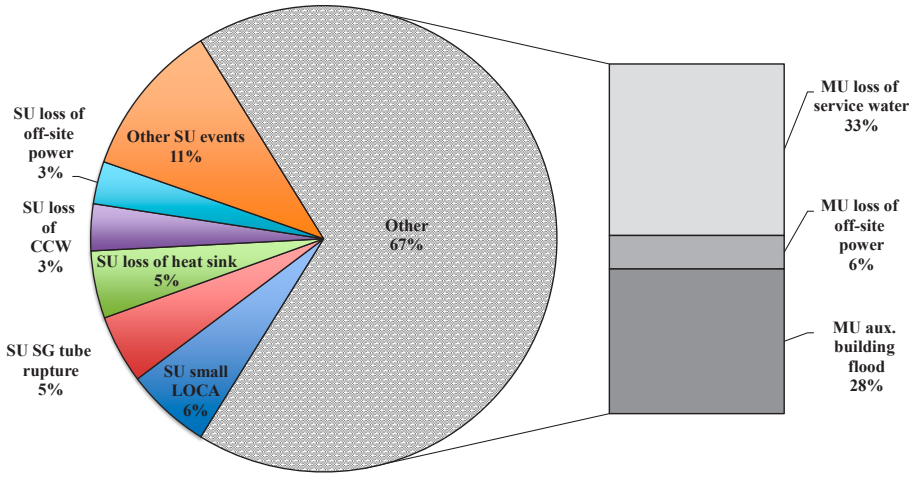
A breakdown of the baseline CDF results for Unit 1 is shown in Fig. 8. The scope of this PSA result is limited to internal events and internal flooding. Internal fires, seismic events, and internal and external hazards are excluded. Nonetheless, loss of service water, internal flooding and LOOP leading to core damage to both units, dominate the results. The MUCDF from this PSA was estimated to be about 3×10^{-5} per site-year, which is approximately the same as found for Seabrook, except that in this case only internal events and internal flooding were included.

TABLE 5. CORE DAMAGE FREQUENCY RESULTS FOR A TWO REACTOR UNIT PRESSURIZED WATER REACTOR WITH SHARED SYSTEMS

Risk metric	Unit 1		Unit 2	
	EDG Train A	EDG Train B	EDG Train A	EDG Train B
CDF_B	4.86×10^{-5}	4.86×10^{-5}	4.86×10^{-5}	4.86×10^{-5}
RAW	2.71	1.07	2.71	1.07
CDF_O	5.80×10^{-5}	4.81×10^{-5}	5.80×10^{-5}	4.81×10^{-5}
$LERF_B$	4.96×10^{-6}	4.96×10^{-6}	4.96×10^{-6}	4.96×10^{-6}
$LERF_O$	5.43×10^{-6}	4.92×10^{-6}	5.43×10^{-6}	4.92×10^{-6}

Source: Table 6 of Ref. [36].

Note: The annual average results from baseline probabilistic safety assessment (probabilistic safety assessment model based on existing technical specifications and measured in reactor-year) is indicated with B and with O for results assuming indicated emergency diesel generator (EDG) out of service. CDF — core damage frequency; LERF — large early release frequency; RAW — risk achievement worth.



Source: Figure 3 of Ref. [36].
Note: aux. — auxillary; CCW — component cooling water; LOCA — loss of coolant accident; MU — multi-unit; SG — steam generator; SU — single unit.

FIG. 8. Analysis of initiating event contributions to core damage frequency for Unit 1 of the two unit pressurized water reactor with shared systems.

It is likely that much higher values of MUCDF would have been identified if seismic events, external flooding and internal fires had been included in the scope. The CPMA for these results is 0.67. The results are similar for Unit 2. Since these plants have fire areas that involved shared equipment, it would be expected that the CPMA for a full scope treatment of hazards, which includes fires and seismic events, would be even greater than shown here. Even without this additional scope, these results indicate that a core damage event at either site is much more likely to involve both units than just a single unit. Compared with the results from the two unit Seabrook plant, in Section 3.1, sharing structures and systems yields a much higher estimate of CPMA.

CPMA alone is not a sufficient metric to evaluate risks in an MUPSA. The sharing of structures and systems often results in additional redundancy for preventing a single unit accident. The three metrics SCDF, SUCDF and MUCDF provide a fuller picture of multi-unit risk in a Level 1 PSA. Sharing systems may reduce the SUCDF, which might tend to offset the increases in MUCDF. It could also be misleading to evaluate multi-unit risks unless a full scope treatment of hazards is included. The external hazards will tend to increase the MUCDF, as they inherently impact all of the units on the site.

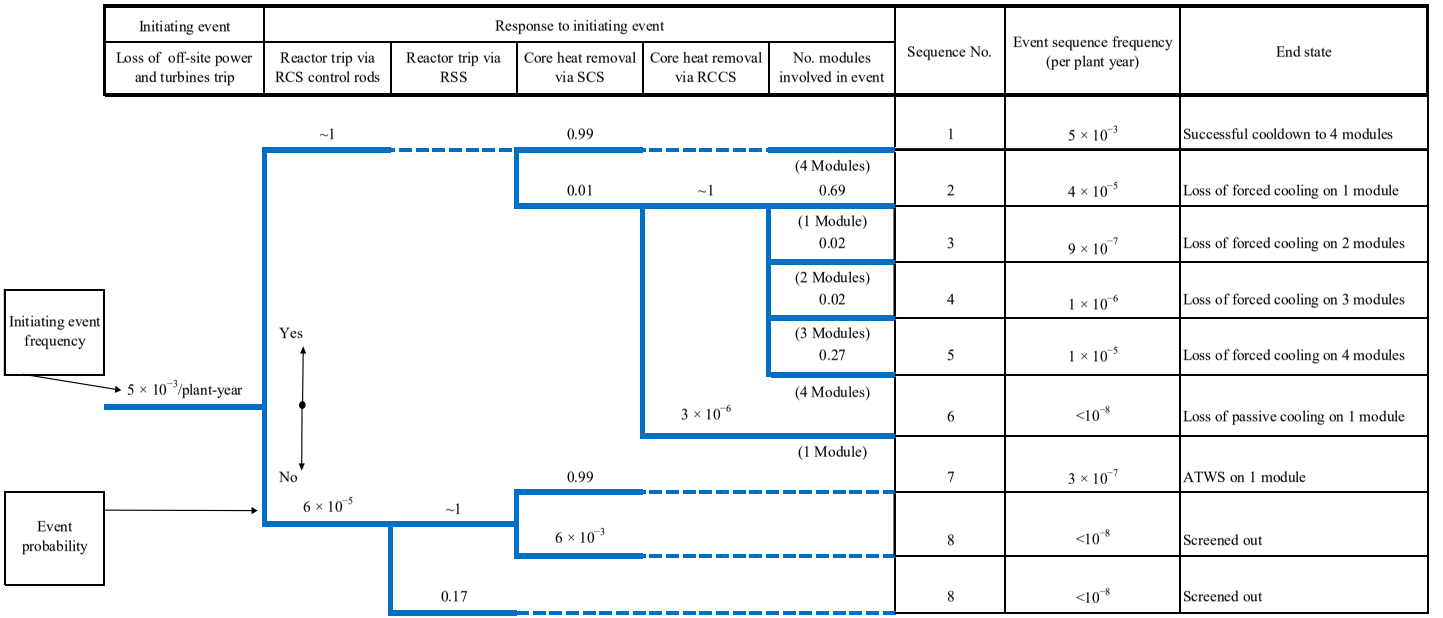
3.3. MODULAR HIGH TEMPERATURE GAS COOLED REACTOR PROBABILISTIC SAFETY ASSESSMENT

Since the early 1990s, the performance of MUPSAs has been a routine part of PSAs on MHTGRs, developed by General Atomics for the United States Department of Energy. The MHTGR was the topic of a pre-application design safety analysis report and PSA that was submitted and reviewed by the NRC. The MHTGR design comprised four reactor modules each with 500 MW(th). The safety analysis report [37] and supporting PSA [38] were performed on the four module plant, including an MUPSA. The purpose of the PSA was to provide input to the selection of licensing basis events and safety classification of SSCs. It included the selection of initiating events and event sequences involving one, two, three and four reactor modules (see Fig. 9). The practice of performing a PSA on a collection of multi-module reactor units was continued in the development of the Department of Energy's Next Generation Nuclear Plant [39]. It should be noted that the likelihood of a loss of cooling to all four modules is higher than that for loss to two or three modules due to the importance of CCFs as evaluated in this example.

3.4. MULTI-UNIT PROBABILITY SAFETY ASSESSMENTS ON CANADA DEUTERIUM–URANIUM REACTOR PLANTS

Dinnie [14] summarizes progress being made in the performance of MUPSAs and in the development of insights into severe accident management guidelines (SAMGs) for CANDU reactor plants:

> "The introduction of SAMG in Canada was motivated by the need to be able to support mitigation of nuclear hazards resulting primarily from security-related threats but the recent events in Japan have extended the scope to include extreme natural phenomena. What these have in common is that emergency response could be required in circumstances that cannot be predicted in advance and which could create plant environmental conditions far more complex than normally assumed when conducting safety analysis or PSA. In Ontario, Canada, the situation is compounded by the fact that the existing CANDU stations are constructed as four highly-integrated units sharing a number of key safety systems, including containment. Analysis of severe accidents involving multiple units has already been undertaken as part of plant PSA so some technical information is available regarding the timing and potential impacts of severe accident progression. If the accident involves multiple units, the decision making and prioritization processes



Source: Figure C-5 of Ref. [38].

Note: ATWS — anticipated transients without scram; RCCS — reactor cavity cooling system; RCS — reactor cooling system; RSS — reactor scram system; SCS — shutdown cooling system.

FIG. 9. Event tree from a modular high temperature gas cooled reactor probabilistic safety assessment identifying reactor module impacts.

of SAMG must be extended to consider the impacts of an action taken at one unit on the status of and resources available to the others, beneficial or otherwise, together with computational aids to support these actions. The aim of the paper is to consider some of the issues raised if SAMG and other post-accident human actions related to severe accident prevention and mitigation are to be incorporated into the plant PSA. It is widely recognized that the quantification of human reliability for actions identified in Level 2 PSA presents challenges over and above those considered in the Level 1. Uncertainties related to physical environment, decision-making processes and resource availability suggest that credit for human actions taken as part of SAMG be limited, especially where multiple reactor units may be affected. This is an area that warrants international standardization if PSA results are to remain inter-comparable."

The nuclear power fleet in Canada comprises 20 reactors at five locations (see Table 6). In 2005, the Canadian Nuclear Safety Commission introduced regulatory requirement S–294 [40] for PSAs applicable to all existing nuclear facilities. Each licensee was required to prepare site specific Level 1 and 2 PSAs for internal and external hazards with the units at full power and shutdown. Although the development of a Level 3 PSA is not a regulatory requirement in Canada, it is being developed by utilities in support of environmental assessment.

The safety goals each utility developed are numerical safety criteria to be used with PSA applications to evaluate nuclear reactor safety. The purpose is to ensure that the radiological risks arising from nuclear accidents associated with reactors will be low in comparison to risks to which the public is normally exposed.

TABLE 6. NUCLEAR POWER FLEET IN CANADA

Province	Utility	Nuclear power plant
Ontario	Bruce Power	Bruce A: four units Bruce B: four units
	Ontario Power Generation	Darlington: four units Pickering: six units
Quebec	Hydro Quebec	Hydro Quebec: one unit
New Brunswick	NB Power	NB Power: one unit

Ontario Power Generation (OPG) and Bruce Power have been operating multi-unit plants in Ontario since the early 1970s. Each site shares many SSCs, including:

— Structures vacuum building, turbine building and main control room.
— Mitigation systems that support all units of the site: negative pressure containment system, emergency core injection system, emergency power supply, emergency water supply.
— Support systems (e.g. instrument air, electrical power and feedwater) are also provided with an inter-unit tie, in case the individual support system fails.

The most recent Canadian PSA study of a multi-unit site was developed by OPG for the Pickering B Station. In December 2011, the Darlington Nuclear Generation Station completed a PSA as part of its compliance with regulatory requirement S–294 [40] and the results and insights were used to support the station refurbishment project [15]. The following reflects the PSA, with an emphasis on the multi-unit considerations.

3.4.1. Full power plant state modelling in Level 1 and 2 probabilistic safety assessments

The OPG PSA study reflects a single reference unit modelled in detail (Unit 2), in which it is assumed that only one unit at a time is in shutdown, with the other three units at high power. A systematic approach has been developed to select initiating events specific to Unit 2 operating at full power. When relevant, the PSA study is extended to address the event impact on an adjacent unit and also an accident on another unit that might impact Unit 2 operation. Initiating event identification and modelling includes events that can affect more than one unit, for example:

(a) Initiating events at an adjacent unit can initiate a process transient on the reference unit.
(b) Initiating events can affect the reliability of shared mitigating systems, for example:
    — A main steam line break on Unit 1 can initiate a process transient on Unit 2 and can affect the reliability of common mitigating systems.
    — A LOOP initiates a process transient on Unit 2 and affects the reliability of common mitigating systems.

To select the initiating events, multiple databases are evaluated, such as the utility specific data collection, the all CANDU reactor industry data collection and also some other designs of nuclear power plants, where relevant. The frequency of occurrence of an initiating event is calculated using a Bayesian approach and is based on reactor-year. Ontario's multi-unit CANDU reactor experience (prior distribution) is generally combined with Darlington's specific experience. If this is unavailable, Jeffrey's non-informed prior distribution is used. The PSA model includes the following:

— Mitigating systems modelled in detail on the reference Unit 2.
— Common mitigating systems modelled in detail on Unit 0, which is the unit that houses the shared systems. These have a dedicated panel in the room labelled the Unit 0 panel of Darlington Nuclear Generation Station (emergency water supply, and emergency coolant injection).
— Mitigating functions supplied from the adjacent Units 1, 3 and 4.

The Level 1 PSA sequence results are interpreted based on the frequency of occurrence and consequences, and assigned a fuel damage category (FDC):

— FDC1 and FDC2 are considered site core damage.
— FDC3 to FDC7 are considered graded core damage, from wide core damage to single channel core damage (Darlington has a 480 fuel channel assembly).
— FDC8 and FDC9 are for events with insufficient steam releases or radioactive releases to trigger an automatic containment box up, but which have a potential for economic impact.

The interface of Level 2 with Level 1 uses FDC1 to FDC7 frequencies of occurrence and consequences to define the following plant damage states (PDSs) [15]:

— PDS1 is defined by FDC1, failure to shut down, where early consequential (i.e. causal) containment failure occurs.
— PDS2 represents sequences affecting a single unit, with loss of heat sinks.
— PDS3 represents sequences with the potential for loss of heat sinks in more than one unit.
— PDS4 represents single unit sequences that bypass the containment.
— PDS5 represents sequences that challenge the containment, resulting in containment failure.
— PDS6 represents sequences that bypass the containment; however, a long term heat sink is available.

Further in the analysis, PDSs are used as entry points in containment event trees, the analysis of which generates multiple end states that are binned in release categories identified by the magnitude of releases of caesium and iodine isotopes (in Bq) and the timing [15].

The goal of the Level 2 PSA is to estimate large release frequencies (LRFs), which are greater than 1×10^{14} Bq of ^{137}Cs in 72 hours (the period generally used to represent the mission time of CANDU reactor design for Level 1 PSAs). Single unit stations use a 72 hour mission time, whereas Level 2 PSAs for multi-unit stations consider seven days.

Thermohydraulic analysis of severe accident progression demonstrated the following:

(i) Single unit failures did not result in containment challenges above the design provisions; therefore, no large external releases occurred.
(ii) Multi-unit accident sequences resulted in containment failure and external releases.
(iii) LRF is dominated by events that have the potential to cause multi-unit impacts, such as a main steam line break and LOOP.
(iv) Internal fire and internal flooding undergo the same treatment as the rest of internal events, sequences that affect a single unit and separate sequences that affect more than one unit.
(v) For seismic events, the assumption is that all four units are impacted at the same time.

3.4.2. Level 1 outage probabilistic safety assessment

OPG developed a systematic process to identify initiating events that occur in one unit during a guaranteed shutdown state (GSS) and calculated the initiating event frequency per reactor-year. A Level 1 outage PSA model was produced with Unit 1 in an outage state GSS configuration, and Units 2–4 in a full power configuration.

Primary and backup heat sinks are modelled and an emergency heat sink configuration is also included as per plant operating procedures. The PSA model is extended from a one unit model to one unit and an adjacent unit when applicable. For example, a main steam line break in Unit 2 at full power operation, outside of containment in the turbine building, is identified as an internal event that might impact an adjacent unit in a GSS. The steam environment created by the event in the turbine building (shared structure) might challenge the power supply availability if the ventilation system is unavailable to mitigate the event. Therefore, both primary and backup heat sinks might be lost and only the emergency heat sink remain available.

3.4.3. Fire, flood and seismic probabilistic safety assessments

In fire, flood and seismic PSAs, internal fires and internal flooding are treated in the same manner as other internal events: sequences are divided into those affecting a single unit only and those with the potential to affect more than one unit. External hazards, such as seismic events, are treated as fully correlated events: the seismic event is assumed to affect all four units in exactly the same manner at exactly the same time. For external hazards, therefore, severe core damage leads directly to a large release (SCDF = LRF), and LRF is both a unit and a site metric.

3.4.4. Future enhancements of multi-unit probabilistic safety assessment

OPG improved the division of sequences applicable to one unit, then those applicable to two units, and then sequences for three or four units. OPG subsequently determined that two unit events do not result in a large external release. Therefore, a future update of the PSA will analyse PDS3 (loss of all heat sinks in two or more units) concerning two aspects, two unit events and three or four unit events.

OPG improved the thermohydraulic method of transient behaviour to distinguish between a thermohydraulic transient of the reference unit and a thermohydraulic transient of the other units. Plant habitability after a severe accident can be more accurately reflected in a PSA model and improvements in modelling will contribute to future editions of the PSA.

3.5. SUMMARY OF TECHNICAL ISSUES FOR SITE SAFETY ASSESSMENT

The reviews in Sections 2 and 3 identify the following technical insights that need to be considered in future MUPSAs:

(a) Single reactor risk metrics such as CDF, LRF and LERF developed in PSAs performed on one reactor unit at a time are not sufficient to characterize the total risk of a multi-unit site. Site based risk metrics are needed to capture more fully the risks to the population surrounding such sites.
(b) The Fukushima Daiichi accident, the PSA results at Seabrook and other completed PSAs show the risk of accidents involving core damage of two or more units concurrently is significant and cannot be ignored. This is true for both internal and external hazards, and applies to multi-unit sites with shared systems as well as those with minimal sharing. At a minimum, all

multi-unit sites may consider station blackout conditions affecting multiple units as well as multi-unit considerations in the evaluation of external hazards. Multi-unit sites with more sharing of systems may consider a more comprehensive treatment of internal events that can produce multi-unit accidents. Examples of such treatment include support system faults and internal fires and flooding in common areas that adversely impact multiple units.

(c) The ideal method available to address the integrated risk of a multi-unit site is to perform a full scope Level 3 PSA that addresses all internal and external events and hazards, as well as multi-unit accidents. Substantial improvements to the current practice of safety assessments on one reactor at a time can be achieved by expanding Level 1 and 2 PSAs to account for multi-unit accidents.

(d) Existing deterministic safety analyses are confined to analysing one reactor at a time with the implicit assumption that the other reactors and radiological sources are safely protected. Future site safety assessments need to undertake supporting deterministic analyses of the entire site response to multi-unit events.

(e) Current guidance for PSA is generally limited to the evaluation of each reactor unit separately and independently. An exception is ASME/ANS RA-S-1.4-2013, Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants [41], which addresses the integrated risks of multi-unit plants. Technical issues that need to be considered in future MUPSAs include:
   - Identification of initiating events that impact more than one reactor unit, including those due to a single hazard or combination of hazards.
   - Modelling of event sequences involving plant response, mitigation and core damage to more than one reactor unit.
   - Treatment of CCFs on multi-unit sites that distinguish between events that impact a single reactor unit and those that impact components of different units.
   - Treatment of human reliability analysis when multiple units are affected or when the plant conditions involve core damage or radiological contamination of the site. This includes how to treat the safe shutdown of one unit when a general emergency is declared and possible releases occur from another unit on the same site.
   - Treatment of seismic fragility correlation for seismically induced LOCAs and other seismically induced initiating events on multiple units.
   - Treatment of fragility correlation for high wind hazards and for other external hazards.

— Definition of appropriate risk metrics for site safety assessments. Examples for consideration include SCDF, site LERF (SLERF), Level 3 CCDFs, risk of fatality to individuals living around a nuclear power plant site (QHO type metrics) and CPMA.
— Development of a multi-unit database for initiating events, CCFs and CCIEs, among others.
— Treatment of consequential (i.e. causal) failure probability of equipment located in multiple units.

4. OVERALL APPROACH TO MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENTS

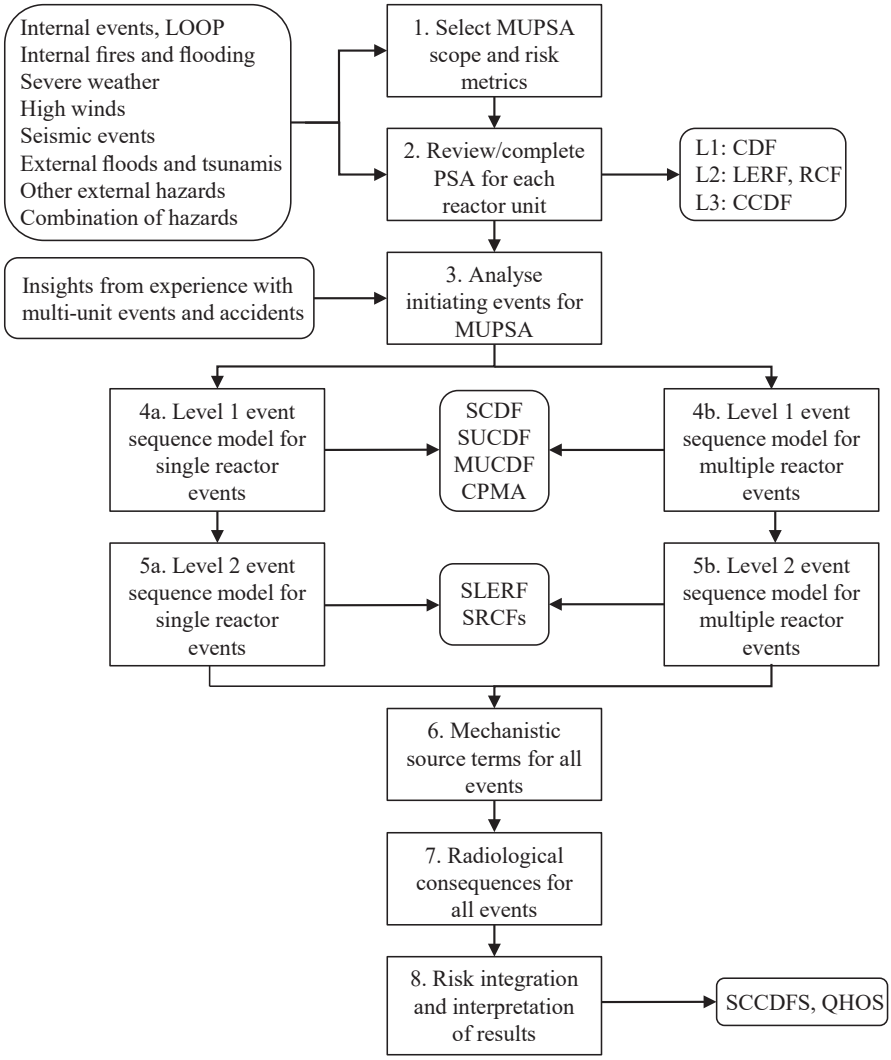
4.1. SUMMARY OF STEPS

The overall process of conducting a site safety assessment for a multi-unit site comprises of eight steps (see Fig. 10). The contents of each step are briefly discussed in the following.

4.1.1. Step 1: Selecting probabilistic safety assessment scope and risk metrics

There are two basic options for performing a site safety evaluation as discussed in this publication. The first option is to limit the evaluation to performing a limited scope Level 2 PSA that is sufficient to estimate the site risk metrics of SCDF (defined as the CDF to one or more reactor units on the site) and SLERF (defined as the frequency of a large early release from one or more reactors or radionuclide sources on the site). The second — and preferred — option is to perform a Level 3 PSA that provides a more complete set of risk metrics, such as CCDF for public health effects and property damage, and individual risks for the QHO type of risk metrics. This option means a more complete treatment of radionuclide sources such as the spent fuel storage system.

For both options, a full scope treatment of external hazards and plant operating states is included. More information on the selection and definition of risk metrics is provided in Section 4.3. The site based metrics are needed for both risk quantification and for screening of events and hazards for multi-unit sites.



Note: CCDF — complementary cumulative distribution function; CDF — core damage frequency; CPMA — conditional probability of multi-unit accident; LERF — large early release frequency; LOOP — loss of off-site power; MUCDF — multi-unit core damage frequency; MUPSA — multi-unit probabilistic safety assessment; PSA — probabilistic safety assessment; QHOs — (site) quantitative health objectives for individual risk; RCF — release category frequency; SCCDF — complementary cumulative distribution function; SCDF — site core damage frequency; SLERF — site large early release frequency; SRCF — site release category frequency; SUCDF — single unit core damage frequency.

FIG. 10. Overview of the process for multi-unit probabilistic safety assessments.

4.1.2. Step 2: Reviewing and completing the single reactor probabilistic safety assessment for each reactor unit and facility

In this step, a PSA is completed to the scope selected in Step 1 for each reactor using established PSA methods. If a PSA already exists for one or more reactor units, it is only necessary to extend the scope, as needed, to achieve the scope selected in Step 1. PSA guides and standards that are available to support various facets of a full scope PSA are listed in Table 7.

ASME/ANS RA-S-1.4-2013 [41] was developed specifically to support MUPSAs on advanced reactors using modular reactor concepts, and it provides useful guidance for MUPSAs on light water reactors (LWRs) as well as non-LWR designs (see Section 5 on how to modify the single unit PSAs to address the technical issues of MUPSAs). Plant walkdowns performed for a single unit PRA will need to be expanded in scope to investigate initiating events that may impact multiple reactor units as well as inter-unit dependencies.

4.1.3. Step 3: Analysing initiating events for multi-unit probabilistic safety assessment

The purpose of this step is to analyse the selection of initiating events to resolve which apply to individual reactor units and which impact two or more reactor units on the site concurrently, and to resolve the initiating event causes, including internal events and internal and external hazards. This may require rescreening the initial list of events considered in the single reactor PSA and some events may need to be subdivided to resolve the multi-unit CCIEs.

4.1.4. Step 4: Level 1 event sequence model

In this step, the event sequence model that was developed for the single unit PSA in Step 2 is modified to clearly distinguish between events involving single reactor units (Step 4a) and multiple reactor units (Step 4b). The single unit event sequence model in Step 4a is largely based on what was already developed in the single unit PSA in Step 2, but it may need to be altered to interface with a more refined definition and selection of initiating events. As with single unit PSAs, plant walkdowns are necessary to identify the potential for accidents involving two or more units. In Step 4b, a new model is developed to identify event sequences involving core damage to two or more units. This can result from a multi-unit CCIE or from the cascading effects of a single unit accident propagating to affect another. The quantification of the models in Steps 4a and 4b provides the necessary information to calculate the SCDF.

TABLE 7. STANDARDS, GUIDES AND PUBLICATIONS TO SUPPORT PROBABILISTIC SAFETY ASSESSMENT AND MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT

Source	Contents
IAEA Safety Standards Series No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [5]	Methodology and guidance for Level 1 PSA for internal and external hazards for full power, low power and shutdown operating states
IAEA Safety Standards Series No. SSG-4, Development and Application of Level 2 Probabilistic Safety Assessments for Nuclear Power Plants [6]	Interfaces with SSG-3 [42] and addresses Level 2 interface, containment event trees, accident progression analysis and source term estimation
IAEA Safety Standards Series No. NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants [42]	Methodology and guidance for the performance of probabilistic human induced hazard analysis
Safety Reports Series No. 86, Safety Aspects of Nuclear Power Plants in Human Induced External Events: General Considerations [43]	Detailed methodology for the performance of margin assessment of a nuclear power plant against human induced events
IAEA Safety Standards Series No. SSG-9, Seismic Hazards in Site Evaluation for Nuclear Installations [26]	Methodology and guidance for the performance of probabilistic seismic hazard analysis
IAEA Safety Standards Series No. NS-G-2.13, Evaluation of Seismic Safety for Existing Nuclear Installations [7]	Methodology and guidance for the performance of seismic PSAs
IAEA-TECDOC-724, Probabilistic Safety Assessment for Seismic Events [44]	Methodology for the performance of seismic PSAs
OECD/NEA, Probabilistic Safety Analysis (PSA) of Other External Events than Earthquake [45]	Methodology for the performance of PSAs on external events other than earthquakes
IAEA Safety Standards Series No. SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations [46]	Methodology and guidance for the performance of a probabilistic meteorological and hydrological hazard analysis
Safety Reports Series No. 92, Consideration of External Hazards in Probabilistic Safety Assessment for Single Unit and Multi-unit Nuclear Power Plants [47]	Methodology for the performance of general, single and multi-unit PSAs on external hazards, flooding and high winds Supplemental information on screening and bounding analyses

TABLE 7. STANDARDS, GUIDES AND PUBLICATIONS TO SUPPORT PROBABILISTIC SAFETY ASSESSMENT AND MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT (cont.)

Source	Contents
NRC, Guidance for Performing a Tsunami, Surge, or Seiche Hazard Assessment: Interim Staff Guidance [48]	Interim staff guidance for the performance of deterministic and probabilistic hazard analysis for tsunamis, surges and seiches
IAEA Safety Standards Series No. SSG-21, Volcanic Hazards in Site Evaluation for Nuclear Installations [49]	Methodology and guidance for the performance of probabilistic volcanic hazard analysis
IAEA-TECDOC-1795, Volcanic Hazard Assessments for Nuclear Installations: Methods and Examples in Site Evaluation [50]	Detailed methodology for the performance of probabilistic volcanic hazard analysis
ASME/ANS RA-Sb-2013, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications [21]	Standard for performing Level 1 and limited scope Level 2 PRAs for core damage frequency and large early release frequency, full power operating states and a full set of internal and external hazards Standard does not address multi-unit PRAs, only one reactor at a time PRAs
ASME/ANS RA-S-1.4-2013, Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants [41]	Standard for performing a full scope Level 3 PRA on any reactor technology, covering operating and shutdown modes, and a full set of internal and external hazards Includes specific requirements for multi-unit PRAs
NUREG/CR-6850, EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities [51]	Detailed guidance and procedures for performing an internal fire PRA for operating LWRs and at-power plant operating states Forms the basis of Part 4 of ASME/ANS RA-Sb-2013 [21] dealing with internal fire hazards
EPRI 1019194, Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment [52]	Guidance and procedures for performing an internal flood PRA and meeting the requirements in Part 3 of ASME/ANS RA-Sb-2013 [21]
NRC, Risk Assessment of Operational Events Handbook [53]	Risk evaluation of operational events and identification of gaps with PSA models

TABLE 7. STANDARDS, GUIDES AND PUBLICATIONS TO SUPPORT PROBABILISTIC SAFETY ASSESSMENT AND MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT (cont.)

Source	Contents
NUREG/CR-6813, Issues and Recommendations for Advancement of PRA Technology in Risk-informed Decision Making [54]	Insights from US PSA peer reviews and NRC staff interviews on limitations of PSA and strategies to address them
EPRI 1022997, Identification of External Hazards for Analysis in Probabilistic Risk Assessment [55]	Methods for selecting, and criteria for screening, external hazards
NUREG/CR-2300, PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants [22]	Guidance and methodology for Level 3 PRAs for internal and external hazards
IAEA-TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants [56]	Detailed methodology for the quality assurance of PSA

Note: ASME — American Society of Mechanical Engineers; ANS — American Nuclear Society; EPRI — Electric Power Research Institute; LWR — light water reactor; NEA — Nuclear Energy Agency; NRC — Nuclear Regulatory Commission; OECD — Organisation for Economic Co-operation and Development; PRA — probabilistic risk assessment; PSA — probabilistic safety assessment.

4.1.5. Step 5: Level 2 event sequence model

In this step, the event sequence models completed in Step 4 are extended to resolve the release categories of a Level 2 PSA. The models in Step 5a are based on what was already done in Step 2 for the individual reactor units if Step 2 had been developed to Level 2. Otherwise, if Step 2 was for a Level 1 PSA, it would be expanded in Step 5a to address Level 2 scenarios involving single reactor units. In Step 5b, the event sequences for the scenarios with core damage to two or more units are developed and quantified. The quantification of the Level 2 event sequence models in Steps 5a and 5b provides the necessary information to calculate the SLERF. If the end states of the Level 2 model are sufficiently complete, the Level 2 model will also have sufficient information to calculate the site release category frequencies (SRCFs) which may involve releases from single or multiple reactor accidents.

4.1.6. Step 6: Mechanistic source terms for all events

The purpose of this step is to develop the radioactive release source terms for all of the event sequences and release categories of Step 5. The step is completed for the Level 3 risk metric option. It should be noted that the single reactor core damage events were already addressed in Step 2. When the single reactor PSA is expanded to a Level 2 PSA, the single unit initiating events and accident sequences are fully developed to support the Level 2 PSA in Steps 3, 4a and 5a, which establishes the scope of single reactor accidents for which mechanistic source terms are needed. To support the MUPSA, it is necessary to address the unique accident sequences associated with multi-unit source terms (already defined in Step 5b).

4.1.7. Step 7: Radiological consequences for all events

The purpose of this step is to develop the radiological consequences for all of the release categories and source terms of Steps 5 and 6. Similar to Step 6, the step is completed for the Level 3 risk metric option. If the single reactor PSA developed in Step 2 was a Level 3 PSA, all that is now required is to analyse the multi-unit core damage sequences for the necessary source term information.

4.1.8. Step 8: Risk integration and interpretation of results

In this step, the results for the event sequence frequencies and consequences are combined into Level 3 risk metrics, such as SCCDF curves for public health and safety impact, property damage and economic impacts. The integrated risk results are compared to the selected risk significance criteria and safety goals. Risk insights are then developed with regard to plant vulnerabilities and site and design specific factors that give rise to risk management opportunities.

4.2. SELECTION OF INITIAL CONDITIONS FOR SEQUENCE DEVELOPMENT

When an initiating event occurs, it is necessary to establish the initial conditions of each plant on the site. In PSA models, it is normally assumed that initiating events occur at random points in time according to a Poisson process. To perform the site safety assessment, it necessary to estimate the fraction of time each plant and facility is in various states of power operation or shutdown for refuelling or maintenance. A full power PSA model is used for reactor units at full power, otherwise a low power and shutdown (LPSD) model is required. At

the time the tsunami hit Fukushima Daiichi, there were three units in operation and three in a shutdown state. An estimate of the fraction of time spent in each possible configuration of the nuclear power plants is the boundary condition of the site safety assessment. This estimate needs to consider that multi-unit plant operators will coordinate the planned outages to align with energy production requirements, which may minimize configurations with multiple units off-line. For example, estimates for a three unit plant would be made for the following site configurations:

— All three units operating at-power;
— Two units at-power and one in shutdown (three combinations);
— One unit at-power and two units in shutdown (three combinations);
— All three units in shutdown;
— Variations of the above with spent fuel pool status.

If the units are identical, the different combinations do not have to be modelled separately. Both an at-power PSA and an LPSD PSA would be needed for each nuclear power plant on the site.

Some existing PSAs that consider LPSD states have many different plant operating states and considering all possible combinations of plant operating states in an MUPSA is often not practical. Hence, assumptions to reduce the number of states is appropriate. Given the lack of experience in performing MUPSAs, it is expected that the focus will remain on addressing the simple case of assuming that all of the reactors are operating at full power, as was the case in the Seabrook MUPSA.

4.3. MULTI-UNIT SITE RISK METRICS

As discussed in Section 3.1, the Seabrook Level 3 PSA, which included an MUPSA of a two unit station, concluded that risk metrics, such as CDF and LERF, were not appropriate for a multi-unit site because each reactor unit's CDF does not specify the state of the other units on the site. Although it is possible to compute an SUCDF on a multi-unit site for each core damage event considered in the computation, there is uncertainty or ambiguity about the status of the remaining units when core damage occurs at either unit. In addition, since some of the core damage scenarios involve core damage to multiple units, it is not possible to simply sum the individual CDF values for each reactor unit and to obtain a meaningful result for an SCDF. That would lead to overcounting multi-unit events that are part of each individual CDF. Different types of core damage metric were used to characterize the Level 1 PSA results for the two

reactor unit station in the Seabrook study. These metrics used a frequency basis of a (two unit) station-year, which is equivalent to a site-year for that site. If the single unit PSA is a Level 3 PSA, there would be additional risk metrics, such as release category frequencies (RCFs) and CCDFs, for single reactor accidents.

In this publication, the following risk metrics are defined to complement the traditional PSA metrics associated with single unit PSAs. The frequency basis for all of the site based risk metrics is events per site-year:

— SCDF: Frequency per site-year of core damage to one or more reactor units.
— SLERF: Frequency per site-year of a large early release from one or more reactors or on-site facilities.
— SRCF: Frequency per site-year of each distinct release category for a multi-unit Level 2 PSA. These release categories include the release categories already defined in a single unit Level 2 PSA for each unit and for releases from a single reactor unit, as well as categories for accidents involving multiple reactor units or facilities.

SCDF can be estimated by using a Level 1 PSA, the scope of which is expanded to include all reactors on the site. Such a PSA would include accidents involving core damage to each reactor separately and to each possible combination of reactors for multiple unit events. The sum of the CDFs from all contributions (measured as frequency per site-year) is the SCDF. The two major categories of core damage events included in the estimation of SCDF are events that involve core damage to a single unit and those that involve core damage to multiple units:

— SUCDF: Frequency per site-year of an accident involving core damage to a single unit on a multi-unit site.
— MUCDF: Frequency per site-year of an accident involving core damage to two or more reactor units on a multi-unit site.

It should be noted that SUCDF is not the same as CDF, the traditional risk metric used in single unit PSAs. CDF is normally expressed in events per reactor-calendar-year for each reactor on the site. SUCDF is the aggregated CDF that accounts for all of the on-site reactors.

SLERF can be estimated by using a limited scope Level 2 PSA that includes accident sequences involving large early releases from each reactor on the site and from each possible combination of reactors for multi-unit events. It is possible that the release from a multi-unit accident may combine to exceed the threshold for a ‘large’ release. Hence, the total SLERF may involve single reactor accident sequences with releases from a single unit that meet the criteria

for a large early release as well as releases from multiple reactor accidents that combine to meet these same criteria.

The definitions for SCDF and SLERF are consistent with those proposed by Schroer [16]. While SCDF is only relevant for accidents involving releases from reactor cores, SLERF and the Level 3 PSA risk metrics can be used for reactors and other facilities with radionuclide inventories, such as spent fuel storage systems. These site risk metrics could then be used to supplement the traditional reactor based risk metrics of CDF and LERF, which would continue to be used for the individual PSAs performed one reactor at a time. The purpose here is to supplement the existing risk metrics — not to replace them. However, risk informed decisions and applications based on CDF and LERF types of metric will need to be reconsidered to determine whether these site based metrics need to be incorporated and, if not, whether the limitations of the CDF and LERF metrics from single reactor PSAs are taken into account in risk informed decision making. For example, existing guidelines for acceptable levels of CDF and LERF are derived from site based safety goals and single unit PSAs. For multi-unit sites, it is necessary to calibrate the site based goals to multi-unit risk metrics; otherwise, the risk of multi-unit accidents is not adequately considered.

An additional risk metric that was used in Section 3.1 as a measure of the relative importance of multi-unit accidents is given by CPMA, defined as the conditional probability of an accident involving multiple units given core damage to a specified reactor unit on the site.

If PSAs are expanded to cover a full Level 2 PSA that addresses multi-unit risk, in addition to the ability to calculate SCDF, MUCDF and SLERF, the frequencies of each release category could be estimated. In this type of Level 2 PSA, the release categories would account for each type of release from a single unit accident as well as those from multi-unit events. For each unique release category, a radioactive material release source term would be developed. Some of these release categories would involve releases from multiple reactor units. In this option, the capability to address releases from non-core sources, such as the spent fuel storage system, would be afforded. As with SCDF, SUCDF, MUCDF and SLERF, the frequency for SRCF is events per site-year.

If the PSA is further expanded to a multi-unit Level 3 PSA, SCCDFs can be developed, similar to those illustrated in Fig. 5, in Section 3.1, for each consequence parameter, such as population dose exposure (man-Sv), latent cancer fatalities, early fatalities, early injuries, property damage costs and land contamination. To distinguish between CCDFs for a single unit PSA and a multi-unit or multi-facility PSA, the latter are designated in this publication as SCCDF. The term multi-facility PSA is used to describe a PSA that addresses releases from sources of radioactive material other than the reactor cores (e.g. spent fuel storage or radioactive waste storage). Hence, a PSA that included

the spent fuel storage system and the reactor system on a single unit site would be classified as a multi-facility PSA. The frequency basis for SCCDFs is events per site-year; for comparison to safety goals or QHOs, the correct unit of individual risks is the probability of individual fatality per site-year.

A final type of risk metric is the individual risk of fatality to those living in the vicinity of a nuclear reactor site. In the United States of America, there are QHOs for these metrics derived from the safety goals, and similar metrics are used in other countries. These QHOs had been used to compare the results of a single unit Level 3 PSA because integrated site Level 3 PSAs were rarely performed. However, individuals in the vicinity of the site are exposed to the risks from every facility on a site, including risks of accidents involving releases from multiple facilities. Hence, a more complete statement of risks for comparison to site safety goals is provided by a multi-unit or multi-facility Level 3 PSA. A summary of the risk metrics that can be used to support an MUPSA is provided in Table 8.

TABLE 8. SUMMARY OF RISK METRICS FOR MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT

Probabilistic safety assessment (PSA)	Risk metric	Abbreviation
Level 1 single unit PSA	Core damage frequency	CDF
Limited scope single unit Level 2 PSA	Large early release frequency	LERF
Level 1 MUPSA	Site core damage frequency	SCDF
	Single unit core damage frequency	SUCDF
	Multi-unit core damage frequency	MUCDF
	Conditional probability of a multi-unit accident	CPMA
Limited scope multi-unit Level 2 PSA	Site large early release frequency	SLERF
Full scope Level 2 single unit PSA	Release category frequency	RCF
Full scope Level 2 MUPSA	Site release category frequency	SRCF
Level 3 single unit PSA	Complementary cumulative distribution function	CCDF
Level 3 multi-unit or multi-facility PSA	Quantitative health objectives	QHO
	Site complementary cumulative distribution function	SCCDF

4.4. SELECTION OF RISK SIGNIFICANCE CRITERIA

For current single reactor PSAs, some IAEA Member States have developed risk significance criteria linked to safety goals and QHOs which are really site based metrics. For MUPSA, these links need to be reconsidered because the integrated risks from multi-unit sites were not addressed. Some considerations in deriving risk significance criteria for MUPSA risk metrics are presented in Section 9.2.

4.5. SUMMARY OF PROBABILISTIC SAFETY ASSESSMENT MODELS FOR SELECTED RISK METRICS

4.5.1. Sites with identical reactor units

To understand the relationship between SCDF and the more traditional CDF used in existing PSAs, two identical reactor units are considered on a site, each with the same CDF when the PSAs are performed one reactor at a time (as was the case at Seabrook, see Section 3.1). The relationships between CDF and SCDF can be seen in the following expressions:

$$\begin{aligned} CDF &= CDF_1 + CDF_2 \\ SCDF &= SUCDF + MUCDF \\ SUCDF &= 2CDF_1 \\ MUCDF &= CDF_2 \\ SCDF &= 2CDF_1 + CDF_2 = 2CDF - CDF_2 \end{aligned}$$

These expressions assume that the single unit core damage events (the frequencies of which are CDF_1) occur on each unit independently and that the dual unit core damage events (frequencies defined by CDF_2) are independent to the single unit events. This development is analogous to a CCF model, except in this case the components are nuclear reactor units and the CCFs are analogous to accidents involving both reactor units concurrently. The units of SCDF are events per site-calendar-year; the units of CDF are events per reactor-calendar-year:

SCDF = (2 reactors per site) × (CDF_1 events per reactor/calendar-year) +
+ (1 pair of reactors per site) × (CDF_2 events per pair of reactors/calendar-year)
= events per site − calendar-year

The CPMA, given core damage to either unit, is given by:

$$\text{CPMA} = \frac{\text{CDF}_2}{\text{CDF}} = \frac{\text{CDF}_2}{\text{CDF}_1 + \text{CDF}_2}$$

To illustrate how complex this becomes with more units, three identical reactor units on a site are considered (where a triple unit core damage event is defined by CDF_3):

$$\begin{aligned} \text{CDF} &= \text{CDF}_1 + 2\text{CDF}_2 + \text{CDF}_3 \\ \text{SUCDF} &= 3\text{CDF}_1 \\ \text{MUCDF} &= 3\text{CDF}_2 + \text{CDF}_3 \\ \text{SCDF} &= 3\text{CDF}_1 + 3\text{CDF}_2 + \text{CDF}_3 \\ &= 3\text{CDF} - 3\text{CDF}_2 - 2\text{CDF}_3 \end{aligned}$$

The CPMA, given core damage to either unit, is then given by:

$$\text{CPMA} = \frac{2\text{CDF}_2 + 3\text{CDF}_3}{\text{CDF}} = \frac{2\text{CDF}_2 + \text{CDF}_3}{\text{CDF}_1 + 2\text{CDF}_2 + \text{CDF}_3}$$

These equations demonstrate that the multi-unit site metrics SCDF and CPMA are dependent on the number of reactor units at the site. It becomes more complex for sites with more reactor units.

4.5.2. Sites with non-identical units

For sites with non-identical units, the single reactor and multiple reactor contributions to the SCDF reflect each reactor and each combination of reactors. For a site with two reactor units (A and B):

$$\text{SCDF} = \text{CDF}_\text{A} + \text{CDF}_\text{B} + \text{CDF}_\text{AB}$$

where CDF_AB is the MUCDF for Units A and B concurrently. As stated above, the general expression for any number of reactor units on a site is:

$$\text{SCDF} = \text{SUCDF} + \text{MUCDF}$$

where SUCDF accounts for contributions from each reactor unit on the site, where each reactor CDF is in units of events per reactor-calendar-year and MUCDF accounts for contributions from each combination of reactor units on the site.

For sites with a large number of units, it might be impractical to model each possible combination of multi-unit accident cases separately. Hence, assumptions would need to be made to simplify it to something manageable. Examples of such assumptions might include selecting one or some selected number of pairs of reactor units to explicitly model and then assume that the consequences of the multiple unit accidents involve more than two reactor releases. Another approach would be to assume that all multiple reactor accidents involve all of the units.

4.6. TREATMENT OF MULTIPLE HAZARDS

An MUPSA is performed to identify and quantify the risk parameters of accident sequences involving multiple reactor units which are not resolved in a collection of single reactor PSAs for the site. It is important that the combined effects of correlated internal and external hazards are considered, such as:

— Seismically induced tsunamis and dam failures (upstream and downstream);
— Seismically induced fires, floods and high energy pipe breaks;
— Combined effects of wind hazards and flooding from severe storms;
— Other correlated hazards.

4.7. ENSURING TECHNICAL ADEQUACY

Strategies to ensure the technical adequacy of an MUPSA are essentially the same as those that have been established for single unit PSAs and include:

— Use of qualified personnel;
— Use of accepted methods, procedures and validated computer programs;
— Use of accepted industry standards for PSAs;
— Transparent documentation of the PSA development and results;
— Performance of in-process and after-the-fact peer reviews;
— PSA maintenance, updates and configuration control process.

A key challenge for technical adequacy is that there is very little experience of performing MUPSAs. Most of the available guides and standards for performing PSAs and conducting peer reviews are based on the single reactor PSA model (see Refs [6, 21, 48]). ASME/ANS RA-S-1.4-2013 [41] was developed for use with modular reactor designs and provides requirements for an MUPSA. To support advanced non-LWR designs, it does not use LWR risk metrics, such as CDF and LERF (or SCDF and SLERF), but it does support the

site metrics of SRCF and SCCDF. To address MUPSAs, Ref. [41] has specific requirements for: (i) delineating appropriate combinations of plant operating states for multiple reactors; and (ii) delineating initiating events and accident sequences from a full range of internal and external hazards over a full set of plant operating states that impact single and every combination of multiple reactor units. For risk quantification, Ref. [41] also has requirements for aggregating the risk contributions from single and multiple reactor accidents and for delineating the significant contributors to risk in this context as well. It is likely that many of these MUPSA requirements will find their way into a revision of the ASME/ANS PRA standard [21]. Hence, Ref. [41] offers useful guidance for performing a multi-unit Level 3 PSA.

4.8. TERMINOLOGY FOR MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT

There are many concepts and terms used in PSA that may be revisited in light of the effort to expand the scope to include the integrated risks from multi-unit sites. This publication defines new site risk metrics, such as SCDF, SLERF, SRCF and SCCDF, which parallel the single unit PSA risk metrics, CDF, LERF, RCF and CCDF, but yet have different meanings. To avoid confusion, the letter 'S' is used when the site based metric is intended, so that the metrics without the 'S' retain their original meaning. There are other terms, such as CCF and CCIE, which have been defined for single unit PSAs and now can be modified to clarify the meaning in the context of an MUPSA. The approach taken in this publication to clarify the meaning is to use the prefix 'single unit' or 'multi-unit' to clarify the scope of the CCFs that are being referred to.

5. LEVEL 1 PLANT AND SYSTEMS MODELS FOR INTERNAL AND EXTERNAL HAZARDS

5.1. PLANT OPERATING STATES

At the time of an initiating event at a nuclear power plant site, it is necessary to establish the plant operating state of each nuclear power plant at the site at the time of the initiating event. In PSA models, it is normally assumed that initiating events occur at random points in time according to a Poisson process. In order to perform the site safety assessment, it is necessary to estimate the fraction of time

each nuclear power plant and facility is in various states of power operation or shutdown for refuelling or maintenance.

5.2. INITIATING EVENT ANALYSIS

5.2.1. Classification of initiating events for multi-unit probabilistic safety assessments

The initiating event analysis refers to Step 3 in Fig. 10, in Section 4.1, which describes the overall process for performing an MUPSA:

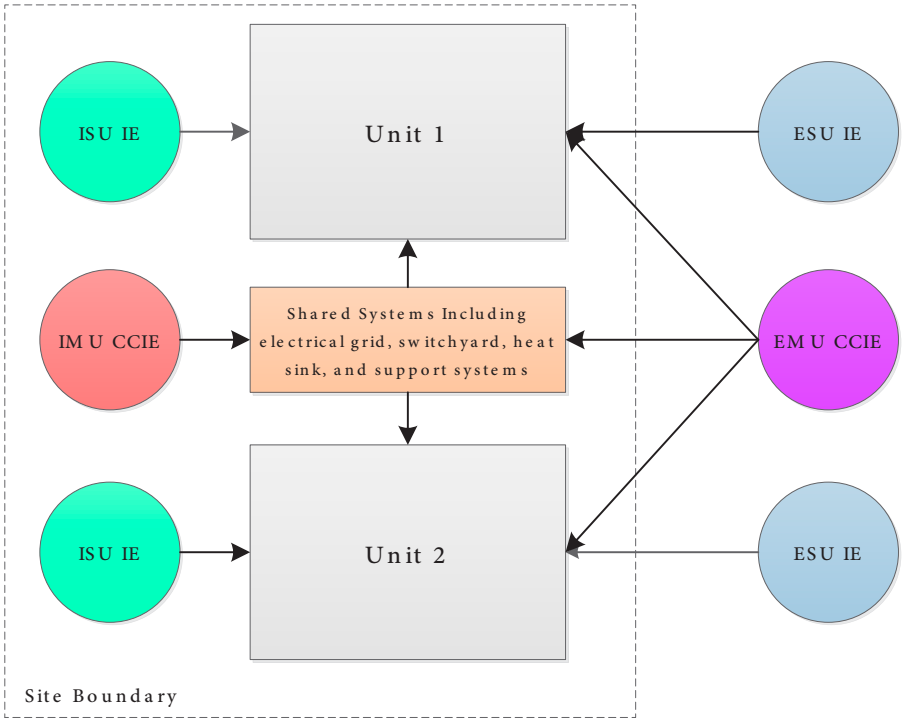
— Identification of initiating events and their causes;
— Classification of the initiating events in terms of which reactor units or combinations of units are challenged by the events;
— Quantification of initiating event frequencies and associated epistemic uncertainties.

Before beginning this step, it is useful to clarify some PSA terminology. The following terms, as they are used in traditional PSAs performed on one reactor at a time, are defined in Ref. [21] as follows:

(a) Initiating event: A perturbation to the plant during a plant operating state that challenges plant control and safety systems whose failure could potentially lead to core damage and/or radioactive material release.
(b) Common cause failure (CCF): A failure of two or more components during a short period of time as a result of a single shared cause.
(c) Common cause initiating event (CCIE): An external or internal event that has the potential for causing an initiating event and an increase in the probability of SSCs that are needed to mitigate the effects of the initiating event.

Examples of CCIEs include total loss of AC power, loss of component cooling water, and internal fires or flooding. Initiating events, CCIEs and CCFs in the context of an MUPSA need to be identified within either the boundary of a single reactor unit or multiple units (see Fig. 11).

In addition to CCIEs, there are other CCFs that do not directly involve an initiating event but involve the failure of two or more components. In a multi-unit plant or site, such CCFs could be confined to a specific reactor unit or facility, or could be components in different reactor units or facilities on the site. Indeed, many examples of multi-unit CCFs have been found in reviews of reactor



Note: CCIE — common cause initiating event; EMU — external multi-unit; ESU — external single unit; IE — initiating event; IMU — internal multi-unit; ISU — internal single unit.

FIG. 11. Definition of initiating event categories for multi-unit probabilistic safety assessment.

operating experience (see Section 2.5). For this publication, two different types of CCF are defined:

(1) Single unit CCF: CCF of two or more components at a single unit either on a single site or multi-unit site.
(2) Multi-unit CCF: CCF of two or more components at different units or facilities on a multi-unit site.

5.2.2. Selection of initiating events for multi-unit probabilistic safety assessments

The basic approach for the selection of internal initiating events for PSA is summarized in para. 5.13 of SSG-3 [5]:

"5.13. A systematic process should be used to identify the set of initiating events to be addressed in the Level 1 PSA. This should involve a number of different approaches including:

(a) Analytical methods such as hazard and operability studies or failure mode and effects analysis or other relevant methods for all safety systems to determine whether their failures, either partial or complete, could lead to an initiating event;
(b) Deductive analyses such as master logic diagrams to determine the elementary failures or combinations of elementary failures that would challenge normal operation and lead to an initiating event;
(c) Comparison with the lists of initiating events developed for the Level 1 PSAs for similar plants and with existing safety standards and guidelines;
(d) Identification of initiating events on the basis of the analysis of operating experience from the plant under investigation and from similar plants;
(e) Review of the deterministic design basis accident analysis and beyond design basis accident analysis and the safety analysis report."

Another possible approach is the screening and grouping of events to simplify the model and to remove events from the model that can be shown to have insignificant risk contributions.

To support an MUPSA, the initiating events and initiating event causes are analysed to determine which could create an internal multi-unit (IMU) CCIE and an internal single unit (ISU) CCIE. As noted earlier, all multi-unit sites are subject to LOOP events that can either be IMU CCIEs or ISU CCIEs, depending on the event. If there are shared structures and systems among the multiple units, the possibilities for an IMU CCIE can quickly multiply.

5.2.2.1. Initiating event categories

In a single unit PSA, it is necessary to capture different categories of initiating events that are characterized by the unique ways that safety functions are challenged as well as the different ways in which the steady state operation of the plant may be disturbed. In an MUPSA, the new dimension of site impacts to be considered is identifying which reactor units or combination of units are impacted by the initiating event. For some causes of initiating events, such as LOOP, failures or disturbances in shared systems, and external hazards, it is necessary to identify the following general initiating event categories:

— Initiating events impacting each reactor unit separately and independently;
— Initiating events impacting specific combinations of reactor units, including the case where all reactor units on the site are impacted;
— Initiating events that may impact two or more reactor units depending on the severity, circumstances or plant conditions at the time of the event.

5.2.2.2. Initiating event screening

For screening out an initiating event from a single unit PSA model, it is necessary to show that its inclusion would not result in a significant contribution to the appropriate single reactor risk metrics (e.g. CDF or LERF). In the ASME/ANS PRA standard [21], a significant accident sequence is one that contributes at least 1% to the CDF or LERF. In the case of an MUPSA, it is necessary to show that inclusion of the event would not result in a significant contribution to the appropriate site risk metrics (i.e. SCDF, MUCDF and SLERF). One such metric is the CDF to two or more reactors concurrently. Using Ref. [21] as guidance, the following screening criteria would be reasonable for an MUPSA of:

(a) A two unit site:
    — An initiating event that impacts only one unit may be screened out if its contribution to CDF_1 is less than 1%.
    — An initiating event that impacts both units may be screened out if its contribution to CDF_2 is less than 1%.
(b) A multi-unit site:
    — An initiating event that impacts two or more units may be screened out if its contribution to MUCDF is less than 1%.

In order to justify the screening out of any initiating event using the above criteria, it is necessary to construct scenarios leading to end states using an appropriate series of assumptions and to have an (often conservative) estimate of the initiating event frequency. It is also necessary to have some estimates of the MUCDF from initiating events expected to be significant contributors to the risk metrics. The assumption is that seismically induced initiating events and LOOP significantly contribute to MUCDF.

If there is an initiating event that only impacts one reactor unit initially and that initiating event leads to an accident or even serious potential for an accident, it is highly likely that the other units on the site would be shut down and not continue operation. In this case, what might start out as a single reactor initiating event and accident sequence may propagate to a multi-unit scenario. For this reason, the list of initiating events for each reactor unit on the site needs to include the occurrence of an accident on another on-site unit. When this is done,

the event sequence that started out as only impacting one unit may propagate into a multi-unit accident.

5.2.2.3. Selection of internal events

In order to perform a good quality PSA of external hazards, such as a seismic or tsunami PSA, it is first necessary to develop the basic logic for accident prevention and mitigation that is part of a good quality PSA of internal events. By the same token, in order to perform a good quality MUPSA that addresses external hazards, it is first necessary to develop a good quality MUPSA for internal events.

All multi-unit sites share a connection to the electrical grid and the ultimate heat sink, and some multi-unit sites share additional structures and systems. Both internally and externally caused initiating events can interact with a multi-unit site in many different ways (see Fig. 11). Each type can cause an initiating event localized to each unit independently (ISU initiating events) and an external single unit initiating event, and lead to a multi-unit CCIE (IMU initiating events) and external, multi-unit CCIEs (single unit CCIEs are not shown in Fig. 11).

An internal event is an initiating event caused by hardware failures or human errors on the site. By convention, LOOP, which may be due to on-site failures, electrical grid disturbances or severe weather, is normally classified as an internal event. All multiple units or multiple facilities are subject to LOOP, and it can be considered an IMU CCIE if it involves a LOOP to multiple units or facilities. Some LOOP events only cause a LOOP to a single unit, and in this instance they are classified as an ISU CCIE. LOOP events are CCIEs because they lead to failure of all equipment powered by non-essential AC electric power and one source of power to each of the essential AC buses in most nuclear power plant designs.

All multi-unit sites are subject to LOOP initiating events, which can impact single units and multiple units, including the case of all of the reactor units on the site. If the multi-unit site involves shared systems or structures, any faults can impact two or more units on the site. Before a meaningful external hazard analysis can be performed, it is critical that these be identified.

For an MUPSA of internal events, it is necessary to rescreen the initiating events for consideration of inclusion into the PSA model because the screening criteria are now based on site risk metrics. The frequency of accidents involving releases from a single reactor unit are now based on a site-year rather than on a reactor-year, which means that for sites with large number of units, the overall likelihood of an independent reactor event is the sum of the individual reactor unit initiating events. The frequency of accidents involving releases from two or more reactor units needs to be separately considered. Following this rescreening,

it is necessary to categorize the initiating events with respect to which reactor units or combinations of reactor units will be affected. For example, LOOP needs to be broken down into events that impact each unit separately and those that impact each combination of reactor units on the site. In addition, initiating events involving support systems and other systems that may be shared among multiple units may need to be subdivided to resolve the reactor unit impact.

5.2.2.4. Selection of internal hazards

Internal hazards, such as fires, flooding and turbine missiles, have the potential to impact each reactor unit separately, as well as to impact two or more reactors on the site, depending on the plant design and layout of structures and systems, and the nature of the internal hazard scenario. If there are existing fire or flood PSAs for the individual reactor units, it is necessary to revisit the selection and evaluation of plant areas and scenarios so that multi-unit impacts can be resolved. Some scenarios involving potential multi-unit effects may have been screened out. However, they now need to be reconsidered. Of particular interest are internal hazard scenarios in common areas or areas with equipment shared by two or more units.

For an MUPSA of internal hazards, it is necessary to rescreen the initiating events because the screening criteria are now based on site risk metrics. The frequency of accidents involving releases from two or more reactor units needs to be considered separately. Following this rescreening, it is necessary to categorize the initiating events with respect to which reactor units or combinations of reactor units will be affected. Some additional modelling of the internal hazard initiating events may be necessary to resolve the reactor unit impacts. For example, fires and flooding in common areas need to be broken down into events that impact each unit separately and those that impact each combination of reactor units on the site. In addition, initiating events involving damage to support systems and other systems shared among multiple units may need to be subdivided to resolve the unique reactor unit impacts.

5.2.2.5. Selection of external hazards

The potential for external, multi-unit CCIEs needs to be considered for all external hazards. Seismic events, external flooding from any source, high winds and wind generated missiles are expected to challenge all of the reactor units and facilities on a site concurrently. Human induced external events, such as aircraft crashes and transport accidents, may have somewhat more localized effects; however, the potential for damage to any shared structures or systems and multi-unit impacts still needs to be considered for all sites. It is important that criteria used

to screen out external hazards be reconsidered to ensure that the potential for multi-unit effects has been adequately addressed. Such screening criteria often consider whether the event has been addressed within the selected design bases. This is problematic because design basis events largely ignore the potential for multi-unit accidents (see Ref. [47] for external event screening criteria).

5.2.3. Treatment of initiating events in the multi-unit probabilistic safety assessment for Seabrook Station

As discussed in Section 3.1, Seabrook Station had a minimal sharing of structures and systems. Each of the two units had a dedicated set of redundant safety systems located in separate structures, including separate mechanical draft cooling towers for the safety related service water systems. The two units did, however, share a common set of intake and discharge tunnels to provide circulating water and non-safety-related service water, and an electrical switchyard that included elements common to both units. Before the MUPSA was performed, a comprehensive list of initiating events was developed for the single unit PSA to include the internal events, and internal and external hazards selected for initiating events and event sequence modelling (see Table 9).

As described by Fleming [33], the next step is to analyse the initiating events and their causes to determine which have the potential to impact both units concurrently or any combination of reactor units or facilities if the site has more than two. In the case of Seabrook, the 58 initiating events selected for the single unit PSA on Unit 1 were analysed in three categories:

— Category A: Events that would impact both units concurrently.
— Category B: Events that, depending on the cause, could impact both units concurrently.
— Category C: Single unit initiating events.

The classification of initiating events is shown in Table 10, which is the same as Table 2 with the addition of the initiating events from Table 9. Of the 58 initiating events, a LOOP, eight seismic events, three tornado and wind events, an external flooding event and a truck crash into the switchyard impact both units concurrently. The loss of the condenser vacuum or service water and turbine missile initiating events impacted both units under certain conditions; the former also on each unit independently.

The initiating events associated with seismic events include a definition of the plant disturbance (e.g. seismically induced LOCA or transient). A seismic event might not cause a plant disturbance. Hence, the occurrence of a seismic event is not necessarily an initiating event. At a two unit station, such as

TABLE 9. SEABROOK INITIATING EVENTS FOR SINGLE UNIT PROBABILISTIC RISK ASSESSMENT*

Initiating event	Designator	Mean frequency events per reactor-year
1. Excessive loss of coolant accident	ELOCA	2.66×10^{-7}
2. Large loss of coolant accident	LLOCA	2.03×10^{-4}
3. Medium loss of coolant accident	MLOCA	4.65×10^{-4}
4. Small loss of coolant accident	SLOCA	1.73×10^{-2}
5. Interfacing systems loss of coolant accident	V	1.84×10^{-6}
6. Steam generator tube rupture	SGTR	1.38×10^{-2}
7. Reactor trip	RT	3.13×10^{0}
8. Turbine trip	TT	1.95×10^{0}
9. Total loss of main feedwater	TLMFW	3.31×10^{-1}
10. Partial loss of main feedwater	PLMFW	2.53×10^{0}
11. Excessive feedwater loss	EXFW	1.38×10^{0}
12. Loss of condenser vacuum	LCV	4.18×10^{-1}
13. Closure of one main steam isolation valve	1MSIV	3.54×10^{-1}
14. Closure of all main steam isolation valves	AMSIV	2.44×10^{-3}
15. Core power excursion	CPEXC	2.73×10^{-2}
16. Loss of primary flow	LOPF	5.60×10^{-1}
17. Steam line break inside containment	SLBI	4.65×10^{-4}
18. Steam line break outside containment	SLBO	6.04×10^{-3}
19. Main steam relief valve opening	MSRV	4.94×10^{-2}
20. Inadvertent safety injection	SI	6.40×10^{-2}
21. Loss of off-site power	LOSP	1.35×10^{-1}
22. Loss of one DC bus	L1DC	1.68×10^{-2}
23. Total loss of service water	LOSW	2.52×10^{-6}

TABLE 9. SEABROOK INITIATING EVENTS FOR SINGLE UNIT PROBABILISTIC RISK ASSESSMENT* (cont.)

Initiating event	Designator	Mean frequency events per reactor-year
24. Total loss of primary component cooling water	LPCC	1.39×10^{-6}
25. Seismic 0.7g large loss of coolant accident	E.7L	1.00×10^{-6}
26. Seismic 1.0g large loss of coolant accident	E1.0L	8.20×10^{-7}
27. Seismic 0.2g transient event	E.2T	3.60×10^{-4}
28. Seismic 0.3g transient event	E.3T	1.12×10^{-4}
29. Seismic 0.4g transient event	E.4T	4.31×10^{-5}
30. Seismic 0.5g transient event	E.5T	1.99×10^{-5}
31. Seismic 0.7g transient event	E.7T	1.97×10^{-5}
32. Seismic 1.0g transient event	E1.0T	2.47×10^{-6}
33. Fire in cable spreading room: LPCC	FSRCC	3.60×10^{-6}
34. Fire in cable spreading room: AC power loss	FSRAC	5.19×10^{-7}
35. Fire in control room: LPCC	FCRCC	9.00×10^{-6}
36. Fire in control room: LOSW	FCRSW	2.10×10^{-6}
37. Fire in control room: AC power loss	FCRAC	2.10×10^{-6}
38. Fire in electrical tunnel 1	FET1	3.40×10^{-4}
39. Fire in electrical tunnel 3	FET2	1.70×10^{-4}
40. Fire in PCC area	FPCC	4.20×10^{-6}
41. Fire in turbine building: LOOP	FTBLP	6.40×10^{-4}
42. Turbine missile (steam line break)	TMSLB	8.30×10^{-5}
43. Turbine missile (LLOCA)	TMLL	7.44×10^{-8}
44. Turbine missile (LCV)	TMLCV	8.30×10^{-5}
45. Turbine missile: Control room impact	MTCR	3.98×10^{-7}
46. Turbine missile: Condensate storage tank impact	TMCST	6.09×10^{-8}

TABLE 9. SEABROOK INITIATING EVENTS FOR SINGLE UNIT PROBABILISTIC RISK ASSESSMENT* (cont.)

Initiating event	Designator	Mean frequency events per reactor-year
47. Turbine missile: LPCC	TMPCC	1.27×10^{-8}
48. Tornado missile (electrical system faults)	MELF	3.40×10^{-10}
49. Tornado missile (electrical and PCC system faults)	MPCC	5.46×10^{-9}
50. Tornado missile (control room impact)	MCR	5.80×10^{-9}
51. Aircraft missile (containment building impact)	APC	1.21×10^{-8}
52. Aircraft missile (control room impact)	ACR	1.39×10^{-7}
53. Aircraft missile (primary auxiliary building impact)	APAB	2.00×10^{-7}
54. Flooding in turbine building: LOSP	FLLP	3.20×10^{-4}
55. Flooding in turbine building: LOSP and one vital switchgear room	FL1SG	2.50×10^{-6}
56. Flooding in turbine building: LOSP and two vital switchgear rooms	FL2SG	8.50×10^{-8}
57. External flooding: LOSW	FLSW	1.60×10^{-6}
58. Truck crash into transmission lines	TCTL	2.76×10^{-4}

* Reproduced courtesy of ABS Group [13].

Seabrook, it can lead to a seismically induced transient or seismically induced LOCA on either unit or on both units.

Although Seabrook had a minimal sharing of structures and systems, other sites have more extensive sharing. In this case, the classification of single versus multi-unit initiating events, and their frequencies of occurrence, would be different.

To simplify the model, the key assumption made in the Seabrook PSA was that both reactor units were at-power when each initiating event occurred. Several years later, the Level 3 PSA was extended to consider accidents initiating during LPSD plant operating states. By then, however, the construction of Unit 2 had already been cancelled, obviating the need to perform an MUPSA with LPSD included.

TABLE 10. CLASSIFICATION OF INITIATING EVENTS FOR THE INTEGRATED SEABROOK RISK MODEL

Category	Initiating event
(A) Events impacting both units concurrently	Loss of off-site power (21) Seismic events (25–32) Tornado and wind (48–50) External flooding (57) Truck crash into switchyard (58)
(B) Events impacting both units concurrently under certain conditions	Loss of condenser vacuum (12) Loss of service water (23) Turbine missile (42–47)
(C) Events impacting each unit independently	Loss of coolant accident (1–6) General transients (7–20) Loss of component cooling (24) Loss of one DC bus (22) Internal fires (33–41) Internal flooding (54–56) Aircraft crash (51–53)

Note: The numbers in parentheses refer to the initiating events in Table 9.

In the Fukushima Daiichi accident, the plant operating states of the six units had a major impact on the station. Units 1–3 experienced core damage and were operating at-power when the earthquake hit, while Units 4–6 were in a shutdown state. The reactor core of Unit 4 had been offloaded to a spent fuel storage pool at the time of the accident. That unit suffered from the same level of degradation as Units 1–3, which included a total loss of AC and DC power, and would have likely experienced core damage had it been in operation. Core damage at Units 5 and 6 was averted due to the successful operation of one EDG that was not flooded. However, that outcome may not have been so favourable if one or both of those units had been in operation. A summary comparison of the different ways that initiating events are analysed in a single unit PSA and MUPSA is provided in Table 11.

TABLE 11. COMPARISON OF INITIATING EVENT TREATMENT IN SINGLE AND MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT

Characteristic	Single unit PSA	MUPSA
Completeness objective	Capture all events that make significant contributions to single unit risk metrics (CDF, LERF, RCF, CCDF)	Capture all events that make significant contributions to site risk metrics (SCDF, MUCDF, SLERF, CPMA, SRCF, SCCDF)
Internal event categories	Events with unique impact on reactor safety functions (transients, LOCAs, steam generator/heat exchange faults), LOOP Support system transients	Single unit internal events impacting each reactor unit or radionuclide source separately LOOP events impacting each combination of two or more reactor units or radionuclide sources Faults in shared systems impacting each combination of two or more reactor units or radionuclide sources
Internal hazards	Flood induced initiating events Fire induced initiating events Other hazard induced initiating events	Single unit or radionuclide source internal events impacting each reactor unit or radionuclide source separately Internal events in common areas impacting each combination of two or more reactor units or radionuclide sources
External hazards	Seismically induced initiating events Tsunami/external flood induced initiating events High wind induced initiating events Other external induced initiating events	Single unit, external events impacting each reactor unit or radionuclide source separately External events impacting each combination of two or more reactor units or radionuclide sources
Initiating event frequency basis	Events per reactor-calendar-year	Events per site-calendar-year

Note: CCDF — complementary cumulative distribution function; CDF — core damage frequency; CPMA — conditional probability of multi-unit accident; LERF — large early release frequency; LOCA — loss of coolant accident; LOOP — loss of off-site power; MUCDF — multi-unit core damage frequency; MUPSA — multi-unit probabilistic safety assessment; PSA — probabilistic safety assessment; RCF — release category frequency; SCCDF — complementary cumulative distribution function; SCDF — site core damage frequency; SLERF — site large early release frequency; SRCF — site release category frequency.

5.2.4. Examples of initiating events with potential multi-unit impacts

A key element of the initiating event analysis for multi-unit sites is the identification of initiating events that impact multiple reactor units concurrently. From the lessons learned from the Seabrook MUPSA, the types of event that have the highest potential for creating concurrent initiating events on two or more reactor units at the same site normally involve an extended or non-recoverable LOOP caused by an external hazard.

5.2.4.1. Loss of off-site power

Based on an analysis of service data, most occurrences of LOOP on a multi-unit site impact all of the units on the site. This does not necessarily mean that all such events involve LOOP to all of the units but that they at least challenge all of the units to maintain off-site supply to the safety related AC buses. Although there are examples of single unit LOOP events on multi-unit sites, they are relatively rare. Most grid and weather related (and some plant and switchyard related, too) LOOP events will challenge all of the reactors on the site, even though some units may be able successfully to prevent such a disturbance from creating a LOOP condition. The events at Maanshan nuclear power plant show that faults in a single electrical breaker may result in electrical disturbances that contribute to a station blackout [57]. This is an important category of multi-unit CCIEs because it applies to all multi-unit sites, even those with little or no sharing of structures and systems on the site. Hence, it is necessary to re-examine the LOOP frequencies for existing single unit PSAs to facilitate a breakdown into single and multi-unit events.

5.2.4.2. External events

Virtually all external events involve challenges to all units on multi-unit sites. Similar to LOOP, this holds irrespective of the extent of sharing of structures and systems, although such sharing could magnify the consequences of the events by providing another means of impacting multiple reactor units. Examples include:

— Seismic events, including seismically induced LOOP, LOCAs, fires and floods;
— External flooding due to tsunamis, storm surges, river flooding and dam failures;
— High winds and wind generated missiles;
— Transport accidents.

Seismic events, including seismically induced LOOP and LOCAs, were found to be the dominant cause of multi-unit accidents at Seabrook, which had minimal sharing of structures and systems. External flooding and high winds and associated wind generated missiles are obviously site wide hazards and, just as seismic events, would challenge all units. Transport accidents (e.g. aircraft crashes) are more localized and may have therefore somewhat less potential for impacting multiple reactor units. Hence, the importance of this hazard may be greatly amplified by the sharing of structures and systems. As a final note, external hazards may cause a LOOP or loss of heat sink, which in turn may impact multiple reactor units. In addition to determining which events involve single or multiple units, there is the consideration whether the loss induced by the external hazard is recoverable. The off-site power recovery curve used to determine the time to recover the power loss can be different for internal and external events. The combination of LOOP frequency and non-recovery probability in time to prevent core damage may still be significant, even when the initiating event frequency is small. Each external hazard can give rise to different initiating events (e.g. an external flood inducing LOOP or loss of ultimate heat sink). By convention, current PSA practice defines initiating events at the point of the plant disturbance, whereas hazards are possible causes of an initiating event.

5.2.4.3. Internal events involving shared structures and systems

If the reactor units on the site do not share structures and systems, there is a reduced potential for internal events (e.g. fires and flooding) to create multiple, concurrent initiating events, as was the case in the Seabrook PSA. However, as discussed in Sections 2 and 3, there have been PSAs completed for multi-unit sites with shared structures and systems in which internal fires or flooding have been found not only to dominate CDF but also MUCDF. This is also true for initiating events such as dual unit loss of service water and dual unit station blackout.

Irrespective of the extent of sharing structures and systems, all multi-unit sites are subject to events that can create concurrent initiating events on two or more reactor units. If there is sharing, the potential is obviously increased relative to cases without any sharing of structures and systems.

Even when a hazard causes an initiating event on only one reactor unit, there is still the potential for a multi-unit accident if an accident on the affected unit creates a challenge to the other units. These domino effects are considered in the event sequence model discussed in Section 5.3.1.

5.2.5. Estimation of initiating event frequencies

5.2.5.1. Event frequency basis

In a PSA carried out for a single unit, the frequency basis for initiating events and accident sequences is events per reactor-calendar-year [21, 46]. For an MUPSA, the appropriate frequency basis for both initiating event and accident sequence frequency is events per site-year. This approach facilitates the aggregation of risk of all sources on the site, including the risk from single reactor accidents as well as those involving two or more reactors or facilities. Another justification is that risk criteria derived from safety goals apply to individuals in the vicinity of a nuclear power plant. To compare the results of the risk assessment to these criteria, aggregations of this risk using site — and not reactor — based risk metrics is needed.

5.2.5.2. LOOP initiating event frequency assessment

A LOOP study performed for the Palisades nuclear power plant, United States of America, offers some useful insights for MUPSAs, even though the analysis was for a single unit site.

As discussed more fully in Ref. [58], a study was performed to analyse site aspects of quantifying initiating event frequencies for LOOP. Service experience from 1980 to 2008 was collected and analysed to develop LOOP frequencies for an update of the Palisades PSA. Various sources of information were used, including surveys sponsored by the Electric Power Research Institute [59–61], a survey sponsored by the NRC [62] and plant specific operating experience at Palisades. The results identified 39 events involving LOOP:

(a) A total of 33 LOOP events in which LOOP impacted only one reactor, including four events at single reactor sites due to grid or weather related causes that could have impacted multiple reactor units if sited there.
(b) Five site events involving LOOP impacting two reactors at the same time.
(c) North-eastern US blackout in August 2003 involving LOOP impacting nine reactors and seven sites. This event affected the grid at Palisades but did not cause LOOP.

In most analyses of LOOP initiating event frequency, it was common to analyse the events and frequencies in the following categories of LOOP:

— Plant centred events;
— Switchyard centred events;

— Grid related events;
— Weather related events.

The primary motivation for this breakdown is based on the use of different off-site power recovery models for the categories. In Ref. [62], there is an additional breakdown of whether the plant affected by LOOP was in operation or shutdown. It is standard practice in PSA to treat each reactor event as though it had occurred independently; in the sense that if two or more reactor plants were affected by a common cause LOOP event, the events are counted as though they were multiple, independent reactor events. Thus, a site LOOP event that impacts two reactors is counted as two reactor LOOP events. In addition, there does not appear to be a consistent treatment of plant to plant variability in the statistical analysis of uncertainties in LOOP frequency estimates, including in Ref. [62]. The traditional approach to modelling LOOP can be viewed as forcing the data analysis to fit an overly simplified model — namely, that the evaluation is performed one reactor at a time. The data collected for the Palisades PSA update suggest a different approach to categorizing LOOP events:

— Reactor related: The event only impacted a single reactor.
— Site related: The event impacted all of the reactors at a given site.
— Region related: The event impacts all of the reactors in an entire region.

The traditional approach to analysing data, and the method used in Ref. [62], is to add up all 52 of the reactor events and then treat them as 52 independent events, each affecting only one reactor. In the update to the Palisades PSA, the data were treated as 39 separate events, each impacting a different set of reactors in the dataset (29 reactor events, 9 site events and 1 region event). A summary of the data partitioning for LOOP frequencies is provided in Table 12.

Treating the data as 52 reactor events in 2832 reactor-years, while acceptable for a point estimate of event frequency, leads to a non-conservative treatment of uncertainty. The reactor event method overstates the frequency supported by the evidence; and when it is applied in Bayes' updating, the result is an understatement of the range of uncertainty, which is non-conservative. This shows how a single reactor at a time mindset can lead to incorrect treatment of the data. For an integrated site risk assessment on a multi-unit site, the various types of LOOP event cannot just be blended together as independent reactor LOOP events, as they are in the traditional PSA approach. Rather, they need to be treated separately, so that the distinct contribution from single unit LOOP events and multi-unit LOOP events can be modelled appropriately (see Table 13 for alternative analysis approaches).

TABLE 12. SUMMARY OF A LOSS OF OFF-SITE POWER EVENT AND EXPOSURE DATA [58]

Category	No. of events	No. of reactor events	Event exposure	Reactor event exposure (reactor-years)
Reactor related	29	29	2832 reactor-years	2832
Site related	9	14	1750 site-years	2832
Region related	1	9	290 region-years	2832
Total	39	52	—	2832

Method A is used in most current PSA models, dividing LOOP events into the common categories. In some models, each is treated as a separate initiating event and different curves for the probability of non-recovery of off-site power versus time are used to analyse the station blackout sequences. Using the methods in Ref. [62], a constrained non-informative prior method, recommended in Ref. [63], is used to characterize uncertainty. These distributions are then normally used as prior distributions, and plant specific data are applied in a Bayes' update process (also discussed in Ref. [63]). A limitation of this approach is that it does not address plant to plant variability. Some PSAs do not break down LOOP into separate events and just use the total LOOP distribution that is obtained by combining the separate distributions via Monte Carlo simulation.

Method B characterizes uncertainty better, as it addresses the site to site variability in the data and thus yields a wider uncertainty distribution as measured by the range factors. However, both Methods A and B are intended for use with the traditional PSA approach, in which each reactor unit is modelled separately as though it were an independent entity.

A more appropriate approach to modelling LOOP events for an MUPSA is to break down LOOP events into reactor centred, site centred and region centred. Only the reactor centred events are assumed to impact each reactor unit separately, as both the site centred and region centred events would cause LOOP across the site and challenge the on-site electrical systems of all site facilities concurrently. Region centred events are separated from site centred events because they would typically take much longer to recover power.

These are important insights because LOOP is a generic challenge to all nuclear power plants worldwide. Whether or not the multi-unit sites have shared systems, all of the reactor units and other facilities will be affected. The

TABLE 13. LOSS OF OFF-SITE POWER (LOOP) INITIATING EVENT FREQUENCIES USING DIFFERENT METHODS [58]

LOOP type	Point estimate	LOOP frequency per calendar-year				RF 1	RF 2
		Mean	5%-tile	50%-tile	95%-tile		
				Method A			
Plant	7.06×10^{-4}	8.83×10^{-4}	3.47×10^{-6}	4.02×10^{-4}	3.39×10^{-3}	31.3	8.4
Switchyard	5.30×10^{-3}	5.47×10^{-3}	2.15×10^{-5}	2.49×10^{-3}	2.10×10^{-2}	31.3	8.4
Grid	9.89×10^{-3}	1.01×10^{-2}	3.96×10^{-5}	4.58×10^{-3}	3.87×10^{-2}	31.3	8.5
Weather	2.47×10^{-3}	2.65×10^{-3}	$1.0\,4\times 10^{-5}$	1.20×10^{-3}	1.02×10^{-2}	31.3	8.5
Total	1.84×10^{-2}	1.90×10^{-2}	2.51×10^{-3}	1.42×10^{-2}	5.16×10^{-2}	4.5	3.6
				Method B			
Reactor	1.84×10^{-2}	2.63×10^{-2}	6.86×10^{-4}	1.17×10^{-2}	9.50×10^{-2}	11.8	8.1

Note: Method A: Traditional probabilistic safety assessment method, constrained non-informative gamma distribution, no plant to plant variability, LOOP broken down into four categories with separate LOOP recovery models; Method B: Single reactor site method with site to site variability. RF — release frequency.

modelling of the site response to LOOP events, whether caused by internal or external events, is an important element of all site safety assessments.

5.2.5.3. LOOP example for a two unit site

To illustrate the steps in estimating the initiating event frequencies for an MUPSA, LOOP at a site with two identical reactor units is considered. Based on information from Table 12, LOOP events for a two unit site can be analysed as follows:

$$F_{\text{Site}} = F_{\text{M}} + 2F_{\text{S}}$$

$$f_{\text{M}} = \frac{F_{\text{M}}}{F_{\text{M}} + F_{\text{S}}}$$

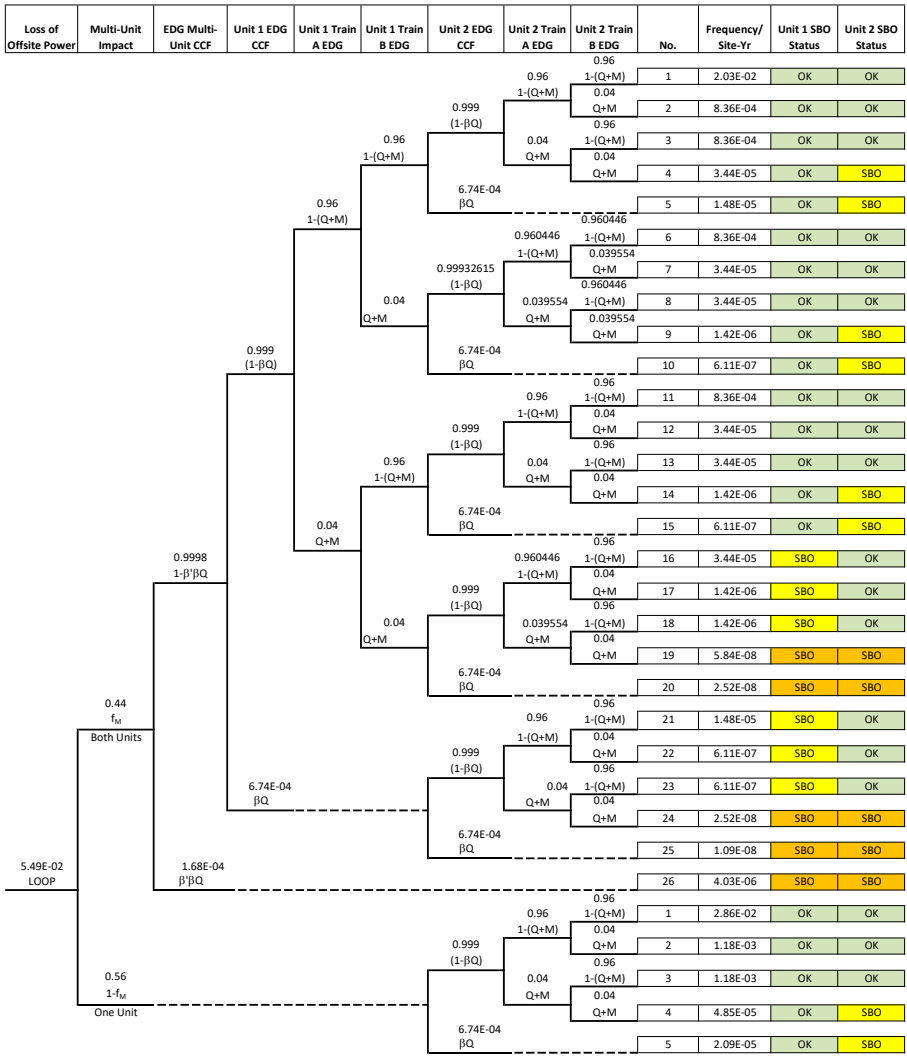
where

F_{Site} is the frequency of LOOP at a two unit site, per site-calendar-year;
F_{M} is the frequency of site and region based events involving LOOP at both units at a two unit site, per site-calendar-year;
F_{S} is the frequency of reactor based events involving LOOP on only one reactor unit, per reactor-calendar-year;

and f_{M} is the fraction of LOOP events at a two unit site involving LOOP at both units.

In traditional PSAs, which are performed on each reactor separately, the initiating event frequencies are analysed on a reactor basis, and each unit is analysed separately for a multi-unit site. In an MUPSA, it is necessary to resolve which events impact each reactor separately and independently, and which impact both units concurrently. This requires careful analysis of the industry data, which can come from a mixture of sites with different numbers of reactors on each site. An example analysis of LOOP and station blackout at a two unit site, similar to that which was performed for Seabrook Station, is presented here to demonstrate initiating event analysis and some aspects of event sequence modelling for an MUPSA. The example is quantified using data for US nuclear plant PSAs, and an event tree is shown in Fig. 12.

The event tree models the occurrence of both multi-unit LOOP and single unit LOOP events at a two unit site, and the response of EDGs at each unit in a manner that is similar to the Seabrook PSA. Like Seabrook, each reactor unit has two EDGs. The event tree models independent failures and maintenance unavailability for all four EDGs as well as their CCFs. Both single unit and multi-unit CCFs are modelled in a manner similar to the Seabrook study. Data



Note: CCF — common cause failure; EDG — emergency diesel generator; SBO — station blackout. See Table 14 for a definition of the parameters shown here.

FIG. 12. Event tree for multi-unit loss of off-site power and station blackout.

to quantify the mean point estimates of the event sequences in the event tree are based on US industry generic sources in Table 14.

These data parameters are considered realistic for a currently operating two unit nuclear power plant. It should be noted that a 24 hour mission time was assumed for the EDGs in this example. In future MUPSAs, the mission time

for the EDGs needs to be consistent with the expected time for the recovery of off-site power, which includes considerations of the cause of LOOP, whether it is recoverable and emergency measures to find alternative sources of AC power.

The event tree shows the split fractions and parameters used to quantify the event sequences for tractability back to the parameter values in Table 14. The end states in this event tree identify whether there is a station blackout of either unit, both units or neither unit on this two unit site. The key results are shown in Table 15.

When comparing these results against those of typical PSAs, the two key differences are: (i) the frequency of a single unit LOOP is increased to reflect that this is a site based frequency; and (ii) there are different results for LOOP events and station blackout events involving single units and both units in the two unit site example. While the frequency of the dual unit station blackout is significantly smaller than for a single unit, it is sufficiently high to avoid screening out of an MUPSA. It should be noted that this example did not include the probability of non-recovery of off-site or on-site power, nor did it include other components (e.g. breakers, and fuel transfer pumps) the failure or unavailability of which could contribute to a station blackout sequence at one or multiple units. The purpose of the simplified example is to illustrate the process of modelling initiating events and accident sequences in a MUPSA and to provide some insights into the relative frequencies of single and multi-unit LOOP and station blackout events.

5.2.5.4. Seismically induced loss of coolant accident example

LOOP is typically included as part of the internal events analysis in a PSA, even though the predominant causes, including severe weather and grid disturbances, are due to events external to the site. LOOP is also considered to be one of the consequences of many external hazard analyses, such as seismic events, external flooding and high winds. The many different initiating events seismic events can cause depend on the combination of components and structures that are damaged, as well as the plant response to these failures, which may involve additional failures independent of the seismic event but could contribute to an accident on one or more reactor units. As with the previous example, this one is simplified in relation to that which would be covered in a full PSA. The example in Annex I illustrates the delineation of single reactor and multiple reactor initiating events in response to a seismic event at the same two unit plant, based on the Seabrook design.

In Annex II, there is another example of a dual unit, seismically induced LOCA initiating event that provides the relationship between the seismic

TABLE 14. PARAMETER DATA FOR LOSS OF OFF-SITE POWER AND STATION BLACKOUT EXAMPLE

Model parameter	Assumed value	Comment
F_M = frequency of site and region based events involving LOOP at both units at a two unit site	2.39×10^{-2} per site-year	Table 12 data for region based and site based LOOP events
F_S = frequency of reactor based events involving LOOP on only one reactor unit	1.55×10^{-2} per reactor-year	Table 12 data for reactor based LOOP events Table 12 was developed for a single unit site, so 1.55×10^{-2} is used in this example for both reactor units
F_{Site} = frequency of LOOP at a two unit site	5.49×10^{-2} per site-year	$F_{Site} = F_M = 2F_S$
f_M = fraction of LOOP events at a two unit site involving LOOP at both units	0.435	$f_M = \frac{F_M}{F_M + F_S}$
λ_s = EDG failure rate to start or to load and run for 1 h	7.45×10^{-3} per demand	NUREG/CR-6928 [64] based on US nuclear power plant service data
λ_r = EDG failure rate to run after first hour	8.48×10^{-4}/h	NUREG/CR-6928 [64] based on US nuclear power plant service data
T = mission time	23 h after the first hour	Model assumption
M = EDG maintenance unavailability	1.26×10^{-2}	NUREG/CR-6928 [64] based on US nuclear power plant service data
Q = EDG failure probability	$Q = \lambda_s + \lambda_r T$	Standard model for a standby component
β = fraction of EDG failures involving common cause failures shared with another EDG	0.025	Assumed for this example

TABLE 14. PARAMETER DATA FOR LOSS OF OFF-SITE POWER AND STATION BLACKOUT EXAMPLE (cont.)

Model parameter	Assumed value	Comment
β' = fraction of EDG common cause failures involving failure of all four EDGs on both units	$\beta' = \frac{4n_4}{4n_4 + 2n_2}$	Multiple Greek letter model equation for non-staggered testing [65], $\beta' = 0.25$
n_2 = No. of EDG common cause events with two component failures on one site	6	Seabrook PSA, one out of seven common cause events of EDGs would impact all four EDGs at a multi-unit site
n_4 = No. of EDG common cause events with four component failures on two sites	1	

Note: EDG — emergency diesel generator; LOOP — loss of off-site power; PSA — probabilistic safety assessment.

TABLE 15. LOSS OF OFF-SITE POWER EVENT TREE QUANTIFICATION RESULTS

LOOP event tree parameter	Value
Total frequency of all modelled event sequences (per site-year)	5.49×10^{-2}
Frequency of no SBO (per site-year)	5.47×10^{-2}
Frequency of SBO of one unit only (per site-year)	1.76×10^{-4}
Frequency of SBO of both units (per site-year)	4.15×10^{-6}
Conditional probability no SBO given site LOOP	0.997
Conditional probability of SBO of one unit only given site LOOP	3.21×10^{-3}
Conditional probability of SBO of both units given site LOOP	7.55×10^{-5}

Note: LOOP — loss of off-site power; SBO — station blackout.

common cause parameter α, defined in Annex I, and correlation coefficients used to generate the component fragilities.

A case study performed by the Japan Nuclear Energy Safety Organization to evaluate the impact of seismic fragility correlation in the evaluation of multi-unit seismic risks at a Japan nuclear power plant site is presented in Ref. [66].

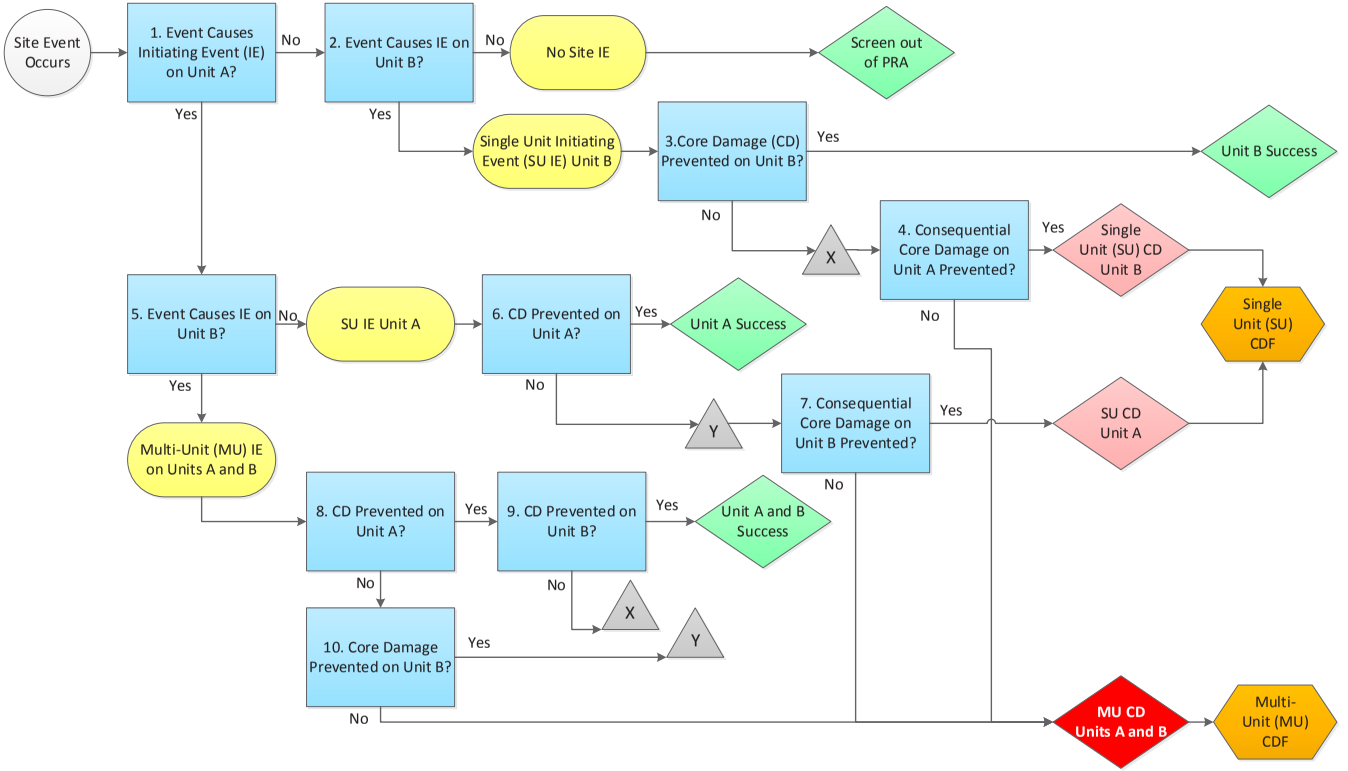
5.3. LEVEL 1 EVENT SEQUENCE MODEL

5.3.1. Event sequence diagram

An event sequence diagram for a two reactor unit site safety assessment is shown in Fig. 13. It is for a general event (internal or external) at the site which may or may not lead to an initiating event at either one unit or both concurrently. The logic resolves whether the event leads to an initiating event on each unit separately or on both units concurrently and how the various paths through the diagram lead to the estimation of the various components of the SCDF, one component for single unit accidents and one for those impacting both units concurrently. Identified as Unit A and Unit B, the reactor units can be identical or differ with any degree of sharing of SSCs.

The path across the top of the diagram (Boxes 1 and 2) is when the event does not cause an initiating event on either unit. In the second row, there is an initiating event only on Unit B, with the outcomes of core damage on Unit B being either mitigated (Unit B success) or, when not, whether consequential (i.e. causal) core damage on Unit A has been prevented (Box 4). This is the domino effect when the occurrence of core damage on one unit represents, in effect, an initiating event and a challenge to safety functions on the other unit. The end state of Box 4 is either a single unit or multi-unit core damage event. This type of consequential multi-unit event was not considered at Seabrook, but it needs to be considered in future MUPSAs. At a minimum, a core damage event on one unit would necessitate the shutdown of the other unit and a challenge to the accident management of the site, which would include mitigating the consequences of the core damage and preventing core damage on the other unit or units. Boxes 5–7 follow the same logic, but this time the initiating event occurs at Unit A, and hence with identical outcomes. Boxes 8–10 is when the event causes an initiating event on both units.

Not shown in the diagram are additional details to resolve the plant operating states at the time of the event, which would impact the definition of each reactor unit's initiating event, its conditional probability of occurrence and the conditional probability of core damage. For a two unit site, there are four possibilities for the site configuration of operating states if it is assumed that each



Note: CD — core damage; CDF — core damage frequency; IE — initiating event; MU — multi-unit; PRA — probabilistic risk assessment; SU — single unit.

FIG. 13. Event sequence diagram for a site event at a two reactor unit site.

unit is either in a power generation state or an LPSD state: both units operating; two combinations of one unit operating and the other shutdown; and both units in a shutdown state. During the Fukushima Daiichi accident, only three units were operating, and those units experienced core damage [1]. Protecting the cores of all six units had a very significant impact on the resources available to manage the accident. An event sequence diagram can show the top level logic of an event sequence model for a multi-unit site and provides guidance for the development of the event tree and fault tree logic needed for quantification.

5.3.2. Single unit accidents

The logic for single unit accidents (Boxes 3 and 6) is essentially what is normally done in a single unit PSA. The major difference here is that only those initiating events that impact each unit separately are quantified. As is common with current MUPSAs, the additional capabilities and redundancies available to prevent and mitigate a single reactor accident need to be considered in this part of the MUPSA model.

5.3.3. Multi-unit accidents

The two types of multi-unit accident to consider are: (i) accidents from initiating events as a result of a common hazard (see Boxes 8–10 in Fig. 13); and (ii) accident sequences leading to consequential (i.e. causal) core damage (see Boxes 4 and 7 in Fig. 13). Although the dual unit initiating event responses are shown in three boxes, the event sequence logic needs to be developed in an integrated manner. While this is where the major differences are between a single unit and a multi-unit event sequence model, the process for developing the model is essentially the same. However, the end states of this model include core damage to both units as well as to each unit individually.

The consequential (i.e. causal) core damage events are modelled just like event sequence models in a single unit PSA, except here the initiating event involves an accident with the other unit. This is not an ordinary initiating event because it imposes many dependencies not normally encountered in a typical PSA. Such dependencies include the challenges imposed by the general site emergency that is declared, which will greatly restrict the operator actions to maintain safety functions and may involve radiological contamination of the site.

Since the modelling becomes more complex the greater the number of units, the examples here only consider a two unit plant. In principle, accidents could occur with any combination of reactor units, so assumptions need to be made for larger sites to simplify the modelling. Some nuclear power plant have as many as seven reactor units, and it is likely that a larger number of units will appear

in the future. Small modular reactor designs being considered can have as many as 12 reactor units. Modelling these more complex configurations is analogous to CCF modelling of redundant components. In the beta factor model [67], the earliest CCF model, CCFs are assumed always to impact the entire set of redundant components. In an MUPSA for a large site, a similar assumption would be accidents impact all of the units or each unit individually. More complex common cause models, such as the multiple Greek letter (MGL) model [68] and the alpha factor model [65], were developed for larger configurations of components; however, the practical limit of these models is four components. In the future, a beta factor database could first be established by including accidents involving all or single reactor units before taking on the added complexity of the additional multi-unit combinations.

All multi-unit sites are subjected to LOOP events that impact all of the units on the site. Some multi-unit sites also have some shared structures and systems (e.g. electric power, cooling water and ultimate heat sink). To construct a multi-unit event sequence model that accounts for multi-unit accidents, it is best to start by developing a multi-unit model for LOOP and station blackout, as this will be a significant risk contributor for all multi-unit sites. For plants with shared structures and systems, the event sequence model for initiating events and accident sequences associated with these shared systems then needs to be developed with due emphasis on the loss of the ultimate heat sink. Once these models are developed, the remaining work to develop the PSA event sequence model for seismic events and other external hazards can progress more efficiently.

5.4. LEVEL 1 SYSTEMS AND DATA ANALYSIS

The systems and data analyses required for an MUPSA are very similar to the traditional, single reactor PSA model. The key difference is the modelling of CCFs in the system models and the estimation of the corresponding CCF parameters. If there are identical, redundant components and systems that are replicated on multiple reactor units, the possibility for a CCF that may impact components on different units needs to be considered. Common cause models used in traditional, single unit PSAs were originally developed for arrays of redundant components within a single nuclear power plant. The most common models used in current PSAs for this purpose are the beta factor model [67], the MGL model [68] and the alpha factor model [65]. An assumption built into these models is an assumption of symmetry; that is, the assumption that the probability of failure of any combination of N redundant components is the same. In a system of four redundant components, for example, the MGL and alpha models would assume that any pair of components and any combination of three components would have

the same CCF. This assumption helps to keep the number of different parameters to be quantified at a practical level.

A very special type of asymmetry was encountered in the Seabrook MUPSA, and the CCF models and data analysis were specialized to account for it. Seabrook employed many 2 × 100% capacity redundant components in the safety systems (i.e. EDGs). Each identical reactor unit had two identical EDGs, which meant a total of four EDGs at the two unit site. A specialized version of the MGL model was developed to reflect that each pair of redundant components within a unit were subjected to a relatively high degree of CCF potential, and CCFs across the units were possible but much less likely than pairs of components in different units. This was based on insights from a review of service data and the fact that maintenance cycles that provide an important common cause coupling mechanism are highly synchronized within a unit but not across. In this situation, there are redundant sets of identical components in which common cause groups can be defined that cross unit boundaries. In these configurations, there are certain classes of CCF that could impact all four components, and still other types of CCF that would be limited to those within a single unit. Examples of these might include maintenance induced failures that are highly dependent within a unit but whose maintenance schedules across units are desynchronized due to coordination of refuelling cycles. The simplified common cause model developed for the Seabrook MUPSA is presented in Fig. 14, which recognizes two types of common cause event: Type 1 occurs within each unit; and Type 2 occurs across all four components in both units.

Simplifying in relation to the basic MGL and alpha models, the common causes in the model impact two components in different units, omitting events impacting three components. Instead of including all possible common cause events that could impact two, three or all four components, the model uses a two tier grouping process: two groups of two components each for intra-unit common cause effects and one group of four components for inter-unit effects. Quantification of this model is discussed below, and the assumptions may be reflected in the evaluation of service data to estimate the common cause parameters.

As discussed in Section 2.5, there have been numerous examples of CCFs involving failures of components in different units on multi-unit sites. It is important to note the formulas used to calculate CCF probabilities. The MGL model is consistent with the full set of common cause events and with the assumption that common cause events act symmetrically on the components in the common cause group. When one or more common cause basic events are omitted to simplify the model, it is necessary to analyse the data with a consistent set of modelling assumptions. This principle is illustrated in Table 16 for the asymmetric model and described in Fig. 14 for a four component group at a two unit station, where only selected common cause events are included in the fault tree. The

parameters are expressed in Q_k, which is the probability of the common cause event that fails k components (independent failure if $k = 1$).

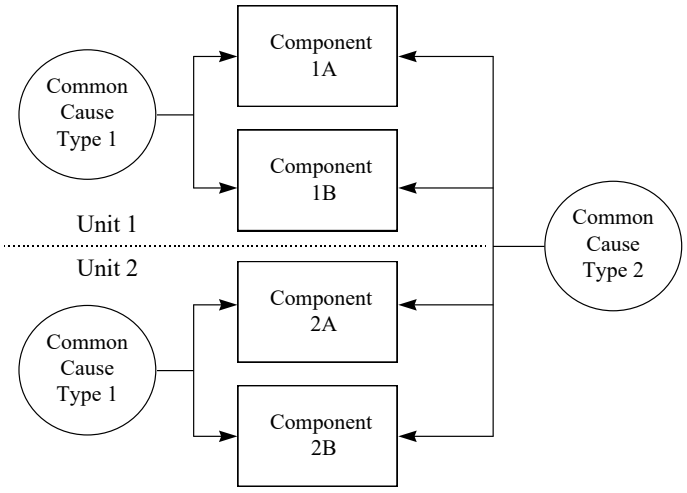


FIG. 14. Multi-unit common cause failure mode.

TABLE 16. COMPARISON OF STANDARD AND SIMPLIFIED MULIPLE GREEK LETTER (MGL) MODELS FOR A FOUR COMPONENT GROUP

Parameter	Fully developed four component model (standard MGL model)	Asymmetric four component model for a two-unit station (simplified MGL model)
Total component failure probability	$Q = Q_1 + 3Q_2 + 3Q_3 + Q_4$	$Q' = Q_1 + Q_2 + Q_4$
Fraction of component failures that are common cause	$\beta = \frac{3Q_2 + 3Q_3 + Q_4}{Q}$	$\beta' = \frac{Q_2 + Q_4}{Q}$
Fraction of common cause failures that fail at least three components	$\gamma = \frac{3Q_3 + Q_4}{3Q_2 + 3Q_3 + Q_4}$	$\gamma' = \frac{Q_4}{Q_2 + Q_4}$
Fraction of common cause failures involving at least three components that fail all four components	$\delta = \frac{Q_4}{3Q_3 + Q_4}$	$\delta' = 1$

The approach to modifying the definitions of the common cause parameters in Table 16, based on the events excluded from the fault tree, provides a roadmap for developing similar models for different types of simplification. With the simplified model, such as the multi-unit model in Fig. 14, the plant specific mapping process needs to reflect the same simplifications. In Fig. 14, common cause events of two types are modelled: those that could only impact two components within a given unit and those that would fail all four components across both units. To map impact vectors, the generic data are first mapped to a general impact vector for four components, $\{N_0, N_1, N_2, N_3, N_4\}$. Each event in this impact vector space is mapped to a special impact vector, $\{N_0, N_1, N_{CCF1}, N_{CCF2}\}$; that is, the event impacts: no components; a single component; two components at one unit; and all four components. The point estimates of the MGL parameters for this model would then be defined as:

$$\beta' = \frac{2N_{CCF1} + 4N_{CCF2}}{N_1 + 2N_{CCF1} + 4N_{CCF3}}$$

$$\gamma' = \frac{4N_{CCF2}}{2N_{CCF1} + 4N_{CCF2}}$$

$$\delta' = 1$$

The corresponding basic event probability are given by:

$$Q_1 = (1 - \beta')Q'$$

$$Q_2 = \beta'(1 - \gamma')Q'$$

$$Q_3 = 0$$

$$Q_4 = \beta'\gamma'Q'$$

The expressions show that when model simplifications are undertaken with respect to the application of the MGL model (e.g. omitting some of the basic events in the full symmetric case), the assumptions impact the formulas for computing the basic event probability as well as how the impact vectors are processed to compute the parameters. The latter of which have somewhat different meanings in a simplified model.

5.5. HUMAN RELIABILITY ANALYSIS

In principle, human reliability analysis for an MUPSA is the same as for a single reactor PSA, except that the accident sequences now involve both single units and a combination of units. However, there are several unique considerations that can influence how human reliability analysis is implemented in MUPSAs.

5.5.1. Pre-initiator human errors

An analysis of pre-initiator human errors is integral to any human reliability analysis for a PSA. Such errors may render equipment unavailable and leave systems and subsystems in unfavourable alignments at the time of the initiating events. The potential for pre-initiator human errors impact two or more units needs to be considered. This can result from human errors impacting systems or components shared by multiple units or from a special type of CCF in which the same human error is repeated on two or more different reactor units. Once identified, the events can be analysed using existing human reliability analysis methods for pre-initiator human errors.

5.5.2. Post-initiator human errors

The event sequence models identify sequences involving both single and multiple reactors concurrently. As shown by the Fukushima Daiichi accident, there is the issue of whether the human resources available to stabilize the plants and to implement emergency procedures and severe accident guidelines will be sufficient or will perhaps be overwhelmed, owing to the magnitude of the accident [1]. There is little or no experience in PSA for modelling human reliability analysis of multiple reactor accidents, so considerable care is needed to support the human reliability analysis treatment for these situations. The work to develop emergency response and accident management provisions for multi-unit accidents is still at an early stage. Accident management and emergency planning guidelines are currently based on the assumption that accidents only occur on one reactor unit at a time.

For some multi-unit accidents, the initial plant conditions, initiating events and plant responses to the initiating events may follow similar paths. However, different accidents can create new challenges. It is important that MUPSA modelling is emphasized in the effort to manage reactor accidents so that appropriate risk insights can be incorporated into emergency planning.

5.6. LEVEL 1 EVENT SEQUENCE QUANTIFICATION

5.6.1. Site core damage frequency quantification

The SCDF needs to be presented together with its major components, including SUCDF, MUCDF and the specific reactor and reactor combinations that comprise these site metrics (see the equations in Section 4.5). This includes the mean point estimate, obtained using mean values for all of the PSA data

parameters, and the uncertainty distribution. SUCDF can be analysed in the individual reactor CDF contributions, and MUCDF can be analysed in the contributions from accidents involving specific combinations of reactors. It should be noted that the units of SCDF, SUCDF and MUCDF are events per site-calendar-year, whereas the individual reactor CDF results are in units of events per reactor-calendar-year. To avoid confusion, the units need to be listed for each frequency value referenced in the results.

For each specific reactor contribution to SCDF and for each specific reactor combination to MUCDF, the significant accident sequences and significant basic events need to be identified and ranked. The SCDF also comprises the CDF for each combination of reactors involved in multi-unit accidents within the scope of the PSA model, and any significant contributors for the total aggregated SCDF and for each of the components identified above (see Tables 3 and 4, in Section 3.1). To meet the requirements of current PSA standards [21, 41], much more information would be necessary to identify all of the significant contributors to SCDF.

5.6.2. Conditional probability of a multi-unit accident quantification

Introducing CPMA given core damage on a specific reactor unit provides an interim measure that can be used with existing singe reactor PSA results to determine the relative likelihood of single versus multiple reactor accidents. The original purpose of the expression MUCDF = CDF_2 was to investigate the likelihood of multi-unit accidents relative to single unit accidents. While metrics such as SCDF, SLERF and MUPSA belong to the site, CPMA belongs to each reactor unit. A rough estimate of CPMA can be derived from an existing single reactor PSA by simply grouping the accidents and dividing the sets into two categories: (i) accidents most likely to involve single reactors; and (ii) accidents most likely to involve at least two reactors. The ratio of the multi-unit contribution to the total CDF is an estimate of the CPMA.

In Section 3.1, estimates of CPMA for with and without sharing of systems are 0.67 and 0.14, respectively. Seabrook was a two unit station with minimal sharing of structures and systems, while the other plant had significant sharing. The estimate for Seabrook includes a full set of internal and external hazards; the estimate for shared systems is for internal events only. The high CPMA for a plant with minimal sharing is strong evidence that a risk assessment that does not address multi-unit accidents is incomplete and unable to identify all risk significant accident sequences.

5.6.3. Sensitivity and uncertainty analysis

To meet the requirements of current PSA standards [21, 41], it is necessary to characterize sources of uncertainty and to quantify the impacts of the uncertainties on all of the quantified risk metrics (see Table 17 for the SCDF uncertainty distribution for Seabrook). Topics to be considered in the performance of sensitivity analyses for SCDF in an MUPSA include the following:

(a) Alternative assumptions about the seismic CCF treatment in the modelling of both seismically induced initiating events and seismic failure of mitigating equipment;
(b) Alternative assumptions about the treatment of non-seismic, multi-unit CCFs in identical, redundant systems;
(c) Alternative assumptions about the treatment of operator actions for event sequences and accidents involving multiple units;
(d) Alternative assumptions with regard to any simplifying assumptions made in the MUPSA modelling and quantification.

5.6.4. Analysis of significant risk contributors

In current PSA standards [21, 41], the concept of risk significance is defined for both accident sequences and basic events in the PSA model: accident sequences contributing at least 1% to the total value of a quantified risk metric are defined as significant. In addition, basic events with Fussell–Vesely values greater than 0.005 are classified as significant. For an MUPSA, these criteria need to be applied to SCDF, SLERF, SUCDF, MUCDF, SRCF and SCCDF, and any other multi-unit risk metric within the PSA scope.

TABLE 17. UNCERTAINTY DISTRIBUTION FOR SITE CORE DAMAGE FREQUENCY (SCDF) FROM THE SEABROOK MULTI-UNIT PROBABILISTIC SAFETY ASSESSMENT

SCDF contributions	Frequency per site calendar-year				Range factor
	Mean value	5%-tile	50%-tile	95%-tile	
Single unit SUCDF	4.0×10^{-4}	1.2×10^{-4}	3.1×10^{-4}	9.0×10^{-4}	2.7
Multi-unit MUCDF	3.2×10^{-5}	1.1×10^{-6}	1.5×10^{-5}	1.2×10^{-4}	10.4
Total SCDF	4.3×10^{-4}	1.4×10^{-4}	3.4×10^{-4}	1.0×10^{-3}	2.7

6. LEVEL 2 EVENT SEQUENCE ANALYSIS

6.1. TREATMENT OF THE LEVEL 1/LEVEL 2 INTERFACE

Assuming the existence of a completed Level 2 PSA, it is necessary to review the Level 1/Level 2 interface for the revisions required for the MUPSA. The main difference here is the need to address multi-unit accidents that will have unique boundary conditions for the Level 1/Level 2 interface.

6.2. LEVEL 2 EVENT SEQUENCE MODEL

6.2.1. Single unit accidents

The Level 2 modelling of single reactor accidents is the same for a single reactor PSA, with the only exception that it is interfaced with a Level 1 model that has both single reactor and multiple reactor accident sequences.

6.2.2. Multi-unit accidents[7]

Following the presentation of the Level 1 PSA results for SCDF, Ref. [13] provides guidance on the Level 2 modelling of multiple reactor accidents, and states that the next step in the analysis of two unit interactions is to estimate the consequences of concurrent core melt accidents in both units having estimated a conservative value for the frequency of such events in single units. Given the hypothetical occurrence of two concurrent accidents, even when the particular cause of the accident is common to both, there is no assurance that the same event sequences will be followed in the respective accidents. For example, in a LOOP event and a hypothesized failure of all four diesel generators, the progression of events could be substantially different at the two units, resulting in different PDSs and release categories.

Hence, for the 39 PDSs and 13 release categories that were selected for single unit analyses, 1521 PDSs (= 39^2) and 169 release category (= 13^2) combinations can be defined for two unit accidents. However, such an approach would be clearly impractical. For the purpose of bounding the risk of two unit events, Ref. [13] follows a much simpler approach to make full use of the detailed results for single unit events and to minimize the need for additional consequence analyses (see Table 18 for the designated states). The first step is to examine the

[7] This section is based on Ref. [13].

TABLE 18. ANALYSIS OF PLANT DAMAGE STATES FOR MULTI-UNIT INITIATING EVENTS

Initiating event	Plant damage state (% contribution to CDF)			
	A	D	FP	F
Seismic events	2	33	63	2
Loss of off-site power	2	98	<1	<1
Truck crash into transmission lines	3	97	<1	<1
External flood	<1	99+	<1	<1

Note: A — core damage with intact and isolated containment with containment heat removal; D — core damage with intact and isolated containment with no containment heat removal; FP — core damage with failure to isolate small penetrations (<7.6 cm in diameter); F — core damage with failure to isolate large penetrations (>7.6 cm in diameter); CDF — core damage frequency.

distribution of accident sequence frequency among the various PDSs for each initiating event analysed in the two unit accident model.

For the case of two concurrent accidents, each can progress differently and can result in a different PDS. However, Ref. [13] assesses CCFs of similar or identical components to dominate the accident frequency. Only in the case of a truck crash into the transmission lines is the frequency contribution of independent concurrent accidents significant (see Table 19). Hence given two concurrent accidents, the PDSs would be highly correlated. Therefore, it seems reasonable and definitely conservative to assume that all dual unit accidents would result in the same PDS. The occurrence of different plant states would tend to reduce the estimated consequences of early health effects, since the probability of concurrent releases would be reduced.

Based on the results of the single unit analysis, Ref. [13] establishes a strong correlation of PDSs to release categories has been established (see Section 3 for further explanation of the abbreviations):

TABLE 19. ANALYSIS OF CONTRIBUTORS TO MULTI-UNIT CORE DAMAGE FREQUENCY*

Risk metric	Loss of off-site power	Truck crash into transmission lines
Initiating event frequency (per site-year)	1.4×10^{-1}	2.8×10^{-4}
Conditional probability of two unit core damage given an initiating event		
Common cause failure of emergency diesel generators	2.1×10^{-5}	3.3×10^{-4}
Independent failures	3.2×10^{-8}	3.7×10^{-5}
Total	2.1×10^{-5}	3.6×10^{-4}
Multi-unit core damage frequency (per site-year)	2.9×10^{-6}	1.0×10^{-7}

* Reproduced courtesy of ABS Group [13].

(a) All of the risk significant sequences in state A result in release category S5 (core damage with intact containment), which has predominantly benign consequences.
(b) The risk significant sequences in state D result in either S3V (core damage with late overpressure failure of containment) or S4V (core damage with base mat melt through), which have similar consequences (i.e. significant numbers of latent health effects and negligible potential for early health effects).
(c) The risk significant sequences in state FP result in release category S2V (core damage with small early containment isolation failure). S2V results in latent health effects and small numbers of early health effects.
(d) The risk significant sequences in state F result in release category S6V (core damage with large early containment isolation failure). S6V dominates the risk of early health effects.

In summary, the Seabrook multi-unit Level 2 analysis made use of insights into the dominant accident sequences in the Level 2 PSA for Unit 1 and a careful consideration of the contribution to MUCDF from CCFs involving EDGs and motor operated valves on multiple units to simplify the multi-unit Level 2 PSA model. This treatment was based in part on the assumption that both units were operating at 100% power at the time of the initiating events and the fact that both units were of identical design. To simplify the model for multiple units, assumptions were made (e.g. both units operating at full power when each

initiating event occurs), which meant building the model required a small fraction of the effort needed to build the original single unit PSA models.

The identical units of the Seabrook design involved and the dominance of CCFs in contributing to system failure meant the dominant accident progression sequences leading to radioactive release source terms for a given initiating event only involved a limited number of dominant paths through the event trees (as reflected in Table 20). In a multi-unit site with non-identical units, a multi-unit release is likely to result in different paths compared with the Seabrook example. Hence, it is important that any assumptions made to simplify are clearly documented.

The subscript 2 in the release category designators in Table 20 indicates a double release (release from both units). It should be noted that both states A and D PDS percentages are conservatively assigned to $S3V_2$, although this needs to be a small effect because of the dominance of state D. In addition, the small percentages assigned to states FP and F (<1%) are neglected for the three initiators other than seismic events. This also has a small, non-conservative effect, since the unconditional frequencies of seismic scenarios assigned to states FP ($S2V_2$) and F ($S6V_2$) are several orders of magnitude greater than the frequencies of the corresponding scenarios resulting from the other initiators.

TABLE 20. ASSIGNMENT OF DOUBLE UNIT CORE DAMAGE FREQUENCY TO RELEASE CATEGORIES*

Initiating event	Percentage of double unit accident frequency assigned to release categories		
	$\overline{S3}V_2$	$\overline{S2}V_2$	$\overline{S6}V_2$
Seismic events	35	63	2
Loss of off-site power	100	0	0
Truck crash	100	0	0
External flood	100	0	0

* Reproduced courtesy of ABS Group [13].

6.3. LEVEL 2 EVENT SEQUENCE QUANTIFICATION

6.3.1. Site release category frequency quantification

In a single reactor unit Level 2 PSA, the accident sequences are binned into a discrete set of release categories, and the frequency of each release category is determined by summing the accident sequence frequencies assigned to each category. The governing criteria for binning is that all of the sequences in the category can be associated with a representative source term, which is comprised of the magnitude, timing, release height and thermal energy of release of radioactive material. In the single unit PSA case, RCFs are expressed in units of events per reactor-calendar-year. If the PSA includes a full set of plant operating states, including LPSD states, there will be unique release categories for those states.

In a multiple reactor Level 2 PSA, the release categories will now include both single unit and multi-unit releases, and the frequencies are expressed in terms of events per site-calendar-year. In Section 4.3, the unique release categories associated with multi-unit releases were discussed, as well as the logic for assigning the MUCDF to the PDSs and then to release categories. For the single unit release categories, the total frequencies reflect the number of reactors on the site. For identical two unit plants, such as Seabrook, the total frequency per site-year of a release category for a release from a single unit is simply twice that of the same release category from the single unit PSA after correcting for the frequency of multiple reactor accidents.

6.3.2. Site large early release frequency quantification

The ASME/ANS PRA standard [21] defines a large early release as the rapid, unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of off-site emergency response and protective actions such that there is a potential for early health effects.

Many PSAs have used specific criteria to define ‘early’ as a release within four hours of the time of core melt through the bottom of the reactor vessel, which considers the warning time to start the evacuation of the emergency planning zone and the time to clear out the near field areas where early health effects could be a concern. At Seabrook, the dominant contributors to early health effects for the single reactor PSA were in two release categories: S2V for core damage with small early containment failure or bypass and S6V for core damage with large early containment failure or bypass. When the source term is doubled to bound the consequences of a dual unit release, the risks of early health effects

also included these same two release categories with a double release, or $S2V_2$ and $S6V_2$. No additional release categories are found to contribute to early health effect risk when the source terms are doubled. However, SLERF will generally include the following components in an MUPSA:

(a) SLERF sequences involving single reactor accidents that correspond to the LERF sequences in the single reactor PSAs for that site;
(b) SLERF sequences involving multiple reactor accidents that correspond to the LERF sequences in the single reactor PSAs with increased source terms reflecting multiple releases;
(c) SLERF sequences involving multiple reactor accidents that involve combinations of non-LERF sequences in the single reactor PSAs but are now sufficient to produce early health effects because of an increased total source term.

6.3.3. Sensitivity and uncertainty analysis

This is essentially the same task as that for SCDF, except that here the Level 2 accident sequences involve both the plant and containment responses contributing to each release category. The uncertainty in the quantification of each release category in the multi-unit Level 2 PSA is quantified. Sensitivity analyses are performed, similar to those defined for SCDF, but the risk metric quantified in this case is the RCF.

6.3.4. Analysis of significant risk contributors

The same risk significance criteria for SCDF are applied here for each SRCF and for SLERF. Accident sequences that comprise at least 1% of the SRCF and SLERF, and basic events with Fussell–Vesely values greater than 0.005 for each SRCF and SLERF are regarded as risk significant.

7. MECHANISTIC SOURCE TERM ANALYSIS

This section is brief because source term analysis in an MUPSA is fundamentally the same as a single reactor unit PSA, except that the release categories involve releases from both single and multi-unit accidents.

7.1. SINGLE REACTOR ACCIDENTS

For each of the release categories in the multi-unit Level 2 PSA, mechanistic source terms need to be provided. Those that involve single reactor accidents are determined as they are for a single reactor Level 2 PSA (see Refs [6, 13] for guidance).

7.2. MULTIPLE REACTOR ACCIDENTS

Some of the Level 2 release categories will involve accidents with multiple reactor units. In general, the releases from each reactor differ owing to differences in:

— Plant operating state at the time of the initiating event;
— Reactor power rating, power level and operating history prior to the accident;
— Accident sequence definition and timing of warning and release;
— Release location and thermal energy of release.

The Fukushima Daiichi accident involved core damage to the three units in operation (Units 1–3), whereas the reactor cores for the remaining shutdown units were protected on account of successful accident management efforts and the fact that one EDG had not failed, helping to protect Units 5 and 6. Among the six units, there were significant differences in power level and plant design features to protect the core and to provide for containment functions. Of the three units involved in the release, Unit 1 had a smaller core (460 MW(e)) than Units 2 and 3 (784 MW(e)), which would have affected thermal hydraulic responses, timing and release magnitudes. Although all three units experienced core damage, the timing of the accident sequences, all of which involved hydrogen explosions, was different (see Fig. 1, in Section 2.1).

In the Seabrook MUPSA, the reactor units were identical, and the analysis was simplified by assuming that both reactor units were operating at full power at the time of the initiating events. As discussed in Section 6.2 and presented in Table 20, the multi-unit releases were assigned to three release categories. The source terms for these three categories of multi-unit releases were developed simply by doubling the source terms of the same release categories for single reactor accidents. All other factors, such as timing, release height and energy, were assumed to be the same as those defined for the same single unit release categories.

7.3. NON-CORE SOURCES

Detailed guidance for mechanistic source term analysis accidents involving non-core sources of radioactive material is beyond the scope of this publication. However, if the MUPSA were to include accidents involving releases from non-core sources, perhaps in combination with releases from one or more reactors, those accident sequences would have unique release categories and mechanistic source terms.

7.4. UNCERTAINTIES

In the Seabrook MUPSA, uncertainties in the mechanistic source terms were treated by defining a discrete set of probabilistically weighted source terms for each modelled release category to represent the uncertainties in the magnitude of the source term. The different source term cases were developed using different computer models and modelling assumptions, yielding differences in release magnitude and timing. Probability weights were assigned using engineering judgement. Details of this approach can be found in Ref. [13].

8. RADIOLOGICAL CONSEQUENCE (LEVEL 3) ANALYSIS OF ALL MODELLED SEQUENCES

8.1. LEVEL 3 ANALYSIS OF ALL SITE RELEASE CATEGORIES[8]

The Seabrook MUPSA [13] describes how the accidents involving multiple releases were quantified and provides guidance on performing the off-site consequence (Level 3) analysis for each modelled release category. It estimates the consequences of the double releases for release categories for the two damage indices latent and early cancer fatalities.

8.1.1. Latent cancer fatalities

In the case of latent cancer fatalities, analyses were performed using special CRACIT, a computer code for consequence analysis, for release categories $S3V_2$ and $S6V_2$, with a conservative set of release parameters and a source term twice

[8] This section is based on Ref. [13].

as great as that established for single unit events. These results demonstrated that the consequences in terms of latent health effects are no more than a factor of 2 greater for the double release case across the full range of the conditional risk curve. These special CRACIT cases employed a conservative set of release parameters directly. For more realistic results, a set of mean conditional risk curves for latent health effects was obtained by scaling up the mean damage scale by a factor of 2. The mean results are the mean values (probability weighted averages) of the results from 12 different CRACIT analyses performed for each release category in the single unit analyses (cases reflect the treatment of uncertainty in source term and consequence modelling). This approach meant it was possible to incorporate the full spectrum of CRACIT cases without having to rerun all of them using a different source term.

8.1.2. Early cancer fatalities

In the case of early health effects, which can potentially occur in release categories $S2V_2$ and $S6V_2$, the special CRACIT analysis indicated that, at certain portions of the conditional risk curve, the consequences for given frequencies increased by much more than a factor of 2. This was expected in view of the threshold aspect of the early health effect model. To obtain appropriate estimates of the mean conditional risk curves for early health effects resulting from the double release events without having to re-analyse all 12 CRACIT cases for each release category, it was judged that one of the cases contained a source term factor of 2 greater than the base case (the remaining being approximately 'average').

8.1.3. Release times

With respect to release times, the double unit events were modelled as simultaneous releases. This is considered a conservative assumption but probably does not have a large effect. The dominant scenarios for the double unit events insofar as early health effects are concerned are seismically induced station blackout scenarios with failed open containment isolation valves. It is conceivable that the times of core damage for the respective accidents could differ by as much as several hours, taking into account the random behaviour of the reactor coolant pump seals, the prior operating histories of the respective cores and the exact timing of the diesel generator failures. However, since the containment isolation valves are failed open, the release times would correspond exactly with the core damage times. Although the release times could still differ appreciably, the difference relative to the evacuation time would be short and the likelihood of near coincident releases cannot be ruled out. The probability that the releases occur at the same time and reduction in consequences for releases at

different times have not been included in these analyses. The elimination of this probability leads to a potentially large conservatism in the results, the effect of which has not been quantified.

8.1.4. Conditional risk curves

The conditional risk curves in the two unit event analysis for release categories $S3V_2$, $S2V_2$, and $S6V_2$ are presented in Figs 15–17. For comparison, the corresponding mean values for the single unit events are plotted (i.e. $S3V_1$, $S2V_1$ and $S6V_1$). The figures show that the early health effects results for the double unit events relate to the single event cases in a more complex way than latent effects. In the case of S2V, the upper tail of consequences for $S2V_2$ is about a factor of 20 greater than that for $S2V_1$. In the case of S6V, the double release case has a frequency of exceedance more than a factor of 3 greater at all damage levels and an upper tail that is about a factor of 2 greater in damage level.

It is important to note that for the early health effects, doubling the source term increases both the frequency of a given damage level and the consequences at a given frequency, and the impacts are highly non-linear. For this reason, obtaining an MUPSA result by simply scaling the results of a single unit Level 3 PSA by the number of units does not work for early health effects. Such scaling is reasonable for latent health effects if the assumption of a linear dose response model is accepted. However, dose thresholds may be required to produce latent health effects, in which case neither type of health effect can be reliably estimated via scaling.

8.2. LEVEL 3 ANALYSIS OF EXTERNAL HAZARDS WITH A HAZARD SPECIFIC EVACUATION MODEL

It is noted that when performing a Level 3 PSA for external hazards, assumptions made with regard to evacuation and sheltering need to account for any adverse impact of the hazard on the infrastructure needed to complete the protective actions. Roads and bridges, for example, may be damaged in relation to the case with internal events and hazards. This concern is equally valid for both single unit and multi-unit accidents.

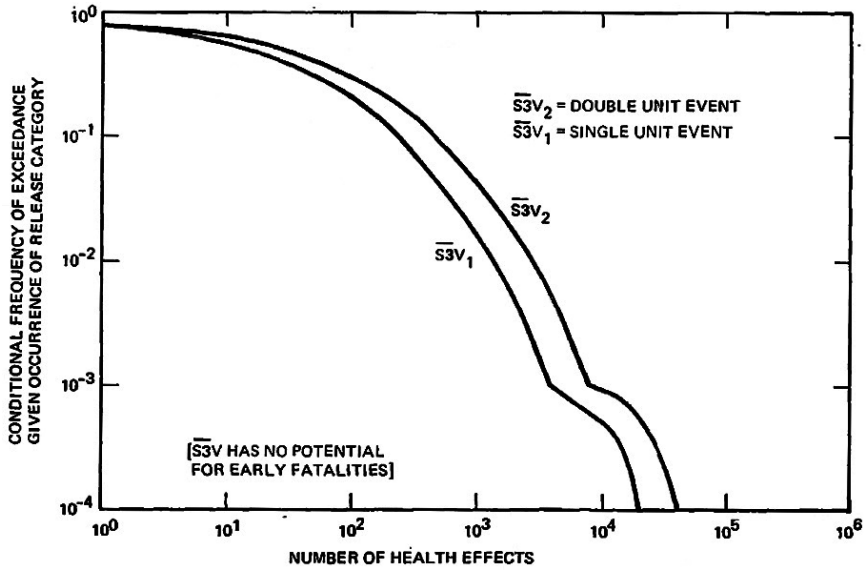


FIG. 15. Conditional exceedance frequency for latent cancer fatalities release category S3V. (Reproduced courtesy of ABS Group [13].)

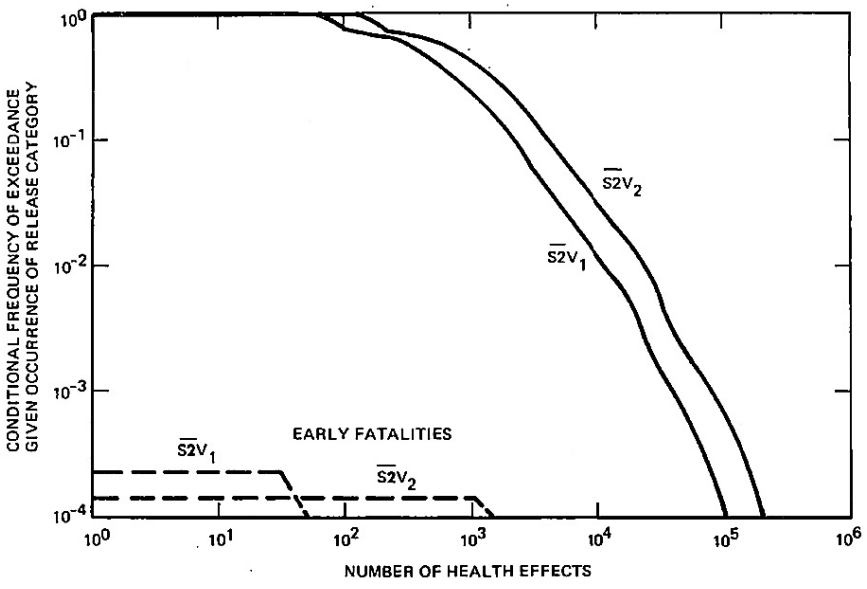


FIG. 16. Conditional exceedance frequency for early and latent cancer fatalities release category S2V. (Reproduced courtesy of ABS Group [13].)

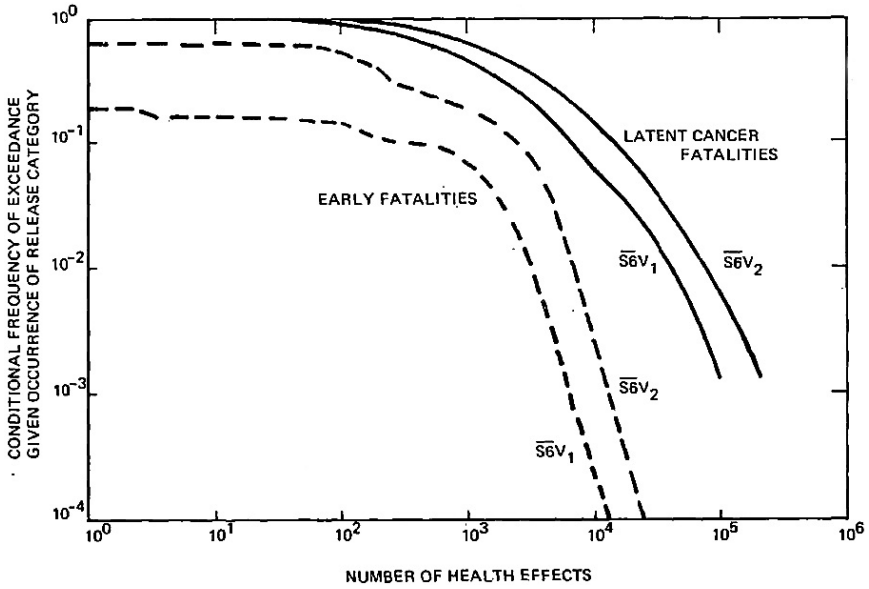


FIG. 17. Conditional exceedance frequency for early and latent cancer fatalities release category S6V. (Reproduced courtesy of ABS Group [13].)

9. RISK INTEGRATION

9.1. AGGREGATION OF COMPLEMENTARY CUMULATIVE DISTRIBUTION FUNCTIONS[9]

In a Level 3 MUPSA, the dimensions of aggregation to be considered to determine the overall integrated risk of the multi-unit site include the following:

— Different plant operating states;
— Different hazard groups;
— Different release categories involving single reactor accidents on each reactor unit;
— Different release categories involving combinations of reactor units on the site.

[9] This section is based on Ref. [13].

For certain PSA applications, aggregation of one or more of these dimensions might not be necessary. For example, estimating the change in risk due to changes in a design or operational feature may be demonstrated to be contained within the internal events group.

The aggregation of risk in the form of SCCDF curves for the MUPSA is performed in the same manner as that for a single unit PSA but with two key differences: (i) frequencies are expressed in terms of events per site-calendar-year rather than events per reactor-calendar-year; and the contributing release categories include those for both single reactor and multiple reactor accidents.

The risk curves in the Seabrook MUPSA [13] for early and latent health effects indicate the contributions from single unit events, which would occur approximately twice as frequently as estimated for each reactor unit separately, and from the double unit events analysed for seismic events, LOOP, truck crashes, and external flooding (see Figs 6 and 7, in Section 3.1). In both sets of curves, the single unit events make the greatest contribution to the overall result except for the upper tails (low frequency — high consequence region) of the distributions. In the case of early fatalities, the double event release category $S6V_2$ makes a small contribution to the overall risk curve over much of the range of early fatalities and begins to take over as the leading contributor in the extreme upper tail. However, it is also clear that had double unit events been neglected entirely, the early fatality results would not have been underestimated by an appreciable amount at accident frequencies greater than 10^{-9} per site year.

For latent health effects, the single reactor events also make the greatest contribution over much of the range and can be said to dominate the results in the region above 10^{-5} events per site year. As was the case with early health effects, the double unit events begin to take over as major contributors in the right hand tail of the risk curve. In this case, release category $S2V_2$ is the most important of the double event cases. Again, the contributions of double unit events are found to be significant. Were these events to be neglected, however, the degree of risk underestimation would be relatively small.

With regard to the double unit events, the numerical results do not reflect important conservative assumptions that tend to overestimate the risk levels. One such example is the treatment of dependence for seismically induced failures; that is, given a seismically induced equipment failure on either unit, the corresponding identical equipment in the other unit is assumed to fail with a conditional frequency of unity. This type of assumption is also employed for multiple equipment items within a unit and therefore constitutes a conservative assumption in the single event analysis as well. Were the conservatism to be removed, both the single event and double event risk curves would be reduced. However, the relative importance of double unit events might stay the same.

The assumption of simultaneous releases in the case of double unit events is only a factor in the analysis of early health effects. A more rigorous analysis of the likelihood and effects of time delays between the respective releases could significantly reduce the risk contribution of the double unit events to the overall site risk curve. Hence, the resulting risk curves need to be regarded as providing upper bounds on the true risk.

The main lessons from Seabrook with regard to aggregation are:

(a) Aggregation is facilitated by expressing the accident frequencies on a per site-year basis rather than reactor-year, on which single unit PSAs are based.
(b) The symmetry of identical units means that the frequency of each single unit accident is doubled for the site frequency of each release category involving a single reactor source term. Non-identical units mean separate CCDF contributions from each.
(c) Two unit sites have separate release categories for two unit accidents. More units necessitate more combinations of reactor unit accidents to be considered.
(d) The total aggregated CCDF is the sum of frequencies over each of the single unit and two unit accident release category CCDFs for the total aggregated risk curve. The process is the same as single unit Level 3 PSA but with both single unit and multi-unit accident release categories, and frequencies are on a per site-year basis.
(e) The aggregated CCDF reflects the increased likelihood of an accidental release because of the multiplicity of reactors contributing single reactor accidents as well as greater consequences of accidents with multiple reactor source terms. The aggregated risk is thus a complex combination of these two effects.

9.2. SAFETY GOAL EVALUATION

Some Member States have safety goals and QHOs that are associated with controlling the levels of risk to individuals near each nuclear power plant site. The QHOs are often framed in terms of the average individual risk of early and latent cancer fatalities for people who live in the vicinity of the site. In the past, comparisons were made between the results of single unit PSAs for these metrics to justify that the health objectives had been met. However, such comparisons are not appropriate for multi-unit sites, as the total risks from all of the reactors on the site and the risks of multi-unit accidents have not been taken into account in these comparisons. Such comparisons have also been used to characterize

the intermediate risk metrics of CDF and LERF, and to establish goals and objectives for CDF as though they were surrogates for the safety goal QHOs. As demonstrated, the risk of a multi-unit site is significantly higher than that for an individual reactor. As more units are added, the frequency of single reactor accidents and the likelihood of multi-unit accidents both increase. Hence, PSA results are not to be used to evaluate the margins against the safety goals unless the PSA addresses the full risk profile. For the same reason, individual reactor metrics, such as CDF and LERF, do not provide adequate surrogates for QHOs because the impact of the higher frequency of single reactor accidents and the risks of multiple reactor accidents is not reflected in the single reactor metrics. Modarres [69] reports:

> "To estimate consequences of a multi-unit accident, it is necessary to estimate large releases of radioactivity that lead to prompt fatalities. Modarres et al. [70] summarized three options for estimation of large release frequency. In the first option the magnitude of release may be measured on the basis of associating a 'large' release with an expectation that it would result in at least one early fatality. For example, the ASME/ANS Standard for PRA (RA-Sa-2009) (Ref. [71]) defines a 'large early release' as a 'rapid, unmitigated release of airborne fission products...such that there is a potential for early health effects.' Incorporating the effectiveness of temporal consequences, such as public evacuation and other protective actions, however, complicates the definition of a large release in this context. NUREG/CR-6094 (Ref. [72]) removes this complication by defining a release as large when it leads to an early fatality (with high probability) for a stationary individual standing one-mile from the site. This is a simple and convincing measure. However, it nevertheless requires some assumptions when applied to a particular site. To determine this measure of LRF, a hypothetical site should be assumed along with subjective meteorological data and an assumption of what constitutes a 'high probability'. While identifying a representative site is possible, major conservatisms may be necessary to make it justifiable.
>
> "The second option measures the large release (i.e., on the basis of magnitude of the source term associated with each multi-unit core damage scenarios) in the form of either absolute or relative quantities of radionuclides released. The absolute measure is often expressed in terms of activity released to the environment as a surrogate for a quantitative calculation of dose. This is typically done for a few isotopes that tend to dominate estimates of offsite health effects, such as I-131 or Cs-137. For relative release, the traditional form expressed is fractional release of core inventory of various

radionuclide groups to the environment and the timing of the release may be specified. NUREG/CR-6595 (Ref. [72]) (Appendix A) suggests specific release fractions that may be considered as large (e.g., 2–3% of the iodine inventory). This option is simple to describe, but selecting the total amount of release or release fractions considered large is subjective and contentious.

"The third option for large release de-emphasizes the amount of radioactivity released, by defining it in terms of the physical condition of systems, pressure boundaries and radionuclide barriers at the time release begins. For example a large release might be considered as one involving failure of multiple reactor pressure vessels and containment pressure boundaries due to isolation failure(s), bypass or structural damage within a few hours of core melting and fission product release from fuel, during which opportunities for attenuation of the airborne concentration are minimal. Conditions associated with multiple units may also be defined, if necessary."

9.3. SENSITIVITY AND UNCERTAINTY EVALUATION

The Seabrook MUPSA [13] included a full treatment of epistemic and aleatory uncertainties in each part of the PSA. This included both parameter uncertainties and modelling uncertainties, and accounted for sources of uncertainty in the Level 1, Level 2 and Level 3 parts of the risk model. The results presented in Section 9.1 for the SCCDF curves reflect the mean values of an underlying uncertainty distribution of SCCDF curves. The Seabrook report [13] presented uncertainty information on the CCDF curves from the single reactor PSA but not on the SCCDF curves for the MUPSA. To illustrate, the CCDF with uncertainty displayed for thyroid cancer cases is shown in Fig. 18 and the underlying uncertainties in the release frequencies used to develop the CCDF curves in Fig. 19. In the lower right hand of Fig. 18, the mean curve exceeds the 95th percentile curve, which only occurs when the uncertainties are very large. Similar results would be obtained in an MUPSA for the SCCDF curves and SRCFs.

Some important lessons from the sensitivity and uncertainty analysis at Seabrook include:

(a) Even though the uncertainties in the estimation of the frequencies and source terms of large early releases, including those from multi-unit accidents, were very large, the level of individual risk to the population surrounding the site was found to be very small and was within the NRC safety goals and QHOs by a large margin. The vast proportion of this risk was located within 1.6 km of the site boundary.

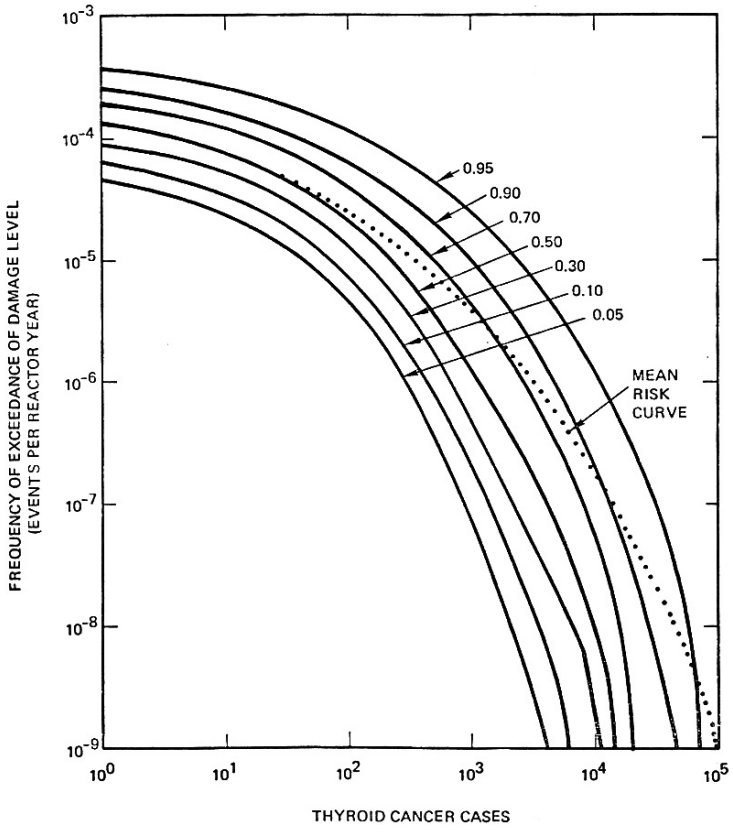


FIG. 18. Complementary cumulative distribution function curves of thyroid cancer cases for single reactor probabilistic safety assessment. (Reproduced courtesy of ABS Group [13].)

(b) The above results were obtained with CDFs that are considered high by today's standards, but with due credit for an exceptionally strong containment design, which rendered the risk of containment failure due to overpressure from severe accident phenomena to be very small. The median pressure capacity of the containment was found to be almost five times the design pressure. This was a consequence of the design approach to protect the containments from a large military aircraft crash owing to the close location to an air force base.

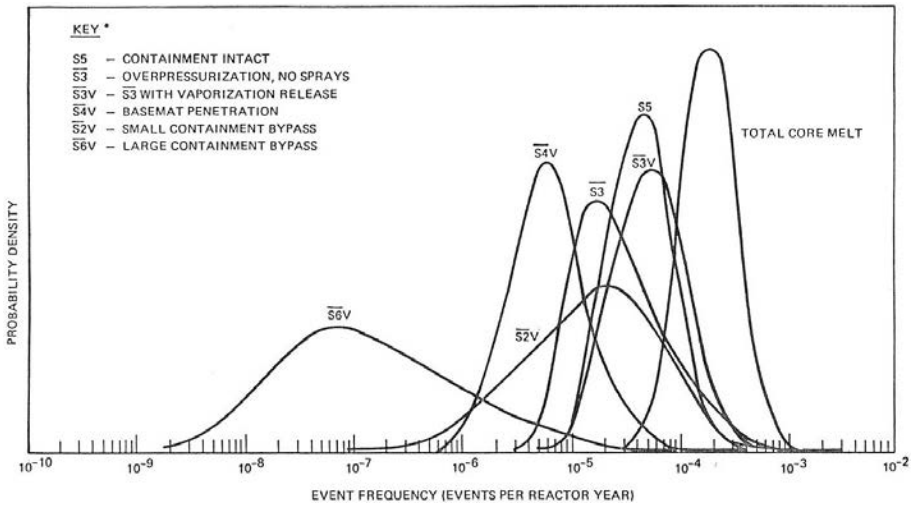


FIG. 19. Uncertainty distribution for Seabrook release category frequencies from single unit probabilistic safety assessment. (Reproduced courtesy of the ABS Group [13].)

10. INTERPRETATION OF RESULTS AND DOCUMENTATION

10.1. IDENTIFICATION OF RISK INSIGHTS WITH REGARD TO SITE SAFETY AND AREAS FOR IMPROVEMENT

It is often said that the main purpose of a PSA is not to produce numerical results but rather to produce risk insights. Many successful PSAs that have addressed single reactor accidents have provided useful risk insights, including identification of weak points, areas for improvement and strategies for risk management in future plant operations. There are additional dimensions to these risk insights that can be derived from future MUPSAs and examples include:

(a) Understanding the integrated risks from a multi-unit site, including the relative contributions to risk from single and multi-unit accidents;
(b) Improved understanding of the risk implications of adding reactor units;
(c) Risk insights into strategies to prevent and mitigate multi-unit accidents;
(d) Insights into the risk significance of shared structures and systems;
(e) Strategies for the prevention of CCFs that impact multiple units;
(f) Evaluation of the adequacy of protection against external hazards;

(g) Evaluation of the adequacy of existing emergency operating and accident management procedures and emergency planning measures;
(h) Risk insights into staffing levels and procedures for accident management and emergency planning.

10.2. EVALUATION OF DEFENCE IN DEPTH

Defence in depth is one of the foundations of the deterministic approach to nuclear reactor safety design and analysis, the principles of which are outlined in Ref. [73]. With the advent of probabilistic approaches, more recent safety design approaches have incorporated risk insights such as the principle of balancing the strategies for prevention and mitigation of core damage events through probabilistic considerations (see Ref. [20] for a summary).

A major limitation of existing guidance for defence in depth is the models employ one reactor at a time when expressing the multiple lines of defence strategies. The structures and systems that offer protection for each line of defence in the current defence in depth concepts are only evaluated in the context of protecting a single reactor unit's inventory of radioactive material. In deriving risk insights into defence in depth from an MUPSA, it is important to add the principle of preventing and mitigating multi-unit accidents, which are not explicitly addressed in the current defence in depth literature. Multi-unit accidents amplify the consequences of an accident in a manner that the traditional concentric barrier model for defence in depth does not consider.

Another limitation of the defence in depth concepts is the use of a concentric barrier model, which is a useful model for a single reactor, with a single reactor coolant pressure boundary, a single containment and a single surrounding site arranged so that each barrier can provide protection to what is inside. A multi-unit site, however, introduces new interactions (i.e. a reactor being compromised by an accident on another unit) that need to be considered. A principle addressed in the current requirements, but one which needs to be reconsidered as experience with MUPSAs grows, is the sharing of SSCs that support safety functions among multiple units. The criteria for evaluating the acceptance of shared structures and systems has not adequately considered how such sharing may increase the likelihood of a multi-unit accident.

10.3. DOCUMENTATION

Documentation of the MUPSA needs to be developed in such a manner as to provide evidence for peer review to justify that the PSA standards have been met. Extensive documentation requirements for an MUPSA are provided in ASME/ANS RA-S-1.4-2013 [41] (see Refs [5, 6, 21] for additional guidance).

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, The Fukushima Daiichi Accident, IAEA, Vienna (2015).

[2] NATIONAL DIET OF JAPAN FUKUSHIMA NUCLEAR ACCIDENT INDEPENDENT INVESTIGATION COMMISSION, The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission, National Diet of Japan, Tokyo (2012).

[3] INSTITUTE OF NUCLEAR POWER OPERATIONS, Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, Rev. 0, INPO 11-005, INPO, Atlanta, GA (2011).

[4] INSTITUTE OF NUCLEAR POWER OPERATIONS, Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, Rev. 0, INPO 11-005 Addendum, INPO, Atlanta, GA (2012).

[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).

[6] 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).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Safety for Existing Nuclear Installations, IAEA Safety Standards Series No. NS-G-2.13, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Consideration of External Hazards in Probabilistic Safety Assessment for Single Unit and Multi-unit Nuclear Power Plants, Safety Reports Series No. 92, IAEA, Vienna (2018).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Approaches to Safety Evaluation of New and Existing Research Reactor Facilities in Relation to External Events, Safety Reports Series No. 94, IAEA, Vienna (2019).

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

[11] NUCLEAR REGULATORY COMMISSION, Domestic Licensing of Production and Utilization Facilities, 10 CFR 50, US Govt Printing Office, Washington, DC.

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[13] PICKARD-LOWE AND GARRICK, Seabrook Station Probabilistic Safety Assessment, PLG-0300, Irvine, CA (1983) Section 13.3.

[14] DINNIE, K., “Considerations for future development of SAMG at multi-unit CANDU sites”, 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (Proc. PSAM11 ESREL 2012, Helsinki, 2012), Curran Associates, Red Hook, NY (2012) 4273.

[15] ONTARIO POWER GENERATION, Darlington NGS Probabilistic Safety Assessment Summary Report, NK38-REP-03611-10072-R001, OPG, Toronto (2015).
[16] SCHROER, S., An Event Classification Schema for Evaluating Site Risk in a Multi-unit Nuclear Power Plant Probabilistic Risk Assessment, Master Thesis, Univ. Maryland (2012).
[17] SCHROER, S., MODARRES, M., An event classification schema for evaluating site risk in a multi-unit nuclear power plant probabilistic risk assessment, Reliab. Eng. Syst. Saf. **117** (2013) 40–51.
[18] NUCLEAR REGULATORY COMMISSION, Recommendations for Enhancing Reactor Safety in the 21st Century, The Near-term Task Force Review of Insights from the Fukushima Dai-ichi Accident, NRC, Washington, DC (2012).
[19] MINOURA, K., IMAMURA, F., SUGAWARA, D., KONO, Y., IWASHITA, T., The 869 Jōgan tsunami deposit and recurrence interval of large-scale tsunami on the Pacific coast of northeast Japan, J. Nat. Disaster Sci. **23** (2001) 83–88.
[20] NUCLEAR REGULATORY COMMISSION, A Proposed Risk Management Regulatory Framework, NUREG-2150, NRC, Washington, DC (2012).
[21] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, AMERICAN NUCLEAR SOCIETY, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sb-2013, ASME, New York (2013).
[22] NUCLEAR REGULATORY COMMISSION, PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, 2 vols, Office of Nuclear Regulatory Research, Washington, DC (1983).
[23] SIU, N., MARKSBERRY, D., COOPER, S., COYNE, K., STUTZKE, M., "PSA technology challenges revealed by the Great East Japan Earthquake" (PSAM Top. Conf. in Light of the Fukushima Dai-ichi Accident, Tokyo, 2013).
[24] NUCLEAR SAFETY ANALYSIS CENTER, ELECTRIC POWER RESEARCH INSTITUTE, DUKE POWER COMPANY, Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3, NSAC-60, NSAC, Palo Alto, CA (1984).
[25] ENGINEERING SAFETY REVIEW SERVICES SEISMIC SAFETY EXPERT MISSION, Preliminary Findings and Lessons Learned from the 16 July 2007 Earthquake at Kashiwazaki-Kariwa NPP (2007).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-9, IAEA, Vienna (2010).
[27] VIAL, E., REBOUR, V., PERRIN, B., "Severe storm resulting in partial plant flooding in Le Blayais nuclear power plant" (presentation at Int. Workshop on External Flooding Hazards at Nuclear Power Plant Sites, Kalpakkam, 2005).
[28] VIAL, E., REBOUR, V., "Results of the reassessment of the protection of French nuclear power plants against external flooding" (Workshop on Physics of Tsunami, Hazard Assessment Methods and Disaster Risk Management (Theories and Practices for Implementing Proactive Countermeasures), 2007).

[29] SANDIA NATIONAL LABORATORIES, Risk Methods Insights Gained from Fire Incidents, NUREG/CR-6738, Office of Nuclear Regulatory Research, Washington, DC (2001).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, OECD NUCLEAR ENERGY AGENCY, IRS Guidelines: Joint IAEA/NEA International Reporting System for Operating Experience, IAEA Services Series No. 19, IAEA, Vienna (2010).
[31] NUCLEAR ENERGY AGENCY, COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES, Working Group on Operating Experience [WGOE]: Report on Fukushima Daiichi NPP Precursor Events, NEA/CNRA/R (2014)1, OECD, Paris (2014).
[32] KULIG, M., TOMIC, B., NYMAN, R., Identification of Common Cause Initiating Events Using the NEA IRS Database: Rev. 0, SKI Rep. 2007:37, SKI, Stockholm (2007).
[33] FLEMING, K.N., "On the issue of integrated risk: A PRA practitioners perspective", Probabilistic Safety Analysis (Proc. AMS Int. Topical Mtg, San Francisco, 2005), ANS, New York (2005) CD-ROM.
[34] KURITZKY, A., SIU, N., COYNE, K., HUDSON, D., STUTZKE, M., "L3PRA: Updating NRC's Level 3 PRA insights and capabilities" (paper presented at IAEA Technical Mtg on Level 3 Probabilistic Safety Assessment, Vienna, 2012).
[35] NUCLEAR REGULATORY COMMISSION, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, WASH-1400, NRC, Washington, DC (1975).
[36] SEUNG WOO LEE, "A study for identifying multi-unit initiating event and estimating frequency" (presentation at PSAM 14: Probabilistic Safety Assessment and Management, Los Angeles, 2018).
[37] UNITED STATES DEPARTMENT OF ENERGY, Preliminary Safety Information Document for the Standard MHTGR, DOE-HTGR-86-024, USDOE, Washington, DC (1988).
[38] UNITED STATES DEPARTMENT OF ENERGY, Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor, Rev. 5, DOE-HTGR-86-011, USDOE, Washington, DC (1988).
[39] IDAHO NATIONAL LABORATORY, Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper, INL/EXT-11-21270, INL, Idaho Falls, ID (2011).
[40] CANADIAN NUCLEAR SAFETY COMMISSION, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, Regulatory Standard S–294, CNSC, Ottawa, Ontario (2005).
[41] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, AMERICAN NUCLEAR SOCIETY, Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants, ASME/ANS RA-S-1.4-2013, ASME, New York (2013).
[42] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-3.1, IAEA, Vienna (2002).
[43] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Aspects of Nuclear Power Plants in Human Induced External Events: General Considerations, Safety Reports Series No. 86, IAEA, Vienna (2017).

[44] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-724, IAEA, Vienna (1993).
[45] OECD NUCLEAR ENERGY AGENCY, Probabilistic Safety Analysis (PSA) of Other External Events than Earthquake, NEA/CSNI/R(2009)4, OECD, Paris (2009).
[46] INTERNATIONAL ATOMIC ENERGY AGENCY, WORLD METEOROLOGICAL ORGANIZATION, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-18, IAEA, Vienna (2011).
[47] INTERNATIONAL ATOMIC ENERGY AGENCY, Consideration of External Hazards in Probabilistic Safety Assessment for Single Unit and Multi-unit Nuclear Power Plants, Safety Reports Series No. 92, IAEA, Vienna (2018).
[48] NUCLEAR REGULATORY COMMISSION, Guidance for Performing a Tsunami, Surge, or Seiche Hazard Assessment: Interim Staff Guidance, Rev. 0, JLD-ISG-2012-06, NRC, Washington, DC (2013).
[49] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-21, IAEA, Vienna (2012).
[50] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanic Hazard Assessments for Nuclear Installations: Methods and Examples in Site Evaluation, IAEA-TECDOC-1795, IAEA, Vienna (2016).
[51] ELECTRIC POWER RESEARCH INSTITUTE, NUCLEAR REGULATORY COMMISSION, EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, NUREG/CR-6850, EPRI, Palo Alto, CA (2005).
[52] ELECTRIC POWER RESEARCH INSTITUTE, Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment, EPRI 1019194, EPRI, Palo Alto, CA (2009).
[53] NUCLEAR REGULATORY COMMISSION, Risk Assessment of Operational Events Handbook, Rev. 1.03, NRC, Washington, DC (2009).
[54] NUCLEAR REGULATORY COMMISSION, Issues and Recommendations for Advancement of PRA Technology in Risk-informed Decision Making, NUREG/CR-6813, NRC, Washington, DC (2003).
[55] ELECTRIC POWER RESEARCH INSTITUTE, Identification of External Hazards for Analysis in Probabilistic Risk Assessment, EPRI 1022997, EPRI, Palo Alto, CA (2011).
[56] 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).
[57] ATOMIC ENERGY COUNCIL, The Station Blackout Incident of the Maanshan NPP Unit 1, AEC (2001).
[58] FLEMING, K.N., BROGAN, B., “Some issues with quantification of station blackout sequences and methods of solution”, 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (Proc. PSAM11 ESREL 2012, Helsinki, 2012), Curran Associates, Red Hook, NY (2012) 2728.
[59] ELECTRIC POWER RESEARCH INSTITUTE, Losses of Offsite Power at US Nuclear Power Plants: Through 2008, EPRI 1019192, EPRI, Palo Alto, CA (2009).

[60] ELECTRIC POWER RESEARCH INSTITUTE, Losses of Off-site Power at US Nuclear Power Plants: Through 1999, EPRI 1000158, EPRI, Palo Alto, CA (2000).
[61] ELECTRIC POWER RESEARCH INSTITUTE, Losses of Off-site Power at US Nuclear Power Plants: Through 1997, EPRI TR-110398, EPRI, Palo Alto, CA (1998).
[62] IDAHO NATIONAL LABORATORY, Reevaluation of Station Blackout Risk at Nuclear Power Plants: Analysis of Loss of Offsite Power Events: 1986–2004, NUREG/CR-6890, Vol. 1, Office of Nuclear Regulatory Research, Washington, DC (2005).
[63] SANDIA NATIONAL LABORATORIES, Handbook of Parameter Estimation for Probabilistic Risk Assessment, NUREG/CR-6823, Office of Nuclear Regulatory Research, Washington, DC (2003).
[64] IDAHO NATIONAL LABORATORY, Industry-average Performance for Components and Initiating Events at US Commercial Nuclear Power Plants, NUREG/CR-6928, Office of Nuclear Regulatory Research, Washington, DC (2007).
[65] ELECTRIC POWER RESEARCH INSTITUTE, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-4780, Nuclear Regulatory Commission, Washington, DC (1989).
[66] EBISAWA, K., et al., Concept and methodology for evaluating core damage frequency considering failure correlation at multi units and sites and its application, Nucl. Eng. Des. **288** (2015) 82–97.
[67] FLEMING, K.N., "Reliability model for common mode failures in redundant safety systems", Modeling and Simulation (Proc. 6th Annual Conf. 1975), Vol. 6(1), Instrument Society of America, Pittsburgh, RI (1975) 579–581.
[68] FLEMING, K.N., KALINOWSKI, A.M., An Extension of the Beta Factor Method for Systems with High Levels of Redundancy, PLG-0289, PLG, Newport Beach, CA (1983).
[69] MODARRES, M., "Multi-unit nuclear plant risks and implications of the quantitative health objectives" (paper presented at PSA 2015 Int. Topical Mtg on Probabilistic Safety Assessment, Sun Valley, 2015).
[70] MODARRES, M., LEONARD, M., WELTER, K., POTTORF, J., "Options for defining large release frequency for applications to the Level-2 PRA and licensing of SMRs" (paper presented at PSA 2011 Int. Topical Mtg on Probabilistic Safety Assessment and Analysis, Wilmington, 2011).
[71] AMERICAN NATIONAL STANDARDS INSTITUTE, AMERICAN NUCLEAR SOCIETY, Addenda to ASME/ANS RA-S-2008: Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009, ANSI, New York (2009).
[72] BROOKHAVEN NATIONAL LABORATORY, Calculations in Support of a Potential Definition of Large Release, NUREG/CR-6094, BNL, Upton, NY (1994).
[73] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

Annex I

MULTI-UNIT SEISMIC PROBABILISTIC SAFETY ASSESSMENT INITIATING EVENT MODELS

Annex I describes the treatment of seismically induced loss of coolant accident (LOCA) initiating event frequencies for multi-unit probabilistic safety assessments (MUPSAs) based on examples from the Seabrook MUPSA [I–1].

Seismic events have the potential for wide ranging effects on nuclear power plants and the surrounding regions. They represent one of the most important types of common cause initiating event (CCIE) considered in a PSA. For an event to be classified as a CCIE, it has to be capable of causing an initiating event and failure of one or more systems or structures that are needed to prevent the initiating event from progressing into an accident and to mitigate the consequences. A seismic event certainly meets these criteria. Moreover, a seismic event at a multi-unit site can cause initiating events and accident sequences on each reactor unit as well as on multiple reactor units concurrently.

This annex explores the modelling of seismically induced initiating events on a multi-unit site and considers the effects of seismic correlation between identical components that share the same fragility curves. Seismic correlation is often used to describe two or more identical components that share a common fragility curve which fail at the same time due to a seismic event because of common analysis elements considered in the fragility development. Such common elements include the frequency content of the seismic waves arriving at the site and the common responses of soil and structures to the ground motion. In this publication, this phenomenon is referred to as seismically induced common cause failure (CCF) because when considering the impact on the components in question, this is really no different than other types of CCF modelled in a PSA, except that in this case the cause of failure and the cause of the synchronization of the times of failure is a seismic event.

The plant selected is the two unit site that was originally designed for Seabrook Station, noting that Unit 2, which was designed to be identical to Unit 1, was never completed or operated. The example chosen is a seismically induced, large LOCA based on information taken from the Seabrook individual plant examination of external events (IPEEE). The large LOCA was caused by seismic failure of the steam generator (SG) supports or reactor coolant pump (RCP) supports. This was modelled in the Seabrook IPEEE by assuming that failure of either component support would result in a single, large LOCA (break flow area $\geq$ 15 cm) in the affected loop. (Seabrook is a four loop Westinghouse pressurized water reactor (PWR)). The LOCA was assumed to result from displacements between the reactor vessel and SG/RCP supports that overstress

the connecting piping. An equivalent break flow area of at least 15 cm in one loop meets the criteria for classifying the pipe break as a large LOCA. As a sensitivity study, the Seabrook IPEEE included a case in which failure of either support was assumed to result in an excessive LOCA on account of the possibility of failures in multiple loops due to a seismically induced CCF of two SG/RCP supports in different loops. As the emergency core cooling system is not designed to deal with multiple breaks, an excessive LOCA was assumed.

Elements of this analysis are recreated here with an expanded treatment of seismically induced CCF to investigate the modelling for a multi-unit LOCA due to a seismic event at a two reactor unit plant based on the original Seabrook Station design and the state of seismic hazard and fragility information at the time of the Seabrook IPEEE. Perceptions of the seismic hazard and the spectral shape of the ground motion may well be different today, and those differences need to be considered in revising the fragilities and upgrading the seismic PSA. However, the analyses here are only for the purpose of understanding the relative importance of seismically induced initiating events on a two unit site. The key interest is the relative frequency of initiating events on both units relative to a single unit. The questions to be addressed include the following:

(1) What is the frequency of two concurrent LOCAs at a two reactor unit station designed like Seabrook Station subject to the seismic hazard assessed during the Seabrook IPEEE?
(2) What is the epistemic uncertainty in the frequency estimates?
(3) How are the answers to (1) and (2) influenced by seismic fragility correlation?

Failure of an SG/RCP support could lead to an excessive LOCA depending on the extent of failure and the degree of displacements resulting from the support failures. This would need to be resolved to calculate the seismically induced core damage or large early release frequency. For this example, however, it is necessary to focus on the initiating event frequency part of the seismic PSA. It is assumed that both identical units at Seabrook are built and are operating for the purposes of this example. For simplicity, additional aspects of seismically induced initiating event development, such as seismically induced loss of off-site power with or without a concurrent LOCA or other initiating event combinations, are not included but would need to be considered in a full scope seismic PSA model.

I–1. SEISMICALLY INDUCED LOSS OF COOLANT ACCIDENT MODEL WITH MULTI-UNIT COMMON CAUSE FAILURE: SIMPLE VERSION

Like many Westinghouse PWR plants, Seabrook as has four nearly identical coolant loops, each with one RCP in the cold leg and one SG per loop. There is one loop with a pressurizer but otherwise all four loops are identical. There is a potential for seismic fragility correlation both within and across multiple units. A seismic CCF within a unit implies that two or more loops failed, and this would be equivalent to an excessive LOCA. A seismic CCF across units means that there would be LOCA on at least one loop at each reactor unit. To keep this first model simple, it is assumed that within each unit, the SG/RCP supports are fully correlated, and varying degrees of correlation are considered across the units. In this model, the three LOCA states to consider following a seismic event are:

— No occurrence of LOCA on either unit (i.e. $j = 0$);
— Only one LOCA (i.e. $j = 1$);
— Two LOCAs ($j = 2$).

All of the LOCAs in this model are considered excessive because of the within unit correlation assumption. A more complex model is presented in Section I–3, in which two tiers of variable correlation are considered, one for correlation between multiple loops at each unit and another for multi-unit correlation. The frequency of a given LOCA state j denoted by $F\{\text{LOCA}_j\}$ is given by the convolution integral for a seismic PSA [I–2]:

$$F\left\{\text{LOCA}_j\right\} = \int_0^\infty \frac{\mathrm{d}H(x)}{\mathrm{d}x} f_{\text{LOCA}_j}(x)\,\mathrm{d}x \tag{I–1}$$

where $H(x)$ is the frequency of seismic events with peak ground acceleration (PGA) of x or greater (exceedance frequency) and f_{LOCA_j} is the conditional probability of a seismically induced failure resulting in LOCA state j given a seismic event with PGA equal to x (LOCA state j fragility). As is typical in actual seismic PSAs, the continuous form of the convolution integral is approximated by a discrete form evaluated at points along the PGA axis of the hazard and fragility curves:

$$F\left\{\text{LOCA}_j\right\} = \sum_{k=1}^{N} h_k f_{k,\text{LOCA}_j} \tag{I–2}$$

where h_k is the frequency of a seismic event with PGA in discrete PGA interval k per site-year and f_{k,LOCA_j} is the conditional probability at the midpoint of interval k. RCP/SG support fragilities are then combined into a composite fragility for the large LOCA initiating event using the law of probability for an OR gate with the two fragilities assumed to be independent inputs:

$$f = f_{\mathrm{RCP}} + f_{\mathrm{SG}} - f_{\mathrm{RCP}} f_{\mathrm{SG}} \tag{I–3}$$

The assumption of independence in combining these fragilities means that there is no seismic common cause potential between an RCP support and an SG support. As is appropriate for any seismic PSA, the exact probability equation for an OR gate can be used in lieu of approximations based on a rare event assumption because the fragilities are to be evaluated over the full range of ground acceleration, where the fragility varies from nearly zero to nearly one. At all fragility values greater than 0.1, the usual rare event approximations do not hold.

A seismic common cause parameter α is now introduced to model the possibilities for seismic CCFs resulting in LOCAs at both identical units, and it represents the fraction of seismic events that result in concurrent LOCAs due to correlated hazards:

— When α = 0, the probability of multiple LOCAs at each unit are fully independent.
— When α = 1, the LOCAs are fully correlated (i.e. multiple LOCAs are always assumed to occur concurrently).

The event tree shown in Fig. I–1 shows a simple model for calculating the probabilities of different LOCA states from a seismic event at a site with two identical reactor units, considering only the possibility of LOCA on each unit due to failure of the SG/RCP supports. This method for correlation is similar to that proposed in Ref. [I–3].

For j = 0, 1, 2, the probability of the three distinct LOCA outcomes given a seismic event at reference level k are thus:

$$f_{k,\mathrm{LOCA}_0} = \alpha(1 - f_k) + (1 - \alpha)(1 - f_k)^2 \tag{I–4}$$

$$f_{k,\mathrm{LOCA}_1} = 2(1 - \alpha) f_k (1 - f_k) \tag{I–5}$$

$$f_{k,\mathrm{LOCA}_2} = \alpha f_k + (1 - \alpha) f_k^2 \tag{I–6}$$

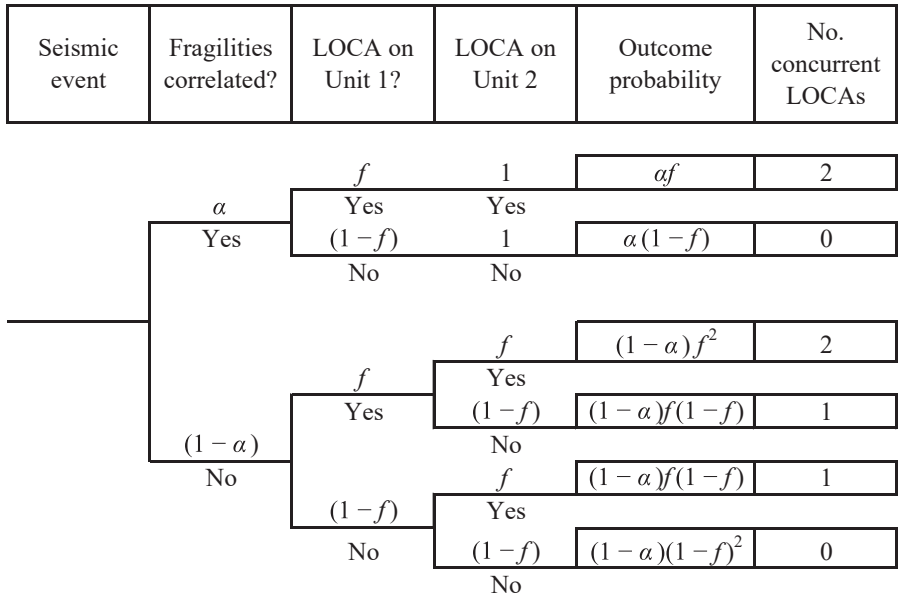


FIG. I–1. Event tree for a two reactor unit loss of coolant accident model.

An implied assumption is that α is independent of seismic intensity. A more refined model would consider that this parameter is also a function of reference PGA level. In this example, α is only used to examine sensitivities to assumptions about correlation. A basis for quantifying it is still to be established. Ebisawa [I–4] performs studies indicating that seismic correlation may increase with seismic intensity. This seismic intensity dependence could easily be incorporated into the current models.

I–1.1. Fragility assumptions

From the Seabrook IPEEE [I–5], the fragility parameters for the RCP supports and SG supports are given in Table I–1.

I–1.2. Seismic hazard characterization

The seismic hazard curves for Seabrook used in the IPEEE are illustrated in Fig. I–2 and Table I–2. Epistemic uncertainty is represented in terms of nine discrete hazard curves, with each assigned a probability. Each of these has been previously aggregated from hundreds of hazard curves, each produced by a different set of modelling assumptions. The mean hazard curve is the probability weighted average of the nine curves.

TABLE I–1. FRAGILITY PARAMETERS FOR REACTOR COOLANT PUMP AND STEAM GENERATOR SUPPORTS

Fragility parameter	Reactor coolant pump support	Steam generator support
Median capacity A_m (g)	1.74	1.71
Standard deviation for random variability β_r	0.35	0.36
Standard deviation for uncertainty β_u	0.32	0.39
Composite variability $\beta_c = \sqrt{\beta_r^2 + \beta_u^2}$	0.47	0.53

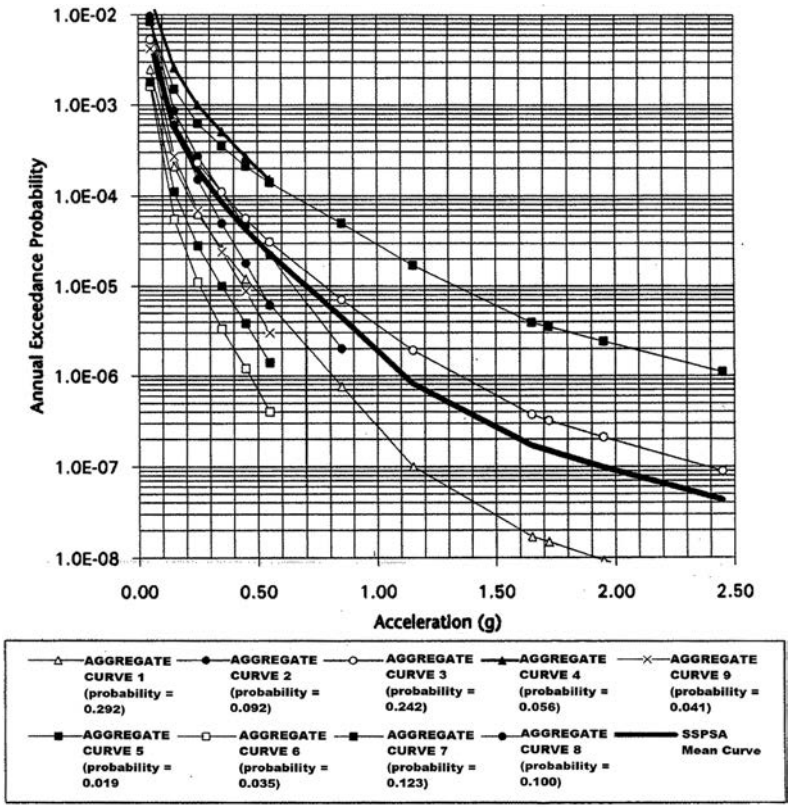


FIG. I–2. Seismic hazard curves from individual plant examination of external events, Seabrook Station Probabilistic Safety Assessment (SSPSA).

TABLE I–2. DISCRETE HAZARD CURVE DATA FROM FIG. I–2

Peak ground acceleration (g)	Frequency of exceedance per site-year									
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8	Model 9	Mean
0.05	2.50×10^{-3}	1.00×10^{-2}	5.20×10^{-3}	1.50×10^{-2}	1.80×10^{-3}	1.50×10^{-3}	8.50×10^{-3}	8.50×10^{-3}	4.00×10^{-3}	5.89×10^{-3}
0.15	2.00×10^{-4}	8.50×10^{-4}	6.60×10^{-4}	2.40×10^{-3}	1.10×10^{-4}	5.50×10^{-5}	1.40×10^{-3}	8.40×10^{-4}	3.00×10^{-4}	7.03×10^{-4}
0.25	6.00×10^{-5}	1.40×10^{-4}	2.20×10^{-4}	9.80×10^{-4}	2.80×10^{-5}	3.20×10^{-6}	6.50×10^{-4}	2.80×10^{-4}	7.00×10^{-5}	2.50×10^{-4}
0.35	2.50×10^{-5}	5.00×10^{-5}	1.10×10^{-4}	5.00×10^{-4}	1.00×10^{-5}	1.20×10^{-6}	3.40×10^{-4}	1.10×10^{-4}	2.30×10^{-5}	1.21×10^{-4}
0.45	1.20×10^{-5}	1.80×10^{-5}	5.60×10^{-5}	2.80×10^{-4}	4.00×10^{-6}	4.00×10^{-7}	2.00×10^{-4}	4.70×10^{-5}	9.00×10^{-6}	6.42×10^{-5}
0.55	6.50×10^{-6}	6.00×10^{-6}	3.10×10^{-5}	1.50×10^{-4}	1.30×10^{-6}		1.30×10^{-4}	2.20×10^{-5}	3.00×10^{-6}	3.67×10^{-5}
0.65	3.20×10^{-6}		1.90×10^{-5}				1.00×10^{-4}	1.00×10^{-5}		1.88×10^{-5}
0.75	1.50×10^{-6}		1.20×10^{-5}				7.00×10^{-5}	4.30×10^{-6}		1.24×10^{-5}
0.85	7.50×10^{-6}		7.00×10^{-6}				5.00×10^{-5}	2.00×10^{-6}		8.26×10^{-6}
0.95	4.00×10^{-7}		4.40×10^{-6}				3.30×10^{-5}			5.24×10^{-6}
1.05	2.00×10^{-7}		3.00×10^{-6}				2.30×10^{-5}			3.61×10^{-6}

TABLE I–2. DISCRETE HAZARD CURVE DATA FROM FIG. I–2 (cont.)

Peak ground acceleration (g)	Frequency of exceedance per site-year									
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8	Model 9	Mean
1.15	1.00×10^{-7}		2.00×10^{-6}				1.70×10^{-5}			2.60×10^{-6}
1.25	7.00×10^{-8}		1.25×10^{-6}				1.20×10^{-5}			1.80×10^{-6}
1.35	5.00×10^{-8}		1.00×10^{-6}				9.30×10^{-6}			1.40×10^{-6}
1.45	3.30×10^{-8}		7.20×10^{-7}				7.00×10^{-6}			1.04×10^{-6}
1.55	2.30×10^{-8}		5.10×10^{-7}				5.20×10^{-6}			7.70×10^{-7}
1.65	1.70×10^{-8}		3.70×10^{-7}				4.00×10^{-6}			5.87×10^{-7}
1.75	1.40×10^{-8}		3.00×10^{-7}				3.30×10^{-6}			$4.83\times10–7$
1.85	1.20×10^{-8}		2.40×10^{-7}				2.80×10^{-6}			4.06×10^{-7}
1.95	9.00×10^{-9}		2.10×10^{-7}				2.30×10^{-6}			3.36×10^{-7}
2.05	7.00×10^{-9}		1.70×10^{-7}				2.00×10^{-6}			2.89×10^{-7}
2.15	6.00×10^{-9}		1.40×10^{-7}				1.70×10^{-6}			2.45×10^{-7}

TABLE I–2. DISCRETE HAZARD CURVE DATA FROM FIG. I–2 (cont.)

Peak ground acceleration (g)	Frequency of exceedance per site-year									
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8	Model 9	Mean
2.25	5.00×10^{-9}		1.20×10^{-7}				1.40×10^{-6}			2.03×10^{-7}
2.35	4.00×10^{-9}		1.00×10^{-7}				1.30×10^{-6}			1.85×10^{-7}
2.45	3.00×10^{-9}		9.00×10^{-8}				1.10×10^{-6}			1.58×10^{-7}

Note: Empty cells are valued at 0.0. Mean frequency at each peak ground acceleration is the probability weighted average over the nine models.

Table I–3 shows the discretization of the seismic hazard and the associated mean seismic hazard frequency for Seabrook IPEEEs for use in Eq. (I–2). The discrete hazard intervals are selected to provide a reasonable approximation to the continuous model. In practice, ten intervals are sufficient for a reasonable approximation.

I–1.3. Treatment of epistemic uncertainty

With input from Eq. (I–3), Eq. (I–2) is evaluated first in terms of mean point estimates and then with a quantification of epistemic uncertainty. For the mean point estimate, the mean hazard curve is used, as shown in Table I–3, and the mean fragility curves are used for the RCP/SG supports. The mean fragility curve is the log-normal distribution defined by the median capacity and the composite variability as shown in the last row of Table I–1.

TABLE I–3. MEAN SEISMIC DISCRETE INTERVAL FREQUENCIES

Interval index k in Eq. (I–1)	Fragility peak ground acceleration reference level (g)	Peak ground acceleration range (g)		h_k in Eq. (I–1) (frequency per site-year)
		Lower	Upper	
1	0.1	0.05	0.15	5.19×10^{-3}
2	0.2	0.15	0.25	4.53×10^{-4}
3	0.3	0.25	0.35	1.2×10^{-4}
4	0.4	0.35	0.45	5.64×10^{-5}
5	0.5	0.45	0.55	2.75×10^{-5}
6	0.7	0.55	0.85	2.84×10^{-5}
7	1	0.85	1.15	5.66×10^{-6}
8	1.4	1.15	1.65	2.02×10^{-6}
9	1.85	1.65	2.05	2.97×10^{-7}
10	2.25	2.05	2.45	1.31×10^{-7}
11	2.5	>2.45		1.58×10^{-7}

For the quantification of uncertainty, the epistemic uncertainty is reflected by the probability weights over the nine discrete hazard curves shown in Fig. I–2 and Table I–2. In the Monte Carlo sampling, a discrete distribution (see Fig. I–3) is sampled to determine which of the nine hazard curves to use for that trial. This is essentially the same method described in Ref. [I–6] as the Monte Carlo method.

For treatment of epistemic uncertainty in the fragility curves, a normal distribution is sampled with a mean of 0 and a standard deviation of β_u, which is denoted as $\Phi(0, \beta_u)$ [I–6]. The fragility f at a given reference PGA level k is then:

$$f_k = \Phi\left(z_k, 0, 1\right) \tag{I–7}$$

$$z_k = \frac{\ln\left(\frac{x_k}{A_m}\right) - \Phi\left(0, \beta_u\right)}{\beta_r} \tag{I–8}$$

where $\Phi(z_k, 0, 1)$ is the cumulative normal distribution with a mean of 0 and a standard deviation of 1, evaluated at z_k and reference level k, and x_k is the PGA at reference level k.

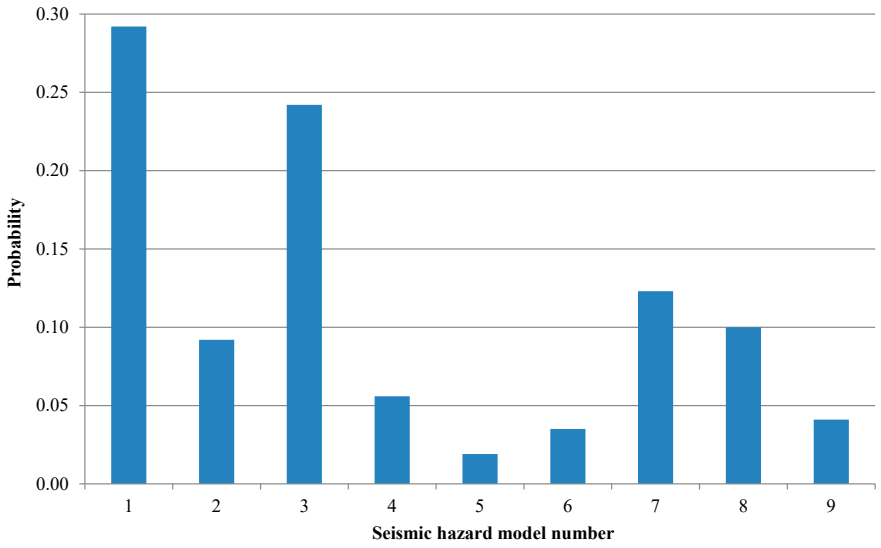


FIG. I–3. Discrete distribution for epistemic uncertainty in seismic hazard.

To check this method of sampling for the fragility uncertainty, a sample run of 10^6 Monte Carlo trials was performed (see Table I–4).[1] The results demonstrate excellent agreement to two significant figures; and hence, the Monte Carlo sampling method is sufficiently robust for these examples. It should be noted that fragilities below 10^{-3} have a questionable meaning. In practice, fragility analysts recommend that log-normal distributions be truncated (i.e. set to 0.0 at some reasonably low level to reflect the realistic seismic capacities of equipment).

I–1.4. Mean point estimate results

The point estimate results obtained using mean estimates for hazard and fragilities are presented in this section. Figure I–4 shows the conditional LOCA outcome probabilities evaluated using Eqs (I–4)–(I–6) for three levels of assumed seismic CCF coupling (0%, 20% and 50%). An important result is the significant probability of multiple LOCAs even when no seismic common cause is assumed. This is due to the high probability of multiple, independent LOCAs when the PGA approaches the median seismic capacity. When the α parameter is set to any value greater than 0.5, the relative importance of multi-unit LOCAs either competes with, or exceeds, that of a single unit LOCA across the entire PGA range.

This highlights an important limitation of earlier seismic PSAs that anchor the initiating models to the types of initiating event included in internal event PSAs. In internal events PSAs, the simultaneous combination of multiple initiating events can be dismissed as long as there is no causal link that makes the frequencies of these combinations significant. In this example, however, the causal link is created by the occurrence of a seismic event that impacts the entire site. Even though the seismic responses of different reactor units and different components within each unit are not necessarily correlated, the time synchronization is forced by the seismic event, so multiple initiating events need to be considered with or without seismic CCF.

The simple seismic CCF model shows that seismic common cause could be a significant contributor to the seismic risk, but that seismic correlation is not necessary to create significant probabilities of multiple initiating events. Such multiple events can involve both single or multiple units, but all combinations need to be considered. Excluding combinations just because they were omitted for internal event purposes is not justified for site wide hazards such as seismic events. The two LOCA case increases with increasing α as would be expected.

---

[1] This large number of trials is not necessary for the uncertainty analysis but was used in this case just to debug the model. The actual uncertainty analysis was performed using 100 000 trials but several thousand trials would have been sufficient according to Ref. [I–6].

TABLE I–4. CHECKING THE MONTE CARLO METHOD FOR SAMPLING FRAGILITY

Peak ground acceleration reference level (g)	Mean*		5%-tile		Median		95%-tile	
	Formula	Monte Carlo	Formula	Monte Carlo	Formula	Monte Carlo	Formula	Monte Carlo
0.1	2.46×10^{-7}	2.42×10^{-7}	3.10×10^{-28}	3.13×10^{-28}	2.50×10^{-18}	2.50×10^{-18}	1.07×10^{-10}	1.06×10^{-10}
0.2	3.15×10^{-4}	3.22×10^{-4}	1.38×10^{-16}	1.39×10^{-16}	2.04×10^{-9}	2.04×10^{-9}	1.73×10^{-4}	1.72×10^{-4}
0.3	6.65×10^{-3}	6.68×10^{-3}	2.66×10^{-11}	2.67×10^{-11}	1.03×10^{-5}	1.03×10^{-5}	2.52×10^{-2}	2.52×10^{-2}
0.4	3.54×10^{-2}	3.54×10^{-2}	3.13×10^{-8}	3.15×10^{-8}	9.41×10^{-4}	9.42×10^{-4}	2.10×10^{-1}	2.10×10^{-1}
0.5	9.89×10^{-2}	9.89×10^{-2}	3.11×10^{-6}	3.13×10^{-6}	1.34×10^{-2}	1.34×10^{-2}	5.35×10^{-1}	5.34×10^{-1}
0.6	1.94×10^{-1}	1.94×10^{-1}	7.56×10^{-5}	7.58×10^{-5}	6.86×10^{-2}	6.86×10^{-2}	7.93×10^{-1}	7.93×10^{-1}
0.7	3.07×10^{-1}	3.07×10^{-1}	7.55×10^{-4}	7.58×10^{-4}	1.92×10^{-1}	1.92×10^{-1}	9.24×10^{-1}	9.24×10^{-1}
0.8	4.23×10^{-1}	4.23×10^{-1}	4.16×10^{-3}	4.18×10^{-3}	3.69×10^{-1}	3.69×10^{-1}	9.75×10^{-1}	9.75×10^{-1}
0.9	5.31×10^{-1}	5.31×10^{-1}	1.51×10^{-2}	1.51×10^{-2}	5.54×10^{-1}	5.54×10^{-1}	9.93×10^{-1}	9.93×10^{-1}
1	6.27×10^{-1}	6.27×10^{-1}	4.04×10^{-2}	4.05×10^{-2}	7.11×10^{-1}	7.11×10^{-1}	9.98×10^{-1}	9.98×10^{-1}
1.1	7.07×10^{-1}	7.07×10^{-1}	8.62×10^{-2}	8.63×10^{-2}	8.26×10^{-1}	8.26×10^{-1}	9.99×10^{-1}	9.99×10^{-1}

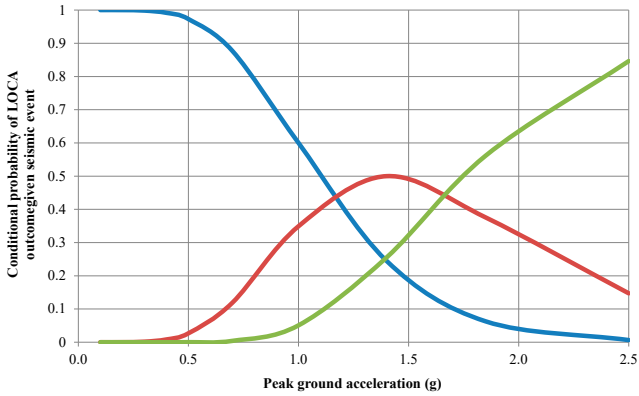
TABLE I–4. CHECKING THE MONTE CARLO METHOD FOR SAMPLING FRAGILITY (cont.)

Peak ground acceleration reference level (g)	Mean*		5%-tile		Median		95%-tile	
	Formula	Monte Carlo	Formula	Monte Carlo	Formula	Monte Carlo	Formula	Monte Carlo
1.2	7.73×10^{-1}	7.73×10^{-1}	1.55×10^{-1}	1.55×10^{-1}	9.01×10^{-1}	9.01×10^{-1}	1.00	1.00
1.3	8.25×10^{-1}	8.25×10^{-1}	2.43×10^{-1}	2.43×10^{-1}	9.46×10^{-1}	9.46×10^{-1}	1.00	1.00
1.4	8.66×10^{-1}	8.66×10^{-1}	3.45×10^{-1}	3.45×10^{-1}	9.71×10^{-1}	9.71×10^{-1}	1.00	1.00
1.5	8.97×10^{-1}	8.97×10^{-1}	4.51×10^{-1}	4.51×10^{-1}	9.85×10^{-1}	9.85×10^{-1}	1.00	1.00
1.6	9.22×10^{-1}	9.22×10^{-1}	5.53×10^{-1}	5.54×10^{-1}	9.93×10^{-1}	9.93×10^{-1}	1.00	1.00
1.7	9.40×10^{-1}	9.40×10^{-1}	6.47×10^{-1}	6.47×10^{-1}	9.96×10^{-1}	9.96×10^{-1}	1.00	1.00
1.8	9.55×10^{-1}	9.55×10^{-1}	7.27×10^{-1}	7.28×10^{-1}	9.98×10^{-1}	9.98×10^{-1}	1.00	1.00
1.9	9.65×10^{-1}	9.65×10^{-1}	7.94×10^{-1}	7.95×10^{-1}	9.99×10^{-1}	9.99×10^{-1}	1.00	1.00
2	9.74×10^{-1}	9.74×10^{-1}	8.48×10^{-1}	8.48×10^{-1}	1.00	1.00	1.00	1.00
2.1	9.80×10^{-1}	9.80×10^{-1}	8.89×10^{-1}	8.89×10^{-1}	1.00	1.00	1.00	1.00
2.2	9.84×10^{-1}	9.85×10^{-1}	9.20×10^{-1}	9.21×10^{-1}	1.00	1.00	1.00	1.00

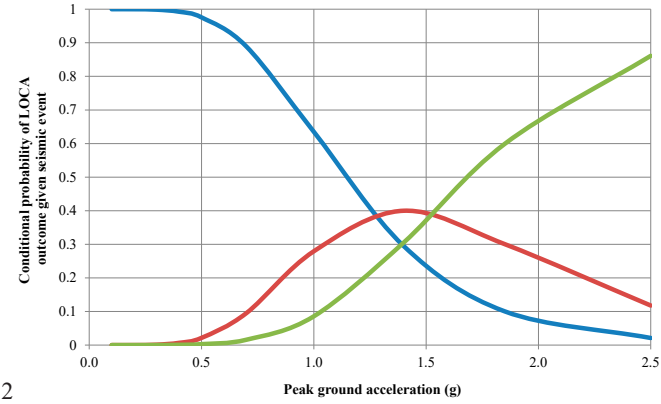
TABLE I–4. CHECKING THE MONTE CARLO METHOD FOR SAMPLING FRAGILITY (cont.)

Peak ground acceleration reference level (g)	Mean*		5%-tile		Median		95%-tile	
	Formula	Monte Carlo	Formula	Monte Carlo	Formula	Monte Carlo	Formula	Monte Carlo
2.3	9.88×10^{-1}	9.88×10^{-1}	9.44×10^{-1}	9.44×10^{-1}	1.00	1.00	1.00	1.00
2.4	9.91×10^{-1}	9.91×10^{-1}	9.60×10^{-1}	9.61×10^{-1}	1.00	1.00	1.00	1.00
2.5	9.93×10^{-1}	9.93×10^{-1}	9.73×10^{-1}	9.73×10^{-1}	1.00	1.00	1.00	1.00

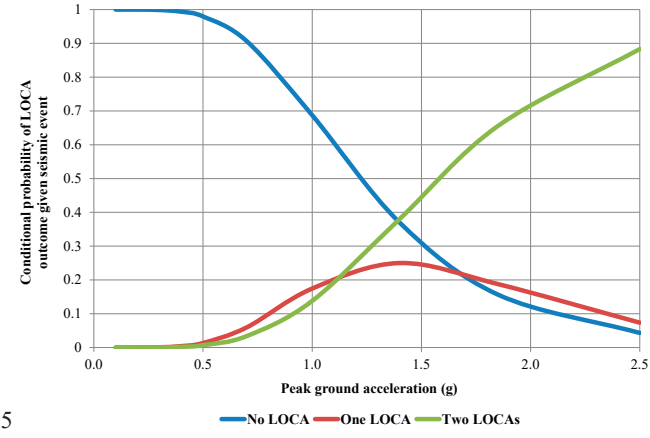
* A comparison check for the following fragility parameters: median capacity = 0.87g, $\beta_r = 0.25$ and $\beta_u = 0.35$.



(a) $\alpha = 0$



(b) $\alpha = 0.2$



(c) $\alpha = 0.5$

FIG. I–4. Loss of coolant accident outcome probabilities versus g level.

In Fig. I–5, the sensitivity of the annual frequency of two concurrent LOCAs is examined as a function of the g level and seismic common cause parameter by applying Eq. (I–2) and the LOCA state probability for two LOCAs in Eq. (I–5). As Fig. I–5 shows, increasing the CCF parameter has a significant influence on the dual unit seismic initiating event frequency; however, even with no seismic CCF ($\alpha = 0$), the frequency of this dual unit LOCA exceeds 10^{-7} per site-year at PGA levels above 0.7g. Given that these are likely excessive LOCAs, the multi-unit core damage frequency would also be very significant. For PGA levels at 1.4g and above, which is approximately the median capacity of the RCP/SG supports, the frequency of a dual unit LOCA is virtually independent of the value of the common cause parameter. This is due to the high probability of multiple, independent failures at these high seismic intensities.

Figure I–6 compares single and dual unit LOCA frequencies for different levels of seismic CCF parameter. In all of these figures, the relative importance of dual unit increases as g levels increase, and with α. When $\alpha = 0.5$, the single and dual unit LOCA frequencies are nearly the same, and for higher levels of α, the dual unit LOCAs begin to dominate.

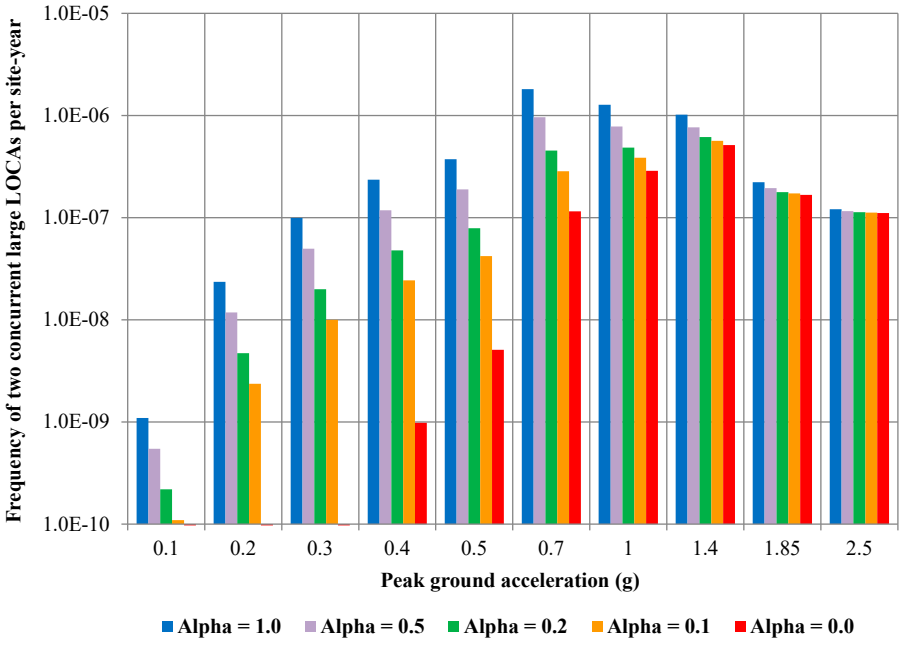
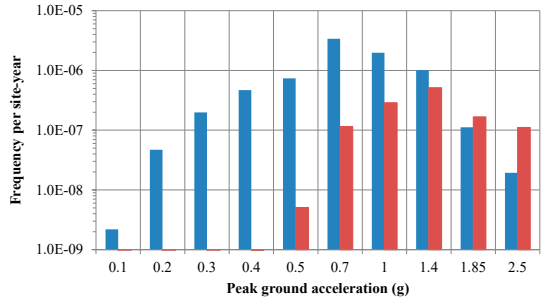
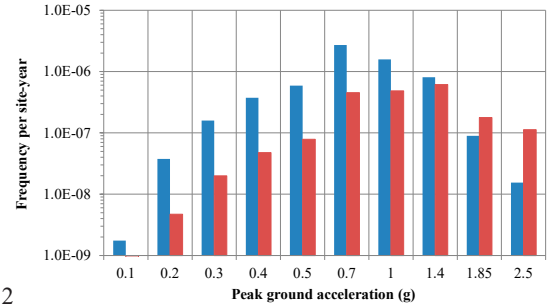


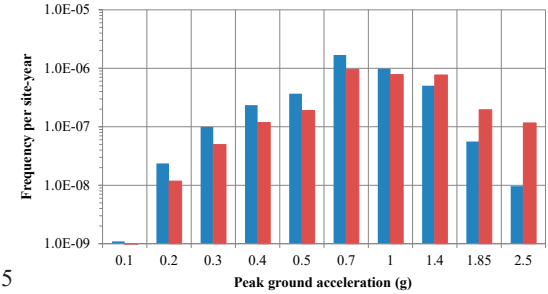
FIG. I–5. Frequency of two concurrent loss of coolant accidents versus peak ground acceleration and the α parameter.



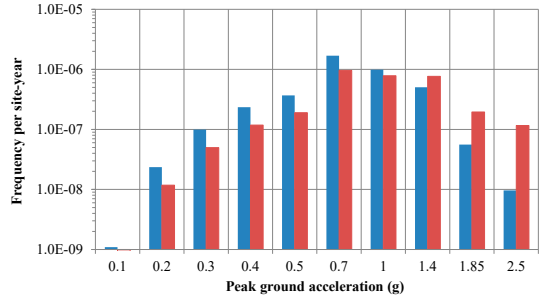
(a) $\alpha = 0$



(b) $\alpha = 0.2$



(c) $\alpha = 0.5$



(d) $\alpha = 0.9$

FIG. I–6. Comparison of loss of coolant accident initiating event frequencies.

In the PRA standard [I–7] of the American Society of Mechanical Engineers and the American Nuclear Society, the risk significance of an accident sequence is defined as one that makes at least a 1% contribution to the total risk associated with that hazard group. Even when there is no seismic CCF ($\alpha = 0$), the frequency of two LOCAs exceeds that of one LOCA at g levels greater than 1.4g; and for $\alpha = 0.2$, 0.5 and 0.9, the dual LOCA frequency is either significant or dominant across the entire PGA range considered (see Fig. I–6).

I–1.5. Results with epistemic uncertainties quantified

Tables I–5 and I–6 present the results of the uncertainty quantification which cover the frequencies of two concurrent LOCAs for α values of 0 and 0.2. The mean of the distributions for two concurrent LOCAs is generally higher than the point estimates (especially for low PGA values) due to state of knowledge correlation. There is a linear and a quadratic term in Eq. (I–6), which is the model for calculating the dual LOCA fragility. The mean point estimate will propagate in the linear term, but this is not the case in the quadratic term.

The other key result of this and every other seismic PSA uncertainty analysis are the large uncertainties as expressed by the range factors. These large uncertainties stem primarily from uncertainty in the hazard curve; however, the uncertainty in fragility curves is also significant. The range factors are greatest when g levels and absolute frequencies are lowest. There are pitfalls to measuring uncertainty with ‘log-normal’ thinking because, as seen in the hazard uncertainty, some seismologists assert that the frequency of larger acceleration levels at the site is essentially zero, which is evidenced by the 5th percentile values of 0 in the LOCA frequency results in Tables I–5 and I–6 at g levels above 0.7g. It should be noted that, the lower tails of the log-normal distributions in these calculations were not truncated as is recommended by fragility analysts. Truncation of the fragilities would increase the number of Monte Carlo samples where the frequency of the initiating event is set to 0.

I–2. SEISMICALLY INDUCED LOSS OF COOLANT ACCIDENT MODEL WITH MULTI-UNIT COMMON CAUSE FAILURE: COMPLEX VERSION

The simple version assumed that LOCAs that occur within each unit are always fully correlated but with the possibility for a variable degree of correlation between LOCAs on different units. In reality, at plants like Seabrook there are four nominally identical reactor coolant loops within each unit. Three of these are identical and the fourth has the same physical dimensions, except that one of

TABLE I–5. FREQUENCY OF TWO LOSS OF COOLANT ACCIDENTS ($\alpha = 0$)

Peak ground acceleration (g)	Mean point estimate	Uncertainty distribution parameters					
		Mean	5%-tile	50%-tile	95%-tile	RF1[a]	RF2[b]
0.1	1.05×10^{-17}	1.08×10^{-14}	2.91×10^{-39}	6.77×10^{-30}	4.13×10^{-21}	1.19×10^{9}	6.10×10^{8}
0.2	3.79×10^{-13}	1.17×10^{-10}	6.90×10^{-27}	1.00×10^{-19}	2.06×10^{-13}	5.46×10^{6}	2.06×10^{6}
0.3	5.06×10^{-11}	3.24×10^{-9}	3.77×10^{-21}	3.08×10^{-15}	2.71×10^{-10}	2.68×10^{5}	8.79×10^{4}
0.4	9.30×10^{-10}	1.82×10^{-8}	1.07×10^{-17}	1.17×10^{-12}	1.17×10^{-8}	3.30×10^{4}	9.96×10^{3}
0.5	5.76×10^{-9}	4.98×10^{-8}	1.91×10^{-15}	4.52×10^{-11}	8.88×10^{-8}	6.81×10^{3}	1.96×10^{3}
0.7	1.49×10^{-7}	4.85×10^{-7}	1.89×10^{-6}	7.90×10^{-9}	1.89×10^{-6}	1.00	2.39×10^{2}
1	3.78×10^{-7}	6.29×10^{-7}	0.00	2.20×10^{-8}	2.88×10^{-6}	∞[c]	1.31×10^{2}
1.4	6.38×10^{-7}	7.44×10^{-7}	0.00	2.20×10^{-8}	5.35×10^{-6}	∞[c]	2.43×10^{2}
1.85	1.91×10^{-7}	1.94×10^{-7}	0.00	7.23×10^{-9}	1.63×10^{-6}	∞[c]	2.26×10^{2}
2.5	1.18×10^{-7}	1.14×10^{-7}	0.00	3.86×10^{-9}	8.83×10^{-7}	∞[c]	2.29×10^{2}
Total	1.48×10^{-6}	2.24×10^{-6}	1.89×10^{-11}	1.58×10^{-7}	1.19×10^{-5}	7.92×10^{2}	7.50×10^{1}

[a] Release frequency, RF1 = (95%-tile/5%-tile)^{½}.

[b] RF2 = 95%-tile/50%-tile.

[c] RF1 is infinity because the 5%-tile is zero. This stems from specific hazard models that predict a maximum seismic intensity of <1.0g at this site.

TABLE I–6. FREQUENCY OF TWO LOSS OF COOLANT ACCIDENTS ($\alpha = 0.2$)

Peak ground acceleration (g)	Mean point estimate	Uncertainty distribution parameters					
		Mean	5%-tile	50%-tile	95%-tile	RF1[a]	RF2[b]
0.1	4.68×10^{-11}	9.20×10^{-11}	6.93×10^{-22}	3.47×10^{-17}	1.00×10^{-12}	3.80×10^{4}	2.88×10^{4}
0.2	2.62×10^{-9}	3.53×10^{-9}	2.78×10^{-16}	1.15×10^{-12}	1.98×10^{-9}	2.67×10^{3}	1.72×10^{3}
0.3	1.62×10^{-8}	2.13×10^{-8}	8.95×10^{-14}	9.95×10^{-11}	3.76×10^{-8}	6.49×10^{2}	3.78×10^{2}
0.4	4.65×10^{-8}	6.50×10^{-8}	2.84×10^{-12}	1.23×10^{-9}	1.79×10^{-7}	2.51×10^{2}	1.46×10^{2}
0.5	8.42×10^{-8}	1.26×10^{-7}	2.40×10^{-11}	5.08×10^{-9}	4.18×10^{-7}	1.32×10^{2}	8.22×10^{1}
0.7	5.30×10^{-7}	8.25×10^{-7}	2.67×10^{-10}	7.08×10^{-8}	3.36×10^{-6}	1.12×10^{2}	4.75×10^{1}
1	5.95×10^{-7}	7.96×10^{-7}	0.00	5.65×10^{-8}	3.71×10^{-6}	∞[c]	6.57×10^{1}
1.4	7.37×10^{-7}	8.17×10^{-7}	0.00	2.76×10^{-8}	5.94×10^{-6}	∞[c]	2.15×10^{2}
1.85	2.01×10^{-7}	2.02×10^{-7}	0.00	7.47×10^{-9}	1.66×10^{-6}	∞[c]	2.23×10^{2}
2.5	1.19×10^{-7}	1.15×10^{-7}	0.00	3.87×10^{-9}	8.85×10^{-7}	∞[c]	2.29×10^{2}

[a] Release frequency, RF1 = (95%-tile/5%-tile)$^{1/2}$.

[b] RF2 = 95%-tile/50%-tile.

[c] RF1 is infinity because the 5%-tile is zero. This stems from specific hazard models that predict a maximum seismic intensity of <1.0g at this site.

the hot legs has a pressurizer attached and the associated surge line piping and connected piping for pressurizer sprays, heaters, and safety and relief valves. The SG/RCP supports are the same on all four loops. In the complex version of the model, it is necessary to ignore the asymmetry resulting from the loop with the pressurizer and consider that there are four identical loops.

If the supports on only one loop fail in a given unit and the breach is limited to a large LOCA with a single break, the LOCA can be mitigated by operation of the emergency core cooling system in that unit if that equipment is available and not damaged by the seismic event.[2] If, however, two or more loops fail in a given unit, this would likely lead to an excessive LOCA and the mitigation possibilities are greatly reduced, if not eliminated. There could be seismic CCFs involving multiple loops in the same unit as well as multiple loops in different units. Presumably, the distance that separates the loops and the fact that each unit resides in a different reactor containment structure would suggest that the common cause potential within a unit is greater than that between units. Hence, this model includes two tiers of seismic CCF.

The possible end states for the two unit plant are also more complex because each reactor unit has either no LOCA, a single break LOCA (assumed here to be a large LOCA) or an excessive LOCA resulting from multiple breaks in a given unit. All nine combinations of outcomes at the two unit station are possible end states in this model (symmetry assumptions can reduce this to six).

In the first stage, the model is built for a single four loop PWR unit with seismic CCF among the loops (see Fig. I–7). From the event tree, the conditional probabilities for no LOCA (N), a large (single loop) LOCA (L) and an excessive (multiple loop) LOCA given a seismic event for a four loop PWR reactor unit are:

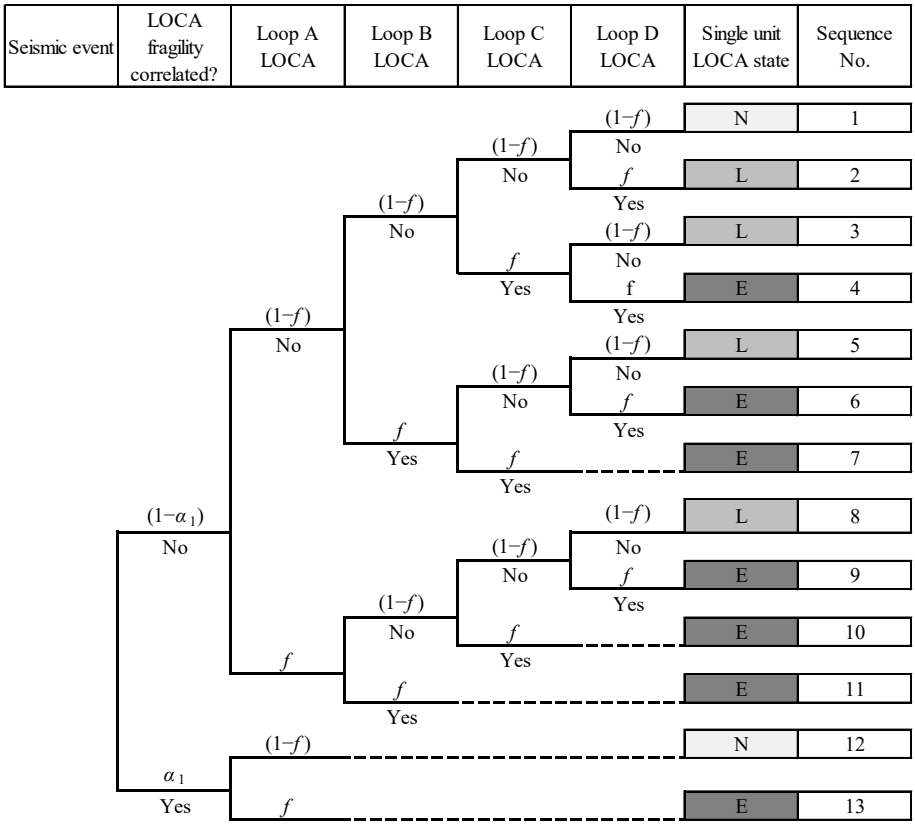
$$P(\mathrm{N}) = \alpha_1(1-f) + (1-\alpha_1)(1-f)^4 \tag{I–9}$$

$$P(\mathrm{L}) = 4(1-\alpha_1)f(1-f)^3 \tag{I–10}$$

$$\begin{aligned} P(\mathrm{E}) &= 1 - P(\mathrm{N}) - P(\mathrm{L}) \\ &= 1 - \alpha_1(1-f) - (1-\alpha_1)(1-f)^4 - 4(1-\alpha_1)f(1-f)^3 \end{aligned} \tag{I–11}$$

---

[2] The seismic capacities of the emergency core cooling system equipment that are needed to mitigate the large LOCA would also need to be considered in a full seismic PSA but are not included in this example. These capacities are in fact lower than those of the SG/RCP supports, and hence, the conditional probability of core damage given a large LOCA due to seismic failures is relatively high. These failures are classified as large or excessive LOCAs and may not have a major influence on the results. Indeed, in the Seabrook IPEEE this was confirmed in a sensitivity analysis.



Note: N — no LOCA; L — large LOCA; E — excessive LOCA.

FIG. I–7. Event tree for loss of coolant accident outcomes in four loss of off-site power pressurized water reactor units.

where f is fragility for LOCA at each reactor unit due to failure of a SG/RCP support (see Eq. (I–3), in Section I–1) and α_1 is within the unit seismic common cause parameter for a seismically induced CCF of multiple loops within a reactor unit.

The next step is to build the model for the two unit plant (see Fig. I–8). In this event tree, a second tier of seismic CCF is introduced to consider seismically induced CCFs involving LOCAs of different types involving multiple units. All nine combinations of LOCA responses between the two units are considered. Invoking the assumption of symmetry, which would be appropriate for identical units such as the original design for Seabrook, the conditional probabilities of each of the six distinct end states can be defined as:

$$P(\mathrm{N}, \mathrm{N}) = (1 - \alpha_2)P(\mathrm{N})^2 + \alpha_2 P(\mathrm{N}) \quad \text{(I–12)}$$

$$P(\mathrm{N}, \mathrm{L}) = 2(1 - \alpha_2)P(\mathrm{N})P(\mathrm{L}) \quad \text{(I–13)}$$

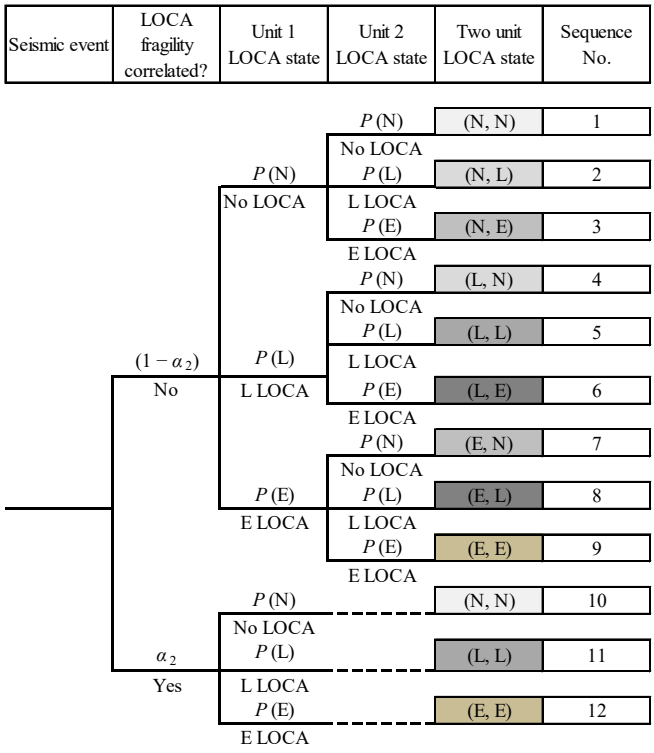
$$P(\mathrm{N}, \mathrm{E}) = 2(1 - \alpha_2)P(\mathrm{N})P(\mathrm{E}) \quad \text{(I–14)}$$

$$P(\mathrm{L}, \mathrm{E}) = 2(1 - \alpha_2)P(\mathrm{L})P(\mathrm{E}) \quad \text{(I–15)}$$

$$P(\mathrm{L}, \mathrm{L}) = (1 - \alpha_2)P(\mathrm{L})^2 + \alpha_2 P(\mathrm{L}) \quad \text{(I–16)}$$

$$P(\mathrm{E}, \mathrm{E}) = (1 - \alpha_2)P(\mathrm{E})^2 + \alpha_2 P(\mathrm{E}) \quad \text{(I–17)}$$

where α_2 is the inter-unit CCF parameter for a seismically induced LOCA response on both units.



Note: N — no LOCA; L — large LOCA; E — excessive LOCA.

FIG. I–8. Event tree for a multi-unit loss of coolant accident response.

It is possible to quantify this complex model using the same inputs as used in the simplified version; except in this case, there are two different seismic CCF parameters to consider, instead of one. In Fig. I–9, the results for no seismic common cause are shown either within each unit or between the units (i.e. both α_1 and α_2 are set to 0). It should be noted that states (N, L) and (N, E) involve LOCA initiating events on one unit only, but states (L, L), (L, E) and (E, E) involve LOCA states on both units. Even though there is no seismic CCF assumed in this case, at PGA levels around 0.5g, the dual unit initiating events become significant, and at around 1.0g and higher, they begin to dominate the LOCA state probabilities. Hence, as with the simple version, this model reaffirms the conclusion that it is not necessary to invoke seismic correlation of any kind to yield significant probabilities of multi-unit initiating events.

An additional case of seismic CCF assumptions is shown in Fig. I–10, where it is assumed that both common cause parameters are equal to 0.3. As these common cause parameters are increased, the relative probabilities of the single unit initiating events are reduced, and those for the multi-unit events are increased. Increasing either common cause parameter increases the likelihood of an excessive LOCA on either or both units.

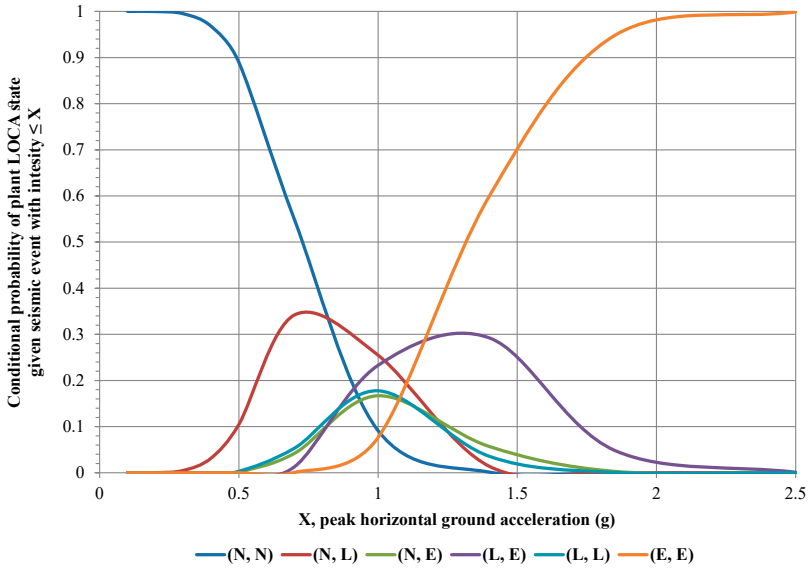


FIG. I–9. Conditional loss of coolant accident outcome probabilities for a two unit plant with no seismic common cause failure (α_1 and α_2 set to 0).

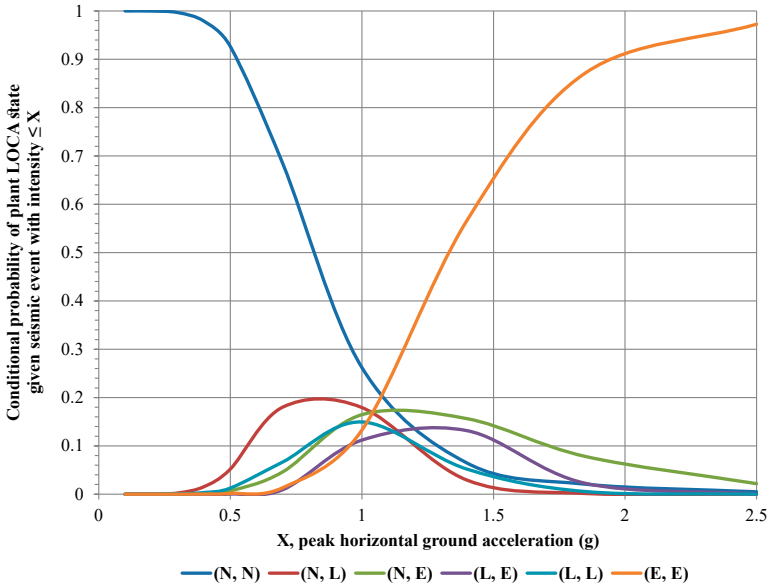


FIG. I–10. Conditional loss of coolant accident outcome probabilities for a two unit plant with a common cause failure (α_1 and α_2 set to 0.3).

When the probabilities of the seismic plant LOCA states are combined with the seismic hazard frequencies, the annual frequencies of the various seismic initiating events can be estimated. This model produces six distinct initiating event frequencies, defined by the six end states in Fig. I–8, which includes for completeness the non-occurrence of LOCA on both units (N, N). In Fig. I–11, the initiating event frequencies for the two unit plant states (N, L), (L, L) and (E, E) are presented for the cases where both seismic common cause parameters are set to 0.0 and 0.3.

I–3. CONCLUSION

Based on the results from the two models and using inputs from seismic hazard and fragility estimates from the Seabrook IPEEE, the following conclusions can be reached about seismically induced initiating events:

(a) Although the examples are limited to identical components in two identical reactor units, many of the insights are applicable to units of different designs and combinations of non-identical components. While the extent of seismic correlation may be amplified in symmetric conditions, the risk significance

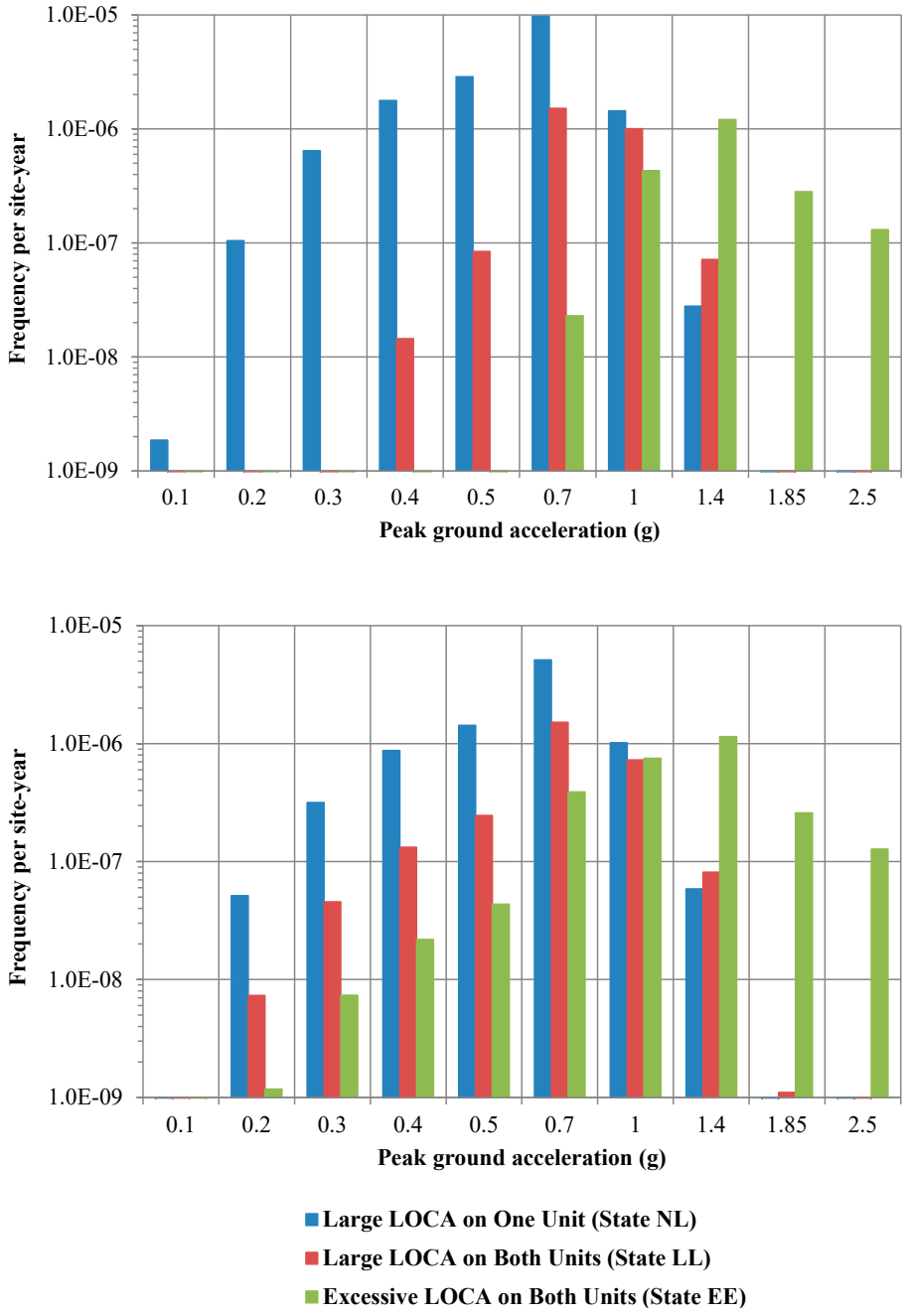


FIG. I–11. Selected initiating event frequencies for a two unit plant with no seismic common cause failure (top: $\alpha_1 = \alpha_2 = 0$; bottom: $\alpha_1 = \alpha_2 = 0.3$).

of multiple combinations of failures in multiple units needs to be carefully considered in an MUPSA.

(b) Current seismic PSA models use a combination of assumptions to treat seismic CCF between identical components that share a common fragility curve. Seismic CCF involving failures in different reactor units is seldom, if ever, treated because PSAs are typically only performed on one unit at a time. The simple and complex versions of the model both permit the explicit modelling of independent combinations and seismically induced CCFs within a unit and across multiple units. Such explicit modelling provides a more structured way to perform sensitivity analyses in seismic PSAs than simply applying individual assumptions with regard to either complete dependence or complete independence among seismic fragilities.

(c) While it is important to consider the extent of seismic correlation assumed in a seismic common cause model, seismic correlation is not necessary to yield a significant frequency of dual unit LOCA initiating events caused by seismic events. The results obtained from both versions of the model strongly support this conclusion. This stems from the fact that as the g level increases, the fragilities increase to levels at which the independent combinations of fragilities cannot be ignored and begin to dominate. Seismic CCF amplifies the importance of multiple seismic initiating events at a site at the lower g levels, but consideration of correlation is not necessary to justify considering them.

(d) In the treatment of identical, redundant equipment for systems required to mitigate a seismically induced initiating event, seismic correlation is often modelled conservatively by assuming that all similar components fail owing to a seismic common cause. This aspect of the treatment is inarguably conservative. However, CCFs in the treatment of seismically induced initiating events have in most cases been ignored, especially with regard to concurrent initiating events on different units at the same site.[3] This aspect of traditional seismic common cause treatment is certainly non-conservative. The examples in this annex illustrate that a more robust way to address correlation is to include a model that addresses both independent combinations and common cause events in a manner similar to the treatment of CCFs in the internal events PSA. In the near term, the correlation parameters similar to α can be used to perform a more robust set of sensitivity analyses to address this source of uncertainty. In the longer term, it will be necessary to expand

[3] The example used in this annex is failures of the SG/RCP supports creating LOCA. Some PSAs have treated this failure mode as an excessive LOCA, in part based on a concern that these might be CCFs impacting multiple loops. However, seismically induced CCF across multiple units is seldom considered.

the fragility analysis to include a quantification of the correlation coefficients. This may be a candidate for an expert elicitation until a more scientific way to quantify these parameters is available.

(e) The continued practice of modelling each seismically induced initiating event as a single isolated occurrence, as done in the internal events analysis, is not justified for g levels at which the fragilities start to rise (conditional probability of failure approaches 1).

(f) There was never any real justification for excluding concurrent, seismically induced accidents on more than one unit at a multi-unit site. It is just that the question has seldom been asked. Existing seismic PSAs for multi-unit sites have been performed for each unit separately and independently without considering the possibility of an accident on multiple units from the same seismic event. When each separate PSA is performed, it is implicitly assumed that there is no damage to the other units because if there were such damage, the operator actions modelled in the PSAs for the implementation of procedures and severe accident management guidelines could not be justified without significant modification. Moreover, if the seismic event damages shared systems (not included in the current example), the likelihood of multi-unit accidents from a seismic event is further increased. Indeed, if there are accidents on more than one unit challenging the existing emergency operating procedures and accident management provisions, or if the site was contaminated due to an accident on one of the units, the protection of the remaining units would be challenged, as evidenced by the lessons from the Fukushima Daiichi accident. Such multi-unit interactions have not been adequately considered in earlier PSAs.

There are many reasons why these conclusions are important. First, the consequences of releases from two or more reactor units can be more than the linear sum of the release consequences from the individual reactor releases. This is due to the fact that the dose thresholds required for early health effects due to radiation sickness create a non-linear relationship between the magnitude of the source term and the number of cases of radiation sickness. If the combined dose is less than the required dose thresholds, few if any cases of radiation sickness would be expected. However, if the combined doses exceed the required dose thresholds, the number of cases can be many times larger than that predicted by the linear sum. Second, the treatment of operator actions to mitigate a seismic event are much more difficult to implement if more than one reactor unit is compromised in the event or if there is site contamination inhibiting the accident management measures. Finally, the risk metrics used to frame the PSA, such as core damage frequency and large early release frequency, are not appropriate and do not capture the risk of multi-unit events.

REFERENCES TO ANNEX I

[I–1] PICKARD-LOWE AND GARRICK, Seabrook Station Probabilistic Safety Assessment, PLG-0300, Irvine, CA (1983) Section 13.3.

[I–2] KENNEDY, R.P., CORNELL, C.A., CAMPBELL, R.D., KAPLAN, S., PERLA, H.F., Probabilistic seismic safety study of an existing nuclear power plant, Nucl. Eng. Des. **59** (1980) 315–338.

[I–3] FLEMING, K.N., MIKSCHL, T.J., "Technical issues in the treatment of dependence in seismic risk analysis", OECD/NEA Workshop on Seismic Risk (Proc. Tokyo, 1999), NEA/CSNI/R(99)28, OECD, Paris (2001) 253–268.

[I–4] EBISAWA, K., "Concept and method for estimating correlation of hazard and SSCs at multi-unit site against multi-hazards and application results" (presentation at IAEA Int. Workshop on Safety of Multi-unit Nuclear Power Plant Sites against External Hazards, Mumbai, 2012).

[I–5] NextERA ENERGY, Seabrook Station Individual Plant Examination for External Events, NextERA Energy, Juno Beach, FL (1992).

[I–6] RAVINDRA, M.K., TIONG, L.W., "Comparison of methods for seismic risk quantification", Probabilistic Safety Assessment, Vol. P (Trans 10th Int. Conf. on Structural Mechanics in Reactor Technology), American Association for Structural Mechanics, Los Angeles, CA (1989) 187–192.

[I–7] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, AMERICAN NUCLEAR SOCIETY, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sb-2013, ASME, New York (2013).

Annex II

DERIVATION OF THE SEISMIC COMMON CAUSE PARAMETER FOR A MULTI-UNIT SEISMICALLY INDUCED LOSS OF COOLANT ACCIDENT

In a multi-unit site, the potential exists for multiple large loss of coolant accidents (LOCAs) to occur simultaneously. The probability of this event could be large if the units are identical. This question of correlation between component failures has been identified as an important uncertainty in seismic probabilistic safety assessments. In this annex, the procedure in Ref. [II–1] will be used to calculate the joint probability of two LOCAs occurring simultaneously, drawing from the seismic fragility analysis.

The seismic fragility of a component in a nuclear power plant is the conditional probability of failure at a given peak ground acceleration (PGA). The ground acceleration capacity of the component is modelled as a log-normal probability distribution with median ground acceleration capacity A_m and logarithmic standard deviations β_R and β_U representing the randomness in capacity and the uncertainty in the median capacity, respectively (see Ref. [II–2] for details on seismic fragility methodology). The median ground acceleration capacity is estimated as the product of a number of median safety factors multiplied by the PGA of the safe shutdown earthquake. The safety factors reflect the conservatisms or non-conservatisms in the seismic design and qualification procedures. The randomness and uncertainties in these procedures are also estimated using the logarithmic standard deviations of the safety factors.

The seismic fragilities of components could be probabilistically dependent on each other because of the common ground motion input, common location within the building, same configuration and anchorage, and similar failure modes. Thus, if one component fails at a particular acceleration, the conditional probability of failure of the second component will be higher if more of these fragilities are common to the two components. The Nuclear Regulatory Commission [II–3] reports:

> "Reed *et al*. (1985) [II–1] describe a procedure to estimate dependency between component failures by searching for common sources of variability in the response and strength calculations. The dependency in the structural parameters can be quantified by examining the process in which the individual factors of safety in a fragility assessment are developed. For example, two components in a building are dependent on each other and on the building through the building response factors (*i.e.*, SSI [soil–structure interaction], spectral shape, frequency, damping and mode shape). Thus,

the corresponding epistemic uncertainty and randomness β values for each of these factors will be the same for both components if they are perfectly dependent. One exception may be the β values for the building modeling factors (*i.e.*, frequency, damping, and mode shape) which could be different if the components are located in different parts of the building where support motion comes from different dynamic building modes. The procedure for developing the system fragilities consists of two stages. In the first stage, the median capacities of all components in the systems are sampled using a Latin Hypercube sampling technique.... The correlation between the median capacities is considered by performing the sampling in two steps. In the first step, the logarithmic standard deviation for uncertainty β'_U is used in place of β_U where β'_U is obtained using the following expression:

$$\beta'_U = \left(\beta_U^2 - \sum \beta_U^{*2}\right)^{\frac{1}{2}} \tag{2-17}$$

"In this equation, the β_U^* is a common logarithmic standard deviation which exists between the component under consideration and other components. Several β_U^* values are generally required to represent different groups of correlation. For example, if components 1, 2 and 3 have a common building response β_U^* value (*i.e.*, because they are in the same building) and components 1 and 4 have a common β_U^* value because of capacity (*e.g.*, they both are the same type pumps); then, by using the above equation, the calculation of β'_U for component 1 will require that two values of β_U^{*2} be subtracted from β_U^2.

"After the sets of median capacity values are obtained using the reduced β'_U values for the various components, modifications are made in the second step to account for the effects of dependency. For each of the common β_U^* values, *N* correction factors are obtained using the Latin Hypercube Sampling procedure (*i.e.*, equal probability slice and weighted random sampling within each slice) where the sampled distribution is lognormal with the median value of 1.0 and logarithmic standard deviation of β_U^*. Then the components in each set which have the common dependency are scaled sequentially by the same corresponding correction factors. For example, if there are 10 sets and the components 1, 2 and 3 have a common dependency, then the first correction factor scales the median values for components 1, 2, and 3 in Set 1, the second factor scales the same component values in Set 2, etc.

"This procedure is repeated for each of the common groups of dependencies. After the scaling operation is completed, the *N* sets of median values reflect the inherent dependencies which exist in the median values.

.....

"For each component the median capacity is independently sampled using the β'_U value; this median capacity is modified by multiplying by correction factors which are also sampled from probability distributions with unit median and β^*_U.

"This procedure aims at the treatment of partial dependency between component fragilities. The analyst should look for similarities and differences between the components that will result in partial dependence. Findings from the review of component design and qualification documents and plant walkdowns will be useful for this purpose. The analyst should carefully examine if the installation of components is indeed identical. Even if the components are nominally identical, there will be inherent variation due to fabrication, material properties, etc. Judgment is needed to identify which variables are common to the group of components and which are independent. It is expected that the term $\sum \beta^{*2}_U$ is less than β^2_U. If the analyst judges that the components in the group are identical, assigning the $\sum \beta^{*2}_U$ as equal to β^2_U may be appropriate. In this case, the median capacity of each component is modified by multiplying by the correction factors which are sampled from probability distributions with unit median and β^*_U. In this extreme case, the full dependency between the components in the uncertainty sense is assumed.

"In the second stage, for each set of dependent median capacity values, a single system fragility curve is calculated which reflects the dependency in the capacity values conditional on known dependent median values. The capacities of components could be dependent because they may have some common variables. The fragility of a sequence is obtained by first calculating the fragility conditional on the given value of the common dependent variable and then integrating this fragility over the probability distribution of the common variable. In the following an example of the use of this procedure is given:

"Consider the probability of failure for components 1 and 2.

$$P_{f1} = P(c_1 < a_g) \qquad (7\text{-}2)$$

$$P_{f2} = P(c_2 < a_g) \tag{7-3}$$

"where c_i are the component capacities and a_g is the peak ground acceleration due to an earthquake. However, c_1 and c_2 can be expressed as $c_1 x$ and $c_2 x$ where c_1 and c_2 are the independent parts of capacity and x is the common dependent part. Now the failure probabilities can be expressed as follows:

$$P_{f1} = P(c_1 < a_g/x) \tag{7-4}$$

$$P_{f2} = P(c_2 < a_g/x) \tag{7-5}$$

"The failure of both components, $P_f(1 \cap 2)$, is given by the following equation:

$$P_f(1 \cap 2) = \int P(c_1 < a_g/x) P(c_2 < a_g/x) p(x) dx \tag{7-6}$$

"In terms of the lognormal model for capacity, the parameters for components 1 and 2 are LN(A_{m1}/x, β_{R1}) and LN(A_{m2}/x, β_{R2}), respectively. The distribution for x is LN(1, β_R^*). The values of A_{m1} and A_{m2} are the median capacities from the i^{th} set of median values selected in Stage 1) and β_R^* is the portion of the randomness logarithmic standard deviation common to both components. β_{R1} and β_{R2} are obtained from the following equation:

$$\beta'_{Ri} = \left(\beta_{Ri}^2 - \sum \beta_R^{*2}\right)^{\frac{1}{2}} \tag{7-7}$$

"It is expected that the term $\sum \beta_R^{*2}$ is less than β_{Ri}^2. As stated in the discussion of β_U, the analyst should look for similarities and differences between the components in terms of their randomness. The components may be nominally identical, but slight variations in the mounting may lead to differences in their dynamic responses. Further, the components in the group may experience different input motions due to the stochastic nature of earthquake time histories. If the analyst concludes that the components are totally identical and respond identically to the seismic input, β_{R1} should be treated as equal to zero. When both β_{R1} and β_U are equal to zero, the extreme case of full dependence between components in the group (in the randomness and epistemic uncertainty sense) will result.

"Extrapolation to the general case of multiple dependencies is straightforward from this two component case. For each group of

dependencies there is one level of integration. The reduced logarithmic standard deviation for each component is obtained by removing the common group β^*s using the above Equation (7-7). The corresponding median values are just the component median values divided by the product of the dummy variables x_1, x_2, ..., x_N which represent the common dependencies. Only the terms x_i corresponding to the groups for which a component has dependencies are included in the expression for that component."

The above method is now applied to the calculation of large LOCAs occurring simultaneously in two reactors on the site. It is assumed that the reactors are identical and located in close proximity. The two steam generator (SG) supports (denoted as components A and B) have response dependencies, since they are similarly mounted in the reactor buildings. They also have high capacity dependence, since they are identical and have been designed and installed in the same fashion. The common portion of the uncertainty comes from the common material, same failure mode and capacity calculation procedures.

The fragility parameters for SG support failure leading to large LOCA are median A_m = 2.02g, β_R = 0.32 and β_U = 0.50. The β values are further broken down into contributions from different variables, some of which are common to the support capacity of the two SGs. According to the fragility model in Ref. [II–2], the estimates are given in Table II–1.

TABLE II–1. β ESTIMATES OF THE DIFFERENT VARIABLES

Variable	Estimate
Uncertainty in material strength, $\beta_{U,mat}$	0.11
Uncertainty in failure mode, $\beta_{U,FM}$	0.15
Randomness due to mode combinations, $\beta_{R,MC}$	0.17
Randomness due to earthquake component combination, $\beta_{R,ECC}$	0.15
Uncertainty in damping, $\beta_{R,\delta}$	0.15
Uncertainty due to modelling assumption, $\beta_{R,model}$	0.3
Randomness in structural response, $\beta_{R,SR}$	0.2
Uncertainty in structural response, $\beta_{U,SR}$	0.25

The common randomness and uncertainty in the SG failure capacity are calculated as shown:

$$\beta_{\mathrm{R}}^{*}=\left(\left(\frac{\beta_{\mathrm{R,SR}}}{2}\right)^{2}+\left(\frac{\beta_{\mathrm{R,ECC}}}{3}\right)^{2}+\beta_{\mathrm{R,MC}}^{2}\right)^{\frac{1}{2}}=0.20$$

$$\beta_{\mathrm{U}}^{*}=\left(\beta_{\mathrm{U,mat}}^{2}+\beta_{\mathrm{U,FM}}^{2}+\beta_{\mathrm{U,SR}}^{2}+\beta_{\mathrm{R},\delta}^{2}+\beta_{\mathrm{R,model}}^{2}\right)^{\frac{1}{2}}=0.46$$

From eq. (2-17) of Ref. [II–3], β'_{U} = 0.30. Using the Latin hypercube sampling procedure, ten samples are obtained for A and B, respectively, from LN(4.45g, 0.30) and are randomly ordered to generate pairs of median values.Using the dependent portion LN(1.0, 0.30), another ten samples are generated and randomly ordered. The combined (correlated) median values are obtained by multiplying the independent and dependent samples (see Table II–2).

In Stage 2, the fragility curves are calculated. For each set of dependent median capacity values, a single system fragility curve is calculated which reflects the dependency in the capacity values conditional on known dependent median values. The reduced randomness logarithmic standard deviation is obtained using β_{R}^{*} = 0.20 as follows:

$$\beta'_{\mathrm{R}i}=\left(\beta_{\mathrm{R}i}^{2}-\sum\beta_{\mathrm{R}}^{*2}\right)^{\frac{1}{2}}=\left(0.32^{2}-0.20^{2}\right)^{\frac{1}{2}}=0.25$$

TABLE II–2. SAMPLE OF MEDIAN CAPACITY VALUES

Sample	Independent step		Dependent step	Combined median	
	A	B		A (g)	B (g)
1	2.48	1.77	1.80	4.46	3.18
2	2.32	1.59	0.77	1.78	1.23
3	1.96	1.13	0.98	1.93	1.12
4	1.47	2.15	1.33	1.96	2.87
5	2.09	2.91	0.89	1.86	2.59
6	2.65	2.49	1.03	2.74	2.58
7	1.64	1.41	1.40	2.30	1.98
8	3.50	3.73	0.47	1.65	1.75
9	1.26	1.98	0.66	0.83	1.30
10	1.81	2.26	1.12	2.04	2.54

For sample Set 1, the median values of A and B are c'_A = 4.46g and c'_B = 3.18g. Substituting these values into eq. (7-8) of Ref. [II–3] yields:

$$P_f(A \cap B) = \int P\left(c'_A < a_g/x\right) P\left(c'_B < a_g/x\right) p(x)\,dx$$

where

$$P\left(c'_A < a_g/x\right) \text{ is } \Phi\left(\frac{\ln\left(\frac{4.46}{a_g/x}\right)}{0.25}\right);\ P\left(c'_B < a_g/x\right) \text{ is } \Phi\left(\frac{\ln\left(\frac{3.18}{a_g/x}\right)}{0.25}\right);$$

and x is ln(1.0, 0.20). With these as input, the integral is calculated for a specific a_g value. By varying the a_g value, a fragility curve for the system is obtained. The process is repeated for other sample sets of median values in Table II–2 to obtain the family of fragility curves. The mean fragility curve for the joint occurrence of two LOCAs is obtained by averaging these curves. The conditional probability of LOCA in B, given that LOCA in A has occurred (called the split fraction α) is obtained as the ratio of the joint probability to the probability of LOCA in A and is shown as a function of the PGA. Figure II–1 displays the split fraction as a function of PGA (see Table II–3 for the values). The split fraction is lower at lower accelerations, which permits realistic evaluation of joint failure probability. At higher acceleration, the split fraction does not have a significant effect on multiple LOCA event frequencies. The split fraction is also a function of the seismic capacity (fragility) of the SG support failure mode.

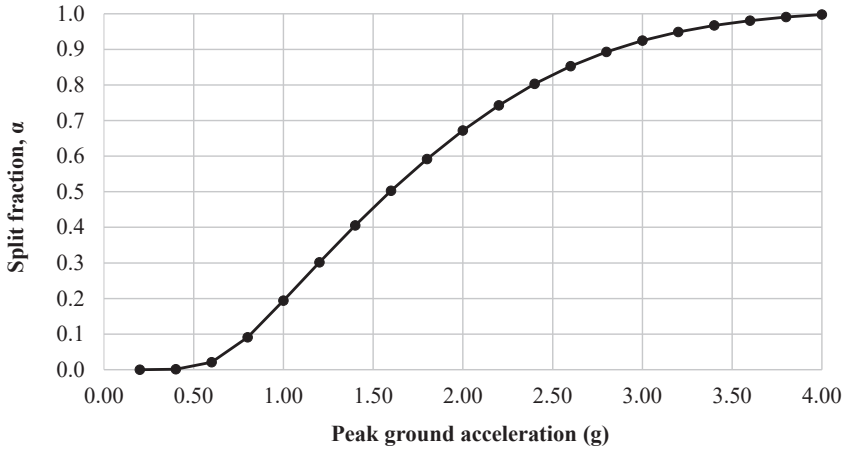


FIG. II–1. Split fraction versus peak ground acceleration.

TABLE II–3. SPLIT FRACTION α AS A FUNCTION OF PEAK GROUND ACCELERATION

Peak ground acceleration (g)	Mean joint probability	Single loss of coolant accident probability	Split fraction α
0.20	3.43×10^{-12}	4.95 × 10–5	6.9×10^{-8}
0.40	3.06×10^{-6}	3.20×10^{-3}	9.6×10^{-4}
0.60	4.32×10^{-4}	2.05×10^{-2}	2.1×10^{-2}
0.80	5.42×10^{-3}	5.95×10^{-2}	9.1×10^{-2}
1.00	2.29×10^{-2}	1.18×10^{-1}	1.9×10^{-1}
1.20	5.74×10^{-2}	1.90×10^{-1}	3.0×10^{-1}
1.40	1.09×10^{-1}	2.69×10^{-1}	4.1×10^{-1}
1.60	1.74×10^{-1}	3.47×10^{-1}	5.0×10^{-1}
1.80	2.50×10^{-1}	4.23×10^{-1}	5.9×10^{-1}
2.00	3.31×10^{-1}	4.93×10^{-1}	6.7×10^{-1}
2.20	4.13×10^{-1}	5.57×10^{-1}	7.4×10^{-1}
2.40	4.93×10^{-1}	6.14×10^{-1}	8.0×10^{-1}
2.60	5.67×10^{-1}	6.65×10^{-1}	8.5×10^{-1}
2.80	6.33×10^{-1}	7.09×10^{-1}	8.9×10^{-1}
3.00	6.91×10^{-1}	7.47×10^{-1}	9.2×10^{-1}
3.20	7.41×10^{-1}	7.81×10^{-1}	9.2×10^{-1}
3.40	7.83×10^{-1}	8.10×10^{-1}	9.5×10^{-1}
3.60	8.19×10^{-1}	8.35×10^{-1}	9.7×10^{-1}
3.80	8.48×10^{-1}	8.56×10^{-1}	9.8×10^{-1}
4.00	8.73×10^{-1}	8.75×10^{-1}	9.9×10^{-1}

REFERENCES TO ANNEX II

[II–1] REED, J.W., McCANN, M.W., Jr., IIHARA, J., TAMJED, H.H., "Analytical techniques for performing probabilistic seismic risk assessment of nuclear power plants", Proceedings of the Fourth International Conference on Structural Safety and Reliability, Vol. III, New York (1985) 253–261.

[II–2] KENNEDY, R.P., RAVINDRA, M.K., Seismic fragilities for nuclear power plant risk studies, Nucl. Eng. Des. **79** (1984) 47–68.

[II–3] NUCLEAR REGULATORY COMMISSION, Correlation of Seismic Performance in Similar SSCs (Structures, Systems, and Components), NUREG/CR-7237, Office of Nuclear Regulatory Research, Washington, DC (2017).

ABBREVIATIONS

ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
CANDU reactor	Canada deuterium–uranium reactor
CCDF	complementary cumulative distribution function
CCF	common cause failure
CCIE	common cause initiating event
CDF	core damage frequency
CPMA	conditional probability of a multi-unit accident
EDG	emergency diesel generator
FDC	fuel damage category
IMU	internal multi-unit
INPO	Institute of Nuclear Power Operations
IPEEE	individual plant examination of external events
ISU	internal single unit
LERF	large early release frequency
LOCA	loss of coolant accident
LOOP	loss of off-site power
LPSD	low power and shutdown
LRF	large release frequency
LWR	light water reactor
MGL	multiple Greek letter
MHTGR	modular high temperature gas cooled reactor
MUCDF	multi-unit core damage frequency
MUPSA	multi-unit probabilistic safety assessment
NRC	Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
OECD/NEA	OECD Nuclear Energy Agency
OPG	Ontario Power Generation
PDS	plant damage state
PGA	peak ground acceleration
PRA	probabilistic risk assessment
PSA	probabilistic safety assessment
PWR	pressurized water reactor
QHO	quantitative health objective
RCF	release category frequency
RCP	reactor coolant pump
SCCDF	site complementary cumulative distribution function
SCDF	site core damage frequency
SG	steam generator

SLERF	site large early release frequency
SRCF	site release category frequency
SSCs	structures, systems and components
SUCDF	single unit core damage frequency
TEPCO	Tokyo Electric Power Company

CONTRIBUTORS TO DRAFTING AND REVIEW

Abe, H.	Nuclear Regulation Authority, Japan
Agrawal, M.K.	Bhabha Atomic Research Centre, India
Ahmad, M.	Pakistan Atomic Energy Commission, Pakistan
Banaseanu, G.	Canadian Nuclear Safety Commission, Canada
Basu, P.C.	Consultant, India
Blahoianu, A.	Canadian Nuclear Safety Commission, Canada
Chokshi, N.C.	Consultant, United States of America
Coman, O.	International Atomic Energy Agency
Devlin, S.	Nuclear Regulatory Commission, United States of America
Ebisawa, K.	Central Research Institute of the Electric Power Industry, Japan
Fleming, K.N.	KNF Consulting Services LLC, United States of America
Freijo, J.L.	National Atomic Energy Commission, Argentina
Georgescu, G.	Institute for Radiological Protection and Nuclear Safety, France
Guohan, C.	National Nuclear Safety Administration, China
Hibino, K.	International Atomic Energy Agency
Jimenez, A.	Nuclear Safety Council, Spain
Katona, T.	Paks nuclear power plant, Hungary
Lusse, L.	South African Nuclear Energy Corporation, South Africa
Lyubarskiy, A.	International Atomic Energy Agency
Madona, A.	ITER-Consult, Italy
Modarres, M.	University of Maryland, United States of America
Morita, S.	International Atomic Energy Agency

Munson, C.	Nuclear Regulatory Commission, United States of America
Nefedov, S.S.	Rosenergoatom, Russian Federation
Nomura, S.	Nuclear Regulation Authority, Japan
Pino, G.S.	ITER-Consult, Italy
Pisharady, A.S.	Atomic Energy Regulatory Board, India
Ravikiran, A.	Bhabha Atomic Research Centre, India
Ravindra, M.K.	MKRavindra Consulting, United States of America
Rebour, V.	Institute for Radiological Protection and Nuclear Safety, France
Roshan, A.D.	Atomic Energy Regulatory Board, India
Roy, S.M.	Atomic Energy Regulatory Board, India
Samaddar, S.K.	International Atomic Energy Agency
Sanchez-Cabanero, J.G.	Nuclear Safety Council, Spain
Sorel, V.	Électricité de France, France
Takada, T.	University of Tokyo, Japan
Ulla, V.	Radiation and Nuclear Safety Authority, Finland
Välikangas, P.	Radiation and Nuclear Safety Authority, Finland
Vickery, P.J.	Applied Research Associates, United States of America
Watanabe, K.	International Atomic Energy Agency
Yamanaka, Y.	Tokyo Electric Power Company, Japan

Consultants Meetings

Madrid, Spain: 27–29 September 2011
Rockville, MD, United States of America: 24–26 September 2012,
11–14 June 2013, 10–11 June 2015
Vienna, Austria: 28–31 August 2012, 5–8 March 2013
Mumbai, India: 15–16 October 2012
Monaco: 21–24 October 2013
Paris, France: 24–26 June 2014

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

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 613 745 7660
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

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/books

DEVELOPMENT AND APPLICATION OF LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. SSG-3
STI/PUB/1430 (195 pp.; 2010)
ISBN 978–92–0–114509–4 Price: €35.00

DEVELOPMENT AND APPLICATION OF LEVEL 2 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. SSG-4
STI/PUB/1443 (88 pp.; 2010)
ISBN 978–92–0–102210–3 Price: €22.00

SAFETY ASSESSMENT FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GSR Part 4 (Rev. 1)
STI/PUB/1714 (38 pp.; 2016)
ISBN 978–92–0–109115–4 Price: €49.00

This publication extracts insights and lessons learned from existing literature on multi-unit safety assessments to provide guidance on the approach and methods for site evaluation and safety assessment for nuclear power plants when establishing a multi-unit probabilistic safety assessment (PSA) on hazards and multiple external events. Using a PSA based approach, it identifies the technical issues to be addressed in an integrated site PSA and proposes solutions for safety assessment practitioners familiar with single unit PSAs against a full range of internal and external hazards.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–102618–7
ISSN 1020–6450