U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-1413

Proposed new Regulatory Guide 1.254, Revision 0

Issue Date: October 2024
Technical Lead: Mihaela Biro

TECHNOLOGY-INCLUSIVE IDENTIFICATION OF LICENSING EVENTS FOR COMMERCIAL NUCLEAR PLANTS

A. INTRODUCTION

Purpose

This regulatory guide (RG) provides the U.S. Nuclear Regulatory Commission (NRC) staff's technology-inclusive guidance for identifying initiating events, delineating event sequences, and identifying licensing events that can be used to inform the design and licensing bases and the content of applications for commercial nuclear plants.

Applicability

This RG applies to nuclear power reactor designers, applicants, and licensees of commercial nuclear plants applying for permits, licenses, certifications, and approvals under Title 10 of the *Code of Federal Regulations* (CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 1); 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 2); and 10 CFR Part 53, "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants" (Ref. 3).

Applicable Regulations

The following regulations are applicable to the identification of licensing events:

- 10 CFR Part 50
  - 10 CFR 50.34(a)(1)(i) requires all power reactor applicants for a construction permit (CP) to provide a description and safety assessment of the site on which the facility is to be located, with appropriate attention to features affecting facility design. Special attention should be directed to the site evaluation factors identified in 10 CFR Part 100, "Reactor Site Criteria" (Ref. 6). The assessment must contain an analysis and evaluation of the major structures,

---

This RG is being issued in draft form to involve the public in the development of regulatory guidance in this area. It has not received final staff review or approval and does not represent an NRC final staff position. Public comments are being solicited on this RG and its associated regulatory analysis. Comments should be accompanied by appropriate supporting data. Comments may be submitted through the Federal-rulemaking website, http://www.regulations.gov, by searching for draft regulatory guide DG-1413. Alternatively, comments may be submitted to Office of the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Rulemakings and Adjudications Staff. Comments must be submitted by the date indicated in the *Federal Register* notice.

Electronic copies of this RG, previous versions of RGs, and other recently issued guides are available through the NRC's public website under the Regulatory Guides document collection of the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html. The RG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML22257A173. The regulatory analysis is associated with a rulemaking and may be found in ADAMS under Accession No. ML24095A166.

systems, and components (SSCs) of the facility which bear significantly on the acceptability of the site under the site evaluation factors identified in 10 CFR Part 100, assuming that the facility will be operated at the ultimate power level which is contemplated by the applicant.

- 10 CFR 50.34(a)(1)(ii) requires stationary power reactor applicants for a CP to provide a description and safety assessment of the site and a safety assessment of the facility. It is expected that reactors will reflect, through their design, construction, and operation, an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products.

- 10 CFR 50.34(a)(4) requires all power reactor applicants for a CP to provide a preliminary analysis and evaluation of the design and performance of SSCs of the facility with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of SSCs provided for the prevention of accidents and the mitigation of the consequences of accidents.

- 10 CFR 50.34(b) requires each application for an operating license (OL) to include a final safety analysis report that describes the facility, presents the design bases and the limits on its operation, and presents a safety analysis of the SSCs and of the facility as a whole.

- 10 CFR 50.34(b)(2) requires each application for an OL to provide a description and analysis of the SSCs of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which such requirements have been established, and the evaluations required to show that safety functions will be accomplished. The description should be sufficient to permit understanding of the system designs and their relationship to safety evaluations.

- 10 CFR 50.34(h) requires applications for light-water reactor (LWR) CPs and OLs to include an evaluation of the facility against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application. This evaluation must include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation must discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of the Commission, or portions thereof, that underlie the corresponding SRP acceptance criteria. The SRP is not a substitute for the regulations, and compliance is not a requirement.[1]

[1] SECY-22-0052, "Proposed Rule: Alignment of Licensing Processes and Lessons Learned from New Reactor Licensing (RIN 3150-AI66)," dated June 6, 2022 (Ref. 4), describes NRC proposed changes to the regulations in 10 CFR Part 50 and 10 CFR Part 52 to align reactor licensing processes and incorporate lessons learned from new reactor licensing into the regulations. The NRC is proposing to remove and reserve the requirements in 10 CFR 50.34(h) that call for an applicant to include an evaluation of conformance with NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP) (Ref. 5).

- 10 CFR Part 52[2]

  - 10 CFR 52.47(a)(2) requires applications for standard design certifications (DCs) to provide a description and analysis of the SSCs of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. It is expected that the standard plant will reflect through its design, construction, and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products.

  - 10 CFR 52.47(a)(9) requires applications for LWR DCs to include an evaluation of the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section must include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where a difference exists, the evaluation must discuss how the proposed alternative provides an acceptable method of complying with the Commission's regulations, or portions thereof, that underlie the corresponding SRP acceptance criteria. The SRP is not a substitute for the regulations, and compliance is not a requirement.

  - 10 CFR 52.79(a) requires applications for combined licenses (COLs) to provide a final safety analysis report that describes the facility, presents the design bases and the limits on its operation, and presents a safety analysis of the SSCs of the facility as a whole.

  - 10 CFR 52.79(a)(1)(vi) requires applications for COLs to provide a description and safety assessment of the site on which the facility is to be located. The assessment must contain an analysis and evaluation of the major SSCs of the facility that bear significantly on the acceptability of the site under the radiological consequence evaluation factors identified in § 52.79(a)(1)(vi)(A) and § 52.79(a)(1)(vi)(B).

  - 10 CFR 52.79(a)(2) requires applications for COLs to provide a description and analysis of the SSCs of the facility, with emphasis upon performance requirements; the bases, with technical justification, upon which these requirements have been established; and the evaluations required to show that safety functions will be accomplished. It is expected that reactors will reflect, through their design, construction, and operation, an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products.

  - 10 CFR 52.79(a)(41) requires applications for LWR COLs to include an evaluation of the facility against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section must include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where a difference exists, the evaluation must discuss how the proposed

[2] SECY-22-0052 describes NRC proposed changes to the regulations in 10 CFR Part 50 and 10 CFR Part 52 to align reactor licensing processes and incorporate lessons learned from new reactor licensing into the regulations. The NRC is proposing to remove and reserve the requirements in 10 CFR 52.47(a)(9), 10 CFR 52.79(a)(41), 10 CFR 52.137(a)(9), and 10 CFR 52.157(f)(30) that require an applicant to include an evaluation of conformance with the SRP.

alternative provides an acceptable method of complying with the Commission's regulations, or portions thereof, that underlie the corresponding SRP acceptance criteria. The SRP is not a substitute for the regulations, and compliance is not a requirement.

- 10 CFR 52.137(a)(2) requires applications for standard design approvals (SDAs) to provide a description and analysis of the SSCs of the facility, with emphasis upon performance requirements, the bases, with technical justification, upon which the requirements have been established, and the evaluations required to show that safety functions will be accomplished. It is expected that the standard plant will reflect through its design, construction, and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products.

- 10 CFR 52.137(a)(4) requires applications for SDAs to provide an analysis and evaluation of the design and performance of SSCs with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of SSCs provided for the prevention of accidents and the mitigation of the consequences of accidents.

- 10 CFR 52.137(a)(9) requires applications for LWR SDAs to include an evaluation of the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section must include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where a difference exists, the evaluation must discuss how the proposed alternative provides an acceptable method of complying with the Commission's regulations, or portions thereof, that underlie the corresponding SRP acceptance criteria. The SRP is not a substitute for the regulations, and compliance is not a requirement.

- 10 CFR 52.157(c) requires applications for manufacturing licenses (MLs) to provide a description and analysis of the SSCs of the reactor to be manufactured, with emphasis upon the materials of manufacture, performance requirements, the bases, with technical justification therefor, upon which the performance requirements have been established, and the evaluations required to show that safety functions will be accomplished.

- 10 CFR 52.157(f)(1) requires applications for MLs to provide an analysis and evaluation of the design and performance of SSCs with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of SSCs provided for the prevention of accidents and the mitigation of the consequences of accidents.

- 10 CFR 52.157(f)(30) requires applications for LWR MLs to include an evaluation of the design to be manufactured against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section must include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where a difference exists, the evaluation must discuss how the proposed alternative provides an acceptable method of complying with the

Commission's regulations, or portions thereof, that underlie the corresponding SRP acceptance criteria. The SRP is not a substitute for the regulations, and compliance is not a requirement.

- 10 CFR Part 53

  - 10 CFR 53.240, "Licensing-basis events," requires CP, OL, DC, SDA, ML, and COL applicants for commercial nuclear plants to identify and analyze licensing-basis events under § 53.450, "Analysis requirements," to support assessments of the safety requirements in 10 CFR Part 53. The identified licensing-basis events must collectively address combinations of malfunctions of plant SSCs, human errors, facility hazards, and the effects of external hazards ranging from anticipated operational occurrences (AOOs) to very unlikely event sequences. The analysis of licensing-basis events must include analysis of one or more design-basis accidents (DBAs) under § 53.450(f). The analysis of licensing-basis events must confirm the adequacy of design features and programmatic controls needed to satisfy safety criteria defined in §§ 53.210, "Safety criteria for design-basis accidents," and 53.220, "Safety criteria for licensing-basis events other than design-basis accidents," or more restrictive alternative criteria adopted under 53.470, "Maintaining analytical safety margins used to justify operational flexibilities," and must establish related functional requirements for plant SSCs, personnel, and programs.

Related Guidance

- RG 1.200, "Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities" (Ref. 7), provides an acceptable approach for determining whether a base probabilistic risk assessment (PRA), in total or in the portions that are used to support an application, is sufficient to provide confidence in the results such that the PRA can be used in regulatory decision-making for LWRs. When used in support of an application, this RG will obviate the need for an in-depth review of the base PRA by NRC reviewers, allowing them to focus on key assumptions and areas identified by the PRA peer reviewers as being of concern and relevant to the application. Consequently, RG 1.200 provides for a more focused and consistent review process.

- RG 1.206, "Applications for Nuclear Power Plants" (Ref. 8), refers to the technical requirements in the SRP, which provides guidance to the NRC staff in performing safety reviews of LWR CP or OL applications under 10 CFR Part 50 and LWR DC, COL, SDA, and ML applications under 10 CFR Part 52.

- SRP Section 15.0, "Introduction—Transient and Accident Analyses," guides the NRC staff in its review of licensing events, specifically including guidance to help ensure that the applicant's selection and assembly of the plant transient and accident analyses represent a sufficiently broad spectrum of transients, accidents, and initiating events.

- SRP Section 19.0, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors," pertains to the NRC staff review of the design-specific PRA for a DC and plant-specific PRA for a COL application.

- RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors" (Ref. 9), provides guidance on using a technology-inclusive, risk-informed, and performance-based methodology to inform the

licensing basis and content of applications for non-LWRs, including, but not limited to, molten salt reactors, high-temperature gas-cooled reactors, and a variety of fast reactors at different thermal capacities. This RG endorses Nuclear Energy Institute (NEI) 18-04, Revision 1, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," issued August 2019 (Ref. 10), with clarifications and points of emphasis, as one acceptable method for non-LWR designers to use when selecting licensing-basis events, classifying SSCs, and assessing defense-in-depth adequacy.

- RG 1.247 (For Trial Use), "Acceptability of Probabilistic Risk Assessment Results for Non-Light-Water Reactor Risk-Informed Activities" (Ref. 11), describes an approach for determining whether a design-specific or plant-specific PRA used to support an application is sufficient to provide confidence in the results, such that the PRA can be used in regulatory decision-making for non-LWRs. In this RG, the term "application" includes preapplication activities, initial licensing applications, and risk-informed applications. When used in support of an application, this RG will help reduce the need for an in-depth review of the PRA by NRC reviewers, allowing them to focus on key assumptions and areas identified as being of concern and relevant to the application and the demonstration of PRA acceptability.

- Interim Staff Guidance (ISG) DC/COL-ISG-028, "Assessing the Technical Adequacy of the Advanced Light-Water Reactor Probabilistic Risk Assessment for the Design Certification Application and Combined License Application," issued November 2016 (Ref. 12), provides guidance for assessing the technical adequacy of the PRA needed for an application for a DC or for a COL of an advanced LWR under 10 CFR Part 52.

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs are acceptable if supported by a basis for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 50, 52, 53, and 100 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget (OMB), under control numbers 3150-0011, 3150-0151, 3150-XXXX and 3150-0093, respectively. Send comments regarding this information collection to the FOIA, Library, and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the OMB Office of Information and Regulatory Affairs, Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

B. DISCUSSION

Reason for Issuance

The NRC is issuing this RG to provide technology-inclusive guidance for identifying a comprehensive set of licensing events without preconceptions or reliance on predefined lists (i.e., "starting with a blank sheet of paper") and determining an appropriate level of information for parts of an application, including preliminary or final safety analysis reports for commercial nuclear plants. NRC regulations require that applications for a CP, OL, DC, COL, SDA, or ML include a level of information sufficient to enable the Commission to reach a safety conclusion before issuing a permit, license, or certification.

Background

This RG provides a technology-inclusive, systematic, and comprehensive approach to identifying licensing events that may be applied to any commercial nuclear plant licensing pathway. It has been developed by considering historical licensing practices and recommendations from the Advisory Committee on Reactor Safeguards (ACRS) and uses information and insights from risk evaluations that may be performed in support of an application for a commercial nuclear plant permit, license, certification, or approval. The sections below discuss the relation between licensing events and commercial nuclear plant licensing pathways, review historical practices for identifying licensing events, and provide the staff's perspectives.

The Relation Between Licensing Events and Licensing Pathways

For ease of reference, this RG uses the term "licensing events" in a generic sense to refer to collections of designated event categories, such as AOOs, DBAs, design-basis events (DBEs), beyond-design-basis events (BDBEs), and postulated accidents. The term "licensing event" does not appear, per se, in NRC regulations; however, various designated licensing event categories are identified in 10 CFR Part 50, 10 CFR Part 52, and 10 CFR Part 53; regulatory guidance; and the NRC SRP for LWRs.

The identification of a comprehensive set of licensing events is fundamental to the safe design of commercial nuclear plants. Specifically, the safety of a commercial nuclear plant is shown by analyses of the responses of the plant to licensing events, which include postulated disturbances in process variables and postulated malfunctions or failures of equipment. The results of such safety analyses are used to (1) demonstrate compliance with NRC regulations or justify requested exemptions from specific NRC regulations, (2) inform the selection of limiting conditions for operation, limiting safety system settings, and design specifications for SSCs to protect public health and safety, and (3) identify the appropriate scope and depth of information that commercial nuclear plant designers and applicants should provide in applications for permits, licenses, certifications, and approvals. Accordingly, it is essential to identify a comprehensive set of licensing events that considers all radiological sources at the plant, all internal and external hazards, and all plant operating states.

NRC regulations provide a variety of regulatory frameworks for commercial nuclear plant licensing, thus giving designers and applicants considerable flexibility while also ensuring an acceptable level of safety. The choices made by designers and applicants have implications concerning the approach used to identify licensing events, as summarized in Table 1.

Table 1. Licensing Pathways and Licensing Events

Regulation and Application Type	Reactor Type	Use of LMP[a]	Licensing Event Categories	Risk Evaluation
10 CFR Part 50 CP, OL	LWR	n/a	• DBEs[b]—this term is used in the 10 CFR 50.2 definition of safety-related SSCs; 10 CFR 50.49 identifies four subcategories of DBEs as follows: o AOOs o DBAs (i.e., postulated accidents) o external events o natural phenomena • non-DBA—this term is used in the 10 CFR 50.2 definition of safe shutdown for station blackout • BDBEs • anticipated transient without scram (ATWS) • station blackout	not required[c]
10 CFR Part 52 DC, SDA, ML, COL				PRA required
10 CFR Part 50 CP, OL	non-LWR	no		not required[c]
10 CFR Part 52 DC. SDA, ML, COL				PRA required
10 CFR Part 50 CP, OL	non-LWR	yes	Licensing events are collectively referred to as licensing-basis events, which include the following categories: • AOOs • DBEs • BDBEs • DBAs	PRA implied
10 CFR Part 52 DC, SDA, ML, COL				PRA required

Table 1. Licensing Pathways and Licensing Events

Regulation and Application Type	Reactor Type	Use of LMP[a]	Licensing Event Categories	Risk Evaluation
10 CFR Part 53 CP, OL, DC, SDA, ML, COL	LWR or non-LWR	n/a[d]	Licensing events are collectively referred to as licensing-basis events, which include the following categories: • AOOs • unlikely event sequences • very unlikely event sequences • DBAs	PRA required

[a]The Licensing Modernization Project (LMP) guidance, which is provided in NEI 18-04, Revision 1, and endorsed in RG 1.233, provides a voluntary technology-inclusive approach to licensing-basis event selection for non-LWRs licensed under 10 CFR Part 50 or 10 CFR Part 52.
[b]Although 10 CFR Part 50 and 10 CFR Part 52 include normal operation in the design bases, the risk evaluation focuses on departures from normal operation.
[c] SECY-22-0052 describes NRC proposed changes to the regulations in 10 CFR Part 50 and 10 CFR Part 52 to align reactor licensing processes and incorporate lessons learned from new reactor licensing into the regulations. The NRC is proposing to add new regulations, 10 CFR 50.34(a)(14) and 10 CFR 50.34(b)(14), to require CP and OL applicants to submit a description of the plant-specific PRA and its results.
[d]The staff intends to revise RG 1.233 in the future to address licensing under 10 CFR Part 53.

Each row in Table 1 denotes a specific licensing pathway, which is characterized by the first three columns labeled "Regulation and Application Type," "Reactor Type," and "Use of LMP." Collectively, the information in the first three columns identifies (1) the regulation under which the application is submitted and the type of application (CP, OL, DC, SDA, ML, or COL), (2) the reactor technology that is proposed (LWR or non-LWR), and (3) the use of the LMP guidance (NEI 18-04, Revision 1, as endorsed in RG 1.233), which provides a voluntary technology-inclusive approach to licensing-basis event selection for non-LWRs licensed under 10 CFR Part 50 or 10 CFR Part 52. The column labeled "Licensing Event Categories" lists the types of licensing events that apply to each licensing pathway. Finally, the column labeled "Risk Evaluation" shows what type of risk evaluation (PRA or none) may be performed to support the application. The information and insights from risk evaluations; specifically, the initiating event analysis and the event sequence analysis, may be used to inform the identification of licensing events as described in detail in Section C of this RG.

Historical Perspective

In the early days of commercial nuclear power, licensing events were identified on an ad hoc basis, relying on the collective engineering judgment of designers and the regulatory staff. Edward Teller, the first chair of the Atomic Energy Commission (AEC) Reactor Safeguards Committee (1947–1949), described the process as follows (Ref. 13):

> To avoid the very real and very great danger of an accidental release of radioactivity from a reactor, our committee established a simple procedure: We asked the planner of each reactor to imagine the worst possible accident and to design safety apparatus guaranteeing that it could not happen. The committee reviewed each reactor plan, trying to imagine an accident even greater than that conceived by the planner. If we could think

> of a plausible mishap worse than any discussed by the planner, his analysis of the potential dangers was considered inadequate.

The AEC regulatory staff recognized the limitations of this ad hoc approach, as described by Clifford Beck in 1959 (Ref. 14):

> It is inherently impossible to give an objective definition or specification for "credible accidents" and thus the attempt to identify these for a given reactor entails some sense of futility and frustration, and, further, it is never entirely assured that all potential accidents have been examined…. It should be noted parenthetically, however, that this systematic search for credible accidents often contributes substantially to the safety of a facility…. In the plants finally approved for operation, there are no really credible potential accidents against which safeguards have not been provided to such extent that the calculated consequences to the public would be unacceptable.

To help standardize and expedite the review of new plant license applications, the AEC issued guidance in 1966 (Ref. 15) that provided, as examples, a list of accidents to be addressed in safety analysis reports. A plan to develop an SRP for the review of LWR applications was developed in 1969 (Ref. 16) that identified various transients and accidents, including ATWS, to be addressed in safety analysis reports. The original version of the SRP was issued in 1975 as NUREG-75/087, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (Ref. 17)." Sections of the SRP were subsequently revised and individually issued (annotated with revision numbers and publication dates) along with an updated table of contents that indicated the revision numbers of the currently effective sections. The SRP was reissued as NUREG-0800 in July 1981 to more completely identify the NRC requirements that are germane to each review topic, to more fully describe how the review effort determines satisfaction of the requirement, and to incorporate the large number of new and revised regulatory positions (primarily related to the accident at the Three Mile Island Nuclear Generating Station) that had already been established. As a result, some SRP sections were added, deleted, split, or combined. With respect to the identification of licensing events, SRP Chapter 15 introduced the expectation that transients and accidents should be categorized as AOOs or postulated events according to their frequency of occurrence and type.

The staff has not developed an SRP for non-LWRs due to the apparent lack of demand and the wide variation among potential non-LWR designs. Licensing events for previously licensed non-LWRs (e.g., Peach Bottom Unit 1, Ft. St. Vrain) were identified, analyzed, and reviewed on a case-by-case basis.

NRC Advisory Committee on Reactor Safeguards

The ACRS has discussed the importance of performing a comprehensive and systematic search for initiating events[1] and delineating a comprehensive set of event sequences to inform the design and review of new commercial nuclear plants. The following ACRS letter reports have, in part, played an important role in the development of this RG:

- letter report, "Review of Draft SECY Paper, 'Population-Related Siting Considerations for Advanced Reactors,'" dated October 7, 2019 (Ref. 18):

  > One specific caveat not raised in the draft SECY, but implied in all the licensing activities for new non-LWR designs flowing out of the vision and strategy process [Ref. 19], is the need for examining new designs with a clean sheet of paper. Improvements in our ability to calculate source terms and consequences in conjunction with the inherent safety aspects of advanced designs can reduce the probability and consequences of many of the events that have historically dominated the risk at LWRs. Nevertheless, one must be sure to think carefully about the failures and combinations of failures that could occur; i.e., what could go wrong. There are many tools that can help in such a search: a simple reframing—asking 'how could I make this system fail'; employing a search scheme similar to the Hazard and Operability Study (HAZOP) approach used in the chemical processing industry; and applying a modified failure modes and effects analysis at the system level rather than at the component level.
  >
  > There is a tendency to believe in the perfection of new designs, especially when they are developed to eliminate the dominant failure scenarios in existing designs. However, one must remain vigilant and remember that nature provides surprises. There will be new accident scenarios and new combinations of events to be considered that challenge our expectations and our assumptions about these advanced reactor systems. Creative thinking will be required to identify such unique situations, to thoroughly identify the scenarios that will be the basis of the safety analysis and the source of releases, and to evaluate the suitability of sites.

- letter report, "10 CFR Part 53 Licensing and Regulation of Advanced Nuclear Reactors," dated October 21, 2020 (Ref. 20): "The staff should ensure that applicants compensate for novel designs with uncertainties due to incompleteness in the knowledge base by performing systematic searches for hazards, initiating events, and accident scenarios with no preconceptions that could limit the creative process."

- letter report, "Preliminary Proposed Rule Language for 10 CFR Part 53, 'Licensing and Regulation of Advanced Nuclear Reactors,' Interim Report," dated May 30, 2021 (Ref. 21): "The two recommendations in our first letter report on 10 CFR Part 53 of October 21, 2020, still apply: for novel designs with uncertainties due to incompleteness in the knowledge base, systematic searches for hazards, initiating events, and accident scenarios should be required; and a licensing

[1] As defined in the non-LWR PRA standard (Ref. 28), "an initiating event is a perturbation to the plant during a plant operating state that challenges plant control and safety systems whose failure could potentially lead to an undesirable end state and/or radioactive material release. An initiating event is defined in terms of the change in plant status that results in a condition requiring a response to mitigate the event or to limit the extent of plant damage caused by the initiating event. An initiating event may result from human causes, equipment failure from causes internal to the plant (e.g., hardware faults, flood, or fires) or external to the plant (e.g., earthquakes or high winds), or combinations thereof."

pathway including additional testing and monitoring akin to prototype testing should be available."

- letter report, "Regulatory Guide 1.247, 'Acceptability of Probabilistic Risk Assessment Results for Advanced Non-Light-Water Reactor Risk-Informed Activities,'" dated October 26, 2021 (Ref. 22): "Include guidance that the initial search for initiating events and scenarios should be done without preconceptions or using existing lists."

Staff Perspective on Identification of Licensing Events

The identification of licensing events should be conducted objectively and without preconceptions or reliance on predefined lists (such as those provided in the SRP; previous applications for permits, licenses, certifications, and approvals; and previous PRAs). The use of a "blank sheet of paper" approach helps to avoid pitfalls such as, but not limited to, the following—

- the unwitting or unquestioning carryover of assumptions about plant design or behavior
- the tendency to focus on which predefined events apply (or do not apply) rather than which events are missing from the list
- the use of predefined lists that are dated and do not reflect contemporary commercial nuclear plant design or operating experience

In short, the identification of licensing events, conducted objectively and without preconceptions or reliance on predefined lists, helps to ensure that the final list of licensing events is comprehensive and, hence, that the plant design is appropriately analyzed and demonstrated to be safe based on the comprehensive set of licensing events.

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA develops Safety Requirements and Safety Guides for protecting people and the environment from the harmful effects of ionizing radiation. This system of safety fundamentals, safety requirements, safety guides, and other relevant reports, reflects an international perspective on what constitutes a high level of safety. To inform its development of this RG, the NRC considered IAEA Safety Requirements and Safety Guides pursuant to the Commission's International Policy Statement (Ref. 23) and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. 24).

This RG is, with the exception of technology-specific topics, generally consistent with the principles and guidance in the IAEA document series, including the following IAEA documents:

- Specific Safety Requirements (SSR), No. SSR-2/1, "Safety of Nuclear Power Plants: Design," issued 2016 (Ref. 25)
- Specific Safety Guide (SSG), No. SSG-2, "Deterministic Safety Analysis for Nuclear Power Plants," issued 2010 (Ref. 26)

C. STAFF REGULATORY GUIDANCE

General Guidance

1. An acceptable technology-inclusive approach for identifying commercial nuclear plant licensing events should address the following overarching principles:

    a. Identify application-specific factors (licensing framework, plant-specific design features, and site characteristics).

    b. Conduct a systematic and comprehensive search for initiating events.

    c. Use a systematic process to delineate a comprehensive set of event sequences.

    d. Group initiating events and event sequences into designated licensing event categories according to the selected licensing framework.

    e. Provide assurance that the set of licensing events is sufficient.

2. Figure 1 presents an acceptable technology-inclusive process for identifying licensing events that addresses each of these overarching principles. The process includes the following substeps:

    a. setting up the project,
    b. collecting application-specific information,
    c. selecting analysis methods,
    d. performing initiating event analysis,
    e. conducting event sequence analysis, and
    f. selecting licensing events.

3. The guidance in the following sections provides additional details on each of these substeps. Substeps a-e apply to all licensing frameworks. Non-LWR designers and applicants that voluntarily seek implementation of the LMP under 10 CFR Part 50 or 10 CFR Part 52 should use the guidance in RG 1.233 to identify licensing events (substep f).

4. The process described in Figure 1 is expected to be performed in an iterative fashion. The design process and the development of licensing basis information is iterative, involving assessments and decisions on system design, operating parameters, and programmatic controls to ensure that a reactor design can be deployed without posing undue risk to public health and safety. The identification of initiating events and event sequences can be performed as the design evolves through the conceptual phases. As the design matures, the licensee or applicant should consider the licensing framework it is planning to use for regulatory review and approval, as this decision influences the technology-inclusive process for identifying licensing events. Specifically, the licensing framework determines the appropriate licensing event categories, whether development of a PRA will be required, and how the risk insights from the PRA will be used. The choice of licensing framework is a complex decision made by applicants. Accordingly, this RG does not provide any associated guidance.

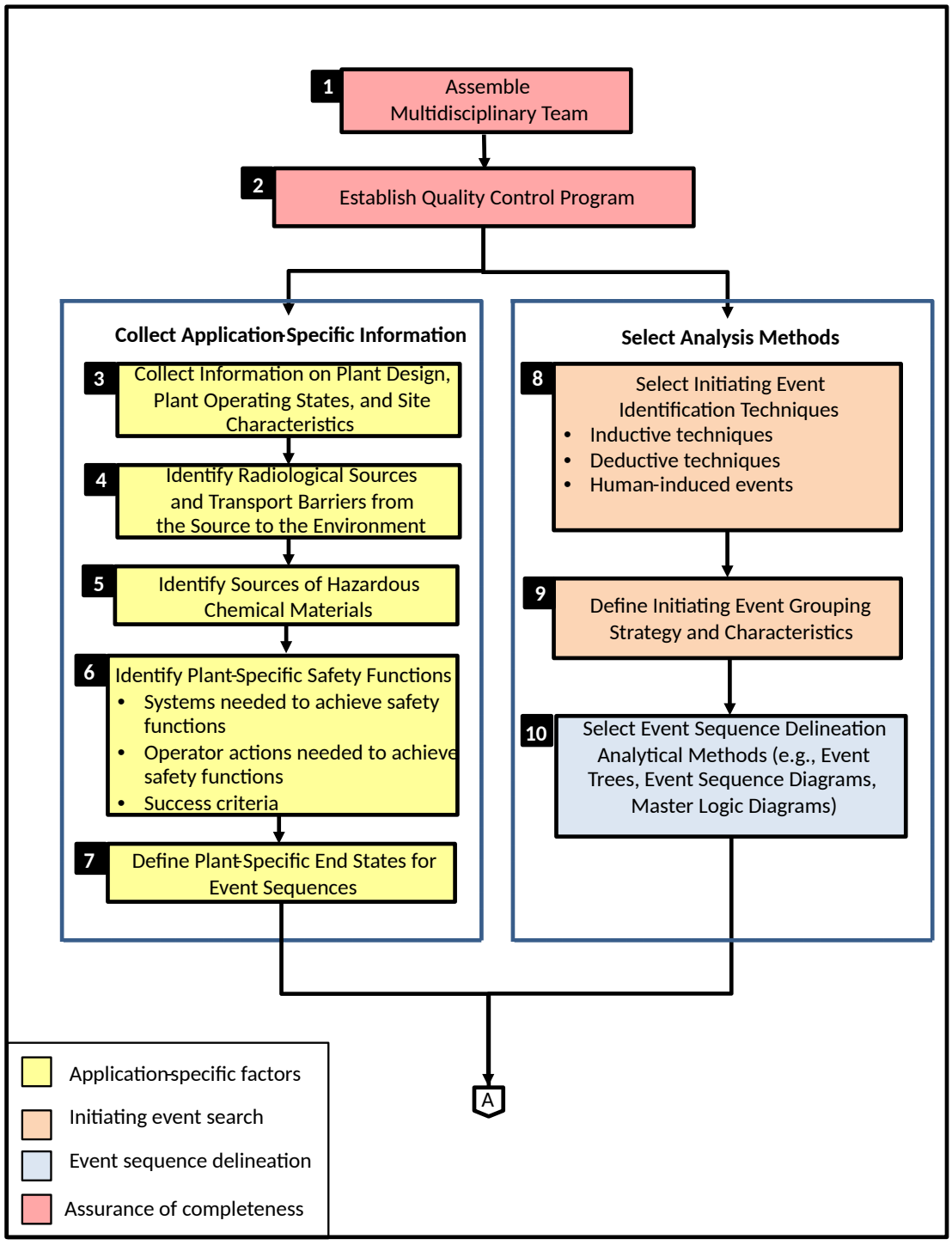


Figure 1 Technology-inclusive identification of licensing events (sheet 1 of 3)

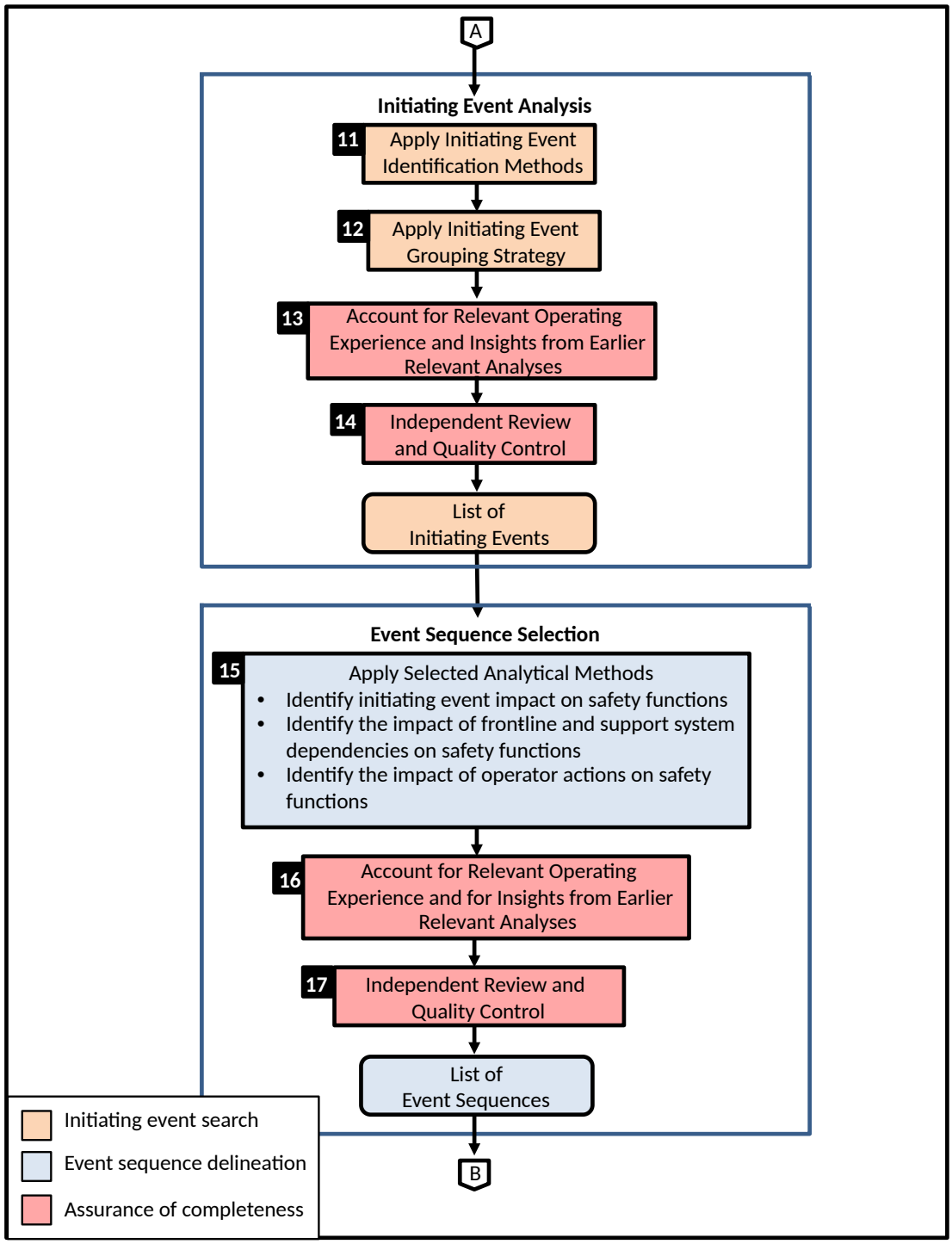


Figure 1 Technology-inclusive identification of licensing events (sheet 2 of 3)

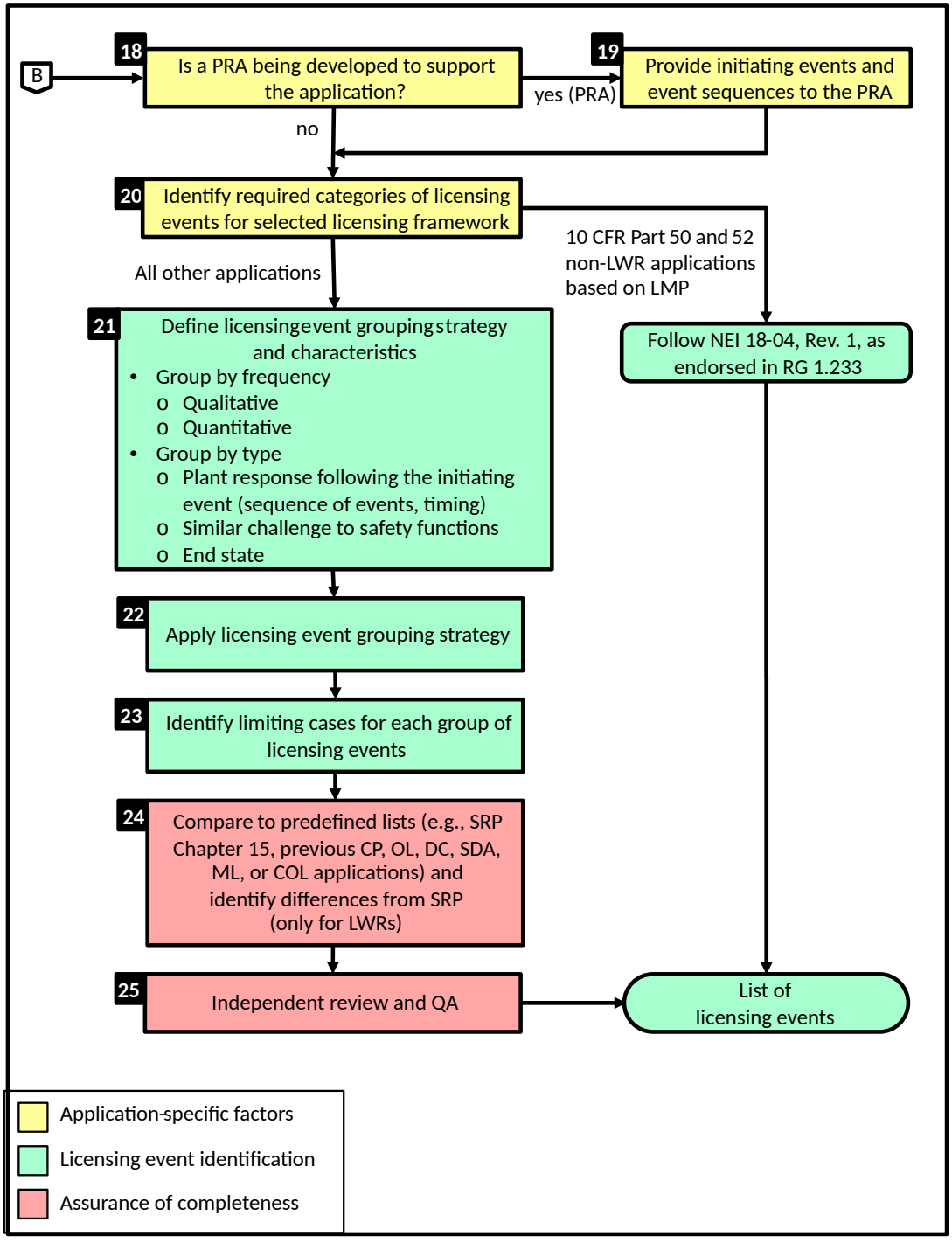


Figure 1 Technology-inclusive identification of licensing events (sheet 3 of 3)

Setting Up the Project

Assemble a Multidisciplinary Team (Box 1, Principle #5)

5. To help ensure that (1) the identification of licensing events is conducted objectively and without preconceptions or reliance on predefined lists and (2) the final list of licensing events is comprehensive, a team should be assembled that provides familiarity with the following disciplines:

    a. licensing,

    b. plant design details:

        (1) reactor,
        (2) spent fuel,
        (3) structures,
        (4) mechanical systems,
        (5) electrical systems,
        (6) instrumentation and control systems, and
        (7) siting,

    c. construction,

    d. plant operations:

        (1) concept of operations, and
        (2) plant operating states,

    e. reactor physics,

    f. thermal-hydraulic analysis,

    g. reliability engineering or PRA methods or both,

    h. expertise in the selected methods of analysis (including hazard identification and assessment), and

    i. expertise in disciplines unique to the chosen technology.

6. A single individual may provide expertise in more than one discipline; however, the team should include at least three people to provide a suitably broad and unbiased perspective.

Establish Process for Quality Control (Box 2, Principle #5)

7. Before engaging in the work, a program for quality control should be established that includes, as a minimum, the following elements:

    a. use of personnel qualified for the analysis;

b. use of procedures that ensure control of documentation, including revisions, and provide for independent review, verification, or checking of calculations and information used in the analyses;

c. documentation and maintenance of records, including archival as well as submittal documentation; and

d. use of procedures that ensure that appropriate attention and corrective actions are taken if assumptions, analyses, or information used previously are changed or determined to be in error.

8. When developing the quality control program, designers or applicants should consider the following items:

a. In accordance with the preamble for the 2007 10 CFR Part 52 rulemaking (72 FR 49365; August 28, 2007), a PRA is not part of the design-basis information. Therefore, the initiating event and event sequence analyses are not subject to the quality assurance (QA) requirements of 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants." However, the licensing event selection analysis, which uses the results of the initiating event and event sequences analyses, is subject to the previously cited QA requirements because the identification of a comprehensive set of licensing events is foundational to establishing the design basis and the licensing basis of the commercial nuclear plant.

b. Applicants may leverage existing programs and processes when addressing this guidance. For example, if a PRA is developed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or in accordance with RG 1.247 (for non-LWRs), then the PRA Configuration Control Program may be used to control the initiating event and event sequence analysis documentation.

c. If a PRA is planned to be developed and peer reviewed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or RG 1.247 (for non-LWRs), then completion of a peer review and disposition of its facts and observations (F&Os) will satisfy the staff's expectations concerning the independent review. Consistent with DC/COL-ISG-028, peer review of the PRA (including the initiating event and event sequence analyses) is not needed before the application. However, a PRA peer review will help reduce the need for an in-depth review of the PRA by the NRC staff, thus allowing the staff to focus on key assumptions and areas identified as being of concern and relevant to the application. If a peer review has not been performed, the applicants or holders should justify why their PRAs are adequate in terms of scope, level of detail, and technical acceptability. PRA self-assessment is an acceptable tool for assessing the technical adequacy of a PRA performed in support of an application.

Collecting Application-Specific Information

Collect Information on Plant Design, Plant Operating States, and Site Characteristics (Box 3, Principle #1)

9. To support the analysis for initiating events, event sequences, and licensing events, the relevant information regarding plant design, operating states, and, if the site is selected, site characteristics should be collected, and made available to the analysis team. For a DC, SDA, or ML (when the applicant has not yet selected a site), postulated site parameters take the place of site characteristics. The level of information should be consistent with the level of detail of the design information available and be sufficient to facilitate the search for initiating events and the analysis of plant response to support event sequence delineation.

Identify Radiological Sources and Transport Barriers from the Source to the Environment (Box 4, Principle #1)

10. The identification of significant radiological sources should involve, first, a search for and review of plant operating states, including refueling outages; other controlled shutdowns; and forced outages. Depending on the design, significant inventories of radioactive material may be relocated during operation or plant shutdown. The search should consider all radiological sources within the plant including, but not limited to, each reactor core and non-reactor-core source, such as spent fuel in the spent fuel storage system, online fuel or salt processing systems (for molten salt reactors), radioactive waste systems, and other process systems with radioactive material (e.g., radioactive material circulating or plated out within the reactor coolant boundary, spent fuel in the spent fuel storage system, fuel/salt processing systems, radioactive waste systems).

11. For each identified source, the barriers that can prevent the release of radioactive material to the environment (e.g., reactor building, containment, or confinement) should be identified to support the development of event sequences.

Identify Sources of Hazardous Chemical Materials (Box 5, Principle #1)

12. In addition to the search for radiological sources, a search for sources of hazardous chemical materials should be performed. Chemical sources of interest are those that are combined with radiological sources, or which can impact the plant response to an initiating event or can affect the properties of the radiological release. Chemical sources that are not combined with radiological sources, and that do not impact plant response, are outside the scope of the search performed in this step.

13. Other hazards, such as those from nearby industrial facilities, that could induce an initiating event to the nuclear plant are expected to be covered during the search for initiating events discussed in paragraphs 26 through 29 below.

Identify Plant-Specific Safety Functions (Box 6, Principle #1)

14. Having identified the radiological sources and sources of hazardous chemical materials, the previously defined plant-specific safety functions that need to be performed to prevent radiological releases should be identified, followed by the identification of systems and operator actions needed to perform each safety function.

15. Safety functions are those functions performed to limit the release of radioactive materials from the facility and control the sources of energy in the plant. The safety functions are established during the design process for the facility. The concept of safety functions forms the basis for selecting initiating events and delineating potential plant responses. Generally, safety functions specify a group of actions that limit the release of radioactive materials from the facility, or

support the retention of radioactive materials, such as controlling reactivity, heat generation, heat removal, and chemical interactions. Such actions can result from the automatic or manual actuation of a system, from passive system performance, or from the natural feedback inherent in the design of the plant.

16. Identification of the safety functions forms the preliminary basis for grouping accident-initiating events and provides the structure for defining and grouping systems to define a complete set of system responses and interactions for each group of initiating events. Additional distinction may be needed in the definition of safety functions to differentiate among groups of initiating events.

17. Following the identification of the safety functions, the systems needed to perform each safety function should be identified, along with associated success criteria and operator actions needed to perform the safety function. Specific success criteria for each safety function or system that performs safety or support functions should be specified. Typically, success criteria specify the minimum criteria for each function, given an initiating event. The derivation of success criteria should be based on acceptable engineering analyses, performed with validated computer codes by qualified personnel, and represent the design and operation of the plant under consideration. For a safety function to be successful, the success criteria may be dependent on the initiator and the conditions created by the initiator.

18. If a PRA is being developed and peer reviewed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or RG 1.247 (for non-LWRs), the corresponding PRA standard specifies the derivation of success criteria.

Define Plant-Specific End States (Box 7, Principle #1)

19. The end states for event sequences should be defined to support event sequence delineation and selection. The end state of each accident sequence should correspond to either a release of radioactive material or to a safe stable state in which each safety function is fulfilled, and a radioactive release has been prevented. Definition of a safe stable state should be specified.

Analysis Methods Selection

Select Initiating Event Identification Techniques (Box 8, Principle #2)

20. The identification of initiating event search techniques is key to conducting a search that is systematic, comprehensive, exhaustive, and without preconceptions or reliance on predefined lists (i.e., “starting with a blank sheet of paper”). The identification methods could involve a number of different approaches, including the following:

- inductive techniques such as hazard and operability studies, failure mode and effects analysis, or other relevant methods for plant SSCs to determine whether their failures, either partial or complete, could lead to an initiating event; and

- deductive techniques 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.

21. Appendix A to this RG summarizes known techniques for conducting the search for initiators and delineating event sequences. Other approaches may be used with sufficient explanation and technical justification.

22. Using a combination of different techniques should be considered, especially for new designs with little or no operating experience, to gain confidence that the list of initiating events is comprehensive.

Define Initiating Event Grouping Strategy and Characteristics (Box 9, Principle #2)

23. After identification of the initiating events, they should be grouped to reduce the number of analyzed initiating events to a manageable and representative selection that supports the efficient development of relevant event sequences. A strategy for initiating event grouping should be established to support a systematic structured process for grouping. The strategy chosen may depend on the intended scope and depth of the analysis, but generally, initiating events grouping can be based on similarity in plant response, the radioactive barriers that prevent the releases, the mitigating systems involved, associated success criteria, timing, or the effect on operator performance. Alternatively, the initiating events can be bounded by the worst case consequences within the group.

Select Event Sequence Delineation Analytical Methods (Box 10, Principle #3)

24. Following the identification and grouping of the initiating events, applicants should determine the response of the plant to each group of initiating events in order to develop event sequences. The methods needed to perform this task should be clearly identified. The methods can include event sequence diagrams, event trees, or other methods.

25. Event trees are one method to order and depict safety functions according to the mitigation goals of each group of initiating events. The systems needed to successfully perform each safety function should be identified and documented. Depending on plant design, a safety function can be performed by one or more systems, some systems may perform more than one function or portions of several functions, and the systems that perform a certain function may be different for different initiators. Because each initiating event group generates a distinctly different plant response as discussed in paragraph 22 above, function event trees should be developed for each initiating event group.

26. Event sequence diagrams similarly order and depict safety functions according to the mitigation goals of each initiating event group. An event sequence diagram is a graphical tool used to illustrate possible success paths from a particular initiating event to a safe shutdown condition.

Initiating Event Analysis

Apply Initiating Event Identification Methods (Box 11, Principle #2)

27. The objectives of the initiating event analysis are to identify and characterize events that challenge plant operation during any plant operating state, that require successful mitigation by plant equipment, and that require personnel to prevent or to mitigate a release of radiological material. The characteristics and attributes needed to achieve the objectives of an initiating event analysis are as follows:

    - The analysis includes sufficiently detailed identification and characterization of initiating events.

    - Initiating events are grouped so that events in the same group have similar requirements for mitigation.

- Any individual or grouped initiating events are properly screened.

28. The initiating event analysis necessitates a structured, systematic process and accounts for plant- or design-specific features. The methods identified in paragraphs 19 through 21 above should be applied to identify the list of initiating events. The initiating event analysis should include both internal hazards (e.g., internal events, internal flooding, internal fires) and external hazards (e.g., seismic events, high winds, external floods, industrial accidents, transportation accidents),[1] considering the radiological sources and the plant operating modes. Additionally, the analysis should consider scenarios that simultaneously affect multiple reactor modules or radiological sources at the plant. If multiple reactor modules are located on the same site, the analysis should also consider those initiating events that are caused by interactions with the other units or by an accident at one or more of the other units.

29. When screening out initiating events from further consideration, a technical basis should be provided that accounts for design and operational uncertainties.

30. If a PRA is being developed and peer reviewed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or RG 1.247 (for non-LWRs), the guidance on identification of initiating events for a PRA in the corresponding RG and associated PRA standard should be followed.

Apply Initiating Event Grouping Strategy (Box 12, Principle #2)

31. After identifying initiating events, the initiating event grouping should use the process and criteria established in paragraph 22 above. Grouping should ensure that events in the same group have similar mitigation requirements to facilitate an efficient analysis of event sequences and the subsequent derivation of licensing events.

32. If a PRA is being developed and peer reviewed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or RG 1.247 (for non-LWRs), the guidance on initiating events grouping in the corresponding RG and associated PRA standard should be followed.

[1] Many references provide lists of external hazards. In contrast to internal initiating events that can be highly design specific, the external hazards to be considered are generally not design specific. Appendix B to RG 1.247 and the associated non-LWR PRA standard American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS) RA-S-1.4-2021, "Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants" (Ref. 28), provides a list and a general description of the external hazards that can be considered. As stated in ASME/ANS RA-S-1.4-2021, this list was compiled based on a review of previous industry studies.

Account for Relevant Operating Experience and Insights from Earlier Relevant Analyses in the Initiating Event Search (Box 13, Principle #5)

33. To ensure that the final list of initiating events is comprehensive, any relevant operating experience should be reviewed to ensure that the list includes any initiating events that have occurred. Additionally, a review of any prior relevant initiating event analyses performed for other designs should be conducted to ensure that any possible insights are considered and captured in the initiating event list.

Conduct an Independent Review and Complete Quality Control Activities for the Initiating Event Search (Box 14, Principle #5)

34. The process and results of the initiating event search should be independently reviewed to help assure that the list of initiating events is comprehensive. If a PRA is developed and peer reviewed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or RG 1.247 (for non-LWRs), then completion of a peer review and disposition of its F&Os will satisfy the staff's expectations concerning the independent review.

35. Since the systematic and comprehensive search for initiating events is used, in part, to inform the selection of licensing events, it should be developed under the established quality control process.

Event Sequence Selection

Apply Selected Event Sequence Delineation Analytical Methods (Box 15, Principle #3)

36. Similar to the initiating event search and grouping, the event sequence analysis should follow a structured, systematic process. The event sequence analysis should describe the scenarios that can lead to the release of radioactive material following each identified initiating event for all plant operating states and sources of radioactive material. These scenarios should address system responses and operator actions that support the key safety functions necessary to protect the radionuclide barriers and to prevent or mitigate the release of radioactive material. The event sequences should account for the systems that are used (and available) and operator actions performed to mitigate the initiator, based on the defined success criteria, plant operating procedures, and training. The availability of a system includes consideration of the functional, phenomenological, and operational dependencies and interfaces among the various systems and operator actions during the accident progression.

37. If a PRA is being developed and peer reviewed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or RG 1.247 (for non-LWRs), the guidance on event sequence analysis for a PRA in the corresponding RG and associated PRA standard should be followed.

Account for Relevant Operating Experience and for Insights from Earlier Relevant Analyses in the Event Sequence Delineation (Box 16, Principle #5)

38. A review of the operating experience of similar plant designs, if any, and any event sequence analyses performed for similar designs should be conducted to ensure that any possible insights are considered in the event sequence delineation.

Conduct an Independent Review and Complete Quality Control Activities for the Event Sequence Delineation (Box 17, Principle #5)

39. The process and results of the event sequence delineation should be independently reviewed to help ensure that the list of initiating events is comprehensive. If a PRA is being developed and peer reviewed in accordance with RG 1.200 and DC/COL-ISG-028 (for LWRs) or RG 1.247 (for non-LWRs), then completion of a peer review and disposition of its F&Os will satisfy the staff's expectations concerning the independent review.

40. Since the systematic and comprehensive event sequence delineation is used, in part, to inform the selection of licensing events, it should be developed under the established quality control process.

Defining Licensing Events

If a PRA Is Being Developed, Provide the List of Initiating Events and Event Sequences to the PRA (Boxes 18 and 19, Principle #1)

41. If the designer or applicant develops a PRA consistent with the selected regulatory framework, the initiating events and event sequences are integral to the development of the PRA models and, as such, should be provided as inputs to the PRA.

Identify Required Categories of Licensing Events for the Selected Licensing Framework (Box 20, Principle #1)

42. Once the list of event sequences has been completed, the designer or applicant should identify categories of licensing events consistent with the selected licensing framework. Table 1 summarizes the licensing event terminology for the various licensing pathways.

43. Non-LWR designers and applicants who voluntarily seek use of the LMP under 10 CFR Part 50 and 10 CFR Part 52 should use the guidance in NEI 18-04 as endorsed by RG 1.233 to identify licensing events.

44. *Note: The following sections of this RG (specifically, the sections "Define the Licensing Event Grouping Strategy and Its Characteristics" through "Conduct an Independent Review and Complete QA Activities for the Licensing Event Identification") apply to all designers and applicants that did not elect to implement the LMP.*

Define the Licensing Event Grouping Strategy and Its Characteristics (Box 21, Principle #4)

45. Once the categories of licensing events have been identified, the event sequences should be grouped and mapped into the defined licensing event categories. The designers and applicants should define the strategy for grouping event sequences. Grouping can be accomplished in many ways. The events can be grouped by frequency, which can be estimated quantitatively or qualitatively. The events can also be grouped by type of event, which considers aspects such as plant response following the initiating events, the similarity of challenges to the safety functions, or similarity in pathways that could lead to the release of radioactive material to the environment.

Apply the Licensing Event Grouping Strategy (Box 22, Principle #4)

46. Licensing events should be identified using the results of the initiating event search, event sequence delineation, and grouping strategy. All identified event sequences should be mapped to a licensing event category, and no event sequences should be eliminated.

Identify the Limiting Cases for Each Group of Licensing Events (Box 23, Principle #4)

47. A number of limiting cases, referred to as bounding or enveloping scenarios, should be selected from each group of licensing events. The bounding or enveloping scenario(s) should be chosen so that individually or collectively they account for the greatest possible challenges and limiting values for the performance parameters of safety-related equipment of those scenarios within the group. Several initiating events may be combined, or their consequences amplified, or both, to develop a bounding scenario that encompasses all initiating events in the group.

Compare the List of Licensing Events to Predefined Lists (Box 24, Principle #5)

48. To ensure that all relevant licensing events have been considered, the licensing event list should be compared with that for similar plants or type of plants and, for LWRs, with the SRP. Any identified differences should be justified.

Conduct an Independent Review and Complete Quality Assurance Activities for the Licensing Event Identification (Box 25, Principle #5)

49. The process and results of the licensing event identification should be independently reviewed to ensure that the list of licensing events is complete. The list of licensing events should be developed under the relevant QA program for the selected licensing framework.

Documentation

50. Documentation of the analysis for identifying licensing events should be sufficient to allow the staff to determine the acceptability of the analysis and the results. Thus, the documentation should include information necessary for the staff to gain a full understanding of the technical bases of the analysis and the establishment of the licensing basis. This documentation should include information on the process used in the initiating event search, the event sequence analysis and licensing event definition, the applied methods, and the results.

    a. For initiating events, documentation should include information about the systematic search for initiators; the approach to identifying initiating events specified to each identified radiological source; the basis for grouping initiating events; the basis for screening out any initiating event from further consideration; the approach for assessing completeness and consistency of initiating events with previous relevant experience; and any analysis assumptions, uncertainties, and limitations.

    b. For event sequences, the documentation should include information on the linkage between the initiating events and event sequences; a description of each event sequence, including system response and operator actions; success criteria, including the bases for the criteria; a clear definition of each event sequence end state; the analysis performed to support the event sequence analysis; and any analysis assumptions, uncertainties, and limitations.

c. For licensing events, the documentation should include information on the method and basis for grouping the event sequences into licensing events; the selection of limiting cases for each group of licensing events; the approach for assessing completeness and consistency of licensing events with similar plants or type of plants; and any analysis assumptions, uncertainties, and limitations.

51. Documentation should be archived and preserved as lifetime quality records.

52. Submittal documentation should follow the application-specific guidance under the selected regulatory framework.

D. IMPLEMENTATION

The NRC staff may use this RG as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this RG to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 50.109, "Backfitting," and 10 CFR 53.1590, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests" (Ref. 28), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," or 10 CFR Part 53, Subpart H, "Licenses, Certifications, and Approvals." The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this RG in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

ACRONYMS AND ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
ADAMS	Agencywide Documents Access and Management System
AEC	Atomic Energy Commission
AOO	anticipated operational occurrence
ATWS	Anticipated Transients Without Scram
BDBE	beyond-design-basis event
CCA	Cause Consequence Analysis
CCFA	Common Cause Failure Analysis
CFR	*Code of Federal Regulations*
CP	construction permit
COL	combined license
DBA	design-basis accident
DBE	design-basis event
DC	design certification
DFM	Double Failure Matrix
FaHA	Fault Hazard Analysis
FMEA	failure modes and effects analysis
FMECA	Failure Mode Effects and Criticality Analysis
FR	*Federal Register*
FTA	fault tree analysis
FuHA	Functional Hazard Analysis
F&Os	Facts and Observations
HAZOP	hazard and operability
IAEA	International Atomic Energy Agency
IE	initiating event
ISA	integrated safety assessment
ISG	interim staff guidance
LMP	Licensing Modernization Project

LWR	light-water reactor
MA	Markov Analysis
ML	manufacturing license
MLD	master logic diagram
NEI	Nuclear Energy Institute
NRC	U.S. Nuclear Regulatory Commission
OL	operating license
O&SHA	Operating and Support Hazard Analysis
PHA	preliminary hazards analysis
PRA	probabilistic risk assessment
QA	quality assurance
RG	regulatory guide
SDA	standard design approval
SHA	System Hazard Analysis
SLFMEA	System-Level Failure Modes and Effects Analysis
SRP	Standard Review Plan
SSC	structure, system, and component

REFERENCES[1]

1. *U.S. Code of Federal Regulations* (CFR) "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy."

2. CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter I, Title 10, "Energy."

3. CFR, "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants," Part 53, Chapter I, Title 10, "Energy."

4. NRC, "Proposed Rule: Alignment of Licensing Processes and Lessons Learned from New Reactor Licensing (RIN 3150-AI66)." SECY-22-0052. Washington, DC. June 6,2022. ML21159A055

5. NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Washington, DC. (Available at https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/index.html)

6. 10 CFR Part 100. *Code of Federal Regulations*, Title 10, *Energy*, Part 100, "Reactor Site Criteria." Washington, DC.

7. NRC, RG 1.200, "Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities," Washington, DC.

8. NRC, RG 1.206, "Applications for Nuclear Power Plants," Washington, DC.

9. NRC, RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," Washington, DC.

10. Nuclear Energy Institute (NEI) 18-04, Revision 1, "Risk-Informed Performance-Based Technology-Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," Washington, DC, August 2019. (Agencywide Documents Access and Management System (ADAMS) Accession No. ML19241A472)[2]

11. NRC, RG 1.247 (For Trial Use), "Acceptability of Probabilistic Risk Assessment Results for Non-Light-Water Reactor Risk-Informed Activities," Washington, DC.

[1] Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public website at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, Maryland. For problems with ADAMS, contact the PDR staff at (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; or email pdr.resource@nrc.gov.

[2] Publications from the Nuclear Energy Institute (NEI) are available at their website: http://www.nei.org/ or by contacting the headquarters at Nuclear Energy Institute, 1776 I Street, NW, Washington, DC 20006-3708, Phone: (202) 739-8000, Fax: (202) 785-4019.

12. NRC, DC/COL-ISG-028, "Assessing the Technical Adequacy of the Advanced Light-Water Reactor Probabilistic Risk Assessment for the Design Certification Application and Combined License Application," Washington, DC, November 2016. (ML16130A468)

13. Teller, Edward with Allen Brown, *The Legacy of Hiroshima*, Double Day & Company, Garden City, New York, 1964.

14. Beck, Clifford K., TID-7579, "Safety Factors to be Considered in Reactor Siting," *Sixth International Congress and Exhibition of Electronics and Atomic Energy*, Rome, Italy, 1959. (Available at https://www.osti.gov/biblio/4200786-sixth-international-congress-exhibition-electronics-atomic-energy-rome-italy-june-papers)

15. Atomic Energy Commission (AEC), "A Guide for the Organization and Contents of Safety Analysis Reports," June 30, 1966. (ML11255A064)

16. Morris, P.L. (Director, AEC Division of Reactor Licensing), "Plan for Preparation of a Standardized Review Plan," December 19, 1969. (ML19308B888)

17. NRC, NUREG-75/087, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Washington, DC. (Available at https://www.nrc.gov/docs/ML0815/ML081510817.pdf)

18. Advisory Committee on Reactor Safeguards (ACRS) Letter Report, "Review of Draft SECY Paper, 'Population-Related Siting Considerations for Advanced Reactors,'" Washington, DC, October 7, 2019. (ML19277H031)

19. NRC, "NRC Vision and Strategy: Safely Achieving Effective and Efficient Non-Light Water Reactor Mission Readiness," Washington, DC, December 21, 2016. (ML16356A670)

20. ACRS Letter Report, "10 CFR Part 53 Licensing and Regulation of Advanced Nuclear Reactors," Washington, DC, October 21, 2020. (ML20295A647)

21. ACRS Letter Report, "Preliminary Proposed Rule Language for 10 CFR Part 53, 'Licensing and Regulation of Advanced Nuclear Reactors,' Interim Report," Washington, DC, May 30, 2021. (ML21140A354)

22. ACRS Letter Report, "Regulatory Guide 1.247, 'Acceptability of Probabilistic Risk Assessment Results for Advanced Non-Light-Water Reactor Risk-Informed Activities,'" Washington, DC, October 26, 2021. (ML21288A018)

23. NRC, "Nuclear Regulatory Commission International Policy Statement," Federal Register, Vol. 79, No. 132, July 10, 2014, pp. 39415–39418 (79 FR 39415).

24. NRC, Management Directive (MD) 6.6, "Regulatory Guides," Washington, DC.

25. International Atomic Energy Agency (IAEA), Specific Safety Requirement (SSR) SSR-2/1, "Safety of Nuclear Power Plants: Design," Vienna, Austria, 2016.[3]

[3] Copies of International Atomic Energy Agency (IAEA) documents may be obtained through their website: www.IAEA.org/ or by writing the International Atomic Energy Agency, P.O. Box 100 Wagramer Strasse 5, A-1400 Vienna, Austria.

26. IAEA, Specific Safety Guide (SSG) SSG-2, "Deterministic Safety Analysis for Nuclear Power Plants," Vienna, Austria, 2010.

27. American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS) RA-S-1.4-2021, "Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants," American Society of Mechanical Engineers and American Nuclear Society, New York, New York, 2021.[4]

28. NRC, MD 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," Washington, DC.

[4] Copies of American Society of Mechanical Engineers (ASME) standards may be purchased from ASME, Two Park Avenue, New York, New York 10016-5990; telephone (800) 843-2763. Purchase information is available through the ASME web-based store at http://www.asme.org/Codes/Publications/.

APPENDIX A

COMPREHENSIVE SEARCH FOR INITIATING EVENTS

The identification of initiating events (IEs) is the first step that needs to be performed prior to the identification of licensing events. This appendix provides technology-inclusive, generic guidance for conducting an IE search that can be used under any licensing framework.

Identification of IEs is the starting point for the safety assessment of nuclear power plants. Having a reasonably complete set of IEs is crucial in determining what events could propagate to undesirable consequences and in assessing the overall plant risk. A blended and robust approach using multiple methods to identify IEs increases confidence that it produces a list of IEs as complete as possible and thus, all foreseeable IEs are reasonably captured. Generating a set of IEs from different perspectives using different methods (tools) provides a high degree of confidence that risk-significant IEs have been identified and evaluated.

An IE is defined as an occurrence that challenges plant control and safety systems and whose failure could potentially lead to an undesirable end state or radioactive material release. IEs are categorized into internal hazards and external hazards. The internal hazards include internal events, internal floods, and internal fires, while external hazards include seismic events, high winds, external floods, and other external hazards. The American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS) probabilistic risk assessment (PRA) standard, ASME/ANS RA-S 1.4-2021, "Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants" (Ref. A.1), as endorsed by Regulatory Guide (RG) 1.247 (For Trial Use), "Acceptability of Probabilistic Risk Assessment Results for Non-Light-Water Reactor Risk-Informed Activities" (Ref. A.2), provides a typical list of internal and external hazards. Table HS-2 of the PRA standard lists the hazards that are compiled based on the review of industry studies such as NUREG/CR-2300, "PRA Procedures Guide," issued 1983 (Ref. A.3); NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," issued 1991 (Ref. A.4); International Atomic Energy Agency (IAEA) SSG-3, "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants," issued 2010 (Ref. A.5); and Electric Power Research Institute (EPRI) Report 1022997, "Identification of External Hazards for Analysis in Probabilistic Risk Assessment," issued 2011 (Ref. A.6). Although Table HS-2 identifies the potential hazards for preliminary consideration, the table does not explicitly list the internal events, internal floods, and internal fires. Therefore, a comprehensive effort with a thorough systematic search using appropriate methods should be performed to exhaustively identify and evaluate IEs to account for design-specific factors.

Identification of the IEs is an iterative process. The search for IEs is not a one-time activity but involves iterations that are generally commensurate with the design development process that starts with a conceptual design. As the design matures and the understanding of the design and operation of the plant increases, the search for IEs continues, and the list of IEs is further refined and iteratively updated. The set of IEs should be revisited throughout the plant life to reflect the as-built and as-operated conditions.

There are many existing sources of literature and guidance regarding the search for IEs and the methods used for identifying them. One of these guidance documents is NUREG-1513, "Integrated Safety Analysis Guidance Document," issued 2001 (Ref. A.7), which provides general guidance to fuel cycle licensees and applicants on how to perform an integrated safety analysis (ISA) and document the results. Another guidance document on the methods used to identify IEs is NUREG-0492, "Fault Tree Handbook," issued 1981 (Ref. A.8), which discusses the basic concepts of inductive and deductive

techniques, specifically the fault tree method. Other guidance, studies, and papers on identifying and conducting hazard evaluation include the following:

- NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," 1990 (Ref. A.9);
- NUREG-1792, "Good Practices for Implementing Human Reliability Analysis," April 2005 (Ref. A.10);
- NUREG-1842, "Evaluation of Human Reliability Analysis Methods Against Good Practices," 2006 (Ref. A.11);
- RG 1.200, "Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities," 2020 (Ref. A.12);
- NUREG-2198, "The General Methodology of an Integrated Human Event Analysis System (IDHEAS-G)," 2021 (Ref. A.13);
- NRC and Canadian Nuclear Safety Commission, "Joint Report on Terrestrial Energy's Methodology for Developing a Postulated Initiating Events List for the Integral Molten Salt Reactor," 2022 (Ref. A.14);
- IAEA-TECDOC-719, "Defining Initiating Events for Purposes of Probabilistic Safety Assessment," 1993 (Ref. A.15);
- IAEA Safety Standard Series, No. SSG-3, "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants," 2010 (Ref. A.16);
- International Electrotechnical Commission (IEC), International Standard IEC 31010, "Risk Management—Risk Assessment Techniques," 2019 (Ref. A.17);
- ASME/ ANS RA-Sa-2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," 2009 (Ref. A.18);
- Center for Chemical Process Safety (CCPS), "Guidelines for Hazard Evaluation Procedures," John Wiley & Sons, Inc. and the American Institute of Chemical Engineers (AIChE), 2008 (Ref. A.19);
- CCPS, "Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis," AIChE, 2015 (Ref. A.20);
- EPRI, Technical Report 3002000509, "Hazard Analysis Methods for Digital Instrumentation and Control Systems," 2013 (Ref. A.21);
- EPRI, Technical Report 3002018340, "Compilation of Molten Salt Reactor Experiment (MSRE) Technical, Hazard, and Risk Analyses: A Retrospective Application of Safety-in-Design Methods," 2020 (Ref. A.22);
- Idaho National Engineering and Environmental Laboratory, NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995," 1999 (Ref. A.23);
- Vladimir Popović and Branko Vasić, "Review of Hazard Analysis Methods and Their Basic Characteristics," FME Transactions, Vol. 36, 2008 (Ref. A.24); and

- B. Chisholm, S. Krahn, and K. Fleming, "A systematic approach to identify initiating events and its relationship to Probabilistic Risk Assessment: Demonstrated on the Molten Salt Reactor Experiment," Progress in Nuclear Engineering, Vol. 129, 2020 (Ref. A.25).

For IE searching, the combination of a deductive technique with an inductive technique has been found to be effective to ensure completeness of an IE set. The set of IEs can be further refined by performing a human reliability analysis to identify potential human-induced events. In addition, comparing the IE set to the generic list of IEs and operational experiences will provide high confidence that IEs have been comprehensively identified. The choice of the deductive and inductive methods or combination of methods is dependent upon a number of factors, including the reason for conducting the analysis, the results needed from the analysis, the information available, the complexity of the process being analyzed, the personnel and experience available to conduct the analysis, and the perceived risk of the process. Therefore, given the availability of numerous methods, it is not necessary to rely exclusively on any specific one in searching for the IEs.

A-1. Inductive Techniques

The inductive techniques provide answers to the generic question "What happens if …?" More formally, analyzing from specific to general, the inductive process initiates by assuming a particular state of existence of a component and examining to determine the effects of that condition on the system. Attempts to identify all possible hazards or all possible component failure modes, both singly and in combination, are challenging for complex systems. For this reason, the inductive techniques are generally circumscribed by considerations of time, budget, and manpower.

Induction constitutes reasoning from individual cases to a general conclusion. The inductive technique assumes some possible conditions and tries to determine the corresponding effect on the overall system. For example, in constructing an inductive system analysis, one would postulate a particular fault or initiating condition and attempt to ascertain the effect of that fault or condition on system operation. In short, inductive methods are applied to determine what failed states are possible. These methods should be carried out by a suitable, experienced, multidisciplinary team and followed by an independent review. Many inductive methods have been developed, such as the following:

- Double Failure Matrix (DFM),
- Failure Modes and Effects Analysis (FMEA),
- Failure Mode Effects and Criticality Analysis (FMECA),
- System-Level Failure Modes and Effects Analysis (SLFMEA)
- Fault Hazard Analysis (FaHA),
- Functional Hazard Analysis (FuHA),
- Hazard and Operability Analysis (HAZOP), and
- Preliminary Hazard Analysis (PHA).

The most common and well-developed ones among them are FMEA, HAZOP, and PHA.

A-1.1 Failure Modes and Effects Analysis

The ASME/ANS PRA standard defines FMEA as a process for identifying failure modes of specific components and evaluating their effects on other components, systems, and subsystems. As discussed in NUREG-2122, "Glossary of Risk-Related Terms in Support of Risk-Informed Decision-Making," issued 2013 (Ref. A.26), FMEA is generally used to identify IEs for a new plant

design with no operational history or failure data. FMEA is aimed at analyzing the effects of a single component or function failure on other components, systems, and subsystems. FMEA can be useful in identifying IEs that involve support system failures and the expected effects on the plant, especially on mitigating systems.

NUREG/CR-6962, "Traditional Probabilistic Risk Assessment Methods for Digital Systems," issued 2008 (Ref. A.27), describes FMEA as a well-known method used to identify the failure modes of a system and their effects or consequences upon it. In this technique, failure modes can be categorized according to how serious their consequences are, how frequently they occur, and how easily they can be detected.

EPRI Report 3002000509 states that FMEA is a step-by-step approach for identifying possible failures in a design, process, or product. "Failure modes" means the ways, or modes, in which something might fail to meet a specified functional or performance characteristic. "Effects analysis" refers to studying the consequences of those failures. The EPRI report also identifies some FMEA limitations, as follows:

- Common-cause failures—It is difficult to postulate and consider the effects of potential common-cause failures. The focus on single failures also limits consideration of adverse interactions between systems or components, including human interactions.

- Software hazards—The FMEA method typically considers hardware failures only, where it can be applied effectively. However, to date, methods for identifying software failures and determining their effects still require further research, especially since there is no clear industry and regulatory consensus on the meaning of "software failure."

- Dependent on analysis boundary—The FMEA method is useful for analyzing failure modes and effects between components of interest and between interfacing systems and components. However, it may not assess the effects of all interfaces if the boundary is not drawn correctly or if the block diagram does not account for all interfaces that actually cross the boundary in the implemented system.

- Coverage of other hazards—Because the FMEA method is a bottom-up method that is focused on single failures of equipment, it does not systematically identify a wider range of hazards that can lead to accidents or losses, such as requirements errors, human errors, or adverse interactions between components that have not failed.

A-1.2 System-Level Failure Modes and Effects Analysis (SLFMEA)

SLFMEA focuses on the effects of system, subsystem, and train failures on plant operation and shows the impacts on equipment needed to control the plant after a trip. The FMEA looks at the impact of each component failure mode on system performance. In a well-engineered designs that have at least a single-failure criterion, those single component failure modes have no negative impact on any safety or support system. Therefore, the SLFMEA is performed to identify system, sub-system, or train failures that can initiate an accident or challenge functions important to risk.

A-1.3 Hazard and Operability Analysis

NUREG-1513 states that the HAZOP method provides a detailed framework for studying each process, line by line, in an exhaustive manner. Each process variable (such as flow, temperature, pressure), a description of deviations from normal values, potential consequences of these deviations, and existing controls, are recorded.

EPRI Report 3002000509 describes the HAZOP method as a systematic review of a process, using "guide words" to visualize the ways in which a system can malfunction. The HAZOP analysis searches for possible deviations from the design intent that can occur in components, operator or maintenance technician actions, or material elements (e.g., air, water, steam) and determines whether the consequences of such deviations can result in hazards. The EPRI report quoted from IEC Document 61882-2001, "Hazard and Operability Studies (HAZOP Studies)—Application Guide" (Ref. A.28), which states that HAZOP is a structured and systematic technique for examining a defined system, with the objective of (1) identifying potential hazards in the system and (2) identifying potential operability problems with the system and, in particular, identifying causes of operational disturbances and production deviations.

A characteristic feature of a HAZOP study is the "examination session," during which a multidisciplinary team under the guidance of a study leader systematically examines all relevant parts of a design or system. It identifies deviations from the system design intent using a core set of guide words. The technique aims to stimulate the imagination of participants in a systematic way to identify hazards and operability problems. The EPRI report also quoted from IEC 61882-2001 on the limitations of the HAZOP method, as follows:

- Interactions between systems or parts of a system—HAZOP is a hazard identification technique that considers system parts individually and methodically examines the effects of deviations on each part. The hazard may need to be studied in more detail using techniques such as event tree and fault tree analyses if it involves the interaction among a number of parts of the system.

- Trained facilitator—It is difficult to navigate the HAZOP process without a facilitator. A trained facilitator helped the team recognize the error traps created by their own mindsets.

A-1.4 Preliminary Hazards Analysis

NUREG-0492 describes PHA as a method for assessing the potential hazards posed by the system. The objectives of a PHA are to identify the potentially hazardous conditions inherent within the system and to determine the significance or criticality of potential accidents that might arise. A PHA study should be conducted as early in the development stage as possible. This will permit the early development of design and procedural safety requirements for controlling these hazardous conditions.

The first step in a PHA is to identify potentially hazardous elements or components within the system. This process is facilitated by engineering experience, the exercise of engineering judgment, and the use of numerous checklists that have been developed from time to time. The second step in a PHA is the identification of those events that could possibly transform specific hazardous conditions into potential accidents. Then the seriousness of these potential accidents is assessed to determine whether preventive measures should be taken.

EPRI Report 3002000509 explains that, in the preliminary or conceptual design phases of a project, preliminary hazards that could be created by or related to a proposed solution or modification should be identified. PHA involves one or more organized meetings, where the identified individuals come together and review, discuss, and identify potential hazards. The method for performing a PHA relies on the judgment and experience of individuals knowledgeable in the design, operations, maintenance, and licensing basis of the potentially affected systems, subsystems, or components.

Limitations of the PHA method include the hazards recognition that must be foreseen by the analysts. Another key concern is the effects of interactions between hazards that are not easily recognized.

A.2. Deductive Techniques

The deductive techniques address the question of "how can it happen?" Deduction constitutes reasoning from the general to the specific. In a deductive technique, a design or system is reviewed to identify the hazards and causes of each hazard, including those that are caused by multiple failures. The approach postulates that the system itself has failed in a certain way and attempts to find out what modes of system or component behavior contribute to this failure. In these deductive techniques, some specific system failure state is postulated, and chains of more basic faults contributing to this undesired event are built up in a systematic way. The deductive methods are applied to determine how a given system state can occur. Like the inductive techniques, the deductive techniques should be carried out by a suitable, experienced multidisciplinary team and followed up by an independent review. Several deductive methods have been developed, such as the following:

- Cause Consequence Analysis (CCA),
- Common Cause Failure Analysis (CCFA),
- Fault Tree Analysis (FTA),
- Markov Analysis (MA),
- Master Logic Diagram (MLD),
- Operating and Support Hazard Analysis (O&SHA), and
- System Hazard Analysis (SHA).

The most common and well-developed ones among them are FTA and MLD.

A-2.1 Fault Tree Analysis

NUREG-0492 discusses FTA in detail and describes it as an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with component hardware failures, human errors, or any other pertinent events that can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event, which is the top event of the fault tree.

A fault tree is tailored to its top event, which corresponds to some particular system failure modes, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive, as they only cover the most credible faults as assessed by the analyst. FTA is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively.

A fault tree is a complex of entities known as "gates," which serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationships of events needed for the occurrence of a "higher" event. The "higher" event is the "output" of the gate; the "lower" events are the "inputs" to the gate. The gate symbol denotes the type of relationship of the input events required for the output event.

NUREG-2122 describes a fault tree as a deductive logic diagram that graphically represents the various failures that can lead to a predefined undesired event. Fault trees describe how failures of top events occur because of various failure modes of components, human errors, and initiator effects, as well as failures of support systems that combine to cause a failure of a top event.

EPRI Report 3002000509 states that FTA is a top-down method, which postulates failures of high-level safety and generation-related functions and identifies the plant mechanical and electrical equipment needed for these functions. This top-down approach can thereby focus the failure analysis of the system by identifying the potentially important failure modes of the mechanical and electrical components controlled or actuated by the digital system. Some limitations of FTA include the following:

- Focusing on failures—The focus of FTA on failure modes limits the ability of the method to consider interactions between systems or components that can lead to adverse behaviors under plant states in which no failures are present.

- Complexity of models—Fault tree logic models can be large, may be difficult to display on a few pages or screens, and require specialized software to present and review. The effort can be burdensome if not managed effectively.

- Time interdependencies—FTA deals only with binary states (i.e., success/failure) and only examines one top event; it does not address the time dependencies.

A-2.2 Master Logic Diagram

Similar to the FTA, MLD is a logic diagram that resembles a fault tree but without the mathematical properties. It is a hierarchical, top-down, logical decomposition of the general undesired end state, which is shown on the top of the tree, proceeding to increasingly detailed event descriptions at lower tiers and displaying basic IEs. MLD begins with a top event in which the end state is the event of concern and grows into a plant-level logic structure with IEs as the fundamental input events.

NUREG-2122 describes MLD as a graphical model that can be constructed to guide the selection of IEs. An MLD is developed using fault tree logic to show general categories of IEs proceeding to increasingly detailed information at lower levels, with specific IEs presented at the bottom level. In a more general sense, an MLD is a fault tree identifying all the hazards that affect a mission, system, or plant. The difference between an MLD and a fault tree is that a fault tree focuses on accounting for the specific causes leading to failure of a system or group of systems, whereas the MLD focuses on listing the hazards that can affect a top event.

The ASME/ANS PRA standard, ASME/ANS RA-S-1.4-2021, defines MLD as a summary fault tree constructed to guide the identification and grouping of IEs and their associated sequences to ensure completeness.

NUREG/CR-2300 states that the MLD can be constructed to guide the selection and grouping of IEs and to ensure completeness. The events in the MLD are identified by the level they appear in the tree, with the top being Level 1. The use of levels is an ordering technique to assist in locating events. The strategy is to achieve completeness of events by level. The limitations of MLD are similar to those described in the FTA discussion

REFERENCES[1]

A.1 American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS) RA-S-1.4-2021, "Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants," American Society of Mechanical Engineers and American Nuclear Society, New York, New York, 2021.[2]

A.2 U.S. Nuclear Regulatory Commission (NRC), RG 1.247 (For Trial Use), "Acceptability of Probabilistic Risk Assessment Results for Non-Light-Water Reactor Risk-Informed Activities," Washington, DC.

A.3 NRC, NUREG/CR-2300, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," Washington, DC, 1983.

A.4 NRC, NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," Washington, DC, 1991.

A.5 International Atomic Energy Agency (IAEA) SSG-3, "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants," Vienna, Austria, 2010.[3]

A.6 Electric Power Research Institute (EPRI) Report 1022997, "Identification of External Hazards for Analysis in Probabilistic Risk Assessment," Electric Power Research Institute, Palo Alto, California, 2011.[4]

A.7 NRC, NUREG-1513, "Integrated Safety Analysis Guidance Document," Washington, DC, 2001.

A.8 NRC, NUREG-0492, "Fault Tree Handbook," Washington, DC, 1981.

A.9 NRC, NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," Washington, DC, 1990.

A.10 NRC, NUREG-1792, "Good Practices for Implementing Human Reliability Analysis," Washington, DC, April 2005.

[1] Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public website at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, Maryland. For problems with ADAMS, contact the PDR staff at (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; or email pdr.resource@nrc.gov.

[2] Copies of American Society of Mechanical Engineers (ASME) standards may be purchased from ASME, Two Park Avenue, New York, New York 10016-5990; telephone (800) 843-2763. Purchase information is available through the ASME web-based store at http://www.asme.org/Codes/Publications/.

[3] Copies of International Atomic Energy Agency (IAEA) documents may be obtained through their website: www.IAEA.org/ or by writing the International Atomic Energy Agency, P.O. Box 100 Wagramer Strasse 5, A-1400 Vienna, Austria.

[4] Copies of Electric Power Research Institute (EPRI) standards and reports may be purchased from EPRI, 3420 Hillview Ave., Palo Alto, California 94304; telephone (800) 313-3774; fax (925) 609-1310.

A.11 NRC, NUREG-1842, “Evaluation of Human Reliability Analysis Methods Against Good Practices,” Washington, DC, 2006.

A.12 NRC, RG 1.200, “Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Washington, DC, 2020.

A.13 NRC, NUREG-2198, “The General Methodology of an Integrated Human Event Analysis System (IDHEAS-G),” Washington, DC, 2021.

A.14 NRC and Canadian Nuclear Safety Commission, “Joint Report on Terrestrial Energy’s Methodology for Developing a Postulated Initiating Events List for the Integral Molten Salt Reactor,” Washington, DC, 2022.

A.15 IAEA, IAEA-TECDOC-719, “Defining Initiating Events for Purposes of Probabilistic Safety Assessment,” Vienna, Austria, 1993.

A.16 IAEA, Safety Standard Series, No. SSG-3, “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants,” Vienna, Austria, 2010.

A.17 International Electrotechnical Commission (IEC), International Standard IEC 31010, “Risk Management—Risk Assessment Techniques,” Geneva, Switzerland, 2019.

A.18 ASME/ANS, ASME/ANS RA-Sa-2009, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” New York, New York, 2009.Center for Chemical Process Safety (CCPS), “Guidelines for Hazard Evaluation Procedures,” John Wiley & Sons, Inc. and the American Institute of Chemical Engineers (AIChE), New York, New York, 2008.

A.19 CCPS, “Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis,” AIChE, New York, NY, 2015.

A.20 EPRI, Technical Report 3002000509, “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” Palo Alto, California, 2013.

A.21 EPRI, Technical Report 3002018340, “Compilation of Molten Salt Reactor Experiment (MSRE) Technical, Hazard, and Risk Analyses: A Retrospective Application of Safety-in-Design Methods,” Palo Alto, California, 2020

A.22 NRC, NUREG/CR-5750, “Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995,” prepared by Idaho National Engineering and Environmental Laboratory, Idaho Falls, Idaho, 1999.

A.23 Popović, Vladimir, and Branko Vasić, “Review of Hazard Analysis Methods and Their Basic Characteristics,” *FME Transactions*, Vol. 36, 2008.

A.24 Chisholm, B., S. Krahn, and K. Fleming, “A systematic approach to identify initiating events and its relationship to Probabilistic Risk Assessment: Demonstrated on the Molten Salt Reactor Experiment,” Progress in Nuclear Engineering, Vol. 129, 2020.

A.25 NRC, NUREG-2122, “Glossary of Risk-Related Terms in Support of Risk-Informed Decision-Making,” Washington, DC, 2013.

A.26 NRC, NUREG/CR-6962, “Traditional Probabilistic Risk Assessment Methods for Digital

Systems," prepared by Brookhaven National Laboratory, Upton, New York, 2008.

A.27 International Electrotechnical Commission, IEC Document 61882-2001, "Hazard and Operability Studies (HAZOP studies)—Application Guide," Geneva, Switzerland, 2001