17.4 Reliability Assurance Program

The reliability assurance program (RAP) applies to the systems, structures, and components (SSCs) that are identified as risk-significant (or significant contributors to plant safety) as determined by using probabilistic, deterministic, and other methods of analysis, including information obtained from sources such as the plant-specific and site-specific probabilistic risk analysis (PRA), industry operating experience, relevant component failure databases and expert panels. Implementing the RAP will enhance safety by focusing on design resources for risk-significant SSCs and on maintaining the reliability of such SSCs during the design and operation stages of the plant.

17.4.1 Reliability Assurance Program Scope, Stages, and Goals

The purpose of the RAP for the U.S. EPR is to provide reasonable assurance of the following considerations:

- The plant is designed, constructed and operated consistent with assumptions and risk insights for risk-significant SSCs.
- Risk-significant SSCs are selected and maintained so that they do not degrade to an unacceptable level during the life of the plant.
- The frequency of challenges (transients) to risk-significant SSCs is minimized.
- These SSCs will function reliably when challenged.

The RAP is implemented as an integral part of the design process and is implemented during the detailed design phase so that the important U.S. EPR reliability assumptions of the PRA are considered throughout the course of plant life.

The RAP is implemented in two stages. The first stage applies to reliability assurance activities that occur before the initial fuel load. The objective of the RAP during the first stage is to provide reasonable assurance that the reactor design meets the four preceding considerations in the areas of design, procurement, fabrication, construction, and preoperational testing activities and programs. The assumed reliability of SSCs in the design stage will be realistic and achievable.

The second stage of the RAP applies to reliability assurance activities for an operating plant. During the second stage of the RAP, the goal is to verify that the reliability of the SSCs within the scope of the RAP is maintained during plant operation. The activities for the second stage will be integrated into relevant existing programs, such as maintenance rule, surveillance testing, inservice inspection, inservice testing, and quality assurance (QA). Individual component reliability may change throughout the course of plant life because of a number of factors, including aging and changes in suppliers and technology. Plant programs will provide reasonable assurance that the reliability of SSCs will remain acceptable.

17.4.2 Reliability Assurance Program Implementation

The RAP for the design stage is implemented in several phases. The first phase is the design certification phase, which defines the overall structure of the RAP, including guidance for procedures and other activities which will be implemented in future phases. A design-specific PRA model is used to develop a list of SSCs and insights. The risk-significant SSCs are identified in this phase for inclusion in the program using the probabilistic, deterministic, or other methods previously indicated.

The second phase is the site-specific phase, which introduces the plant site-specific design information to the RAP process. A COL applicant that references the U.S. EPR design certification will identify the site-specific SSCs within the scope of the RAP.

Also in this phase, the RAP is modified or appended based on consideration of conditions specific to the site.

17.4.2.1 Design Consideration

The RAP is established to provide sufficient documentation during the design and operation of the U.S. EPR. As part of the design process, SSCs are evaluated to determine their dominant failure modes and the associated effects. Most components have an industry operating history available that defines the significant failure modes and their likely causes.

Strategies for failure prevention or mitigation are developed through the identification and prioritization of the various possible failure modes for each component. This information is provided as input for the operational program phase.

During the design phase, appropriate design reviews and reliability assessments evaluate the reliability of risk-significant SSCs that are identified by the PRA and other sources. As part of the design reliability process, design engineers provide quality and reliability to the development of the SSCs while verifying that the PRA properly models the basis for the design of SSCs. PRA model development during the design phase mostly relies on generic information, bounding assumptions, or design requirements as a basis for model development. An assessment of the model can be performed when changes occur during the plant design phase, as well as during normal plant operations. The assessment considers reliability concepts, such as human reliability, redundancy, diversity, and external events to improve the system design. A further evaluation of design options is pursued if the results of the assessment reveal that the proposed design change could conflict with the results and insights derived from the PRA, or could cause significant unavailability of a safety function.

The design changes that affect the PRA model are reviewed and appropriate revisions are prepared in accordance with the PRA update process.

17.4.2.2 SSC Identification and Prioritization

The first task of the RAP is to identify the risk-significant SSCs that are to be included in the scope of the program. A table that includes a list of design-specific SSCs is included in the RAP. This preliminary list is prepared and controlled under the RAP program. This list is updated when the plant-specific PRA is developed. The selection of risk-significant SSCs uses a combination of probabilistic and deterministic insights such as PRA analytical results, industry experience, regulations, expert panel process, and engineering judgment to identify and prioritize the SSCs.

The Level 1 PRA provides an evaluation of the accident sequences from initiating events and failures of safety functions that lead to core damage. The analysis of external events considers events caused externally to systems associated with power or plant shutdown operations. These events include internal fire, high winds, internal flooding, and seismic margins. Level 2 risk significance is determined qualitatively by identifying dominant contributors to severe accidents and offsite fission product releases.

Risk-significant SSCs can be judged by using the PRA Level 1 model based on the risk achievement worth (RAW) or Fussell-Vesely worth (FVW) of the respective SSCs. Components with an RAW value of two or greater or FVW of 0.005 or greater can be considered risk-significant. The RAW of a component is the factor by which the plant core damage frequency increases if the component reliability is assigned the value of 1.0 (assumed guaranteed to fail). FVW is a measure of the component's contribution to the overall core damage frequency.

17.4.2.3 Expert Panel

An expert panel is established to assess the qualitative and quantitative inputs related to risk-significant SSCs. A preliminary list of risk-significant SSCs is developed using a combination of probabilistic and deterministic insights. This includes information obtained from sources, such as design-specific PRA, nuclear plant operating experience, relevant component failure databases.

The expert panel will use their expertise and PRA insights to develop the list of the risk-significant SSCs. The panel members will use input from the specific risk importance calculational methods (i.e., FVW and RAW) to determine risk-significant SSCs. Each calculational method will identify a different set of SSCs based on differing concepts of importance. Each method is useful for providing insights into the selection of risk-significant SSCs. The expert panel may use all of these methods in the decision making process.

The use of an expert panel compensates for the limitations of the PRA model, such as model assumptions, treatment for support systems, level of definition of cut sets, cut sets truncation, shadowing effect of very large (high frequency) cutsets, and inclusion

of repair or restoration of failed equipment and limitations in the meanings of the importance measures in the Nuclear Energy Institute Guideline NUMARC 93-01 (Reference 1).

The expert panel consists of individuals who possess extensive knowledge in the areas of PRA, risk and reliability, plant operation, system engineering and maintenance. A process is developed for the selection and the qualification of the members.

Meetings are held on an as-needed basis to discuss the final selection of the risk-significant SSCs that are to be included in the RAP. Industry-wide information sources and engineering judgment will be used to consider the addition of SSCs to the RAP.

17.4.3 Organization, Design Control, Procedures and Instructions, Corrective Actions, and Audit Plans

AREVA NP is an integrated design and engineering organization that is responsible for formulating and implementing Phase 1 of the RAP.

The AREVA NP RAP implementation plan includes RAP scope, objectives, design consideration, the identification and prioritization of SSCs, RAP organization, and expert panel. This RAP implementation plan is described in the following paragraphs.

The AREVA NP engineering organization is responsible for the safety analyses, risk and reliability analyses, and the PRA necessary to support the development of the RAP. PRA and design engineering personnel report to the manager of nuclear island engineering. Therefore, risk and reliability personnel are directly involved with the design organization and are responsible for keeping the design staff cognizant of the risk-significant items of the RAP, program needs, and project status. Risk and reliability personnel participate in the design change control process to incorporate RAP-related inputs into the design process. Additionally, a cognizant representative of risk and reliability is present at design reviews to identify interfaces between the performance of risk-significant SSCs and the reliability assumptions in the PRA. Meetings between risk and reliability personnel and the designer are held to manage interface issues.

AREVA NP engineering design procedural controls are applied to the RAP. Specific procedures provide guidance for the design control process, control of design changes, and storage and retrieval controls.

The design control procedure defines the process for performing, documenting, and verifying design activities. This includes the development or modification of system designs, evaluations, analyses, calculations and design document preparation (e.g., specifications, drawings, reports).

The procedure for design change control defines the process for evaluating design changes in engineering controlled documents so that the total effect is considered before a change is approved, and the affected documents are identified and changed accordingly. The procedure identifies the information and organizations responsible for these interfaces, including PRA review. If a proposed change could affect the safety, availability, or capacity factor of the U.S. EPR, system reliability is analyzed.

There are several AREVA NP corporate quality assurance and design control procedures which provide guidance for the development of a high-quality process for the reliability assurance program and for maintaining the appropriate documentation of it. The documentation development and maintenance procedure establishes the requirements and responsibilities for the preparation, approval, and issue of documents controlled by the engineering design organizations. The QA records procedure provides requirements for QA record retention. The self-assessment, corrective action, and audit procedures specify the responsibilities associated with respective audits of the engineering organization. This self-assessment is also used to promptly identify, document, and determine corrective actions for conditions that are adverse to quality.

The above AREVA NP corporate processes provide configuration control of the list of SSCs within the scope of RAP thereby demonstrating that the U.S. EPR reliability assurance implementation program will maintain the scope of RAP SSCs throughout the design process.

17.4.4 Reliability Assurance Program Information Needed in a COL Application

A COL applicant that references the U.S. EPR design certification will provide the information requested in Regulatory Guide 1.206, Section C.I.17.4.4.

17.4.5 References

1. NUMARC 93-01, Nuclear Utilities Management and Resources Council, “Industry Guideline for Monitoring Effectiveness of Maintenance at Nuclear Power Plants,” April 1996.