Annals of Nuclear Energy xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Preliminary risk assessment of the Integral Inherently-Safe Light Water Reactor

Kellen R. McCarroll [a,*], John C. Lee [a], Annalisa Manera [a], Matthew J. Memmott [b], Paolo Ferroni [c]

[a] University of Michigan, United States
[b] Brigham Young University, United States
[c] Westinghouse Electric Company, United States

A R T I C L E   I N F O

Article history:
Received 20 October 2015
Received in revised form 7 September 2016
Accepted 9 September 2016
Available online xxxx

Keywords:
Integral reactor
PRA
Initiating event
Conditional probability
Plant damage frequency

A B S T R A C T

The Integral, Inherently Safe Light Water Reactor (I^{2}S-LWR) concept seeks to significantly increase nuclear power plant safety. The project implements a safety-by-design philosophy, eliminating several initiating events and providing novel, passive safety systems at the conceptual phase. Pursuit of unparalleled safety employs an integrated development process linking design with deterministic and probabilistic safety analyses. Unique aspects of the I^{2}S-LWR concept and design process present challenges to the probabilistic risk assessment (PRA), particularly regarding overall flexibility, auditability and resolution of results. Useful approaches to initiating events and conditional failures are presented. To exemplify the risk-informed design process using PRA, a trade-off study of two safety system configurations is presented. Although further optimization is required, preliminary results indicate that the I^{2}S-LWR can achieve a core damage frequency (CDF) from internal events less than 1.01×10^{-8}/ry, including reactor vessel ruptures. Containment bypass frequency due to primary heat exchanger rupture is found to be comparable to non-vessel rupture CDF.

1. Introduction

The Integral Inherently-Safe Light Water Reactor (I^{2}S-LWR) aims to set a new standard for nuclear power plant safety while maintaining the economic advantages of large, gigawatt-scale plants. Achieving this standard begins with a conceptual design that eliminates multiple accident scenarios and reduces the risk of others. However, development of the I^{2}S-LWR concept's complement of passive, highly reliable safety features continues to elevate these standards by integrating deterministic and probabilistic safety analyses.

1.1. Safety philosophy

The I^{2}S-LWR concept's focus on safety is driven by three primary objectives:

1. Eliminate initiating events where possible; minimize risk otherwise
2. Maximize passivity in safety systems
3. Balance redundancy, diversity, and simplicity of safety systems

From the initial proposal, the I^{2}S-LWR concept eliminated several key design basis accidents (DBAs), including large-break (LB) and medium-break (MB) loss of coolant accidents (LOCAs), seal LOCAs, and rod ejections via an integral reactor pressure vessel (RPV) (Petrovic et al., 2012). Where initiating events (IEs) were not eliminated, many were reduced in frequency. For example, by utilizing high-pressure secondary loops and micro-channel heat exchangers (MCHXs) instead of traditional steam generators, the probability of accidents similar to steam-generator tube ruptures (SGTRs) is reduced (Petrovic et al., 2012). Similarly, minimizing the number of RPV penetrations reduces small-break (SB) LOCA frequency. Additionally, the I^{2}S-LWR concept's large coolant inventory buffers the risk of many accident classes, as do the concept's highly passive safety systems. Even the static containment vessel is designed to slow SBLOCA break flow rates and eventually return condensate back to the RPV.

Design of reliable safety systems for I^{2}S-LWR focuses on maximizing passivity. This approach has been shown to reduce overall plant risk in several instances (Welch et al., 2014). Table 1 illustrates the International Atomic Energy Agency's definitions of degrees of passivity in water-cooled plants. Level C passivity, the

* Corresponding author.
E-mail address: mckellen@umich.edu (K.R. McCarroll).

http://dx.doi.org/10.1016/j.anucene.2016.09.019
0306-4549/

Table 1
Categories of passive safety systems (Safety related terms for advanced nuclear plants, 1991).

Passive system elements	Class			
	A	B	C	D
Structures	x	x	x	x
Working fluids		x	x	x
Moving mechanisms			x	x
Stored operating power				x
External activation signals				x
Degree of passivity				

lowest level acceptable for many I^{2}S-LWR safety systems, may utilize moving parts, but not stored operating power or an external activation signal. By relying on natural phenomena, high probability failure modes such as losses of electrical power and operator error are minimized or eliminated altogether. The I^{2}S-LWR concept is being developed to utilize natural circulation loops, gravity, and air as an ultimate heat sink wherever possible. Valves are designed to fail to a safe line-up without an applied motive force. Where motive forces are required, highly reliable sources of stored energy are used, either with safety-grade batteries, pressurized tanks or accumulators, compressed springs, or gravitational potential energy. However, few mechanical components will require long-term motive forces to operate. Additionally, a relatively small, hydraulically-coupled containment structure facilitates rapid, fully passive pressure equalization, slowing and eventually stopping LOCA break flows.

Finally, high levels of safety require a balance of redundancy, diversity, and simplicity amongst safety systems. Redundancy is essential to satisfy the General Design Criteria of 10 CFR 50 Appendix A, ensuring that a single component or system failure does not cause severe consequences (Design Criteria for Nuclear Power Plants, 1971). However, deployment of many identical components or systems leaves the plant vulnerable to common cause failures (CCFs). Therefore, diversity of safety systems with similar objectives but fundamentally different strategies is essential. Still, numerous diverse safety systems, each with a large degree of redundancy, can be counterproductive from a safety (and economic) standpoint. In this case, the number of unexpected, complex system interactions can become overly burdensome on operators during unforeseen accident scenarios (Perrow, 1984). Therefore, a risk-informed design process assuring low-levels of risk without unnecessary complexity is required.

The balancing of redundancy, diversity, and simplicity whilst maximizing passivity and eliminating accident initiators presents an organizational challenge to the I^{2}S-LWR safety team.

1.2. Preliminary probabilistic risk assessment

Although the conceptual design sets the stage for achievement of unprecedented nuclear safety, the I^{2}S-LWR safety team is organized to execute and improve the concept's inherent safety. The I^{2}S-LWR Preliminary Probabilistic Risk Assessment (PRA) is integrated with several other efforts in plant design and development. Hence, a brief overview of safety-team dynamics and common safety approach is given.

1.2.1. Safety team organization

For I^{2}S-LWR development with three primary objectives, ensuring comprehensive safety requires a cooperative, iterative design approach from several working groups. Fig. 1 diagrams this integrated process.

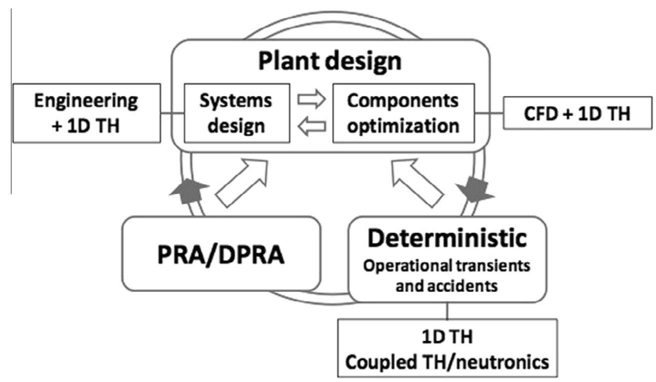

Fig. 1. Safety-design team interactions (Petrovic et al., 2012).

To initiate this scheme, a conceptual design was created specifying high-level system and component designs based on engineering judgment, 1-D thermal-hydraulic (TH) analyses, and safety, economic, and performance goals (Petrovic et al., 2012). With a concept proposed, a list of anticipated limiting transient events (LTEs) was generated based on the U.S. Nuclear Regulatory Commission (NRC) Standard Review Plan (SRP) for consideration in both deterministic and probabilistic safety analyses (NUREG/CR-0800, 2007). Deterministic analyses of accident transients using coupled TH-neutronic codes give direct feedback for design parameters, as well as suggested success criteria and accident progression information for the PRA. The PRA, which will eventually evolve into a dynamic PRA (DPRA), identifies risk-significant design and operational factors, suggesting critical design modifications and deterministic analyses. This iterative process continues, ensuring the I^{2}S-LWR concept evolves to meet its three primary objectives.

1.2.2. Preliminary PRA purposes

To support the advancing I^{2}S-LWR design in parallel with deterministic safety analyses, the PRA team is developing a Level-1 Preliminary PRA focused on internal IEs. Traditionally, PRAs are performed after a plant is built (Generation II) or as part of the initial licensing process (Generation III+) (Mizuno et al., 2002). However, preliminary PRAs such as those of the I^{2}S-LWR concept and its predecessor, IRIS, are performed alongside the design of the plant itself (Mizuno et al., 2002). Integrated, simultaneous development of the I^{2}S-LWR concept with its associated risk assessment minimizes costly redesigns and maximizes safety. Section 1.2.1 discussed this iterative process amongst systems design, deterministic safety analyses, and PRA. One significant challenge of a Preliminary PRA is the large number of requisite assumptions since many "blanks" exist in the preliminary designs. However, despite many unknowns and significant uncertainty, simultaneous PRA and design development can obtain six vital objectives:

Please cite this article in press as: McCarroll, K.R., et al. Preliminary risk assessment of the Integral Inherently-Safe Light Water Reactor. Ann. Nucl. Energy (2016), http://dx.doi.org/10.1016/j.anucene.2016.09.019