Nuclear Engineering and Design 239 (2009) 1699–1702

Contents lists available at ScienceDirect

Nuclear Engineering and Design

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

Implementing risk-informed life-cycle design

Ralph S. Hill III*

Westinghouse Electric Company, LLC, 4350 Northern Pike, Monroeville, PA 15146, USA

ARTICLE INFO

Article history:
Received 30 October 2007
Received in revised form 16 April 2009
Accepted 16 April 2009

ABSTRACT

This paper describes a design process based on risk-informed probabilistic design methodologies that cover a facility's life-cycle from start of conceptual design through decontamination and decommissioning. The concept embodies use of probabilistic risk assessments to establish target reliabilities for facility systems and components. The target reliabilities are used for system based code margin exchange and performance simulation analyses to optimize design over all phases (design, construction, operation and decommissioning) of a facility's life-cycle. System based code margin exchange reduces excessive level of construction margins for passive components to appropriate levels resulting in a more flexible structure of codes and standards that improves facility reliability and cost. System and subsystem simulation analyses determine the optimum combination of initial system and component construction reliability, maintenance frequency, and inspection frequency for both active and passive components. The paper includes a description of these risk-informed life-cycle design processes, a summary of work being done, and a discussion of additional work needed to implement the process.

1. Introduction

This paper describes a future design process based on risk-informed probabilistic methodologies that cover a facility's life-cycle from start of conceptual design through end of operations. A facility specific "living PRA", system based code margin exchange and performance simulations are integral parts of the process. Process and methodology development activities that are needed for the design process to be realized are identified. Finally, a path forward is recommended.

2. Background

A probabilistic risk assessment (PRA) is a systematic and comprehensive analysis of the potential events that can occur at a plant along with their consequences and probability of occurring. It incorporates system reliability as well as human behavior factors. Results provide a thorough description of the frequency and consequences of potential events.

PRAs have been used for many years to assess and determine reliability and safety of existing nuclear power plants. PRAs, in combination with deterministic system and engineering analysis, are used to make risk-informed decisions at operating plants on in-service inspection, in-service testing and, more recently, repair and replacement.

Application of these risk-informed decision making methodologies has increased safety by focusing plant resources on areas of highest safety significance. This results in enhanced public and worker safety while reducing operation and maintenance costs that support shorter plant outages. A logical next step is to apply risk-informed probabilistic analysis methods to plant design.

Probabilistic design analysis methods have been developed to address uncertainty and randomness through statistical modeling and probabilistic analysis. Historically, the computational resources to accurately capture uncertainties and estimate probability of failure made application of these methods impractical. Current computing resources, failure databases, and the availability of probabilistic design tools provide an environment for applying probabilistic risk analysis and risk optimization effectively.

Previously discussed risk-informed in-service inspection, testing, and repair and replacement methodologies have been adopted by the American Society of Mechanical Engineers (ASME) nuclear codes and standards (ASME, 2002 and Code Cases). The American Institute of Steel Construction (AISC) and the American Concrete Institute (ACI) have incorporated probabilistic methodologies into their design codes (AISC, 1994, 2003) (Cornell, 1969). Probabilistic design methodologies are being considered for ASME nuclear (Section III) and non-nuclear (Section VIII, Division 2) code applications.

Despite these advances, design processes used in the nuclear industry today are predominately deterministic and not risk-informed. New design processes are needed that incorporate risk insights derived from a PRA that evolves along with the design.

* Tel.: +1 412 374 4264; fax: +1 412 374 4210.
E-mail address: hillrs@westinghouse.com.

0029-5493/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.nucengdes.2009.04.006

3. Process overview

The proposed concept embraces the use of PRAs to provide a thorough description of the frequency and consequences of potential events, to develop risk-consequence curves that are then used to determine system safety classification, and to establish system and component reliabilities. Component reliabilities are used to determine the appropriate partial safety factors for use in design equations expressed in the reliability-based Load Resistance Factor Design (LRFD) format. The resulting design can be further evaluated using System Based Code margin exchange methodologies for passive components and system and subsystem performance simulations using Monte Carlo analyses for both active and passive components to determine the optimum combination of initial component fabrication and construction reliability, maintenance frequency, and inspection frequency.

3.1. Margin exchange

Current material, design, construction, inspection and maintenance codes are well established, but independent and self-complete. Each code provides safety margins to assure integrity. Through the current design process, margins accumulate and can become excessive resulting in overly conservative and costly designs. The System Based Code concept introduced by Professor Emeritus Yasuhide Asada (Asada et al., 2002a,b) and further developed by Morishita, Asayama and Tashimo (Asada, 2006), proposes to resolve this problem.

The System Based Code is a design process that reduces the excessive level of margins for passive (pressure boundary and structural integrity) functions to appropriate levels based on design to target reliability. It embraces expansion of technical options beyond what current codes and standards allow and exchange of margin among the technical options. Margin exchange utilizes the flexible structure of codes and standards and optimizes both reliability and cost.

3.2. Performance simulations

As demonstrated by Hill and Nutt (2003) performance simulations can be used to evaluate and optimize designs of individual facility systems over the facility's life-cycle. Active (pumps, valves, etc.) and passive (vessels, piping, etc.) system components are included in the model. Reliability of conceptual system designs is evaluated using different variables for each of the system components. These component variables include: reliability, based on quality of initial construction; failure rate; maintenance frequency; and inspection frequency. Stochastic simulation is used to evaluate alternative combinations of these variables against the system target reliability established by the conceptual PRA. Cost may be assigned to each of the variables permitting evaluation and optimization of life-cycle system costs. Decontamination and decommissioning costs can be included to evaluate alternative conceptual designs for cost over the complete life-cycle.

Outputs of the performance simulations include initial subsystem and component target reliabilities, safety classifications, failure rates, inspection and maintenance frequencies, and documented assumptions on system operation and operator actions. These outputs are inputs into the margin exchange process step for passive components and also feed back in to the next iteration of the PRA.

4. Risk-informed design process

During evolution of design from conceptual system design to final system design, the PRA and design evolve in sequential fashion, as illustrated in Fig. 1. A PRA is developed for a facility based on conceptual system design. Results of the conceptual PRA are used to develop risk-consequence curves that are used to determine system safety classification and to establish system reliabilities. System reliabilities are used to determine component classifications. New ASME code rules will be required for design to the component reliabilities specified by the component classification.

During design evolution from preliminary to final, trade-offs are made between subsystem and component reliabilities as long as the parent system target reliability is maintained. System Based Code methodologies may be applied for passive components to optimize reliability levels for passive components. Similarly, performance simulations using Monte Carlo analysis may be used to perform trade-offs between component construction reliabilities, maintenance frequency, and inspection frequency as long as system reliability is maintained over the facility life-cycle.

A practicing engineer would not see a great deal of difference from the way analysis is performed today. Current design equations apply deterministic factors, based on years of experience and limited testing, to account for variances in loading conditions and strength of materials. Application of reliability-based LRFD replaces safety factors in these deterministic design methods with partial safety factors that account for uncertainties in loading conditions, prediction models, and strength of materials. These partial safety factors would be incorporated in the new code rules as look-up tables, e.g., for a given load condition and a given reliability, the tables would provide the appropriate partial safety factors. These tables would be transparent to the engineer because they would be incorporated into design analysis software.

5. Process and methodology needs

As shown at the top of Fig. 1, the reliability-based LRFD methods and PRA standards (for other than light water reactors) require further development to enable the realization of a risk-informed design process. Table 1 depicts the current status of the development of the risk-informed design methods as applicable to nuclear power plant components.

Until recently, the development of PRA standards has focused on current-design light water reactors (LWRs). The LWR PRA standards are now being used as a starting point for development of new standards that would be compatible with gas cooled and other non-light water reactor designs.

6. Path forward

Work to date to develop the methodologies and processes needed to realize a risk-informed design process has been piecemeal and ad hoc. The ASME Board on Nuclear Codes and Standard's Risk Management Strategic Plan provides a high level vision of a future risk-informed design process and tracks risk-informed initiatives being pursued within the ASME codes and standards committees. However, there has not been an integrated plan and funding to accomplish the needed development in accordance with a pre-established schedule.

Table 1
Status of risk-informed design methodologies.

Component	Risk-informed design methodologies
Safety classification	Code Case N-720 under development
Vessels	Section VIII, Div. 2 Re-write
Piping	Section III, proof of concept completed for primary loadings—further development required
Pumps	Section III, new development required
Valves	Section III, new development required
Supports	LRFD version of AISC N-690 Code Case N-721 to incorporate LRFD version of AISC N-690