Nuclear Engineering and Design 333 (2018) 63–75

Contents lists available at ScienceDirect

Nuclear Engineering and Design

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

A case study of time-dependent risk informed integrated safety assessment under complex accident sequences

Kyung-min Yoon[a,c], Hyun-gook Kang[a,b,*]

[a] Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 305-701, Republic of Korea
[b] Department of Mechanical, Aerospace and Nuclear Engineering, Rensselaer Polytechnic Institute, 110 8th Street, Troy, NY, USA
[c] Department of Safety Analysis, KEPCO Nuclear Fuel, 242, Daedeok-daero 989, 34057 Daejeon, Republic of Korea

ARTICLE INFO

Keywords:
Time-dependent risk informed integrated safety assessment
Design extension conditions
Complex accident sequences
Failures of multiple engineered safety features
Consequential failure probability
Central limit theorem
Point-estimate failure time
Non-parametric order statistics
Containment bypass accident

ABSTRACT

A time-dependent risk informed integrated safety assessment methodology is suggested to evaluate the response of nuclear power plants under complex accident sequences caused by failures of multiple safety features. Event propagation is modeled based on the combination of deterministic and probabilistic safety assessment methods, with results representing changes in plant risk over time. Operators can utilize the time-dependent risk information as a quantitative basis, and results can determine the degree of safety enhancement by the improvement of emergency operator action procedures or by strengthening the design of safety features. The concepts of consequential failure probability and point-estimate failure time are introduced. The consequential failure probability, calculated from central limit theorem, identifies the key safety system and provides a precise risk calculation. The point-estimate failure time, using non-parametric order statistics, justifies the crediting of emergency operator actions. As a case study, risk of large early radioactive release due to pressure-induced multiple steam generator tube rupture following main steam line break accident in Advanced Power Reactor 1400 is considered. Results are used to discuss the credibility of operator mitigation actions, and a remedy to enhance plant safety to satisfy safety goals is suggested.

1. Introduction

1.1. Research background

Traditionally, the design basis states of nuclear power plants (NPPs) are classified into operational states (i.e., normal operation, anticipated operational occurrences) and design basis accidents (DBAs). Design basis accidents are composed of a set of accidents categorized by expected occurrence frequency and consequences. The purpose of DBA analysis is to ensure the safety of NPPs by assessing the performance of the safety systems, the applicability of design and operating parameters, and the validity of technical specifications.

In a historical view, there have been three occurrences of beyond design basis accidents (BDBAs): Three Mile Island in 1979, Chernobyl in 1986, and Fukushima in 2011. The term BDBAs is used for accidents that are not included in DBAs and not fully considered in design and operation; their occurrence is judged to be highly improbable. However, following the Fukushima Daiichi accident, global safety analysis methods have been evolving to cope with BDBAs. As part of this effort, the International Atomic Energy Agency (IAEA) has established a new NPP state called design extension conditions (DEC) (IAEA, No. SSR-2/1, 2012).

The main purpose of the introduction of DEC was to further improve the safety of NPPs by actively including BDBAs in design basis states and operation. The goals of safety analysis under DEC are to identify additional threats that may potentially lead to severe conditions, to prevent the occurrence of these threats, and to mitigate the consequences. Compared to safety assessment for DBAs though, which assume a single initiating event with a single failure of safety features, challenges arise for DEC on account of their complex sequences.

1.2. Objective and scope

The main objective of this research is to suggest a time-dependent risk informed integrated safety assessment methodology (TRISAM) for performing systematic and comprehensive safety assessment of NPPs to support a determination of safety enhancement measures under complex accident sequences (CAS). These accident sequences involve failures of multiple engineered safety features (ESF), which cause the loss of single or multiple safety functions. As a type of DEC, significant fuel

* Corresponding author at: Department of Mechanical, Aerospace and Nuclear Engineering, Rensselaer Polytechnic Institute, 110 8th Street, Troy, NY, USA.
E-mail address: kangh6@rpi.edu (H.-g. Kang).

https://doi.org/10.1016/j.nucengdes.2018.03.044
Received 10 December 2017; Received in revised form 30 March 2018; Accepted 31 March 2018

Abbreviations

APR1400	Advanced Power Reactor 1400
AFW	Auxiliary Feedwater
BDBA	Beyond Design Basis Accident
BEPU	Best Estimate plus Uncertainty
CAS	Complex Accident Sequences
CFP	Consequential Failure Probability
CDF	Core Damage Frequency
CLT	Central Limit Theorem
DEC	Design Extension Conditions
DBA	Design Basis Accident
DSA	Deterministic Safety Assessment
DTET	Discrete Time-dependent Event Tree
ET	Event Tree
ESF	Engineered Safety Features
EOP	Emergency Operation Procedure
EUR	European Utility Requirement
FT	Fault Tree
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
IE	Initiating Event
IRWST	In-containment Refueling Water Storage Tank
KSS	Key Safety System
LER	Large Early Release
LWR	Light Water Reactor
MSLB	Main Steam Line Break
MSI	Main Steam Isolation
NPP	Nuclear Power Plant
PZR	Pressurizer
PDF	Probabilistic Density Function
PFT	Point-estimate Failure Time
PSA	Probabilistic Safety Assessment
RCS	Reactor Coolant System
RRW	Risk Reduction Worth
RAW	Risk Achievement Worth
SRS	Simple Random Sampling
SGTR	Steam Generator Tube Rupture
SG	Steam Generator
SI	Safety Injection
SCN	Scenario
TRISAM	Time-dependent Risk informed Integrated Safety Assessment Methodology
TRI	Time-dependent Risk Information
T&M	Test and Maintenance
Unc.	Uncertainty
VOPT	Variable Over Power Trip

Symbols

N	Minimum required number for SRS calculation
T^{γ}	γ*100th percentile of a true failure time
$\hat{T}^{\gamma}$	Point estimator of T^{γ}
$\hat{T}_i^{\gamma}$	Point estimator of T^{γ} of scenario i
T_o	Operator action initiating time
γ	Degree of percentile for PFT
δ	Degree of confidence level for PFT
P	True value of consequential failure probability
$\hat{P}$	Maximum Likelihood Estimator of P
$\hat{P}^{\frac{\alpha}{2}}$	The upper limit of estimation interval of P at two sided $(1-\alpha)*100$ confidence interval
$\hat{P}_i^{\frac{\alpha}{2}}$	$\hat{P}^{\frac{\alpha}{2}}$ of scenario i
$Z_{\frac{\alpha}{2}}$	The point at which $P(Z > Z_{\alpha/2}) = \alpha/2$, $Z \sim N(0,1)$
E_n	nth event
E_{n-1}	n-1th event
E_n^i	nth event of scenario i
$P(E_n^i$: $t_n)$	Probability of Occurrence of nth event at time t_n
$P(E_i^{OP})$	Unreliability of operator action
P_{IE}	Initiating Event Frequency
$F_i(t_n)$	System unreliability of scenario i at time t_n
C_i	Consequence of scenario i
X_j	Random variable of bernoulli trial
$R_i(t)$	Time-dependent Risk of scenario i at time t
R_T	Total potential risk
R_c	Acceptable target risk criterion
C_P	Conditional probability for one or more tube ruptures during transient
C_A	Conditional probability for one or more tube ruptures during MSLB accident
ΔP_i	Peak differential pressure across tubes during transient
ΔP_n	Normal operating pressure differential across tubes
ΔP_a	Peak differential pressure across tubes during MSLB accident

degradation must be prevented under CAS (IAEA, No. SSR-2/1, 2016; EUR for LWR NPPs, 2012).

This research includes an overview, research survey, procedure, and case study. In the overview, a general description of TRISAM is given by comparing the existing safety assessment methodologies. Relevant research is then introduced, followed by the procedure section where a detailed description is given for all steps of TRISAM: scenario identification using time-dependent event trees, accident consequence analysis, system reliability analysis, and time-dependent risk information (TRI) generation. In the case study, availability and applicability are shown by applying the TRISAM to a containment bypass accident analysis. As this research aims at preventing severe core damage occurrence under CAS, it is considered out of present scope to address phenomenological aspects after the core damage condition is reached.

2. Overview of TRISAM

At present, there are two main safety analysis methodologies: deterministic safety assessment (DSA) and probabilistic safety assessment (PSA). The former has served a vital role in DBA analysis under the defense in depth philosophy. The deterministic approach has strengths regarding familiarity to utility and regulatory bodies, completeness of its application, clarity in predicting the sequence of an accident in a pre-determined scenario, and a straightforward interpretation of results where, based on a margin calculation, status is regarded as safe or unsafe depending on the margin for the acceptance criteria.

Since the deterministic approach assumes that system and operator behaviors can be captured and modeled with a fixed frame, it has limitations in handling unknown threats such as: the possibility of multiple ESF failures, internal hazards, external hazards, digital system failures, and operator error. In this perspective, the DSA is regarded as an incomplete methodology for BDBA analysis.

To overcome the limitations of the deterministic approach, PSA was introduced in 1975 to identify unknown threats in NPPs (U.S. NRC, NUREG-75/014, 1975). The probabilistic approach identifies possible scenarios not considered in the deterministic approach, and calculates the frequency of scenario occurrence that can potentially lead to core damage. The biggest advantage of the probabilistic approach is that it can provide insights for decision-making in the process of design and operation.

While the deterministic approach aims to evaluate safety in a dichotomous way, the probabilistic approach perceives safety as a