Reliability Engineering and System Safety 160 (2017) 136–150

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

An approach to address probabilistic assumptions on the availability of safety systems for deterministic safety analysis

S. Martorell[a,*], P. Martorell[a], I. Martón[a], A.I. Sánchez[b], S. Carlos[a]

[a] Department of Chemical and Nuclear Engineering. Universitat Politècnica de València, Valencia, Spain
[b] Department of Statistics and Operational Research. Universitat Politècnica de València, Valencia, Spain

ARTICLE INFO

Keywords:
Extended BEPU
PSA
Option 4
Realistic approach
Probabilistic
Deterministic
Uncertainty
Safety analysis
Best Estimate Plus Uncertainty methodology
Design basis conditions
Design extension conditions

ABSTRACT

There is an attempt nowadays to provide a more comprehensive and realistic safety assessment of design and operation of Nuclear Power Plants. In this context, innovative approaches are being proposed for safety assessment of nuclear power plants design including both design basis conditions and design extension conditions. An area of research aims at developing methods for combining insights from probabilistic and deterministic safety analyses in Option 4, also called realistic approach, from the International Atomic Energy Agency specific safety guide. The development of Option 4 or realistic approach involves the adoption of best estimate computer codes, best estimate assumptions on systems availability and best estimate of initial and boundary conditions for the safety analysis. This paper focusses on providing the fundamentals and practical implementation of an approach to integrate PSA-based probabilistic models and data, which incorporate best estimate assumptions on the availability of safety systems, into Option 4. It is presented a practical approach to identify relevant, i.e. most probable, configurations of safety systems and to assess the associated occurrence probability of each configuration using PSA models and data of a NPP, which is based on the use of a Pure Monte Carlo method. An example of application is provided to demonstrate how this approach performs. The case study focusses on an accident scenario corresponding to the initiating event “Loss Of Feed Water (LOFW)” for a typical three-loops Pressurized Water Reactor (PWR) NPP.

1. Introduction

Nuclear industry has relied on the concept of defense in depth and safety margins to deal with the uncertainties associated with the design and operation of nuclear facilities. In this context, both deterministic and probabilistic safety analyses are performed with an aim to achieve regulatory approval of Nuclear Power Plant (NPP) design and operation according to well-established licensing basis.

The adoption by regulators of the risk-informed decision-making philosophy [1] represents a key milestone to understand both the evolving regulatory framework and the growing research interest towards developing methods for using Probabilistic Safety Analysis (PSA) results into requirements and assumptions in Deterministic Safety Assessment (DSA) and vice versa. There is an attempt to provide a more comprehensive and realistic safety assessment of reactor design and operation. In addition, Fukushima Daiichi accident has raised new challenges such as the revision of current design license basis accounting for not only design basis conditions (DBC), e.g. anticipated occupational occurrences and design basis accidents (DBA), but also design extension conditions (DEC), e.g. DEC without and with fuel damage, in a context where innovative approaches of safety assessment of current NPP are welcome.

What concerns DSA (Deterministic Safety Analysis), the International Atomic Energy Agency (IAEA) produced guidance on the use of deterministic safety analysis for the design and licensing of nuclear power plants (NPPs): “Deterministic Safety Analysis for Nuclear Power Plants Specific Safety Guide,” Specific Safety Guide No. SSG-2 [2], which is now under revision [3]. SSG- 2 addresses four options for the application of DSA.

Options 1 and 2 are conservative and they have been used since the early days of civil nuclear power, and are still widely used today. However, the desire to utilize current understanding of important phenomena and the availability of reliable tools for more realistic safety analysis without compromising plant safety has led many countries to use option 3. Option 3 involves the use of best-estimate codes and data together with an evaluation of the uncertainties, the so called BEPU (Best Estimate Plus Uncertainty) methodology. Several BEPU approaches have been developed [4–11], some of them in scopes that

* Corresponding author.
E-mail address: smartore@iqn.upv.es (S. Martorell).

http://dx.doi.org/10.1016/j.ress.2016.12.009
Received 7 April 2016; Received in revised form 21 November 2016; Accepted 19 December 2016
Available online 21 December 2016
0951-8320/

Nomenclature

AFW	auxiliary feedwater system
AS	accidental sequence
BE_k	basic event k belonging to the boolean equation (BE) of a TC_{ij}
BEAS	boolean equation of AS
BEPU	best estimate plus uncertainty methodology
$BESF_i$	boolean equation of SF_i
$BETC_{ij}$	boolean equation of TC_{ij}
CCF	common cause failure
CD	core damage
CDF	core damage frequency
DBA	design basis accidents
DBC	design basis conditions
DEC	design extension conditions
DSA	deterministic safety analysis
EBEPU	extended BEPU methodology
ET	event tree
FB	feed and bleed
FOM	figure of merit
FOS	first order statistics
FT	fault tree
IAEA	international atomic energy agency
IE	initiating event
IHI	high pressure injection system – recirculation mode
IHR	high pressure injection system – recirculation mode
LB	licensing basis
LOFW	loss of feed water initiating event
MCS	minimal cut set
MSIV	main steam isolation valve
NRC	nuclear regulatory commission
NPP	nuclear power plant
OS	order statistics
PDF	probability distribution function
PMCM	pure monte carlo method
PORV	pressure operated relief valves
PRZ	pressurizer
PSA	probabilistic safety analysis
PWR	pressurized water reactor
RCS	reactor coolant system
RPS	reactor protection system
RV	relief valve
SD	steam-dump valve
SF_i	safety function *i*
SG	steam generator
STL	standard tolerance level
SV	safety valve
TC_{ij}	train/component *j* of safety function *i*
TH	thermal hydraulic
TOPs	top events

are accepted by the regulator authorities nowadays. Most of them are based on propagation of input uncertainties and make use of the Wilks'–based methods to determine the number of calculations of the output (usually safety-related parameters) needed to verify compliance of acceptance criteria with "Standard Tolerance Levels (STL)" (typically 95/95) in accordance with current regulatory practice. Ref. [4] provided a review of groups of tools and methods being proposed up to 2008 to perform BEPU analysis, e.g. statistical methods, use of surrogate models, etc. Pourgol-Mohammad, [5] and D'Auria et al. [6] published the fundamentals of several of them. Wilsom, [7] presented historical insights in the development of BEPU safety analysis. Unal et al. [8] proposed an improved BEPU methodology including advanced validation concepts to license evolving nuclear reactors and more recently Queral et al. [9] presents an application of the BEPU methodology for the safety analysis of a Large-Break LOCA with TRACE code of an advanced NPP.

Development of Option 4 of the IAEA Specific Safety Guide SSG-2 [2,3], which is also called realistic deterministic safety analysis, is currently under research. An area of research in this context aims at developing methods for combining insights from probabilistic and deterministic safety analyses [12,13]. Even more, some research aims at developing methods for integrating deterministic and probabilistic safety assessment or even at developing an integrated safety assessment methodology [14–16]. The new methods, such as the one presented in [13], are intended to be used for safety assessment of some current NPP design basis conditions, e.g. anticipated occupational occurrences also called DBC-2, and design extension conditions without and with significant fuel degradation, which are also called DEC-A and DEC-B accidents respectively. Option 4 is not allowed for design basis accidents (DBA) within the design basis conditions, called DBC-3 and DBC-4, where it is proposed only the adoption of Options 1–3 (see section 2.15 in Ref. [3]).

In this research context, it is proposed to face the challenge of combining the use of well stablished BEPU methods and probabilistic-based assumptions on systems availability to build an extended BEPU methodology, called EBEPU methodology [12,13], following the fundamentals of Option 4 based on the IAEA SSG-2 guide, which can be used for realistic deterministic safety analysis of current NPP designs [2,3]. In Ref. [13], a novel EBEPU approach was introduced merging traditional BEPU methods and PSA-based assumptions on the availability of safety systems, which consists of the following steps:

1. Selection of the accident scenario.
2. Selection of the safety criteria linked to the accident scenario under study and the FOMs (Figures of Merit) involved in the acceptance criteria.
3. Identification and ranking of relevant physical phenomena based on the safety criteria.
4. Selection of the appropriate TH (Thermal Hydraulic) parameters to represent those phenomena.
5. Identification of relevant safety-related systems involved in the accident scenario.
6. Selection of relevant components/trains of the above redundant safety systems that are responsible for performing the intended safety function to mitigate accident consequences.
7. Development of the TH computer model of the accident scenario, e.g. develop an input for TRACE code [17].
8. Association of PDF (Probability Density Functions) for each selected TH parameter.
9. Identification of relevant, i.e. most probable, system configurations based on the availability of safety components/trains and association of a probability of occurrence for each configuration.
10. Random sampling of the selected TH parameters and plant configurations. Sample size (N) will depend on the particular statistical method and the acceptance criterion adopted to verify compliance of safety criteria. Perform N computer runs to obtain FOMs for each run.
11. Processing the results of the multiple computer runs (N) to estimate either the probability distribution of the FOMs, or rather some descriptor of this distribution, such as for example a percentile of the FOM, or a tolerance level of each FOM with STL using OS, e.g. the FOS.
12. Verify compliance of acceptance criterion for each FOM