Reliability Engineering and System Safety 145 (2016) 9–18

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis

Francesco Di Maio [a,*], Ajit Rai [b], Enrico Zio [a,c]

[a] Energy Department, Politecnico di Milano, Via La Masa 34, 20156 Milano, Italy
[b] Grenoble Institute of Technology- PHELMA, Grenoble, France
[c] Chair on System Science and Energetic Challenge, Fondation EDF, Ecole Centrale and Supelec, Paris, France

ARTICLE INFO

Article history:
Received 7 January 2015
Received in revised form
27 July 2015
Accepted 28 August 2015
Available online 8 September 2015

Keywords:
Risk-Informed Safety Margins
Dynamic probabilistic safety margins
Order Statistics
Grace time

ABSTRACT

The challenge of Risk-Informed Safety Margin Characterization (RISMC) is to develop a methodology for estimating system safety margins in the presence of stochastic and epistemic uncertainties affecting the system dynamic behavior. This is useful to support decision-making for licensing purposes. In the present work, safety margin uncertainties are handled by Order Statistics (OS) (with both Bracketing and Coverage approaches) to jointly estimate percentiles of the distributions of the safety parameter and of the time required for it to reach these percentiles values during its dynamic evolution.

The novelty of the proposed approach consists in the integration of dynamic aspects (i.e., timing of events) into the definition of a dynamic safety margin for a probabilistic Quantification of Margin and Uncertainties (QMU).

The system here considered for demonstration purposes is the Lead–Bismuth Eutectic- eXperimental Accelerator Driven System (LBE-XADS).

1. Introduction

Risk assessment and safety analysis are traditionally supported by a Deterministic Safety Analysis (DSA) of a limited set of Design Basis Accidents (DBAs) under largely conservative assumptions [27]. For this, IAEA defines four possible options that combine differently computer codes availability, realism of assumptions and boundary conditions [17]. Among these options, traditional DSA using Best Estimate (BE) Thermal-Hydraulic (TH) codes based on conservative (pessimistic) assumptions on the system dynamics and physical models (i.e., IAEA option 3) is limited in the consideration of system failure modes and sequences, timing and order of failure events.

Probabilistic Safety Assessment (PSA) overcomes the limitation of considering only DBAs by extending the set of accidents through a systematic analysis of the failure events and sequences (e.g., by Event Trees (ETs)/Fault Trees (FTs)). Yet, PSA does not give full account to the timing of failure events and to the magnitude of component failures, which can be important especially when the system dynamics significantly influences the system failure behavior [31].

Dynamic reliability approaches [33,9,20,19,14,10,2] have been developed, aimed at giving explicit account to the interactions among the physical parameters of the process (such as temperature, pressure, speed, etc.), the human operators actions and the failures of the hardware and software components. This creates the opportunity of DSA and PSA integration into one framework of Integrated Deterministic and Probabilistic Safety Analysis (IDPSA) [2,45] and as a by-product for the quantification of operational safety margins within a dynamic reliability scheme [44].

Traditionally, a safety margin is defined as the minimum distance between the system "loading" and its "capacity" [34]. The challenge is the effective representation of the uncertainties inherent in the TH code parameters, correlations and approximations.

Uncertainty is typically distinguished into two types: randomness due to inherent variability in the system behavior and imprecision due to lack of knowledge and information on the system [5]. The former type of uncertainty is often referred to as objective, aleatory, stochastic, whereas the latter is often referred to as subjective, epistemic, state of knowledge [5,16]. To deal with these uncertainties, traditional safety margins quantification in DSA analysis has implied conservatism in both the analysis of the TH code outputs and the evaluation criteria [28]. Best Estimate (BE) methodologies have reduced the amount of conservatism for the evaluation of safety margins, but do not take into account all

* Corresponding author.
E-mail address: francesco.dimaio@polimi.it (F. Di Maio).

http://dx.doi.org/10.1016/j.ress.2015.08.016
0951-8320/

Notation And List Of Acronyms

BDBA	Beyond Design Basis Accident
BE	Best Estimate
DBA	Design Basis Accident
DET	Dynamic Event Tree
DSA	Deterministic Safety Analysis
DSM	Dynamic probabilistic safety margin
ECCS	Emergency Core Cooling System
ET	Event Tree
FT	Fault Tree
IDPSA	Integrated Deterministic and Probabilistic Safety Assessment
LBE-XADS	Lead Bismuth Eutectic- eXperimental Accelerator Driven System
LOCA	Loss of Coolant Accident
MC	Monte Carlo
NPP	Nuclear Power Plant
OS	Order Statistics
PCT	Peak Cladding Temperature
PID	Proportional- Integral-Derivative controller
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
QMU	Quantification of Margin and Uncertainties
RISMC	Risk Informed Safety Margin Characterization
TH	Thermal Hydraulic
U	Upper Safety Threshold
L	Lower Safety Threshold
$T_{o,max}$	Maximum Temperature of Diathermic Oil
$P(t)$	Thermal power
$Q(t)$	Proton Beam
$\tau_{LB}^{C,P}$	Temperature of LBE liquid leaving from the top of the core of the LBE XADS
$\tau_{LB}^{P,C}$	Temperature of LBE liquid re-entering the core from the bottom of the LBE XADS
$T_{LB}^{av,C}$	Average in-core temperature of LBE liquid
$\Gamma_a(t)$	Airflow
$T_o^{av,S}$	Average temperature of diathermic oil
$T_o^{th,u}$	Upper safety threshold of LBE XADS diathermic oil temperature
$T_o^{th,l}$	Lower safety threshold of LBE XADS diathermic oil temperature
m_1	Flow rate of air when PID controller fails stuck
m_2	Airflow mass flow when air coolers fail stuck
m_3	Flow rate of air when feedforward controller fails stuck
Ta_{in}	Air inlet temperature from air cooler
$\bar{x}$	Input values vector
x_m	mth element of the input vector
$\bar{x}^{(i)}$	ith element of the representative sample of independent input vectors
J	Number of safety parameters
j	Index of the safety parameter
y	Set of values of first output vector (e.g., safety parameter)
$y_j(a)$	j-th safety parameter for accidental scenario a
y_{jref}	Reference value for $y_j(a)$
$M(y_j,a)$	Safety margin for the j-th safety parameter during accidental scenario a
$M(\gamma,\beta)$	Probabilistic safety margin
$M(\gamma_1,\gamma_2,\beta_1,\beta_2)$	Dynamic probabilistic safety margin
y	Set of values of first output vector (e.g., safety parameter)
y_t	Set of values of second output vector (e.g., time)
$\bar{y}$	Safety parameter output vector
$\bar{y}^*$	Ordered set of the safety parameter output vector
$\bar{y}_t$	Time output vector
$\bar{y}_t^*$	Ordered set of the time output vector
$f(y)$	Probability density function of y
$f(y_\gamma)$	Probability density function of the γ-th percentile of y
k	Number of outputs
N	Number of simulations
β	Confidence value
β_1	Confidence value of the safety parameter (e.g., 95%)
β_2	Confidence value of the time (e.g., 95%)
γ	Coverage value
γ_1	Coverage value of the safety parameter (e.g., 95th percentile)
γ_2	Coverage value of the time (e.g., 5th percentile)
m	Number of values that lie beyond the γ coverage extent
y_γ	Real γth percentile
$\hat{y}_{\gamma 1}$	Estimated γth percentile of the safety parameter
$\hat{y}_{t\,\gamma 2}$	Estimated γth percentile of the time
y_{γ_1}	Real value of the γth percentile of the safety parameter
$y_{t_{\gamma_2}}$	Real value of the γth percentile of the time
y_{95}	Real 95th percentile
$\hat{y}_{95}$	Estimate of the 95th percentile

aleatory and epistemic uncertainties in the physical models stochastic behavior and model parameter values [11,34].

In order to more realistically quantify the uncertainty of TH code outcomes, a probabilistic safety margin definition has been proposed for PSA, which better deals with epistemic uncertainties [43]. However, the effect of timing, order and magnitude of the component failures on the system dynamics is not considered.

In this respect, a Dynamic probabilistic safety margin (DSM) approach is proposed in this paper, based on time-dependent phenomenological models of stochastic system evolution including possible dependencies between failure events [2]. For this, we introduce a novel definition of a DSM by the combined quantification of a percentile (e.g., 95th) of the safety parameter distribution (e.g., oil temperature, peak cladding temperature) and a percentile (e.g., 5th) of the distribution of the earliest time required to the safety parameter to reach the given percentile value. The uncertainties affecting the DSM are treated using Order Statistics (OS) (i.e., Bracketing and Coverage approach) [28]. By doing so, we are able to compute the confidence that, for a selected accidental scenario of a Dynamic Event Tree (DET) obtained by a IDPSA analysis, the estimated 95th percentile of the safety parameter cannot be reached before the 5th percentile of the estimated time: if these estimated percentiles meet the safety criteria with the required confidence, the NPP can be licensed as "safe" to withstand the selected accidental scenario.

The rationale behind the choice of the selection of the 95th and the 5th percentiles for the safety parameter and the estimated time, respectively, lies in the attempt of assuring that there is no significant evidence of exceedance of the safety parameter threshold which could lead to a higher than accepted probability of failure within an extremely unavoidable (fast) time (i.e., the unlikely condition that the safety parameter reaches the threshold within the 5th percentile value of the time distribution). With these assumptions, the proposed definition of DSM provides the analyst with the additional resilience information on the available time for counteracting the occurrence of an accidental scenario,