Reliability Engineering and System Safety 147 (2016) 170–193

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Application of the Integrated Safety Assessment methodology to safety margins. Dynamic Event Trees, Damage Domains and Risk Assessment

L. Ibánez [a], J. Hortal [b], C. Queral [a], J. Gómez-Magán [c,*], M. Sánchez-Perea [b], I. Fernández [c], E. Meléndez [b], A. Expósito [a], J.M. Izquierdo [b], J. Gil [c], H. Marrao [c], E. Villalba-Jabonero [a]

[a] Universidad Politécnica de Madrid, Alenza, 4, Madrid, Spain
[b] Consejo Seguridad Nuclear, Pedro Justo Dorado Dellmans, 11, Madrid, Spain
[c] NFQ Solutions, Claudio Coello, 78, Madrid, Spain

A R T I C L E I N F O

Available online 31 May 2015

Keywords:
Damage Domain
Dynamic Event Tree
Integrated Safety Assessment
Damage Exceedance Frequency
Probabilistic Safety Analysis

A B S T R A C T

The Integrated Safety Assessment (ISA) methodology, developed by the Consejo de Seguridad Nuclear, has been applied to an analysis of Zion NPP for sequences with Loss of the Component Cooling Water System (CCWS).

The ISA methodology proposal starts from the unfolding of the Dynamic Event Tree (DET). Results from this first step allow assessing the sequence delineation of standard Probabilistic Safety Analysis results.

For some sequences of interest of the outlined DET, ISA then identifies the Damage Domain (DD). This is the region of uncertain times and/or parameters where a safety limit is exceeded, which indicates the occurrence of certain damage situation. This paper illustrates application of this concept obtained simulating sequences with MAAP and with TRACE.

From information of simulation results of sequence transients belonging to the DD and the time-density probability distributions of the manual actions and of occurrence of stochastic phenomena, ISA integrates the dynamic reliability equations proposed to obtain the sequence contribution to the global Damage Exceedance Frequency (DEF).

Reported results show a slight increase in the DEF for sequences investigated following a power uprate from 100% to 110%. This demonstrates the potential use of the method to help in the assessment of design modifications.

List of acronyms

- **ADS-IDAC**, Accident Dynamics Simulator-Information, Decision and Action in a Crew context cognitive model
- **AFW**, Auxiliary Feed Water
- **AOP**, Abnormal Operating Procedure
- **CF**, Containment Fan coolers
- **CS**, Containment Spray
- **CR**, Containment spray Recirculation
- **CCWS**, Component Cooling Water System
- **CCW/SW**, Component Cooling Water / Service Water
- **CSNI**, Committee on the Safety of Nuclear Installations
- **DD**, Damage Domain
- **DDET**, Discrete Dynamic Event Tree
- **DEF**, Damage Exceedance Frequency
- **DET**, Dynamic Event Tree
- **DH**, Deterministic Header
- **DM**, Dynamic MAAP sequences
- **DPI**, Differences PSA-ISA
- **DSA**, Deterministic Safety Analysis
- **DT**, Dynamic TRACE sequences
- **ECCS**, Emergency Core Coolant System
- **EOP**, Emergency Operating Procedure
- **ES**, End State
- **ET**, Event Tree
- **FB**, Feed and Bleed
- **GA**, Genetic Algorithm
- **GET**, Generic Event Tree
- **GRS**, Gesellschaft für Anlagen- und Reaktorsicherheit
- **GETU**, Generic Event Tree with Uncertainty
- **HPSI**, High Pressure Safety Injection
- **IAEA**, Internacional Atomic Energy Agency
- **IDPSA**, Integrated Deterministic-Probabilistic Safety Assessment
- **INL**, Idaho National Laboratory

* Corresponding author.
E-mail addresses: fjhr@csn.es (J. Hortal), cesar.queral@upm.es (C. Queral), javier.magan@nfq.es (J. Gómez-Magán), ema@csn.es (E. Meléndez), jesus.gil@nfq.es (J. Gil).

http://dx.doi.org/10.1016/j.ress.2015.05.016
0951-8320/

- **ISA**, Integrated Safety Assessment
- **JRC**, Joint Research Centre
- **LCCWS**, Loss of Component Cooling Water System
- **LOCA**, Loss of Coolant Accident
- **LPSI**, Low Pressure Safety Injection
- **MBLOCA**, Medium Break Loss of Coolant Accident
- **MCDET**, Monte Carlo Dynamic Event Tree
- **MIT**, Massachusetts Institute of Technology
- **NEA**, Nuclear Energy Agency
- **NRC**, Nuclear Regulatory Commission
- **NPP**, Nuclear Power Plant
- **NDH**, Non Deterministic Header
- **OSU**, Ohio State University
- **PCT**, Peak Cladding Temperature
- **PDF**, Probability Density Function
- **PSA**, Probabilistic Safety Assessment
- **PSI**, Paul Scherrer Institute
- **RCP**, Reactor Coolant Pump
- **RCS**, Reactor Coolant System
- **SBO**, Station Black Out
- **SBLOCA**, Small Break Loss of Coolant Accident
- **SCAIS**, Simulation Codes system for ISA
- **SIMPROC**, Procedures Simulator
- **SLOCA**, Seal Loss of Coolant Accident
- **SMAP**, Safety Margin Action Plan
- **SM2A**, Safety Margin Assessment Application
- **TSD**, Theory of Stimulated Dynamics

1. Introduction

The process of Safety Margin Assessment, as proposed in the Safety Margin Action Plan (SMAP) framework [39], is based on the identification of the Risk Space and the extensive application of uncertainty analysis methods aiming at obtaining an estimation of the exceedance frequency of specified safety limits, Damage Exceedance Frequencies (DEF). The Risk Space can be understood as an extension of both the Probabilistic Safety Assessment (PSA) event trees and the design scenarios intending to include every possible malfunction susceptible to challenge any safety limit of interest.

The Safety Margin Assessment Application (SM2A) expert group was created by the Committee on the Safety on Nuclear Installations (CSNI) with the specific mandate to explore the practicability of the SMAP framework. To this purpose, the Task Group on SM2A carried out a pilot application project, completed late in 2010, see [40], aiming at computing the increase in Damage Exceedance Frequency resulting from a 10% power uprate at Zion NPP (PWR-4 loop Westinghouse design). Each participant analyzed a particular event tree according to the PSA of the plant (see [68] and Table 1 for more details).

The participation of CSN in SM2A project included a sound collaboration of CSN with Universidad Politécnica de Madrid (UPM) and NFQ Solutions, to perform an analysis of sequences of Loss of Component Cooling Water System (LCCWS) applying the Integrated Safety Assessment methodology (ISA). This methodology aims at computing the contribution to DEF from the sequences stemming from one or more initiating events. For this purpose ISA carries out an automatic delineation of Dynamic Event Trees (DET), and allows accounting of the uncertainties of the sequences. These uncertainties include time variability (as in, e.g., human actions or stochastic phenomena) and parameter values (break area, thermal power, pressures, mass flows, etc.). The method, developed by the Modeling and Simulation (MOSI) branch of the Spanish Nuclear

Table 1
Initiating events and codes used by each SM2A participant.

Initiating event	Organization	Thermohydraulic code
LLOCA	EDF	CATHARE/TRACE
MLOCA	PSI	TRACE
SLOCA	PSI	TRACE
LOSP	CNSNS	CATHARE
MSLB	STUK	ATHLET
SGTR	KAERI/KINS	MARS
TT	JNES	RELAP5
LOFW	NRC	TRACE
LCCWS	CSN	MAAP/TRACE

Regulatory Body, entails several simulations of DET sequences in the application presented in this paper.

This paper describes the ISA method as well as its related software tool, SCAIS (Simulation Code system for ISA, see [24]) designed and developed in a tight collaboration between CSN, UPM and NFQ Solutions (Section 2). Particular emphasis is made in describing the added value provided by this type of dynamic reliability method. The paper covers successive steps required in ISA application: analysis of human actions in CCWS sequences (Section 3), identification of headers considered in the Loss of CCWS analysis (Section 4), Dynamic Event Tree generation (Sections 5 and 6), identification of sequences with Damage Domain (Section 7), obtaining Damage Domains using MAAP, see [13], and using TRACE, see [41] (Sections 7.2 and 7.3); the last step of ISA methodology, computation of Damage Exceedance Frequency, is described in Section 8. Finally, Section 9 outlines main conclusions of this work.

2. Materials and methods

This section describes the SM2A exercise hypotheses (Section 2.1), a brief overview of ISA methodology (Section 2.2), the details on the SCAIS tool used for simulating (Section 2.3) and a comparison of ISA with other IDPSA methodologies (Section 2.4).

2.1. SM2A exercise hypotheses and approximations

The results of the calculations described in this paper are conditioned by the particular choices and approximations used in the input data. In many cases, these choices and approximations were necessarily poor due to lack of availability of detailed data and information. However, it must be pointed out that the methodology is perfectly able to use more detailed modeling approaches and data when adequate sources of information are available.

The capability to use data of different levels of quality and detail can be considered a value of the methodology but the results that can be obtained from its application are obviously conditioned by the quality of data. The conclusions outlined in this paper are referring to the applicability and the type of results that can be obtained from the methodology, not to the feasibility of the power uprate in the analyzed plant.

The following hypotheses and approximations were included in SM2A exercise:

- The strong time constraints imposed on SM2A expert group made to decide to limit the analysis to the evaluation of a single safety variable, PCT.
- As the available information about fault tree models on the PSA for Zion NPP was very limited ([56] contains only final values of conditional values of each event tree header), the analysis was done at PSA sequence level in many cases, without exploring all the possible configurations of safety systems. In some instances