Reliability Engineering and System Safety 145 (2016) 250–261

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Probabilistic Safety Assessment of twin-unit nuclear sites: Methodological elements

Tu Duong Le Duy*, Dominique Vasseur, Emmanuel Serdet

Industrial Risk Management Department Electricity of France, Lab Clamart, France

ARTICLE INFO

Article history:
Received 13 March 2015
Received in revised form
8 June 2015
Accepted 6 July 2015
Available online 21 July 2015

Keywords:
PSA
Multi-unit
Inter unit common cause failures

ABSTRACT

When assessing the risk related to Nuclear Power Plants in terms of impacts on the population health and on the environment, multi units issues should be taken into account. Generally speaking, to date mainly models relating to a single unit have been developed by operators. The purpose of this paper is to present possible solutions or methodological options, suggested by EDF (Electricity of France) R&D, in order to switch from a risk assessment for the unit to a risk assessment for the site. The case of a site with two units is addressed here. A review of practices and standards showed that the specific aim of a PSA at site level was to deal with the dependencies existing between the units on that site. The risk calculation for the site is therefore proposed for six configurations resulting from the combination of two types of scenarios and three types of systems which are defined. The treatment of CCF events and the adaption of the assessment of the Human Errors Probabilities to the case of multiple units are also addressed in this paper. The proposed approach is illustrated using a simplified case inspired by the EDF 900 MWe units level 1 PSA model.

1. Introduction

1.1. State-of-the-art

Most nuclear generation sites worldwide have more than one reactor in operation. This should be taken into account when assessing the risk related to these installations, in particular, when assessing the consequences in terms of impacts on the health of the population and on the environment.

However, by the early 2000s, K. Fleming identified the deficiencies of existing PSAs regarding consideration of multiunit aspects [1,2]:

- Multi-unit initiating events are often not modelled and hence shared systems are fully credited for one unit without considering the case they might be needed by other units and ignoring dependencies between systems and human resources shared at the site level.
- Cross connection and mutual backup are credited without considering the possible problems arising from these systems (e.g. propagation of an initiating event from one unit to another one) and their potential dependencies (Common Cause Failures).

This situation had not changed a lot until 2011 and, for example, the NRC made the following observation: “Because the Commission's safety goals, QHOs, and subsidiary numerical objectives are applied on a per reactor basis, most PRAs developed to date do not explicitly consider multi-unit accidents in which initiating events lead to reactor core damage in multiple units at the same site. Current PRA models therefore do not generally identify and address dependencies between systems at multi-unit sites, particularly those with highly interdependent support systems involving systems and subsystems that are shared by multiple units. To understand the contribution of these multi-unit effects to the risk associated with a NPP, PRA models need to be enhanced to include both initiating events that might simultaneously impact multiple units and equipment and human action dependencies in responding to multi-unit accidents”.

However PSA standard documents include multiunit aspects and rules in the form of high-level requirements. The requirements or good practices contained in the documents [3,4,5,6,7,8] are summarised below:

1.1.1. Initiating events

We must identify and model the initiating events that could impact several units of a site at once. These events are related to dependency factors:

- An event occurring on one unit can have an impact on another unit because of their physical proximity.

* Corresponding author. Tél.: +33147655817; fax: +33147655797.
E-mail address: tu-duong.le-duy@edf.fr (T.D. Le Duy).

http://dx.doi.org/10.1016/j.ress.2015.07.014
0951-8320/

Nomenclature

CCF	common Cause Failure
CDF	Core damage frequency
CVCS	Chemical and Volume Control System
EDG	Emergency Diesel Generator
HEP	Human Error Probability
HF	Human Factor
SCDF	Site core damage frequency
RAW	Risk Achievement Worth
FV	Fussell–Vesely
IE	Initiating Event
LPSD	Low Power and Shutdown mode
LOOP	Loss of offsite power
LUHS	Loss of Ultimate Heat Sink
QHO	Quantitative Health Objectives
PSA	Probabilistic Safety Assessment
PRA	Probabilistic Risk Assessment
MCS	Minimal Cut Set
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
SI	Identical Systems
SB	Systems with unit cross ties
SP	Shared system
$P(meltdown_A)$	core meltdown risk on unit A
$P(meltdown_B)$	core meltdown risk on unit B
$P(meltdown_{site})$	core meltdown on the site
$P(meltdown_A \cup meltdown_B)$	core meltdown risk on unit A or unit B
$P(meltdown_A \cap meltdown_B)$	"Simultaneous" core meltdown risk on both units A and B

Example: Impact on unit B resulting from missiles due to the destruction of unit A turbine.

- An event occurring in a common building or in a building unit A connected (tunnel, cable tray, etc.) to unit B building can generate an initiating event on both units.
  Example: propagation of a fire scenario from one unit to the other one.
- An external event, typically extreme weather or earthquake, can lead to a multiunit initiating event.

Example: LOOP (Loss of offsite power) or LUHS (Loss of Ultimate Heat Sink) for all units of a site.

1.1.2. Sequence analysis

The number of units involved in accident scenarios must be taken into account in order to accurately assess the consequences in terms of potential releases. It is quite obvious for a twin unit site but may be more difficult for a larger number of units on a site.

1.1.3. Success criteria

For a system that is shared between several units, it is important to know the way this sharing is done (priority).

It is important to take account of the reactor modes for the different units involved in a multi-unit event. Actually, the technical specifications for a given system may be different in different modes and it may have consequences on the definition of success criteria for this system.

1.1.4. System analysis

The potential for inter unit common cause failures (CCF) must be studied for systems that are identical in the different units. As an example, the document [9] shows the impact of such CCF events on the site LOOP frequency assessment.

1.1.5. Human factor

On the one hand, the units on a same site can benefit from shared systems (emergency power source, etc.) and on the other hand, problems on a specific unit can mobilise the resources from another one.

When sharing of equipment or cross connexions are credited, operator actions must be carefully assessed (existing procedure, feasibility of the action given the initiator, etc.)

If there are possible actions, their probability of success must be adapted. Their success is a priori less likely in case of multi-unit event, in situations where such actions are required on several units simultaneously. It is therefore necessary to clearly identify these situations and to be able to assess their frequency.

1.1.6. Data

For the analysis of a given unit, it is important to take into account the different modes in which may be the other units. In particular, the possible ongoing maintenance on shared systems must be considered in the evaluation of unavailability data.

1.1.7. Quantification

There is no specific requirement in standards regarding multi-unit aspects for quantification. However, there is a general requirement that applies all the same in this case: correct the minimal cutsets that contain mutually exclusive events. The application of this requirement applies indeed to combinations of events that concern maintenance situations or connexions prohibited on systems shared by multiple units.

The Fukushima accident presented to the forefront the issue of risk assessment for a multi-unit site and restart the works on this subject.

A classification recently proposed in [10] attempts to explore the wide breadth of potential dependencies that occur at multi-unit sites. Moreover, this study made a quick survey and identified existing PRA methods that could potentially be used, with or without expansion, to account for multi-unit dependencies. The paper [11] proposes the principles of an approach to build a site PRA model taking into account single and multiunit initiating events. The approach identifies and counts all possible accident scenarios and proposes a formula to quantify the site core damage frequency (SCDF) that is the frequency of at least single core damage per site per year.

Inspired by previous works, the present paper focuses mainly on a twin-unit site and proposes a *practical* approach that attempts to fulfill the requirements of the existing standards to assess the CDF at unit or site level based on an updated single unit PSA. Only the level 1 PSA model is covered in this paper.

1.2. Presentation of the problem

The specificity of a site PSA is to deal with the dependencies existing between the units on the site. These dependencies may come from various sources:

- Units are on the same site and are therefore subject to the same environmental constraints, in particular in terms of external hazards.
- Systems may exist that are "shared" by both units. These common systems may be of three types:
- Identical systems present on each unit but dedicated to one unit.
- Systems that are shared on a site level.