



Ricerca di Sistema elettrico

Rapporto tecnico sulle metodologie di analisi degli eventi esterni e sulla stima del rischio

*L. Burgazzi, A. Cervone, N. Davidovich, P. Meloni, G. Forasassi,
R. Lo Frano, G. Pugliese*



RAPPORTO TECNICO SULLE METODOLOGIE DI ANALISI DEGLI EVENTI ESTERNI E SULLA STIMA DEL RISCHIO

L. Burgazzi, A. Cervone, N. Davidovich, P. Meloni (ENEA), G. Forasassi, R. Lo Frano, G. Pugliese (UNIFI)

Settembre 2013

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dello Sviluppo Economico - ENEA

Piano Annuale di Realizzazione 2012

Area: Produzione di energia elettrica e protezione dell'ambiente

Progetto: Sviluppo competenze scientifiche nel campo della sicurezza nucleare e collaborazione ai programmi internazionali per il nucleare di IV Generazione

Obiettivo: Sviluppo competenze scientifiche nel campo della sicurezza nucleare

Responsabile del Progetto: Felice De Rosa, ENEA

Il presente documento descrive le attività di ricerca svolte all'interno dell'Accordo di collaborazione "Sviluppo competenze scientifiche nel campo della sicurezza nucleare e collaborazione ai programmi internazionali per il nucleare di IV generazione"

Responsabile scientifico ENEA: Felice De Rosa.

Responsabile scientifico CIRTEN: Giuseppe Forasassi

Titolo

Rapporto tecnico sulle metodologie di analisi degli eventi esterni e sulla stima del rischio

Descrittori

Tipologia del documento: Rapporto Tecnico

Collocazione contrattuale: Accordo di programma ENEA-MSE: Piano Annuale di Realizzazione 2012, Linea Progettuale 1, Obiettivo B: Metodologie avanzate per la valutazione delle conseguenze incidentali, Task B.2

Argomenti trattati: Sicurezza nucleare
Analisi incidentale
Analisi di sicurezza probabilistica

Sommario

Il presente documento riporta le attività svolte nell'ambito della Linea Progettuale 1 (LP1), obiettivo B (Metodologie avanzate per la valutazione delle conseguenze incidentali), task B.2, del PAR 2012, ADP ENEA-MSE.

Lo studio presenta una metodologia del tipo "risk-informed" per la analisi di rischio di impianti nucleari a fronte di eventi esterni, così come emerge dall'incidente di Fukushima. L'approccio proposto integra gli aspetti probabilistici con quelli deterministici per perfezionare gli strumenti attualmente in uso ai fini dell'analisi di sicurezza.

Un' applicazione pilota, in termini di definizione di sequenza dell'incidente e relativa valutazione è indicativamente proposta come significativo caso di studio. In particolare, gli incidenti di perdita di alimentazione elettrica alla centrale (o "Stazione Black-Out") causati da eventi esterni, come tifoni e tornado, vengono analizzati sia dal punto di vista deterministico che da quello probabilistico.

Note:


Questo documento è stato preparato col contributo congiunto del seguente personale di ricerca ENEA e CIRTEC:

- L. Burgazzi, A. Cervone, N. Davidovich, P. Meloni (ENEA)
 - G. Forasassi, R. Lo Frano, G. Pugliese (Università di Pisa)
- Sigla doc. rif.: CIRTEC-Università di Pisa: CERSE-UNIFI RL 1526-2013

2			NOME			
			FIRMA			
1			NOME			
			FIRMA			
0	EMISSIONE	05/09/13	NOME	L. Burgazzi	F. De Rosa	F. De Rosa
			FIRMA			
REV.	DESCRIZIONE	DATA		REDAZIONE	CONVALIDA	APPROVAZIONE

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. di 2 52
--	--	------------------	----------------------	------------------------

Sommario

L'incidente di Fukushima in Giappone nel 2011 ha evidenziato diverse lacune legate all' utilizzo dell'approccio probabilistico per la valutazione del rischio degli impianti nucleari (PSA, Probabilistic Safety Assessment). Ciò ha richiesto la riconsiderazione e/o il perfezionamento nella applicazione della metodologia probabilistica relativamente alle nuove problematiche emerse a fronte di determinati eventi incidentali: questi includono, per esempio, l'analisi di rischio per eventi esterni.

Un approccio cosiddetto "risk-informed" implica l'integrazione dell'analisi di rischio con le informazioni di tipo deterministico ai fini della valutazione della sicurezza dell'impianto. In questa prospettiva, si presume che l'utilizzo di tecniche di valutazione di rischio possa portare ad un miglioramento della sicurezza dell'impianto ed una più razionale assegnazione delle limitate risorse disponibili.

In questo ambito, l'approccio IDPSA (Integrated Deterministic Probabilistic Safety Analysis), cioè l'analisi integrata di sicurezza deterministica-probabilistica, qui descritto, promuove l'utilizzo combinato della analisi probabilistica della sicurezza, PSA, e dell'analisi deterministica, DSA (Deterministic Safety Assessment).

Il presente studio ha come obiettivo lo sviluppo di una strategia per la realizzazione di nuovi approcci che fondano considerazioni sia deterministiche che probabilistiche per completare gli strumenti attualmente in uso ai fini dell'analisi di sicurezza.

Per esempio il concetto di "Dynamic PSA" (DPSA) è stato proposto al fine di individuare importanti scenari incidentali sconosciuti o inutili conservatorismi.

Le problematiche relative alla connessione tra PSA e DSA sono affrontate; un'applicazione pilota, in termini di definizione di sequenza dell'incidente e relativa valutazione è indicativamente proposta come significativo caso di studio, come fase iniziale per l'implementazione di una metodologia appropriata per affrontare una delle principali questioni, così come emerge dall'incidente di Fukushima, cioè la valutazione dell'evento esterno.

In particolare, gli incidenti di perdita di alimentazione elettrica alla centrale (Stazione BlackOut) causati da eventi esterni come tifoni e tornado, vengono analizzati sia dal punto di vista deterministico che da quello probabilistico.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. di 3 52
--	--	------------------	----------------------	------------------------

Table of contents

Executive Summary

List of acronyms

1. Introduction

2. Deterministic approach

3. Probabilistic Safety Assessment

3.1 Concept of risk

3.2 Methods for Probabilistic Safety Assessment

3.3 Risk criteria

3.4 Risk-informed Decision making

4. Risk-informed regulatory approach

5. IDPSA Integrated Deterministic-Probabilistic Safety Assessment

5.1 Motivation, background and concepts

5.2 State of the art

6. Case Study

7. Probabilistic safety analysis

7.1 Accident sequence modeling

7.2 Generic event tree modeling

8. Deterministic safety analysis

8.1 General considerations

8.2 Deterministic safety assessment: SMA evaluation

8.3 Collection of data: support global response of plant

8.3.1 Input data

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. di 4 52
--	--	------------------	----------------------	------------------------

8.3.2 Design basis event condition

8.3.3 Geotechnical data

8.3.4 Data on building structures

8.3.5 Data on SSCs, piping and equipment

9. Safety evaluation of a NPP subjected to tsunami event: Analysis step by step

10. Conclusions

References

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 5	di 52
--	--	------------------	----------------------	------------------	-----------------

Executive summary

The Fukushima accident of Japan in 2011 has revealed various gaps related to the current PSA (Probabilistic Safety Assessment) approach usage for plant risk assessment. This makes some issues to be re-considered and/or improved in the PSA application and state of practice: these include, for instance, PSA for external events.

A risk-informed regulatory approach implies that risk insights be used as supplement of deterministic information for safety decision-making purposes. In this view, the use of risk assessment techniques is expected to lead to improved safety and a more rational allocation of the limited resources available.

The IDPSA (Integrated Deterministic Probabilistic Safety Analysis) approach, here described, promotes the use of the combination of PSA (Probabilistic Safety Assessment) and DSA (Deterministic Safety Assessment) on the merit of improved safety, within a risk-informed framework.

The present study aims at the development of a strategy for the implementation of new approaches that merge both deterministic and probabilistic considerations into practice of safety analysis to complement currently used tools. For instance the concept of “dynamic PSA” (DPSA) has been proposed in order to identify unknown important scenarios (weaknesses) or unnecessary conservatism.

The issues related to the connection between PSA and DSA are addressed, a pilot application, in the form of accident sequence definition and assessment is tentatively proposed as significant case study, as initial stage for the implementation of an appropriate methodology to address one of the main issues as emerging from the Fukushima accident, such as the external event assessment. In particular the LOOP/SBO (Loss Of Offsite Power/Station BlackOut) caused by external event as typhoon and tornado, is analyzed both on the deterministic perspective and on the probabilistic standpoint.

List of Acronyms

AC	Alternating Current
ADS	Accident Dynamic Simulation Methodology
AFW	Auxiliary Feed Water
ATWS	Advanced Transient Without Scram
BWR	Boiling Water Reactor
CET	Continuous Event Tree methodology
CETL	Containment Event Tree Language (developed for STUK's level 2 PSA code SPSA)
CCMT	Cell-to-Cell Mapping Technique
CCCMT	Continuous Cell-to-Cell Mapping Technique
CSN	Consejo de Seguridad Nuclear
DC	Direct Current
DDP	Diesel Driven Pump
DET	Dynamic Event Tree
DETAM	Dynamic Event Tree Analysis Method
DFM	Dynamic Flowgraph Methodology
DID	Defence-in-depth
DI&C	Digital I&C
DPSA	Dynamic PSA
DSA	Deterministic safety analysis
DYLAM	Dynamic Logical Analytical Methodology
ECCS	Emergency core cooling systems
EOP	Emergency operating procedures
EPS	Emergency Power Systems
ESBWR	Economic Simplified Boiling Water Reactor
ET	Event tree
FT	Fault tree
GA	Genetic Algorithms
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
I&C	Instrumentation and control
IDPSA	Integrated Deterministic-Probabilistic Safety Analysis
ISA	Integrated safety analysis methodology
JRCI	Joint Research Centre – Ispra, Italy
JSI	Jožef Stefan Institute
KTH	Kungliga tekniska högskolan, Royal Institute of Technology, Stockholm
MIT	Massachusetts Institute of Technology, U.S.A.
LOCA	Loss of coolant accidents
LOOP	Loss of offsite power
LWR	Light water reactor
OSU	The Ohio State University
PORV	Power-Operated Relief Valve
PRA	Probabilistic risk analysis
PSA	Probabilistic safety assessment, Probabilistic safety analysis
PWR	Pressurized water reactor
SCAIS	Code system for integrated safety analysis

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. di 7 52
--	--	------------------	----------------------	------------------------

SBO	Station blackout
SMA	Safety Margin Assessment
SPSA	STUK PSA code
TDP	Turbine Driven Pump
ULB	Universite Libre de Bruxelles, Belgium
UM	University of Maryland, U.S.A

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. di 8 52
--	--	------------------	----------------------	------------------------

List of Figures

Figure 1- Probability consequence diagram	11
Figure 2 - Example of an event tree.....	13
Figure 3 - Example of a fault tree	14
Figure 4 - Generic PWR event tree for station blackout	28
Figure 5 - Generic BWR event tree for station blackout.....	29
Figure 6- Example of peak cladding temperature acceptance criteria based on deterministic evaluation [30]	33
Figure 7 - Severe tsunامي in the history	35
Figure 8- Tsunami waves impact at Fukushima Daiichi reactor.....	36
Figure 9 – Methodological approach for tsunami evaluation	40
Figure 10 - Tsunami phases.....	40
Figure 11 - Wave elevations vs. vertical building wall height [36].	41
Figure 12 - Scheme of typical BWR NPP	43
Figure 13 - Containment building FEM model view (a) and section (b).....	44
Figure 14 - Directions of the pressure breaking-wave.....	45
Figure 15 - Von Mises stress distribution for BFE=20 m.	46
Figure 16 - Overviews of the damages of the outer surface of containment building in the case of BFE=10 (a) and BFE=20 m (b).....	47

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 9	di 52
--	--	------------------	----------------------	------------------	-----------------

1. Introduction

IDPSA - Integrated Deterministic-Probabilistic Safety Assessment, is a family of methods to enable risk-informed decision-making. The starting point of the IDPSA framework is that safety justification must be based on the coupling of deterministic (consequences) and probabilistic (frequency) considerations to address the mutual interactions between:

- stochastic disturbances (e.g. failures of the equipment) and
- deterministic response of the plant (i.e. transients).

According to (ref.1) IDPSA is considered as a complementary approach to PSA (Probabilistic Safety Assessment) and DSA (Deterministic Safety Assessment) approaches intended to help in:

- Resolving time dependent interactions between physical phenomena, equipment failures, control logic, operator actions in analysis of complex scenarios;
- Identification and characterization of a-priori unknown vulnerable scenarios, or “sleeping threats”;
- Consistent treatment of different sources of uncertainties;
- Reduction of reliance on expert judgment and assumptions about interdependencies;
- Potential reduction of the cost of safety analysis due to larger involvement of computers in what they can do better: multi-parameter, combinatorial exploration of the plant scenarios space.

In order to illustrate these new possibilities provided by the frontiers in safety assessment process to PSA/DSA practitioners in utilities, vendors, regulators and research organizations, a foreword to recall main features of either methodologies is given, with greater emphasis on PSA, to achieve risk-informed decision-making approach, which will be extensively described in section 4.

The remainder of the report illustrates the IDPSA approach, pointing out the relative benefits as well as issues, an illustrative example is given and finally the path towards its implementation within a risk-informed framework is tracked.

2. Deterministic approach

This analytical procedure has been widely used throughout the world in the design of nuclear reactors for the purpose of generating electricity. It attempts to ensure that the various situations, and in particular accidents, that are considered to be plausible, have been taken into account, and that the monitoring systems and engineered safety and safeguard systems will be capable of ensuring the containment of radioactive materials. The deterministic approach is based on the two principles referred to as leak tight barriers between the radioactive source and the public and the concept of defense-in-depth (DID). The leak tight "barriers", of which there are generally three, consist of: the fuel cladding, the primary reactor coolant system, and the containment building. Defense-in-depth consists of taking into account potential equipment failures and human errors, so that suitable preventive measures may be applied, and of making provisions for the installation of successive devices to counter such failures

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 10	di 52
--	--	------------------	----------------------	-------------------	-----------------

and limit their consequences. It consists of several successive stages (or levels), hence the term "defense-in-depth":

- **Prevention and surveillance:** all necessary measures are taken to ensure that the plant is safe; items of equipment are designed with adequate safety margins and constructed in such a way that under normal operating conditions the risk of an accident occurring in the plant is kept to a minimum;
- **Protection:** it is assumed that operating incidents may occur; provisions are made to detect such incidents and to prevent them from escalating. This is achieved by designing safety systems that will restore the plant to a normal state and maintain it under safe conditions.
- **Safeguard:** it is assumed that severe accidents might occur that could have serious consequences for the public and the environment. Special safety systems are therefore designed to limit the consequences to an acceptable level.

3. Probabilistic Safety Assessment

3.1 Concept of risk

Nuclear facilities are designed so that the risks associated with their operation are within acceptable limits for both the public and the environment. There is no precise definition, however, of what constitutes an "acceptable risk"; it is basically a subjective notion. In its simplest form, risk denotes the level of uncertainty associated with an individual's given action. The acceptance of risk is generally governed by the degree to which it is considered to be relatively improbable and of limited consequence. In a nuclear facility, as in any industrial plant, risk assessment distinguishes between the potential hazards that might be encountered in the absence of any protective measures, and the residual risks that will still remain despite the measures taken. The problem lies in assessing the latter, since there is no way of ensuring that they have been completely eliminated.

The concept of event probability and its associated consequences was rapidly incorporated into safety analysis procedures, by taking account of the fact that the probability of an accident must be inversely proportional to the severity of the potential consequences for the public and the environment. This approach may be represented schematically in a probability/consequence diagram (known as a "Farmer curve"), which sets out acceptable and prohibited domains (Figure 1).

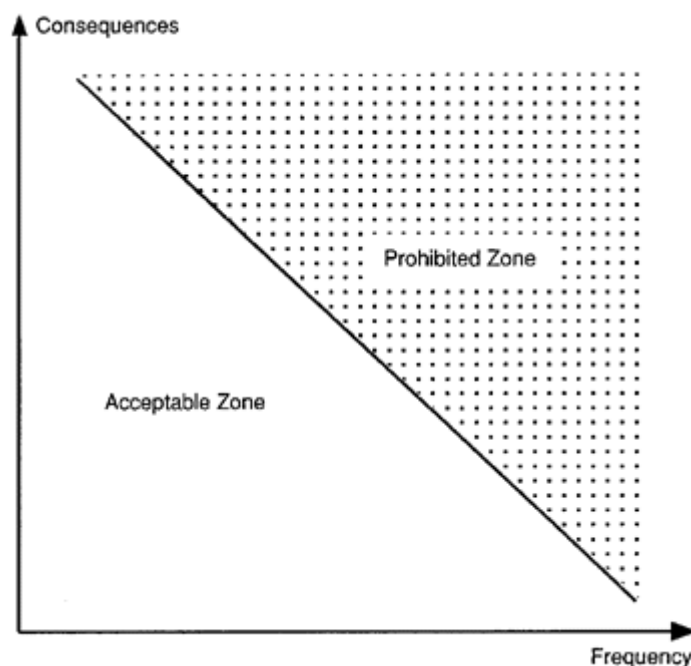


Figure 1- Probability consequence diagram

The question that the analyst asks himself when performing a risk assessment is which accident conditions should he take into consideration and to what level of probability should he pursue his analysis. As the use of probabilistic risk analysis became more widespread, the safety authorities asked design engineers to introduce appropriate measures whenever such analyses indicated that the probability of an event occurring that might potentially have unacceptable consequences for the public and the environment was sufficiently high.

3.2 Methods of Probabilistic Safety Assessment

PSA methodology widely used in the nuclear power industry is deemed helpful to the safety assessment of the facility and along the correspondent licensing process: probabilistic safety assessment can provide insights into safety and identify measures for informing designers of the safety of the plant.

The first comprehensive application of the PSA dates back to 1975, to the United States Nuclear Regulatory Commission's (U.S. NRC) Reactor Safety Study [4]. Since that pioneering study, there has been substantial methodological development, and PSA techniques have become a standard tool in the safety evaluation of the nuclear power plants (NPPs) and industrial installations in general. Due to historical reasons, the PSA sometimes is called PRA.

As the most important area of PSA projects remains nuclear power plants, mainly due to the specific features of the nuclear installations, three levels of PSA have evolved:

Level 1: The assessment of plant failures leading to core damage and the estimation of core damage frequency. A Level 1 PSA provides insights into design weaknesses and ways of preventing core damage. In the case of other industrial assessments, Level 1 PSA provides estimates of the accidents frequency and the main contributors.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 12	di 52
--	--	------------------	----------------------	-------------------	-----------------

Level 2: As possible releases are additionally protected by containment in most NPPs, PSA at this response and severe accident management possibilities. The results obtained in Level 1 are the basis for Level 2 quantification. In the case of other industrial assessments, Level 2 PSA might be fully covered by Level 1, as containment function is rather unique feature and is not common in other industries.

Level 3: The assessment of off-site consequences leading to estimates of risks to the public. Level 3 incorporates results on both previous levels.

Level 1 PSA is the most important level and creates the background for further risk assessment, therefore it will be presented in detail. The structure of the other levels is much more application specific, and will be discussed only in general.

The methodology is based on systematically: 1) postulating potential accident scenarios triggered by an initiating event (IE), 2) identifying the systems acting as “defences” against these scenarios, 3) decomposing the systems into components, associating the failure modes and relative probabilities, 4) assessing the frequency of the accident scenarios. Two elements of the PSA methodology typically stand out:

- The event tree (ET) which is used to model the accident scenarios: it represents the main sequences of functional success and failure of safety systems appointed to cope with the initiating events and the consequences of each sequence. These consequences, denoted also as end states, are identified either as a safe end state or an accident end state.
- The fault tree (FT) which documents the systematic, deductive analysis of all the possible causes for the failure of the required function within an accident scenario modelled by the ET. A FT analysis is performed for each of the safety systems, required in response to the IE.

Assigning the safe end state to a sequence means that the scenario has been successfully terminated and undesired consequences have not occurred. In contrast the accident end state means that the sequence has resulted in undesired consequences.

Synthetically, the methodology embraced for the analysis consists of the following major tasks:

- identification of initiating events or initiating event groups of accident sequences: each initiator is defined by a frequency of occurrence;
- systems analysis: identification of functions to be performed in response to each initiating events to successfully prevent plant damage or to mitigate the consequences and identification of the correspondent plant systems that perform these functions (termed front-line systems): for each system the probability of failure is assessed, by fault tree model;
- accident sequences development by constructing event trees for each initiating event or initiating event groups;
- accident sequences analysis to assess the frequencies of all relevant accident sequences;
- identification of dominant sequences on a frequency-consequence base, i.e. the ones presenting the most severe consequences to the personnel, the plant, the public and the environment and definition of the reference accident scenarios to be further analysed

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 13	di 52
--	--	------------------	----------------------	-------------------	-----------------

through deterministic transient analysis (for instance by t-h code simulation), in order to verify the fulfilment of the safety criteria. Consequences in the case of Level 1 PSA of NPPs are usually defined as degrees of reactor core damage, including ‘safe’ state and ‘severe’ accident state.

One of the main issues encountered in probabilistic analysis concerns the availability of pertinent data for the quantification of the risk, which eventually raises a large uncertainty in the results achieved. Usually these data are accessible from consolidated data bases (e.g. IAEA), resulting from the operational experience of the plants. They pertain, for instance, to component failure rates, component probability on demand, initiating event frequency: for this reason within a PSA study usually an uncertainty analysis, in addition to a sensitivity analysis, is required in order to add credit to the model and to assess if sequences have been correctly evaluated on the probabilistic standpoint. Event trees are used for the graphical and logical presentation of the accident sequences. An example of an event tree is shown in Figure 2. The logical combinations of success/failure conditions of functions or systems (usually safety systems, also called front-line systems) in the event tree are modelled by the fault tree.

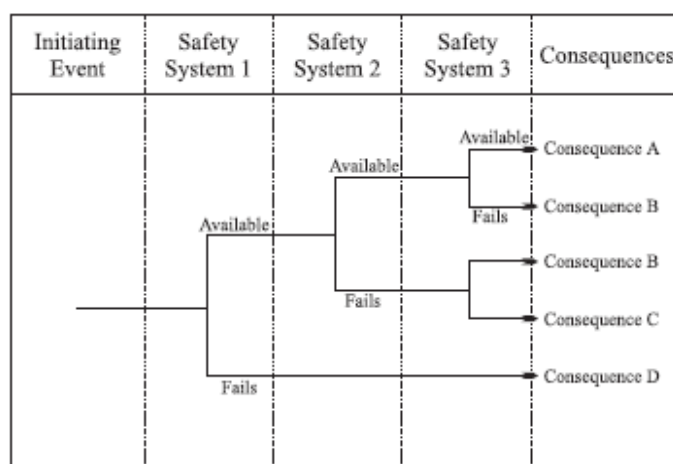


Figure 2 - Example of an event tree

A fault tree logically combines the top event (e.g. complete failure of a support system) and the causes for that event (e.g. equipment failure, operator error etc.). An example of the fault tree is shown in Figure 3. The fault tree mainly consists of the basic events (all possible causes of the top event that are consistent with the level of detail of the study) and logical gates (OR, AND, M out of N and other logical operations). Other modelling tools, like common cause failures, house or area events are also used in the fault trees. All front-line and support systems are modelled by the fault trees and then combined in the event trees depending on the initiating event.

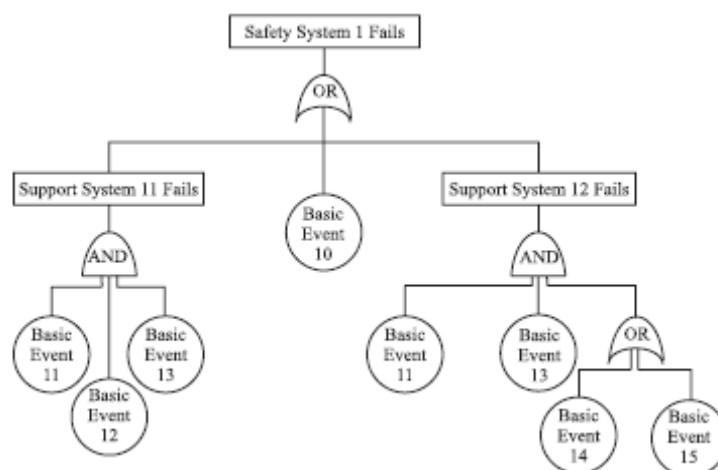


Figure 3 - Example of a fault tree

A fault tree is capable to include rather special cases, usually identified in complex systems. These include system and components dependencies, called common cause failures (simultaneous failures of several components due to the same reason), area events (usually fire, flood etc., which damages groups of components in certain rooms), human actions (operator errors or mitigation actions).

The PSA is a powerful tool that can be used in many different ways to assess, understand and manage risk. Its primary objectives are the following:

- estimate risk level of the facility,
- identify dominant event sequences affecting safety of the facility,
- identify systems, components and human actions important for safety,
- assess important dependencies (among systems or man-machine interactions),
- provide decision support in various application areas.

The growing area of PSA use is extensive support of probabilistic results in risk management and decision-making processes. The main areas of the PSA applications are assessment of design modifications and back-fitting, risk informed optimization of the Technical Specifications, accident management, emergency planning and others. Several modern tools of risk management are also based on the PSA model, such as risk monitoring, precursor analysis and others.

Despite its popularity among the risk assessment tools, the PSA has a number of imitations and drawbacks. The main limitations of the PSA model are the following:

Binary representation of the component state. Only two states are analyzed: failed state or fully functioning state. However, this is not always realistic, as intermediate states are also possible. The same limitation exists for the redundant systems with certain success criteria – system is in failed state (success criteria is not satisfied) or in full power. The intermediate states for redundant systems are even more important.

Independence. In most cases, the components are assumed to be independent (except modelled by CCF), however there are many sources of dependencies, not treated by the model.

Aging effect. The aging effect is ignored because of the constant failure rate assumption. The only conservative possibility to treat the aging impact is to perform sensitivity study.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 15	di 52
--	--	------------------	----------------------	-------------------	-----------------

Time treatment. The FT/ET model is not capable to treat time explicitly during the accident progression. This is one of the major drawbacks of the methodology. In realistic systems, many parameters and functions depend on time and this is not encountered in the model and only approximate chronological order is assumed.

Uncertainty of the calculations. Uncertainties are inevitable in the PSA results and calculations and therefore direct treatment of the quantitative PSA estimates might be misleading. Due to the fact of uncertainties, the qualitative PSA results (identification of dominant accident sequences, comparison of different safety modifications) are of greater importance than quantitative.

3.3 Risk criteria

The risk criterion is a term, which distinguishes between what is considered as an acceptable level of safety and what it is not (ref.2).

The national approaches about risk criteria differ notably from country to country, so no commonly accepted international agreement exists (ref.2).

Quantitative risk objectives in United States of America consider individual and societal risk:

- The mean risk of an individual near a nuclear power plant (living within 1 mile radius) to receive an acutely lethal dose through a reactor accident is not to exceed $5E-7$ /year (this corresponds roughly to 0,1% of the risk from all fatal accidents).

- The risk for the general population within ten-mile-radius around a nuclear power plant to die of cancer as a result of the reactor operation should not exceed $2E-6$ /year (this corresponds to about 0,1% of the total cancer risk conditional on industrial activities).

In spite of the fact that no common criteria exist internationally, one can conclude that the production of electrical energy from nuclear power should not contribute notably to the overall risk is common to the national approaches.

The ALARA (As Low As Reasonably Achievable) principle is mostly acceptable, which states that the risk should be as low as it is reasonably achievable.

In addition, a common position exists that the future power plants should be better and safer than the current ones, which is the position of International Atomic Energy Agency.

Namely, the existing and future plants are distinguished in sense that the criteria are stricter in case of future plants for an order of magnitude.

The objective for core damage frequency for existing plants is $1E-4$ /reactor-year and for future plants it is $1E-5$ / reactor-year.

The objective for large early release frequency for existing plants is $1E-5$ / reactor-year and for future plants it is $1E-6$ / reactor-year.

3.4 Risk-informed Decision making

We have seen that Probabilistic Safety Assessment is a standardized tool for assessing and improving nuclear power plant safety, in terms of risk criteria. For the case of new nuclear power plants it may be required as a part of the safety analysis report, which is the main document needed for licensing of the plant operation.

The risk-informed decision-making is a term describing the process of assessing risks connected with technical decisions and considering of the risk results together with other means or with safety analyses to reach the most appropriate decisions.

In addition to the risk criteria for the nuclear power plant operation, the risk criteria, in some countries, are developed in two aspects considering the acceptability of changes.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 16	di 52
--	--	------------------	----------------------	-------------------	-----------------

- The first aspect includes permanent changes; e.g. assessment of acceptability of plant modifications.
- The second aspect includes temporary changes; e.g. consideration about the on-line maintenance.

Plant modification is a permanent change in the plant, which may be a physical change (e.g. an upgrade of a system, an addition of redundant equipment, a replacement of some components) or a non-physical change (e.g. improved plant operating procedure or improved testing and maintenance procedure, a change connected with certain requirement). An assessment of acceptability of plant modifications requires the risk criteria for permanent changes in the plant, because modification is a permanent change and it represents a potential for permanent change in risk.

The main and the most general rule is that the activities, which results in decrease of risk, are appreciated and mostly approved. Further, the activities, for which a small increase of risk is evaluated, can be considered acceptable, if the risk increase is small and if there are benefits of the change, which overrule the increase of risk, or if there are no methods and tools to evaluate completely the proposed change in terms of positive and negative aspects in terms of risk. Namely, sometimes it is difficult to evaluate quantitatively all the positive and negative aspects of proposed change in such extent that risk models qualitatively and quantitatively include all the positive and negative aspects of the proposed change.

Finally, if a large increase of risk is connected with proposed change, such change is not acceptable.

A typical example consists in the assessment of risk change, in terms of core damage frequency, related to inoperability of standby safety equipments due to test or maintenance.

4. Risk-informed regulatory approach

Previous treatment in sections 3.2 through 3.4 lay the foundations for the development of a broader risk-informed framework, focused on regulating the risk from a nuclear power plant, as reported in ref.3.

Classically, the control of the risk associated to the operation of a nuclear power plant has been founded on the definition of a group of events representing credible *worst-case* accident scenarios (the so-called *Design Basis Accidents*, DBAs) and on the prediction and analysis of their consequences by deterministic calculations. Then, the safety and protection of the system is designed against such events, to prevent them and to protect from, and mitigate their associated consequences. This traditional approach to regulating nuclear safety by the verification that a nuclear plant can withstand a set of prescribed accident scenarios judged as most adverse, conjectures that if a plant can cope with the DBAs, it will also be capable of handling any other accident.

In this view to safety, the underlying concept for protecting a nuclear power plant is the so called *defense-in-depth* which has become the design philosophy for attaining acceptable levels of safety. This *structuralist defense-in-depth* viewpoint and the safety margins derived from it, have been embedded into conservative regulations aimed at enveloping all credible accidents, for what concerns the challenges and stresses posed on the system and its protections. In fact, such view to nuclear safety has been embraced into a number of design and operating regulatory requirements, including: i) the use of redundant active and/or passive engineered safety systems, to avoid the risks from single failures; ii) the use of large design safety margins to cope with the uncertainty in the actual response of the safety systems under accident conditions; iii) the demand of quality assurance practices on materials,

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 17	di 52
--	--	------------------	----------------------	-------------------	-----------------

manufacturing and construction; iv) the restriction of system operation within predetermined bounds; v) the definition of requirements for the testing, inspection and maintenance of the structures, systems and components to guarantee the desired safety levels.

The approach to safety above illustrated has been regarded effective in providing a conservative means for managing the uncertainties in the system behavior and its modeling within the safety analyses. However, it is widely recognized that the reliance on purely deterministic analyses for the verification of nuclear safety may not be rational nor sufficient for bounding the required high levels of safety across all potential accident events and protective safety systems. On one side, the practice of referring to DBAs may lead to the consideration of excessively conservative scenarios, but also highly unlikely, with a penalization of the industry due to the imposition of unnecessarily stringent regulatory burdens on the protective barriers for defense-in-depth. On the other hand, the conjecture that protecting from DBAs would give reasonable assurance of protecting from any accident has been proven wrong, e.g. by the occurrence of the Three Mile Island accident in 1979.

The above considerations have led to the arising of the *Probabilistic Risk Assessment (PRA)* approach for nuclear safety, based on the inclusion into the analysis of the likelihood of all potential accident scenarios by considering the reliability of the protection systems through the introduction of probabilistic measures for the treatment of the uncertainty in their behaviour, as detailed in section 3. This allows addressing some of the shortcomings of the DBAs thanks to a systematic modelling of more realistic scenarios, including multiple failure events (the so-called *Beyond Design Basis Accidents, BDBAs*) and to the definition of the level of risk from the plant in quantitative terms. Furthermore, the PRA analysis can be used to prioritize improvements in the design and operation of the plant for greatest risk reduction. On the other hand, it is impossible to guarantee that PRA captures all the accident events and scenarios contributing to risk and its quantitative results may be affected by very large uncertainties which make difficult their direct use for decision making.

Today's trend in the control of nuclear safety is drifting towards an integrated decision making process that combines the insights from the deterministic and probabilistic analyses with the regulatory requirements and cost-benefit considerations. This approach is increasingly adopted for a more efficient use of resources for increased safety and reduced regulatory burden in the application of a *rationalist* defense-in-depth philosophy. Since according to this approach risk information is to be used as adjunct to the deterministic and prescriptive body of regulations, it is often termed *risk-informed*, to unambiguously differentiate it from the *risk-based* approach based solely on insights from a PRA.

The risk-informed approach aims at systematically integrating deterministic and probabilistic results to obtain a rational decision on the utilization of resources for safety. In such rationalization, explicit consideration is given to the likelihood of events and to their potential consequences.

The undertaking of this approach has led to a number of efforts of risk-informing of existing regulations, i.e. rationalizing regulatory requirements by risk information.

This has meant in particular the possibility of allowing changes in safety requirements upon demonstration that the corresponding change in the risk from the plant is acceptably small and still within the design bounds.

Several instances of these efforts have demonstrated the effectiveness of the approach, perhaps the best still being the application in practice of the maintenance rule which has provided a foundation for making risk insights and prioritization of use in day to day operations.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 18	di 52
--	--	------------------	----------------------	-------------------	-----------------

In order for the integrated, risk-informed decision making process to virtuously benefiting from the combination of the systematic deterministic and probabilistic analyses of the safety of a nuclear power plant, it is necessary to address some relevant issues: for instance an adequate representation and treatment of the related uncertainties has to be provided. This motivates the research on the implementation of new tools in safety assessment practice.

5. IDPSA Integrated Deterministic-Probabilistic Safety Assessment

5.1 Motivation, background and concepts

As previously pointed out, past accidents in nuclear reactors worldwide indicate that existing methods for safety assessment can provide an incomplete and sometimes misleading view of the extremely complex safety systems and modes of their failures.

The most beneficial use of deterministic/probabilistic safety analysis methods in securing safety margins for existing plants, promoted the introduction of a new collective name Integrated Deterministic-Probabilistic Safety Analysis (IDPSA) for the variety of different approaches and tools developed for combined probabilistic and deterministic analysis during the last decades. IDPSA is a family of methods which use tightly coupled probabilistic and deterministic approaches to address aleatory (stochastic aspects of scenario) and epistemic (modelling) uncertainties in a consistent manner. For example, what has been referred to in the past as Dynamic PSA (DPSA) belongs to the family of IDPSA methods. The concept “Dynamic PSA” (DPSA) has been proposed, in order to address issues when timing of the events defines accident progression. DPSA is also used to identify unknown important scenarios (weaknesses) or unnecessary conservatism in the state-of-the-art safety analysis (ref.1).

IDPSA combines deterministic and probabilistic approaches to safety analysis and is suitable to be generally applicable to safety justification of different generations of nuclear systems, especially those which employ digital I&C or heavily rely on physics of the plant or operator actions. Of course, each system and each plant design requires application of adequate deterministic tools, but the general methodology which is being developed here, will be valid for solving different tasks of safety analysis and reduction of uncertainty in decision making process. As such IDPSA basic elements are:

- Deterministic analysis tools (thermal hydraulics, neutronics and severe accident codes);
- Computationally efficient mathematical operations in multi-dimensional space (e.g. numerical integration and probabilistic assessments).

Increasingly stringent safety and licensing requirements and new design solutions necessary to match the expectations present new challenges for classical PSA / DSA. For instance:

- Increasing complexity of the existing plant systems for prevention and mitigations of events and respective PSA models, which lead to:
 - o Growth of resources necessary for development and maintenance of PSA models;
 - o Increased complexity of the input models and associated uncertainties in the different accident analysis codes;
 - o Non-transparency of very complex PSA models aiming at realistic presentation of complex system design;

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 19	di 52
--	--	------------------	----------------------	-------------------	-----------------

- o Increasing reliance on expert judgement in providing conservative assumptions about uncertainties in time dependent scenarios;
 - o Increased complexity in assessment of the impact of human operator actions on time dependent scenarios.
- New designs which on one hand achieve very low core damage frequencies by reducing the number of equipment that can break, on the other hand rely more on physics of passive safety systems and complicated digital control systems than on human operator:
 - o Passive safety systems in new plants and retrofits in existing plants;
 - o Severe accident management in design;
 - o Digital I&C.
- Risk informed decision making for:
 - o Development of design and operational procedures;
 - o Safety and licensing.

Importance of operator actions in accident conditions can be hardly over-estimated, as well as timing and history of the events and operator actions which are difficult to model in PSA.

IDPSA is considered as a complementary to PSA and DSA approaches intended to help in:

- Resolving time dependent interactions between physical phenomena, equipment failures, safety and non-safety systems interactions, control logic, operator actions;
- Identification and characterization of a-priori unknown vulnerable scenarios, or “sleeping threats”;
- Consistent treatment of different sources of uncertainties;
- Reduction of reliance on expert judgment and simplifying assumptions about interdependencies;
- Potential reduction of the cost of safety analysis due to larger involvement of computers in what they can do better: multi-parameter, combinatorial exploration of the plant scenarios space.

However, it would be a mistake to consider IDPSA as a tool that is called to replace PSA and DSA approaches and experts in the decision making process. IDPSA is a complementary tool that can provide additional help to PSA and DSA practitioners and experts by reducing and quantifying uncertainties in a consistent and resource- and time-efficient manner.

5.2 State-of-the-art

In the following a review of the state-of-the-art approaches to deterministic/probabilistic safety analysis is reported. The main stimulus for development of the IDPSA and previously DPSA methods was early realization that static logic models applied in PSA has inherent limitations in resolving of time dependent interactions between

- Physical phenomena;
- Control logic;
- Operator actions;
- Equipment failures.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 20	di 52
--	--	------------------	----------------------	-------------------	-----------------

These interactions can make the result contingent upon the order and timing of the events sequences. PSA can quantify probability of known threats, but it cannot reveal unknown vulnerable sequences and state-of-the-art PSA can not reveal such unknown vulnerable sequences. PSA event trees and “master level” fault trees are based on those threats, which are defined by expert judgement and analysed in detail with deterministic plant simulations, e.g. thermo-hydraulic and reactor-physical transient accident analyses. If the accident scenario simulations are not covering vulnerable sequences, the threats remain unknown. As a consequence PSA “success” paths can end up with core damage and “failure” scenarios might lead to no damage. Even if the threat is known, scenarios with significant timing factors and process-system feedback loops are challenging for static event tree-fault tree approach. Dynamic process failures in Digital I&C (DI&C) and passive plants are also difficult to resolve with static fault/event trees approach because a “process” failure is achievable even if none of the system components fails.

Finally, operator action or human intervention, in general, cannot be properly modelled with the traditional approach to PSA.

Integrated deterministic - probabilistic safety analysis is considered as a means to enable risk-informed decision making in safety assessment and justification. Both deterministic and probabilistic considerations are necessary to address the mutual interactions between: (i) stochastic disturbances (e.g. failures of the equipment), and, (ii) deterministic response of the plant (i.e. transients). Past accidents in nuclear reactors worldwide indicate that the traditional methods for safety assessment can provide an incomplete and sometimes misleading view of the extremely complex safety systems and modes of their failures.

Significant progress has been achieved in the development and application of new tools which combine probabilistic and deterministic approaches in order to address issues when timing of the events defines accident progression.

Several activities have been in progress around the world since early 1980’s towards the development to methodologies that are capable of performing IDPSA. A common feature of these methodologies is that the possible sequencing of events in scenario evolution is not predetermined by the analyst (as it is the case with the traditional PSA), but rather by a dynamic system model (usually a computer code) as the system evolves in time based on a user specified partitioning of the uncertainty space. The IDPSA methodologies can be broadly categorized as: (i) continuous-time methods, (ii) discrete-time methods, (iii) methods which can consider both continuous and discrete times, and (iv) methods with graphical interfaces. While the methods with graphical interfaces are also either continuous or discrete time methods, they are classified as a separate category because the availability of a graphical interface is usually regarded as rendering them more user friendly. Continuous time methods developed to date are the CET (ULB) (ref. 4,5), CETL (SPSA) and CCCMT (OSU, ULB) (ref. 6,7). Discrete time methods include DYLAM (JRCI) (ref. 8,9), DETAM (MIT) (ref.10), ADS (UM) (ref.11), ISA (CSN) (ref.12), CCMT (OSU) (ref. 13, 14). GA (KTH) (ref. 15) and MCDDET (GRS) (ref. 16, 17) methods can consider both continuous and discrete random times. Finally, methods with graphical interfaces include Petri Nets, the Dynamic Flowgraph Methodology (ASCA, Inc.) (ref. 18, 19) and GO-FLOW (ref. 20, 21) developed in Japan. The list is not comprehensive and only includes some examples of the methodologies proposed to date. However, in spite of the large number of methodologies proposed, there are only few computational platforms available for actual plant applications. These platforms are briefly described below. Since 1985, the ISA (Integrated Safety Analysis Methodology), developed at the Modeling and Simulation Department (MOSI-CSN) of the Spanish nuclear regulatory agency CSN, has been implemented in a computer code cluster (SCAIS, Code

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 21	di 52
--	--	------------------	----------------------	-------------------	-----------------

system for integrated safety analysis), by MOSI-CSN together with several Madrid Polytechnical University departments (UPM) and INDIZEN software company. Université Libre de Bruxelles (ULB) and Lietuvos Energetikos Institutas (LEI) have also cooperated. ISA-SCAIS distinctive feature is its regulatory orientation towards the development of diagnostic tools able to check the fulfillment of essential regulatory aspects in specific safety assessments made by the industry in defending their safety cases. The ADAPT (Analysis of Dynamic Accident Progression Trees) (ref. 22, 23) methodology developed at OSU with support from the Sandia National Laboratory (SNL). In conjunction with a computer code describing the dynamic system behavior, ADAPT uses dynamic event trees for the systematic and mechanized quantification of the joint contribution of the impact of aleatory and epistemic uncertainties on the consequences of possible event sequences and their likelihoods. The methodology is implemented using massively parallel processing using the ADAPT software. The output of ADAPT consists of possible event sequence or scenarios, as well as their frequencies, originating from a user specified initiating events and based on user specified branching rules. ADAPT has various graphical capabilities for the display of the results. It has been linked to MELCOR and RELAP5 codes and implemented for the analysis of various initiating events, including station blackout (SBO) with power recovery in two PWRs and aircraft crash on the towers of the reactor vessel auxiliary heat removal system of an example sodium cooled fast breeder. The MCDET methodology developed by GRS combines dynamic event tree (DET) analysis with Monte Carlo (MC) simulation. MCDET is capable of accounting for any discrete and continuous aleatory and epistemic uncertainties. Any probabilistic model may be applied without need for simplifications or for focusing on specific probability distributions. Discrete aleatory uncertainties are treated by the DET approach. It keeps track of all combinations of potential alternatives for the discrete uncertainties. More than two alternatives for a discrete uncertainty can be considered. MC simulation is applied in combination with the DET approach to consider continuous aleatory uncertainties. The values obtained from MC simulation are successively supplied as input to the further calculation of a DET. The output of MCDET consists of a huge amount of event sequences and (conditional) probability distributions. The final probabilistic assessments are derived from the mean probability distributions over all DETs which are given together with confidence intervals. So far, MCDET has been linked to the MELCOR code and has been implemented for various type of initiating events in a Konvoi type PWR. The implemented MCDET module system can in principal be coupled with any deterministic dynamic code. The GA-IDPSA approach jointly developed by KTH and Moscow Power Engineering Institute uses global optimum search method (genetic algorithm) to increase computational efficiency in exploration of the uncertainty and plant accident scenarios space. In the exploration process the GA method imposes no restrictions on consideration of different types of (i) uncertain variables (continuous and discrete), (ii) uncertainties (aleatory and epistemic), and (iii) branching (binary and non-binary). This method is best suited for identification of failure domains including worst case scenarios (maybe rare but high consequence hazards). Stochastic properties of the GA are used for estimation of the probabilities. DET can be constructed based on post-processing of the GA-IDPSA search data. The methodology is implemented using massively parallel calculations implemented in the GA-NPO software. It has been linked to RELAP5 code and implemented for the analysis of various initiating events of the WWER-1000 type reactor and model of the typical PWR. It can be adapted to any other deterministic code. The modeling strategy of ADS (Accident Dynamic Simulation Methodology) developed at UM is based on breaking down the accident analysis model into different parts according to the nature of the processes involved, simplifying each part while

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 22	di 52
--	--	------------------	----------------------	-------------------	-----------------

retaining its essential features, and developing integration rules for full scale application. Whenever a hardware system state transition point or an operator interaction point is reached, the accident scheduler chooses one path to follow. After the simulation process reaches an end point, the scheduler directs the simulation back to the previous branch point, reinitializes every simulation module back to this time point, and follows the other branch point path. In the multiprocessor version of ADS, the simulations are distributed among multiple client computers. A central server is responsible for managing assignment of simulation tasks to individual clients and post-simulation reassembly of the simulation results. ADS has been linked to the RELAP code and is mostly used for human reliability analysis. The dynamic flow graph methodology (DFM) is a digraph-based technique. A process variable is represented by a node discretized into a finite number of states. The system dynamics is represented by a cause-and-effect relationship between these states which can be obtained from a system code, but could be qualitative relations as well. Instead of minimal cut sets, the DFM yields the prime implicants for the system. A prime implicant is any monomial (conjunction of primary events) that is sufficient to cause the top event, but does not contain any shorter conjunction of the same events that is sufficient to cause the top event. DFM has been implemented for the reliability analysis and PSA of control systems, human behaviour and software. The GO-FLOW methodology is a success-oriented system analysis technique, capable of evaluating system reliability and availability. The modelling technique produces the GO-FLOW chart, which consists of signal lines and operators. The operators model function or failure of the physical equipment, a logical gate, and a signal generator. Signals represent some physical quantity or information. The system model is assembled from the available hardware models (e.g. valves, pumps) in the GO-FLOW library through a graphical user interface. The analysis is performed from the upstream to the downstream signal lines, and is completed when the intensities of the final signals at all-time points are obtained. GO-FLOW output includes time dependent system reliability/availability, cut sets, common cause failure analysis and, uncertainty analysis. One particular point that becomes an important practical issue in all IDPSA developments is the consistency between the assumptions made in state-of-the-art static PSAs and its dynamic counterparts, in order to ensure that they do not contradict each other. The large industry and regulatory engineering effort that underlies the present use of DSA transient analysis codes and PSA FT/ET plant models, imposes as a strong requirement that the new methods and codes will add-to, but not replace the existing ones. A consistent link between IDPSA, DSA and PSA approaches is necessary to solve well recognized deficiencies of stand-alone or weakly linked present tools and methods.

The work to date with IDPSA tools briefly overviewed above indicates that while they provide information that can complement the traditional PSA and DSA towards better coverage of the uncertainty space and also provide better modeling capability when there is hardware/software/process/ human interaction during system evolution, a number of issues challenge their utilization in practical applications:

1. Consistent approaches to connecting IDPSA to PSA and DSA: This is the most challenging aspects of using IDPSA and the most critical for deployment of IDPSA in industrial practice of safety analysis. IDPSA methods do not need to be used for the whole system. System specific input for the stochastic modelling of dynamic aspects is usually at the subsystem level and there is no need to include every piece of hardware individually in the dynamic model. Subsystem level information can be obtained from an existing PSA. Similarly, dynamic methods are usually not needed unless there is hardware/process/software/human interaction and IDPSA can provide information about the consequences of such interactions to an existing plant PSA. Also, it may be possible

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 23	di 52
--	--	------------------	----------------------	-------------------	-----------------

to reduce the size of the uncertainty space through pre-screening by DSA. An important point in this regard is to ensure the consistency among the assumptions of the state-of-the-art PSA and IPSA methods. Experience gained in addressing realistic pilot applications about consistent and efficient ways for coupling between IDPSA, PSA and DSA approaches will be summarised by the project participants in order to promote further progress beyond the state-of-the-art.

2. Methods for IDPSA data mining: Due to the large number of scenarios generated for proper coverage of the uncertainty space, analysis of the output data through visual inspection in its entirety is not practical. Tens of terabytes of data can be produced in the analysis of a single initiating event. Efficient means of data mining and clustering will be developed for the transparent analysis of the IDPSA results.
3. Computational efficiency: The IDPSA platforms need to be linked to system codes for specific applications. The system models constructed through codes such as RELAP, TRACE, ATHLET, MELCOR, ASTEC have quite long run times. For example, the analysis of a single 3-day PWR SBO scenario with MELCOR requires a 3-day run time. In IDPSA, hundreds and possibly thousands of such scenarios need to be generated for proper coverage of the uncertainty space. In that respect the IDPSA platforms need to function in a massively parallel and distributed environment. Also advanced methods for computationally efficient exploration of the uncertainty space will be developed.
4. Graphical user interface: Having fairly complex mathematical structures and large input files, the IDPSA tools are not easy to use by non-developers. User friendly graphical user interfaces need to be developed both for input and output processing that will make the internals of the platform transparent for the user.
5. Flexible platform structure requirement for linking with different system codes: Most of the IDPSA tools overviewed above are hardwired to a particular system code. In order to provide capability to function with different codes with minimum user effort, the platform needs to be flexible enough to accommodate different input-output requirements and structures.

While there have been some efforts to address these issues, additional efforts are required aiming at advancing the state-of-the-art to the point where IDPSA tools can be installed and used by non-developers in a computationally feasible manner with a few weeks of training. Long term dynamic reliability modelling of control systems including I&C (Instrumentation and Control) components and their interaction with a physical process is a challenging task for the state-of-the-art PSA or DSA approaches. Control systems and protection systems are sensitive to “context error” failures. They occur in situations where a control system follows its logic, exempt of intrinsic errors, but concludes to an inappropriate order, given the context. There are two main causes for such a situation: an order in an unexpected context or an order based on erroneous information about the context.

The modelling of dynamic reliability of hybrid systems which are described by continuous variables (temperature, pressure, flow...), deterministic events (planned operational profile change...) and stochastic events (e.g. control logic and mechanical parts failures, unplanned variations of operational profile...) has to be done for relatively long period of time (weeks, or months). The Monte Carlo techniques that are typically used to simulate a large number of stories have to be modified to be able to cover rare events and long periods of time.

The problem of combining hybrid-dynamic modelling with PSA will have to be addressed based on a realistically complex benchmark case. The synthesis will have also to include a proposal of a general approach based on criteria like modelling simplicity, possibility of verification, parallelisation capability, capability to represent continuous variables, size of the

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 24	di 52
--	--	------------------	----------------------	-------------------	-----------------

state space, relevance to various aspects of decision making (reliability, safety, availability estimation, critical sequence identification, decision making and optimisation...).

Therefore a coordination of the collaborative efforts on development of the IDPSA methodology is essential for success of a related project, given the challenging complexity of the issues to be addressed, diverse experience accumulated by the partners in their previous works, similarity of the general requirements to functionality of the joint application of IDPSA, PSA and DSA methods (ref. 24).

6. Case study

Along the path towards the implementation of the approach in safety assessment practice, pilot applications and benchmarks are required in order to endorse and add credit to the proposed methodology.

They should be focused on the needs for:

- Realistic quantification of safety margins with uncertainty estimation for:
 - Assessment of the plant design change impacts on safety and operation;
 - Integral risk assessment and risk informed regulation.
- Identification and characterization of undiscovered plant vulnerabilities (safety and/or operational) to:
 - Identify possible incompleteness, over- or false- conservatism in existing PSA and DSA models;
 - Reduce reliance on assumptions in engineering judgment about complex time dependencies and scenarios;
 - Improve PSA models with IDPSA generated data (e.g. sequences, probabilities, etc.) and to use PSA generated data as initial and boundary conditions in IDPSA.
- Increasing transparency and robustness of risk-informed decision making;
- Improvement of plant safety and operation

In the present treatment, a case study is tentatively presented, in the form of preliminary accident sequence definition and analysis, specifically as regards safety system evaluation to cope with external events, mainly for illustrative purposes, acknowledging the “demonstrative” character of the study, the fact that the actual available tools don’t allow a more thorough and realistic analysis for quantification of plant safety.

To define realistic pilot applications for joint analysis by IDPSA, PSA and DSA, we could consider:

- LOOP/SBO scenarios with possibility of power recovery for PWR and BWR;
- LOCA with variable size and locations and possible operator actions for a PWR;
- Hydrogen production, combustion and containment over-pressurization scenarios;
- Benchmark on dynamic reliability of control systems.

The implications of the extension of the accident coping capability on the safety of the nuclear power plant will be analyzed with state-of-the-art probabilistic and deterministic methods applied on reference models of the nuclear power plants.

The LOOP/SBO scenarios (with possibility of power recovery for PWR and BWR) is being considered: do to the early stage of the methodology development, we’ll limit our analysis to

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 25	di 52
--	--	------------------	----------------------	-------------------	-----------------

considerations about the fundamental probabilistic aspects of the accident and the deterministic assessment as regards a specific reactor case.

Hence the first task of this work will be the state-of-the-art of the PSA approach with reference to the specific LOOP/SBO accident sequence modeling, including the development of generic event trees.

The second and more relevant task will be the application of a deterministic code to evaluate a specific LWR plant accident transient.

7. Probabilistic safety analysis

7.1 Accident sequence modeling

Ref. 25 outlines the modeling of LOOP and possible SBO events in the context of PRA. LOOP/SBO accident sequence logic is represented using a combination of event tree and fault tree logic modeling. The choice of specific modeling techniques is not as important as the content of the underlying logic. The next subsection will address key aspects of the model. These aspects are referred to as nodes where nodes could represent event tree top events, event tree branch assignments, fault tree gates, or some combination. This section does not provide specific requirements for model structure but, rather, outlines the considerations necessary for the development of realistic plant specific logic models.

The development of LOOP and SBO accident sequences is somewhat complicated by the need to incorporate sequence specific success criteria and functional reliability challenges that vary in time. The intention is to develop event trees that are representative of the functional and sequential aspects of LOOP/SBO accident progression. The principal elements of the LOOP/SBO accident sequence model development include the following:

- Development of an understanding of plant response, safety functions, design features, EOPs, and Abnormal Operating Procedures.
- A set of thermal-hydraulic or other (e.g., accident sequence timing, inventory expenditure) calculations necessary to support the development of the accident sequences.
- Determination of key timing considerations with respect to safety system operation.
- Identification of:
 - Success criteria, and operator actions needed to establish stable plant conditions (core cooling)
 - System and component dependencies
 - Internal and external operating environmental limitations to equipment operability
- Development of accident sequence event tree logic to account for functional, systemic, time phasing, and procedural elements.

There is no one specific event tree structure that has been used and accepted as a standard in PRAs for development of LOOP and LOOP/SBO accident sequences. Provided herein are the critical characteristics of the underlying model logic. These can be represented effectively by a multitude of modeling techniques. For LOOP/SBO these will include functional, systems, operational, and timing elements.

Typically the event tree top logic will include explicit or implicit representation of the following LOOP/SBO event tree nodes:

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 26	di 52
--	--	------------------	----------------------	-------------------	-----------------

- The initiating event: LOOP (includes consideration of transient and LOCA induced challenges leading to LOOP)
- Reactor trip: Reactor Protection System (if unsuccessful, transfer analysis to Anticipated Transient Without Scram (ATWS) event tree otherwise assess in the LOOP/SBO event tree)
- Availability of onsite emergency AC power (a separate event tree node to segregate SBO events; otherwise treat it in the fault tree logic)
- Reactor cooling systems operation and mission time
 - LOOP only sequences: like reactor transient event tree, transfer to transient event tree
 - SBO sequences: steam turbine driven and/or dedicated diesel driven systems
- RCS cool down (pressure and temperature control)
- LOOP/SBO transient induced LOCA
 - Stuck open SRV or PORV (initial LOOP or subsequent)
 - RCS seal integrity (loss magnitude may vary with time and RCS pressure reduction)
- A method to address the cause factors for a LOOP initiator and their subsequent effect on the AC power non-recovery probability
 - Extended SBO coping (continued operation of SBO reactor cooling systems)
 - Extended SBO recovery (restore AC and bring plant to safe, stable shutdown cooling condition)
 - Containment heat removal

Depending on timing and associated success criteria, combinations of the above will lead to stable shutdown conditions, transfers to other accident sequence event trees (e.g., ATWS), or core damage. The major consideration will be the availability of AC power supplies for mitigative functions. SBO sequences will include the following for assessment of severe accident progression:

- SBO core damage with AC recovery prior to containment failure (typical Containment Event Tree modeling will apply to these scenarios, but may include reduced capability of containment systems if only limited AC is restored).
- Extended SBO core damage and containment failure without AC recovery
 - Core melt accident progression nodes
 - Severe accident management capabilities and strategies
 - Emergency preparedness response

The accident sequence mitigation and recovery modeling should consider equipment and operator capability and reliability up to the time a safe and stable reactor decay heat removal condition has been achieved consistent with PRA mission time requirements. This involves a determination of whether the factors affecting the ability to restore stable core cooling are realistic and includes five basic elements:

- Front line system functionality (such as pressures and flow rates) and any “off normal” means of core cooling to be relied upon to mitigate core damage.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 27	di 52
--	--	------------------	----------------------	-------------------	-----------------

- Support system functionality (such as cooling or motive power like air pressure or electricity).
- Procedures and training on the necessary recovery actions including implementation of AC/DC power alignments upon recovery of offsite or onsite AC power.
- Ability to place the reactor/steam generators/containment in an appropriate state to allow for support/front line systems to function (such as manual depressurization) upon recovery of offsite or onsite AC power.
- Environmental conditions (such as temperature and radiation conditions that may impact equipment performance or operator actions).

Based on results from many PRAs the probability of operator failure to carry out the SBO recovery actions properly are a potentially significant consideration in SBO mitigation effectiveness. There are many human performance factors that will influence the ability of operators to execute the recovery actions reliably. While the HRA assessment is not outside the capabilities of existing HRA methods, the analyst must be aware of factors and conditions specific to the scenario under consideration that affect capability of the equipment and ability of the operators to implement recovery actions.

Another important point is the credit for passive system operation to cope with the accident. This implies the capability to assess the potential success paths for “black operation” of decay heat removal systems during the phase of a SBO when DC power has been depleted and AC independent decay removal systems are still potentially functional, to buy additional time to restore offsite or onsite AC power supplies. Credit for the “black operation” of equipment should be thoroughly justified on a plant specific basis.

Ultimately, it has to be recognized that this approach has several areas of acknowledged uncertainty, including, especially, the failure times of safety systems, execution times of human actions or physical quantities like injection rates, depressurization rates or leakage rates.

7.2 Generic event tree modeling

For achievement of the PRA perspective, in the following we propose some typical event trees relative to LWR reactors, not on a plant specific basis: therefore, on the basis of this, only qualitative considerations are drawn from their analysis, postponing a more quantitative evaluation to further explicit reactor related studies.

A subset of LOOP scenarios involves the total loss of AC power at a commercial nuclear power plant as a result of complete failure of both offsite and onsite AC power sources. These are termed station blackout (SBO) scenarios. In SBO situations, safe shutdown must be accomplished by relying on components that do not require AC power, such as turbine-driven pumps or diesel-driven pumps. The reliability of such components, along with direct current battery depletion times and the characteristics of offsite power restoration, are important contributors to SBO risk.

SBO risk in terms of core damage can be thought of as the product of the LOOP frequency, the failure probability of the onsite emergency power system (EPS), and the composite failure probability of SBO coping features at a given plant. Each of these three contributors to SBO risk is discussed below. Following the LOOP initiating event, the next top event questions whether the control rods drop into the core to shut down the reactor. If not, the sequence transfers to the anticipated transient without scram (ATWS) event tree for further development. The third top event questions whether the onsite AC EPS successfully starts and

provides power to essential buses. If the EPS fails, then the plant is in an SBO situation, and the sequence transfers to the SBO event tree for further development.

As described in ref. 26, in general three main phases of a station blackout can be identified. The first phase includes the need for promptly actuating decay heat removal systems [in case of PWRs by the AFW TDP (or DDP for some plants), by isolation condenser in case of BWRs (BWR-2 and 3 designs and ESBWR)] and controlling the reactor coolant inventory (including e.g. the failure to close of the PORV or stuck-open relief valve) to assure the RCS integrity.

The second phase includes operational limitations in the capability of continued decay heat removal and coolant inventory control considering limited capacities (such as DC power due to battery depletion, condensate storage tank due to insufficient make-up) to assure actuation of the AC-independent decay heat removal systems, or interactive failure [for example, high temperature effects due to loss of heating, ventilation, and air conditioning (HVAC)], and the potential for reactor coolant loss (such as, through pump seal leakage and PORV stuck-open). The third phase involves the need to eventually recover AC power and establish a stable, controllable mode of decay heat removal.

Note that the loss of all AC electrical power sources doesn't include the loss of available AC power to buses fed by station batteries through inverters, to supply the power needed by vital safety equipment.

Figure 4 shows the event tree for PWRs; Figure 5 shows it for BWRs that use an Isolation Condenser.

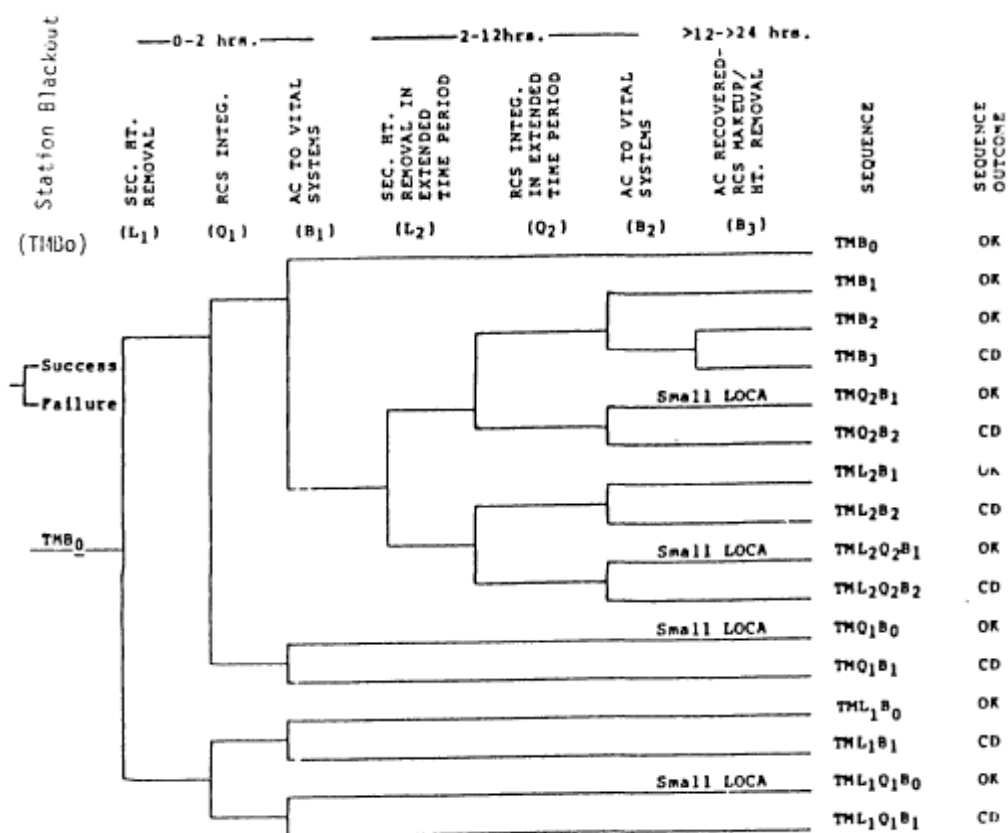


Figure 4 - Generic PWR event tree for station blackout



Figure 5 - Generic BWR event tree for station blackout

Depending upon the combinations of safety system successes and failures, the event trees end with a sequence outcome state designated as "OK," meaning that stable, long-term core cooling is achieved or achievable, or "CD," meaning that an inadequate core cooling state is reached and some reactor core damage can be expected. For the latter case, core damage can be expected to proceed to core melt if effective and timely measures to restore AC power and core cooling *are* not taken or available.

The event trees are characterized not only by the systemic and functional considerations important to station blackout accident sequences, but also by the phases of the transient that would affect the plant response and system operability for station blackouts of various durations.

The event trees show the loss of all AC power as the initiating event and proceed through decay heat removal, reactor coolant inventory (integrity), and restoration of AC power to enable operation of the normal decay heat removal and makeup systems.

Detailed plant transient response analyses are required to cover the spectrum of sequences identified in the event trees, aiming at (1) better understanding the accident progression characteristics related to the timing of events and physical parameter values during the transient, (2) determining success states for systems, trains, components, and operator actions during station blackout sequences and (3) the available time for the system recovery, before the onset of the severe accident.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 30	di 52
--	--	------------------	----------------------	-------------------	-----------------

8. Deterministic safety analysis

8.1 General considerations

In the formulation of a program for safety (re)evaluation (and -or upgrading- design support), deterministic methodology plays an important role because this type of approach will allow to evaluate the inherent capability of nuclear power plants to resist also severe external events, not considered in their original design.

In respect to the probabilistic approach the deterministic one will allow to simulate the behaviour of plant structures, systems and components, in a much detail and as real as possible, in order to determine the strength capacity or reserve of the any analyzed structure.

Conservatism is also present in such a type of approach due to the fact that it is compounded through the safety analysis and the design chain.

Traditionally, the effects of internal/external events on the behavior of structures have been characterized in part in terms of the maximum displacement or by the maximum ductility factor and in parts in terms of stresses. These concepts have been and are widely employed as a measure of the damage sustained during the dynamic response of a plant.

Therefore the inherent capability or robustness, usually indicated [27] as ‘design margin’ to failure, is a direct measure of the load (structural) bearing capability to be used in the design and qualification procedures of nuclear plant, according to current practices.

It is known the design margin exists and is ensured through the use of design criteria in industry standards and guidelines, particularly those applicable to nuclear installations, as demonstrated through the implementation of safety margin assessment (SMA) or PSA methodologies for existing plants.

The design margin typically varies greatly from one location in the plant to another and from one system or component to another, in relation also of the wide range of internal and external extreme loads, i.e. flooding, earthquake or other environmental loads due to accident conditions, aircraft crash, tornado or pipe break, that are site depending.

In addition, the evaluation and quantification of the structural capacity (by adopting thermal hydraulics, neutronics, thermo-mechanical and severe accident codes) of an existing or next/under development nuclear installation, according to the current requirements, which became more stringent especially after the accident event of Fukushima, represents a way to understand the true state of the SSCs in terms of required safety functions and capacities.

It is therefore important to use realistic and best estimate values for the as-is condition of the SSCs and not to introduce safety factors that may unnecessarily bias the results.

The approach used by the SMA methodology, for example, is to consider a higher level of hazard by defining the intensity/magnitude of the initiating event, often to be conservative greater than the design basis one, and to determine/associate on this the really strength capacity.

In so doing, the inherent additional capacity of the SSCs may be taken into account as well all significant information concerning material property (taking into account failure mechanism and deterioration process), SSCs geometry (progressive damage of component and structure) and operational status, boundary and initial conditions and deriving from all relevant sources, such as vulnerability of selected structures and/or non-structural elements (e.g. masonry walls), etc.

In this light, a measure of the damage is mainly associated with nonlinear behavior of facilities which is dependent on many factors, of which the maximum displacement, the

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 31	di 52
--	--	------------------	----------------------	-------------------	-----------------

inherent straining of the materials at critical sections or elements, the stress level and excursion evaluated at critical sections or elements as well as the total energy that must be absorbed.

8.2 Deterministic safety assessment: SMA evaluation

In this framework, deterministic safety assessment develops with the intent to evaluate the performance of the installation for design and beyond design basis conditions in order to provide confidence that there is no ‘cliff edge effect’, that is, to demonstrate that no significant failures would occur.

As for the DSA concerned, linear elastic and non linear analyses may be carried out.

Elastic analysis concepts, where the single values of maximum stress or maximum deformation are the only parameters required for design control, were extended many years ago through limit design concepts to reflect maximum stress and strength through use of the ductility factor (maximum displacement divided by the yield displacement). This approach, firstly employed in the blast dynamics field for structures under monotonic loading conditions, is currently used, jointly to superposition solution, also when external excitation is oscillatory in nature as a descriptor of inelastic deformation [28] [29]. The ductility factor concept also is employed in design in other less obvious forms. For example, in building code design provisions the pseudo-static design force levels that may be encountered in many situations may lead to nonlinear behavior of the structure.

The structural design is planned to accommodate the energy absorption and to implicitly limit the maximum ductility to some accepted value, wherein damage will be present but collapse is hopefully precluded. This approach requires the adoption of non linear analysis and the designer to be knowledgeable about materials properties in the nonlinear range: the maximum “drift” limits or also the allowable maximum stress, as presently used in many applications, are used to control that the maximum deformation or stress is below the limit value.

The two approaches (linear and non linear) just described, in view of the imposed constraints, are not necessarily consistent: observations of the physical behavior of structures and structural elements, in the field and laboratory, indicated that the deformation process is difficult to describe by linear approach so non linear behaviour might be preferred to determine damaging process.

The results of these evaluations may be:

- a) Measures of the capacity of the nuclear installation;
- b) Identification of consequences/damages associated mainly to external event and relevant from a safety point of view;
- c) Identification of operational modifications to improve safety;
- d) Identification of influence and interactions among the plant systems, etc.;
- e) Identification of actions to be taken before, during and after the occurrence of an external that could jeopardize the overall plant safety.

To reduce the uncertainties related to the evaluation methodology, the following aspects should be accurately considered and covered:

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 32	di 52
--	--	------------------	----------------------	-------------------	-----------------

1. Definition of the flooding or other external event input, that is, in the case of tsunami or flooding, the parameters characterizing the design flood elevation;
2. Verification of the site characteristic and stability with respect to the potential for inland inundation or in the case of earthquake from surface faulting;
3. Definition of the (newly, if the case) site hazard/ risk, through also the data collected during the experienced past external events;
4. Material experimental data based on the qualification or fragility tests of system and components, supplied by manufacturer. Specifically to analyze with a high degree of accuracy the behaviour of SSCs it is necessary to correctly characterize their behavior and determine the factors which mainly may influence it.
Particularly the ageing degradation should be considered, because it is considered one of the most important parameters that could reduce the capacity of SSCs.
Typical ageing degradation effects include: corrosion and erosion of piping, tanks and metallic components; thermal and neutron irradiation effects (e.g. embrittlement of the reactor pressure vessel, deterioration of concrete structures, components and anchors, deterioration of electrical systems); stress corrosion cracking (for the core shroud of a boiling water reactor, primary piping, etc.); and ageing of electrical systems and devices.

8.3 Collection of data: support global response of plant

The starting point in the definition and setting up of a methodology capable to determine the safety margin (that simply means if the stress level is acceptable or exceeds the allowable limit) the first step is represented by the collection of the general documentation of plant and its SSCs (BOP, lay-out, drawings, site characteristics).

Emphasis should be put on any specific data and information on the nuclear installation used at the design stage, that may represent the initial conditions (ICs), including:

- 1) Standards and code (International rules and guidelines in THs, neutronics, structural integrity, SA, etc. issue to investigate) adopted to:
 - a. specify the nominal properties of materials used and their mechanical characteristics;
 - b. define the load combinations, in view of the verification of components;
 - c. evaluate/calculate design parameters, depending on accident conditions, of structures, components, piping systems and other items;
- 2) General arrangement and layout drawings for structures, equipment and distribution systems (e.g. piping, cable trays, ventilation ducts), etc..
- 3) Results of the safety assessment of internal (and external) events Figure 6, if performed in order to be able to define the “correct” intensity of the event that could be occurred on site.
- 4) Data and information on results of qualification tests for SSCs performed during the pre-operational period, including any information available on inspection, maintenance, and non-conformance reports and corrective action reports.

- 5) Quality assurance and quality control documentation with particular emphasis on the as-built conditions for materials, geometry and configuration, for assessing the modifications during construction, fabrication, assembly and commissioning, including non-conformance reports and corrective action reports.
- 6) The accuracy of the collected input data in order to guarantee lesser uncertainty affect deterministic analysis and to carry out the real behaviour of component analyzed.



Figure 6- Example of peak cladding temperature acceptance criteria based on deterministic evaluation [30]

8.3.1 Input data

Specifically data or information of the SSCs allowing a realistic simulation of component under transients condition (dynamic, thermal, TH ect. ones) should include:

- a. System design:
 - System description documents (e.g. reactor vessel components, valves, piping, pumps, filter, gasket, etc.);
 - Safety, quality and seismic classification;
 - Design reports;
 - Report on confirmation of the functionality of systems;
 - Instrumentation and control, including details.
- b. Geotechnical design (site risk category on the basis of natural external event to analyze):

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 34	di 52
--	--	------------------	----------------------	-------------------	-----------------

- Coastal information;
 - Sea bed slope characteristics; or
 - Weather characteristics
 - Soil characteristics (shear velocity, cohesion, etc.);
 - Soil–foundation–structure failure modes and capacities (e.g. estimated settlements, sliding, overturning, uplifting, liquefaction).
- c. Structural design:
- Stress analysis reports for all structures of interest;
 - Structural drawings (e.g. structural steel, reinforced and/or prestressed concrete), preferably as-built documentation;
 - Material properties (specified and test data);
 - Typical details (e.g. connections, reinforcement type, leaktightness system, etc.);
- d. Component design:
- External design basis event analysis and design procedures;
 - Qualification procedures, including test specifications, test reports, etc.;
 - Typical anchorage requirements and types used;
 - Stress analysis reports;
 - Pre-operational test reports, if any;
- e. Distribution system design (piping, cable trays, cable conduits, ventilation ducts):
- Systems (safety and non safety) description documents;
 - Piping and instrumentation diagrams;
 - Diagrams of cable trays and cable conduits and their supports;
 - Diagrams of ventilation ducts and their supports;
- f. Service and handling equipments (although some of these are non-safety-related systems, their evaluation may be needed for analysis and study of interaction effects in operational and storage configurations):
- Main and secondary cranes;
 - Refuelling machines.

8.3.2 Design basis event condition

The definition of input of an external events is often conditioned by the state of information on the past event experienced on site. In the absence of these information it could be useful to apply probabilistic analysis in order to determine the intensity of external event in relation to its low or high probability of occurrence, although this approach seemed to be not accurate in the light of Fukushima accident.

Specifically, when considering tsunami event, it is important to take into account the past events occurred worldwide and the initiating causes of such a type of phenomena [31] [32].

A tsunami is a natural phenomenon characterized by the formation of a series of water waves, propagating from the point of generation (known as tsunamigenic source) to the shore. Generally it may be impulsively generated by an undersea earthquake or, less frequently, by a volcanic eruption, meteor impact, submarine slumps or coastal landslides. It may also be generated in lakes and other inland bodies of water by similar mechanisms [32].

The impact of the water waves or of the possible entrained missiles (debris and/or stiffer structures) is considered primarily responsible for the massive and/or catastrophic damages of the on-land buildings, infrastructures, environment and of fatalities, particularly during the flooding.

It is important to stress that the occurrence of external event of this sort may cause, and have caused more than 1000 deaths, as indicated in the overview of historical tsunamis (Figure 7). The data of event occurred at Fukushima (flood elevation, courtesy of TEPCO©, shown in Figure 8) [33] are summarized in Figure 7 (b).

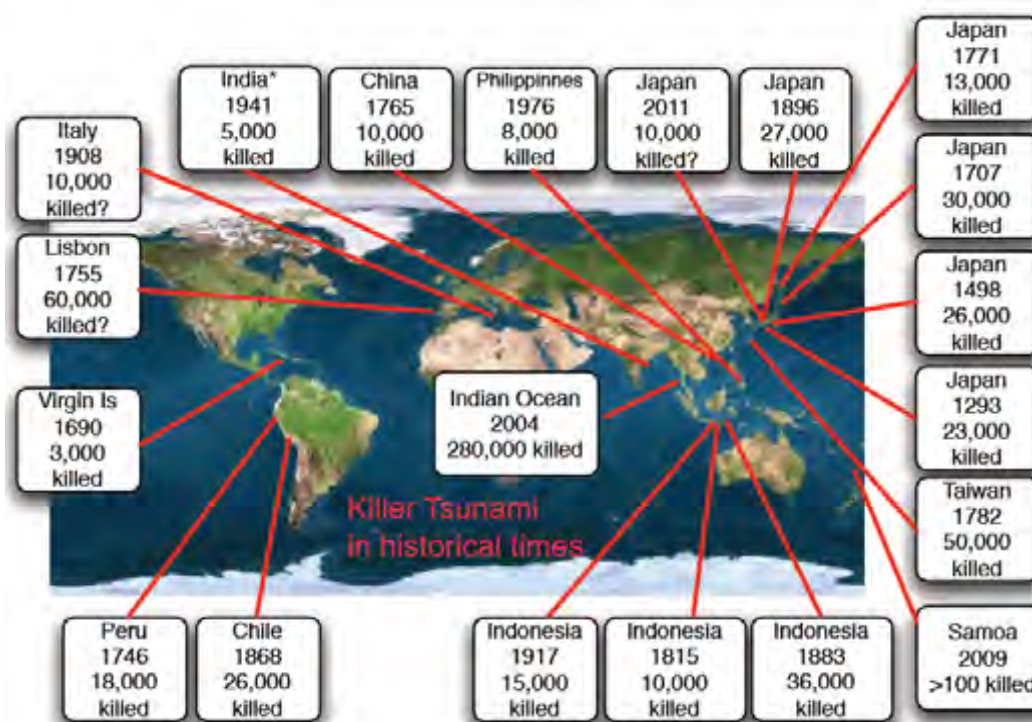
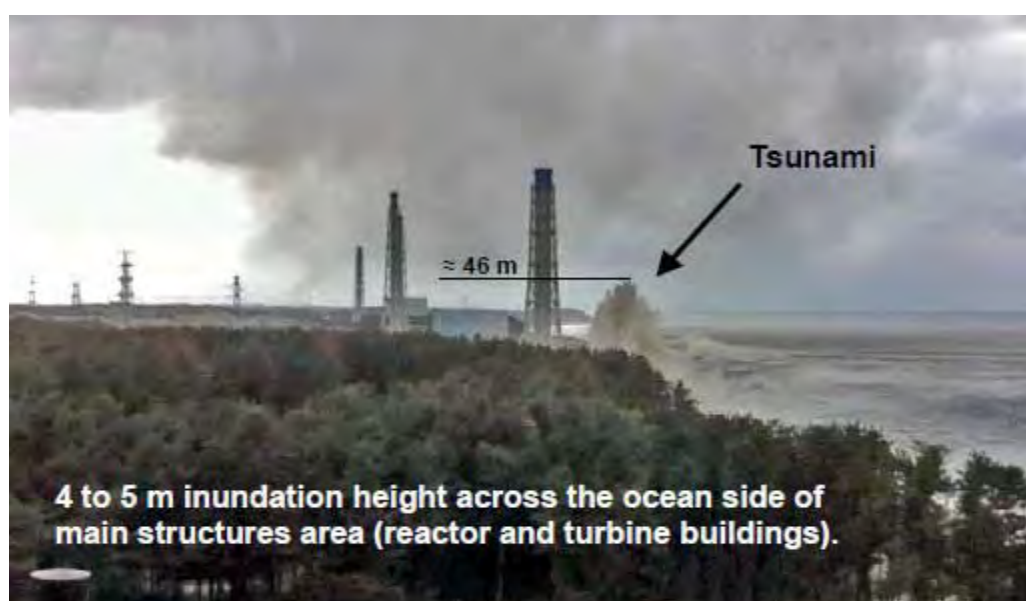
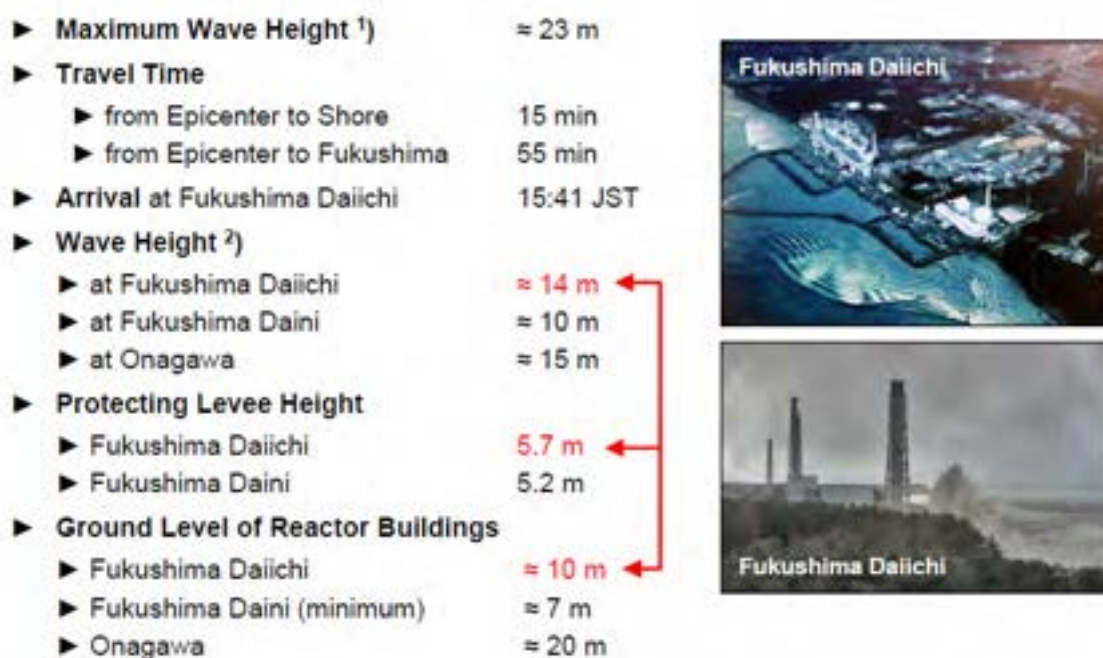


Figure 7 - Severe tsunami in the history



(a)



(b)

Figure 8 - Tsunami waves impact at Fukushima Daiichi reactor

So, when considering tsunami event, the analysis of historical data, demonstrating that 16 large tsunamis, caused by undersea earthquake, with amplitudes of at least 10 m in past 513 years occurred, that means that one event once thirty years on Japan, particularly, as indicated in the data reported in Table 1.

On the basis of this input data, it is possible to define the evaluation of water waves, which, in turn, will allow to calculate the hydrostatic and hydrodynamic forces exerted by the breaking water waves themselves to be used as IC in the deterministic analysis.

In addition, several correlation may be found in literature, like that of Inamura, to correlate earthquake event to the intensity of tsunami, and applied to evaluate the design flood elevation.

Table 1- Large tsunamis with high amplitudes

Date	Affected Region	Earthquake ¹⁾	Tsunami ²⁾
11.03.2011	Japan	M = 9.0	23 m
04.10.1994	Kuril Islands	M = 8.3	11 m
12.07.1993	Sea of Japan	M = 7.7	31.7 m
26.05.1983	Noshiro	M = 7.7	14.5 m
07.12.1944	Kii Peninsula	M = 8.1	10 m
02.03.1933	Sanriku	M = 8.4	30 m
01.09.1923	Tokaido	M = 7.9	12 m
07.09.1918	Kuril Islands	M = 8.2	12 m
15.06.1896	Sanriku	M = 7.6	38 m
24.12.1854	Nankaido	M = 8.4	28 m
29.06.1780	Kuril Islands	M = 7.5	12 m
24.04.1771	Ryukyu Islands	M = 7.4	85 m
28.10.1707	Japan	M = 8.4	11 m
31.12.1703	Tokaido-Kashima	M = 8.2	10,5 m
02.12.1611	Sanriku	M = 8.0	25 m
20.09.1498	Nankaido	M = 8.6	17 m
Resulting Actual Design Basis		M ≈ 7.5	> 10 m

8.3.3 Geotechnical data

Information on coastal location of the site, sea bed characteristics (specifically the slope variation) or on soil type (free surface finished grade, foundation mat level or base rock level; stiffness and damping properties, etc.) and on the possible soil–structure interaction, used at the time of the original design, should be collected because their knowledge may influence to a great extent the evaluation of safety of structure.

In the case of flooding the variation of the sea bed slope is the parameters that may influence the motion (velocity and elevation) of waves during the run-up phase, before flooding phase begins [34] [35].

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 38	di 52
--	--	------------------	----------------------	-------------------	-----------------

8.3.4 Data on building structures

The as-is concrete classes used for the construction of the safety related structures should be verified on the basis of existing plant specific tests and industry standards for concrete. Either destructive or non-destructive methods may be used.

The data collected of all significant load bearing members, instead of the original design data, should be used for further analyses and capacity evaluations.

If there is significant deviation from the design values, the cause of this deviation and its consequences should be investigated: moreover actual material properties, which are mainly concrete and steel should be adopted.

The analyses of the reinforcement steel, as an example, rebars, tendon and reinforcing plates, penetrations and anchorage, should include both mechanical properties and detailing (e.g. size of reinforcement bars, placement, geometric characteristics, concrete cover, distances between reinforcement bars).

Ageing effects should be evaluated for concrete building in order to detect the presence of cracks, effects of erosion/corrosion and surface damage, degree of carbonization, thickness of concrete cover and degree of degradation of foundation below grade due to environmental condition (e.g. chlorides or other corrosive contaminants present in groundwater).

8.3.5 Data on SSCs, piping and equipment

If design information is inadequate for piping, equipment and their supporting structural systems, analysis and/or testing should be performed to establish their dynamic characteristics and behaviour.

To the aim a representative sample may be sufficient.

9. Safety evaluation of a NPP subjected to tsunami event: Analysis step by step

Step 1: Non linear analysis outline

As already mentioned, while buildings are usually designed for external event resistance using elastic analysis, most will experience significant inelastic deformations under large event like tsunami or earthquake. Modern performance-based design methods require ways to determine the realistic behavior of structures under such conditions.

Enabled by advancements in computing technologies and available test data, nonlinear analyses provide the means for calculating structural response beyond the elastic range, including strength and stiffness deterioration associated with inelastic material behavior and large displacements. As such, nonlinear analysis can play an important role in the design of new and existing buildings facilities, in conventional and nuclear field.

Nonlinear analyses involve significantly more effort to perform and should be approached with specific objectives in mind.

Typical instances where nonlinear analysis is applied in structural engineering practice are: (1) to assess and design retrofit solutions for existing plants; (2) to support the design new SSCs with materials, systems or other features that do not conform to current building code requirements; (3) to assess or re-evalaute the plant performance for specific requirements, like those of the stress tests.

To the aim, the design basis must be clearly defined and agreed upon, according to the significant performance levels to comply, which are a) immediate occupancy, b) life safety

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 39	di 52
--	--	------------------	----------------------	-------------------	-----------------

and c) collapse prevention, and the demand parameters, typically peak forces, stresses and deformations, story drifts, etc..

Nonlinear analyses require thinking about inelastic behavior and limit states that depend on deformations as well as forces. They also require definition of component models that capture the force-deformation response of components and systems based on expected strength and stiffness properties and large deformations.

Depending on the structural configuration, the results of nonlinear analyses can be sensitive to assumed input parameters and the types of models used.

It is advisable to have clear expectations about those portions of the structure that are expected to undergo inelastic deformations and to use the analyses to (1) confirm the locations of inelastic deformations and (2) characterize the deformation demands of yielding elements and force demands in non-yielding elements.

In this regard, capacity design concepts are encouraged to help ensure reliable performance. While nonlinear analyses can, in concept, be used to define/trace structural behavior up to the onset of collapse, this requires sophisticated models capable to capture the highly nonlinear response and phenomena characterizing the dynamic behaviour of structures approaching the collapse.

In this respect it is important to remember that the collapse load represents a limit load beyond which damages will occur and it does not determine a sudden loss of integrity and failure of structure.

Finally, since the uncertainties in calculating the demand parameters increase as the structure becomes more nonlinear, for design purposes, the acceptance criteria should limit deformations to structures of known behavior, where sudden strength and stiffness degradation does not occur or is predictable.

Step 2: Definition of methodology

Appendix A, “General Design Criteria for Nuclear Power Plants,” to Title 10, Part 50, “Domestic Licensing of Production and Utilization Facilities,” to the Code of Federal Regulations (10 CFR Part 50), Criterion 2, “Design Bases for Protection Against Natural Phenomena,” requires, in part, that nuclear power plant relevant components for safety must be designed to withstand the effects of natural phenomena (such as earthquake, tsunami-flooding, tornado, etc.) without loss of capability to perform their safety functions. Such component systems must also be designed to accommodate the effects of and be compatible with the environmental conditions associated with normal operation and postulated accidents. From the foregoing and with reference to the case study of flooding effects of a tsunami onto a NPP, to evaluate the safety margin and strength “capacity” of an existing nuclear plant, a deterministic approach has been proposed and adopted; the effects caused by water breaking waves loads (ASME approach) along/within the structure are thus calculated.

The deterministic assessment is made possible by means of the numerical evaluation based on the use of the finite element method (FEM codes). Non linear analysis has been also carried out.

Indeed the modelling of structure represents the basis for applying the Substructure approach considered necessary when very complex and/or large structures have to be analysed. It allows to analyse complex structure, like a nuclear power plant, in a simpler way studying each component separately and in an independent way, even if respecting the overall mass and energy balances.

ENEA Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 40	di 52
---------------------------------------	---	-----------	---------------	------------	----------

To correctly address the issues related to the case study of tsunami-flooding, an outer containment building (last safety barrier in Defence in Depth concept) has been considered. The assumptions made have been of: 1) station black out condition, 2) safety systems not operating and 3) plant isolated. Based on that a conservative evaluation has been performed. The main points of the methodological approach, based on the numerical FEM evaluation, considering appropriate initial and boundary conditions as well as plant geometry and data, are summarized in Figure 9.

The phase of tsunami, which was analysed in this case study, is the flooding phase Figure 10 that begins, after the inundation one, with the run-up of water waves near the shore: the water waves shorten in wavelength and increase in height amplitude.

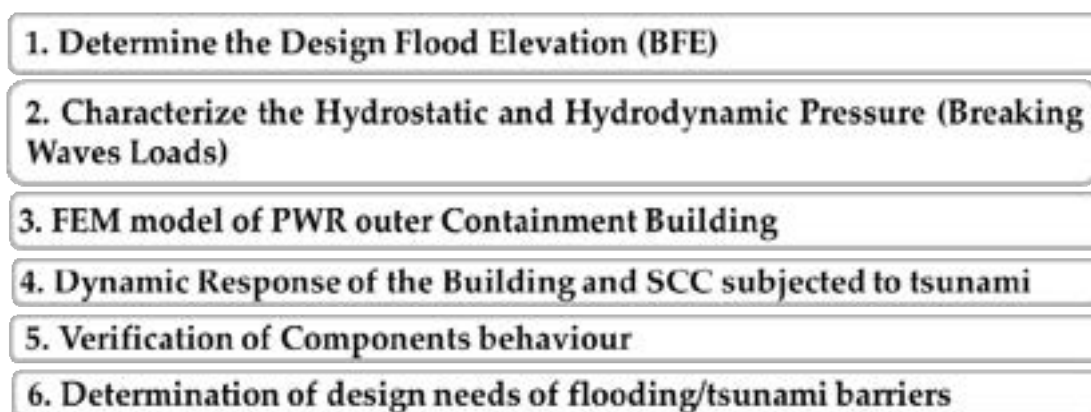


Figure 9 – Methodological approach for tsunami evaluation

The impact and lateral pushing of the waves (“water wall” traveling at high speed) as well as the destructive power of a large volume of water dragging debris and missiles inland are responsible of plant damages (like observed in Fukushima plants).

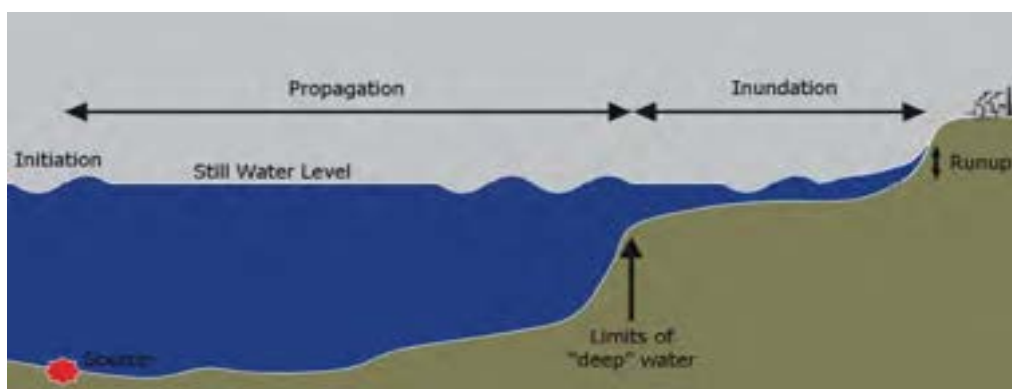


Figure 10 - Tsunami phases

Setp 3: Evaluation of breaking waves loads

Taking into account the scheme represented in previous Figure 9, to determine the effects induced by the impact of tsunami breaking waves, hydrostatic and dynamic pressure values (representative of the tsunami phenomenon) have to be calculated. To the aim, the criteria

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 41	di 52
--	--	------------------	----------------------	-------------------	-----------------

indicated in the ASCE/SEI 7-10 rules [36] have been applied to calculate the initial flooding loads to be used, in turn, as input data in non linear dynamic analyses.

First of all, it was considered the site of NPP as a coastal area of high risk (V-zone [36]). After that, the pressure loads acting on the outer containment building walls surfaces have been calculated on the basis of the assumed flooding breaking-waves height [36] H_b , like:

$$H_b = 0.78d_s \quad (1)$$

where the term d_s indicates the local still-water depth, which may be calculated applying the Eq. 5.4-3 of [36]:

$$d_s = 0.65(BFE - G) \quad (2)$$

G represents the ground level, whilst BFE is the design flood elevation. Afterwards, the maximum pressure (sum of the dynamic and static contributions) and the resultant force of the breaking-waves were calculated, as given by:

$$P_{\max} = C_p \gamma_w d_s + 1.2 \gamma_w d_s \quad (3)$$

$$F_t = 1.1 C_p \gamma_w d_s^2 + 2.4 \gamma_w d_s^2 \quad (4)$$

where γ_w is the water unit weight, equal to 10.05 kN/m^3 for the sea water; C_p the dynamic pressure coefficient, defined in table 5.4-1 of [36], whose value depends on the category of risk associated with the extreme natural events considered, i.e. the flooding and earthquake. Furthermore, the below Figure 11 represents the distribution of hydrodynamic and hydrostatic pressure acting on a vertical wall to be taken into account for a correct representation of the pressure loads along the containment building walls. Figure 11 shows also the different wave elevations to be considered when calculating the pressure loads.

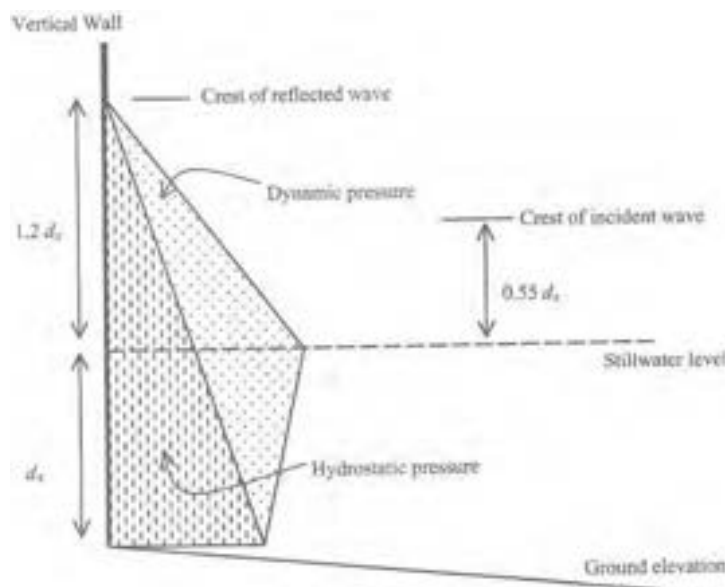


Figure 11 - Wave elevations vs. vertical building wall height [36].

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 42	di 52
--	--	------------------	----------------------	-------------------	-----------------

After having determined P_{max} , the dynamic response of a PWR or BWR containment building, in agreement with the WENRA and International regulatory bodies suggestions [37], can be evaluated.

Step 4: Modelling of a NPP safety relevant structures

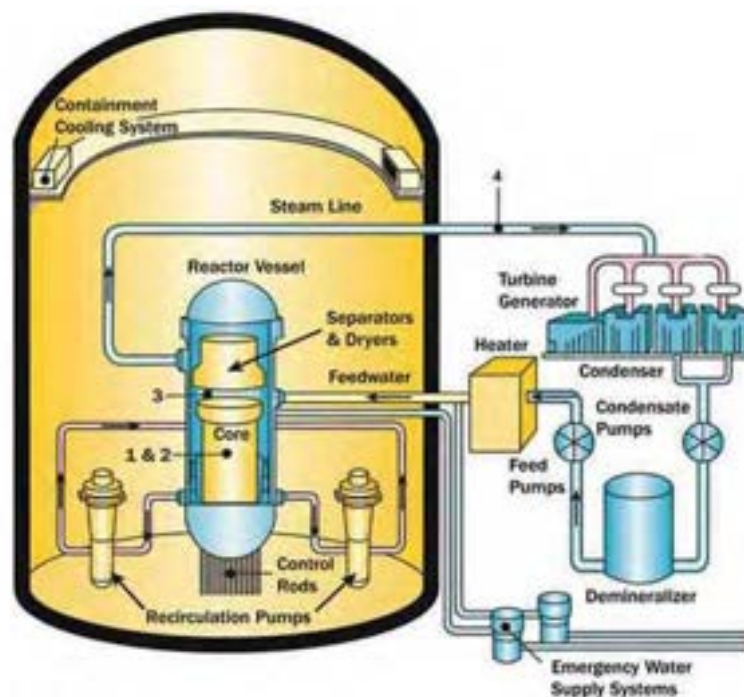
Nuclear power plants are always composed of a number of adjacent structures, so in order to ensure an adequate treatment of the interaction effects among structures, all the most relevant structural components have been considered, in the implemented example BWR model, with their real geometry and material characteristics.

In Figure 12 it is represented a typical scheme of a Boiling Water Reactor (BWR) NPP (courtesy of NRC USA) taken into account.

The containment structure, of about 60 m tall and 42-45 m in diameter, is similar to a standard dry containment and can be designed as either a free standings' steel containment, surrounded by a concrete shield building or as a concrete pressure vessel with a liner.

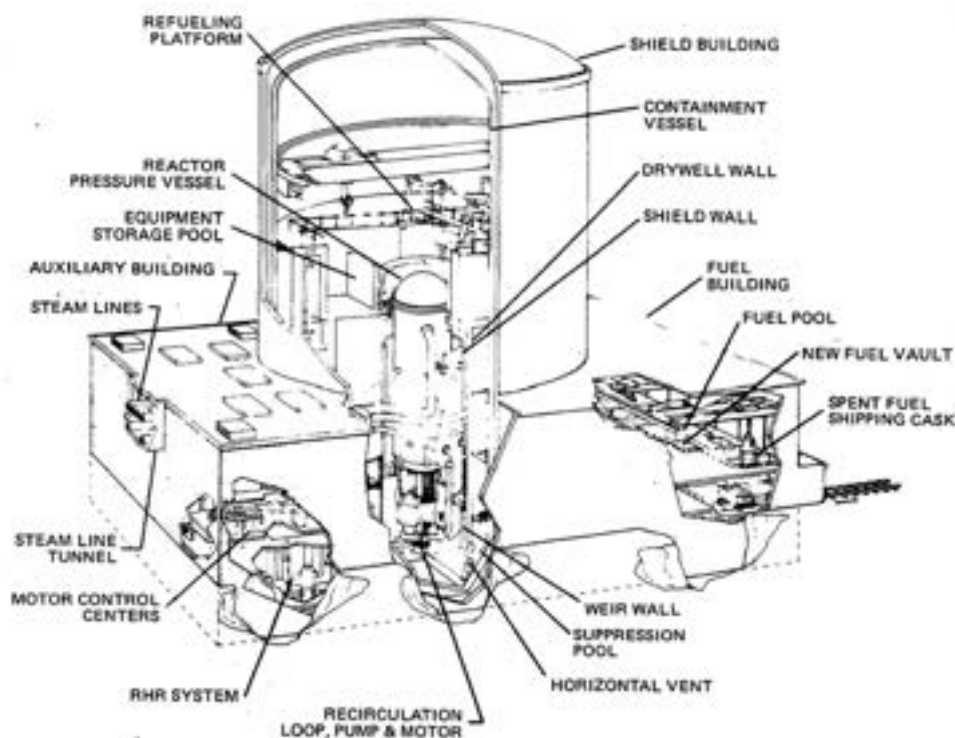
Its general basic features are extensively described in [38] and [39]: the secondary or outer containment, as indicated in [38], completely encloses the primary containment and those components that may be postulated to contain primary system fluid.

It performs no active function; however, its leak tightness is required to prevent any release of radioactive materials from the primary containment.



(a)

	Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. di 43 52
---	----------------------------------	--	------------------	----------------------	-------------------------



(b)

Figure 12 - Scheme of typical BWR NPP

The FE modelling process BWR outer building has required the setting up of appropriate meshes assembled with suitable elements, as for example three-dimensional 20-nodes, (3-D), solid and/or shell isoparametric type elements, available in the used FEM code [40], to represent the spatial discretization of the structure and thus the behaviour of each mentioned structure. The nodal points of the finite element model of the structure are assumed to have three translational degrees of freedom about x, y, and z-axis and three rotational degrees of freedom about x, y, and z-axis.

The mathematical models and the degree of discretization have been chosen such that the natural behaviour of the structure, in the relevant frequency range, could be computed with good reliability.

Horizontal and vertical steel rebars, distributed according to the ASCE rules [41] and ACI standards requirements [42], are spaced in the containment wall thickness in order that the maximum spacing does not exceed 300 mm in the FEM model of the building (made by more than 68.000 element).

In the analyses performed, reinforcing steel rebars were considered embedded in the concrete containment building walls. Moreover rebar thickness has been determined by assuming its cross-sectional area uniformly spread along the respective pitch of the layers.

In Figure 13 it is represented the FEM model of BWR considered.

Non-linear characteristics of concrete and steel have been considered: the behaviour of concrete was assumed to be linear elastic up to the point of failure, while the steel reinforcement members as elastic-perfectly plastic. In addition, the damaging and failure processes of material constituting the containment building have been taken into account.

ENEA Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 44	di 52
---------------------------------------	---	-----------	---------------	------------	----------

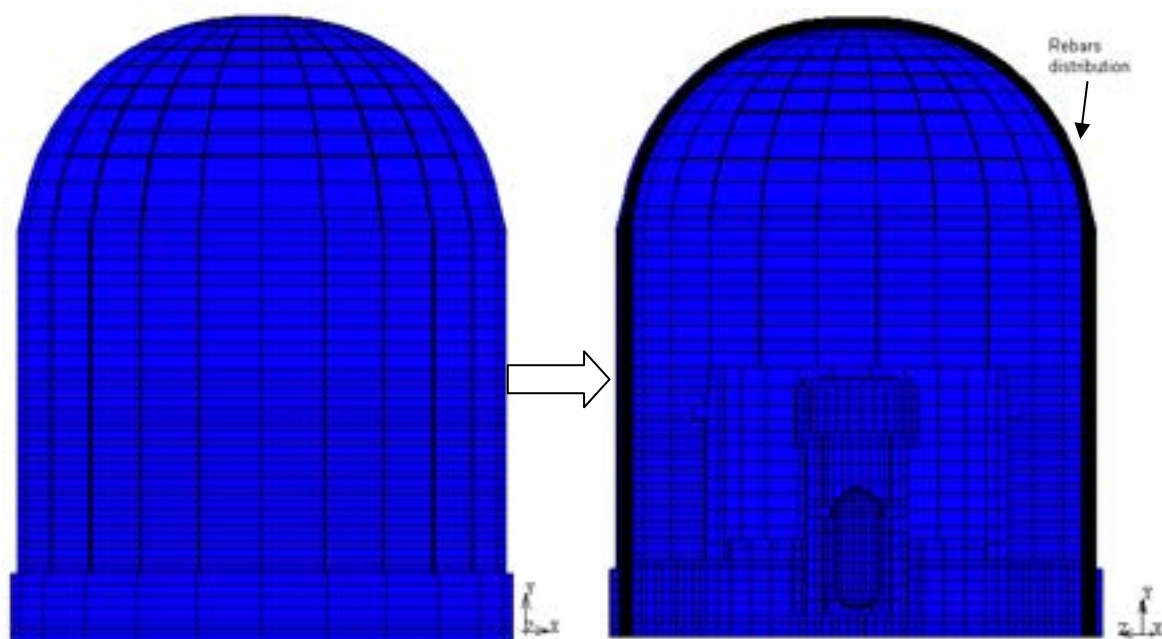


Figure 13 - Containment building FEM model view (a) and section (b)

Furthermore a proportional damping for each structure, according to the Equivalent Rayleigh damping has been considered: the dissipation of energy is represented with decoupled equations that approximate the damping matrix by a linear combination of the mass and stiffness matrices. The damping matrix $[C]$ is therefore:

$$[C] = \alpha [M] + \beta [K] \quad (5)$$

In Eq. 5 $[M]$ is the mass matrix of the structure; $[C]$ the damping matrix of a physical system and $[K]$ the stiffness matrix of the structure. α and β are predefined constants.

A direct integration method employing a finite difference approximation is used to obtain structural responses according to the considered material behaviour.

The unconditionally stable Newmark's implicit integration method is adopted for the solution of the dynamic equilibrium equations. An unconditionally stable average acceleration integration scheme is adopted with $\gamma=0.5$ and $\beta=0.25$, where γ and β are the parameters used to control the accuracy and stability of the method of integration. The Newton Raphson iteration scheme is used to carry out iterative corrections to the displacement increment for solving the non-linear equations of equilibrium.

A validation analysis has been (to be) carried out to evaluate the performance of the MSC©MARC code and the reliability of simulation methodology used so far. The analyses have been performed with different (1) mesh refinements and 2) elements types. The results indicated that a relatively insensitiveness to different mesh sizing, while the choice of a 3D element type allow to obtain a lesser discrepancy (that was at maximum 10%) in the results.

Subsequently the dynamic behaviour of containment structure was simulated by performing nonlinear analyses for a duration of 0.5 s (time step = 0.001 s) (time interval considered sufficient to represent the effects of water breaking loads), and assuming large strain (Lagrangian formulation).

ENEA Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 45	di 52
---------------------------------------	---	-----------	---------------	------------	----------

The directions of the application of the pressure loads, representative of the breaking waves, as shown in Figure 14, have been assumed to be orthogonal and tangential to the outer containment walls.

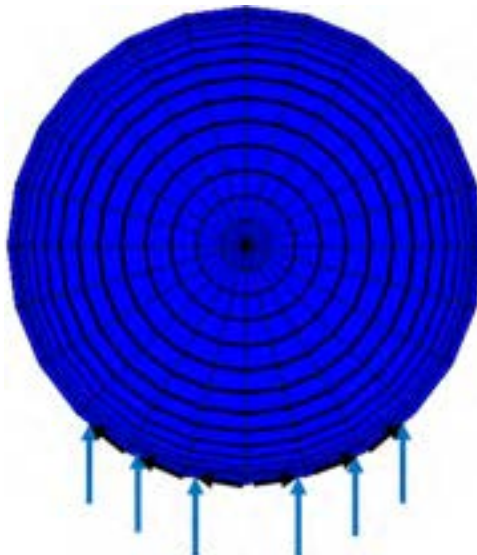


Figure 14 - Directions of the pressure breaking-wave

Step 5: Results obtained

The results obtained, mainly in terms of stress and displacement, for several breaking wave heights, in view of the assumptions made and containment building geometry considered, confirmed that the calculated stress level is strictly dependent on the wave height (though not linearly) and on the failure and/or damaging processes. These latter are related to the stress level of containment building wall which arises during the flooding transient (the pressure load has been calculated in previous Step 3).

In what follows, only the results obtained for a hypothetical wave height of 20 m will be presented, since it was the most severe accident scenario analysed.

The normal stresses in the concrete in the direction of loading, shown in Figure 15, has been found to be under compression in the waves impact region, while away (in longitudinal and/or circumferential directions) from this zone tensile stresses were also observed.

This is due to the fact that the containment building, when subjected to a high localized compression loads, develops outwards bulging in the surrounding area. However, in general, the compressive stresses have been found to be higher and predominant compared to the tensile ones in the outer surface.

The stress values indicated that the containment begins to suffer local damages/failure phenomena: even if suffering void nucleation of cracking its walls, jointly with the rebars, it has/retains sufficient strength capability to withstand the waves impact and guarantee the overall structural integrity.

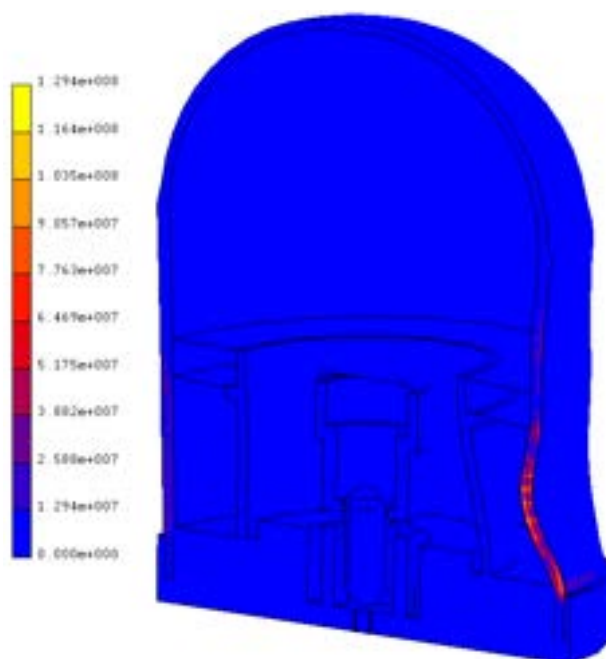
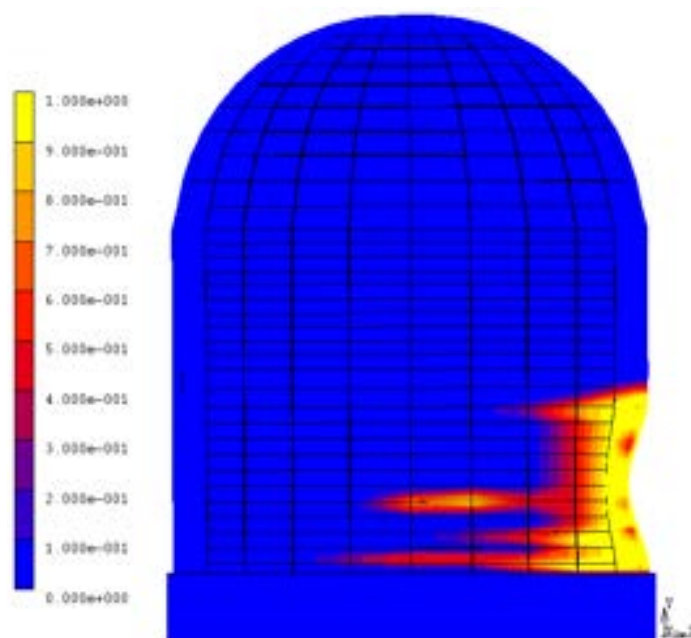
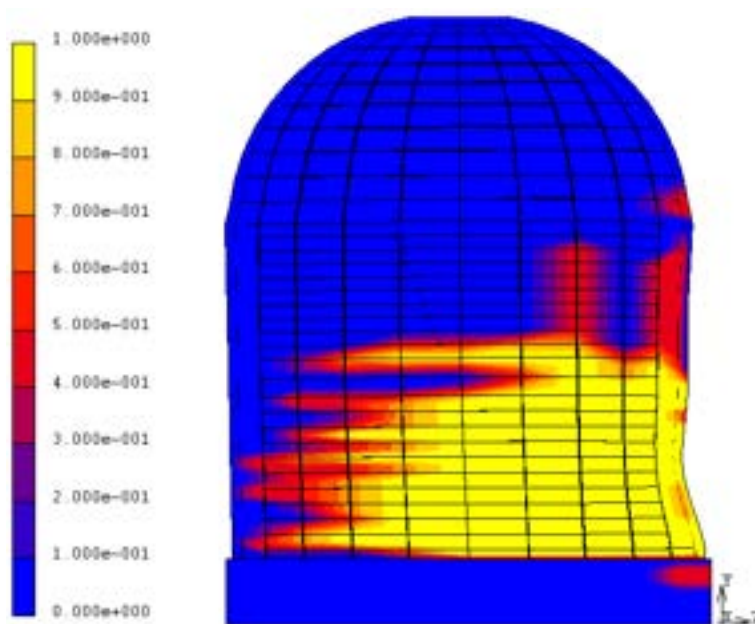


Figure 15 - Von Mises stress distribution for BFE=20 m.

Although the damaged area seems quite wide (Figure 16), it involves only the elements of the containment walls on the outer surface; in addition for wave elevation less than 10 m, the containment structure did not experience such a large area of damage. No plastic strain was instead observed in the reinforcing steel rebars.



(a)



(b)

Figure 16 - Overviews of the damages of the outer surface of containment building in the case of BFE=10 (a) and BFE=20 m (b)

The maximum displacement values were observed in the area of the waves impact, ranging from 5 to 15 cm depending on the elevation of BFE.

The data obtained may be used to evaluate more accurately the fragility of containment building.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 48	di 52
--	--	------------------	----------------------	-------------------	-----------------

10. Conclusions

This study purports to address the NPP risk evaluation related to external events, as emerging from the Fukushima accident: to this aim the risk informed approach is being proposed to tackle the issue.

A risk-informed regulatory approach implies that risk insights be used as supplement of deterministic information for safety decision-making purposes. In this view, the use of risk assessment techniques is expected to lead to improved safety and a more rational allocation of the limited resources available.

The IDPSA approach, here described, promotes the use of the combination of PSA and DSA on the merit of improved safety.

On the other hand, it is recognized that, as far as new tools are being implemented, some open issues still remain to be addressed and conveniently worked out. For instance, in order for the risk-informed decision making process to be effective, the adequate representation and treatment of uncertainties that affect both the deterministic safety analyses and the risk assessments is mandatory.

Being not a part of every-day practice of safety assessment and decision making process, the need for methodology advance to facilitate IDPSA advanced tool deployment into industrial practice comes up among the researchers in nuclear safety.

The issues related to the connection between PSA and DSA are addressed, some significant pilot applications, in the form of accident sequence definition and assessment are proposed as case studies, for verification and implementation of the approach, as a step towards development of best practice guidelines.

In particular the LOOP/SBO (Loss Of Offsite Power/Station BlackOut) caused by external event, as typhoon and tornado, is analyzed both on the deterministic perspective and on the probabilistic standpoint.

Specifically the comprehensive review of the treatment of the loss of AC power in the PRA, identified some technical issues and guidance for the implementation of the probabilistic analysis:

- The implementation should provide greater consistency in LOOP modeling treatment for routine plant operational and regulatory applications.
- The need for additional technical work is identified with respect to SBO frequency and duration, plant recovery potential and operation of AC independent decay heat removal systems
- The importance of the uncertainties in the assessment process

With reference instead to the DSA, a numerical methodological approach has been adopted to “quantify” the safety margin of BWR simplified structure, according to the stress tests requirements.

The treatment allowed to simulate, with a good reliability the water waves inundation phase and, in particular, the effects of the water breaking waves (interms of pressure values, calculated accordingly to the ASCE-SEI rules).

So the overall plant performance, considering the assumptions of safety systems not operating, plant isolated and in station black-out conditions was evaluated.

The preliminary results obtained highlighted that the resulting stress values were localized in the region of containment subjected to the water impact. The concrete was placed under compression as a consequence of the waves impact, while away from this part of the outer

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 49	di 52
--	--	------------------	----------------------	-------------------	-----------------

surface (in longitudinal and circumferential directions) of the containment building tensile stresses were also observed, mainly due to the development of bulging in the surrounding area.

Although the containment building is suffering localized high stress values and material damaging seemed to occur, particularly in the case of high BFE, no loss of structural integrity occurs.

Finally further developments are necessary to analyze deeply the aspects of the hydrodynamic behaviour of water waves (e.g. influence of building shape, secondary and splashing waves, etc.), in order to correctly evaluate the performances of containment building, in form of displacement and stresses, to be used to determine fragility curves of plant SSCs, that is the main goal of IDPSA itself.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 50	di 52
--	--	------------------	----------------------	-------------------	-----------------

References

- [1] Proceedings of the Deterministic/probabilistic safety analysis workshop October 2011, Research report VTT-R-07266-11
- [2] M. Cepin, Probabilistic Safety Assessment and Risk-Informed Decision Making in Nuclear Power, Edited by Pavel V. Tsvetkov, ISBN 978-953-307-110-7, September 2010
- [3] E. Zio, Risk-informed regulation: handling uncertainty for a rational management of safety, Nuclear Engineering and Technology, Vol.40 No.5, August 2008
- [4] J. Devooght and C. Smidts, "Probabilistic Reactor Dynamics I: The theory of continuous event trees," *Nucl.Sci.Eng.*, 111, 229-240 (1992)
- [5] J. Devooght and C. Smidts, "Probabilistic reactor dynamics - III: A framework for time dependent interaction between operator and reactor during a transient involving human error," *Nucl.Sci.Engng.*, 112, 101-113 (1992)
- [6] B. Tombuyes , T. Aldemir, "Dynamic PSA of Process Control-Systems Via Continuous Cell-To-Cell-Mapping," *Probabilistic Safety Assessment and Management PSAM3*, 1541-1546, Elsevier, New York (1996)
- [7] B. Tombuyses and T. Aldemir, "Continuous Cell-to-Cell Mapping," *J.Sound and Vibration*, 202, 395-415 (1997)
- [8] Amendola , G. Reina, "DYLAM-1, A Software Package for Event Sequence and Consequence Spectrum Methodology", EUR-924, CEC-JRC ISPRA, Commission of the European Communities, Ispra, Italy (1984)
- [9] G. Cojazzi, "The DYLAM Approach to the Dynamic Reliability Analysis of Systems," *Reliab.Engng & System Safety*, 52, 279-296 (1996)
- [10] C. Acosta , N. Siu, "Dynamic Event Trees in Accident Sequence Analysis: Application to Steam Generator Tube Rupture," 41, 135-154,(1993)
- [11] H. Kae-Sheng and A. Mosleh, "The Development and Application of the Accident Dynamic Simulator for Dynamic Probabilistic Risk Assessment of Nuclear Power Plants," *Reliab.Engng & System Safety*, 52, 297-314 (1996)
- [12] R. Munoz, E. Minguez, E. Melendez, J. M. Izquierdo, and M. Sanchez-Perea, "DENDROS: A Second Generation Scheduler for Dynamic Event Trees," J. M. Aragonés, C.Ahnert, and O. Cabellos .(Eds.) Senda Editorial, S. A., Madrid, Spain (1999)
- [13] T. Aldemir, "Computer-Assisted Markov Failure Modeling of Process Control Systems," *IEEE Transactions on Reliability*, R-36, 133-144 (1987)
- [14] T. Aldemir, "Utilization of the Cell-To-Cell Mapping Technique to Construct Markov Failure Models for Process Control Systems," G. Apostolakis (Eds.), 1431-1436, Elsevier, New York (1991)
- [15] Y.Vorobyev, P. Kudinov, Development and Application of a Genetic Algorithm Based Dynamic PRA Methodology to Plant Vulnerability Search, ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Wilmington, NC, March 13-17, 2011.
- [16] M. Kloos, E. Hofer, and ET AL, "Dynamic Event Trees for Probabilistic Safety Analysis", GRS, Garsching, Germany (2004)
- [17] E. Hofer, M. Kloos, B. Krzykacz-Hausmann, J. Peschke, and M. Woltereck, "An approximate epistemic uncertainty analysis approach in the presence of epistemic and aleatory uncertainties," *Reliab.Engng & System Safety*, 77, 229-238 (2002)
- [18] S. Guarro, M. Yau, and M. Motamed, "Development of Tools for safety Analysis of Control Software in Advanced Reactors", NUREG/CR-6465, U.S. Nuclear Regulatory Commission, Washington, D.C. (1996)

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 51	di 52
--	--	------------------	----------------------	-------------------	-----------------

- [19] M.Yau, Dynamic Flowgraph Methodology for the Analysis of Software Based Controlled Systems, Ph.D. Thesis, University of California, Los Angeles, California (1997)
- [20] T. Matsuoka , M. Kobayashi, "An Analysis of a Dynamic System by the GO-FLOW Methodology," P. C. Cacciabue , I. A. Papazoglou .(Eds.), 1547-1436, Elsevier, New York (1991)
- [21] T. Matsuoka And M. Kobayashi, "GO-FLOW: A New Reliability Analysis Methodology," *Nuclear Science and Engineering*, 98, 64-78 (1988)
- [22] Hakobyan, R. Denning, T. Aldemir, S. Dunagan, and D. Kunsman, "A Methodology for Generating Dynamic Accident Progression Event Trees for Level 2 PRA," B034, 1-9,(2006)
- [23] Hakobyan, T. Aldemir, R. Denning, S. Dunagan, D. Kunsman, B. Rutt, and U. Catalyurek, "Dynamic generation of accident progression event trees," *Nuclear Engineering and Design*, 238, 3457-3467 (2008)
- [24] Proceedings of the IDPSA 2012, Integrated Deterministic-Probabilistic safety analysis workshop November 2012, Research report VTT-R-08589-12
- [25] P. Baranowsky et al., "Best Practices for Treatment of LOOP in PRAs", Proceedings of PSAM10, International Probabilistic Safety Assessment and Management Conference, Seattle, Washington, (USA), 7-11 June 2010
- [26] NUREG-1032, Evaluation of Station Blackout Accidents at Nuclear Power Plants, NRC, May 1988.
- [27] IAEA, Evaluation of seismic safety for existing nuclear installations, IAEA safety standards series No. NS-G-2.13, 2009.
- [28] N. M. Newmark, A method of computation for structural dynamics, Journal of Engrg. Mech. Div., ASCE, 121, 45-64, 1956
- [29] N. M. Newmark and W. J. Hall, Development of criteria for seismic review of selected nuclear power plants, NUREG CR0098, U.S. Nuclear Regulatory Commission, Washington, D.C., 1978.
- [30] M. Khatib-Rahbar, Deterministic & Probabilistic Safety Assessment, How much do we know about the risk associated with operation of nuclear power plants? Energy Research, Inc., Ecole Normale Supérieure, Paris, 14-16 November 2011
- [31] G. Forasassi, R. Lo Frano, V. Baudanza, Preliminary evaluation of a severe flooding effects in an innovative SMR, 2nd International Technical Meeting on Small Reactors, Ottawa, Canada, November 7-9, 2012.
- [32] US NRC, Tsunami Hazard Assessment at Nuclear Power Plant Sites in the United States of America, Final Report, March 2009.
- [33] V. Baudanza, R. Lo Frano, G. Forasassi, Preliminary evaluation of the flooding effects on an existing PWR, Proceedings of the ASME 2013 Pressure Vessels & Piping Division Conference, PVP2013, July 14-18, 2013, Paris, France.
- [34] F.I. Gonzalez, E. Bernard, P. Dunbar, E. Geistis et al., Scientific and technical issues in tsunami hazard assessment of nuclear power plant sites. NOAA Tech. Memo. OAR PMEL-136, Pacific Marine Environmental Laboratory, Seattle, WA, pp.125, 2007.
- [35] F. Leone, F. Lavigne, R. Paris et al., A spatial analysis of the December 26th, 2004 tsunami-induced damages: Lessons learned for a better risk assessment integrating buildings vulnerability, Applied Geography, 31, 363- 375, 2011.
- [36] ASCE Standard, Minimum design loads for buildings and other structures, ASCE/SEI 7-10, 2010.

 Ricerca Sistema Elettrico	Sigla di identificazione ADPFISS – LP1 - 005	Rev. 0	Distrib. L	Pag. 52	di 52
--	--	------------------	----------------------	-------------------	-----------------

- [37]ENSREG, Stress tests performed on European nuclear power plants, Stress Test Peer Review Board, 2012.
- [38]US NRC, Standard Technical Specifications–General Electric Plants (BWR/6) (NUREG-1434, Revision 4), 2012.
- [39]IAEA, Design of Reactor Containment Systems for Nuclear Power Plants SAFETY GUIDE No. NS-G-1.10, 2004.
- [40]MSC©Software, MSC.MARC user’s guide, 2010.
- [41]ASCE Standard, Minimum design loads for buildings and other structures, ASCE/SEI 7-10, 2010.
- [42]American Concrete Institute, Code Requirements for Nuclear Safety-Related Concrete Structures, ACI Standard 349-01 and Commentary, 2001.