Proceedings of the
1st NARSIS Workshop

Training on
Probabilistic Safety Assessment
for Nuclear Facilities

September 2-5, 2019

Warsaw University of Technology
Poland

ACKNOWLEDGEMENTS

These proceedings and each publication were prepared in the frame of NARSIS Project, that has received funding from the Euratom research and training programme 2014-2018 under Grant Agreement No. 755439.

We would like to thank the European Nuclear Education Network (ENEN) Association for providing 20 grants from the ENEN+ Project to students and young researchers. This funding played an important role in the success of the workshop.

We would like to acknowledge the Centre for Innovation and Technology Transfer Management of Warsaw University of Technology for providing a facility well suited for the workshop.

Finally, we are grateful to all the authors involved in the preparation of these proceedings.

TABLE OF CONTENTS

ABBREVIATIONS

AFW Pumps	Auxiliary Feedwater
AOO	Anticipated Operational Ocurrences
ASME	American Society of Mechanical Engineers
ASN	French Authority for Nuclear Safety
BI	Birnbaum Importance
BN	Bayesian Networks
BNI	Basic Nuclear Installations
CBD	Conditional Probability Distributions
CCDP	Conditional Core Damage Probability
CCF	Common Cause Failures
CDF	Core Damage Frequency
CFD	Computational Fluid Dynamics
DBA	Design Basis Accidents
DC	Direct Current
DCH	Direct Containment Heating
DEC	Design Extension Conditions
DFC	Diagnostic Flow Chart
DG	Diesel Generator
ECFC	Event and Causal Factor Charting
EDP	Engineering Demand Parameter
EOP	Emergency Operation Procedure
F-V	Fussell-Vesely
FA	Frequency Analysis
FE	Finite Element
FSAR	Final Safety Analysis Report
HI	Historical Information
HPES	Human Performance Enhancement System
HPME	High Pressure Melt Ejection
HSS	High-Safety-Significant
IAEA	International Atomic Energy Agency
IDP	Integrated Decision-making Panel
IEEE	Institute of Electrical and Electronics Engineers
JPD	Joint Probability Distribution
LERF	Large Early Release Frequency
LHS	Latin Hypercube Sampling
LOCA	Loss Of Coolant Accident
LSS	Low-Safety-Significant
MCCI	Molten Core-Concrete Interactions
MCS	Minimal Cut Sets
MORT	Management Oversight and Risk Tree Analysis
NNS	Non-Nuclear Safety
NPPs	Nuclear Power Plants
NR	Narrow Range
NRC	Nuclear Regulatory Commission
PCT	Peak Clad Temperature
PGA	Peak Ground Acceleration

PORV	Pressurizer Power Operated Valves
PoT	peak- over-threshold
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RAW	Risk Achievement Worth
RCS	Reactor Coolant System
RFA	Regional frequency analysis
RFS	Reference Flood Situation
RHR	Residual Heat Removal
RISC	Risk-Informed Safety Classifications
RPV	Reactor Pressure Vessel
RRW	Risk Reduction Worth
RWST	Refueling Water Storage Tank
SA	Spectral Acceleration
SAG	Severe Accident Guidelines
SAMG	Severe Accidents Management Guidelines
SBO	Station Black Out
SC	Safety Classes
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SPH	Smoothed-Particle Hydrodynamic
SSCs	Structures, Systems and Components
TC	Thermo-Couples
TSC	Technical Support Center
UQ	Uncertainty Quantification
USNRC	United States Nuclear Regulatory Commission
VVUQ	Verification, Validation, and Uncertainty Quantification

NARSIS Workshop
Training on Probabilistic Safety Assessment for Nuclear Facilities
International Training Course
Warsaw, Poland, September 2-5, 2019

I Introduction to External Hazard Events: Background, Parameters and Interactions

James DANIELL
Geophysical Institute, Karlsruhe Institute of Technology (KIT)
Hertzstrasse 16
76187, Karlsruhe, Germany
James.daniell@kit.edu

Andreas SCHAEFER, Hugo WINTER, Vito BACCHI, Lucie PHEULPIN
KIT, EDF UK, IRSN, IRSN
Andreas.schaefer@kit.edu, hugo.winter@edfenergy.com, vito.bacchi@irsn.fr, lucie.pheulpin@irsn.fr

ABSTRACT

This paper sets the outline to the workshop topic by providing a background and investigation into the following questions:

1) A background to the event types which can hit nuclear power plants (NPPs)
2) What type of events can occur in Europe?
3) How do we model hazards and their interactions?

I.1 INTRODUCTION

The different external hazard events which can impact nuclear power plants (NPPs) are complex and numerous. ASAMPSA_E (2014) [1] identified 81 external hazard event types which can impact a plant. These types of interactions can occur as single events or combinations can occur as cascades or coinciding events. The influence of natural hazard types upon one another can be presented in various interactions:

1) Directly via inducing the second hazard;
2) Common root cause (causally correlated), and some have little correlation with the others (i.e. volcanoes with heatwaves);
3) Mutually exclusive (i.e. high water level and low water level);
4) Coincidental hazards (events which occur simultaneously but are independent).

For these four types of multi-hazard relationships, different temporal and spatial settings are needed for the investigation.

I.2 BACKGROUND TO POSSIBLE EVENT TYPES

Within D1.1 of the NARSIS project [2], a significant number of methodologies were described in terms of external hazards characterisation such as IRDR DATA and [1]. Both have the same broad scale definitions with slight differences in the depth of characterisation of external hazards such as seen in Table I-1 and Table I-2.

Table I-1: Different classes of external hazards

Family	Geophysical			Meteorological					Hydrological			Climatological			Biological			Extraterrestrial	
Main Event	Earthquake	Mass Movement	Volcanic Activity	Convective Storm	Extratropical Storm	Extreme Temperature	Fog	Tropical Cyclone	Flood	Landslide	Wave Action	Drought	Glacial Lake Outburst	Wildfire	Animal Incident	Disease	Insect Infestation	Impact	Space Weather

Table I-2: Different external hazards and their parameters

Disaster Type	Parameters
Storm Surge, Tsunami, Flood (Pluvial and Fluvial)	Water depth (m), velocity (m/s), and energy, flow, debris metrics, sediment transport, duration
Earthquake	Intensity, and shaking footprint; Ground motion (Sa, Sv, Sd + 100s of other parameters)
Landslide	Debris volume, displacement
Volcano	Tephra quantity (kPa), pyroclastic flow, lahar flow
Hail/Storm	Pressure, Hail track and hail size (mm), Reflectivity (dBz), Kinetic Energy, kA (current), duration
Wind, Tornado, Lightning	Pressure, Wind speed (gust, sustained, height) Vorticity, Missile speeds, Electric current
Rainfall	Intensity, frequency, duration curves
Extreme temperature, bushfire	Temperature, wind speed, heat output, energy

I.2.1 Temporal Scales and Interactions

These types can then be broken down into 81 typologies (or more within each of these). This means that there are many external hazards which can impact a plant with different interactions as per [1]. Important are the temporal overlaps of such events (Figure I-1) which have been studied in [3] as per the figure below when looking at the correlations of such events.

Different measurements are used for each event type in practice with the following only being a small subset of the possible parameters for each hazard. Each hazard parameter comes with positives and negatives with the most important characteristic being often their correlation to damage seen empirically, and what can be readily measured.

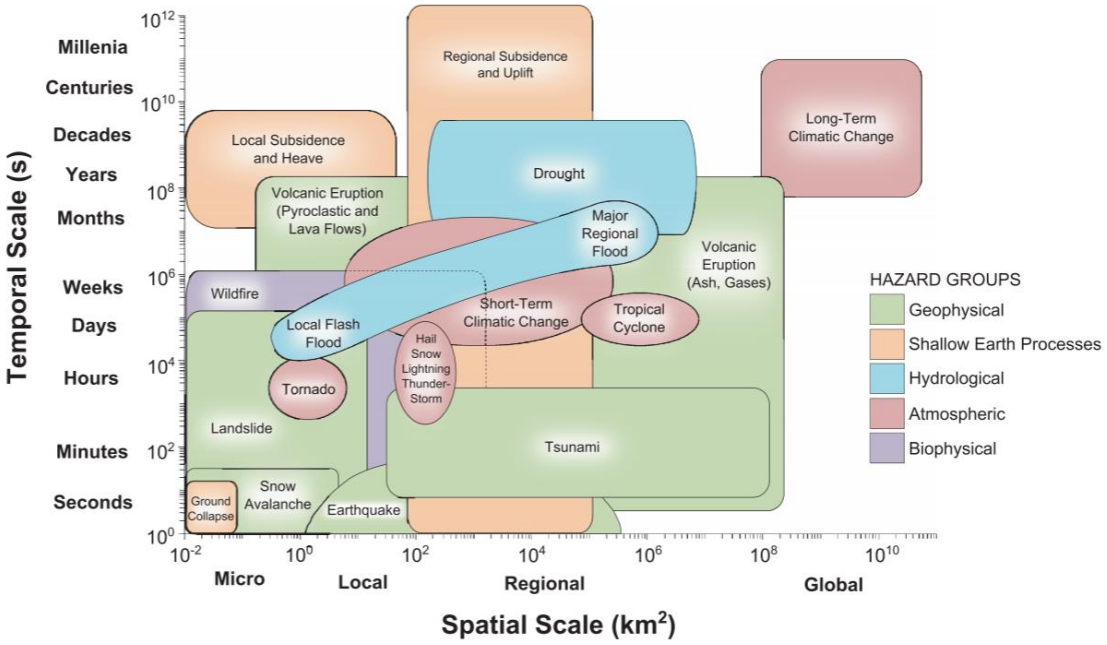


Figure I-1: Temporal Scales of disaster typologies (Gill and Malamud, 2014 - [3])

I.2.2 What NPPs could this impact?

The sites where nuclear power plants are in use were removed from the analysis within NARSIS (Figure I-2), but full lists are available at nucleus.iaea.org (i.e. where both active and non-active units are present). The reduction of sites for the workshop was done given that the operating sites have more extensive examination, and likely more details than we can glean from public data, thus it is not the purpose to disagree with such analysis. Removing some of the never started Spanish plants such as Regodola yields in total 67 sites housing 86 units across Europe.

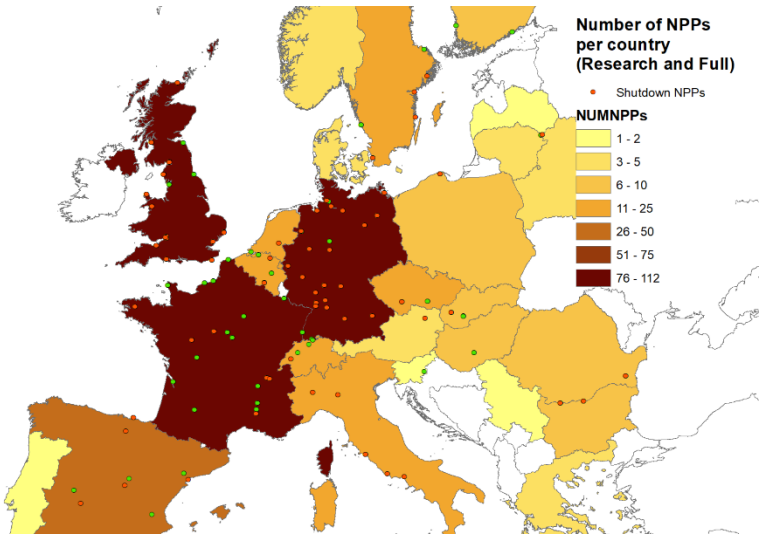


Figure I-2: Locations of identified NPPS, with countries shaded by number of NPPs. Red locations are where at least 1 decommissioned, shut down or suspended unit or NPP exists.

I.3 GEOPHYSICAL HAZARDS

I.3.1 The case of Kaikoura: knowledge as to what is possible

In the Kaikoura earthquake in 2016 in New Zealand, over 21 faults ruptured in 3 minutes, with stress release changing what had been known before the event as to what could occur within a singular event [4] [5]. Very detailed singular fault source models failed in this case to determine the ground motion expected from such an event. This would suggest that distributed area models and greater emphasis on area sources and smoothed models and that over-engineered models should be used with caution. For NPPs, the same has been true for many years with different combinations of sources being used and often transposed to the site. This shows the need for use of elicitation processes such as in the PEGASOS project of 2009.

I.3.2 Earthquake Shaking

Earthquake shaking is most commonly modelled using Probabilistic Seismic Hazard Assessment taking into account all possible area and fault sources to determine the various probabilities. Within Europe there are a number of national and international assessments which have been done with the most common being that of the SHARE model from 2013 [6] (Figure I-3) and the subsequent updates for 2020. Detailed site-specific interactions are needed. In addition, spatial correlation of parameters as well as other measures of uncertainty are required.

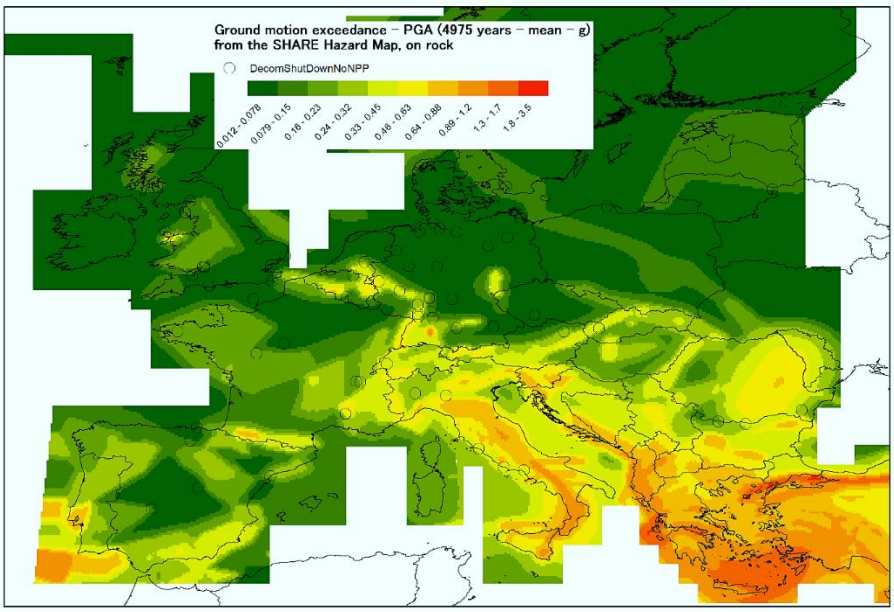


Figure I-3: Spatial distribution of average expected ground motions with a return period of 5000 years based on the SHARE model

The process is usually as follows:

1) Import of historic earthquake data and source model (zones and faults);
2) Computing of data completeness and declustering of earthquake catalogue;
3) Selection of fault and source model;
4) Selection of Ground Motion Prediction Equations (GMPE) and ground motion parameters;

5) Calculation of ground motion through logic tree analysis;
6) Estimation of site and topographic effects;
7) Stochastic calculation of a model catalogue for x years of events;
8) Ground motion sensitivity analysis and secondary effect analysis with combination into the analysis;
9) Checks within the Probabilistic Safety Assessment (PSA) for the parameters used.

I.3.3 Tsunami

Two of the main NPP interactions in the past have been from tsunamis with the 2004 Indian Ocean tsunami impacting Madras (shutdown) and Kalpakkam (under construction), as well as the 2011 Tohoku earthquake at Fukushima with earthquake followed by tsunami. Tsunami analyses within Europe have generally relied on the same source modelling as described in [7] with the use of stochastic slip distributions (Figure I-4), and wave modelling. Within Europe, two types of modelling have been used – deterministic and probabilistic (Figure I-5).

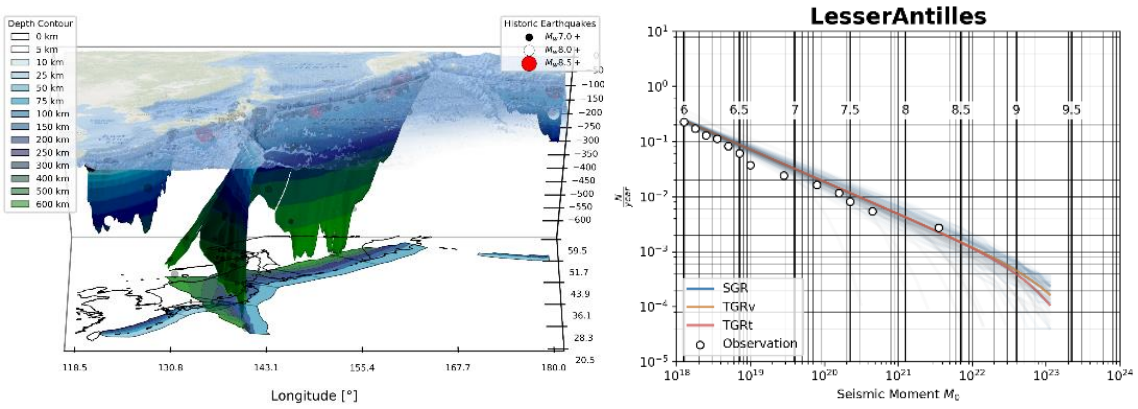


Figure I-4: 3D models of fault zones observed (left) vs. modelled (right) G-R relations

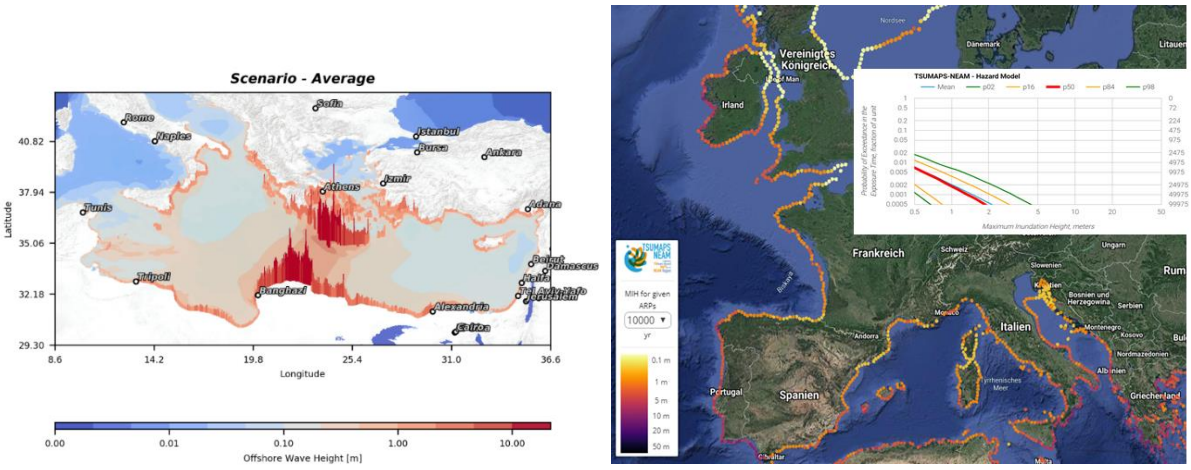


Figure I-5: Deterministic (left) vs. Probabilistic (right) results for tsunami in Europe

Deterministic which consists of single scenario modelling which allows for coping with uncertainties associated with adequacy of safety features, all conceivable hazard events examined and many safety margins. The other probabilistic method uses hazard curves which

are produced using the properties of past hazards, earth dynamics, and various statistical relationships to characterise the temporal probability of an event occurring. Combinations of events, residual risk and very rare events can be examined through fault trees for the probabilistic results. The Tsumaps-NEAM project has done a probabilistic tsunami hazard model for Europe [8]. Other work such as the TANDEM and ASTARTE projects and TsuPy give various models within Europe.

I.4 HYDROMETEOROLOGICAL HAZARDS

I.4.1 Usual methodology for analysis of hydrometeorological hazards

There exist a number of hydrometeorological datasets for station data across Europe. Station data is required in order to develop the extreme value statistics in order to derive the possible wind speeds, temperatures, flows or other parameters at the site. These methods usually employ taking a group of close stations to the site in order to derive the most likely correlation of site conditions. It may also be however, that similar stations inside of a certain radius could be used where station heights, aspect and type match well. Most NPP assessments involve some form of extreme value statistical modelling of the different perils, the most common involving annual maxima or the PoT (peak- over-threshold) methods. Some of the best datasets include ECA&D, GSOD, ESWD and the RAIN project [4]. The problem of completeness and filling of these datasets where there are gaps in reading are the main source of uncertainties.

I.4.2 Flood Modelling

Detailed modelling is employed via the use of flow gauges below and above the site, included then in the riverine flood modelling. Flow modelling is generally used rather than direct historic regression of water heights, using rainfall and other parameters. These approaches still rely on station data for the rainfall, thus the points made above with completeness of station data play a major role as to the quality of fit expected and the uncertainties in the analysis.

Depending on the country in Europe there are varying levels of flood modelling employed for different locations. Some employ 2D-3D modelling on various reaches from engineering companies, whereas there are some, which employ much simpler modelling. The changes in upstream conditions will always affect the site, thus various control structure changes often change significantly the chance for a flood over time. The GRDC houses flow data for Europe.

Although global models employing broad scale approaches exist such as AQUEDUCT and JRC, detailed modelling is done for individual NPPs, but datasets such as the state level maps from Germany (Figure I-6), allow for detailed modelling given the large investment made. During the stress tests from ENSREG, it could be seen that the detailed modelling approach was reasonable.

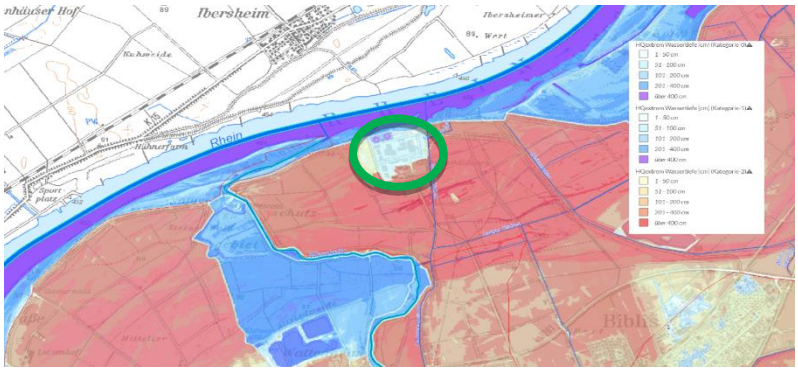


Figure I-6: 1m resolution extreme event (1000-year) flooding at the Biblis NPP site via HLNUG (Hessen State Institute for Environment, Survey and Nature Conservation Flood Portal - [9])

I.4.3 Wind, Lightning and Tornado Modelling

Among the hazards which can impact NPPs most are tornadoes, lightning and wind within Europe. Most of these have been characterized using various regressions of historical data, combined with extreme value statistics. The RAIN project used ESWD databases of tornadoes, wind and lightning data [4] in order to create rasterized annual probabilities of occurrences (Figure I-7). Using various adjustments and standards, it is possible to derive also hazard curves of the wind speed or electric current vs. return period as shown for Trino Vercellese (Figure I-8).

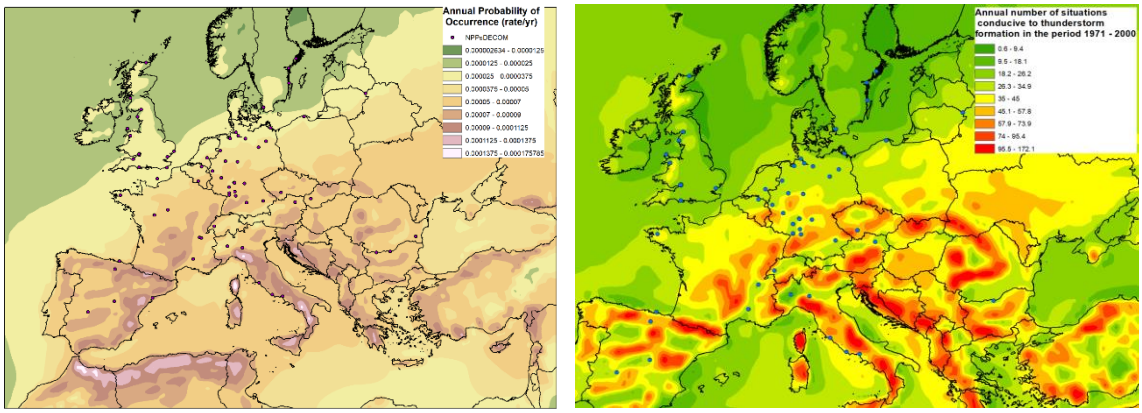


Figure I-7: Left: annual probabilities of tornado occurrence; Right: annual number of thunderstorm conditions from 1971-2000.

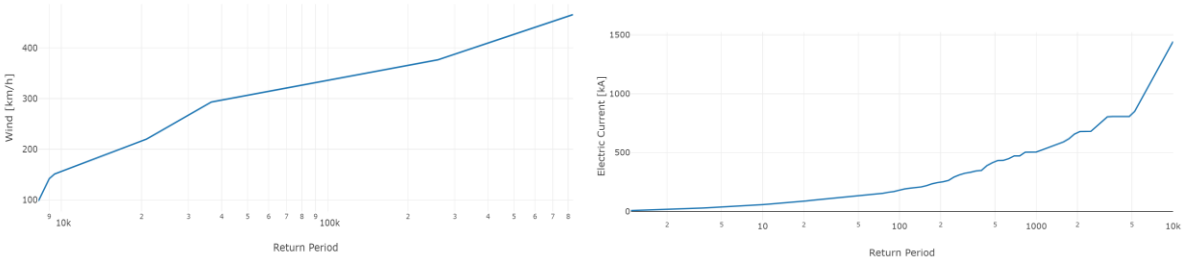


Figure I-8: Left: annual probabilities of tornado occurrence; Right: annual number of thunderstorm conditions from 1971-2000.

I.5 CONCLUSION

There are many methods for external hazards characterisation and much data and work exists in the field including standards for each hazard type for Europe. Uncertainties are found throughout every step of the hazard modelling chain and are important to characterise as part of PSA. Deterministic and probabilistic methods both have their place and can both be employed for each hazard type. Extreme value statistics and real-life examples are key to understanding NPP external hazard modelling.

REFERENCES

[1] Decker, K., Brinkman, H. (2016), List of external hazards to be considered in ASAMPSA_E, Technical report, WP21/D21.2/2017-41.

[2] Narsis Consortium (2019). Del 1.1 - Review of state-of-the art for hazard and multi-hazard characterisation, Deliverable 1.1, WP1, NARSIS-EU Project.

[3] Gill, J. C., and B. D. Malamud. 2014. "Reviewing and Visualizing the Interactions of Natural Hazards." Rev. Geophysics 52 (4): 680–722. doi:10.1002/2013RG000445.

[4] European Severe Storms Laboratory; TU Delft, and RAIN consortium (2016). RAIN: Pan-European gridded data sets of extreme weather probability of occurrence under present and future climate. TU Delft. Dataset.

[5] Stirling, M. W., Litchfield, N. J., Villamor, P., Van Dissen, R. J., Nicol, A., Pettinga, J., ... & Mountjoy, J. (2017). The Mw7. 8 2016 Kaikōura earthquake. Bulletin of the New Zealand Society for Earthquake Engineering, 50(2), 73-84.

[6] Giardini D. et al., (2013), Seismic Hazard Harmonization in Europe (SHARE): Online Data Resource, doi: 10.12686/SED-00000001-SHARE, 2013.

[7] Schaefer, A.M. (2018). Development of a global tsunami model, PhD Thesis, Karlsruhe.

[8] TSUMAPS_NEAM (2018) NEAM Tsunami Hazard Model 2018 (NEAMTHM18): online data of the Probabilistic Tsunami Hazard Model for the NEAM Region from the TSUMAPS-NEAM project. Istituto Nazionale di Geofisica e Vulcanologia (INGV); http://doi.org/10.13127/tsunami/neamthm18.

[9] HLNUG (2019). Hessisches Landesamt für Naturschutz, Umwelt und Geologie – Flood maps for Hesse, https://www.hlnug.de/themen/wasser/hochwasser

II Modelling External Floodings – The quantification of the Extreme Sea Level according to the French flooding guide (ASN n°13) recommendations

Vito Bacchi, Claire-Marie Duluc, Lise Bardet
Institute for Radiological Protection and Nuclear Safety (IRSN)
31, avenue de la Division Leclerc, B.P. 17
92262, Fontenay-aux-Roses, France
vito.bacchi@irsn.fr, claire-marie.duluc@irsn.fr, lise.bardet@irsn.fr

ABSTRACT

This paper aims to illustrate how the flooding hazard induced by an "Extreme Sea Water Level" situation must be evaluated according to French regulations recommendations adopted in the demonstration of nuclear safety of basic nuclear installations (BNI). With this aim, we first introduce the French flooding guide published by the French Authority for Nuclear Safety (ASN) in 2013, which proposes a list of recommendations concerning the external flooding hazard assessment. Then, we will focus on the main scientific challenges related to extreme storm surge assessment, namely (i) the statistical models employed for the analysis of the outlier storm surge and (ii) the use of historical information in the statistical modelling. In conclusion, we will present the mentioned concepts with a practical evaluation of extreme storm surges at "La Rochelle" harbour.

II.1 EXTERNAL FLOODING IN THE FRENCH GUIDE FOR THE SAFETY OF BASIC NUCLEAR INSTALLATIONS

The French regulations require that the flooding hazard must be taken into consideration in the demonstration of nuclear safety of basic nuclear installations (BNI). With this aim, the French Authority for Nuclear Safety (ASN) published in 2013 the recommendations concerning the external flooding hazard in the ASN's guide n°13. In this guide, the external flooding hazard is defined as being a flood whose origin is external to the structures, areas or buildings of the BNI accommodating systems or components to be protected, whatever the cause(s) of that flooding (rainfall, river spates, storms, pipes failures, etc.).

The purpose of the guide is (i) to define the situations to consider when assessing the flood hazard for the site in question, (ii) to propose an acceptable method of quantifying them and (iii) to list the recommendations for defining means of protection adapted to the specifics of the flooding hazard, implemented by the licensee according to the life cycle phases of the installation. Moreover, the guide has taken into account climate change according to the state of the art of 2013 and underlines the importance to evaluate the "predictable" effects of climate changes for a period representative of the installations' foreseeable life times.

The guide identifies a list of water sources that could initiate (or contribute) to a flood affecting a site, namely the rainfall (1), groundwater (2), the seas and oceans (3), the rivers and canals (4), and the natural (i.e. likes, glaciers) and man-made (i.e. storage dams, pipes, etc…) reservoirs (5). Then, the guide defines eleven "Reference Flood Situation" (RFS) as an event or

a combination of events generated by the identified water sources (see Figure II-1), whose characteristics may be increased if necessary (i.e. unfavourable combination or additional margin to compensate the limitations of the actual knowledge).

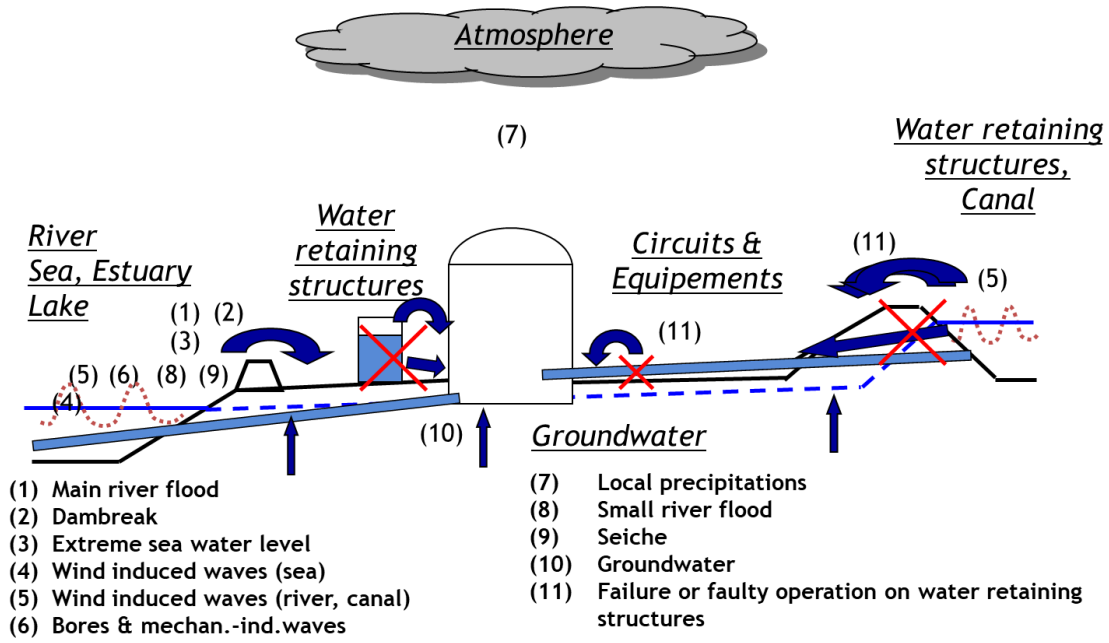


Figure II-1: Reference Flood Situations as reported in the ASN guide n°13. The red crosses indicate the failure of a water-retaining structure.

According to the characteristics of the site accommodating the installation (i.e. a coastal area or a river), a list of RFSs shall be drawn up. The design of the installations with regard to the flood hazard shall be justified in view of these RFSs, taking into account any dynamic effects. The list of RFSs shall take into account the various water sources at and around the site, and the identified events or combinations.

Even if not specifically mentioned in the guide, from a statistical point of view, the intended target for the definition of the RFS is a return period of 10,000 years. This value is consistent with other published standard recommendations on nuclear safety [1].

In this short communication, we will focus on the principles for the evaluation of the RFS "Extreme Sea Water Level" according to the flooding guide recommendations (section II.2.1), the main challenges around this topic (section II.2.2) and we finally illustrate an example of application to the "La Rochelle" harbour (section II.2.3).

II.2 EVALUATION OF THE RFS "SEA LEVEL AND WAVES" ACCORDING TO THE ASN GUIDE PRINCIPLES

II.2.1 Reference Flood Situations for Sea level and Waves defined in the French regulatory guide

According to the ASN guide n°13, the reference high sea level is the conventional sum of:

- the maximum level of the theoretical tide[1];
- the one-thousand year return period storm surge[2] (upper bound of the 70% confidence interval), increased to take into account uncertainties associated to the evaluation of the rare storm surges, and resulting from outliers (see section II.2.2);
- the change in mean sea level extrapolated to the next periodic safety review.

As an alternative to the first two points above, a statistical analysis of the tide levels and storm surges may be conducted to determine the probability of exceedance of the water level resulting from the two phenomena combined (joint probability method), considering a ten-thousand-year return period. This approach shall use a statistical extrapolation model that can cover outliers, and include an estimate of the sampling uncertainty that will be covered by the reference sea level.

Characterizing the wave conditions at a coastal site in principle combines ocean waves generated by offshore wind and propagated beyond the area on which they are generated, and waves generated by the local wind. The reference waves are characterized from the one-hundred-year return period significant height wave conditions (upper bound of the 70% confidence interval) determined offshore of the site and propagated over the reference sea level. In this case it is recommended not to separate the ocean waves and the local wind waves, and to perform the analysis on the total wave height data.

Depending on the exposure and configuration of the site, it is possible to simplify the analysis by determining the predominance of the contribution of the ocean waves or the local wind waves to the total wave height. More specifically, if the effects of the local wind are found to be predominant over the ocean waves due to the site configuration or existing structures, reference local wind waves is used. This is defined by the local wind waves resulting from a hundred-year return period wind (upper bound of the 70% confidence interval) propagated over the reference sea level.

The duration of this RFS is determined from the variations in sea level caused by the tide.

II.2.2 Focus on a typical challenge in extreme hazard assessment: outliers in surges

High return period surges can be estimated on the basis of observed surges at a local site, by using statistical models. The annual maxima method [6]-[9] or the Peaks Over Threshold (POT) method [7]-[10] are widely used to estimate extreme events for many environmental processes: precipitation, waves, sea level, sea surge, river discharge, earthquake or wind, for instance.

However, it was demonstrated that this statistical fitting based on local analyses (also known as frequency analysis “FA”) cannot recreate some extreme events called “outliers” [11]. An outlier is an exceptional event in a sample: it is an observation whose value is significantly distant from the values of the other observations of the same sample. In particular, a statistical fitting of the sample is not representative of this exceptional observation and the confidence intervals are often inadequate. As an example, Figure II-2 shows the surge data set at La Rochelle, in which the event corresponding to the Xynthia storm of 2010 is an outlier.

[1] The impact of astronomical tide and radiational tide on the sea is theoretically known. A sea level, also called *theoretical tide*, can be thus predicted owing to the harmonic components of the tide signal ([2], [3]).

[2] The tide level which is observed can be different from the tidal prediction, mainly because of meteorological phenomena ([3], [4]). The difference between the observed and predicted sea levels is called *surge*.

As a consequence, according to the authority guide for nuclear safety [12], the calculation of thousand-year return period storm surges on a local scale using the conventional extrapolation laws is at present unable to take satisfactory account of exceptional events (outliers) observed at several monitoring stations. An additional increase in reference sea level of 1 m is applied to allow for this.

Another approach - based on a regional analysis for example - can be used to calculate the thousand-year return period storm surge, subject to demonstration of the suitability of the statistical extrapolation model used and its relevance for the outliers observed by various monitoring stations. In this case, there is no need to apply an additional margin.

Regional frequency analysis (RFA), in which on-site observed exceptional events may become normal regional extreme observations and do not appear to be outliers any more, was considered by the scientific community to be a serious track to analyze the frequency of occurrence of the surges [13]-[15]. The objective of an RFA is to use information, within a homogeneous region, from gauged sites to an ungauged or poorly gauged target site. The stages of a standard RFA are: (i) delineation of homogeneous regions; (ii) regional frequency estimation of the quantiles of interest. A comparative study of various RFAs was presented by GREHYS [16]-[17]. One of the simplest and most popular approaches, privileged by engineers and widely used in hydrology, is the index flood method [18]. Its major hypothesis is that the probability distributions at different sites in the region are identical, except for a scale parameter.

When applied to coastal hazards (e.g. [13]-[14]), the RFAs are limited by the problem of the inter-site dependence issue and its impact on the variance of local and regional quantiles and on the statistical homogeneity [19]. Indeed, recent developments go a step further and involve a procedure to consider the spatial dependence structure using copulas [20] and to form statistically homogenous regions. Weiss [21] proposed a criterion (related to the spatial propagation of storms) to form homogeneous regions. However, the existing delineation procedures do not give specific weight to the target site, which may lead to a loss of some relevant local effects. Furthermore, the delineation of a homogenous region usually leads to the problem of the so-called “border effect” (information at a site located on the other side of the target site region is excluded even though both sites have similar asymptotic properties). As a consequence, an alternative method based on the empirical spatial extremogram to define a homogenous region around a target site was proposed [22]. The neighborhood between sites is measured by a degree of inter-site tail dependence. The region constituting the neighboring sites moves from one target site to the other, by permitting to overcome the “border effect” problem.

Finally, it has been shown in the literature that the use of historical information (HI) can significantly improve the probabilistic and statistical modeling of extreme events for both FA (i.e.[23]) and RFAs approaches (i.e. [24]). In fact, the use of additional HI over longer periods than the gauging one can significantly improve the probabilistic and statistical treatment of a dataset containing an exceptional observation considered as an outlier [23]. However, it must be underlined that the documentary data related to the extreme events are often not freestanding enough to directly extract water levels and subsequently skew surge levels, and hence auxiliary information such as dike sketches was used to interpret the collected data [25]. As a consequence, it is of primary importance to trace the methodology and the hypotheses taken for the surges reconstruction, to inform potential users about the different degrees of reliability of estimated values [25].

II.2.3 Example of application: the case of La Rochelle [24]

As reported in Hamdi et al. [24], both RFA and HI strongly improve the probability distribution fit of storm surges, respect the classical FA method without regional analysis. The analysis presented here, issued from the mentioned study, was performed at La Rochelle (as a target site). One of the most important features of the La Rochelle site is the fact that the region in which this site is located has experienced significant storms during the last two decades (Martin in 1999 and the Xynthia in 2010).

From Figure II-2b, it can be observed that the fitting results at the right tail of the distribution appear more adequate and that combining regional data and HI leads to an increase in the 100-year quantile (the mean trend value) of about 30 cm since the shape parameter is positive and greater than that obtained when regional data alone is used [24]. In other words, the 100-year return level (the mean trend value) in the initial fitting has a return period of only 30 years in the new fitting with regional and historical information included. Lastly, despite the facts that there is more variability in the sample (the sample size is the same but the effective duration has doubled, as reported in Hamdi et al. [24]), and that the 100-year quantile has significantly increased, the relative width of the confidence interval has remained almost constant.

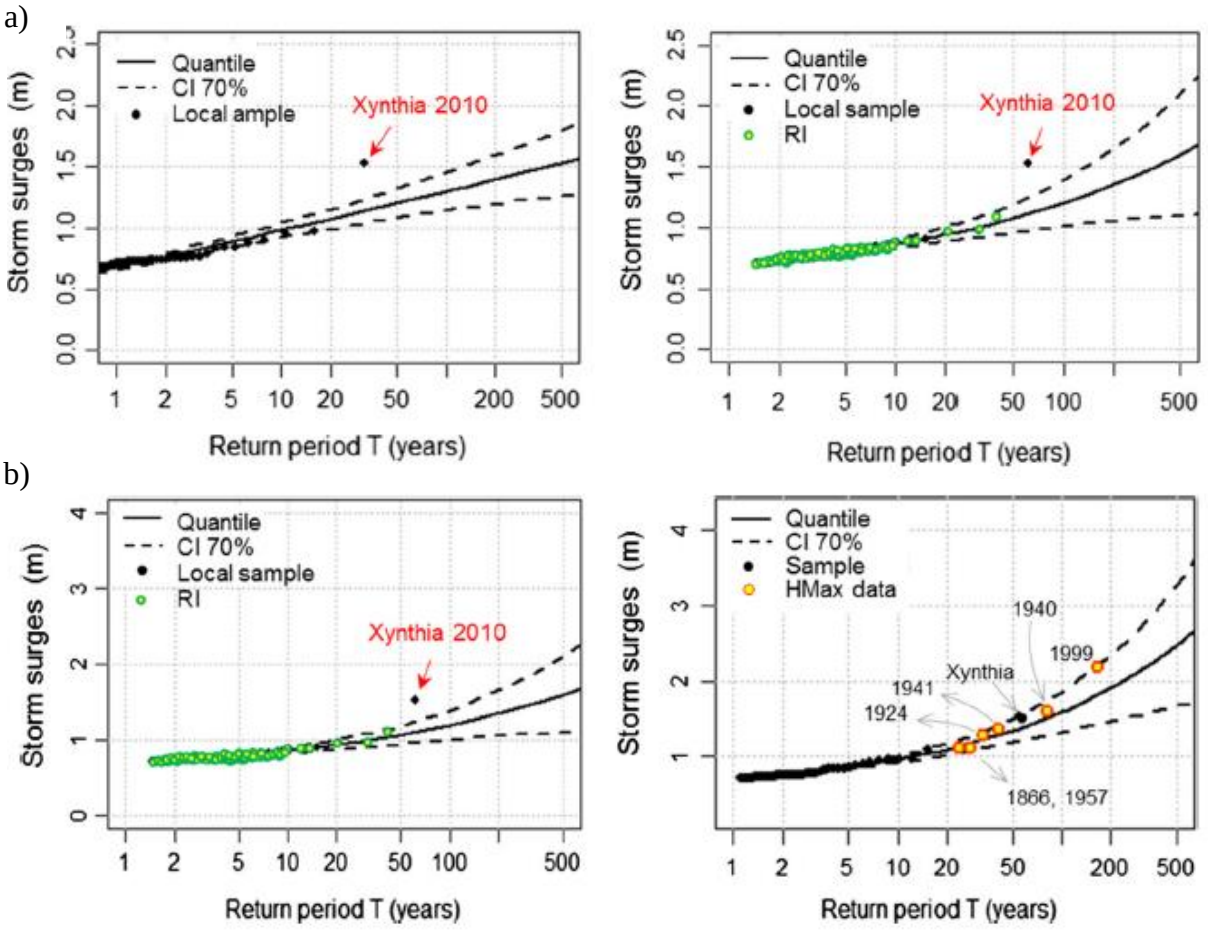


Figure II-2: a) Generalized Pareto Distribution (GPD) fitted to the extreme surges: with no HI included (left) and with local data enriched with Regional Interpolation (RI) on the right; b) the GPD fitted to local extreme surges enriched with RI with no HI (left) and with HI included (right). Figure and hypothesis from Hamdi et al. [24].

II.3 CONCLUSIONS

The aim of this short communication was to illustrate the methodology classically employed in the field of French nuclear safety for the evaluation of the flooding hazard induced by an "Extreme Sea Water Level". Especially, we focused on the main scientific challenges related to extreme storm surge assessment, namely (i) the statistical models employed for the analysis of the *outlier* storm surge and (ii) the use of historical information in the statistical modelling. The impact of different statistical models and data on the evaluation of the extreme storm surge was finally illustrated through a practical example at "La Rochelle" harbour, issued from Hamdi et al. work [24].

REFERENCES

[1] WENRA, R., Guidance Document Issue T: Natural Hazards Head Document. Guideline for the WENRARHWG Safety Reference Levels for Natural hazards introduced as lesson learned from TEPCO Fukushima Daiichi accident, 2015.

[2] Whitcombe, L. J.: A Fortran program to calculate tidal heights using the simplified harmonic method of tidal prediction, Computers and Geosciences, 22, 817–821, 1996.

[3] Simon, B.: La mar´ee oc´eanique cˆoti`ere, Institut Oc´eanographique-SHOM ed., 433 pp., 2007.

[4] Bode, L. and Hardy, T. A.: Progress and recent developments in storm surge modeling, J. Hydraul. Eng., 123, 315–331, 1997.

[5] Olbert, A. I. and Hartnett, M.: Storms and surges in Irish coastal waters, Ocean Model., 34, 50–62, 2010.

[6] Thompson, K. R., Bernier, N. B., and Chan, P.: Extreme sea levels, coastal flooding and climate change with a focus on Atlantic Canada, Nat. Hazards, 51, 139–150, 2009.

[7] Pandey, M. D., Van Gelder, P. H. A. J. M., and Vrijling, J. K.: Dutch case studies of the estimation of extreme quantiles and associated uncertainty by bootstrap simulations, Environmetrics, 15, 687– 699, 2004.

[8] Van Den Brink, H. W., K¨onnen, G. P., and Opsteegh, J. D.: Uncertainties in extreme surge levels estimates from observational records, Philos. T. Roy. Soc. A, 363, 1377–1386, 2005.

[9] Fawcett, L. and Walshaw, D.: Improved estimation for temporally clustered extremes, Environmetrics, 18, 173–188, 2007.

[10] Haigh, I. D., Nicholls, R., and Wells, N.: A comparison of the main methods for estimating probabilities of extreme still water levels, Coast. Eng., 57, 838–849, 2010.

[11] Masson, J. M.: Un probl`eme parmi d'autres dans l'analyse des distributions des variables hydrologiques: Les horsains (outliers), in: Statistique impliqu´ee. Paris: ORSTOM (Colloques et S´eminaires), S´eminfor 5: cinqui`eme s´eminaire informatique de l'ORSTOM, 1991/09/02-04, Montpellier (France), 303–311, 1992.

[12] ASN – Nuclear Safety Authority: Protection des installations nucléaires de base contre les inondations externes, guide No. 13, France, 2013.

[13] Bardet, L., Duluc, C.-M., Rebour, V., and L'Her, J.: Regional frequency analysis of extreme storm surges along the French coast, Nat. Hazards Earth Syst. Sci., 11, 1627–1639, https://doi.org/10.5194/nhess-11-1627-2011, 2011.

[14] Bernardara, P., Andreewsky, M., and Benoit, M.: Application of regional frequency analysis to the estimation of extreme storm surges, J. Geophys. Res., 116, C02008, doi:10.1029/2010JC006229, 2011.

[15] Weiss, J., Bernardara, P.: Comparison of local indices for regional frequency analysis with an application to extreme skew surges. Water Resources Research, VOL. 49, 2940-2951, doi:10.1002/wrcr.20225, 2013.

[16] Groupe de Recherche en Hydrologie Statistique, Presentation and review of some methods for regional flood frequency analysis. Journal of Hydrology, 186, pp. 63–84, 1996a. https:/doi.org/10.1016/S0022-1694(96)03042-9

[17] Groupe de Recherche en Hydrologie Statistique, Inter-comparison of regional flood frequency procedures for Canadian rivers. Journal Hydrology, 186, pp. 85–103, 1996b. https:/doi.org/10.1016/S0022-1694(96)03043-0.

[18] Dalrymple, T., Flood-Frequency Analyses. Manual of Hydrology: Flood-Flow Techniques, Geological Survey Water-Supply: Washington, 1960

[19] Bardet, L. and Duluc, C.-M.: Apport et limites d'une analyse statistique régionale pour l'estimation de surcotes extrêmes en France, Congrès de la SHF, Paris, 1–2 février 2012 (in French).

[20] Renard, B., A Bayesian hierarchical approach to regional frequency analysis. Water Resources Research, 47(11), W11513, 2011. https:/doi.org/10.1029/2010WR010089.

[21] Weiss, J., Analyse régionale des aléas maritimes extrêmes. Thèse de doctorat. Sciences de l'ingénieur, Université Paris-Est, France, p. 256, 2014.

[22] Hamdi Y, Duluc C-M, Bardet L, Rebour V (2016) Use of the spatial extremogram to form a homogeneous region centered on a target site for the regional frequency analysis of extreme storm surges. J Saf Secur Eng 6(4):777–781. https://doi.org/10.2495/SAFE-V6-N4-777-781.

[23] Hamdi Y, Garnier, E, Giloy, N., Duluc C-M, Rebour V (2018a) Analysis of the risk associated with coastal flooding hazards: a new historical extreme storm surges dataset for Dunkirk, France. Nat. Hazards Earth Syst. Sci., 18, 3383–3402, 2018.

[24] Hamdi Y, Duluc C-M, Bardet L, Rebour V (2018b) Development of a target-site-based regional frequency model using historical information. Nat Hazards. https://doi.org/10.1007/s11069-018-3237-8 https://doi.org/10.5194/nhess-18-3383-2018.

[25] Giloy, N., Hamdi, Y., Bardet, L., Garnier, E., Duluc C-M (2018).Quantifying historic skew surges: an example for the Dunkirk Area, France. Natural Hazards. https://doi.org/10.1007/s11069-018-3527-1.

III Identification of Critical Elements within NPPs Screening and Ranking Methods

Andrej Prošek
Jožef Stefan Institute (JSI)
Jamova cesta 39
1000 Ljubljana, Slovenia
andrej.prosek@ijs.si

Andrija Volkanovski
JSI
andrija.volkanovski@ijs.si

ABSTRACT

This paper presents deterministic and risk informed methodologies for classifying all equipment into one of the safety classes according to its importance to nuclear safety. Before deterministic method is presented, some fundamentals are given what is nuclear safety, which are fundamental safety functions, how safety functions are protected from hazards, and nuclear design criteria. The deterministic classification system provides for a rational basis of determining relative stringency of design requirements applicable to equipment. Then some probabilistic safety assessment (PSA) description is given. Namely, risk-informed process for categorizing structures, systems and components (SSCs) according to their safety significance is as an alternative to deterministic classification. Important to safety SSCs are those safety-related and non-safety related SSCs whose function is to protect the health and safety of the public, while safety-related SSCs are those important to safety SSCs that perform important safety functions during and following design basis events.

III.1 INTRODUCTION - NUCLEAR SAFETY FUNDAMENTALS

Nuclear safety is defined by International Atomic Energy Agency (IAEA) [1] as: "The achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks."

The prime purpose of the nuclear safety is prevention of the release of radioactive materials formed in the fuel, ensuring that the operation of nuclear power plants (NPPs) does not contribute significantly to individual and societal health risk. Prevention of radiation risk is achieved by preventing major damage of the reactor core or the used nuclear fuel bundles. If this is not successful, release of radioactive nuclides from the damaged core to the environment need to be prevented.

Safety function is defined as specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions. The fundamental (basic) safety functions are:

1) control of reactivity - preventing uncontrolled reactor power increase and shutting down the reactor when needed ;
2) removal of heat from the reactor and from the fuel store - cooling of shutdown reactor and used nuclear fuel ;
3) confinement of radioactive material - preventing significant radioactive releases to the environment.

Fundamental (basic) safety functions shall be assured in all situations. Preferably by means of inherent safety features relying on the laws of nature, and as the second alternative by reliable active safety systems designed to carry out these functions (high quality, redundancy, diversity). The systems and structures providing the basic safety functions shall be protected from hazards that may threaten their integrity and intended function. Hazard are the physical effects of a natural phenomenon such as flooding, tornado, or earthquake that can pose potential danger [1]. 10 CFR 50, Appendix A [2] describes general design criteria for NPPs, including the following overall requirements:

1) **Criterion 1- Quality standards and records:** "Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed."
2) **Criterion 2-Design bases for protection against natural phenomena:** "Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions."
3) **Criterion 3-Fire protection:** "Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions." (e.g. non-combustible and heat resistant materials used, fire detection and fighting systems provided).
4) **Criterion 4-Environmental and dynamic effects design bases:** "Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit."

Final Safety Analysis Report (FSAR) is submitted with each application for an operating license and includes a description of the facility, the design bases and limits on its operation and a safety analysis of the SSCs of the facility as a whole. FSAR demonstrates the applicant's qualifications; capability, and planned controls to assure safe plant operation within the constraints of plant design, operating limitations and regulatory requirements.

III.2 DETERMINISTIC CLASSIFICATION OF SSC

The classification system provides for a rational basis of determining relative stringency of design requirements applicable to equipment. For example, Nuclear Regulatory Commission (NRC) regulations define the plant equipment necessary to meet the deterministic regulatory

basis as “safety-related.” This equipment is subject to NRC special treatment regulations. The plant equipment categorized as “non-safety-related” is not subject to special treatment requirements.

ANSI standards 18.2 and 18.2a were written to amplify the general design criteria of 10 CFR 50 Appendix B [3]. ANSI 18.2 standard defines design operating conditions from normal operating conditions to limiting faults:

- Condition I - Normal Operation;
- Condition II - Moderate Frequency Incidents;
- Condition III - Infrequent Incidents;
- Condition IV - Limiting Faults.

Each operating condition is defined by the plant parameters associated with that condition and its probability of deteriorating to a worse condition.

Conditions I to IV design requirements are:

- Condition I occurrences shall be accommodated with margin between any plant parameter and the value of that parameter which would require either automatic or manual protective action.
- Condition II incidents shall be accommodated with, at most, a shutdown of the reactor with the plant capable of returning to operation after corrective action.
- Condition III incidents shall not cause more than a small fraction of the fuel elements in the reactor to be damaged, although sufficient fuel element damage might occur to preclude resumption of operation for a considerable outage time.
- Condition IV faults shall not cause a release of radioactive material that results in an undue risk to public health and safety exceeding the guidelines of 10 CFR 100, "Reactor Site Criteria". A single Condition IV fault shall not cause a consequential loss of required functions of systems needed to cope with the fault including those of the reactor coolant system and the reactor containment system.

ANSI 18.2a defines the safety classes as used in the design of safety related systems and components. A methodology is given for classifying all equipment into one of three Safety Classes (SC) according to its importance to nuclear safety (SC-1, SC-2, SC-3) or into a Non-Nuclear Safety Class. ANSI 18.2a defines a safety system as any system that is necessary to:

- shut down the reactor,
- cool the core,
- cool another safety system, or
- cool the reactor containment after an accident.
- or is any system that contains, controls, or reduces radioactivity released in an accident.

Safety Class 1, SC-1 applies to components whose failure could cause a Condition III or Condition IV loss of reactor coolant. Safety Class 2, SC-2 generally applies to reactor containment and reactor coolant system (RCS) pressure boundary components not in Safety Class 1. Also included in Safety Class 2 are safety systems that remove heat from the reactor or reactor containment, circulate reactor coolant, or control radioactivity or hydrogen in containment. Safety Class 3, SC-3, applies to those components not in SC-1 or SC-2 the failure of which would result in release to the environment of radioactive gases normally required to be held for decay, or that are necessary to provide or support any safety system function, control outside the reactor containment airborne radioactivity released, or remove decay heat from

spent fuel. Non-nuclear safety (NNS) applies to those components not in SC-1, SC-2 or SC-3 (example turbine-generator). The equipment assigned to SC-1, -2 or -3 is that relied upon in the plant design to perform safety function.

ANSI/ANS-51.1-1983 [4], which is revision and combination of N18.2-1973/ANSI-51.1 and N18.2a-1975/ANS-51.8 presents the design criteria for the nuclear safety-related SSCs, functionally grouped: reactor core and internals, reactivity control systems, protection systems, reactor coolant system, shutdown heat removal system, reactor coolant auxiliary systems, cooling water systems, emergency core cooling systems, primary containment, emergency secondary heat removal systems, containment auxiliary systems, safety-related area cooling systems, fuel storage and handling, electrical power systems, fire protections systems, control complex, radioactive waste processing systems, other structures, power conversion system, multi-unit stations.

American Society of Mechanical Engineers (ASME) code classification consists of code classes 1, 2, and 3 for fluid system components and code class MC for reactor (metal) containment components (design and quality assurance requirements) as shown in Table III-1.

Table III-1: Relation of safety classes to ASME code classes [5]

Safety Class (SC)	**Code Class**
SC-1	1
SC-2 for reactor containment components	MC
SC-2 for other than reactor containment components	2
SC-3	3

Institute of Electrical and Electronics Engineers (IEEE) standards are used in the design, operation, and testing of NPP electrical, and instrumentation components and systems. IEEE standards define as Class IE, electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

III.3 PSA DESCRIPTION

Probabilistic Safety Assessment (PSA/PRA) is a systematic method for assessing "risk“. It answers questions: (1) What can go wrong, (2) How likely it is, and (3) What its consequences might be. PSA provides insights into the strengths and weaknesses of the design and operation of a NPP.

Level 1 PSA estimates the frequency of accidents that cause damage to the nuclear reactor core. This is commonly called core damage frequency (CDF). Level 2 PSA, which starts with the Level 1 core damage accidents, estimates the frequency of accidents that release radioactivity from the NPP. Level 3 PSA, which starts with the Level 2 radioactivity release accidents, estimates the consequences in terms of injury to the public and damage to the environment.

Qualitative results include minimal cut sets - MCS (how systems, NPP fail), qualitative importance (qualitative rankings of contributions), and common cause potentials (MCS susceptibility to common cause failures - CCF).

The quantitative results include numerical probabilities/frequencies (CDF/LERF – large early release frequency), quantitative importance (importance measures), and sensitivity evaluations.

The Birnbaum Importance (BI) is a well-known measure that evaluates the relative contribution of components to system reliability:

$$BI(i) = Q_s(Q_i = 1) - Q_s(Q_i = 0). \quad (1)$$

where Q_s is system unavailability, Q_i is unavailability of component i, $Q_s(Q_i = 0)$ is system unavailability when unavailability of component i is 0, and $Q_s(Q_i = 1)$ system unavailability when unavailability of component i is 1.

Fussell-Vesely importance of a modeled plant feature (usually a component, train, or system) is defined as the fractional decrease in total risk level (usually CDF) when the plant feature is assumed perfectly reliable (failure rate = 0.0):

$$FV(i) = (Q_s(Q_i) - Q_s(Q_i = 0))/Q_s(Q_i). \quad (2)$$

If all the sequences comprising the total risk level (e.g. CDF) are minimal, the F-V also equals the fractional contribution to the total risk level of all sequences containing the (failed) feature of interest. Note that F-V = 1-1/RRW. (See Risk Reduction Worth.)

Risk Achievement Worth (RAW) of a modeled plant feature (usually a component, train, or system) is the increase in risk if the feature is assumed to be failed at all times. It is expressed in terms of the ratio of the risk with the event failed to the baseline risk level:

$$RAW(i) = Q_s(Q_i = 1)/Q_s(Q_i). \quad (3)$$

Risk Reduction Worth (RRW) of a modeled plant feature is the decrease in risk if the feature is assumed to be perfectly reliable. It is expressed in terms of the ratio of the baseline risk level to the risk with the feature guaranteed to succeed (see Fussell-Vesely Importance):

$$RRW(i) = Q_s(Q_i)/Q_s(Q_i = 0). \quad (4)$$

III.4 DEFINITION OF RISC CATEGORIES AND UTILIZATION FOR IDENTIFICATION OF NPP CRITICAL ELEMENTS

The 10CFR50.69 rule [4] is risk-informed process for categorizing SSCs according to their safety significance. This is a process in place (for operating reactors) to address a risk-significant categorization process as an alternative to 10 CFR 50 Appendix B [5]. Namely, 10 CFR 50 Appendix B applies to safety related SSCs.

Safety-related SSCs are subject to NRC special treatment regulations. Other plant equipment is categorized as “non-safety-related”, and is not subject to special treatment requirements. There is a set of non-safety-related equipment that is subject to a select number of special treatment requirements or a subset of those requirements. This third set is often referred to as “important-to-safety.”

The terms safety-related and important to safety are not the same. Important to safety SSCs are those safety-related and non-safety related SSCs whose function is to protect the health and safety of the public. Safety-related SSCs are those important to safety SSCs that perform one of three important safety functions during and following design basis events. The three main safety functions assure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown conditions or the

capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guidelines exposures.

The objective of 10CFR50.69 rule [4] is to adjust the scope of equipment subject to special regulatory treatment to better focus licensee and regulator attention and resources on equipment that has safety significance.

The 10CFR50.69 categorization scheme is shown in Figure III-1. It divides the existing "safety–related" and "non-safety-related" categorizations into two subcategories based on high or low safety significance. Safety significant function means a function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk. Safety significance of SSCs is determined by an integrated decision-making process, incorporating risk and traditional engineering insights.

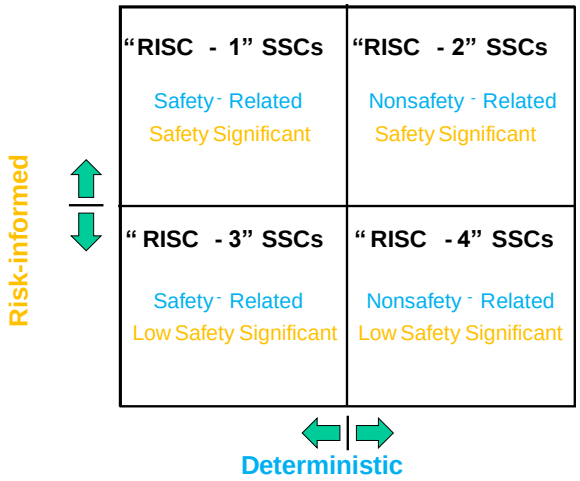


Figure III-1: Risk-informed safety classifications (RISC) (adapted per Figure 1-1 of [5])

Industry developed categorization process that utilizes a series of evaluations to determine the proper risk-informed safety classification for SSCs. The NEI 00-04 [1] categorization process which embodies the principles of risk-informed regulation, is shown in Figure III-2. The plant-specific risk analyses provide an initial input to the process. SSCs identified as high-safety-significant (HSS) by the risk characterization process are identified for an integrated decision-making panel (IDP). SSCs identified as HSS by any of the following may not be re-categorized:

- An SSC identified as HSS by the risk characterization portion of the process (which addresses internal events, external events, shutdown, and integrated importance),
- An SSC identified as HSS by the internal events PRA assessment,
- An SSC identified as HSS by a non-PRA method to address external events, fire, seismic, or shutdown,
- An SSC identified as HSS by the defense in depth assessment.

SSCs not meeting any of the above, but identified as HSS through a seismic PRA, external events PRA, fire PRA, shutdown PRA, or through the sensitivity studies, may be presented to the IDP for categorization as LSS, if this determination is supported by the integrated assessment process and other elements of the categorization process.

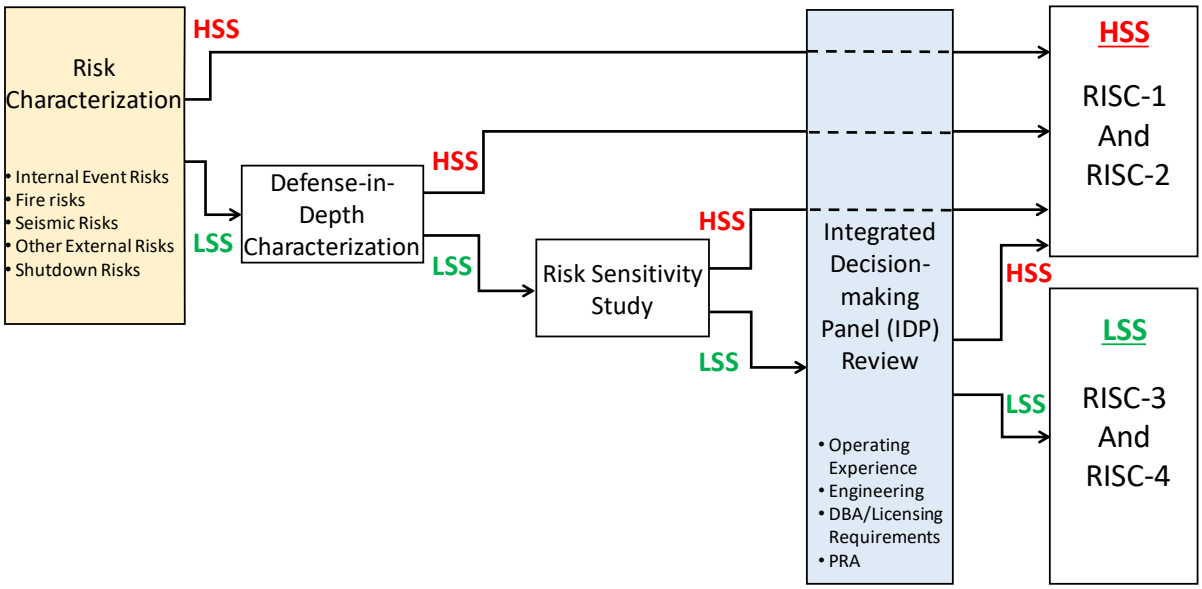


Figure III-2: Summary of NEI 00-04 Categorization Process (adapted per Figure 1-2 of [5])

Finally, an example of the risk importance process using two standard PRA importance measures, RAW and Fussell-Vesely (F-V), as screening tools to identify candidate safety-significant SSCs is shown. The criteria chosen for safety significance using these importance measures are based on previously accepted values for similar applications. They are:

- Sum of F-V for all basic events modeling the SSC of interest, including CCF > 0.005.
- Maximum of component basic event RAW > 2.
- Maximum of applicable common cause basic events RAW > 20.

If any of these criteria are exceeded it is considered candidate safety significant SSCs.

REFERENCES

[1] International Atomic Energy Agency, IAEA Safety Glossary: 2018 Edition, IAEA, Vienna (2019).

[2] ANSI/ANS-58.21-2003: External Events PRA Methodology, 2003.

[3] Nuclear Regulatory Commission, Appendix A to Part 50-General Design Criteria for Nuclear Power Plants.

[4] Nuclear Regulatory Commission, Appendix B to Part 50-Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.

[5] ANSI/ANS-51.1-1983 (revision and combination of N18.2-1973/ANSI51.1 and N18.2a-1975/ANS-51.8); R1988; W1998: Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.

[6] Nuclear Energy Institute, 10 CFR 50.69 SSC Categorization Guideline, NEI 00-04, July 2005.

IV Methods for the Derivation of Fragility Functions

Pierre Gehl, Jeremy Rohmer
BRGM, 3 Avenue Claude-Guillemin, 45060 Orléans, France
p.gehl@brgm.fr, j.rohmer@brgm.fr

Karol Kowal, Sławomir Potempski
NCBJ, A. Soltana 7, 05-400 Otwock-Swierk, Poland
karol.kowal@ncbj.gov.pl, slawomir.potempski@ncbj.gov.pl

Marine Marcilhac-Fradin, Yves Guigueno
IRSN, B.P. 17, 92262 Fontenay-aux-Roses, France
marine.marcilhacfradin@irsn.fr, yves.guigueno@irsn.fr

Irmela Zentner
EDF, 7 Boulevard Gaspard Monge, 91120 Palaiseau, France
irmela.zentner@edf.fr

Marie-Cécile Robin-Boudaoud, Manuel Pellissetti
Framatome, Paul-Gossen-Str. 100, 91058 Erlangen, Germany
marie-cecile.robin-boudaoud@framatome.com, manuel.pellissetti@framatome.com

ABSTRACT

This paper proposes a critical appraisal of current approaches for the derivation of fragility functions for structures, systems and components related to nuclear power plants. Fragility functions express the conditional probability of reaching or exceeding a limit state, given the level of the external hazard loading(s), represented by intensity measures. The dispersion in the fragility function may be caused by a wide range of uncertainty sources, such as the variability in the modelling parameters, the variability in the hazard loading or the quality of the statistical estimation of the fragility parameters. Therefore, this paper demonstrates some of these issues, while applying several fragility methods to an equipment component subjected to earthquake loadings. More specifically, a quantitative analysis of the most suitable intensity measures is detailed: it consists in the identification of the ground-motion parameters that are representative of the ground motions and that are well correlated with the response of the component. Finally, the case of two intensity measures, used as predictors in a vector-based fragility function, is introduced in order to reduce the inherent dispersion in the fragility function (i.e., aleatory uncertainty).

IV.1 INTRODUCTION

Within a Nuclear Power Plant (NPP), the vulnerability of the structures, systems and components (SSC) must be quantified with respect to a wide range of external loadings induced by natural hazards. To this end, fragility curves, which express the probability of an SSC to reach or exceed a predefined damage state as a function of an intensity measure representing the hazard loading, are common tools developed in the nuclear industry. Their probabilistic nature makes them well suited for PSA (probabilistic safety analysis) applications, at the

interface between probabilistic hazard assessments and event tree analyses, in order to estimate the occurrence rate of undesirable top events.

Therefore, the aim of this paper is to present current approaches for the derivation of fragility curves (Section 2), with a focus on seismic hazard. Then, in Section 3, the challenge of using a scalar intensity measure (IM) to represent a ground-motion time-history is discussed, through the review of several criteria for the selection of IMs. Finally, in Section 4, vector-IM fragility functions (or fragility surfaces) are introduced; and some examples applied to SSC demonstrate a reduction in the aleatory uncertainty that is related to the record-to-record variability.

IV.2 STATE-OF-THE-ART OF CURRENT METHODS

This section provides an overview of current approaches for the derivation of fragility functions for SSC in the nuclear industry. The review applies mostly to the case of seismic hazard, which has been the object of the most comprehensive studies in the past.

IV.2.1 Theoretical framework

Fragility functions express the probability of reaching or exceeding a damage state DS given the level of seismic loading, represented by an intensity measure IM = *im*. Thus, they are written in the form of conditional probabilities. The damage state is defined by the engineering demand parameter (EDP) exceeding a given threshold: the EDP represents the physical demand that is applied to the SSC, until its capacity is reached. Depending on the type of SSC and the type of damage mechanism investigated, EDPs may be represented by a wide range of physical variables, such as the maximum deformation during the loading, the stress level reached by a structural element, or the ductility ratio.

Due to the statistical distribution of IM and EDP in practical applications, fragility curves are usually represented as a cumulative lognormal distribution [1], as follows:

$$P_f(im) = P(ds \geq DS | IM = im) = \Phi\left(\frac{\ln im - \ln \alpha}{\beta}\right) \quad (1)$$

where α represents the median and β the logarithmic standard deviation of the capacity expressed in terms of the IM, i.e. the fragility parameters.

Kennedy et al. [2] have proposed a formal framework for the treatment of uncertainties related to nuclear applications. The standard dispersion β may be decomposed into:

- a term β_R representing aleatory randomness (e.g., the record-to-record variability);
- a term β_U representing epistemic uncertainty (e.g. modelling or parameter uncertainties due to lack of knowledge).

Therefore, they have proposed the following mathematical expression, which allows the definition of a family of fragility functions for various confidence levels *Q*:

$$P_f(im) = \Phi\left(\frac{\ln im - \ln \alpha + \beta_U \Phi^{-1}(Q)}{\beta_R}\right) \quad (2)$$

Thus, the epistemic uncertainty on the estimation of the median α, due to lack of knowledge for instance, is represented by the logarithmic standard deviation β_U. As a result, the value $Q = 0.5$ yields the median fragility function, which is flanked by a set of fragility functions representing confidence intervals (e.g., $Q = 0.05$ and 0.95 for the 5%-95% confidence interval).

On the other hand, the aleatory uncertainty, represented by β_R, directly acts on the general shape of the curve (i.e., the "slope").

Within this framework, it is also possible to aggregate both types of uncertainty into a composite fragility function with a larger dispersion:

$$P_f(im) = \Phi\left(\frac{\ln im - \ln \alpha}{\sqrt{\beta_U^2 + \beta_R^2}}\right) \quad (3)$$

Such an expression represents the mean fragility function, for which the total dispersion is obtained through a quadratic combination of β_U and β_R:

$$\beta_C = \sqrt{\beta_U^2 + \beta_R^2} \quad (4)$$

The graphical constructions related to these mean and median fragility functions are illustrated in Figure IV-1.

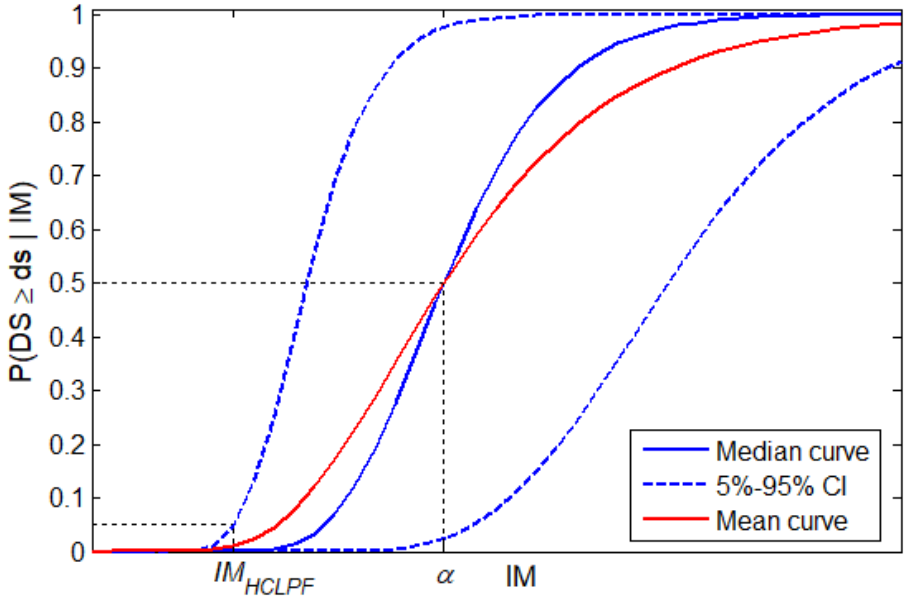


Figure IV-1: Representation of the mean and median fragility functions, along with their 5%-95% confidence interval.

Finally, this uncertainty decomposition enables the computation of the so-called HCLPF (High Confidence Probability of Failure) capacity, which corresponds to the intensity measure leading to a failure probability of 5% on the 95% confidence curve. From Equation 2, it may be expressed as follows:

$$IM_{HCLPF} = \alpha \cdot \exp[-1.645(\beta_U + \beta_R)] \quad (5)$$

The HCLPF capacity has a practical use in the seismic margin assessment framework, where the capacities of all components may be assembled in order to quantify the capacity of the NPP. Such an approach leads to the identification of "weak links" and to the estimation of the plant's capacity to withstand beyond-design earthquakes (i.e., margin with respect to the safe shutdown earthquake).

IV.2.2 The separation-of-variables method (safety factor method)

Due to the large number of SSCs within a NPP, a simplified approach for the estimation of seismic fragility parameters has been developed for nuclear applications [3]. This method assumes a given seismic design level IM_S (i.e., the intensity measure corresponding to the design event). The median fragility parameter α is expressed through a safety factor F that represents the seismic margin over the design level:

$$\alpha = IM_S \cdot F \tag{6}$$

In the case of structures, the safety factor F is decomposed into three categories [4]:

$$F^{(struct)} = F_S \cdot F_\mu \cdot F_{SR} \tag{7}$$

where F_s is the strength factor, F_μ is the inelastic energy absorption factor and F_{SR} is the structural response factor, which is further decomposed as follows (see definition of factors in Table IV-1).

$$F_{SR} = F_{SA} \cdot F_{GMI} \cdot F_\delta \cdot F_M \cdot F_{MC} \cdot F_{EC} \cdot F_{SSI} \tag{8}$$

In the case of an equipment within a structure, the safety factor F takes the following form [4]:

$$F^{(equip)} = F_S \cdot F_\mu \cdot F_{SR} \cdot F_{ER} \tag{9}$$

where the strength factor F_s and the inelastic energy absorption factor F_μ now refer to the behaviour of the equipment; F_{SR} is the structural response factor, and F_{ER} is the equipment response factor (relative to the structure).

Table IV-1: Definition of the structural response factors used in the safety factor method.

Safety Factor	Definition
F_{SA}	Spectral shape factor
F_{GMI}	Factor related to the spatial incoherency of ground motion
F_δ	Damping factor
F_M	Modelling factor
F_{MC}	Factor related to the structural mode combination rules
F_{EC}	Factor related to the combination of horizontal earthquake components
F_{SSI}	Soil-structure-interaction factor

These factors are evaluated through various means, such as seismic design calculations, engineering judgement, plant walkdown, past earthquake experience, qualification through testing or numerical analysis (static or dynamic). Depending on the estimation method used and on the type of safety factor, various levels of standard deviations $\beta_{U,i}$ and $\beta_{R,i}$ are proposed for each of the safety factor F_i. Thanks to the lognormal assumption, a quadratic combination is used to assemble the global uncertainty terms β_U and β_R from the list of safety factors. The following equation is an example of the computation of β_U for a structure:

$$\beta_U = \sqrt{\beta_{U,S}^2 + \beta_{U,\mu}^2 + \beta_{U,SA}^2 + \beta_{U,GMI}^2 + \beta_{U,\delta}^2 + \beta_{U,M}^2 + \beta_{U,MC}^2 + \beta_{U,EC}^2 + \beta_{U,SSI}^2} \tag{10}$$

The EPRI [3,5] guidelines contain recommendations and standard values for some of the safety factors and their associated uncertainty terms.

IV.2.3 Regression models from numerical simulations

For specific types of critical SSCs, more in-depth analyses than the safety factor method can be justified. Numerical analyses of structural models of SSCs are an efficient way to generate a cloud of data points representing IMs and EDPs, for instance through non-linear time-history analyses (NLTHAs). Two main types of statistical regression are then used for the derivation of the fragility parameters, namely least-squares regression (or 'regression on a cloud') or regression using a binomial distribution.

IV.2.3.1 Regression on the IM-EDP cloud

First, Cornell et al. [6] have proposed to perform a least-squares regression on the IM-EDP dataset, i.e. the so-called "regression on a cloud". It is based on the lognormal assumption, where the following functional form is regressed from the data points:

$$\ln \widehat{edp} = a + b \ln im + \varepsilon \tag{11}$$

The error term ε is also assumed to follow a normal distribution, of mean zero and standard deviation σ. Therefore, by identifying the terms of the fragility function in Equation 1, the fragility parameters α and β are expressed as follows:

$$\begin{cases} \alpha = \exp\left(\frac{\ln EDP_{th} - a}{b}\right) \\ \beta = \frac{\sigma}{b} \end{cases} \tag{12}$$

where EDP_{th} corresponds to the response of the SSC (e.g., deformation, drift, stress values) that is considered to be threshold of the studied damage state.

Due the simplicity of this model, the least-squares regression tends to yield stable estimates, even with a reduced number of data points [7]. Therefore, it is possible to estimate fragility parameters even when very few simulation outcomes exceed the damage threshold. However, the extrapolation of the regression beyond the IM interval defined by the data points should be avoided. Moreover, as seen in Equation 12, the standard deviation β is independent from the damage state threshold, which means that all fragility curves would present the same "slope" (in the lognormal space) if different grades of damage states were to be studied from the same dataset: this constraining assumption does not necessarily comply with the variability in the response of the studied SSC when higher loading levels are applied (i.e., increased dispersion).

IV.2.3.2 Regression using a binomial distribution

Alternatively, another approach consists in applying a Generalized Linear Model (GLM) regression or a maximum likelihood estimation (MLE) to a set of binary damage variables Y: all points that exceed the damage state threshold take the value $y_i = 1$, and 0 otherwise. This statistical approach has been introduced by Shinozuka et al. [8].

As a result, due to the independent sampling of successes and failures given IM, the Y variables follow a binomial or Bernoulli distribution. Thus, the likelihood function of the fragility parameters α and β, given N data points, takes the following form:

$$L(\alpha, \beta) = \prod_{i=1}^{N} \left[P_f(im_i, \alpha, \beta)\right]^{y_i} \left[1 - P_f(im_i, \alpha, \beta)\right]^{1-y_i} \tag{13}$$

Then, a maximization of L through a search algorithm leads to the best estimates of the fragility parameters α and β.

In the GLM framework, a linear combination of the input (i.e. ln *im*) is estimated from the distribution of the *Y* variables:

$$f\left[P_f(im)\right] = c_1 + c_2 \ln im \tag{14}$$

If the link function $f = \Phi^{-1}$ (i.e. *probit* model), the fragility function can be written as:

$$P_f(im) = \Phi(c_1 + c_2 \ln im) \tag{15}$$

Then, by identification with Equation 1, the fragility parameters are expressed as follows:

$$\begin{cases} \alpha = \exp\left(-\frac{c_1}{c_2}\right) \\ \beta = \frac{1}{c_2} \end{cases} \tag{16}$$

The MLE approach provides the same numerical outcomes as the GLM regression when the *probit* (i.e., inverse of normal cumulative distribution) is used as the link function *f*. Other link functions have been proposed, such as the logistic or Poisson model; however, the *probit* model presents the benefit of generating a lognormal cumulative distribution function, which stays within the original fragility framework.

The use of a binomial distribution does not require exact values of EDP, as long as the simulation outcomes that exceed the damage threshold are identified. Therefore, this approach may be more suited in case the studied SSC is experiencing strong non-linear behaviour (e.g., near the collapse state), which cannot be accurately modelled by the simulation tools. For a given damage state threshold, a clear separation between intact and damaged states is made, which leads to the estimation of a damage-state-specific standard deviation β. Moreover, this approach does not rely on a linear relation between the logarithms of IM and EDP, which is often not justified when plotting the data points. However, a stable estimation of the fragility parameters requires a larger amount of data points and, especially, an appropriate balance between SSC responses that are below and over the damage state threshold.

Table IV-2: Comparative analysis of the characteristics of various statistical methods for the derivation of fragility functions.

Approach	**Main feature**	**Added value**	**Main Limits**	**Example of application**
Separation-of-Variables	Decomposition into safety factors w.r.t the design level	- Reuse existing design calculations (high level of quality assurance!) -> cost-effective, good enough for vast majority of components;	- Assumes linearity of demand w.r.t. IM (partial correction with inelastic energy absorption factor);	- EPRI guidelines [3];
Least squares Regression	Regression of a log-linear IM-EDP relationship.	- Simple and intuitive approach; - Stable fragility estimates may be obtained with a few data points;	- Constrained by the functional form of the IM-EDP relationship; - Constant standard-deviation over the IM range	- seismic fragility of an RC structure [9];
MLE-based regression / GLM regression	Maximisation of the likelihood function, built from damage and no-damage events.	- Applicable to empirical fragility assessment (if only damage data are available); - Ability to treat complete	- Loss of information (i.e., the true values of the EDP are not used); - More data points are required to	- seismic fragility of a masonry structure [10]; - empirical tsunami fragility of buildings [11];

		damage/collapse cases (where EDP values are usually inaccurate); - Compatible with multivariate regression;	achieve stable fragility estimates;	

IV.3 SELECTION OF SEISMIC INTENSITY MEASURES

One of the main issues of current fragility functions pertains to the representation of a complex ground-motion time history by a scalar IM: such an assumption potentially ignores essential measures related to the severity of the external loading, such as the frequency or energy content, the duration of the strong motion, the number of loading cycles, etc.

As a result, with the same IM level (e.g. *PGA*), different ground motions records have the ability to induce different levels of structural response (i.e., the so-called record-to-record variability). The selection of an appropriate scalar IM as an input to a fragility function aims at capturing as much information as possible from the ground-motion time histories that are used in the numerical simulations. For instance, Luco & Cornell [12] have started to propose some criteria for an adequate IM selection:

- The *efficiency* of an IM represents the ability of an IM to induce a low dispersion in the distribution of the structural response (i.e., fragility curve with a steep "slope"). The efficiency is measured by evaluating the standard deviation σ of the error term ε in the log-linear relation between IM and EDP (i.e., Equation 11): the lower the standard deviation, the more efficient the IM.
- The *sufficiency* of an IM represents the ability of an IM to "carry" the characteristics of the earthquake that has generated the ground motion: a sufficient IM should render the distribution of EDP conditionally independent, given the IM, from the magnitude and the distance of the related earthquake events. Using Equation 11 again, the sufficiency of an IM can be checked qualitatively by plotting the residuals of the regression with respect to the magnitude or the distance. In other words, an IM is assumed to be sufficient if the following equality is verified [12]:

$$P\left(EDP\middle|\ddot{x}_g\right) = P\left(EDP\middle|IM\left(\ddot{x}_g\right)\right) \tag{17}$$

where the term x_g represents the whole range of acceleration time-histories that can occur at the considered site. This definition refers, of course, to an ideal case. Therefore Jayaler et al. [13] introduce the concept of relative sufficiency, which measures the additional quantity of information provided by an IM_2 with respect to a reference IM_1:

$$I(EDP|IM_2|IM_1) = \int log_2 \frac{P\left(EDP\middle|IM_2\left(\ddot{x}_g\right)\right)}{P\left(EDP\middle|IM_1\left(\ddot{x}_g\right)\right)} \cdot p\left(\ddot{x}_g\right) \cdot \mathrm{d}\ddot{x}_g \tag{18}$$

If IM_2 is more sufficient than IM_1, then the relative sufficiency index I will be positive, and vice versa. The use of the base 2 logarithm enables an interpretation of the results in terms of bits of information. Finally, the integration over all possible ground motions at the site requires accurate knowledge of the hazard level and of the relative contributions of each seismic zone at the given site.

Moreover, Padgett et al. [14] have proposed additional metrics in order to assess an IM, such as:

- *Practicality*: this metric reflects the strength of the link between IM and EDP. A practical IM will generate a large slope (i.e., coefficient *b* in Equation 11) in the log-linear relation between IM and EDP.
- *Proficiency*: this metric combines practicality and efficiency, since it is evaluated as the ratio b/σ in Equation 11. A high ratio (i.e., high practicality, high efficiency) means a proficient IM.
- *Computability* (or *Hazard compatibility* – cf. Hariri-Ardebili & Saouma [15]): this essential criterion checks whether the selected IM may be computed accurately with current GMPEs, in order to ensure the link between the fragility function and the probabilistic seismic hazard curve. Computability is a qualitative concept; however, the following grades may be proposed:
  1. IM associated with many well-constrained GMPEs thereby providing an estimate of the epistemic uncertainty;
  2. IM associated with few well-constrained GMPEs and it is hence difficult to judge the epistemic uncertainty;
  3. IM associated with no reliable GMPEs.

This classification is used to assign the considered IMs to one of the three categories (see Table IV-3), based on the existing GMPEs in the literature [16,17].

Table IV-3: Qualitative assessment of the computability of some IMs.

Computability grade	IM
1	PGA, PGV, AI, SA(T), RSD75, RSD95
2	PGD, ASI, SI, NED, JMA, CAV, NCy
3	ARMS, A95, SL75, SL95, SMA, SMV, DCy

Finally, most of the aforementioned metrics are specific to the SSC considered (i.e., strong link with the vibration mode of the component) and to the studied site (i.e., location and characteristics of the seismic sources generating the ground-motion time histories). The derivation of fragility functions should therefore be associated with an *ad hoc* study of the most relevant IMs, for a given case study.

IV.4 MULTI-VARIATE FRAGILITY FUNCTIONS

Experience has shown that finding a scalar IM that fulfils all the aforementioned criteria is usually not feasible. For instance, the sufficiency criterion is especially difficult to be fully satisfied by a single IM, which is why the relative sufficiency measure has been introduced [13]. Therefore, Baker & Cornell [18] have introduced an additional IM, epsilon ε (i.e., the deviation between the spectral acceleration of a record and the mean of a ground motion prediction equation at a given period), which is used as a proxy for the spectral shape of the time history, in order to reduce the dispersion in the prediction of the mean annual collapse rate.

Seyedi et al. [9] have applied the concept of seismic fragility surfaces (e.g., use of two IMs as predictors) to an eight-story regular frame RC structure. Using the outcomes of NLTHAs, the spectral displacements at the periods of the first two vibration modes have been selected as IMs, based on the strength of the correlation between IMs and EDPs. A similar framework has been exploited by Gehl et al. [10], who have derived fragility surfaces for a two-

story unreinforced masonry building. A Receiver Operating Characteristics (ROC) analysis has been performed in order to test the adequacy of dozens of scalar IMs and vector-valued IMs. Modica & Stafford (2014) have also searched for the most efficient vector-valued IMs, with respect to a series of European low- and mid-rise reinforced concrete frames. Seismic fragility surfaces have also been applied to other types of structures, such as RC bridges [19]. Within the specific context of the fragility analysis of structures and components in NPPs, Cai et al. [20,21] have introduced a simplified approach for the derivation of fragility surfaces, where the fragility parameters are estimated with the separation-of-variables method, with respect to two IMs.

A possible approach, which relies on similar concepts as the scalar-IM case, is to assume the following functional form:

$$\begin{aligned} P_f(im_1, im_2) &= P(ds \geq DS | IM_1 = im_1, IM_2 = im_2) \\ &= \frac{1}{2}[1 + erf(c_1 + c_2 \ln im_1 + c_3 \ln im_2)] \end{aligned} \quad (19)$$

where the coefficients c_1, c_2 and c_3 are obtained through a GLM regression or a MLE, by considering an additional parameter representing the secondary IM in Equations 13 and 14.

Vector-IM fragility functions are applied to the case of a NPP main steam line [22], for which *PGA* and *SA*(0.29s) are proposed as a combination of IM (see Figure IV-2). The contribution of the record-to-record variability to the global uncertainty structure may be estimated thanks to the comparison between scalar-IM fragility curves and vector-IMs fragility surfaces. This operation should consider the correlation between the two IMs, in order to preserve the hazard consistency of the applied loading. Therefore, a first step consists in estimating the distribution of the secondary IM (i.e, *PGA*) w.r.t. *SA*(0.29s), using the dataset of the input ground-motion records: a median line and its 16%-84% confidence intervals is then plotted (see Figure IV-2, left). The space delimited by this interval provides also practical guidance on the validity domain of the fragility surface, in the sense that it identifies the IM combinations that are very unlikely. It is then proposed to generate "slices" of the fragility surfaces by following the distribution of *PGA* as a function of *SA*(0.29s). As a result, the "slices", now represented as a function of the unique IM *SA*(0.29s), may be compared to the original scalar-IM fragility curve (see Figure IV-2, right).

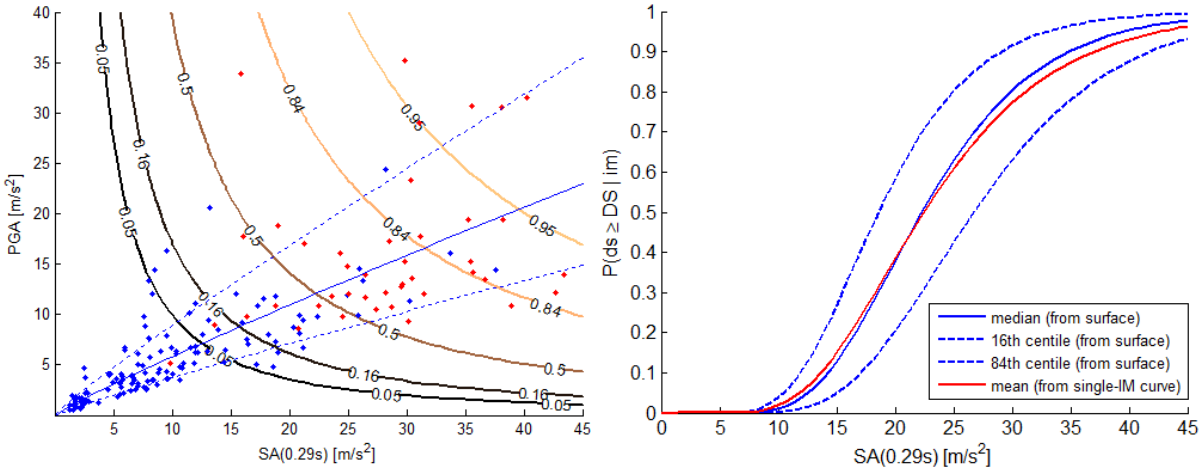


Figure IV-2: Left: fragility surface w.r.t. *PGA* and *SA*(0.29s), the solid blue line represents the median of the *PGA*-*SA*(0.29s) distribution and the dashed blue lines the 16%-84% confidence

intervals, the blue dots represent simulations that have not exceeded the damage threshold and red dots represent damage events; Right: Equivalent fragility curves w.r.t. *SA*(0.29s).

Finally, this family of fragility functions corresponds to the probabilistic framework by Kennedy et al. [2], which has been detailed in Section 2. The mean fragility curve, w.r.t. to *SA*(0.29s), has a total standard deviation β_{tot} = 0.390. Meanwhile, the median fragility curve, obtained from the fragility surface w.r.t. *PGA* and *SA*(0.29s), has a standard deviation of 0.342, which actually corresponds to the aleatory randomness term (i.e., β_R). The confidence intervals obtained from the graphical construction in Figure IV-2 are then used to estimate the epistemic uncertainty term, i.e. $\beta_U \approx 0.187$.

It may be concluded that the vector-IM fragility functions lead to the transfer of a part of the record-to-record variability to a form of epistemic uncertainty, which is related to the description of the seismic loading given the hazard at the specific site. In other words, this uncertainty source may be characterised and reduced when coupling the vector-IM fragility functions with a vector-based probabilistic seismic hazard assessment procedure.

IV.5 CONCLUDING REMARKS

This paper has presented a detailed overview of potential fragility derivation methods in the case of SSC within NPP. The main emphasis of the study consists in the generation of vector-based fragility functions (i.e., use of vector-IMs as conditioning variables) and the impact of the latter on the identification of the various sources of uncertainties. When focusing mostly on fragility assessment related to seismic hazard, the following observations may be made:

- Carefully selected vector-IMs make excellent candidates in terms of IM sufficiency and efficiency, when compared to scalar IMs.
- Vector-valued fragility functions tend to generate less dispersion (i.e., aleatory uncertainty due to record-to-record variability) than scalar-IM fragility curves: this difference may be interpreted as a partial transfer from the record-to-record variability to an epistemic uncertainty component that is related to the description of the seismic loading given the hazard at the studied site.

Further steps will concentrate on the application of such approaches to other hazard types (e.g., flood, wind), while the main challenge resides in the development of fragility models that account for the combined effects of multiple hazard loadings.

REFERENCES

[1] Ellingwood, B. (1990). Validation studies of seismic PRAs. *Nuclear Engineering and Design*, *123*(2-3), 189-196.

[2] Kennedy, R.P., Cornell, C.A., Campbell, R.D., Kaplan, S., & Perla, H.F. (1980). Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant. *Nuclear Engineering and Design*, *59*(2), 305-338.

[3] EPRI (1994), *Methodology for Developing Seismic Fragilities*, EPRI, Palo Alto, CA: June 1994. TR-103959.

[4] EPRI (2009). *Seismic Fragility Application Guide Update*, EPRI, Palo Alto, CA: December 2009. TR-1019200.

[5] EPRI (2003). *Seismic Probabilistic Risk Assessment Implementation Guide*, EPRI, Palo Alto, CA: December 2003. TR-1002989.

[6] Cornell, C.A., Jalayer, F., Hamburger, R.O., & Foutch, D.A. (2002). Probabilistic basis for 2000 SAC federal emergency management agency steel moment frame guidelines. *Journal of Structural Engineering*, *128*(4), 526-533.

[7] Gehl, P., Douglas, J., & Seyedi, D.M. (2015). Influence of the number of dynamic analyses on the accuracy of structural response estimates. *Earthquake Spectra*, *31*(1), 97-113.

[8] Shinozuka, M., Feng, M., Lee, J., & Naganuma, T. (2000). Statistical analysis of fragility curves. *Journal of Engineering Mechanics*, *126*(12), 1224-1231.

[9] Seyedi, D.M., Gehl, P., Douglas, J., Davenne, L., Mezher, N., & Ghavamian, S. (2010). Development of seismic fragility surfaces for reinforced concrete buildings by means of nonlinear time-history analysis. *Earthquake Engineering & Structural Dynamics*, *39*(1), 91-108.

[10] Gehl, P., Seyedi, D.M., & Douglas, J. (2013). Vector-valued fragility functions for seismic risk evaluation. *Bulletin of Earthquake Engineering*, *11*(2), 365-384.

[11] De Risi, R., Goda, K., Yasuda, T., & Mori, N. (2017). Is flow velocity important in tsunami empirical fragility modeling?. *Earth-science reviews*, *166*, 64-82.

[12] Luco, N., & Cornell, C.A. (2007). Structure-specific scalar intensity measures for near-source and ordinary earthquake ground motions. *Earthquake Spectra*, *23*(2), 357-392.

[13] Jalayer, F., Beck, J.L., & Zareian, F. (2011). Analyzing the sufficiency of alternative scalar and vector intensity measures of ground shaking based on information theory. *Journal of Engineering Mechanics*, *138*(3), 307-316.

[14] Padgett, J.E., Nielson, B.G., & DesRoches, R. (2008). Selection of optimal intensity measures in probabilistic seismic demand models of highway bridge portfolios. *Earthquake Engineering & Structural Dynamics*, *37*(5), 711-725.

[15] Hariri-Ardebili, M.A., & Saouma, V.E. (2016). Probabilistic seismic demand model and optimal intensity measure for concrete dams. *Structural Safety*, *59*, 67-85.

[16] Douglas, J. (2012). Consistency of ground-motion predictions from the past four decades: peak ground velocity and displacement, Arias intensity and relative significant duration. *Bulletin of Earthquake Engineering*, *10*(5), 1339-1356.

[17] Douglas, J. (2018). "Ground Motion Prediction Equations 1964-2018", www.gmpe.org.uk.

[18] Baker, J.W., & Cornell, C.A. (2005). A vector-valued ground motion intensity measure consisting of spectral acceleration and epsilon. *Earthquake Engineering & Structural Dynamics*, *34*, 1193-1217.

[19] Li, Z., Li, Y., & Li, N. (2014). Vector-intensity measure based seismic vulnerability analysis of bridge structures. *Earthquake Engineering and Engineering Vibration, 13*(4), 695-705.

[20] Cai, Z., Xie, W.C., Pandey, M.D., & Ni, S.H. (2018a). Determining seismic fragility of structures in nuclear power plants using multiple ground motion parameters – Part I: Methodology. *Nuclear Engineering and Design, 335*, 195-201.

[21] Cai, Z., Xie, W.C., Pandey, M.D., & Ni, S.H. (2018b). Determining seismic fragility of structures in nuclear power plants using multiple ground motion parameters – Part II: Application. *Nuclear Engineering and Design, 335*, 186-194.

[22] Gehl, P., Marcilhac-Fradin, M., Rohmer, J., Guigueno, Y., Rahni, N., & Clément, J. (2019). Identifying uncertainty contributions to the seismic fragility assessment of a nuclear reactor steam line. In *Proceedings of the 7th International Conference on Computational Methods in Structural Dynamics and Earthquake Engineering*, Crete, Greece.

V Latent Weakneses and Root Causes In The Feedback Of Operating Experience Programmes

Milorad Dusic
Nuccon GmbH
Schoenbrunner Allee 9, 1120 Wien, Austria
m.dusic@nuccon.eu

ABSTRACT

The paper introduces the concept of latent weaknesses that can exist in a system for longer time periods and if undetected can result with a triggering event in incidents or even accidents. The concept is demonstrated on the case of Davis Besse nuclear power plant (NPP) near miss where primary coolant boundary was due to corrosion reduced to stainless steel lining within the reactor pressure vessel. The operating organization's feedback of operating experience programme should be able to deal with the existing latent weaknesses by thorough investigation of all incidents. The paper describes three main methods that are being used; classical root cause analysis, probabilistic precursor analysis and deterministic transient analysis. The first of these three methods is used to identify the underlying causes that if corrected would prevent similar events from happening in the future, the precursor analysis is the only method that can quantify the safety significance of the event and transient analysis is used to identify physical phenomena in fast developing reactor transients.

The paper describes various root cause methodologies that are being used today, their brief description and their strengths and limitations. Further, it describes the procedure for applying precursor analysis using the plant specific probabilistic safety assessment and the use of deterministic safety analysis for determination of eroded/still available safety margins during the event being analysed.

The paper is based entirely on the NARSIS deliverable 3.1 prepared jointly by Nuccon and TU Delft.

V.1 INTRODUCTION

This paper is a short summary of NARSIS deliverable 3.1 prepared in the first year of the NARSIS project [1] where all the relevant references are cited and therefore will not be repeated in this paper.

The Incidents are inevitable part of operational life of any complex industrial facility. It is very hard to predict the way that various contributing factors combine to cause the undesired outcome, but it is possible to detect the existence of latent weaknesses that together with the triggering failure(s) result in abnormal events.

Such latent weaknesses are poor management practices, deficiencies in design, gaps in supervision, maintenance faults, inadequate procedures, shortfalls in training, etc. they by themselves are not events or incidents, they by themselves don't make any harm to the system, they are for the most of the time invisible, they just "sit" in the system and wait for a triggering event to manifest themselves in a small incident or a major accident.

In order to have a beneficial feedback from operating experience within an organization, it is essential to establish a sound Root Cause Analysis programme in order to be able to deal with the existing latent weaknesses in the organization by performing a thorough incident investigations. The three main methods are being used worldwide for the event analysis, all three complementing each other:

- classical root cause analysis,
- probabilistic precursor analysis,
- deterministic transient analysis.

V.2 LATENT WEAKNESSES

In order to prevent as many as possible incidents and accidents at complex industrial facilities, we must try to detect and eliminate as many as possible such latent weaknesses bearing in mind that we will never be able to find them all. The key to latent weaknesses detection is a good surveillance program. A good surveillance program should be able to detect the most apparent latent weaknesses and eliminate them before they have a chance to develop into incidents or accidents.

Surveillance of design, i.e. re-evaluation of a design, being periodic within a periodic safety review or at the time of any design modification will detect latent weaknesses in design which might be present from the start of operation of the facility. Periodic surveillance of procedures to verify and validate their intended use will detect inadequate procedures. Surveillance of the training programmes will reveal any potential gaps in operator knowledge. Periodic surveillance of the maintenance programmes will identify potential flaws. The same applies also to other operational activities in any complex industrial facility.

The root causes of incident and accidents should therefore be looked at the management of the surveillance programmes which were not able to eliminate the latent weaknesses that were responsible for the undesired event.

Examples of large industrial accidents (non-nuclear as well as nuclear), well described in open literature can be used to demonstrate the pre-existence of such latent weaknesses and in most cases how easy it would have been to identify and eliminate them with a good surveillance programme. To illustrate this principle, Davis Besse near miss will be described below.

V.2.1 Davis Besse Reactor Pressure Vessel Head Corrosion

In 2002 an inspection of the control rod drive mechanism nozzle cracking on the head of the reactor pressure vessel was performed. After the nozzle crack repair by welding, the nozzle was observed to tip sideways. This was obviously very strange as the nozzle was penetrating the reactor vessel head and would normally have no room to tilt to such angle. After removing the control rod drive mechanism nozzle and cleaning the deposited boric acid from the top of the reactor pressure vessel head a large cavity was discovered (see Figure V-1). Ultrasonic testing measured 3/8 inch of the remaining thickness of the reactor pressure vessel head, which corresponds exactly to the thickness of the stainless steel cladding. The ultimate barrier of the primary circuit was reduced to 3/8 inch of the stainless steel cladding.

The corrosive effects of the boric acid were known for a long time. It was first reported in 1987 at Turkey Point and Salem NPPs and in 1988 Nuclear Regulatory Commission (NRC) issued the NRC Generic Letter 88-05 addressing the corrosive effects of the boric acid and informing all utilities about the possible consequences. From 1996 onwards, the boric acid deposits were found on the top of the reactor pressure vessel also at Davis-Besse NPP. The

amounts of boric acid were so large, that they also clogged filters inside the containment. At the beginning, they were entering the containment every few months in order to clean filters; towards the end they were entering the containment on a two-weekly basis. Nobody, including the NRC resident inspector, has asked the question why was it necessary to enter the containment during normal operation and why so often.

Figure V-1: Davis Besse RPV Head corrosion effects

Utility believed that the boric acid was coming as the leakage through the control rod drive mechanism flange and that elevated temperatures at that location would prevent corrosion.

For several years, warning signs have been ignored; industry reports, coolant leakage, boron on filters, amount of boric acid on the reactor pressure vessel head – all indications of poor safety culture.

V.3 EVENT INVESTIGATION METHODS

Not all events are alike in nature and it is very important to be able to determine which method to apply in the event analysis depending on the type of the event and the answers that we are looking for.

For most unusual events a traditional **root cause analysis** techniques are being used. There is the whole spectrum of techniques being used, depending on the depth of analysis that should be achieved, the nature of the event and other factors. These methods are used to determine a root cause which is in most cases defined as the most fundamental reason for an incident or condition, which if removed will prevent recurrence of incident or condition.

In cases when our aim is to determine the safety significance of the event the best method to be used is the **probabilistic precursor analysis**. Probabilistic precursor analysis gives a quantitative estimation of safety significance of the event that happened. It uses the concept of conditional core damage probability (CCDP) to determine the safety significance of the event. It is basically a measure, in a PSA model, how far is the event which is being analysed from the core damage scenario.

The tried type of the event analysis is known as **deterministic transient analysis.** They are used to analyse the fast developing events. It is the only method, which can give us the quantitative estimation of the remaining safety margins throughout the event.

V.3.1 Root Cause Analyses

There are many definitions of root causes but most commonly used in the nuclear industry is that the root cause is the most fundamental reason for an incident or condition, which if removed will prevent recurrence of such or similar events in the future. Similarly, direct cause is the simplest action(s) or conditions that directly resulted in a problem, and which require(s) immediate attention and contributing causes are actions or conditions not directly responsible for the problem but whose existence contributed to the problem or made the consequences more severe.

The following root cause analysis techniques are predominantly used throughout the nuclear industry; they are below described in more detail, giving descriptions, strengths and weaknesses of each individual technique:

- ECFC - Event and causal factor charting
- ASSET/PROSPER
- HPES – Human performance enhancement system
- MORT – Management oversight and risk tree analysis

V.3.1.1 Event and Causal factor Chart (E&CF Chart)

Description

An E&CF Chart is a graphically displayed flowchart of an entire event plotted on a time line (Figure V-2). It is probably the most useful tool for recording and understanding the event progression. As an event line is established, additional features such as related conditions, secondary events and presumptions are added.

Strengths

- An excellent opportunity to graphically display barriers, changes, causes, effects, and human performance interactions.
- Organizes data and provides a broad picture.
- Easy to understand and communicate with those not familiar with the techniques (management, operators).

Limitations

- Can be time consuming.
- Rarely stands alone and greatly enhanced by superimposed barrier and change analyses.

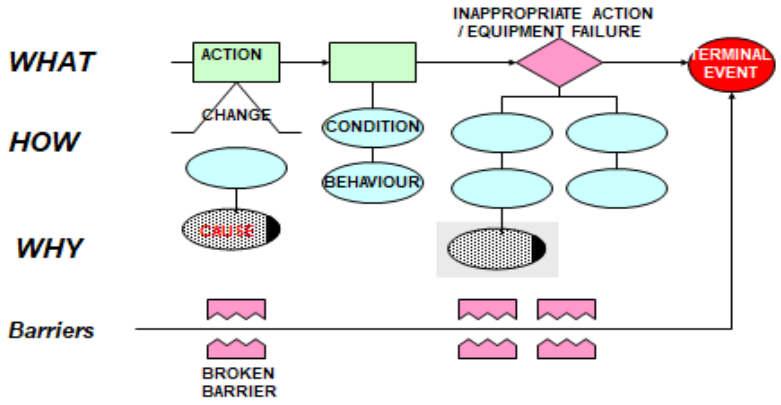


Figure V-2: Event and Causal factor Charting

V.3.1.2 ASSET/PROSPER

Description

The root cause methodology developed to support the IAEA ASSET/PROSPER Services program. Root causes are clearly defined as the answer to the question: why was it not prevented through a comprehensive surveillance programme?

Strengths

- Freely available to use.
- Used numerous times on ASSET/PROSPER Missions.
- Output is directed at NPP management.
- Training available by the IAEA.

Limitations

- Has a different definition of root cause from other techniques.
- Identifies deficiencies in management and policy, therefore requires knowledgeable senior staff to do the analyses.

V.3.1.3 HPES – Human Performance Enhancement System

Description

The techniques encompassed within the HPES package include:

- Task analysis, Change analysis, Barrier analysis, ECFC.
- Behavioral analysis, Situational analysis.
- Interviewing techniques.

Strengths

- Provides a toolbox of techniques.
- Proven methodology used worldwide.
- Training courses and handbooks available.

Limitations

- Requires experience and training to apply effectively.
- The process does not specifically identify organizational issues.

V.3.1.4 MORT – Management Oversight and Risk Tree

Description

The method consists of a Fault Tree together with a long series of interrelated questions.

Strengths

- Comprehensive Manual and Training available.
- Uses detailed Fault Trees.
- Flexible (can use parts of Fault Tree for small events).
- Uses Barrier analysis.
- Computerized version is available.

Limitations

- Requires experience to use.
- Time consuming due to extensive task analysis.

V.3.2 Probabilistic Precursor Analyses

Precursor analysis uses the concept of Conditional Core Damage Probability (CCDP) to determine the safety significance of an event. It is a measure in the PSA model of how far was an event which is being analysed from the core damage scenario. CCDP is defined as the probability of core damage given that either:

- an initiating event has happened at the plant or
- safety related equipment was out of service for prolonged time duration.

In some cases both can happen simultaneously, which would also be classified as a precursor. The Figure V-3 schematically represents a precursor with the initiating event and the prolonged safety system unavailability. In accordance with the above definition, there are two types of precursors:

- a transient which interrupts normal operation;
- unavailability or a degradation of equipment/systems for a longer time period.

In the first case when we are dealing with the transient that interrupts normal operation, we see a real effect on plant operation. In this case, it is easy to relate the event to an initiating event in the PSA. Scenarios or sequences in PSA that are affected by this event are all those developing from that particular initiating event.

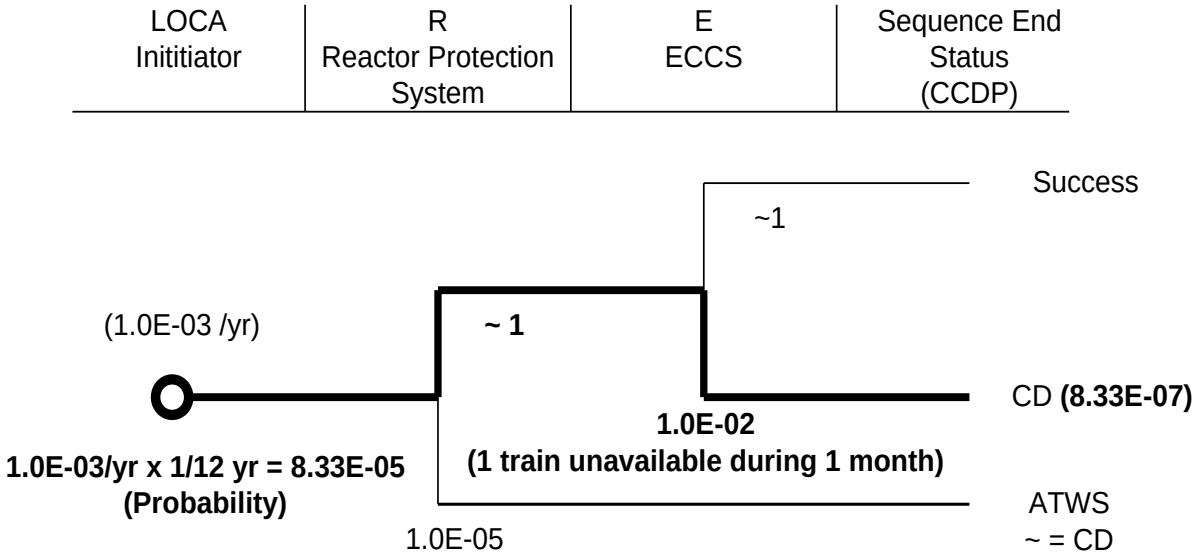


Figure V-3: Conditional Code Damage Probability (CCDP)

In the second case, when we are dealing with longer unavailability of safety systems, there is no immediate impact on plant operation. It is therefore harder to associate the event with any particular initiating vent in the PSA study. Precursor affects several safety functions that and all sequences, which involve the affected safety systems/functions for all initiating events need to be considered.

V.3.3 Deterministic transient analyses

Deterministic transient analyses are used for fast developing events i.e. transients. It is a simulation of the plant behaviour with a computer code. The NPP model is constructed by combination of smaller parts by the so-called nodalization process. By applying initial and boundary conditions as input data, the behaviour or the response of the plant is then calculated by simulation.

Such analyses are essential for better understanding of the physical phenomena taking place during a specific event. It is the only method that can calculate the erosion of safety margin while the event is happening. As such it is a great tool for simulating the plant behaviour and is therefore essential for operator training and procedure validation and verification.

In performing deterministic analyses we are basically comparing code predictions with the actual failures. Both code predictions and failures have uncertainties and are therefore a distribution functions (see Figure V-4).

Distribution of code predictions/results is a consequence of uncertainties in initial and boundary conditions data as well as in computer model.

Distribution of failures is on the other hand a consequence of our limited knowledge of the precise phenomena that cause failures.

Figure V-4 demonstrates the concept of safety margin. On the left hand side the calculation results are presented as the probability distribution and on the right hand side the probability distribution of failures. Both distributions are the consequence of above mentioned uncertainties. The difference between both distribution picks can be termed an “apparent

margin". The term is not fixed and also not universally accepted, it can be termed also differently, it is only important that it is precisely defined.

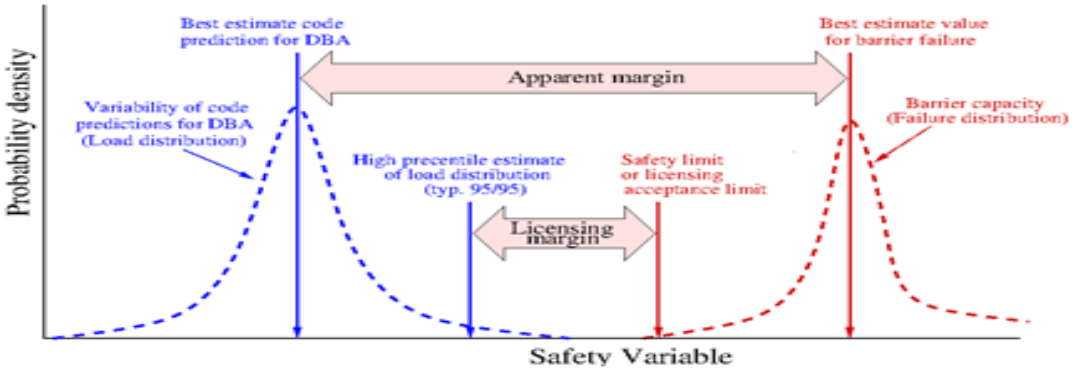


Figure V-4: Distribution of code predictions and distribution of failures

V.4 CONCLUSIONS

For the use of different event investigation techniques it can be generally concluded that:

- The Root Cause Analyses remain the predominant technique for incident evaluation as it reveals the true root causes that have caused the event to happen.
- Precursor analyses are the best method for determination of event safety significance.
- The Deterministic Transient Analyses are the only way to fully understand the physical behaviour of the plant during fast developing transients.

All three methods complement each other as not all events are alike and therefore it needs to be carefully examined when to apply each of the above methods on a particular event.

REFERENCES

[1] V.K. Duvvuru Mohan, P. Vardon, M. Dusic; Del 3.1 – Risk integration methods for high risk industries; NARSIS 2018.

VI Uncertainties and Risk Integration

Jeremy Rohmer
BRGM
3, av. Claude Guillemin, 45060, Orleans, Cedex 2, France
j.rohmer@brgm.fr

Varenya Duvvuru Mohan, Philip J. Vardon
Geo-Engineering Section, Faculty of Civil Engineering and Geosciences,
Delft University of Technology
Stevinweg 1, 2628 CN Delft, The Netherlands
v.k.duvvurumohan@tudelft.nl, p.j.vardon@tudelft.nl

Pierre Gehl
BRGM
3, av. Claude Guillemin, 45060, Orleans, Cedex 2, France
p.gehl@brgm.fr

ABSTRACT

The present communication addresses the problem of uncertainty quantification (UQ) within risk assessment frameworks used for nuclear power plants (NPPs). We first clarify the notion of uncertainty by analysing its link with risk and decision-making. Due to the difficulty in giving a single "fit-to-all" definition, we adopt a less ambitious (but more practical) approach, and define uncertainty through a classification. We highlight the necessity for separating two types of uncertainty, namely aleatory uncertainties (inherent to the variability/randomness of the system under study) and epistemic uncertainties (inherent to incomplete/imprecise nature of available information). By focusing on the problem of quantifiable uncertainty for any models supporting risk analysis of NPPs (whatever their type, analytical, expert-based, numerical), we further describe the main steps of a generic framework for UQ. In this study, Bayesian networks (BNs) are proposed as an integrative tool at each step of this framework, i.e. for uncertainty propagation, sensitivity analysis, what-if scenario study and probability updating. A simplified, 'toy' BN representing a flooding related station blackout event at a NPP, is used to show how BNs allow incorporation of all evidence in the probabilistic risk assessment and quantification of both aleatory and epistemic uncertainties.

VI.1 INTRODUCTION

The present study addresses the problem of uncertainty quantification (denoted UQ) with application for risk analysis of nuclear power plants (NPPs). The field of uncertainty is very broad, and we adopt here the view of modelling, i.e. we focus on the problem of quantifiable and quantification of uncertainty for any models (whatever their type, analytical, expert-based, numerical) supporting a risk analysis for NPPs. The objective is twofold: (1) clarifying the notion of uncertainty with respect to its role in risk modelling and decision-making; (2) describing the main steps of the framework for UQ. To support the second objective, we

propose Bayesian networks (BNs) as an integrative tool at each step of this framework. The study is organized following the afore-described objectives.

VI.2 SETTING FOR UNCERTAINTY QUANTIFICATION

Uncertainty can be interpreted differently depending on the discipline and context where it is applied, therefore we have avoided defining a single "fit-to-all" definition. A less ambitious (but more practical) approach is adopted, similar to that adopted by several other authors, in particular [1], who define uncertainty through a classification (Sect. VI.2.1). Such an approach presents the appealing feature of enabling the risk practitioners to differentiate between uncertainties and to communicate about it in a more constructive manner. Sect. VI.2.2 then aims at going a step further by describing a generic framework for UQ. The description of this generic framework is mainly based on practices for uncertainty assessment and management in an industrial context [2].

VI.2.1 Uncertainty classification

The basis of the classification is the distinction of two major types of uncertainty as discussed by [3] [4]:

- Aleatory uncertainty/variability (also referred to as randomness). The physical environment or engineered system under study can behave in different ways or is valued differently spatially or/and temporally. The aleatory variability is associated with the impossibility of predicting deterministically the evolution of a system due to its intrinsic complexity. Hence, this source of uncertainty represents the "real" variability and it is inherent to the physical environment or engineered system under study, i.e., it is an attribute/property;
- Epistemic uncertainty. This type is also referred to as "knowledge-based", as the Greek term *episteme* means knowledge. In contrast to the first type, epistemic uncertainty is not intrinsic to the system under study and can be qualified as being "artificial", because it stems from the incomplete/imprecise nature of available information, i.e., the limited knowledge of the physical environment or engineered system under study.

Such a definition remains quite broad and a sub-categorization is proposed:

- Data uncertainty: This source stems from the difficulties in measuring the properties of the system under study or from the recording and processing procedure;
- Parameter uncertainty: This source arises from the difficulties in estimating the input parameters (in a broad sense) of models/analysis due to the limited size, poor representativeness (caused by time, space and financial limitations), and imprecision of the observations/data. An alternative to overcome the described difficulties is to rely on information based on experts' judgments. But, such information can be qualitative and vague. In any case, from one expert to another, views can change, hence this procedure can possibly end in conflict (i.e., disagreement);
- Model uncertainty: This source can appear at two main levels: (1) Uncertainty in the structure/form of the model, which depends on the choice of variables, dependencies, processes, etc., regarded as "relevant and prominent" for the required role of the model; (2) Uncertainty can also arise from the unambiguous choice of the "best" model to be used. The general purpose of modeling is to reproduce the behavior of the real system

and the "quality" of such a task can be appreciated through the validation of model-based predictions with respect to real observations. Yet, in some cases, several types of models (e.g., differing in their structure and input variables) can achieve a comparable "goodness of fit" to the observations. Figure VI-1 illustrates this aspect by providing a series of "plausible" PGA-frequency relationships.

- Scientific uncertainty: this broad class is difficult to define in an exhaustive manner and can be understood as the current state of scientific knowledge and understanding of the natural processes governing the behavior of a system.

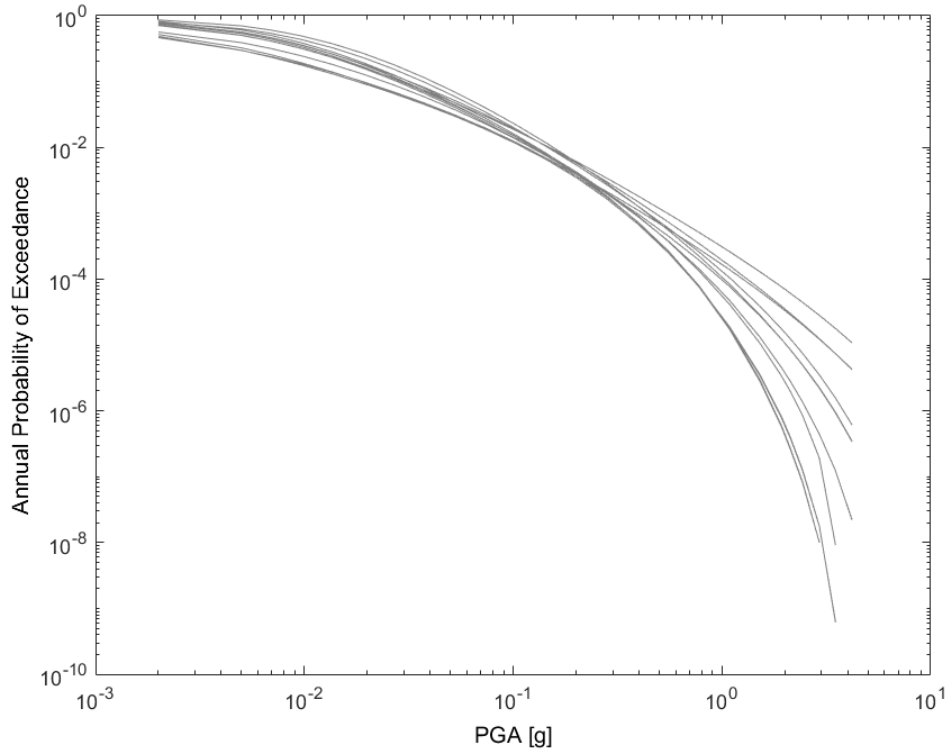


Figure VI-1: Series of plausible models to describe the variability of PGA on a site in Italy (adapted from [5]).

VI.2.2 Treatment setting

Sect. VI.2.1provides a pragmatic approach for dealing with uncertainties, namely by proposing a classification procedure. Though simple, this approach has the great advantage to invite the risk practitioners to reflect on the available knowledge at hand before conducting the risk analysis. To put it simply, the classification approach should be seen as an invitation of the risk practitioner to answer the question about "what do I know?" before addressing the question of "what can I do?". Sect. VI.2.2aims to describe a generic framework for UQ mainly based on practices of uncertainty assessment and management in an industrial context [2]. This framework follows different steps, which are summarized in Figure VI-2.

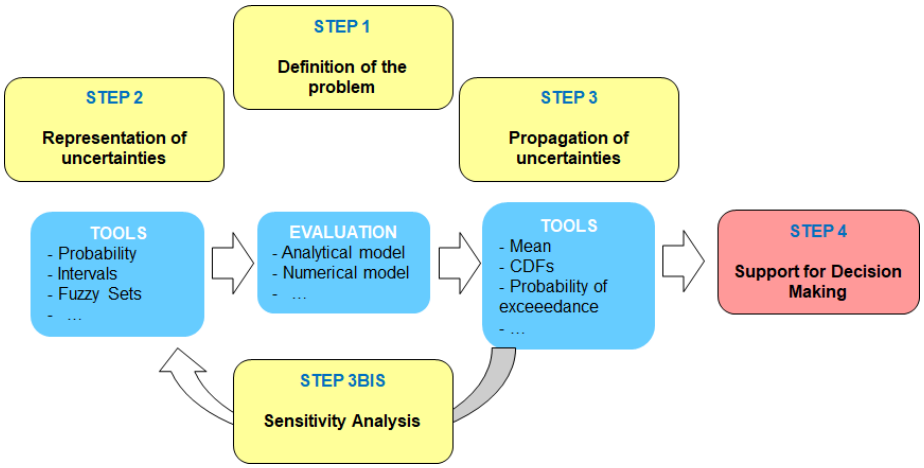


Figure VI-2: Main steps of the generic framework for UQ (adapted from [2])

VI.2.2.1 Step 1: Problem definition

The first step aims at defining the problem by clarifying the decision and the modelling context. The purpose of UQ can be multifold and depends on the decision context. In step 1, the following questions about the decision context should be first addressed, namely: "what type of question do I seek understand to support decision-making?" After [2], different objectives can be followed, namely: (1) Understanding the influence of uncertainties, which can help guiding additional measurements, modelling or R&D efforts; (2) Giving credit to the model, i.e. to reach an acceptable quality level for its use. This may involve calibrating parameters of the model inputs, simplifying the model (e.g., by neglecting some physical processes), fixing some model inputs; (3) Comparing different scenarios and optimizing them with respect to the design of the system for instance; (4) Demonstrating the compliance of the system with a given criterion or regulatory threshold.

VI.2.2.2 Step 2: Uncertainty representation

The second step aims at mathematically modelling the available knowledge i.e. at selecting the most appropriate mathematical tools and procedures for representing the available data/ information while "accounting for all data and pieces of information, but without introducing unwarranted assumptions" [6]. The most widespread tool for this task is the one provided by the probabilistic setting. When a large number of observations are available, the probability distribution can be fitted to data/observations within a frequentist approach. When experimental data / observations are insufficient, alternative approaches can rely on the use of Bayesian methods. See an application example using Bayesian network in [7]. This basically allows mixing subjective and objective information, i.e. perception regarding a probabilistic model (subjective probabilities consistent with the axioms of probability), and observations/data for model update. Further details are provided in Sect. VI.3.

VI.2.2.3 Step 3: Uncertainty propagation and sensitivity analysis

This step focuses on the quantification of uncertainty in the model output. When Step 2 has selected probabilities as an appropriate tool for uncertainty representation, the most versatile and popular propagation method for Step 3 is based on Monte-Carlo random sampling. A major advantage of Monte-Carlo sampling technique is that it can be easily implemented and can take into different pieces of information (in particular probabilistic distribution on the inputs and potentially their dependence). Yet, the major drawback is the number of samples required,

which can depend on the type of quantity of interest. To overcome the computational burden, a combination with surrogate techniques (known also as metamodels or response surfaces) can be envisaged (e.g., [8]). The "uncertainty propagation" part of Step 3 is usually run in tandem with the "sensitivity analysis" part, which aims to study "how uncertainty in the output of a model (numerical or otherwise) can be apportioned to different sources of uncertainty in the model input" [9].

VI.3 BAYESIAN-NETWORK AS AN INTEGRATIVE TOOL

VI.3.1 Introduction to Bayesian Network

A BN is a specific application of Bayesian probability theory. A BN is a directed acyclic graph which is composed of nodes that correspond to random variables, and arcs that link dependent variables [10]; see an example in Figure VI-3. The direction of the arcs indicate the cause-effect relationships between the nodes ("directed"), and these arcs never cycle back to parent nodes ("acyclic"). Hence, a BN is a visually explicit representation ("graph") of the mutual causal relationship between random variables (denoted Xi), and represents the joint probability distribution (JPD) of all random variables within the model.

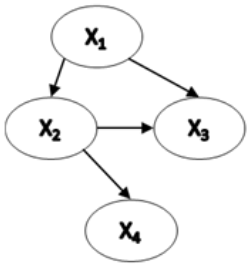


Figure VI-3: An example Bayesian network

The dependencies between random variables are usually encapsulated within conditional probability tables (given by ($P(X_i)|Parents(X_i)$)) at each node of the BN. The JPD is given by the chain rule of BNs:

$$P(X_1, X_2, \dots, X_n) = \prod_{i=1}^{n} P(X_i|Parents(X_i)) \quad (1)$$

The JPD of the static BN shown in Figure VI-1 is given by:

$$P(X_1, X_2, X_3, X_4) = P(X_1)P(X_2|\,X_1)P(X_3|X_1, X_2)P(X_4|\,X_2) \quad (2)$$

Through Bayesian inference, the JPD can be queried to infer the state of a random variable given our beliefs regarding the other variables. In other words, BNs can be used to answer probabilistic queries when one or more variables have been observed.

To demonstrate the capabilities of BNs in UQ, a simplified example of a flooding related station blackout situation was considered, where alternate current power sources have failed. The power plant has been assumed to be dependent on direct current (DC) sources, i.e. a battery and two diesel generators (DG1 and DG2). This DC power system was modelled by a simple fault tree obtained from [11], with hypothetical annual probabilities of failure, as shown in Figure VI-4. DG1 was assumed to be housed in Building 1 and, DG2 and the battery were assumed to be located in Building 2. These are reinforced concrete buildings with two damage states - fully functional or fully damaged - and their fragilities against flood water levels are

identically modelled based on [12]. The generators and battery were assumed to be situated at a height of 8 m above ground level. The buildings could be subject to flood loading - a water level, and it was assumed that the components inside cannot be flooded (due to their elevation) unless there is structural failure. The entire scenario, of course, is neither representative of the configuration of backup power systems in an actual NPP, nor is it an accurate model of the flooding related SBO situation. The purpose of this example is merely to demonstrate the use of BNs in UQ.

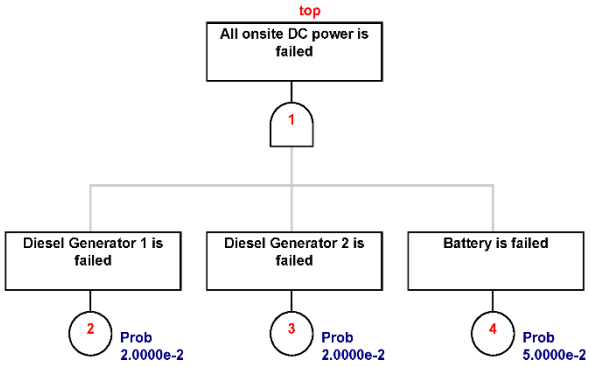
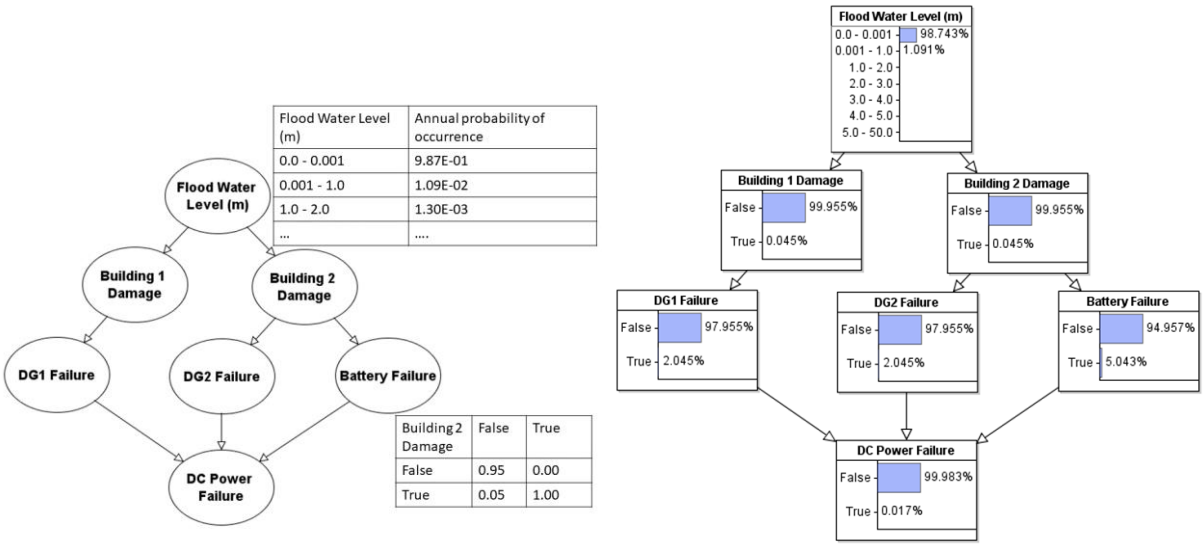


Figure VI-4: Example fault tree of DC power system, assumed for demonstrative purposes

VI.3.2 Uncertainty representation

Figure VI-5a shows a BN representation of the assumed scenario, where the top event is the failure of all onsite DC power during flooding. The structure of the BN, i.e. the random variables and the arcs, is modelled based on the above problem definition. The uncertainty in the flood water level is represented within the BN as a probability distribution (assumed) within the corresponding node. Similarly, fragilities of the buildings, and failure probabilities of DG1, DG2 and the battery are represented as conditional probability distributions (CPDs) at their corresponding nodes, conditional on their respective parent nodes. Thus, the existing uncertainty in input variables are elegantly represented within the BN via CPDs at the nodes. The CPDs can be filled using data or expert judgement. Figure VI-5a shows example CPDs at the ‘Flood Water Level’ and ‘Battery Failure’ nodes. The BN structure and CPDs together represent the JPD of the random variables in this problem.



(a) (b)

Figure VI-5: (a) Uncertainty representation - BN structure and CPDs at "Flood Water Level" and "Battery Failure" nodes; (b) Uncertainty propagation – Marginal probability distributions at each node, calculated within the BN, i.e. predictive inference.

VI.3.3 Uncertainty propagation

Since, the Bayesian network definition does not limit the type of conditional probability distribution, multi-state discrete or continuous random variables can be represented. Figure VI-5b shows the marginal probability distributions at each node as calculated by the BN using the CPDs. At the 'Flood Water Level' node uncertainty is represented via a discrete probability distribution, where the most likely state is that of negligible flood levels (between 0 and 0.001 m with a probability of almost 0.99). There is, however, a non-zero probability for even a high flood level (greater than 5 m). Nevertheless, it is not certain that the buildings will be damaged given any flood level. The probability of building damage is estimated using the CPD of "Building 1 (or 2) Damage" given "Flood Water Level". Given building damage, the generators and batteries are certain to fail, but there is also an inherent unreliability in the functioning of these equipment. This, for instance, is represented in the CPD at the "Battery Failure" node where the battery has a 5 percent chance of failure even when there is no building damage. Thus, the uncertainty in the input variables is propagated using the CPDs and the BN structure, all the way to the top event probability.

VI.3.4 Sensitivity analysis and probability updating

Given evidence for the state of one or more variables, the BN can be used to obtain the posterior marginal probabilities of all other variables – the process of Bayesian inference within the BN. Predictive inference, for instance, is when evidence is set for one of the input variables and the updated top event probability is obtained. In addition, the BN also allows for diagnostic inference, wherein updated posterior marginal distributions of input variables can be obtained, conditional on a given state of the top event. Figure VI-6 shows examples of using inference within the BN. Through predictive and diagnostic inference, sensitivity analyses can be easily performed using the BN by setting evidence and updating the network. In Figure VI-6a, the water flood level is set to a specified level, the BN then propagates the probabilities, i.e. uses

predictive inference, and predicts the likelihood of the top event, here the DC power failure. In Figure VI-6b, the DC power failure has been set to be true, and by using diagnostic inference, the marginal probabilities of different flood water levels have been calculated. Figure VI-7 shows the sensitivity of the top event to various input parameters using a tornado diagram. Parameters are varied individually from their minimum to maximum values and the effect on the probability of the top event occurring is plotted in order of impact. This shows the high influence of the 'Flood Water Level' node on the probability of DC power failure.

Similarly, when new data is available, it is easily integrated into the BN to provide updated probability estimates via probability updating procedures.

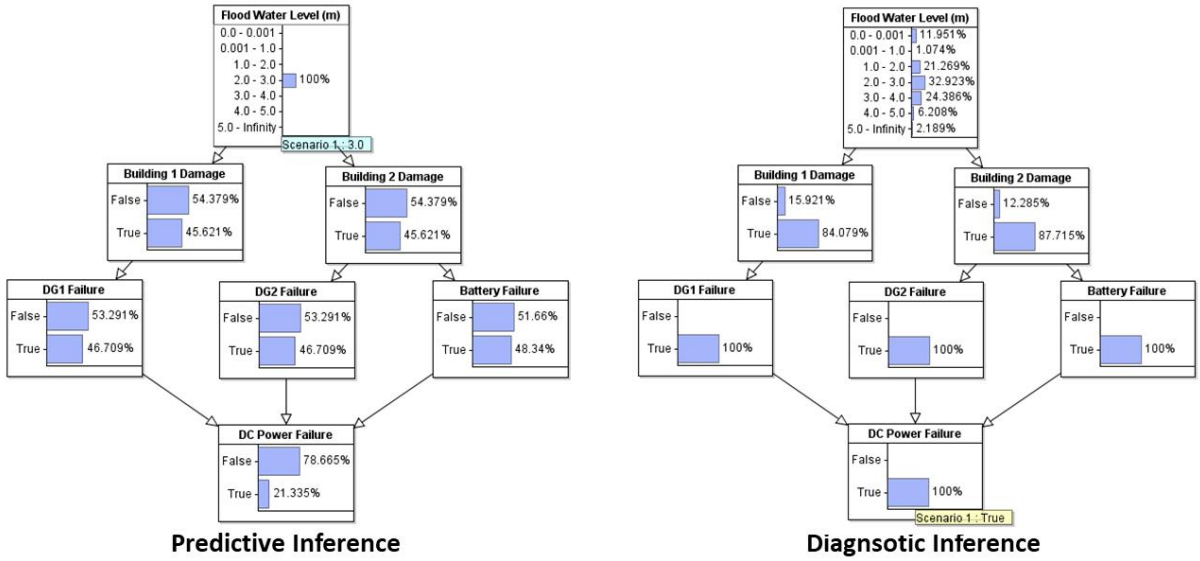


Figure VI-6: Predictive and diagnostic inference in BN, used in sensitivity analysis and probability updating.

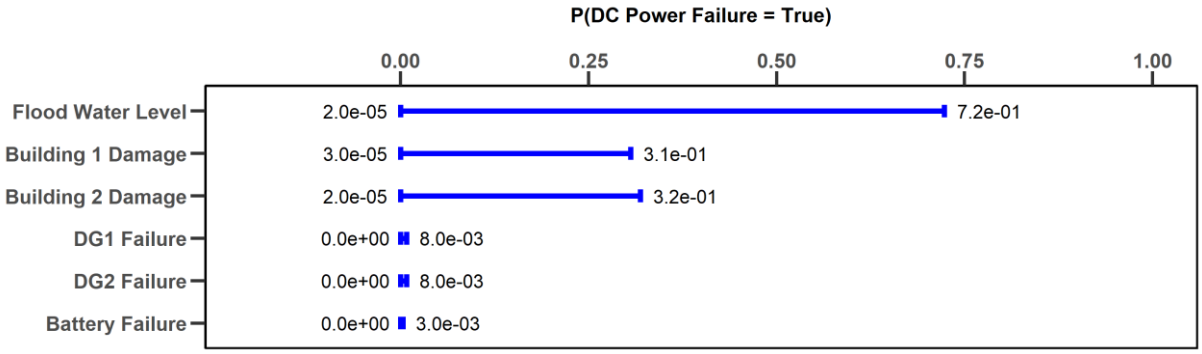


Figure VI-7: Sensitivity analysis in the BN – Change in probability of top event being true, for variation between minimum and maximum values of each random variable

VI.4 CONCLUDING REMARKS

Risk analysis of NPP are associated with large uncertainties. The UQ setting described in the present study can be applied to first clarify the types of uncertainty (by using the proposed classification) and to provide quantification of the impacts and influences of the identified uncertainties. In this framework, BNs appear as a valuable tool to fulfil the objectives all stages

of the UQ setting (uncertainty representation, propagation and sensitivity analysis) in addition to the capability to perform probability updating, which are useful to explore what-if scenarios.

REFERENCES

[1] M. B. A. van Asselt, J. Rotmans, "Uncertainty in Integrated Assessment Modeling", Climatic Change, 54(1-2), 2002, pp. 75-105.

[2] E., de Rocquigny, N. Devictor, S. Tarantola (Eds.), "Uncertainty in industrial practice - A guide to quantitative uncertainty management", John Wiley & Sons, 2008

[3] M. E. Paté-Cornell, "Uncertainties in risk analysis: Six levels of treatment", Reliability Engineering & System Safety, 54(2-3), 1996, pp. 95-111.

[4] G. Apostolakis, "The concept of probability in safety assessments of technological systems", Science, 250(4986), 1990, pp. 1359-136.

[5] P. Gehl, J. Rohmer, "Vector intensity measures for a more accurate reliability assessment of NPP sub-systems". Proc. International Conference on Technological Innovations in Nuclear Civil Engineering, Saclay, France, 2018.

[6] M. Beer, S. Ferson, V. Kreinovich, "Imprecise probabilities in engineering analyses". Mechanical Systems and Signal Processing, 37(1), 2013, pp. 4–29.

[7] S. Kwag, A. Gupta, "Probabilistic risk assessment framework for structural systems under multiple hazards using Bayesian statistics". Nuclear Engineering and Design, 315, 2017, pp. 20-34.

[8] B. Auder, A. De Crecy, B. Iooss, M. Marques, "Screening and metamodeling of computer experiments with functional outputs. Application to thermal–hydraulic computations", Reliability Engineering & System Safety, 107, 2012, pp. 122-131.

[9] A. Saltelli, M. Ratto, T. Andres, F. Campolongo, J. Cariboni, D. Gatelli, M. Saisana, S. Tarantola, "Global Sensitivity Analysis: The Primer". Chichester, UK: Wiley, 2008.

[10] Jensen, F., "Bayesian Networks and Decision Graphs". Springer, New York, 2001.

[11] Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. "Fault tree handbook (No. NUREG-0492)". Nuclear Regulatory Commission Washington DC, 1981.

[12] De Risi, R., Goda, K., Mori, N., & Yasuda, T. "Bayesian tsunami fragility modeling considering input data uncertainty". Stochastic Environmental Research and Risk Assessment, 31(5), 2017, pp. 1253-1269.

VII Risk Assessment Using Bayesian Approach: Risk Informed Validation Framework and Multi-Hazard Risk Assessment

Abhinav Gupta
Center for Nuclear Energy Facilities and Structures (CNEFS)
North Carolina State University
27695, Raleigh, USA
agupta1@ncsu.edu

Saran Bodda, Harleen Kaur Sandhu, Nam Dinh
North Carolina State University
27695, Raleigh, USA
ssbodda@ncsu.edu, hksandhu@ncsu.edu, ntdinh@ncsu.edu

ABSTRACT

USNRC and IAEA have developed methodologies to assess the safety vulnerabilities of nuclear plants against site specific extreme hazards following the Fukushima-Daiichi nuclear accident. In many cases, high fidelity simulation tools are being employed to simulate multi hazard, multi-physics, multi-scale phenomena and to evaluate vulnerability of nuclear facilities. The accuracy of simulation codes is essential so that they can be used with confidence for decision making. The credibility of high fidelity simulation tools is assessed based on a formal verification, validation, and uncertainty quantification (VVUQ) procedure. One of the key limitations in validation is lack of relevant experimental data at system-level and sub-system level. Subsequently, this limitation leads to excessive reliance on expert opinion and decrease in confidence levels in the prediction of system level results. Probabilistic risk assessment (PRA) has been widely used to examine the risk posed by nuclear facilities and to identify the key components whose failure can have the most impact on safety. However, a traditional PRA approach has its limitations in the use of fault trees and event trees. The limitations can be addressed by implementing Bayesian network (BN) representation of PRA. In this manuscript, we present a state-of-the-art review on external multi-hazard risk assessment methodologies and a risk informed validation framework for a simplistic external flooding scenario.

VII.1 MULTI-HAZARD RISK ASSESSMENT FRAMEWORKS

Multi-hazard scenarios have not been considered in traditional PRA studies because the possibility of simultaneous occurrence of two different extreme events such as earthquake and hurricane or earthquake and flood is extremely rare and almost impossible. However, there have been several instances of closely-related multiple hazards that have resulted in significant damage or a major disaster. Only a limited number of studies [1]-[5] have been conducted to consider multi-hazard scenario in the design or risk assessment. The common theme in all these studies is that the risk is calculated separately for each individual hazard and the overall risk is computed by using the total probability theorem.

The fundamental assumption in using the total probability theorem is that individual hazards are statistically independent, mutually exclusive, and collectively exhaustive.

Therefore, it cannot be used for assessment of risks associated with multi-hazard scenarios in which the undesirable response of the plant to one hazard acts as the initiator of another hazard making them correlated events. Traditional PRAs do not exhibit such correlated events because failures of these types are not encountered in a plant that is well designed to withstand the design basis events. Consequently, there is a need for developing multi-hazard risk assessment methodologies to account correlated events beyond the design basis levels and to determine a plant's vulnerability. As additional studies are conducted, and new data becomes available, such methodologies should allow easy and continued updating of plant risk.

Design and retrofit approaches for multi-hazard scenarios have received considerable attention in recent years. However, the concept of multi-hazard analysis is quite broad and the nature of existing studies varies across a wide spectrum of problems [6].

The concept of Bayesian networks for multi-hazard risk assessments has been investigated by a few researchers and it has provided promising results in this field. Wang et al. [7] provided a methodology to develop powerful earthquake disaster chains by using Bayesian networks. This study summarized 23 earthquake disaster chains including the serial, parallel and the serial-parallel chain types. A Bayesian network model for a disaster chain, as earthquakes, landslides, barrier lakes and floods, is constructed and the most critical links are identified using probabilistic inference. This paper also describes the Bayesian network concepts in detail and how to apply to the disaster chain concepts.

A study by Kwag and Gupta [8] introduces a Bayesian framework for PRA of structural systems under multiple hazards. This framework allows for consideration of correlations and dependencies between various initiating events and for updating the framework to incorporate newly collected data at any level. A systems analysis for a traditional PRA usually consists of fault tree analysis and event tree analysis. Instead, a Bayesian network with Bayesian inference is used to conduct a multi-hazard risk assessment in this paper by mapping the conventionally used fault tree approach into a Bayesian network. An example of a simple fault tree and corresponding mapped Bayesian network is illustrated in Figure VII-1.

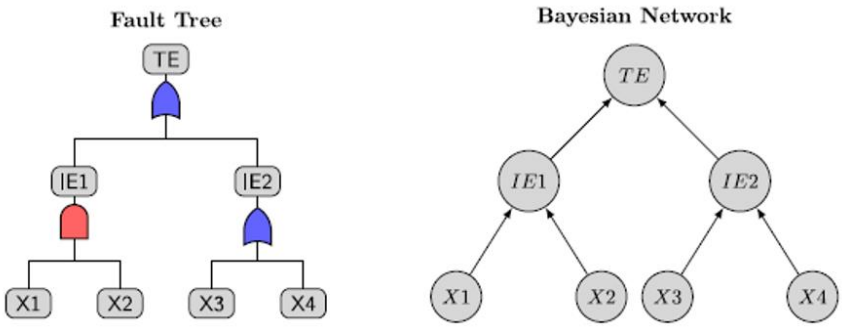


Figure VII-1: Example of Simple Fault Tree (left) and Corresponding mapped BN (right) [8]

Incorporating Bayesian inference provides a new way to explore system-level vulnerability. It is likely that the system-level vulnerability may produce different results than the original one due to consideration of correlation and dependency between the initiating events. This method can also give better results for scenario with a single hazard since it will allow for consideration of the correlation between multiple failure modes of various SSCs of an NPP. Kwag and Gupta [4] further illustrates the approach by employing it for a single hazard

PRA and a multi-hazard PRA (earthquake, high winds and flooding). A correlated seismically induced internal flooding hazard scenario is also illustrated in Kwag and Gupta [8].

VII.1.1 EARTHQUAKE INDUCED EXTERNAL FLOODING HAZARDS

Jang and Yamaguchi [9] proposed a dynamic PRA approach for considering earthquakes and internal flooding events. It is assumed that an earthquake induces a tube rupture in the power plant and a numerical simulation is carried out for incorporating internal flood propagation. The continuous Markov model and Monte Carlo methods are utilized in the proposed approach in order to generate the accident scenario quantification.

Another study was recently conducted to include the accident-sequence analysis methodology considering seismic-tsunami events [10]. The paper proposes a PRA approach for seismic-tsunami events by characterizing the dependencies and correlations between various nuclear power plant SSCs; creating logic trees for failure of SSCs; and modeling of an intermediate state (degraded state) between the normal and failure state of the core-damage logic tree. The proposed model is applied to the reliability analysis of parallel and series systems.

VII.1.2 FUTURE WORK RECOMMENDATIONS

As can be inferred from the discussion above, the field of multi-hazard PRA is still developing and much of the research is still in its infancy. A few aspects stand out that need further investigations are listed below.

- **Cascading Events:** A key observation relates to primary shortcoming of treating different hazards independently. Events in individual hazard PRA can be correlated and eventually change the critical path. Subsequently, one can exhibit cascading events which otherwise get ignored. Such scenarios are critical to identify. More work is needed to develop appropriate methodologies such as Bayesian network based methodology to address this issue.
- **Role of Multi-hazard PRA in Decision Making under Accident and Emergency Conditions (Level 2 PRA):** As evident from many events in both nuclear and non-nuclear applications, the operators or other decision makers are often left clueless under a multi-hazard scenario. All training procedures relate to a single hazard. It is very essential for the decision makers to understand what SSCs in plant are related to cascading failures under a multi-hazard accident scenario. It is also important to relate the real time plant data under such extreme conditions to the potential strategies of mitigation and rank different options based on the prior knowledge, plant data, and simulation data. However, doing so in real time is almost impossible given the response time of any search algorithm under a vast set of possible scenarios. It is possible to address this concern through the use of a network of networks approaches wherein each hazard PRA is one network and a multi-hazard PRA represents network of networks.
- **Role of Dynamic Bayesian Network in PRA:** In conventional PRA methodologies, Event trees and Fault trees are widely used to analyze accident scenarios. Dynamic event trees are employed to capture the transient behavior of the events. However, these trees have limitations in certain applications such as: (1) statistical correlations between basic events, (2) non binary or distributional relationship between intermediate and basic events, (3) more than one initiating event (multi-hazard), (4) treatment of uncertainty quantification, and (5) time dependencies between variables. Dynamic Bayesian

networks (BN) have been successful in addressing these issues through a unified single formulation. Mapping algorithms are required to transform the conventional fault trees and event trees into a BN, and dynamic event trees into a dynamic BN.

- **Role of FLEX Equipment in PRA:** FLEX equipment is a portable power-generating equipment that is stored at a pre-selected geographical location, as is identified with almost zero probability of occurrence of natural disasters. FLEX equipment provides an effective alternative cooling method in case of a severe accident due to natural hazards. It can alter the risk profiles and can significantly decrease the core damage frequency (CDF). Validation for multi-hazard PRA is necessary to quantify the credibility of risk estimates that are based on high fidelity simulation codes. However, traditional deterministic approaches for validation are not effective. As a first step to develop a validation approach, we propose a new validation framework for a single hazard PRA which is based on risk informed methodology.

VII.2 RISK INFORMED VALIDATION FRAMEWORK

The framework employs two key stages that are described below. The complete framework is illustrated through the flowchart in Figure VII-2.

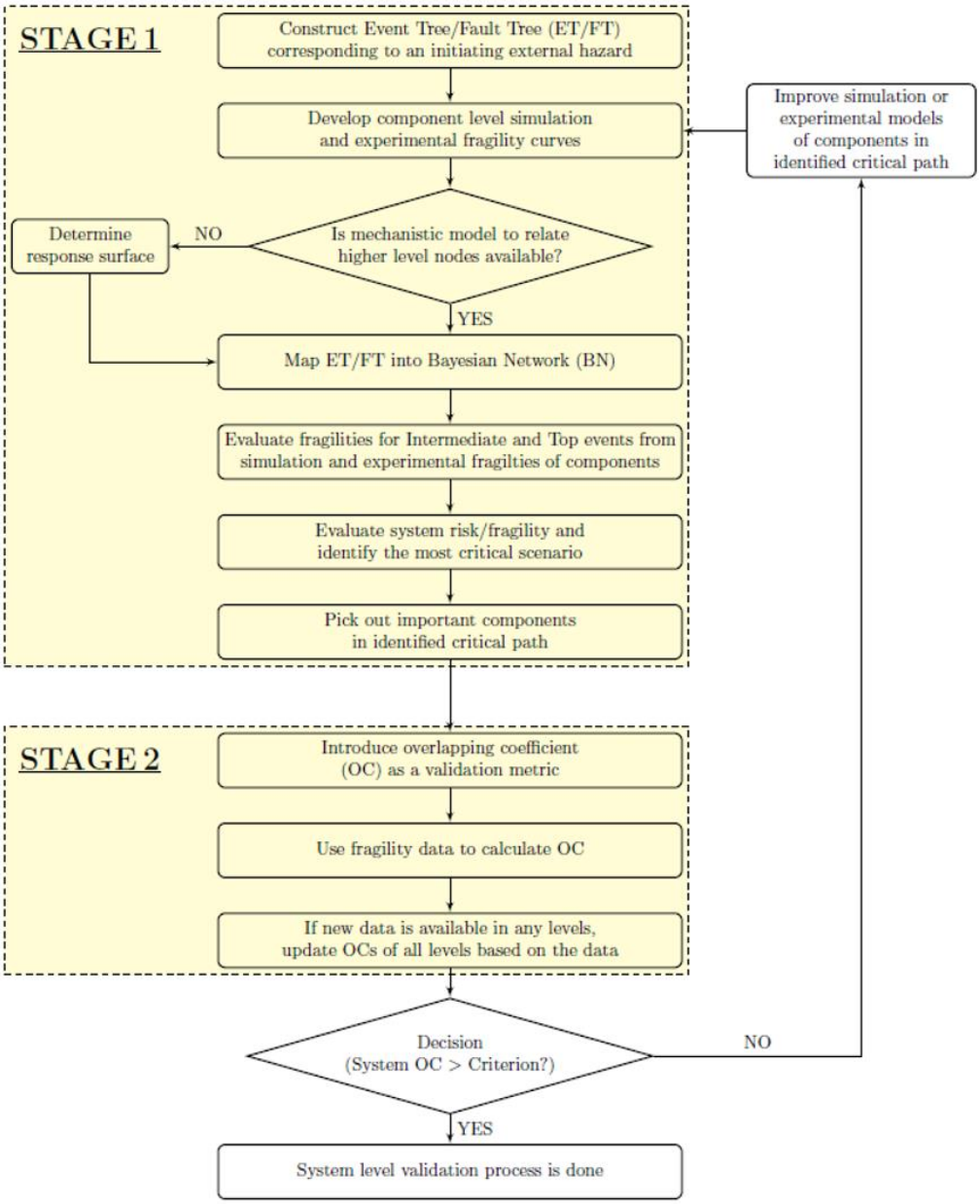


Figure VII-2: Flowchart of Proposed Validation Framework

STAGE 1

- Develop an event tree to represent all possible accident scenarios resulting from an initiating external flood hazard.
- Construct required fault trees to obtain the failure probability of each event in the event tree.
- Develop simulation and experiment based fragility curves for all the basic events. In general, fragility assessment requires use of a Monte Carlo approach to include uncertainties from various sources. However, if sufficient knowledge base has been developed then one can make use of the standard lognormal fragility parameters.
- Develop response surfaces between the basic events and intermediate events especially if a mechanistic relationship is not directly known.

- Map the event tree and fault trees into a Bayesian network.
- Evaluate system fragility by propagating the simulation based fragility information from basic events through the Bayesian network.
- Identify critical events with respect to system vulnerability.

STAGE 2

1) Calculate overlapping coefficient based on simulation and experimental fragility curves.
2) At this stage if new data becomes available, update overlapping coefficients.

DECISION

- Compare system level overlapping coefficient with a predefined acceptance criterion.
- If the adequacy of system level validation is not satisfied, collect more experimental data or improve simulation models of the identified critical events.

VII.3 ILLUSTRATION/CASE STUDY: FLOODING

In this section, we illustrate the application of the proposed framework to a synthetic example of a simplistic flooding scenario. The synthetic example is shown in Figure VII-3 and the scenario begins with an external flooding event caused by a storm surge. The floodwall protecting the plant can either fail or be overtopped due to the storm surge. In either case, it leads to flooding at the plant. This is known as Landscape flooding. When the landscape starts overowing, the vent at the diesel generator (DG) room can break and be overtopped. Failure of vent will eventually lead to flooding of the DG room and failure of the DG. For simplicity, we consider the accident sequence up to the DG failure. Next, we connect the individually validated events through the PRA informed validation framework proposed in this study.

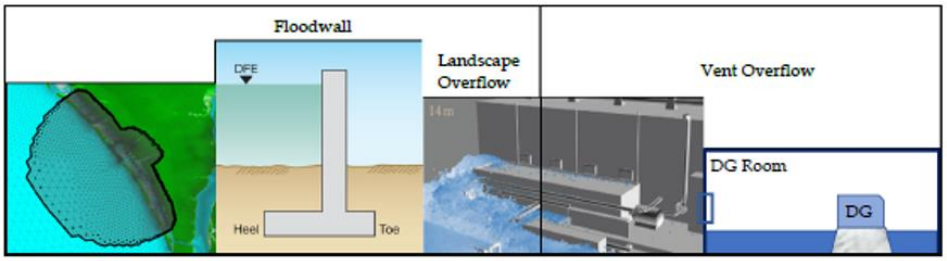


Figure VII-3: Accident sequence layout of Synthetic Example

VII.3.1 Event Tree / Fault Tree Logic

The event tree resulting from this synthetic example is shown in Figure VII-4, and includes the following top events: Initiating Event, Protective Floodwall, Protective Vent, and Onsite AC Power.

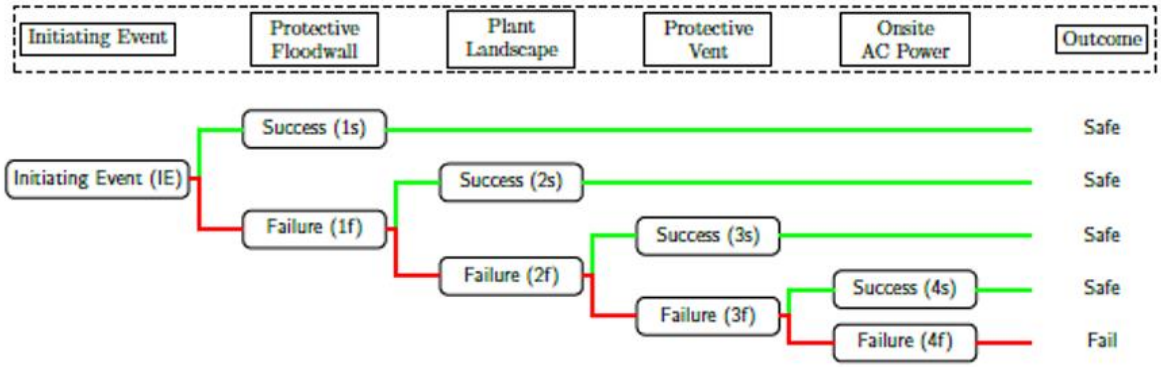


Figure VII-4: Event Tree logic for the synthetic example

VII.3.2 Fragility Estimates

Development of simulation-based fragility models for the top events mentioned in the previous section can be either a finite element (FE), computational fluid dynamics (CFD) or a smoothed-particle hydrodynamic (SPH) simulations [11]-[15]. In this study, the intensity measure for the initiating event is storm surge height. Therefore, all the fragility models need to be developed based on the surge height for risk calculation. Moreover, in a PRA informed validation framework as we propagate fragilities from basic events to intermediate-level events, the intensity measure must be same for all the events. However, the intensity measure for the flooding fragility analysis of individual events can be different. For example, the water level in the DG room depends on the flood elevation over the vent. Similarly, the landscape flooding inundation depends on the height of the water over the floodwall which in turn depends on the surge height. In order to have same intensity measure for all the events, it requires interaction between different models, software, and domains.

Table VII-1: Simulation and Data-driven fragility parameters

TOP EVENT	*Simulation Fragility*		*Data-driven Fragility*	
	Median, $\hat{\lambda}$ (ft.)	SD, β_{AU}	Median, $\hat{\lambda}$ (ft.)	SD, β_{AU}
1. Floodwall Failure	1.9	0.20	1.7	0.30
2. Landscape Flooding	2.0	0.20	1.6	0.35
3. Vent Overflow	2.2	0.15	2.3	0.25
4. DG Failure	3.9	0.20	3.1	0.35

VII.3.3 Critical Events

The critical events are obtained based on simulation models. When we propagate fragilities through the Bayesian network, the end state fragilities are governed by the DG Failure event as shown in Figure VII-5 and the reason is explained as follows. The end state fragility is simply obtained by multiplying all the top event fragilities. As seen in Figure VII-5, the simulation fragility of DG Failure event starts around a storm surge height of 2.5 ft and the rest all events reach a failure probability of 1 around this surge height. Therefore, when the end state simulation fragility is computed, the DG Failure event nullifies the effect of all other events.

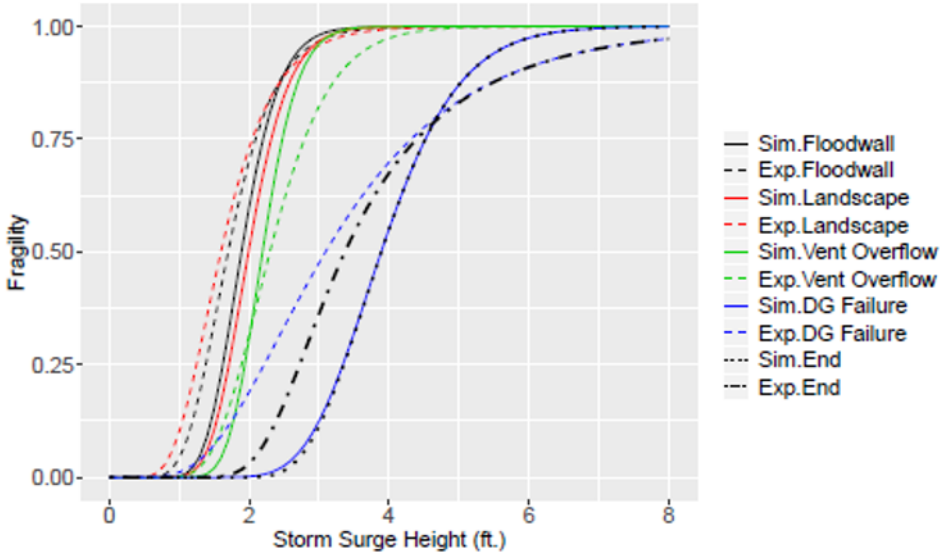


Figure VII-5: Simulation and Experimental (median) fragility curves

VII.3.4 Validation Metric

In the next step, overlapping coefficient is calculated for all the top events as shown in **Erreur ! Source du renvoi introuvable.**. The OC for the system level has a mean of 59% which would be unacceptable if an acceptance criterion of 75% is adopted. Therefore, the overall validation has to be improved either by enhancing the simulation model or collecting additional experimental/field data for the DG Failure event until the adequacy of the system level validation is satisfied.

Table VII-2: Validation Metric of all Top Events and System level

TOP EVENT	Overlapping Coefficient
1. Floodwall Failure	71.86 %
2. Landscape Flooding	60.06 %
3. Vent Overflow	63.67 %
4. DG Failure	50.04 %
System Level (End State)	58.55 %

VII.3.5 Additional Data - Updating

In this study, we assume additional field data is collected for the DG Failure event. The additional data is given in terms of failure rate as shown in **Erreur ! Source du renvoi introuvable.**. Based on this new information, the experimental fragility curves and the subsequent OCs are updated using Bayesian inference [16].

The updated value of OC for the DG Failure event is 71.40% and the OC for the system level is 75.1%. Therefore, the validation of DG Failure event has improved due to the additional data and thereby improving the overall system level validation.

Table VII-3: Additional Failure data for DG Failure event

Surge Height (ft.)	No. of Failures	Total Test Cases
3	5	50
4	28	50
5	45	50
6	49	50

VII.4 SUMMARY AND CONCLUSIONS

In addition to traditional single hazard based safety assessments, multi-hazard risk assessments of nuclear facilities is gaining significant importance as the facility might be subjected to different external hazards at same time. This paper presents a state-of-the-art review for multi-hazard risk assessment and a novel approach to quantitatively assess the system-level validation for a single hazard through a PRA informed validation framework. Event tree and fault trees are constructed for the system level performance, and they are mapped into a Bayesian network that allows propagation of fragility information from component level to system level. In this study, the system level validation and the identification of critical events are evaluated based on fragility estimates. To improve the overall validation, we either enhance the simulation models of events along the critical path or collect additional field data until the adequacy of the system level validation is satisfied. This process helps in allocating the resources efficiently thereby reducing the effort to conduct high fidelity simulations and large-scale experiments. The robustness of the proposed framework is illustrated by enabling clarity, consistency, and completeness for a synthetic example of a simplistic flooding scenario.

ACKNOWLEDGMENTS

This research was partially supported by US Department of Energy under the grant DE-NE0008530. In addition, this research was partially supported by Center for Nuclear Energy Facilities and Structures at North Carolina State University. Resources for the Center come from the dues paid by member organizations and from the CCEE Department and College of Engineering in the University.

REFERENCES

[1] B. R. Ellingwood, \Acceptable risk bases for design of structures," Progress in Structural Engineering and Materials, vol. 3, no. 2, pp. 170{179, 2001.

[2] B. M. Ayyub, W. L. McGill, and M. Kaminskiy, \Critical asset and portfolio risk analysis: An all-hazards framework," Risk Analysis, vol. 27, no. 4, pp. 789{801, 2007.

[3] Y. Li and B. R. Ellingwood, \Framework for multihazard risk assessment and mitigation for wood-frame residential construction," Journal of Structural Engineering, vol. 135, no. 2, pp.159{168, 2009.

[4] J. E. Beavers, Multihazard Issues in the Central United States. American Society of Civil Engineers, 2009.

[5] S. Kameshwar and J. E. Padgett, \Multi-hazard risk assessment of highway bridges subjected to earthquake and hurricane hazards," Engineering Structures, vol. 78, pp. 154 { 166, 2014.

[6] Performance Based Engineering: Current Advances and Applications.

[7] H. K. Sandhu, P. Patel, A. Gupta, and Y. Mihara, \External multi-hazard probabilistic risk assessment methodology and applications: A review of the state-of-the-art," in Transactions of the 25th International Conference on Structural Mechanics in Reactor Technology, 2019.

[8] J. Wang, X. Gu, and T. Huang, \Using bayesian networks in analyzing powerful earthquake disaster chains," Natural Hazards, vol. 68, pp. 509{527, Sep 2013.

[9] S. Kwag and A. Gupta, \Probabilistic risk assessment framework for structural systems under multiple hazards using Bayesian statistics," Nuclear Engineering and Design, vol. 315, pp. 20{34, 2017.

[10] S. Jang and A. Yamaguchi, \Dynamic Probabilistic Risk Assessment of Combined Event of Earthquake and Internal Flooding Using Continuous Markov Model and Monte Carlo Method," Asian Symposium on Risk Assessment and Management, 2018.

[11] H. Muta, Y. Ohtori, and H. Yamakawa, \Development of Seismic-Tsunami Accident Sequence Analysis Methodology," Asian Symposium on Risk Assessment and Management, 2018.

[12] L. Lin, Development and Assessment of Smoothed Particle Hydrodynamics Method for Analysis of External Hazards. PhD thesis, North Carolina State University, 2019.

[13] S. Bodda, \Multi-Hazard Risk Assessment of a Flood Defense Structure," Master's thesis, North Carolina State University, 2018.

[14] N. Dinh, H. Abdel-Khalik, A. Gupta, X. Sun, I. Bolotnov, J. Baugh, M. Avramova, P. Bardet, R. Youngblood, C. Rabiti, S. Prescott, and W. Ren, \Development and Application of a Data-

[15] Driven Methodology for Validation of Risk-Informed Safety Margin Characterization Models," North Carolina State University, 2015.

[16] S. Prescott, D. Mandelli, R. Sampath, C. Smith, and L. Lin, \INL/EXT-15-36773 - Light Water Reactor Sustainability Program - 3D Simulation of External Flooding Events for the RISMC Pathway," 2015.

[17] C. Smith, D. Mandelli, S. Prescott, A. Alfonsi, C. Rabiti, J. Cogliati, and R. Kinoshita, \Analysis of pressurized water reactor station blackout caused by external ooding using the RISMC toolkit," Idaho National Laboratory INL/EXT-14-32906, 2014.

[18] NIMBLE Development Team, \Nimble: Mcmc, particle _ltering, and programmable hierarchical modeling," 2019.

VIII Metamodels for Reducing Computational Costs in Probabilistic Safety Analyses

Jeremy Rohmer
BRGM
3, av. Claude Guillemin, 45060, Orleans, Cedex 2, France
j.rohmer@brgm.fr

ABSTRACT

Probabilistic safety analyses for nuclear power plant require running a large number of times the numerical simulator (typically thousands of times). This may be incompatible with the computation time cost of a single simulation run, which can typically reach several hours. A first solution can rely on large computing clusters. Yet, this is not achievable by all companies / research institutes and in the present communication, we explore an alternative solution of statistical nature, namely meta-modelling. This corresponds to a function constructed using a few computer experiments (i.e. a limited number of time consuming numerical simulations). It aims at reproducing the behaviour of the "true" numerical model in the domain of model input parameters and at predicting the model responses with a negligible computation time. We describe the key elements for implementing such a technique and provide an application where the objective is to identify all uncertain parameters that lead to the failure of considered system.

VIII.1 INTRODUCTION

Probabilistic safety assessments (PSA) has become a key procedure to identify and understand key nuclear power plant (NPP) vulnerabilities. Over the last years, the recent advances in numerical modelling has enabled to provide high resolution, highly accurate prediction of the physical processes. Yet, despite the increasing computer power, conducting thousands of different simulation runs, as required by PSA, is hampered by the very high computation time cost of such numerical simulations. In this communication, we present a technique, of statistical nature, to overcome this computational burden, namely meta-modelling. The procedure is first described in Sect. VI.2and applied on a synthetic test case in Sect. VIII.3.

VIII.2 PROCEDURE

VIII.2.1 Principles

Let us consider *f* the complex large-scale computationally intensive numerical model. The meta-modelling technique consists in replacing *f* by a mathematical approximation referred to as "meta-model" (also named "response surface", or "surrogate model"). This corresponds to a function constructed using a few computer experiments (i.e. a limited number of time consuming simulations, see Figure VIII-1). It aims at reproducing the behaviour of the "true" model in the domain of model input parameters and at predicting the model responses with a negligible computation time. In this manner, any approach relying on intensive multiple

simulations like probabilistic analysis, are made achievable at a "reasonable" computation time cost. The main steps of the methodology are summarized in Table VIII-1.

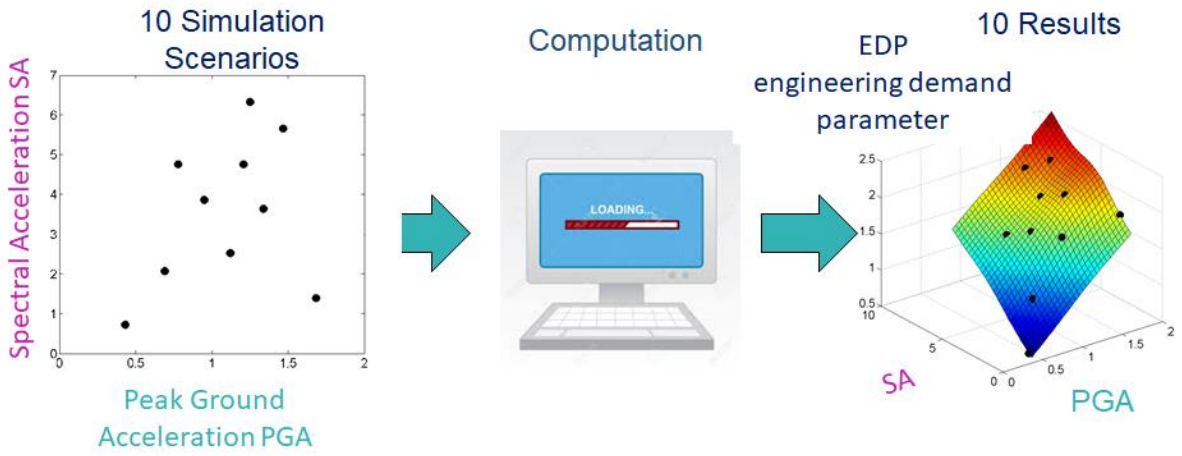


Figure VIII-1: Schematic overview of the principles of metamodeling using a synthetic example in the domain of earthquake engineering with two inputs (PGA and SA) and one variable of interest, namely EDP. The coloured surface on the right corresponds to the predictions of a polynomial metamodel fitted using ten simulation results (black dots).

Table VIII-1: Main steps of meta-modelling strategy using computationally intensive numerical models

Step	Description
1	Generate n_0 different values for the input parameters $\boldsymbol{x}$ of the model (for instance using a LHS technique);
2	Evaluate the corresponding model outputs y by running the computationally intensive model. The pairs $(\boldsymbol{x}_i ; y_i)$ with i=1,…,n_0 constitute the training data, based on which the meta-model can be constructed;
3	Assess the approximation and the predictive quality using cross-validation procedure;
4	Using the validated "costless-to-evaluate" meta-models, the computationally intensive procedure of interest can be conducted. Depending on the type of application, additional simulation scenarios can be selected using the meta-model to add iteratively new the training data to increase the accuracy of the prediction.

VIII.2.2 Step 1: setting the training data

The approximation is constructed by running f given a limited number n_0 of different model input parameters x, named training samples. Hence, the objective is to create a mapping (named training data) between x and the quantity of interest, for instance the maximum displacement at a given location of the considered system under seismic shaking. A trade-off should be found between maximizing the exploration of the offshore conditions domain and minimizing the number of simulations, i.e. a trade-off between the accuracy of the

approximation and the compu-tation time cost. To fulfil such requirements, I propose to randomly select the training samples by means of the Latin Hypercube Sampling (LHS) method [1]. LHS is a stratified random sampling method (also named quasi-random), which can lead to convergence with smaller sample size than simple random samples.

VIII.2.3 Step 2: construction of the meta-model

Using the training data, the approximation can be carried out relying on several types of meta-models, either using simple polynomial regression techniques, non-parametric regression techniques [2], kriging modelling [3], polynomial chaos expansions [4], etc. The choice of the meta-model type is guided by the a priori non-linear functional form of the simulator, as well as the number of input parameters.

VIII.2.4 Step 3: validation of the meta-model

The third step aims at validating the meta-model quality. Two issues should be addressed: 1) the approximation quality, i.e., to what extent the meta-model manages to reproduce the simulated model outputs, and 2) the predictive quality, i.e., to what extent the meta-model manages to predict the model outputs for "yet-unseen" input parameter configurations. The approximation quality can be assessed using the differences between approximated and "true" model outputs (i.e., the residuals) and by computing the coefficient of determination, R^2. The latter can be done as follows:

$$R^2 = 1 - \frac{\sum_{i=1}^{n} (\tilde{y}_i - y_i)^2}{\sum_{i=1}^{n} (y_i - y_m)^2} \quad (1)$$

where the yi correspond to the "observed" model outputs (i.e., to the model outputs which were simulated using the long-running flow simulator), ym corresponds to the mean of the "observed" model outputs, and the $\tilde{y}_i$ correspond to the approximated model outputs (i.e., the outputs which were estimated using the meta-model). A coefficient R^2 close to one indicates that the meta-model has been successful in matching the observations.

Regarding the second quality issue, a first approach would consist of using a test sample of new data. Although the most efficient, this approach might often be impractical because additional numerical simulations are costly to perform. A possible option to overcome such a situation relies on q-fold cross-validation procedures (see, e.g., [6]). This technique involves: 1) randomly splitting the initial training data into q equal subsets (q is typically between 5 and 10); 2) removing each of these subsets in turn from the initial set and fitting a new meta-model using the remaining q-1 sub-sets; 3) using the subset removed from the initial set as a validation set and estimating it using the new meta-model. Using the residuals computed at each iteration of this procedure, a coefficient of determination R^2 can be computed using a formula similar to Eq. (1). For small training sets, the cross validation procedure with q=1 is usually used corresponding to the so-called "leave-one-out" cross validation procedure. A typical threshold above 80% is commonly used to qualify the predictive quality as "satisfactory" (e.g. [6]). Once validated, the meta-model can replace the long-running flow simulation to conduct probabilistic analysis.

VIII.2.5 Step 4: use of the meta-model

Since the meta-model is costless-to-evaluate, it can easily be used in place of the long running numerical simulator to perform the probabilistic analysis. Depending on the purpose of the analysis, additional simulation results may be required to increase the accuracy of the meta-model-based prediction. A particular situation is when the goal is to estimate low probability of failure. In this case, the meta-model can be used to select additional simulation scenarios to enrich the training dataset in the domain of interest, i.e. close to the frontier separating the inputs leading to failure to the ones avoiding it. This is the purpose of active learning as described for instance by [7] using kriging meta-models.

VIII.3 CASE STUDY

In this section, we illustrate the different steps of the metamodeling procedure using the example of a beam in elastic deflection. The deflection δ is given by the following equation:

$$\delta = \frac{PL^3}{3ES^2I} \quad (2)$$

where I is the normalized moment of inertia (assumed to be constant at 0.08333), E is the Young Modulus (assumed ot be constant at 600 GPa), P is the vertical loading (assumed to be constant at 600N. The uncertain parameters are described in Table VIII-2. The objective is to identify all pairs of $\boldsymbol{x}=(L;S)$ leading to the failure of system, i.e. the critical set $\Gamma=\{\boldsymbol{x} : \delta(\boldsymbol{x})>1\}$

Table VIII-2: Uncertainty range of the uncertain parameter

Parameter	Lower bound	Upper bound	Unit	Symbol
Beam length	10	20	m	L
Beam section surface	1	2	m²	S

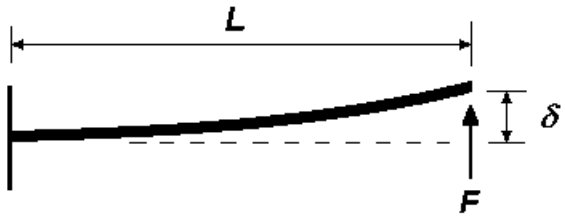


Figure VIII-2: Schematic overview of the beam deflection3.

Given the domain of variation of the different source model parameters (Table VIII-2), 10 simulation scenarios were generated (each being associated to a different setting of source parameters' values) using the LHS method. A kriging meta-model is constructed and validated using a leave-one-out cross-validation procedure. This confirms the predictability of the different meta-models: this showed $R^2 > 90\%$ hence confirming the validity of replacing the long running simulator by the meta-model (Figure VIII-3).

[3] Adapted from http://www.clag.org.uk/beam.html

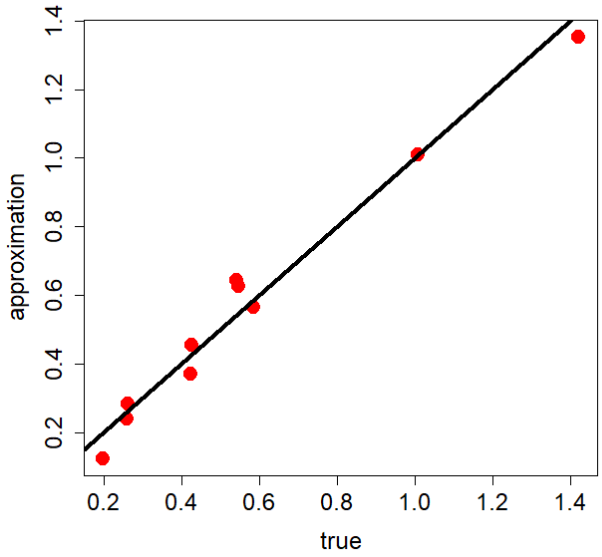


Figure VIII-3: Comparison between observations (i.e. the results derived from the long running simulations) and the kriging-based predictions.

On this basis, the critical set Γ is calculated (see dark and light grey coloured zone in Figure VIII-4(a)) using the validated meta-model. The comparison with the true frontier (in red in Figure VIII-4(a)) reveals that the level of accuracy of the meta-model is here not sufficient to fulfil the Γ estimates. We complement the analysis with an active learning using the following error criterion for selecting additional simulation scenarios $\boldsymbol{x}$:

$$\mathrm{Error}(\boldsymbol{x}) = s^2(\boldsymbol{x})\mathrm{I}_{[T-\epsilon;T+\epsilon]}(\boldsymbol{x}) \quad (3)$$

where $s^2(.)$ the kriging variance, T is the deflection threshold (here 1), ϵ is a small tolerance value around T, and $\mathrm{I}_{[T-\epsilon;T+\epsilon]}$ is the indicator function which reaches 1 when $\boldsymbol{x}$ belongs to $[T-\epsilon; T+\epsilon]$ and 0 otherwise.

The estimations of the error criterion is provided in Figure VIII-4(b) using the meta-model constructed with the initial set of simulation results. By maximizing this criterion, we identify that a good candidate to be used as input of a new numerical simulation is located in the top right hand corner. Figure VIII-4(c,d) shows the results of the active learning procedure at the third iteration. Figure VIII-4(e) gives the final results after 15 iterations. Figure VIII-4(f) confirms that for this number of iterations, the error criterion can be considered as stable.

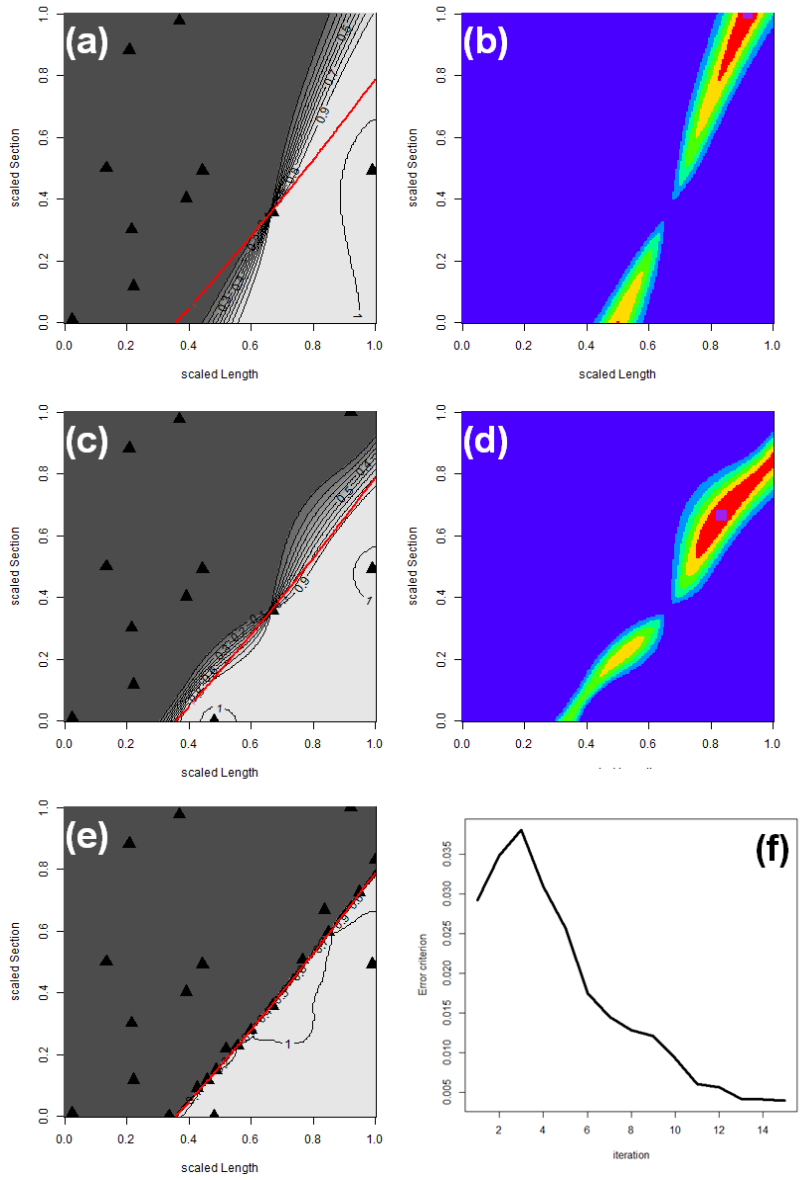


Figure VIII-4: illustration of the active learning procedure to estimate the critical set using the metamodel at (a) iteration 0 (using 10 training data), (c) iteration 3, and (e) iteration 15. The dark and light grey-coloured zone respectively corresponds to the low and high probability of belonging to the critical set. The true frontier is outlined in red. Left figures (b,d) provides the map of the error criterion used to improve the meta-model prediction accuracy. Figure (f) gives the evolution of the error criterion as a function of the number of iterations.

VIII.4 CONCLUDING REMARKS

In the communication, we have shown how meta-models can be useful to reduce computational costs in PSA. The key ingredients are: (1) a careful validation of the predictive capability of the meta-model; (2) a combination with active learning technique to increase the prediction accuracy depending on the purpose of the considered analysis. An example of real life application in the domain of NPP is provided by [8].

REFERENCES

[1] M. D. McKay, R. J. Beckman, W. J. Conover, Comparison of three methods for selecting values of input variables in the analysis of output from a computer code. Technometrics, 21(2), 1979, pp. 239–245.

[2] C. B. Storlie, L. P. Swiler, J. C. Helton, C. J. Sallaberry. Implementation and evaluation of nonparametric regression procedures for sensitivity analysis of computationally demanding models. Reliability Engineering & System Safety, 94(11), 2009, pp. 1735–1763.

[3] A. Forrester, A. Sobester, A. Keane, Engineering design via surrogate modelling: a practical guide. JohnWiley & Sons, 2008.

[4] R. G. Ghanem, P. D. Spanos, Stochastic finite elements: a spectral approach, 387974563. Springer, 1991.

[5] T., Hastie, R. Tibshirani, J. Friedman, T. Hastie, J. Friedman, R. Tibshirani, The elements of statistical learning, volume 2. Springer, 2009.

[6] A. Marrel, B. Iooss, F. Van Dorpe, E. Volkova, An efficient methodology for modeling complex computer codes with gaussian processes. Computational Statistics & Data Analysis, 52(10), 2008, pp. 4731–4744.

[7] J. Bect, D. Ginsbourger, L. Li, V. Picheny, E. Vazquez, Sequential design of computer experiments for the estimation of a probability of failure. Statistics and Computing, 22(3), 2012, pp. 773-793.

[8] C. Chevalier, J. Bect, D. Ginsbourger, E. Vazquez, V. Picheny, Y. Richet, Fast parallel kriging-based stepwise uncertainty reduction with application to the identification of an excursion set. Technometrics, 56(4), 2014, pp. 455-465.

IX Severe Accident Assessment with Uncertainty and Sensitivity Analysis

Piotr Darnowski and Piotr Mazgaj
Institute of Heat Engineering, Warsaw University of Technology
Nowowiejska 21/25
00-665, Warsaw, Poland
piotr.darnowski@pw.edu.pl and piotr.mazgaj@pw.edu.pl

ABSTRACT

The paper introduces the concept of sensitivity and uncertainty analysis (S&UA) for severe accidents. Studies of an accident progression with the assessment of uncertainties is a standard approach in Deterministic Safety Analysis and especially for modern design basis studies. Uncertainty analyses are also common in the case of severe accident investigations. Plant scale severe accident simulations are performed in the framework of the Probabilistic Safety Analysis (Level 2) but also as a part of other safety-related studies. Proper knowledge about the uncertainty of results is an important issue due to complex phenomenology and simulation models. The sensitivity analysis allows getting a broader understanding of the studied accident and gaining knowledge which and how different phenomena or circumstances impact the results. In this paper, the methodology is demonstrated with a simple example of hydrogen production in the Phébus FPT-1 integral experiment. The popular Wilks' based non-parametric approach is described. This methodology is applied in the NARSIS project WP4.

IX.1 INTRODUCTION

In the past, the usual approach in deterministic studies of Nuclear Power Plants (NPPs) was to use conservative methods with conservative computer codes, boundary conditions and initial conditions [1,2]. With the development of knowledge, understanding of the physical phenomena, growing experimental databases and computational capabilities, new approaches were introduced. Conservative codes were exchanged with best-estimate (BE) codes, and in the next step, the conservatism in boundary conditions (BC), initial conditions (IC) and systems availability were reduced . The trend was to decrease conservatism with the application of more sophisticated computational and statistical methods, including the assessment of uncertainties. The reduction of conservatism has a price, which is the increase in the complexity of methodology and necessary computational effort [1,2]. This problem is especially crucial for design basis type studies of NPP, but it also present in severe accident studies. Nowadays, in severe accident analysis, we attempt to use best-estimate methods and codes as far as possible. Nevertheless, uncertainties are unavoidable, and their quantification is useful.

Basically, BE computational tools were developed in parallel with statistical methods to assess uncertainty. For more than thirty years a large number of best-estimate computer codes were developed, like thermal-hydraulics codes RELAP5, CATHARE, TRACE and severe accident integral codes like MAAP, MELCOR or ASTEC but also other tools for different purposes. Computer codes were extensively verified and validated with different separate effect tests, integral experiments and real accidents like TMI-2, Chernobyl or Fukushima Daiichi. All

that effort was made in order to ensure that we are able to realistically predict what will happen during the accident and reduce the uncertainty of engineering estimations [3,4]. Nowadays, uncertainty analysis is a standard approach also in severe accident analyses, and the aim of this paper is to introduce the idea to the reader.

IX.2 SEVERE ACCIDENT SIMULATIONS

Accident simulations using best-estimate computer codes in a purely deterministic manner do not provide the guarantee that the physical situation can be adequately simulated. Usually, we cannot merely make a statement that the obtained results (the answer) are certain with high precision. It is especially the case for such a complex object as NPP and circumstances as a core meltdown. The phenomenology of a severe accident is still a very active field of research, and our lack of understanding of many phenomena is substantial. Recommended publications for non-experienced readers are two monographs about severe accidents [3,4].

The simple, intuitive argument can be presented in the form of Figure XI-1, which shows (Left) typical core state predicted with best-estimate severe-accident tool MELCOR and a real (Right) state of the core during the accident. The reader can imagine the occurrence of uncertainties is inevitable. Those uncertainties are introduced by both the lack of knowledge or data (epistemic uncertainty) but also due to the random nature of processes (aleatory uncertainty) [5].

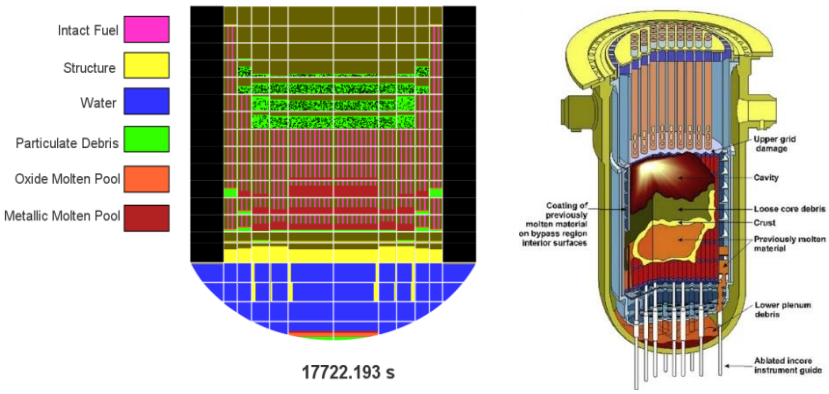


Figure IX-1: Left - An example of a core state during a severe accident predicted with MELCOR computer code. Based on [6]. Right – State of the core in TMI-2 accident. Taken from [3].

Moreover, we introduce uncertainties by application of analytical tools with limited capabilities (see Figure IX-1) with non-negligible user effects and due to the modelling practices. The severe accidents are full of complex multi-physical problems with time-scales different by orders of magnitude. Uncertainties inevitably propagate with time and with time, new aspects may gain importance. In consequence, even using best-estimate computer code with best possible assumptions, the obtained result has limited value for an analyst. Uncertainties exist, which is also part of physical reality. What is important is the awareness of that fact and the main problem is how to properly express them in quantitative and qualitative terms.

The popular State-of-the-Art approach to Deterministic Safety Analysis (DSA) with uncertainty assessment is the Best Estimate Plus Uncertainty (BEPU) [7–10]. Usually, the BEPU approach is applied for Design Basis (DB) type studies, especially, for Loss of Coolant Accidents (LOCAs) but also other transients. It can also be used in severe accident studies, and example of its application is presented in the papers [11–14] and in Chapter 3.

IX.3 UNCERTAINTY ANALYSIS

Uncertainty analysis provides the knowledge of how precise are the results, based on the knowledge about phenomenology, analytical and numerical methods, and using proper statistical tools. The most popular approaches allow obtaining proper statistical tolerance limits for the requested probability with requested confidence levels [15]. We can also study additional measures like percentiles, mode, median and mean values which allow results and uncertainty qualification and quantification (see [12]).

The obstacle in uncertainty study is that the accident analysis demands massive computational resources and computations of many cases. A modern approach which was applied in NARSIS project and which is popular in the World is the so-called Wilks' method [16]. This non-parametric approach allows removing the connection between the number of calculated cases and a number of uncertain parameters [11]. It opens the possibility to reduce the necessary computational effort and allows to obtain a statistically satisfying answer. Table IX-1 presents the number of necessary calculations to obtain the proper confidence level with proper probability for two-side and one-sided problems. The typical approach is to obtain 95%/95%, which is called Standard Tolerance Level (STL). For example, in typical BEPU LOCA calculations where figure-of-merit (FOM) can be the maximum cladding temperature, the one-sided problem is studied with STL, and it demands 59 cases.

Table IX-1: Statistical tolerance limits and a minimum number of necessary computations. Based on [15].

Confidence Level	Sample size to span p					
	One-sided tolerance			Two-sided tolerance		
%	0.9	0.95	0.99	0.9	0.95	0.99
90	22	45	230	38	77	388
95	29	**59**	299	46	**93**	473
99	44	90	459	64	130	662

One of the most popular realizations of the BEPU is the GRS methodology [15]. The idea is depicted in Figure IX-2. It applies the probabilistic approach for uncertainty propagation based on Wilks method, which can be classified as black-box from the point of view of modelling, and it has input-driven uncertainty propagation [15]. The basic idea is to select proper input parameters with probability distributions (see example in Table IX-2), sample them for all selected parameters and for all studied computational cases. The simulation model can be treated as black-box, which transforms sampled input variables into output, and it is also responsible for the uncertainty propagation present in the output sample.

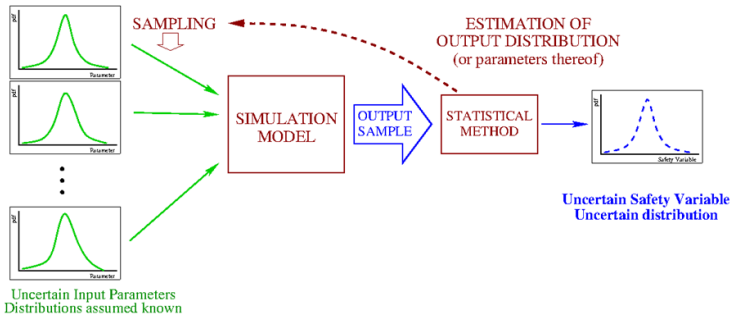


Figure IX-2: BEPU approach proposed by GRS. Taken from [15].

The procedure applicable for severe accident analysis with uncertainty (and sensitivity) and the step-by-step procedure is described below (see [14]):

1) Identification of uncertain input variables and models (see Table IX-2).
2) Assignment of uncertainty information (probability distributions) to proper variables and models (see Table IX-2).
3) Determination of the sample size for the statistical significance of the uncertainty measures for the output variables. Based on the Wilks' formulas. For example, to obtain 95% /95% two-sided STL, we apply 93 input decks (see Table IX-1).
4) Sampling procedure – typically Simple Random Sampling (SRS).
5) Computer code execution for all cases (in the example it is MELCOR code).
6) Post-processing of results.
7) Statistical analysis. Uncertainty and Sensitivity quantification (see Figure IX-3 and Chapter 4).
8) Study of individual cases/outliers.

Table IX-2: Example - list of uncertainty parameters.

No	Parameter	Probability Distribution
1	Zr Melt Breakout Temperature	Normal
2	Fuel Rod Failure Temperature	Normal
3	Candling Heat Transfer Coefficient - Zr Freezing	Log-Normal
4	Core-Region Particulate Debris Diameter	Log-Normal
5	Debris porosity	Triangular
6	Radiation Exchange Factor Radial	Normal
7	Radiation Exchange Factor Axial	Normal
8	Molten clad drainage rate	Log-Normal
9	Secondary UO2 Content	Normal

The example results for hydrogen production uncertainty in the FPT-1 experiment is presented in Figure IX-3. The Simple Random Samples (SRS) for uncertain parameters (Table IX-2) was used with Wilks for 95%/95% two-sided STL limit to obtain upper and lower limits. Limiting results from the sample represent the 95% confidence interval within which 95% of all the possible values lie.

Studying Figure IX-3, we can observe that the experimental data is within the uncertainty limits, and it can be considered a satisfactory outcome. Otherwise, it is worth to mention that there are situations where we can calculate the problem with satisfying tolerance limits, but we can obtain results which do not reproduce the Physics. It is one of the fundamental problems in accident studies that the results can be precise with low uncertainty, but accuracy can be low due to results being far from experiment and physical reality.

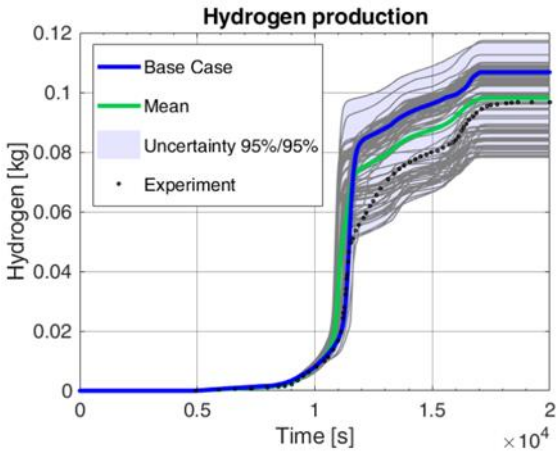


Figure IX-3: Example - hydrogen production during bundle phase of the Phébus experiment FPT-1 with uncertainty bands, compared with best-estimate calculation (Base case) and experimental data. Based on [17].

IX.4 SENSITIVITY ANALYSIS

Sensitivity analysis is naturally coupled with uncertainty analysis. Computations of many cases allow an analyst to perform sensitivity study. It usually covers the application of statistical methods to describe the impact of the investigated parameter on a figure-of-merit.

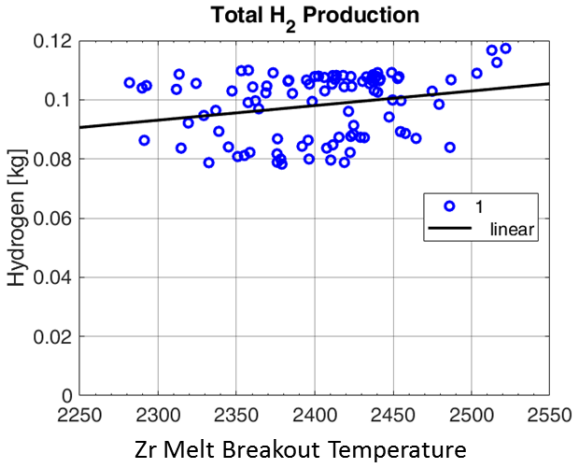


Figure IX-4: Example - total hydrogen production vs zirconium melt breakout temperature for Phébus test. Based on [17].

One of the simplest methods is linear regression, which is popular in the literature. We can simply plot the studied parameter versus FOM. The example is presented in Figure IX-4, where we can observe the dependence of the hydrogen production on parameter Zirconium breakout temperature (see Table IX-2). Linear regression allows the analyst to rapidly assess quantitatively and qualitatively possible correlations.

The more sophisticated, popular, but still not very difficult approach is to study the Pearson linear and Spearman non-linear coefficients. Example results are presented in

Figure IX-5, which shows the Pearson and Spearman coefficients for hydrogen production in FPT-1 experiment. Typically, the contributions with ρ-value less than 0.2 are considered to be poorly correlated [18]. On the contrary, the low p-value indicates a correlation.

In the studied example, the most significant ρ-values are slightly larger than 0.2 for both coefficients, and in consequence, correlations are poor. What is interesting, a weak correlation for #1 is also possible to observe in Figure IX-4, in spite of being relatively most correlated parameter among all studied. We can observe that parameters #1 and #7 are characterized by the strongest correlation. On the contrary parameters: #4, #5, #8 and #9 are weakly or not correlated.

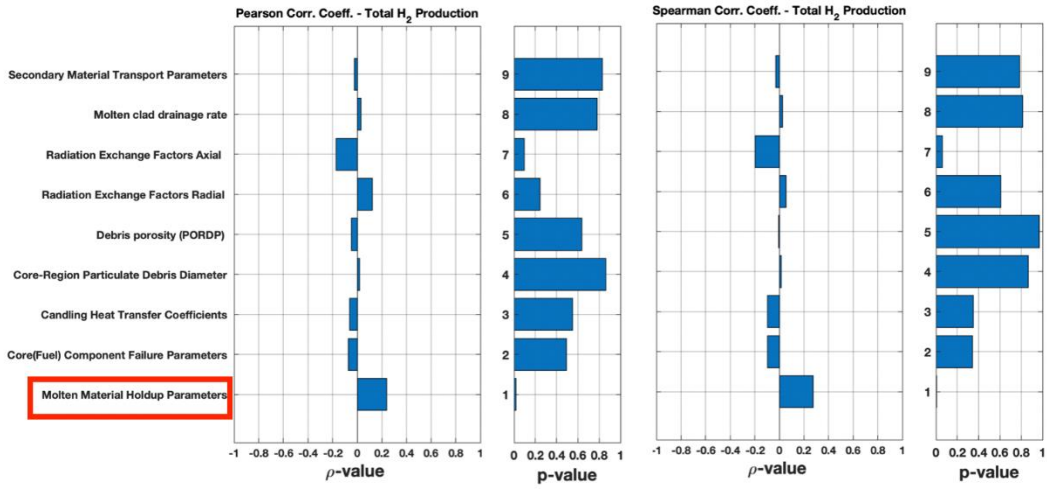


Figure IX-5: Example - Pearson (linear) and Spearman (non-linear) correlations coefficient for Total hydrogen production during the Phébus experiment. Based on [17].
In the presented example, only simple first-order methods were studied. There are several other more sophisticated statistical methods (i.e. Sobol indices) which allow studying higher-order dependences [19]. It is the current and important research topic.

IX.5 SUMMARY AND CONCLUSIONS

In this paper, the reader was introduced to the application of the S&UA in accident analysis with a focus on severe accidents. In the NARSIS Horizon 2020 Project WP4.3 "Safety Analysis of NPP" different S&UA methodologies are applied for both severe accident and design basis type analysis. The novel approach to study transients the so-called Extended Best Estimate and Uncertainty (E-BEPU) is being developed in Work Package 3 and Work Package 4 of the NARSIS Project. It will be applicable to both non-DB transients, DB accident but also it will allow studying Design Extension Conditions. The critical part of the E-BEPU methodology is uncertainty analysis with Wilks' based BEPU methodology, which was presented in this paper.

REFERENCES

[1] IAEA, Deterministic Safety Analysis for Nuclear Power Plants - IAEA SSG-2 Revision 0, 2009.

[2] IAEA, Deterministic Safety Analysis for Nuclear Power Plants - IAEA SSG-2 Revision 1, 2019.

[3] B.R. Sehgal, Nuclear Safety in Light Water Reactors Severe Accident Phenomeneology,

Academic Press Elsevier, 2012.

[4] A. Bentaïb, H. Bonneville, G. Cénérino, D. Jacquemain, A. Bentaïb, H. Bonneville, G. Cénérino, Nuclear Power Reactor Core Melt Accidents, Current State of Knowledge, EDP Sciences, 2015.

[5] B. Galyean, J. Rempe, Accident Progression Analysis (P-300), (2005). https://www.nrc.gov/docs/ML1204/ML12044A213.pdf.

[6] P. Darnowski, P. Mazgaj, E. Skrzypek, MELCOR Simulations of the SBO in Gen III PWR with EVMR, in: NENE-2019, 28th Int. Conf. Nucl. Energy New Eur., 2019: pp. 1–8.

[7] F. D'Auria, C. Camargo, O. Mazzantini, The Best Estimate Plus Uncertainty (BEPU) approach in licensing of current nuclear reactors, Nucl. Eng. Des. 248 (2012) 317–328. doi:10.1016/j.nucengdes.2012.04.002.

[8] G.E. Wilson, Historical insights in the development of best estimate plus uncertainty safety analysis, Ann. Nucl. Energy. 52 (2013) 2–9. doi:10.1016/j.anucene.2012.03.002.

[9] M. Perez, F. Reventos, L. Batet, A. Guba, I. Tóth, T. Mieusset, P. Bazin, A. De Crécy, S. Borisov, T. Skorek, H. Glaeser, J. Joucla, P. Probst, A. Ui, B.D. Chung, D.Y. Oh, R. Pernica, M. Kyncl, J. MacEk, A. Manera, J. Freixa, A. Petruzzi, F. D'Auria, A. Del Nevo, Uncertainty and sensitivity analysis of a LBLOCA in a PWR Nuclear Power Plant: Results of the Phase v of the BEMUSE programme, Nucl. Eng. Des. 241 (2011) 4206–4222. doi:10.1016/j.nucengdes.2011.08.019.

[10] A. Prošek, B. Mavko, Review of Best Estimate Plus Uncertainty Methods of Thermal-Hydraulic Safety Analysis, Int. Conf. - Nucl. Energy New Eur. Proc. (2003) 217–224.

[11] R.P. Martin, M.W. Bingham, E. Williams, A. Caillaux, Relevant scenarios and uncertainty analysis of severe accidents in the U.S. EPR, Int. Conf. Adv. Nucl. Power Plants, ICAPP 2008. 2 (2008) 1102–1109.

[12] U.S. Nuclear Regulatory Comission, State-of-the-Art Reactor Consequence Analysis (Soarca) Project: Sequoyah Integrated Deterministic and Uncertainty Analyses, 2018.

[13] S. Tina Ghosh, P.D. Mattie, C.J. Sallaberry, Uncertainty analysis for the U.S. NRC state-of-the-art consequence analyses, 11th Int. Probabilistic Saf. Assess. Manag. Conf. Annu. Eur. Saf. Reliab. Conf. 2012, PSAM11 ESREL 2012. 2 (2012) 1203–1212.

[14] R.O. Gauntt, N. Bixler, K.C. Wagner, An Uncertainty Analysis of the Hydrogen Source Term for a Station Blackout Accident in Sequoyah Using MELCOR 1.8.5, 2001.

[15] H. Glaeser, GRS Method for Uncertainty and Sensitivity Evaluation of Code Results and Applications, Sci. Technol. Nucl. Install. Vol. 2008, Artic. ID 798901,7pages Doi10.1155/2008/798901. (2008).

[16] S.S. Wilks, Determination of Sample Sizes for Setting Tolerance Limits, Ann. Math. Stat. 12 (1941) 91–96. doi:10.1214/aoms/1177731788.

[17] P. Mazgaj, P. Darnowski, G. Niewinski, Uncertainty Analysis of the Hydrogen Production in the PHEBUS FPT-1 Uncertainty Analysis of the Hydrogen Production in the PHEBUS FPT-1 Experiment, (2019) 1–8.

[18] J. Freixa, T.W. Kim, A. Manera, Post-test thermal-hydraulic analysis of two intermediate LOCA tests at the ROSA facility including uncertainty evaluation, Nucl. Eng. Des. 264 (2013) 153–160.

[19] P.M. Stano, M. Spirzewski, Bayesian Integrated Global Uncertainty & Sensitivity Analysis of System's Availability, Proc. 65th RAMS. (2019).

X Severe Accident Phenomenology and Management

Luka Štrubelj
GEN energija, d.o.o.
Vrbina 17
8270, Krško, Slovenia
luka.strubelj@gen-energija.si

ABSTRACT

During severe accident in nuclear power plants (NPPs), the priority of personnel is to assure fundamental safety functions: control of reactivity, removal of heat from fuel and confinement of radioactive material. In particular, the previous last two functions can be specially challenging. At the beginning of a severe accident, the NPP operators are responsible for actions; later on, the technical support center takes over the responsibility. The severe accident management starts when the core exit thermos-couples are greater than 650 ºC. The decisions of technical support center are made based on timely and accurate information. The effectiveness of strategy is monitored, and the plant status is checked. During the severe accident, the mitigation of the challenges is constantly monitored. Main strategies during the severe accident are:

- injection of water into the steam generator in order to remove heat,
- depressurization of reactor coolant system in order to be able to inject water,
- injection of water into reactor coolant system, to flood fuel,
- injection of water into containment,
- reduction of fission product releases,
- control of containment conditions,
- flooding the containment and
- refilling the spent fuel pool.

However, all of these actions have negative impacts, which can be mitigated with appropriate mitigation actions.

X.1 INTRODUCTION TO SEVERE ACCIDENTS

The accidents in nuclear power plants (NPPs) can be grouped to [2]-[3]:

- Anticipated operational occurrences – AOO – (transients)
  - Expected, no fuel damage
- Design basis accidents – DBA
  - Possible, no radiological impact
- Design extension conditions A – DEC A – (Complex sequences)
  - Unlikely, radiological consequences within limits

    - For which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved

- Design extension conditions B – DEC B – (Severe Accidents)
    - Very unlikely, emergency response may be needed
    - With postulated severe fuel damage

To protect environment from radiological releases the defense-in-depth is used. The defense-in-depth methodology uses five protective barriers:

1) Fuel,
2) Fuel Cladding,
3) Primary Circuit Pressure Boundary,
4) Containment, and
5) Emergency Measures

It is assumed that during a severe accident the first two barriers namely fuel and fuel cladding have lost their safety function. Radiological releases prevention during severe accident is thus based on the third and fourth barriers, which are primary circuit pressure boundary and containment. The objective of severe accident management is to defend these two barriers. In the case these two are also lost, the only protection left against radiological releases are emergency measures.

There are multiple definitions of severe accident, hereafter some of them are mentioned. Severe accident is an event which is outside the design basis of the plant, and which leads to damage of the core. It may or may not progress further to core melt, vessel failure, containment failure, and radioactive releases. In the probabilistic safety analyses (PSA), the severe accident starts when the peak clad temperature (PCT) is higher than 1204 °C, calculated using conservative models. When best estimate approach is used, the start of severe accident is when the temperature of the hottest cladding temperature is higher than 650 °C for 30 minutes or 1075 °C instantaneously. The NPP operators, according to their procedures, define onset of severe accident when core exit thermocouples is higher than 650 °C.

X.2 PHENOMENOLOGY OF SEVERE ACCIDENTS

Severe accident progress in three phases. Before the severe accident starts, the initiating event takes place, which causes reactor coolant system (RCS) inventory depletion and core uncover. The Zirconium (Zr) in Ziracloy fuel cladding oxidations starts. The typical duration of this phase is 2 hours. All important phenomena are presented in Figure X-1 and described in more detail in the next subsections.

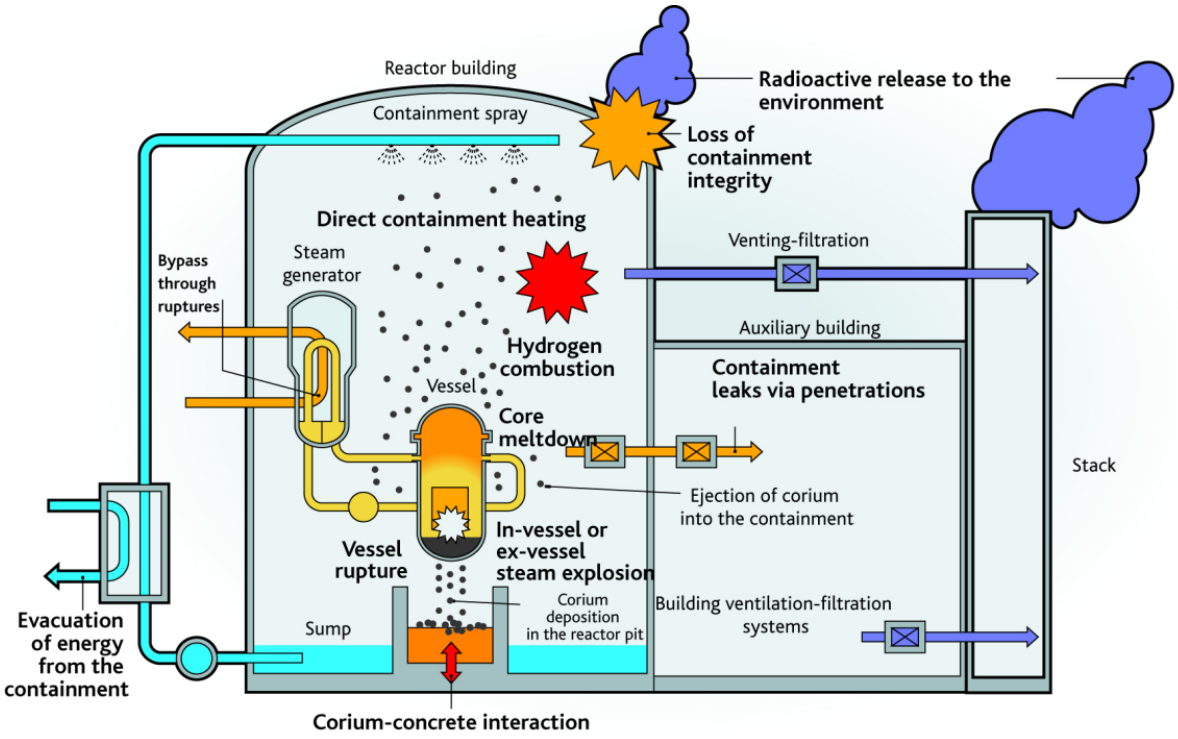


Figure X-1: Severe accident phenomena [4].

X.2.1 In-vessel phase

Second phase is in-vessel phase, where core heats up and melt progress. The fuel cladding fails due to high temperatures and core melt relocates to lower plenum of reactor pressure vessel. The steam explosions can happen. The typical duration of this phase is 4 hours.

Zircaloy – steam reaction is oxidation and is the major source of hydrogen to containment. The chemical equation of exothermal oxidation is:

$$Zr + 2H2O \rightarrow 2H2 + ZrO2 + 6400\ kJ/kg\ Zr \quad (2)$$

Heat of reaction causes significant increase in fuel assembly heat up rate. The potential melting and downward “candling” of molten control rod & clad material can reduce coolant flow area, while refreezing at lower elevation. Zr inventory is about 12 000 kg in 2000 MWt reactor and can theoretically produce 525 kg of H_2. In severe accident analyses it is assumed that only 35%-60% of Zr will oxidase and produce 184-315 kg of H_2.

X.2.1.1 Steam explosions

Steam explosion is a dynamic process that can occur when a large quantity of molten core debris relocates into a pool of water. The process can occur during in-vessel phase, when corium is pour onto reactor pressure vessel overhead, containing water; or during ex-vessel phase, when low-pressure corium is pour into wet reactor cavity. A steam explosion requires four sequential phases of melt-coolant interaction to occur: course mixing of melt and water; collapse of vapour film at heat transfer interface causing an accelerated energy release (“trigger”); propagation of the pressure pulse through the mixture to form a shock wave; outward expansion of the shock wave (damage mechanism).

X.2.1.2 Corium relocation

Corium is a mixture of melted nuclear fuel, fission products, control rods and structural materials. The maximum linear power is approximately at the middle of the core height. Taken into account that water level in reactor pressure vessel that is gradually decreasing, the core degradation starts somewhere on the upper half of the core. After the core is melted, it is relocated to lower plenum.

X.2.2 Ex-vessel phase

Next phase is ex-vessel phase, where reactor vessel fails and the core is relocated from reactor vessel to containment. This can be quite fast if the reactor coolant system is at high pressure. This phenomenon is called high-pressure melted ejection, where debris can be dispersed into containment. The molten corium can interact with concrete. The steam explosions can occur. The debris of core are quenched with water, or they can attack concrete.

X.2.2.1 High pressure melt ejection

The high-pressure melt ejection (HPME) can be the cause of largest pressure increase in a PWR containment. It combines reactor vessel blowdown from high pressure, steam and hydrogen generation from melt-coolant interactions and airborne debris radioactive particles, which directly heat containment atmosphere. Measures are taken to prevent HPME and proceed to low pressure melt release from reactor pressure vessel.

X.2.2.2 Low pressure melt release

The initial event such as loss of coolant accident (LOCA), or depressurization leads to low pressure melt release. Debris is “pour” out of reactor pressure vessel lower head onto cavity that is containment floor. The corium interact with water, if present in reactor cavity and quench. After the corium reaches cavity the core-concrete interaction begins.

X.2.2.3 Molten Core-Concrete Interactions

Molten Core-Concrete Interactions (MCCI) is exothermic chemical reaction between core debris and concrete. Large quantities of gas are generated by concrete decomposition due to following reaction:

$$Zr + 2\ CO2 \rightarrow ZrO2 + 2\ CO \quad (3)$$

Physical and chemical interactions between concrete decomposition gases and core debris release non-volatile fission products. Vertical and horizontal erosion of concrete basement can destroy containment foundation. Due to exothermal reaction, the high local atmosphere temperatures in containment are achieved. There is potential for local heating of containment pressure boundary and failure. The non-condensable gas generated, significant contribute to containment pressure increase and can be the reason for containment structure penetration failure.

X.2.2.4 Creep failure

Hot gases released from top of core during early phases of fuel damage create natural circulation flow patterns. The heat of hot gases is transferred to colder surfaces, including pressure boundary of reactor coolant system (RCS) that may be still at high pressure. This can lead to creep failure. The concerned locations are hot leg nozzles, pressurizer surge line, and

steam generator tubes. Leads to loss of coolant in RCS or steam generator tube rupture (SGTR), where radioactive coolant can bypass the containment.

X.2.3 Containment response

The last phase is containment response. The containment can be pressurized with steam and non-condensable gases, the hydrogen can burn or explode and there is a risk of containment failure. The typical duration of this phase is from 16 to 35 hours.

X.2.3.1 Hydrogen combustion

Hydrogen is released to containment from reactor coolant system through pressurizer power operated valves (PORV) during depressurization, or pipe break in case of LOCA. Hydrogen mixes with containment atmosphere; however, the distribution and local concentrations depend on flow field in containment. This flow is driven by pressure difference, natural convection or ventilation systems. Combustion is possible when local conditions exceed flammability criteria and explosion when local conditions exceed explosion criteria. The criteria depends on temperature, pressure, percentage of air, hydrogen and steam and is aggregated in a Shapiro diagram. The increase in temperature and pressure during combustion presents a challenge on the containment and the containment penetrations. Hydrogen explosion presents even higher challenge in terms of pressure peak.

X.3 BASIC SCENARIOS OF SEVERE ACCIDENTS

There are two basic scenarios during severe accidents. High-pressure scenario and low-pressure scenario. The high-pressure scenario is transferred to low-pressure scenario if there is a successful depressurization of RCS.

X.3.1 High RCS pressure sequence (e.g. SBO)

The High RCS pressure sequence starts with initiating event like station black out (total loss of internal and external electricity power), or loss of ultimate heat sink, where decay heat removal is lost in certain time window and the depressurization of reactor coolant system fails. The core is uncovered, fuel and its cladding temperature start to rise and hydrogen production occurs because of the contact of hot water and cladding. RCS pressure is stacked at pressurizer (PRZ) PORVs or safety valves set point pressure. The core lost coolable geometry and finally starts to melt. RPV can fail due to the different failure mechanisms but without RCS depressurization molten corium can be ejected to the containment at high pressure. High pressure molten ejection (HPME) can introduce direct containment heating (DCH) phenomena when fragmented corium can suddenly dissipate huge energy to containment atmosphere and produce pressure peak above design value. Containment pressure boundary can be jeopardized also by ejected corium fragments to the containment wall. If reasonable amount of corium is collected on RPV cavity floor the molten corium interaction with concrete (MCCI) can start to produce even more hydrogen and carbon monoxide, which either can form explosive mixture or increase containment pressure. After initial dynamic peak pressure at the time of RPV failure, the containment pressure starts to increase. Containment pressure boundary can fail either by initial peak pressure at RPV failure (HPME and DCH), hydrogen burn, long-term pressurization by non-condensable gases (MCCI without containment heat removal) or melt through by not quenched and cooled corium on cavity floor due to MCCI.

X.3.2 Low RCS pressure sequence (e.g. LB LOCA)

The low-pressure sequence starts with initiating event like LOCA where the water in reactor coolant system is loss and there is no available means to remove decay heat. The core is uncovered, fuel and its cladding temperature starts to rise. Hydrogen is produced by cladding oxidation with hot steam until water present in RPV. The core temperature starts to rise. The core starts to melt and RPV fails at the bottom due to corium melt through its vessel. The reactor cavity bellow the reactor pressure vessel can be flooded with water or not. Hot corium in contact with water can initiate steam explosions, which can threaten containment integrity. The corium collected on RPV cavity floor can evaporate existing water (if there is no containment injection) in cavity or immediate starts the molten corium interaction with concrete (MCCI) if cavity is dry and it starts to produce even more hydrogen and carbon monoxide, which either can form explosive mixture or increase containment pressure. Containment pressure boundary can fail either by initial peak pressure at RPV failure (or steam explosion if some water exists in RPV cavity), hydrogen burn, long term pressurization of non-condensable (MCCI without containment heat removal) or melt through by not quenched and cooled corium on cavity floor due to MCCI.

X.4 SEVERE ACCIDENTS MANAGEMENT GUIDELINES (SAMG)

This SAMG is entered when core exit thermo-couples (TC) are greater than 650 °C and emergency operation procedures (EOP) actions from function restoration guidelines to cool the core are not successful. At the beginning, the control room operators are making decisions; later on the technical support center (TSC) is then formed to make the decisions and to manage the severe accident.

X.4.1 Diagnostic Flow Chart (DFC)

The DFC provides a method for the TSC to diagnose the plant conditions during a severe accident and to select the appropriate Severe Accident Guidelines (SAGs) for implementation. Specifically, the information contained in DFC relates to:

- Plant conditions that indicate a controlled stable state has been reached.
- Plant conditions that represent a challenge to a containment fission product boundary.
- Insufficient SFP cooling.
- Instrumentation that can be used to provide an indication of the plant status for the parameters on the DFC.

The main parameters and its purpose are listed here:

- SG Water Level
    - To determine if there is an RCS heat sink available.
    - To determine if creep rupture of the SG tubes is a concern.
    - To mitigate fission product releases from faulty or leaking SG tubes.
- RCS Pressure
    - To determine the ability to inject into the RCS.
    - To determine if HPME is a concern.
    - To determine if there is an uncontrolled opening in the RCS.
    - To determine if creep rupture of the SG tubes is a concern.

- Core Temperature (RCS Temperature)
    - To determine if the core is covered with water.
- Containment Water Level
    - To determine if equipment and instruments are flooded.
    - To determine if ECCS and/or containment spray recirculation is possible.
    - To determine if the core is coolable if RPV failure occurs.
- Site Release
    - To determine if release mitigation is desired.
- Containment Pressure
    - To determine if there is a challenge to the containment due to over pressurization or due to sub atmospheric condition.
    - To determine if the containment atmosphere is steam inert.
- Containment Hydrogen
    - To determine if there is a long-term challenge to the containment due to hydrogen flammability.
- SFP level
    - To determine if the spent fuel pool has sufficient water inventory.
    - To mitigate fission product releases from the fuel handling building.

X.4.2 Severe Challenge Status Tree

The severe challenge status tree is presented on Figure X-2.

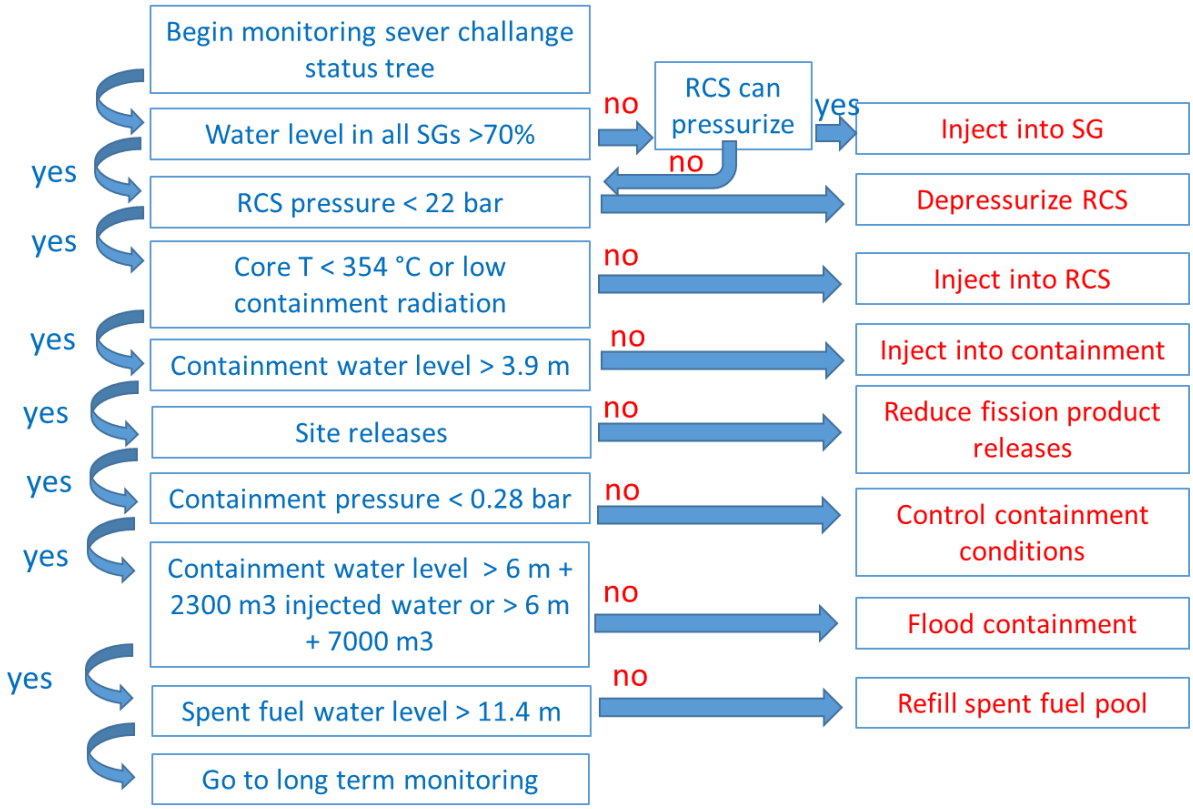


Figure X-2: Severe challenge status tree.

X.4.3 Severe Accident Control Room Guidelines

The severe accident control room guidelines steps are:

1) Check entry conditions
2) Evacuate Containment
3) Restore Containment Integrity
4) Isolate RHR system from RCS
5) Check Containment penetration isolation
6) Depressurize RCS if RHR is NOT isolated from RCS.
7) Check Main if Control Room Charcoal Clean-up System is Actuated
8) Place Control Switches for any of the Non-Operating Equipment in PULL-OUT (e.g.: Charging Pumps, SI Pumps, RH Pumps, Containment Spray Pumps, Containment Fan Coolers, AFW Pumps, SW Pumps…)
9) Turn on Containment Hydrogen Monitors
10) Check Containment Recirculation Sump Level - GREATER THAN 3.9 m
11) Check TSC Status
12) Reset SI
13) Reset Containment Isolation Phase "A" and Phase "B"
14) Establish Instrument Air to Containment
15) Check If Any RCPs Should Be Stopped
16) Check If RCS Should Be Depressurized
17) Verify that associated SW and CC train are in operation
18) Establish RCS Injection Flow
19) Check if Containment Fan Coolers should be stopped
20) Check Containment Recirculation Sump Level - GREATER THAN 3.9 m

21) Determine Containment Spray Requirements (Suction from RWST)
22) Check if Containment Spray should be running in recirculation
23) Initiate actions to isolate idle flow paths that penetrate the containment boundary
24) Check SG levels
25) Initiate actions to isolate idle secondary release flow paths
26) Initiate sampling / monitoring
27) Evaluate plant status:
28) Return to Step 11. OBSERVE NOTE PRIOR TO STEP 11.

X.4.4 Severe Accident TSC Guidelines

The severe accident technical support (TSC) guidelines steps are repeated in loop:

1) Follow TSC directions on starting any non-operating components
2) Check for potential release paths
3) Evaluate instrumentation response
4) Evaluate plant equipment
5) Update TSC on most recent sample results (RCS, Radioactivity, Boron concentration, Containment Sump, Radioactivity, pH…)
6) Inform TSC of any tanks (RWST, CST, Reactor make-up water tank, boric acid storage tank…) that are being depleted of water inventory
7) Implement actions as directed by TSC:
8) Return to Step 1

X.4.4.1 Inject into the Steam Generators

The injection into SG (SAG-1) starts when the water level in all SGs is below 70% of narrow range (NR) and RCS is pressurized (no large opening).

The purposes of injecting into the steam generators are:

- to protect the steam generator tubes form creep rupture,
- to scrub fission products that enter the steam generators via tube leakage,
- to provide a heat sink for the RCS.

The Table X-1 presents negative impacts (what), applicability (when) and mitigation actions of injection into SG.

Table X-1: Negative impacts and mitigation actions of injection into SG

NEGATIVE IMPACT	APPLICABILITY	MITIGATING ACTIONS
Thermal shock of SG	**Feeding a hot, dry SG** If steam generator wide range level is less than 4%	• Limit flow to SG to 22 m/hr to the first 10 minutes of injection • Feed only one dry SG at a time to minimize consequences of SG tube failure until minimum wide range SG level is indicated. • Feed only isolatable SGs to minimize consequences of SG tube failure.

Fission product release from leaking SG tubes	**Feeding a ruptured or leaking SG**	• Feed/steam only intact SGs. • Depressurize the RCS to minimize primary to secondary leakage (refer to SAG-2, depressurize the RCS). • Depressurize SG by dumping steam to the condenser.
Creep rupture of SG tubes	**Depressurizing a SG with low water level** If steam generator wide range level in SG being depressurized is less than 12% AND if RCS pressure is greater than SG pressure.	• Depressurize only one hot, dry SG at a time to minimize consequences of SG tube failure. • Establish feed flow as soon as possible once SG pressure is below the shutoff head of the feed source. If SG WR level is less than 4%, then limit flow to SG to 22 m3/hr for the first 10 minutes of injection. • Depressurize the RCS (refer to SAG-2, Depressurize the RCS).
Degraded heat transfer	All means of SG injection with raw water sources	• Limit use of raw water to prevent build-up of precipitated materials on metallic surfaces
Component corrosion	All means of SG injection with raw water sources	• Limit use of raw water to prevent corrosion of metallic surfaces.

X.4.4.2 Depressurize the RCS

The depressurization of RCS (SAG-2) starts when the RCS pressure is below 22 bar. The purposes of depressurizing the RCS are:

- to prevent a high pressure melt ejection,
- to prevent creep rupture of the steam generator tubes when the SGs are dry,
- to allow RCS makeup from low pressure injection sources,
- to maximize RCS makeup from any centrifugal pump injection source,
- to prevent RHR system overpressure if still aligned for service.

The Table X-2 presents negative impacts (what), applicability (when) and mitigation actions of injection into SG.

Table X-2: Negative impacts and mitigation actions of depressurization of RCS

NEGATIVE IMPACT	APPLICABILITY	MITIGATING ACTIONS
Containment severe challenge from overpressure	**All RCS vent paths that release to containment** • IF containment pressure is greater than 3.48 bar	• Use SGs or aux pressurizer spray • Start containment heat sinks (refer to SAG-6, Control containment conditions). • Use one pressurizer PORV to reduce rate of containment pressurization.

SG fission product releases	**Depressurizing a ruptured or leaking SG**	• Use intact SGs that are isolated from ruptured SGs. • Use pressurizer PORVs or aux pressurizer spray • Use the steam dumps instead of the SG PORVs to provide additional fission product scrubbing. • Maintain SG NR water level above 70%
Loss of SG inventory	**Depressurizing a SG with low feed flow** • IF the SG feed rate is low	• Maintain SG NR water level above 70% • Use pressurizer PORVs or aux pressurizer spray.
Containment fission product releases	**All RCS vent paths that release to containment** • IF containment integrity is impaired	• Establish containment integrity • Use SG or aux pressurizer spray to depressurize the RCS • Maximize containment spray and fan coolers.

X.4.4.3 Inject into the RCS

The injection into RCS (SAG-3) starts when temperature is higher than 354 °C or containment radiation is high. The purposes of injection into the RCS are:

- to remove stored energy from the core when it has been uncovered,
- to provide an ongoing decay heat removal mechanism, by:
  - continuous injection and steaming of the water through an opening in the RCS, or
  - short-term injection into an intact RCS to establish a heat transfer pathway with the steam generators,
- to prevent or delay vessel failure,
- to provide a water cover to scrub fission products released from the core debris,
- to provide water to cool fuel in the refueling cavity.

The Table X-3 presents negative impacts (what), applicability (when) and mitigation actions of injection into RCS.

Table X-3: Negative impacts and mitigation actions of injection into RCS

NEGATIVE IMPACT	APPLICABILITY	MITIGATING ACTIONS

Creep rupture of SG tubes	**All means of RCS injection** • If steam generator wide range level in any steam generator is less than 12%, AND if RCS pressure is greater than SG pressure	• Maximize injection flow to SGs • Open RCS vent paths • Control the initial RCS injection flow so pressure across the SG tubes remains less than 34.32 bar • Close SG PORVs and steam dump valves
	Bumping RCPs • If steam generator wide range level in any steam generator is less than 12%	• Establish SG water wide range level greater than 12% BEFORE Bumping RCPs in that loop • Open RCS vent paths
Containment flooding	• All means of RCS injection with external water sources • If a large inventory of water will be injected, AND if there is an uncontrolled opening in the RCS. • Determine equipment and monitoring capabilities that may be lost.	• Use pumps in ECCS recirculation mode to prevent containment water level increase • Limit RCS injection flow, to limit rate of containment water level increase
Containment overpressure Severe challenge	**All means of RCS injection** • If MCCI is occurring • Containment pressure greater than 4.02 bar	• Stop injection to the RCS to limit containment pressure increase
Aux Building Habitability	**All Recirculation Pathways**	• Position portable shielding • Evaluate impact on critical local actions • Notify local work crews
RCP Seal Degradation	**Bumping RCPs**	• None
Component corrosion	**All means of RCS injection with non-reactor grade sources**	• Limit RCS injection flow • Switch RCS injection to a reactor grade water source, when sufficient inventory available

Fission product releases	**Using RWST gravity drain to RCS**	• Monitor RWST level and containment pressure, RWST gravity drain to RCS, to ensure no backflow • Identify potential containment heat sinks

REFERENCES

[1] Narsis Deliverable 5.2 Report on characterized EOP/EDMG/SAMG, Klemen Debelak, Luka Štrubelj, Ivica Bašić, November 2018

[2] Safety Reference Levels for Existing Reactors, Western European Nuclear Regulators Association, September 2014

[3] SSG-2: Deterministic Safety Analysis for NPP, IAEA Vienna 2009

[4] https://www.intechopen.com, 30.5.2019

XI Probabilistic Safety Analysis (PSA): Main Elements and Role in the Process of Safety Assessment and Verification

Ivan Vrbanić
APOSS
Repovec 23B
49210 Zabok, Croatia
ivan.vrbanic@zg.t-com.hr

Ivica Bašić
APOSS
Repovec 23B
49210 Zabok, Croatia
basic.ivica@kr.t-com.hr

ABSTRACT

The paper provides brief introduction to a concept of risk expressed in terms of likelihood consequences as well as to some basic principles of safety or risk management. This is followed by a high-level overview of main elements of probabilistic safety analysis and discussion of the role of probabilistic and deterministic safety analyses in the design safety verification.

XI.1 INTRODUCTION

Safety analyses for nuclear power plants are usually divided in two major types: deterministic safety analyses (DSA) and probabilistic safety analyses (PSA). This paper discusses, in a very simplified manner, why the two types of analyses, deterministic and probabilistic, are both required in the design and safety verification process for the nuclear power plants (or other facilities) when the overall safety, or the overall risk, is to be considered. Additionally, a basic overview of the main principles and technical elements of PSA is provided.

XI.2 RISK CURVE

At the beginning of a discussion of this kind, an appropriate technical definition is needed for a quantitative measure of the "overall safety". One of the, arguably, best ways is to present it through its inversion, the "overall risk", which is, in engineer's terms, quantitatively defined by the famous "risk curve", illustrated by Figure XI-1 (Ref. [1]).

Risk increases with likelihood of undesired event and with its consequences. Considering Figure XI-1, the overall risk can be defined by the area below the risk curve, i.e.:

$$R = \int_0^\infty |C(P_E) dP_E| \quad (1)$$

Two points regarding Figure XI-1 need to be noted (Ref. [2]):

1) Risk curve is defined in terms of a probability (or frequency!) of exceedance, which mathematically implies that it is a monotonously decreasing curve;
2) The simplistic formula "Risk = Probability x Consequence" (which can be found in handouts from numerous training courses on risk assessment for engineers) is valid only for a class of events with same consequence, where the term "Probability" represents a probability of occurrence (P_O) of an event from the class (for which it can be shown that it is a differential of a probability of exceedance), i.e.:

$$\Delta R = C\Delta P_E = CP_O \tag{2}$$

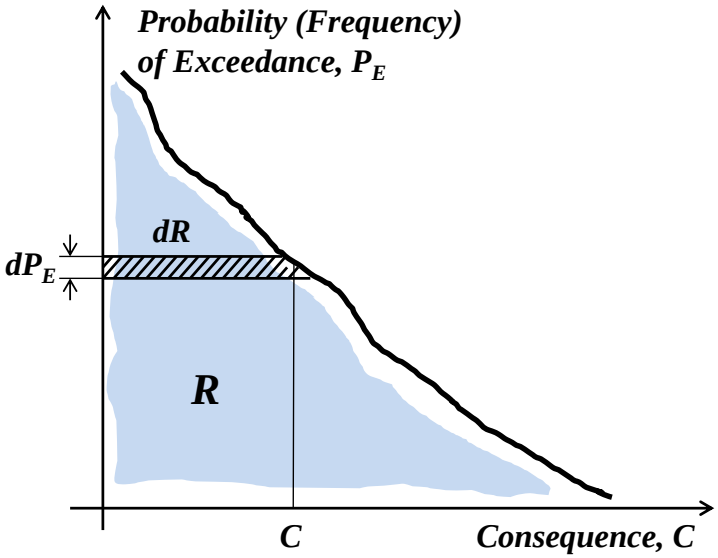


Figure XI-1: Risk Curve or Definition of Risk for an Engineer

XI.3 SAFETY MANAGEMENT (RISK MANAGEMENT)

From Figure XI-1 it can be seen that the purpose of the "safety management" or "risk management" basically is to minimize the area below the risk curve, or to suppress its "belly" as much as (practicably) achievable. This is illustrated by Figure XI-2, which also shows the two basic and most obvious principles of the risk / safety management.

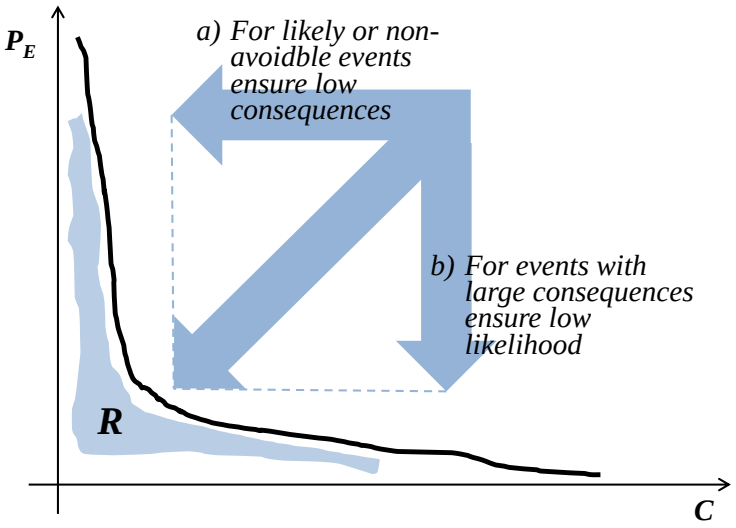


Figure XI-2: Two Basic Principles of Safety / Risk Management

A simple example for the principle a) from Figure XI-2 could be: if an area contains ignition sources, then move away or minimize the presence of combustibles (to minimize potential consequences of an ignition). This can, also, be rephrased to represent an example for a principle b): if an area contains combustibles, then move away or minimize the presence of ignition sources (to minimize a likelihood of an ignition) (Ref. [2]).

In the real world, neither consequences nor incredible scenarios can be completely eliminated. It should, therefore, be clear that an enforcement of safety / risk management from Figure XI-2 is possible only with two different sets of the safety goals in the risk space. Those are: A) deterministic, and B) probabilistic safety goals, indicated in Figure XI-3.

Compliance with the safety goal A) is only possible to demonstrate through a set of deterministic safety analyses. This is, simply, so because the required analyses need to demonstrate by calculation the consequences (e.g. maximum pressure, maximum stress, maximum temperature, maximum exposure to radioactivity, etc.) resulting from the postulated events and conditions. Deterministic safety analyses are performed with objective to demonstrate existence of adequate *safety margins* (e.g. demonstrate that maximum pressure is safely below the design basis pressure). This type of analysis is usually referred to as *design basis analysis*. Therefore, design basis analyses are inherently deterministic.

On the other hand, a compliance with the safety goal B) is only possible to demonstrate through a set of probabilistic safety analyses. In this case, this is simply so because the required analyses need to provide a calculation of likelihood (i.e. probability or frequency) for all the initiating events and scenarios for which the consequences were not demonstrated acceptable. This kind of analysis is usually referred to as *risk analysis* because its purpose is to assess the risk from exceeding the design basis (e.g. the risk that pressure exceeds the design basis pressure). Therefore, risk analysis is inherently probabilistic (with a due notion to the possibility that, sometimes, probability may be expressed qualitatively).

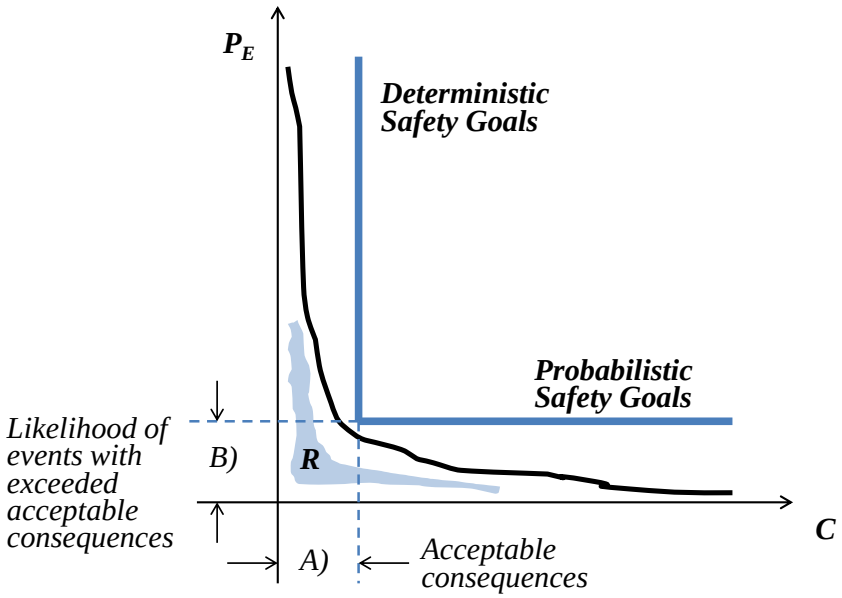


Figure XI-3: Two Types of Safety Goals

To continue with previous example: if the strategy a) was selected and presence of combustibles reduced but not eliminated, then it shall be deterministically demonstrated that release of energy from the remaining combustibles in a case of fire would not exceed the safety goal A). If strategy b) was selected and all combustibles retained (so that it was obvious that the goal A) cannot be achieved), then it shall be probabilistically shown that the likelihood of combustion due to the presence of ignition sources is such that goal B) is complied with.

Thus, on the basis of the above discussion, the overall process of "design for safety" would include the following stages: 1. Design postulation and development; 2. Design basis analyses to demonstrate that safety goals of type A) are met (deterministic safety analyses); 3. Design risk analyses to demonstrate that safety goals of type B) are met (probabilistic safety analyses); and 4. Loop back and iterations, if required.

In practice, the risk curve from Figure XI-1 is many times simplified by use of predefined consequences for "measuring" the risk. The examples of such predefined consequences associated with NPP design or operation are reactor core damage or large early release of radioactivity into the environment. With introduction of a predefined consequence equation (2) further simplifies into:

$$\Delta R = P_O \tag{3}$$

where the term P_O is the probability (or frequency!) of events or scenarios leading to predefined consequences. This term represents a quantitative *risk measure*. Some very famous risk measures in NPP safety assessment / verification processes include core damage frequency (CDF) and large early release frequency (LERF). Such risk measures are many times used as a basis for setting probabilistic safety goals indicated in Figure XI-3.

XI.4 OVERVIEW OF PSA AND ITS MAIN TECHNICAL ELEMENTS

Calculation or, rather, assessment of risk measures such as CDF or LERF is done by means of PSA analyses. PSA analysis is performed in order to develop a "PSA model" to be used as a tool to assess a CDF or a LERF or other risk measure. A "PSA model" can, basically, be thought of as a logic-probabilistic structure composed at three layers.

The first layer is *logic model* of initiating events, accident sequences and failures of equipment and human operators ultimately leading to predefined consequence (e.g. reactor core damage). This logic model is in most cases developed by means of event trees and fault trees.

The second layer is *quantification* of basic elements of the logic model. The basic elements are usually referred to as basic events and quantification refers to assessing and assigning a probability to each of them. This involves principles of reliability theory, principles of reliability parameters estimate, principles of assessing human errors probabilities, as well as some other disciplines.

The third layer is *characterization of uncertainty* involved in the risk assessment. This one deals, generally speaking, with assessing the uncertainty of the results due to uncertainty in parameters used, completeness of the model(s) employed and state of knowledge.

In short, it can be said that:

- Establishing the first layer (*logic model*) enables identification of combinations of failures (or sequences of events) leading to predefined consequence (e.g. reactor core damage);
- Establishing the second layer (*quantification*) upon the first one enables calculation of probabilities of those combinations / sequences and, ultimately, assessment of probability of predefined consequence or – risk measure; additionally, it enables to identify the main contributors to the risk and possibilities to reduce the risk;
- Establishing the third layer (characterization of uncertainty) upon the first two enables assessing the range of uncertainty in obtained value of risk measure and identifying its main sources.

PSA analysis which is, with its three layers, meant to be used in support of design or operation of NPPs is expected to be developed systematically by means of technical elements and their attributes which are defined by existing PSA guidelines and standards. A list of well-known documents in this field would include the IAEA guides for "Level 1" PSA and "Level 2" PSA, SSG-3 (Ref. [3]) and SSG-4 (Ref. [4]), the famous ASME PRA Standard (Ref. [5]) and also famous U.S. NRC's RG 1.174 (Ref. [6]), just to mention some. Although there are certain differences, mentioned documents establish a set of some eight or nine main technical elements of a PSA with a scope for assessing reactor CDF (so called "Level 1" PSA) for internal initiating events at power. They can be summarized as:

- Initiating Events Analysis;
- Accident Sequence and Success Criteria Analyses;
- Systems Analysis;
- Human Reliability Analysis;
- Data Analysis;
- Dependent Failures Analysis;

- Model Integration and Quantification; and
- Results Interpretation.

Analogously, sets of technical elements are also established, by some of mentioned documents and by some others, for other initiating event categories (e.g. external hazards), other modes of operation (e.g. shutdown modes) and other risk measures (e.g. risk from radioactivity releases).

A "PSA model" can be thought of as a large logic equation in which a top event (predefined consequence such as reactor core damage, as mentioned above) is expressed in terms of initiators / hazards, equipment failures and human errors. Such logic equation is usually built by means event trees (ET) and fault trees (FT) as illustrated by Figure XI-4.

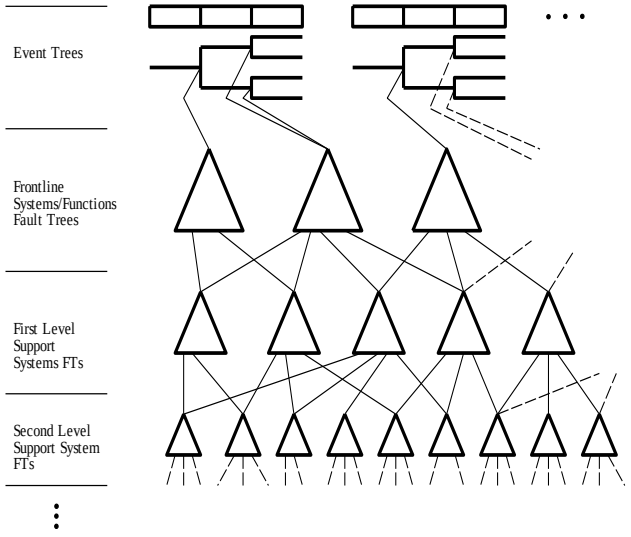


Figure XI-4: Logic Structure of PSA Model Built by ET and FT Linking

Mentioned initiators / hazards, failures and errors are in the PSA model's structure represented by "basic events". The top event (e.g. core damage) is, thus, expressed as logic function of "basic events". The key term in top event analysis and quantification is "minimal cutset" (MCS) which represents minimal combination of events leading to the top event (e.g. minimal combination of equipment failures and operator errors leading to core damage). The top event analysis / quantification are usually done in two major steps:

- Identification of MCSs: Logic function presented by ETs and FTs is by the rules of Boolean algebra resolved into the form of logic sum of MCSs; (a list of MCSs is generated, with application of certain truncation or cut-off value);
- Quantification of top event: logic sum of MCSs is used as a basis for calculating the top event probability or frequency (e.g. CDF).

The list of MCSs serves as a basis for identification of dominant failure combinations. It is also used for identifying risk-important equipment and operator actions. For this purpose risk increase and risk decrease measures are calculated. (E.g. how much would top event probability

increase or decrease assuming that certain equipment is failed or is "perfect".) These features are used for design safety verification and improvements.

XI.5 COMBINED USE OF DSA AND PSA IN DESIGN VERIFICATION

From the above discussion on the safety / risk management it can be seen that for design safety verification both types of safety analyses, deterministic and probabilistic, are needed. Principles of their combined use are illustrated by Figure XI-5 which shows simplified event tree for the design basis large LOCA.

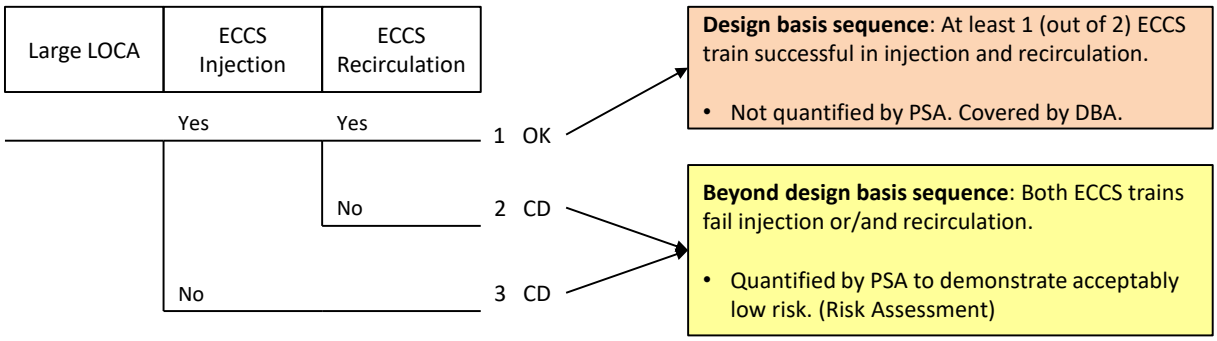


Figure XI-5: Combined Use of DSA and PSA in Design Verification (Illustration)

The Emergency Core Cooling System (ECCS) is a design basis (DB) system for mitigating such an initiator. For the sake of illustration it can be assumed that it consists of two independent trains. As indicated in Figure XI-5, sequence #1 is a DB sequence and it is not quantified in the PSA. It was covered by a design basis analysis (DBA) which deterministically demonstrated successful cooling of reactor core, with sufficient margin, by one out of two ECCS trains. Sequences #2 and #3, however, represent beyond design basis condition as both ECCS trains fail to perform injection or / and recirculation. Therefore, these two sequences need to be quantified by the PSA to calculate their probability (frequency) and demonstrate that it is acceptably low (i.e. the risk is acceptably low).

REFERENCES

[1] I. Vrbanic, P. Samanta and I. Basic, "Risk Importance Measures in the Design and Operation of Nuclear Power Plants", The American Society of Mechanical Engineers, New York, 2017, pp. 3-5.

[2] I. Vrbanic and I. Basic, "DSA vs. PSA, Why DSA and PSA Are Complementary", Article published in RiskSpectrum Magazine 2014, Lloyd's Register Consulting, 2014

[3] "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants", Specific Safety Guide No. SSG-3, International Atomic Energy Agency, Vienna, 2010

[4] "Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants", Specific Safety Guide No. SSG-4, International Atomic Energy Agency, Vienna, 2010

[5] ASME/ANS RA-Sa–2009. 2009, Addenda to ASME/ANS RA-S–2008, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications", An American National Standard, The American Society of Mechanical Engineers, New York, 2009

[6] U.S. NRC Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-specific Changes to the Licensing Basis", Revision 2, U.S. Nuclear Regulatory Commission, May 2011.

NARSIS Workshop
Training on Probabilistic Safety Assessment for Nuclear Facilities
International Training Course
Warsaw, Poland, September 2-5, 2019

XII Principles Of Severe Accident Risk Analysis

Ivica Bašić
APOSS d.o.o.
Repovec 23B
HR-49210, Zabok, Croatia
basic.ivica@kr.t-com.hr

Ivan Vrbanić
APOSS d.o.o.,
Repovec 23B
HR-49210, Zabok, Croatia
ivan.vrbanic@zg.t-com.hr

Marko Bohanec
Jožef Stefan Institute,
Dept of Knowladge Technologies
Jamova cesta 39
SI-1000, Ljubljana, Slovenia
marko.bohanec@ijs.si

ABSTRACT

The paper first presents the generic principles of Severe Accident Risk Analysis and then continues with discussing how the general principles were used and customized under the NARSIS Project's Work Package 5 (Supporting Tool for Severe Accident Management), Task 5.3:: Definition of Hazard-Induced Damage States and Development of State-Specific APETs for Demonstration Purposes, [1].

XII.1 INTRODUCTION

In developing appropriate logic model of severe accident progression, the main issue to be dealt with is that once an accident is triggered by certain initiator the sequences of events may progress in, for practical purposes, an infinite number of ways. Therefore, what generally needs to be done can be summarized by two points:

- Establish a methodology which can be used to put all possible accident sequences into some kind of systematic order so that they can be analytically (e.g. logically) processed; and
- Based on such methodology, define a set of induced damage states resulting from those sequences, for further analysis (e.g. for risk quantification).

The challenge is in how to put an infinite number of possible sequences into a limited number of damage states (or sequence groups) in a way that no relevant sequence is omitted and that resulting number of states / sequence groups is reasonably small (in order to be analytically manageable).

XII.2 ACCIDENT PROGRESSION LOGIC MODEL

Probabilistic safety assessment (PSA) for nuclear power plants is an attempt to put all possible accident sequences into a logic system which is manageable for practical purposes concerning plant safe design and operation. PSA, as defined and known today, is considered to be the best method currently for the purpose of accident progression logic modelling. Here, the

term “as defined and known today” refers to PSA attributes and uses established in accordance with internationally recognized standards and technical guiding documents, such as safety guides and technical documents [5], [6], [7] and other PSA-related documents of International Atomic Energy Agency (IAEA); PSA standards [2] and [3] of American Society of Mechanical Engineers (ASME); regulatory guides [14], [15], and others of U.S. Nuclear Regulatory Commission (NRC); as well as a number of other internationally known guidelines from the side of regulators, industry or utilities.

The complexity of the logic model of severe accident sequences, as well as their very large numbers to be dealt with, can be appropriately illustrated as in Figure XII-1, which is taken from the IAEA’s SSG-4, [6]. The set of all possible (imaginable) initiators is usually partitioned in two major categories: loss of coolant accidents (LOCA) and transients. (“Transient” category, in this context, represents anything that remains after all the LOCA-type events (direct or consequential) are addressed). They are usually further divided into a number of initiating event (IE) categories. Each IE category is “passed” through appropriately developed “event tree”, resulting in a number of accident sequences leading to end states involving some degree of reactor core damage. These sequences are usually referred to as “core damage” (CD) sequences. This is in Figure XII-1 represented by the first box on the left side, “Level 1 PSA”. A Level 1 PSA for a nuclear power plant (which is currently operating around the world) would have hundreds if not thousands of CD sequences explicitly modelled.

Each CD sequence from the Level 1 PSA is further “passed” through a response of containment systems (such as containment spray, fan coolers and isolation) which is usually modelled by some kind of containment systems event trees. Those are usually referred to as the “bridge trees” or “Level 1 - Level 2 interfacing event trees”. In Figure XII-1 this is represented by the box “Level 1-2 Interface”. Level 1 event trees together with bridge trees represent logic model of response of plant’s safety systems and engineered safety features (ESF) to the initiating events. It is not difficult to imagine that such a model would have thousands, if not tens of thousands of accident sequences modelled. A kind of logic “discipline” and rules are needed in order to keep such a model manageable. This is usually achieved by grouping or “binning” of the sequences into a manageable number of groups / bins. The end-states of the bridge trees are usually referred to as “Plant Damage States”.

The logic model for severe accident sequences can, thus, be divided into two parts: logic model for the response of plant systems / engineered safety features (Level 1 event trees and Level 1 - Level 2 bridge trees) and logic model for severe accident phenomenology. These two parts are distinguished in many PSAs.

It should be noted that severe accident progression and phenomenology can be evaluated only by dedicated deterministic severe accident models and codes (e.g. MAAP, MELCOR, ASTEC, etc.) [9] and [10]. Deterministic analyses are used to define time windows for success of certain assumed operator actions or systems/components performance (e.g. L1-L2 interface), for assessment of fission product barriers status (fuel, cladding, RCS, containment), etc.

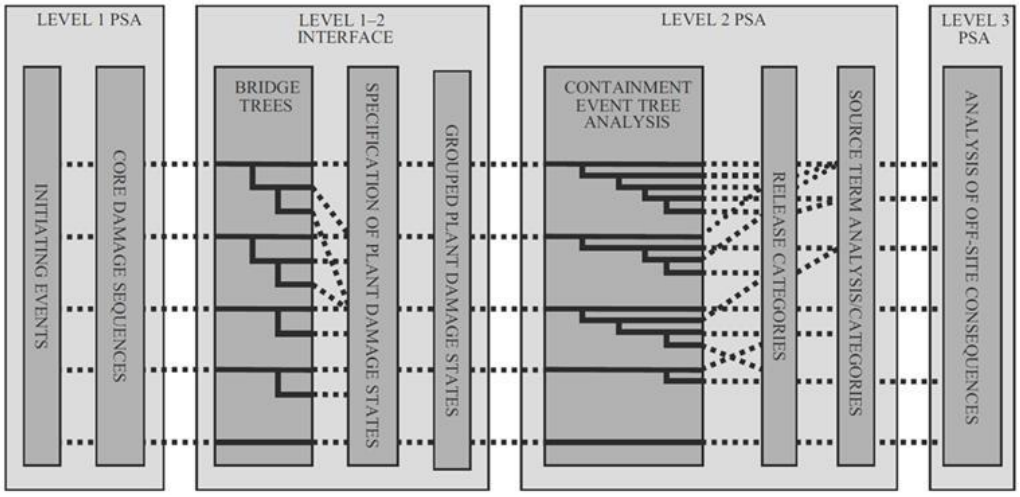


Figure XII-1: Outline of Logic Model for Severe Accident Sequences in PSA (Taken from the IAEA's SSG-4, [6]

Part of the described model (as depicted by Figure XII-1) from the initiators to the release categories is considered to be a proper basis for development of the supporting tool for severe accident management for demonstration purposes, under NARSIS Work Package 5. However, it should be clear that the above logic model needs to be simplified for the demonstration purposes and for investigating of the feasibility of this kind of accident management supporting tool (i.e. for the purposes of the NARSIS project).

XII.2.1 Principles for Characterization of Plant Damage States (PDS)

Term Plant Damage State (PDS), as used here, represents a group of accident sequences resulting with similar response of plant systems / ESFs, similar damage to the reactor core and similar challenge to the containment.The PDSs (induced by a hazard / initiator or by progression of triggered accident sequence) are typically characterized by a set of attributes. Those attributes usually include:

- Initiating event type ;
- Time of core damage;
- Pressure at reactor vessel failure;
- Status of ECCS;
- Status of containment heat removal (CHR);
- Status of containment integrity.

Each of these functional characteristics (attributes) can significantly influence the progression of a severe accident (pre- and/or post- core damage) and, thus, the resulting performance of the containment. What is in a PSA referred to as a "plant damage state" is a particular combination of states defined for such pre-established attributes.

For the purpose of NARSIS project, under Work Package 5 [1], a set of hazard damage states (HDS) is established by considering the PSA-based plant damage state framework discussedabove, see Table XII-1. (Term "HDS" is used because trigger of accident sequence is external hazard, such as seismic event.) The initial condition for the purpose of [1] is start of core damage with (initially) intact containment.

Table XII-1: Hazard Damage States

Attribute	**Status**
Pressure at Reactor Vessel Failure (RVF)	H = Reactor Vessel fails at high pressure; L = Reactor Vessel fails at low pressure; R = Pre-requisites for in-vessel recovery (IVR);
Emergency Core Cooling (ECCS) Status	B = Refueling Water Storage Tank (RWST) inventory transported into the RCS / containment before RVF; A = RWST transported after RVF; N= RWST not transported;
Containment Heat Removal (CHR) Status	Y = Yes (CHR available); N = No (CHR not available);

XII.2.2 Principles of Containment Event Tree, Accident Progression and Quantification

Particular plant damage states need to be "passed" through the event tree which represents a logic model of severe accident phenomena taking place inside the reactor vessel and primary system (many times referred to as "in-vessel" phenomena) as well as outside of the vessel / primary system (usually referred to as "ex-vessel" phenomena). This event tree is usually referred to as a "containment event tree" (as in Figure XII-1) or as an "accident progression event tree" (APET). In this paper the second term will be used (accident progression event tree), since the abbreviation for the first term is the same as for the "core exit thermocouples" (CET), which is one of the key terms in the frame of Work Package 5in, [1] and [13]. Generally, APET approach is used to provide framework for identifying, displaying and quantifying severe accident sequences. The APET generally contains top events related to the severe accident phenomenology. APET split fractions are developed using detailed event decomposition and describing uncertainties in physical phenomena by means of probability distribution. APETs are evaluated using "stress-strength interference" combinations of the specifically derived load distribution with the calculated containment structural capacity distribution.

For the purpose of Work Package 5 the simplified APET approach is used. The core damage sequences are, depending on the pressure at which core degradation starts and on the implementation of the RCS depressurization, broadly divided into three major categories:

- Low Pressure (LP) core damage sequences which lead to in-vessel recovery or to low pressure reactor vessel failure (SUB1);
- High Pressure (HP) core damage sequences which lead to RCS creep rupture (at locations other than SG tubes) or to high pressure reactor vessel failure, whichever comes first (SUB2);
- High Pressure (HP) core damage sequences with SG tube creep rupture; these sequences would lead to direct and early releases of radioactivity into the environment (SUB2);

A diagram representing the overall APET structure is shown in Figure XII-2. As shown, the APET structure to be incorporated into the future tool would consist of three main parts:

- Main tree;
- Sub-trees SUB1 and SUB2 mentioned above, with their sets of HDSs;
- Phenomenological trees which would map HDSs into the release categories (RC) and which would be incorporated into the tool in the form of the HDS-RC matrix.

Detailed sub-trees can be founded in [1].

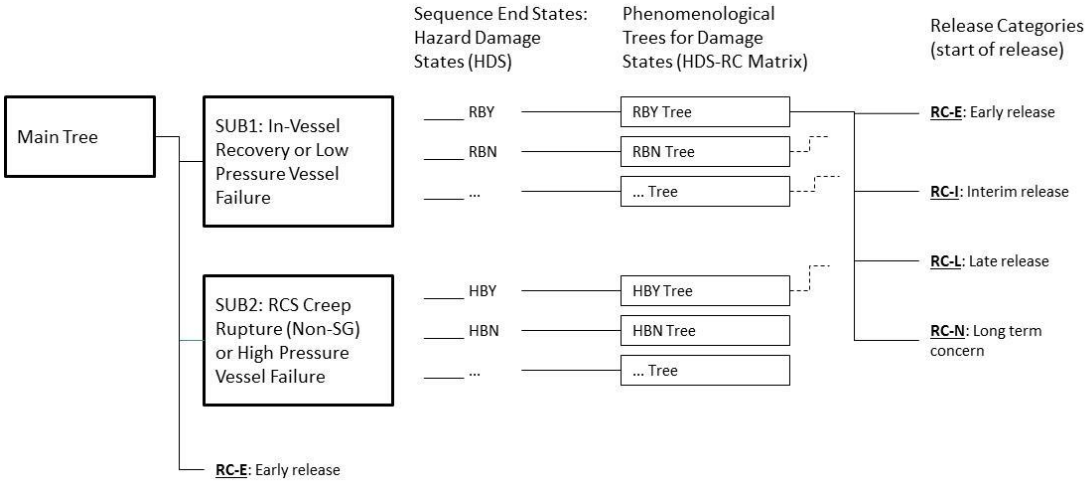


Figure XII-2: Overall simplified APET structure

XII.2.3 Principle characterization of Release Categories (RC)

The end states of the accident progression event tree represent states with different releases of radioactivity into the environment, depending on the accident phenomena and containment failure modes. They are, in most of the cases, grouped into categories which are usually referred to as "release categories" (which is also the case in Figure XII-1). Many times, a Level 2 PSA model would have about 10 to 20 release categories. For each release category a "source term" is usually calculated, including the inventories, amounts and timing of radioactivity releases. The whole model is, eventually, extended to the so-called Level 3 PSA, which represents the analysis of the offsite consequences. The source term analysis and offsite consequences analysis are, in principle, considered not to be relevant for Work Package 5, as the focus is on preserving the containment integrity (avoid large releases), rather than response to large releases (e.g. emergency planning).

Severe accident progression and degrees of severity

In the case of an accident sequence with sustained loss of core cooling, the accident progression can involve two phases, with fundamental differences in the challenges to safety functions and the source term: the **in-vessel phase** and the **ex-vessel phase**. As it is mentioned above, severe accident progression and phenomenology can be evaluated only by dedicated deterministic severe accident models and codes (e.g. MAAP, MELCOR, ASTEC etc.).

Figure XII-3 illustrates the severe accident progression diagram with typical times (from various severe accident analyses) of phenomenologically critical events (e.g. core uncovering, starting of fuel cladding oxidation (hydrogen production), reactor pressure vessel failure and containment failure) for the reference plant (2000 MWth) without implemented operator preventive or mitigative actions. Also, Figure XII-3 illustrates severe accident progression for two major groups of initiating events/sequences grouped based on RCS pressure at time when reactor pressure vessel (RPV) fails (low pressure (LP) presented by Large Break Loss of Cooling Accident (LB-LOCA) or high pressure (HP) sequences Loss of All Feedwater (LOAF)).

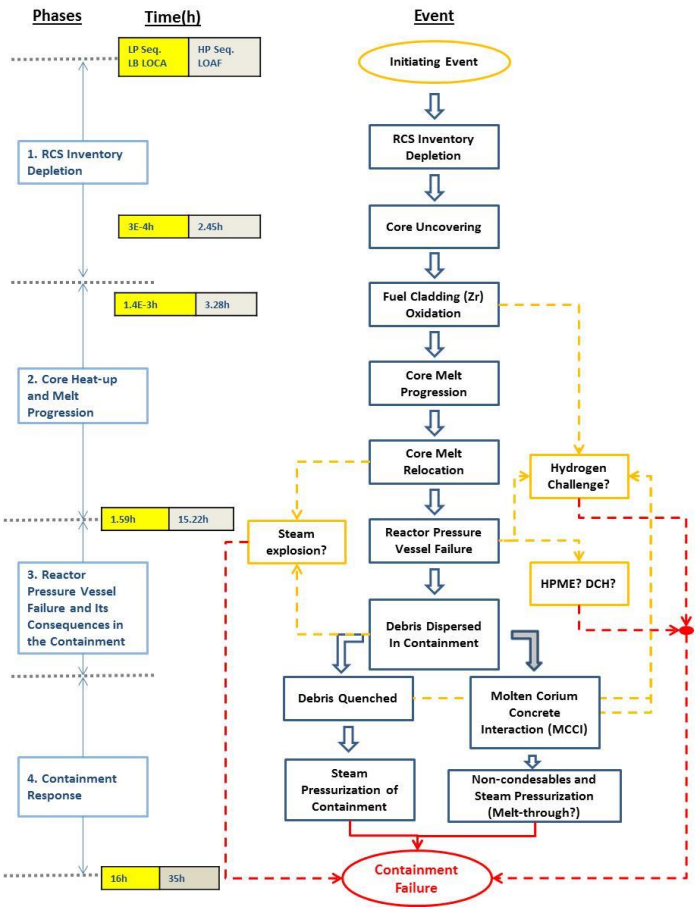


Figure XII-3: Severe Accident Progression Diagram

XII.3 TYPES OF DECISION AND STRATEGIES/ACTIONS PERFORMED IN SEVERE ACCIDENT MANAGEMENT

Depending on the level of defense in depth breached, the following are the four main objectives of accident management ([4], [8]):

1) Prevention of the accident from leading to core damage,
2) Termination of core damage,
3) Maintaining the integrity of the containment for as long as possible,
4) Minimizing on-site and off-site releases and their adverse consequences.

The NARSIS report 5.2 [13] describes a general concept of Emergency Operating Procedures (EOP), Extreme Damage Management Guidelines (EDMG) and Severe Accident Management Guidelines (SAMG) typically used in the second generation operating nuclear power plant, representing the European fleet.

The report [13] provides also detailed description and major steps of representative SAMG Diagnostic Flowchart (DFC) and the major four SAGs used for demonstration of SAMG diagnostic tool through two chosen scenarios (severe accident scenario with high RCS pressure at RPV failure and severe accident scenario with low RCS pressure at RPV failure):

- SAG-1 Inject into SG
- SAG-2 Depressurization of RCS
- SAG-3 Inject into RCS
- SAG-6 Control Containment Condition

Status of plant is determined and entering of SAMG done based on behavior of 6 major dedicated plant parameters (core exit temperature, steam-generator level, reactor pressure vessel level, reactor coolant system pressure, and containment pressure and containment hydrogen concentration).Once entered, SAMGs are used to:

a. determine the availability of equipment to perform the strategies;
b. determine the positive and negative impacts associated with implementation of each of the available strategies;
c. determine the limitations dictated by plant conditions associated with implementation of a strategy;
d. determine the impact of not implementing any of the strategies;
e. determine the short term and long term plant response after strategy implementation, and
f. determine if an implemented strategy should be stopped due to excessive negative impacts.

However, the safety functions in SAMGs to be accomplished are the same as those addressed in the EOPs, but more focused on the conditions faced with when core damage has begun and on any available equipment (SSCs) to mitigate the consequences, e.g.:

- Design basis SSCs (as equipment to implement the function, which is considered adequate and is available now or in near future),
- Alternate SSCs (as equipment to implement the function which is considered adequate, but is usually not available immediately. E.g., evaluator considers that it will be available in less than 2 hours), and
- Mobile (or sometimes called “FLEX”) (as equipment is to be available in, e.g., less than 2 hours, but it may or may not be really adequate (e.g. 50% confidence)).

XII.4 ATTRIBUTES FOR USE IN DECISION-MAKING

The attributes presenting quantitative risk for comparing different alternatives in Supporting Tool for Severe Accident Management will be the likelihood of containment failure and general time frame at which the failure is expected to occur. They will be expressed through the four categories of radioactivity release which were included in Figure XII-2 (RC-I, RC-E, RC-N and RC-L). Figure XII-4 presents illustrative comparison of two alternative severe accident strategies for HP accident sequence using the simplified APET model as presented on Figure XII-2.

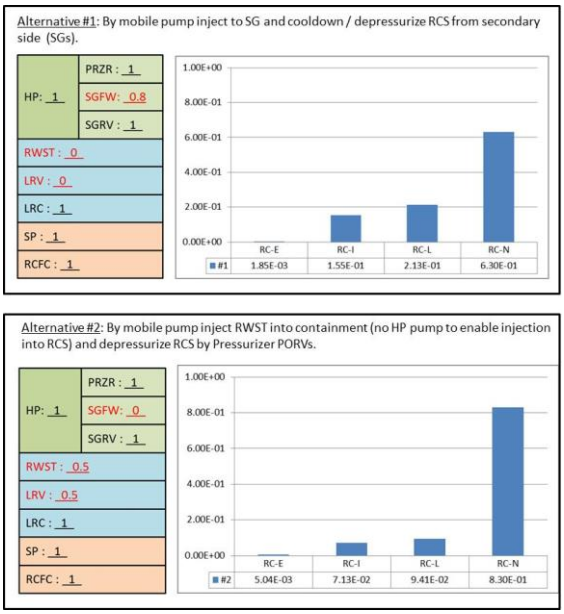


Figure XII-4: Illustration of Comparison of Two Alternatives

Supporting tool is preliminary named “SEVERA” [1] and is still under development in NARSIS Task 5.4. Supporting tool concept is presented on Figure XII-5 bellow.

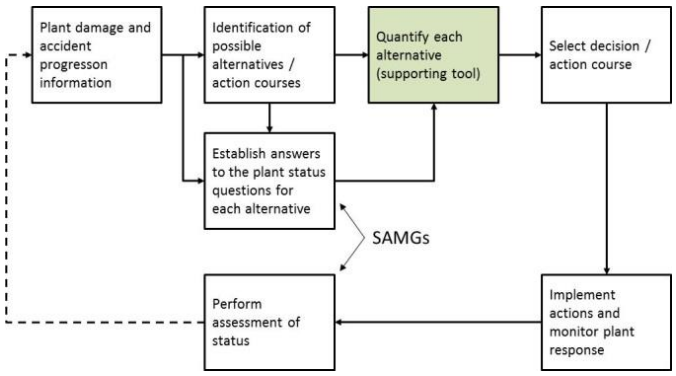


Figure XII-5: Conceptual Diagram for Use of the Tool

XII.5 SUMMARY

The paper summarizes the NARSIS Project Task 5.3 which has the objective to establish the hazard damage states and the logic model for accident progression, to be used as a basis for the accident management supporting tool for demonstration purposes.

First, the paper provides some background on hazard-induced damage states and on accident progression logic modeling by means of event trees and similar techniques such as sequence diagrams, based on the probabilistic safety analyses for the nuclear power plants.

Next, accident progression logic model structure which was established as a basis for the supporting severe accident management tool is briefly described..

Paper also briefly describes the types of decisions and actions which form the basis for establishing the available alternatives for severe accident management to be supported by the mentioned tool.

The main attributes for making quantitative comparisons among the available alternatives are expected to be the likelihood of containment failure and time frame at which the failure is expected to occur.

REFERENCES

[1] I. Vrbanić, I. Bašić (APOSS), L. Štrubelj, K. Debelak(GEN), M. Bohanec(JSI), D5.3 - Definition of Hazard-Induced Damage States and Development of State-Specific APETs for Demonstration Purposes, NARSIS Project, Horizon 2020, 2019

[2] M. Bohanec(JSI), I. Vrbanić, I. Bašić (APOSS), L. Štrubelj, K. Debelak(GEN), Conceptual Design of a Decision Support Tool for Severe Accident Management in Nuclear Power Plants, Paper for International Conference on Smart Computing and Artificial Intelligence (SCAI 2019)

[3] ASME/ANS RA-Sb-2013, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addendum B, ASME/ANS, New York, 2013;

[4] ASME/ANS RA-S-1.2-2014, Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), ASME/ANS, 2014;

[5] IAEA Safety Reports Series No. 32, Implementation of Accident Management Programmes in Nuclear Power Plants, 2004;

[6] IAEA Specific Safety Guide No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, 2010;

[7] IAEA Specific Safety Guide No. SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, Vienna, 2010

[8] IAEA-TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA, Vienna, 2016

[9] IAEA Draft Specific Safety Guide (DS483), Severe Accident Management Programmes for Nuclear power Plants, 2019;

[10] EPRI TR-1025295-V1, Severe Accident Management Guidance Technical Basis Report (TBR), Volume 1: Candidate High-Level Action and Their Effects, 2012;

[11] EPRI TR-1025295-V2, Severe Accident Management Guidance Technical Basis Report (TBR), Volume 2: The Physics of Accident Progression, 2012;

[12] European Commission Directorate-General Research and Innovation, Grant Agreement number: 755439 — NARSIS — NFRP-2016-2017/NFRP-2016-2017-1, ANNEX 1 (part A), Research and Innovation action

[13] Characterization of the Referential NPP for Severe Accident Management Analyses, NARSIS Deliverable D5.1, 2018

[14] Report on Characterized EOP/EDMG/SAMG, NARSIS Deliverable D5.2, 2018

[15] U.S. NRC Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis, Revision 2, U.S. NRC, 2011

[16] U.S. NRC Regulatory Guide 1.200, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, Revision 2, U.S. NRC, 2009