ASAMPSA_E SEVENTH FRAMEWORK PROGRAMME	Advanced Safety Assessment Methodologies: extended PSA	EURATOM

"NUCLEAR FISSION "

Safety of Existing Nuclear Installations

Contract 605001

Report 6: Guidance document MAN-MADE hazards and ACCIDENTAL AIRCRAFT CRASH hazards modelling and implementation in extended PSA

Reference ASAMPSA_E

Technical report ASAMPSA_E/WP21&WP22 / D50.20/ 2017-38

Reference IRSN PSN/RES/SAG/2017- 00013

S. Kahia (NRG), H. Brinkman (NRG), A. Bareith (NUBIKI), T. Siklossy (NUBIKI), T. Vinot (IRSN), T. Mateescu (IRSN), J. Espargillière (IRSN),L. Burgazzi (ENEA), I. Ivanov (TUS), D. Bogdanov (TUS), P. Groudev (INRNE), S. Ostapchuk (SSTC), O. Zhabin (SSTC), T. Stojka (VUJE), R. Alzbutas (LEI), M. Kumar (LR), M. Nitoi (RATEN ICN), M. Farcasiu (RATEN ICN), M. Borysiewicz (NCBJ), K. Kowal (NCBJ), S. Potempski (NCBJ)

Period covered: from 01/07/2013 to 31/12/2016	Actual submission date: 31/12/2016	
Start date of ASAMPSA_E: 01/07/2013	Duration: 42 months	
WP No: 21/22	Lead topical coordinator : H. Brinkman, S. Potempski	His organization name : NRG, NCBJ

Project co-funded by the European Commission Within the Seventh Framework Programme (2013-2016)		
Dissemination Level		
PU	Public	Yes
RE	Restricted to a group specified by the partners of the ASAMPSA_E project	No
CO	Confidential, only for partners of the ASAMPSA_E project	No

ASAMPSA_E Quality Assurance page

Partners responsible of the document :	**IRSN**
Nature of document	Technical report
Reference(s)	Technical report WP21&WP22 / D50.20/ 2017-38 Reference IRSN PSN/RES/SAG/2017-00013
Title	Report 6: Guidance document - MAN-MADE hazards and ACCIDENTAL AIRCRAFT CRASH hazards modelling in extended PSA
Author(s)	S. Kahia (NRG), H. Brinkman (NRG), A. Bareith (NUBIKI), T. Siklossy (NUBIKI), T. Vinot (IRSN), T. Mateescu (IRSN), J. Espargillière (IRSN),L. Burgazzi (ENEA), I. Ivanov (TUS), D. Bogdanov (TUS), P. Groudev (INRNE), S. Ostapchuk (SSTC), O. Zhabin (SSTC), T. Stojka (VUJE), R. Alzbutas (LEI), M. Kumar (LR), M. Nitoi (ICN), M. Farcasiu (ICN), M. Borysiewicz (NCBJ), K. Kowal (NCBJ), S. Potempski (NCBJ)
Delivery date	31th December 2016
Topical area	PSA, external hazards, man-made hazards, aircraft crash, extended PSA
For Journal & Conf. papers	No

Summary :

This report provides guidance on modelling and implementation of MAN-MADE hazards and ACCIDENTAL AIRCRAFT CRASH hazards in Extended Level 1 PSA.

This report is a deliverable of the ASAMPSA_E work packages WP21 (“Initiating events (internal and external hazards) modelling”) and WP22 (“How to model and introduce hazards in L1 PSA and all possibilities of events combinations”) aiming at identifying good practices on the modelling and implementation of extreme events related hazards of low probability in L1 PSA.

The End Users recommendations formulated at the beginning of the ASAMPSA_E project (work package WP10) have been taken into account as far as possible and also the recommendations of the ASAMPSA_E final survey and external review of draft guidance reports.

Visa grid

	Main author(s) :	**Verification**	**Approval (Coordinator)**
Name (s)	S. Kahia (NRG), S. Potempski (NCBJ)	H. Brinkman (NRG)	E. Raimond (IRSN)
Date	16-01-2017	16-01-2017	16-01-2017

MODIFICATIONS OF THE DOCUMENT

Version	Date	Authors	Pages or paragraphs modified	Description or comments
1	15-10-2015	S. Kahia (NRG), H. Brinkman (NRG) (coordinating authors)	All	First version available for the ASAMPSA_E technical meetings in November 2015, Fontenay-aux-Roses, France
5	15-04-2016	M. Borysiewicz , K. Kowal, S. Potempski (NCBJ) coordinating authors) with support of other authors (see above)	All	First complete version available for approval before release for external review.
6	23-05-2016	E. Raimond (IRSN)		Final review (approval). Editorial modifications and few additions. There is a need to suppress little duplication in the report in the final version. Some consistency modifications related to other ASAMPSA_E reports shall also be done in the final version.
7	13-11-2016	H. Brinkman (NRG), S. Potempski (NCBJ)	All	End user comments related mostly to conclusions and list of open issues added following September 2016 workshop in Vienna. Editorial modifications made and duplications removed.
8	14-12-2016	M. Kumar (LR)	All	Consistency modifications with other ASAMPSA_E reports done.
9	16-12-2016	H. Brinkman (NRG), S. Potempski (NCBJ)	All	Final check, list of publications corrected.
10	13-01-2017	E. Raimond	Few	Approval and final editorial reading.

LIST OF DIFFUSION

European Commission (scientific officer)

Name	First name	Organization
Passalacqua	Roberto	EC

ASAMPSA_E Project management group (PMG)

Name	First name	Organization	
Raimond	Emmanuel	IRSN	Project coordinator
Guigueno	Yves	IRSN	WP10 coordinator
Decker	Kurt	Vienna University	WP21 coordinator
Klug	Joakim	LRC	WP22 coordinator until 2015-10-31
Kumar	Manorma	LRC	WP22 coordinator from 2015-11-01
Wielenberg	Andreas	GRS	WP30 coordinator until 2016-03-31
Löffler	Horst	GRS	WP40 coordinator WP30 coordinator from 2016-04-01

REPRESENTATIVES OF ASAMPSA_E PARTNERS

Name	First name	Organization
Grindon	Liz	AMEC NNC
Mustoe	Julian	AMEC NNC
Cordoliani	Vincent	AREVA
Dirksen	Gerben	AREVA
Godefroy	Florian	AREVA
Hurel	François	AREXIS
Schirrer	Raphael	AREXIS
De Gelder	Pieter	Bel V
Gryffroy	Dries	Bel V
Jacques	Véronique	Bel V
Van Rompuy	Thibaut	Bel V
Cazzoli	Errico	CCA
Vitázková	Jirina	CCA
Passalacqua	Roberto	EC
Banchieri	Yvonnick	EDF
Bernadara	Pietro	EDF
Bonnevialle	Anne-Marie	EDF

Name	First name	Organization
Pierre	Cecile	AREVA
Kollasko	Heiko	AREVA
Pellisseti	Manuel	AREVA
Michaud	Laurent	AREVA
Hasnaoui	Chiheb	AREXIS
Bordes	Dominique	EDF
Brac	Pascal	EDF
Coulon	Vincent	EDF
Gallois	Marie	EDF
Hibti	Mohamed	EDF
Jan	Philippe	EDF
Lopez	Julien	EDF
Nonclercq	Philippe	EDF
Panato	Eddy	EDF
Parey	Sylvie	EDF
Romanet	François	EDF
Rychkov	Valentin	EDF

Vasseur	Dominique	EDF
Burgazzi	Luciano	ENEA
Hultqvist	Göran	FKA
Kähäri	Petri	FKA
Karlsson	Anders	FKA
Ljungbjörk	Julia	FKA
Pihl	Joel	FKA
Löffler	Horst	GRS
Mildenberger	Oliver	GRS
Sperbeck	Silvio	GRS
Tuerschmann	Michael	GRS
Wielenberg	Andreas	GRS
Benitez	Francisco Jose	IEC
Del Barrio	Miguel A.	IEC
Serrano	Cesar	IEC
Apostol	Minodora	RATEN ICN
Farcasiu	Mita	RATEN ICN
Nitoi	Mirela	RATEN ICN
Groudev	Pavlin	INRNE
Stefanova	Antoaneta	INRNE
Armingaud	François	IRSN
Bardet	Lise	IRSN
Bonnet	Jean-Michel	IRSN
Bonneville	Hervé	IRSN
Clement	Christophe	IRSN
Corenwinder	François	IRSN
Denis	Jean	IRSN
Duflot	Nicolas	IRSN
Duluc	Claire-Marie	IRSN
Dupuy	Patricia	IRSN
Georgescu	Gabriel	IRSN
Guigueno	Yves	IRSN
Guimier	Laurent	IRSN
Lanore	Jeanne-Marie	IRSN
Laurent	Bruno	IRSN
Ménage	Frédéric	IRSN
Pichereau	Frederique	IRSN
Rahni	Nadia	IRSN
Raimond	Emmanuel	IRSN
Rebour	Vincent	IRSN
Scotti	Oona	IRSN
Prošek	Andrej	JSI
Volkanovski	Andrija	JSI
Alzbutas	Robertas	LEI
Matuzas	Vaidas	LEI
Rimkevicius	Sigitas	LEI
Häggström	Anna	LRC
Klug	Joakim	LRC
Kumar	Manorma	LRC
Olsson	Anders	LRC
Borysiewicz	Mieczyslaw	NCBJ
Kowal	Karol	NCBJ
Potempski	Slawomir	NCBJ
La Rovere	Stephano	NIER
Vestrucci	Paolo	NIER
Brinkman	Hans	NRG
Kahia	Sinda	NRG
Bareith	Attila	NUBIKI
Lajtha	Gabor	NUBIKI
Siklossy	Tamas	NUBIKI
Caracciolo	Eduardo	RSE
Morandi	Sonia	RSE
Dybach	Oleksiy	SSTC
Gorpinchenko	Oleg	SSTC
Claus	Etienne	TRACTEBEL
Dejardin	Philippe	TRACTEBEL
Grondal	Corentin	TRACTEBEL
Mitaille	Stanislas	TRACTEBEL
Oury	Laurence	TRACTEBEL
Yu	Shizhen	TRACTEBEL
Zeynab	Umidova	TRACTEBEL
Bogdanov	Dimitar	TUS
Ivanov	Ivan	TUS
Holy	Jaroslav	UJV
Hustak	Stanislav	UJV
Jaros	Milan	UJV
Kolar	Ladislav	UJV
Kubicek	Jan	UJV
Decker	Kurt	UNIVIE
Halada	Peter	VUJE
Prochaska	Jan	VUJE
Stojka	Tibor	VUJE

REPRESENTATIVE OF ASSOCIATED PARTNERS (External Experts Advisory Board (EEAB))

Name	First name	Company
Hirata	Kazuta	JANSI
Hashimoto	Kazunori	JANSI
Inagaki	Masakatsu	JANSI
Yamanana	Yasunori	TEPCO
Coyne	Kevin	US-NRC
González	Michelle M.	US-NRC

EXECUTIVE SUMMARY

The goal of this report is to provide guidance on practices to model man-made hazards (mainly external fires and explosions) and accidental aircraft crash hazards and implement them in extended Level 1 PSA. This report is a joint deliverable of work package 21 (WP21) and work package 22 (WP22). The general objective of WP21 is to provide guidance on all of the individual hazards selected at the first ASAMPSA_E End Users Workshop (May 2014, Uppsala, Sweden). The objective of WP22 is to provide the solutions for purposes of different parts of man-made hazards Level 1 PSA fulfilment. This guidance is focusing on man-made hazards, namely: external fires and explosions, and accidental aircraft crash hazards. Guidance developed refers to existing guidance whenever possible.

The initial part of guidance (WP21 part) reflects current practices to assess the frequencies for each type of hazards or combination of hazards (including correlated hazards) as initiating event for PSAs. The sources and quality of hazard data, the elements of hazard assessment methodologies and relevant examples are discussed. Classification and criteria to properly assess hazard combinations as well as examples and methods for assessment of these combinations are included in this guidance. In appendixes additional material is presented with the examples of practical approaches to aircraft crash and man-made hazard.

The following issues are addressed:

1) Hazard assessment methodologies, including issues related to hazard combinations.
2) Modelling equipment of safety related SSC,
3) HRA,
4) Emergency response,
5) Multi-unit issues.

Recommendations and also limitations, gaps identified in the existing methodologies and a list of open issues are included.

At all stages of this guidance and especially from an industrial end-user perspective, one must keep in mind that the development of man-made hazards probabilistic analysis must be conditioned to the ability to ultimately obtain a representative risk analysis.

As it was recommended by end users (WP10), this guidance covers questions of developing integrated and/or separated man-made PSA models. Methods to model the combinations/correlations/dependencies of hazards, possible secondary effects, mitigating and aggravating factors are also proposed in the report. This report contains approaches to model mobile equipment but despite this fact, input data related to this (reliability and related human actions, assessment of time for its running) remains a source of significant uncertainty.

From an industrial end-user perspective, the PSA methodology must be proportionate to the importance of risks (this can be also required by national laws such as the French Law). The adoption of a graded approach for External Hazards PSA would better focus resources and direct them to identify and address issues that present the highest significance to NPP Risks and Safety. Therefore, there is no relevance to use complex methodologies if a simplified analysis gives sufficient and representative insights.

ASAMPSA_E PARTNERS

The following table provides the list of the ASAMPSA_E partners involved in the development of this document.

1	Institute for Radiological Protection and Nuclear Safety	IRSN	France
5	Lloyd's Register Consulting	LRC	Sweden
10	Nuclear Research and consultancy Group	NRG	Netherlands
11	IBERDROLA Ingeniería y Construcción S.A.U	IEC	Spain
12	Electricité de France	EDF	France
13	Lietuvos energetikos institutas (Lithuanian Energy Institute)	LEI	Lithuania
14	NUBIKI	NUBIKI	Hungary
17	NCBJ Institute	NCBJ	Poland
18	State Scientific and Technical Center for Nuclear and Radiation Safety	SSTC	Ukraine
19	VUJE	VUJE	Slovakia
25	Institute of nuclear research and nuclear energy – Bulgarian Academia of science	INRNE	Bulgaria
26	Regia Autonoma Pentru Activatati Nucleare Droberta Tr. Severin RA Suc	INR/RAAN	Romania
27	Technical University of Sofia – Research and Development Sector	TUS	Bulgaria

CONTENT

GLOSSARY

AEP	Annual Exceedance Probability
ARP	Alarm Response Procedure
CCF	Common Cause Failure
CDF	Core Damage Frequency
DPD	Discrete Probability Distributions
DSG	Design Safety Guide
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
EPZ	Emergency Planning Zones
ETL	Event Tree Linking
FDF	Fuel Damage Frequency
FTL	Fault Tree Linking
HCLPF	High Confidence of Low Probability of Failure
HEP	Human Error Probability
HFE	Human Failure Events
HRA	Human Reliability Analysis
IE	Initiating Event
IPEEE	Individual Plant Examination of External Events
ISRS	In Structure Response Spectra
LERF	Large Early Release Frequency
LHS	Latin Hypercube Sampling
LOCA	Loss of Coolant Accidents
LOOP	Loss of Off-Site Power
MCS	Monte Carlo Simulation
PDF	Probability Density Functions
PIE	Postulated Initiating Event
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PSHA	Probabilistic Seismic Hazard Analysis
PSR	Periodic Safety Review
QRA	Quantitative Risk Assessment
RLE	Review Level Earthquake
NDC	NPH Design Category
NPH	Natural Phenomena Hazards
NPP	Nuclear Power Plant
SAM	Severe Accident Management
SAP	Safety Assessment Principles
SAR	Safety Analysis Report
SBO	Station Black Out
SMA	Seismic Margin Assessment
SPAR	Standardized Plant Analysis Risk
SPRA	Seismic Probabilistic Risk Assessment
SSC	Structure System and Component

SSI	Soil Structure Interaction
THERP	Technique for Human Error Rate Prediction
WP	Work Package

DEFINITIONS

These definitions come from IAEA and US NRC safety glossaries.

Accident Sequence Analysis	The process to determine the combinations of initiating events, safety functions, and system failures and successes that may lead to core damage or large early release.
Bounding Analysis	Analysis that uses assumptions such that assessed outcome will meet or exceed the maximum severity of all credible outcomes.
Event Tree Analysis	An inductive technique that starts by hypothesizing the occurrence of basic initiating events and proceeds through their logical propagation to system failure events. • The event tree is the diagrammatic illustration of alternative outcomes of specified initiating events. • Fault tree analysis considers similar chains of events, but starts at the other end (i.e. with the 'results' rather than the 'causes'). The completed event trees and fault trees for a given set of events would be similar to one another.
Fault Tree Analysis	A deductive technique that starts by hypothesizing and defining *failure events* and systematically deduces the *events* or combinations of *events* that caused the *failure events* to occur. • The fault tree is the diagrammatic illustration of the *events*. • *Event tree analysis* considers similar chains of *events*, but starts at the other end (i.e. with the 'causes' rather than the 'results'). The completed *event* trees and fault trees for a given set of *events* would be similar to one another.
Cliff Edge Effect	In a nuclear power plant, an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small *deviation* in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.
Design Basis	The range of conditions and *events* taken explicitly into account in the *design* of a *facility*, according to established criteria, such that the *facility* can withstand them without exceeding *authorized limits* by the planned *operation* of *safety systems*.
Design Basis External Events	The *external event(s)* or combination(s) of *external events* considered in the *design basis* of all or any part of a *facility*.
External Event	An event originated outside a nuclear power plant that directly or indirectly causes an initiating event and may cause safety system failures or operator errors that may lead to core damage or large early release. Events such as earthquakes, tornadoes, and floods from sources outside the plant and fires from sources inside or outside the plant are considered external events. By historical convention, LOOP not caused by another external event is considered to be an internal event. According to NUREG 2122, the term external event is no longer used and has been replaced by the term external hazard.
External Hazard Analysis	The objective is to evaluate the frequency of occurrence of different severities or intensities of external events or natural phenomena (e.g., external floods or high winds).
Fragility	The fragility of a structure, system or component (SSC) is the conditional probability of its failure at a given hazard input level. The input could be earthquake motion, wind speed, or flood level.
Fragility Analysis	Estimation of the likelihood that a given component, system, or structure will cease to function given the occurrence of a hazard event of a certain intensity. • In a PRA, fragility analysis identifies the components, systems, and structures susceptible to the effects of an external hazard and estimates their fragility parameters. Those parameters are then used to calculate fragility (conditional probability of failure) of the component, system, or structure at a certain intensity level of the hazard event. • Fragility analysis considers all failure mechanisms due to the occurrence of an

	external hazard event and calculates fragility parameters for each mechanism. This is true whether the fragility analysis is used for an external flood hazard, fire hazard, high wind hazard, seismic hazard, or other external hazards. For example, for seismic events, anchor failure, structural failure, and systems interactions are some of the failure mechanisms that would be considered.
Fragility Curve	A graph that plots the likelihood that a component, system, or structure will fail versus the increasing intensity of a hazard event. • In a PRA, fragility curves generally are used in seismic analyses and provide the conditional frequency of failure for structures, systems, or components as a function of an earthquake-intensity parameter, such as peak ground acceleration. • Fragility curves also can be used in PRAs examining other hazards, such as high winds or external floods.
Hazard	The ASME/ANS PRA Standard defines a hazard as “an event or a natural phenomenon that poses some risk to a facility. • Internal hazards include events such as equipment failures, human failures, and flooding and fires internal to the plant. • External hazards include events such as flooding and fires external to the plant, tornadoes, earthquakes, and aircraft crashes.”
Hazard Analysis	The process to determine an estimate of the expected frequency of exceedance (over some specified time interval) of various levels of some characteristic measure of the intensity of a hazard (e.g., peak ground acceleration to characterize ground shaking from an earthquake). The time period of interest is often taken as 1 year, in which case the estimate is called the annual frequency of exceedance.
Human Reliability Analysis	A structured approach used to identify potential human failure events and to systematically estimate the probability of those events using data, models, or expert judgment.
Individual plant examination for external events (IPEEE)	While the "individual plant examination" takes into account events that could challenge the design from things that could go awry internally (in the sense that equipment might fail because components do not work as expected), the "individual plant examination for external events" considers challenges such as earthquakes, internal fires, and high winds.
Initiating Event	An identified *event* that leads to *anticipated operational occurrences* or *accident conditions*. • This term (often shortened to ***initiator***) is used in relation to *event* reporting and *analysis*, i.e. when such *events* have occurred. For the consideration of hypothetical *events* considered at the *design* stage, the term *postulated initiating event* is used.
Large early release	The rapid, unmitigated release of air-borne fission products from the containment to the environment occurring before the effective implementation of off-site emergency response and protective actions such that there is a potential for early health effects.
Large early release frequency (LERF)	Expected number of large early releases per unit of time.
Loss of coolant accident (LOCA)	Those postulated accidents that result in a loss of reactor coolant at a rate in excess of the capability of the reactor makeup system from breaks in the reactor coolant pressure boundary, up to and including a break equivalent in size to the double-ended rupture of the largest pipe of the reactor coolant system.
Loss of Offsite Power (LOOP)	The loss of all power from the electrical grid to the plant. In a PSA/PRA, loss of offsite power (LOOP) is referred to as both an initiating event and an accident sequence class. As an initiating event, LOOP to the plant can be a result of a weather-related fault, a grid-centred fault, or a plant- centred fault. During an accident sequence, LOOP can be a random failure. Generally, LOOP is considered to be a transient initiating event.
Postulated Initiating Event (PIE)	An *event* identified during *design* as capable of leading to *anticipated operational occurrences* or *accident conditions*. • The primary causes of *postulated initiating events* may be credible equipment *failures* and *operator* errors (both within and external to the *facility*) or human induced or natural *events*.
Structures, Systems And Components (SSCs)	A general term encompassing all of the elements (items) of a *facility* or *activity* which contribute to *protection and safety*, except *human factors*. • ***Structures*** are the passive elements: buildings, vessels, shielding, etc. • A ***system*** comprises several *components*, assembled in such a way as to perform a specific (active) function. • A ***component*** is a discrete element of a *system*. Examples of components are

	wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves.
Severe accident	A type of accident that may challenge safety systems at a level much higher than expected.
Screening	A process that distinguishes items that should be included or excluded from an analysis based on defined criteria.
Screening criteria	The values and conditions used to determine whether an item is a negligible contributor to the probability of an accident sequence or its consequences.
Sensitivity Analysis	A quantitative examination of how the behaviour of a *system* varies with change, usually in the values of the governing parameters. A common approach is parameter variation, in which the variation of results is investigated for changes in the value of one or more input parameters within a reasonable range around selected reference or mean values, and perturbation *analysis*, in which the variations of results with respect to changes in the values of all the input
Uncertainty	A representation of the confidence in the state of knowledge about the parameter values and models used in constructing the PRA. OR Variability in an estimate because of the randomness of the data or the lack of knowledge.
Uncertainty Analysis	An *analysis* to estimate the uncertainties and error bounds of the quantities involved in, and the results from, the solution of a problem.

1 INTRODUCTION

1.1 BACKGROUND

An *extended PSA* (probabilistic safety assessment) applies to a site of one or multi-units Nuclear Power Plant(s) (NPP(s)) and its environment. It intends to calculate the risk induced by the main sources of radioactivity (reactor core and spent fuel storages, other sources) on the site, taking into account all operating states for each main source and all possible relevant accident initiating events (both internal and external), including possible combination of them, affecting one NPP or the whole site [1].

A strategic reasoning regarding the topics on external hazards that can be examined within the ASAMPSA_E project has been applied to focus the activities where technical exchanges on identification of best practices will be the most useful.

During the ASAMPSA_E End-Users workshop held in Uppsala [1], 10 important external hazards were identified as the minimum required to be addressed by the project. These hazards are the following: Earthquake, External Flooding, Extreme air temperatures, Snow packs, Lightning, Storm, Strong wind, Biological infestation, Aircraft crash, External fire and External explosion. Consequently, it has been decided to focus on those external hazards for developing guidance and that different reports would be prepared according to the hazards considered.

This report proposes guidance on man-made hazards (mostly external fires and external explosions, occasionally release of toxic substances and related hazard) and aircraft crash. It includes:

- the characterization of the hazards and the modelling of the corresponding initiating events (work package WP21 of ASAMPSA_E),
- the implementation of the hazards in the L1 PSA (SSC modelling, Human Reliability Assessment (HRA), the site impact modelling covering emergency response and multi-unit response,
- the correlated events modelling.

1.2 STARTING CONSIDERATIONS

All sites could be exposed to aviation accident hazards to some extent; plants near airports face a higher exposure rate to aviation hazards due to the higher aircraft traffic density, and the higher accident rates for aircraft taking off and landing. Civil aviation could pose a significant hazard and be worth to be considered. However, private aircraft have less potential to occur and to lead to severe consequences given their traffic density, their size, and their speed. Military aviation is a concern if the plant is situated near an operating military airbase or a training area. Agricultural aviation also can be eventually considered in some cases, when such aircrafts are used in the vicinity of the plant. Usually the likely impact of eventual aircraft strike is one of the parameters taking into account in design of the plant, in particular the containment, but this does not exclude the need this hazard to be a subject of the extended PSA.

An explosion is defined as a rapid and abrupt energy release, which produces a pressure wave and/or shock wave. It can take the form of a deflagration (flame speeds are relatively low) or a detonation (extremely rapid and sharp compression occurring in a shock wave). The duration of the event is very short, differing from some others hazard durations, which may be much longer (hours). The intensity of the pressures acting on a targeted building can be several orders of magnitude greater than other hazards, but the explosive pressures decay extremely rapidly with distance from the source.

External fire can be more or less frequent depending on the area where the nuclear plant is located (nature and combustible load of the surroundings). The impact on the plant will largely depend on the materials used for the confinement and the buildings.

The sources for man-made hazards under consideration (external fire and external explosion) could be divided into stationary and mobile, as follows:

- Stationary sources in the vicinity of the plant under consideration such as oil refineries, chemical plant, mines, forests, storage facility, other nuclear facilities, high energy rotating equipment, military facilities, and pipelines (gas and oil);
- Mobile sources such as railway trains, road vehicles, ships, and aircraft (civil, military, and agricultural, if needed).

Each external hazard may result in a combination of various impact factors (external or internal) that have to be considered, because they may be great enough to affect the plant and to result in core damage and release of radioactive materials to the environment. For example, an aircraft crash may cause direct damage by the impact, or indirect via explosion, fire and vibration. Transportation or pipeline accidents in or near a nuclear power plant can result in the release of toxic chemicals, or burning/detonation of flammable or explosive materials, and may produce also missiles that can affect different parts of the plant. Additionally, vehicles with or without hazardous materials may collide with nuclear plant structures, resulting in damage to equipment.

For a collision, the key parameter should be related to the impact; in the case of an aircraft colliding with a structure, the main parameters will be mass and velocity of the impacting object. If an explosion is induced after the direct impact, the key parameters should involve some combination of the amount of fuel and the other aircraft combustible loads (seats, cables, luggage…) and the mass of heavy engines that could damage a structure. In case of aircraft crash, we have to consider the effects on the plant of the projectiles; fire; explosion of fuel tanks and the other aircraft combustible loads.

For many transportation related hazards, the actual danger is explosion or release of a dangerous material, and the key parameter should be the amount of material being carried or the maximum amount that could be released in an accident. For hazards such as pipeline accidents, the inventory of materials that could be released and the nature and pressure of the materials should be the appropriate parameters for characterization (in some cases also toxicity could be considered). In case of an explosion one has to consider the effects on the plant of the explosion pressure wave (deflagration, detonation); projectiles; smoke, toxicity, gas and dust; associated flames and fires. For explosions, a safe distance (explosion would yield a pressure less than a critical one) can be calculated [2].

The fire analysis should take into account the side effects of external fires like impact on external grid, habitability of control room, induced internal fires, impact of smoke on equipment and human performance, impact of heat on equipment close to walls in adjacent compartments, etc.

External hazards have a potential for affecting many different parts/pieces of equipment simultaneously. The analysis needs to consider both externally induced failures as well as unrelated failures caused by internal plant faults. Some external hazards could compromise the containment, safety and accident mitigation systems and/or their supporting systems, and/or can cause significant off-site damage and therefore the emergency response personnel may not be available and the communications, evacuation and sheltering/concealment may be affected. Consequently, the impact of external events on the results of a Level 2 and a Level 3 PSA may be more significant than on those of a Level 1 PSA.

Another important issue is the treatment of human actions in case of external hazard occurrence, due to the fact that the stress levels, conditions and type of the impact in the plant may differ considerably from the ones after an internal initiating event. Modelling the external hazards in multi-unit context is also a challenging topic, so as the consideration of combination of hazards. Reasonable assumptions should be made on the probability of simultaneous occurrence of hazards or its transfer between the units. Also, there may be a need to consider combinations of more frequent / less extreme event, which may be not relevant as single event, but which might need to be considered for combined events.

1.3 STRUCTURE OF THE REPORT

The first chapters (Chapters 1 to 5) of this document are dealing with the characterization of the man-made hazards (chapter 3 for single events and chapter 4 for hazard combinations) and the methodologies for their assessment.

The second part (from Chapter 6) of the report deals with the introduction of relevant external hazards in an existing (internal events) L1 PSA. Chapter 6 presents the general structure of man-made hazards PSA. The developed solutions for modelling man-made hazards are covering the modelling of external fire, explosions and aircraft crash in L1 PSA (chapter 7), the modelling of SSC (chapter 8), the modelling of human errors for these particular hazards (chapter 9), the modelling of additional emergency response (including mobile equipment, special provisions and help from outside the plant in chapter 10) and the modelling of multi-unit PSA (chapter 11).

The quantification aspects are covered in chapter 12 Conclusion and recommendations of the document are presented in chapter 13, along with a list of open issues presented in chapter 14. The last chapter includes a list of references to the document chapters. In Appendix 1 interface Level1 – Level 2 is described. Appendix 2 contains general principles of the French and Swedish approaches to characterize and assess man-made hazards. It includes also an example of the used methodology. Appendix 3 contains a description of various methods for calculating frequencies of aircraft crashes. In Appendix 4 additional material on emergency response related to aircraft crash hazard is included. In Appendix 5 an example of PSA tool for hazard assessment is presented.

2 DATA FOR HAZARD CHARACTERISATION

The data necessary for appraisal and evaluation of hazards resulting from human activities discussed in this report can be divided into two groups:

- data related to hazard sources;
- data related to plant design.

Additionally data related to site specifics and its vicinity should be taken into account.

2.1 DATA RELATED TO HAZARD SOURCES

In general, the sources may be stationary (located around or near the plant site), or mobile (moving in vicinity of the plant). This data is always considered to be site-specific.

The stationary sources represent mainly industrial and storage facilities, in which combustible or explosive substances are produced or stored. The mobile sources represent mainly transport of such substances. Within the hazards resulting from the mobile sources air transport is considered separately due to its specifics and possible direct physical contact of the aircraft with the plant or its part(s).

The data on stationary sources should include information on:

- structure of industry in vicinity of NPP site,
- distance of stationary industrial facilities from NPP site with emphasis on those, in which chemical, flammable or combustible materials are stored or transported via pipelines,
- types and amount of hazardous substances produced and stored in the facilities or transported via pipelines,
- information on storage, manipulations and internal safety measures adopted in these facilities in relation to the hazards resulting from their operation,
- meteorological and hydrological data.

It should be mentioned that, if available, safety reports of chemical installations can be used as a basic source of the information needed. The safety reports typically contain data on frequency and possible consequences of the accidents in stationary installations, which can be relevant for surrounding region. They can also contain data from the simulations of the development of major accidents.

The data on mobile sources should include information on:

- structure of transport lines (roads, railways, water roads, product lines[1)], piping) in vicinity of NPP site,
- distances of the transport lines from NPP site,
- type and amount of transported hazardous substances,
- data on technical means used for transport of hazardous substances,
- frequency of the transports,
- conditions of roads, repairs, restrictions.

[1] Product lines are usually classified as mobile sources due to transport of substances.

As a part of this data, also the national legislative measures related to hazardous materials (requirements for storage and transport of such substances) may be considered.

The above mentioned data are intended to be used mainly for appraisal of hazards related to external fires and explosions. Among the fires there is also a special category of "forest fires" for which also data on surrounding vegetation and landscape are required.

The data base on air traffic should include information on:

- nearby airfields or airports (civil, military) and their distances from NPP site; data related to the type (unpaved or hard surfaced) and orientation of airways,
- number of airport operations (take-offs, landings) related to the airports,
- airways around and across the NPP site; data on transit civil transport flights within airways (statistics on number of flights in these corridors, types of aircraft operated within area of interest, etc.),
- other aviation activities within region of interest (military bases or training areas, agriculture, sport and special purpose flights).

The above mentioned data are intended to be used in the analysis of the aircraft crash hazard.

2.2 DATA RELATED TO PLANT DESIGN

To be able to evaluate real effects of the external events to NPP, data on NPP design are needed. This data represents a group of data covering both plant specific and generic data.

The main sources of plant specific data are:

- plant design technical documentation,
- plant specific analyses (elaborated for SAR, PSA studies, etc.), and
- plant historical data from operational experience.

The main sources of generic data are:

- generic data from or for plants of the same or similar design,
- internationally accepted databases (IAEA, OECD, NRC) especially as a source of frequencies and screening values,
- knowledge and results from analyses of real external events similar to those under consideration for specific plant, and
- data from available calculation/simulation studies.

The above mentioned data are intended to be applied in analysis of potential effects of external events on the NPP.

As far as numerical simulation data are considered, the following can be useful (mostly for fires and toxic releases):

- meteorological data from the numerical weather forecasts made in the past. This can be particularly useful if re-analysis data and/or the results from weather forecast systems are available, as they can improve statistics.

- meteorological data from the simulations of climatic models, as they provide projection of the development of weather conditions in the period of the future operation of NPP.
- data on fires in previous periods and optionally data from the simulations of fires and explosions in the vicinity of NPP; this may be relevant if advanced calculations are used to produce such data (for example using models of the class of computational fluid dynamics), as otherwise simple models can be applied,
- optionally data on simulations for similar facilities as the ones located in the vicinity of NPP.

An important issue is data completeness and quality assessment. This pertains to the following problems:

- identification of the methods for assessing key input parameters: this can be done mostly by detailed analysis of the consequences of the external events related to man-made hazards and the response of NPP to such events; in principle, a full risk analysis (like QRA – Quantitative Risk Assessment) for the external event could provide good initial data for the response analysis; however this can be hardly done, therefore, the analysis of the major or enveloping accidents outside the NPP, should be performed at least,
- assessing data completeness via statistical methods and/or expert judgement: in a number of cases there are mathematical rules when and how to apply statistical methods. However, in the considered case, typical situation is the lack of data, then missing or censoring techniques can be applied, but in any case this should be supported by expert judgement,
- accuracy or uncertainty of the measurement and numerical simulation data: in most cases observations or simulated numerical data should include information on their accuracy; if not, they should be treated carefully and additional analysis of their uncertainty could be performed.

It should be added that the last two items mentioned above, are far beyond what is normally used in Hazards PSA, hence it is an open question to what extend this is needed and feasible.

3 HAZARD ASSESSMENT METHODOLOGIES

3.1 INTRODUCTION

3.1.1 EXTERNAL FIRE AND EXPLOSION

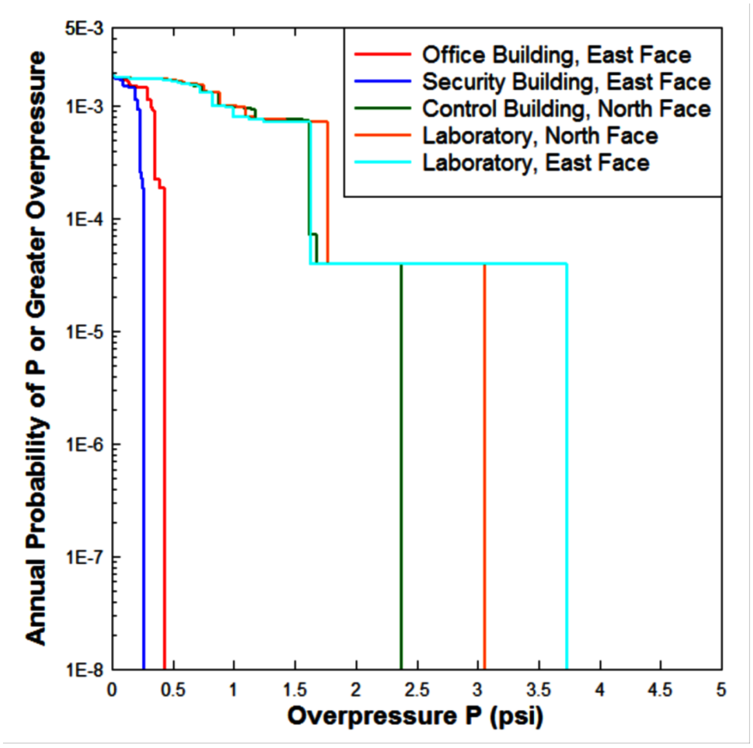
In order to implement man-made and accident aircraft hazards as external events in PSA studies, the following steps should be performed:

1. For man-made hazards like fires, explosions and releases of toxic substances a kind of risk assessment should be performed (like QRA). The input parameters are related to the frequency of the event, while the output contains the result of the consequence analysis, typically in the form of the frequency (or probability) of the occurrence of different consequences for each event. In the first phase of this analysis, screening is performed in order to eliminate events or sources, which are not relevant for the considered plant, for example, due to the distance or the very low probability (events with very low probability but with potential very strong impact on the plant have to be considered and assessed separately). In fact screening criteria are usually based on these two factors. In the second phase, detailed evaluation should be made for the events that are not screened out. ASAMPSA_E Deliverable D30.3 "Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA" [3] describes the basic methodology to be applied for the screening process.
2. The consequences of man-made hazards should be transformed into initiating events of the NPP (or in some cases common conditioning events incorporated in the model structure on higher level), for example, by fragility curves, which represent the probability of exceeding a given damage state as a function of an engineering demand parameter. This step corresponds to the analysis of vulnerability of the plant to the external events.
3. These initiating events are further evaluated in PSA model for a given NPP.

Methodologies for the assessment of man-made hazards have to take into account a number of various factors and usually utilize different approaches and methods in order to make full image of the real processes. In general, man-made hazards are related to the physical properties of the material and these properties determine the inherent risk and the potential consequences in case of accident with the release of dangerous substances. Various processes have to be taken into consideration and various characteristics of the material should be examined, like: flammability, combustibility, toxicity, corrosiveness, reactivity, explosiveness, radioactivity, etc. In case of transportation different initiating events have to be considered, like the situations where there are immediate fires, explosions (or the releases of toxic substance) or conditions for such events have happened with probability that cannot be negligible. This depends on the type of transportation; in general one can identify the ones shown in Table 3-1, below.

IAEA Safety Guide NS-G-3.1 provides general guidance on the assessment of the external explosion hazard. The explosion hazard can come from stationary or mobile sources. The IAEA safety guide could be applied to external fire hazards as well. The final result of the explosion hazard assessment is a list of potential explosion sources, including the amount and nature of the explosive substance, the distance to the site and the annual frequency of explosion for each source. From these values, probabilistic analysis procedures can be used for calculating the frequency of exceeding different levels of overpressure at the NPP structures from accidents in stationary or mobile sources [4]. Overpressure values are the basic input for the structural capacity assessments. Figure 3-1 shows an example of overpressure hazard curves.

Figure 3-1: Overpressure hazard curves for buildings in a sample facility [5]



In general, as potential sources of fires and explosions one should consider: industrial facilities, pipelines, transportation and aircraft crash. In case of fires, vegetation can be also included because forest fires are often caused by human.

Table 3-1: Accident initiated events for transportation of dangerous goods (based on [6])

Road	Rail	Waterway	Air	Pipeline
Car-car obstacle Collision Overturning Level Crossing Cargo Shifting Fire (engine/brakes) Loss of containment (tank/container failure)	Train-train obstacle Collision Fire (axel boxes, brakes) Derailment Level Crossing Loss of containment (tank/container failure)	Ship-ship Collision*) Grounding Capsizing Allision*) Fire	Crash Cargo Shifting	External Impact Failure due to corrosion, static electricity in broken /missing protection

*) "Allision" is used to mean the striking of a stationary object, while "collision" is used to mean the striking of a moving object ([6]).

3.1.2 AIRCRAFT CRASH

A number of guidance documents, standards as well as technical publications exist on hazard assessment methodology for aircraft crash. In general, the main analysis steps to quantify the crash rates can be considered identical in the different commonly applied methods, although there are some differences in the formulas and factors to be taken into account for quantification. The authors consider [7] and [8] as the most relevant ones with respect to site level hazard characterization. The aim of this chapter is to provide generic information, while the specificities of the state-of-the-art concerning site level hazard characterization of aircraft crash are included in the Appendix 3. The approach discussed there takes the widely used methodology of [7] and [8] as a basis and supplements it with other related documents as well as with additional considerations to ensure the applicability of the method in a PSA context.

The primary objective of site level hazard assessment for aircraft crash is to determine aircraft crash frequencies for different aircraft categories. This should be based on a statistical evaluation of accidents and air traffic information and on data applicable to the vicinity of a specific site. The results should be presented in accident frequencies specific to a unit ground area (event/year/unit area). If the evaluation concludes that aircraft crash hazard cannot be screened out on a probabilistic basis, the aircraft crash potential effects on the nuclear facility located at the site have to be characterised.

3.2 HAZARD CATEGORIZATION

3.2.1 EXTERNAL FIRE AND EXPLOSION

In assessing the **external fire hazard,** distinction can be made between different types of fire. The main categories of the fire are:

I. Boiling Liquid Expanding Vapour Explosions (BLEVE): this is sudden rupture of a vessel containing liquefied flammable gas under pressure. The primary cause is usually an external flame impinging on the shell of a vessel above the liquid level, weakening the container and leading to sudden shell rupture. The pressure burst and the flashing of the liquid to vapour creates a pressure wave and potential missile damage. The immediate ignition of the expanding mixture of fuel and air leads to intense combustion and the creation of a fireball. The majority of BLEVEs have occurred during the transport of pressurized liquefied gases but a number have occurred at fixed installations. As BLEVE reduces the consequences of the fires to heat only, it can be treated as explosion. Specific cases of BLEVE are: external mechanical strike, transport collisions between vehicles loaded with vessels containing liquefied gases and other without subsequent fire.

II. Pool Fires: liquid is spilt onto a flat surface spreads out to form a pool. If the liquid is volatile, evaporation takes place and if the liquid is flammable then the atmosphere above the pool will be in the flammable range. If ignition takes place, then a fire will burn over the pool. The heat from this fire will vaporize more liquid and air will be drawn in from the sides of the pool to support combustion. The system will then consist of a solid cylinder of flame burning above the pool.

III. Flash Fires: this occurs when a cloud of a mixture of flammable gas and air is ignited. The shape of the fire closely resembles the shape of the flammable cloud prior to ignition but it also depends upon where within the cloud ignition occurred. In many cases the cloud extends back to the original point of release and can then give rise to a torch or pool fire depending on the mode of release. When ignition occurs, the flame front races or 'flashes' through the cloud very quickly. It is also possible that the flame may accelerate to a sufficiently high velocity for an explosion to occur.

IV. Jet or Torch Fires: it usually occurs when a high pressure release from a relatively small opening (ruptured pipe, pressure relief valve, etc.) ignites. This gives rise to a torch which can burn with flame lengths several meters long. The flame is a hazard to persons nearby but the main hazard is generally its effect on adjacent vessels which may contain flammable liquids, or effects on adjacent facilities/equipment from flammable materials.

The main risk for all categories comes from thermal radiation effects, but it can be combined with pressure waves and missiles.

The **explosion hazard** can be classified as follows:

- industrial explosion;
- military explosion;
- transportation explosion;
- pipeline explosion.

While military explosions are related to missiles or projectiles, transportation or industry-type of explosions can be categorised as: dense-phase explosions, confined, partially confined or unconfined vapour cloud explosions, boiling liquid expanding vapour explosions (BLEVE) or dust explosions.

A dense-phase explosion occurs when a liquid or solid is suddenly converted to a gaseous form. The rapid increase in volume results in a pressure wave which radiates from the source at a velocity greater than the speed of sound in air. The requirement for vapour cloud explosion is a large pre-mixed cloud of flammable vapour and air within the flammable range and the presence of some confinement or obstructions.

A BLEVE described shortly above is an example of a combined fire and explosion hazard.

A Dust explosion is a hazard whenever combustible solids of small particle size are handled.

Probably the most precise categorization of fires and explosions could be based simply on the substance, but from practical point of view it is better to combine them based on the underlying physical processes as these determine the consequences that are relevant for the PSA study for NPP. This is the basic idea for the categories of fires and explosions shown above.

3.2.2 AIRCRAFT CRASH

As the first step of aircraft crash hazard assessment, it is necessary to classify all aircrafts relevant to the airfields of the region in the vicinity of the site into different categories. In general, country-specific data is taken into consideration to identify all aircraft types that should be covered in the assessment. The categorization should be based on the differences in flying characteristics, reliability as well as the damage potential on structures. The damage potential of an aircraft is influenced by many physical characteristics thereof, although in practise, the commonly applied approaches take only mass and velocity into consideration for categorization.

One example of aircraft categorization applicable to hazard assessment (based on [7]) is:

- drones, remote controlled ultra-light aircraft, sailplanes, gliders and aircrafts carrying negligible amount of fuel (e.g. gliders with engines),
- light civil aircraft - fixed wing civil and military aircrafts having a maximum take-off mass authorized less than 2.3 tons (agricultural aircraft can be assigned to this category),

- helicopters – all civil and military helicopters,
- small transport aircraft – fixed wing civil and military aircrafts having a maximum take-off mass authorized between 2.3 to 20 tons,
- large transport aircraft – fixed wing aircrafts not covered in any other categories,
- military combat and jet trainers – all military fixed wing aircraft with a maximum take-off mass authorized up to 50 tons and capable of acrobatic style flying.

In contrast, the Swiss Federal Nuclear Safety Inspectorate (ENSI) defines the following categories that shall be analysed [9]:

- commercial aircraft (maximum take-off mass > 5.7 tons),
- military aircraft,
- light aircraft (maximum take-off mass < 5.7 tons).

The same approach is also applied in France.

The magnitude of the hazard depends and thus the impact on the plant depends on the size of the aircraft in the possible impact scenarios. However a continuous variation of size does not occur in practice, since size depends on the categories of aircraft in operation. Table 3-2 defines four categories of civil aircraft and a single category of military aircraft [4]. Velocity ranges correspond to generally accepted limits for low level flying close to an industrial facility [10]. At present, there is no international standard giving aircraft impact velocity values for assessment of beyond design conditions.

Table 3-2: Aircraft categories for capacity assessment [10]

Category	**Maximum Take-Off Weight MTOW (kg)**	**Velocity range (m/s)**	**Examples**
A	< 20000	70 - 160	**General aviation planes** Cessna 210, LearJet 23, Canadair WaterBomber
B	< 100000	70 - 160	**Light weight passenger planes** Boeing 720, Boeing 737, Airbus A320
Ct	< 200000	70 - 160	**Medium weight passenger planes** Boeing 767, Airbus A300
D	> 200000	70 - 160	**Heavy weight passenger aircraft** Boeing 747, Airbus A340, Airbus A380
Military fighters	< 35000	< 220	Eurofighter, Rafale, Phantom

Subsequently, for structural response evaluation, one (or more) representative(s) or surrogate aircraft design is assigned to each category reflecting all damage potential characteristics relevant to the category. The following aircraft and flight parameters may influence the structural response:

- aircraft mass,
- impact velocity distribution,
- descent angle (alternatively, a conservative value may also be sufficient),
- mass and cross-sectional area of potential missiles,
- mass distribution along the aircraft, location of rigid parts like engines,
- type, mass and location of fuel,
- type and amount of fuel and other combustible loads (seats, cables, luggage…).

These parameters have also some impact on fires and explosions response evaluation, in particular the latter one.

3.3 FREQUENCY ASSESSMENT METHODOLOGY

3.3.1 EXTERNAL FIRE AND EXPLOSION

The frequency of human-made hazards which can be considered as initiating events for PSA analysis is not straightforwardly calculated. In principle the following steps should be undertaken:

- estimation of the frequency of external fires and explosions that can have impact on NPP;
- analysis of the consequences of these fires and explosions.

These steps correspond to QRA methodology for chemical hazards (which is an analogy of a PSA study with all three levels). Hence the frequencies can be formally calculated as follows:

$$F_{i,j} = \sum_k N_i \cdot P_{i,k} \cdot f_{i,j,k}$$

where:

$F_{i,j}$ annual frequency specific to each category of fire and explosion (i) leading to consequences (j), that can be dangerous for NPP [event/year],

N_i annual number of the transportation of hazardous substances related to category (i); in case of stationary installations rather a number of major accidents should be taken [event/year],

$P_{i,k}$ probability per transportation that an accident of type (k) happens (or conditions that such hazard can appear) in the vicinity of the site for category (i); in case of stationary installation this should be probability per major accident (k) in this installation that this leads to the category of hazard (i) at NPP site,

$f_{i,j,k}$ conditional probability that for given category (i) an accident of type (k) leads to consequences (j).

The main problem is the estimation of $p_{i,k}$ and $f_{i,j,k}$. For the latter one a deterministic approach can be the only reasonable to use (which means probability equal 1 is assumed), like the situation when the concentrations of the substance is within flammability limits (then fire is assumed with probability 1). In some cases probit functions (i.e. quantile functions associated with standard normal distribution) can be used in the consequence analysis, but their application is rather limited because validated formulas are available for not many substances. Another possibility is to apply deterministic models for consequence analysis of fires and explosions in the statistical way by the variation of key parameters (simulations of Monte Carlo type), and this finally can produce requested probabilities. Estimation of $p_{i,k}$ can be based on the data from databases on transportation accidents.

The frequency of the events (N_i) can be estimated basing on the archive data and current activities. For the transportation, it should be mentioned that there are various regulations applying for the safe and secured transportation of hazardous materials. In Europe, the following regulations are obligatory:

- ADR (Accord européen sur le transport des marchandises Dangereuses par Route) for Road Transport) — The European Agreement concerning the International Carriage of Dangerous Goods by Road;
- RID (Règlement International concernant le transport des marchandises Dangereuses par chemin de fer) for Rail Transport — International Regulations concerning the Transport of Dangerous Goods by Rail;
- The European Agreement Concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN).

Data concerning both actual events and near-misses (i.e. events that could have happened with high probability) should be taken into account, as this can improve understanding of the development of accident scenarios and provide a wider spectrum of possible events which should be analysed. It should be added, however, that availability of such information (in particular on near-misses events) can be weak. For accident initiating events, among the variety of causes or factors having essential impact on the development of the accident scenarios, one can mention the following ones: equipment failures, road or rail defects, human factors, control system failures, navigational errors, improper balancing or ballasting and external events. In case of non-accident type of initiating events, the most typical elements that should be considered are: incorrect securement, corrosion or metallurgical failure, over- or under-filling, overpressure, component failures (valves, rupture disk, etc.), activation of relief devices, control system failures and contamination.

It should be added that the simplest and most often used approach is to use accident frequencies and data of random failures of equipment for non-accident situations.

According to the combustion mode, an explosion can take the form of a deflagration, which generates moderate pressures, heat or fire, or a detonation, which generates very high near field pressures and associated drag loading: usually thermal effects are present only in the case of special fuel–air mixtures. Whether or not the ignition of a particular chemical vapour or gas behaves as a deflagration or detonation in air depends primarily on the concentration of the chemical vapour or gas present. At concentrations two to three times the deflagration limit, detonation can occur. A possibility of direct and delayed ignition should be considered. In case of delayed ignition a gas cloud can for instance enter the ventilation system and explode inside the NPP buildings.

For identification of initiating events induced by explosions, the following methods could be used:

- analysis of operating experience involving functional degradation or unavailability of systems due to external events (such data are usually limited);
- analysis of possible consequences and failures caused by occurrence of the external event.

The estimation of the frequency of external events is more or less related to the observation of phenomena occurrences, but this could be difficult, since the explosions are quite rare phenomena. The frequencies estimates can be based on analysis of local and worldwide industrial statistics, but in case of extremely scarce data for these events, the frequency and distributions are usually estimated by expert opinion, taking into account insights gained from analysis and operating experiences. The consequence distribution of external explosion pressure waves can be successfully assessed by means of the Monte Carlo simulation. On the other hand, Dutch QRA guidelines provide frequencies, conditional probabilities for a number of accidents and scenarios, including direct and delayed explosions and fires.

3.3.2 AIRCRAFT CRASH

For each aviation category, the following three aircraft crash quantities based on flight phase should be determined and then summed up to quantify the overall aircraft crash frequency:

- background crash rate (caused by free air traffic);
- airport related crash rate (caused by take-off and landing);
- airway related crash rate (caused by route and waiting loop traffic).

Eventually one also considers intentional crash rates (for example caused by hijacker or pilot). Other cases are technical failures of aircraft and forced change of route and/or emergency landing. The scope of this report is limited to accidental aircraft crash.

The standard on accident analysis for aircraft crash into hazardous facilities [8] developed by the U. S. Department of Energy proposes the quantification of all the three types of flight phase based crash rates defined above by using one general formula. After minor modifications, the following formula can be applied to determine the aircraft crash frequency that is appropriate for use in PSA:

$$F_{i,j} = \sum_{k} N_{i,j,k} \cdot P_{i,j,k} \cdot f_{i,j,k}(x,y)$$

where:

$F_{i,j}$ annual aircraft crash frequency specific to a unit ground area for each aircraft category (j) and flight phase based crash rate type (i) [event/year/unit area];

$N_{i,j,k}$ annual number of site-specific aircraft operations (i.e., take-offs, landings and in-flights) for each applicable parameter (i.e. aircraft category (j), flight phase based crash rate type (i), flight sources as runways, non-airport operations, etc. (k)) [event/year];

$P_{i,j,k}$ aircraft crash probability per operation in the vicinity of the site for each applicable parameter (i.e. i, j, k, as discussed above) [-];

$f_{i,j,k}(x,y)$ aircraft crash location conditional probability (per unit ground area) given a crash evaluated at the facility location for each applicable parameter (i.e. i,j,k, as discussed above) [1/unit area].

Because of the limited number of historical in-flight crashes, particularly for commercial and large military aircraft, frequency calculations for non-airport operations are based on modelling directly the number of crashes per unit ground area per year, i.e., the product $N_{i,k}*P_{i,k}*f_{i,k}(x,y)$.The document [8] defines a detailed quantification method to assess $f_{i,j,k}(x,y)$ in the vicinity of airports as well as a table for the product of $N_{i,k}*P_{i,k}*f_{i,k}(x,y)$ for non-airport operations relevant to different areas in the United States. However, this enables a simple application of the approach in the United States; it does not include a methodology to quantify uncertainty. Although the above methodology is widely used in the U.S. and in some other countries (e.g. Switzerland), an alternative method is presented in Appendix 3, that provides empirical formulas to assess the different types of flight phase based crash rates. It also addresses, to some extent, uncertainties using a traditional approach based on frequencies.

In order to enable plant risk quantification characterization of impact for each aircraft category to the extent of the parameters described in chapter 3.2.2 should be included for aircraft categorization, calculation of aircraft crash frequency thereof, as well as trend analysis and hazard assessment.

3.4 CONSEQUENCE ANALYSIS

An important step of the hazard definition is the consequence analysis. The size of exposed area, is the first parameter that has to be estimated, and such estimation depends on the following factors: physical-chemical properties of the hazardous material and its volume, design and characteristics of the container, pressure and temperature of the substance, conditions during accident and release mechanism and ambient meteorological conditions (wind direction and strength, temperature, humidity). Various scenarios should be analysed, depending on the dangerous material – the most important ones are: fire, BLEVE (Boiling liquid expanding vapour explosion), VCE (Vapour cloud explosion), explosions, flammable vapour cloud, asphyxiating cloud, chemical, biological or radioactive contamination. Event tree methodology can be applied to characterize the events leading to the accident, and finally to determine probabilities of the releases resulting in potentially high consequences. These consequences stand as the basis for further analysis for translating hazard into initiating event of NPP. Therefore consequence analysis of transportation accident has to be performed carefully taking into account all possible release mechanisms and scenario developments.

In case of fire and flammability hazards, the ignition of the material can lead to the formation of pool fire, flash fire or jet fire. This depends on the properties of the material and conditions during the release. In order to determine the impact of thermal radiation for objects and people, a number of parameters have to be known such as: quantity released; physical-chemical properties of the substance; flame surface; meteorological conditions and distance to exposed objects and possibility of sheltering/concealment.

The area of a pool fire depends on whether the spill is confined or not. In the first case, it is naturally limited, while in the second case it depends on the volume of the liquid and its burning rate. When pressurized material is released and ignited at once, typically a jet fire is formed. Instantaneous release with immediate ignition can lead to fireball, while delayed ignition of pressure flammable material leads to flash fire or explosion. The latter case is related to VCE (vapour cloud expansion), which is the effect of rapid combustion with flame speed close to the sonic velocity. In consequence a blast wave can be produced. The combustion energy and the energy of the ignition source are the parameters determining the potential explosion. The characteristic of the material is a deciding factor for calculating how big the fraction of combustion energy is converted to the explosive one. In order to produce blast overpressure the turbulence is required, otherwise the flame front will not be accelerated enough, and finally hazard will be limited to thermal radiation caused by a burning cloud. The turbulence is usually due to the interaction between the flame front and obstacles; hence the localization plays an important role. Thus, the effects depend on flame speed, location and the type of the material – in this respect it should be mentioned that highly reactive substances are more likely to lead to VCE than the ones having lower reactivity.

While the consequences of fire and explosion can be significant for objects, in case of the release of toxic substances, essentially people are exposed. Inhalation, skin or in-depth burn, blindness and also carcinogenic hazards are the main types, but the latter one can have negative effects only later in life. The most important are immediate incapacitating effects. In order to determine toxic dispersion zones the following parameters should be known:

- physical-chemical properties of the substance;
- quantity released;
- condition of the release: duration, elevation;
- surrounding terrain, topography, structure and building density, prerequisites for inversion;
- atmospheric conditions: wind direction and velocity, humidity (rain), temperature, stability of atmosphere; and
- limiting concentration: while defining receptors it is important to distinguish between concentration with serious effect and concentration with just observable effect.

As far as the meteorological data are considered, in the consequence analysis it is important to provide a series of calculations with different sets of parameters. Often a conservative approach is applied, for example, stable conditions of the atmosphere are used, resulting in an increased zone.

Chemical Process Quantitative Risk Analysis (CPQRA) is probably one of the most adequate methods that can be applied to risk analysis [11] [12]. Analogous methodology has been proposed by TNO [13], [14]. The Dutch guidelines based on these reports include a computer program, mandatory to use for all hazardous activities. Table 3-3 below contains the summary of CPQRA hazards, event sequences, incident outcomes, and consequences. It is related both to stationary and transportation accidents with dangerous chemicals.

Table 3-3: CPQRA hazards, event sequences, incident outcomes, and consequences [15]

Process hazards	Event Sequences			Incident outcomes
	Initiating events	Intermediate events		
Significant inventories of: Flammable materials Combustible materials Unstable materials Corrosive materials Asphyxiants Shock sensitive materials Highly reactive materials Toxic materials Inerting gases Combustible dusts Pyrophoric materials **Extreme physical conditions:** High temperatures Cryogenic temperatures High pressures Vacuum Pressure cycling Temperature cycling Vibration/liquid hammering	**Process upsets** Process deviations Pressure Temperature Flow rate Concentration Phase/state change Impurities Reaction rate/heat of reaction **Spontaneous reaction** Polymerization Runaway reaction Internal explosion Decomposition **Containment failures** Pipes, tanks, vessels, gaskets/seals **Equipment malfunctions** Pumps, valves, instruments, sensors, interlock failures **Loss of utilities** Electrical, nitrogen, water, refrigeration, air heat transfer, fluids, steam, ventilation **Management systems failure** **Human error** Design Construction Operations Maintenance Testing and inspection **External events** Extreme weather conditions Earthquakes Nearby accidents' impacts Vandalism/sabotage	**Propagating factors** Equipment failure safety system failure Ignition sources Furnaces, flares, incinerators Vehicles Electrical switches Static electricity Hot surfaces Cigarettes Management systems failure Human errors Omission Commission Fault diagnosis Decision-making Domino effects Other containment failures Other material release External conditions Meteorology Visibility	**Risk reduction factors** Control/operator responses Alarms Control system response Manual and automatic ESD Fire/gas detection system Safety system responses Relief valves Depressurization systems Isolation systems High reliability trips Back-up systems Mitigation system responses Dikes and drainage Flares Fire protection systems (active and passive) Explosion vents Toxic gas absorption Emergency plan responses Sirens/warnings Emergency procedures Personnel safety equipment Sheltering Escape and evacuation External events Early detection Early warning Specially designed structures Training Other management systems	**Analysis** Discharge Flash and evaporation Dispersion Neutral or positively buoyant gas Dense gas **Fires** Pool fires Jet fires BLEVES Flash fires **Explosions** Confined explosions Unconfined vapour cloud explosions (UVCE) Physical explosions (PV) Dust explosions Detonations Condensed phase detonations Missiles **Consequences** Effect analysis Toxic effects Thermal effects Overpressure effects Damage assessments Community Workforce Environment Company assets

The results of CPQRA are usually presented depending on applied risk measure (risk indices, individual risk or societal risk) in the form of risk contours, F-N curves or similar graphs (as this is a case of mandatory Dutch QRA program).

3.5 UNCERTAINTY ASSESSMENT

The treatment of uncertainty is another issue which should be taken into the consideration in the consequence analysis. According to [13], the sources of uncertainties can be classified with the three following levels:

- starting points — the choice between conservative and best estimate calculations leads to different types of models and different sets of parameter values and assumptions;
- parameter values — input data are the source of uncertainty, like impact from exposure to a hazardous material (toxicity, thermal radiation, blast overpressure), properties of the substance, accident data;
- models — uncertainties are related to the ability of the models to represent reality.

Dealing with uncertainties demands proper documentations of all inputs and assumptions, and performing sensitivity analysis to identify the impact of the parameter values on the results. It is also worth to mention that the estimates of risk should not be treated as exact values or as absolute measures, rather relative risk comparison ought to be considered. Prioritization of uncertainties and selection of the most important from them is need for minimization of the analysis and practical application of the suitable method for assessment.

As discussed in appendix 3, for aircraft crash hazards, the application of the Poisson process for quantifying the background crash rate enables the use of the x^2 (chi-squared) distribution to determine the estimated background crash rate at any given level of confidence. Moreover, [16] proposes an approach to uncertainty analysis for all crash rate types that cannot be justifiably derived by assuming a Poisson process. This approach requires the identification of the potentially significant (or all) contributors to the uncertainty of the results and the quantification thereof by subjective probability distributions. The selected distributions and parameter values express how well the value of uncertain parameter values of the model are known. It should be noted that the selection of the distributions and their parameters relies to a large extent upon expert judgement. The results of the quantitative uncertainty analysis can be expressed as quantiles (e.g. 5% and 95%) of the uncertainty distribution.

In practice the quantiles are estimated using the parameters of subjective probability distributions and Monte Carlo simulations. The simulations are performed for each sample set (all random parameters varied simultaneously). The reader can referred to references [16] and [17] for a detailed description of this uncertainty analysis approach.

3.6 FROM HAZARD TO INITIATING EVENT

3.6.1 EXTERNAL FIRES AND EXPLOSIONS

The analysis of initiating events for a PSA from External Fires and Explosions is strictly related to the type of their consequences, which can be evaluated by QRA-type techniques, already mentioned in chapter 3.4. It means that the following consequences should be considered as possible initiating events: pressure waves (explosions), heat (fire), projectiles (or missiles), releases of toxic substances- separately or in combination between them.

In the transformation process of risks related to fires and explosions into initiating events, fragility curves are the most popular representation as they reflect the vulnerability of the component, structure or system to the considered event. Formally one can define a fragility curve as the conditional frequency of failure of the component as function of the hazard characterization parameter (i.e. for a given value of the parameter). Sometimes the hazard characterization parameter is taken as the hazard intensity. The capacity of the component, derived from design criteria and test data, is expressed in terms of the hazard intensity. There are external events where the component fragility can be taken as 1.0. This is the case when the hazard intensity reaches a specific value. In case of accident sequences with more than one SSC involved, information on the correlation of responses and capacities between the components coupled with the fragilities of individual components can be used to calculate the conditional frequencies of such sequences. In some situations, the fragilities of individual components may not be meaningful; the conditional frequency of accident sequence can be calculated directly.

3.6.2 AIRCRAFT CRASH

In general, in a PSA for external events, the initiating events correspond to the occurrence of the external events themselves (e.g. earthquake, high wind) that may induce multiple transients at the plant. Most of these induced transients are usually initiating events considered in the internal events PSA.

An aircraft crash may have different primary and secondary impact areas depending on the location where the aircraft hits the plant. The primary impact area is the area where the aircraft hits the plant and the crash has direct impact on systems, structures and components (SSCs) located thereon. The secondary impact area is defined as an area where the aircraft has indirect impact on due to secondary effects. These secondary effects may include the following:

- secondary missiles (from the aircraft like engines, landing gear, etc., and projectiles from the impacted structures);
- fuel fire;
- explosion and shockwaves resulting from the crash;
- hazardous effects induced by an accident on a conventional non-nuclear industrial facility located on the site.

All those locations near or on the site that may be directly hit by an aircraft and have similar primary and secondary impact areas with respect to safety functions are grouped into an impact zone. Commonly, at least one impact zone is assigned to each safety related structure, group of outdoor systems and components. Aircraft crashes not having primary but only secondary effects on safety related SSCs are also taken into consideration in impact zone definitions. The aircraft crash frequency for each impact zone is determined by taking into account the effective area of the impact zone (including SSCs located in the impact zone) and the crash rate probability in the vicinity of the site. This is performed for all aircraft crash categories.

Reference [8] describes a methodology that is appropriate to assess the effective area of impact zones. A summary of the approach is presented hereby using the example of a stand-alone, single rectangular building. The effective area represents the ground surface area surrounding a building such that if an aircraft were to crash within the area, it would impact the building, either by direct fly-in or skid into the building. The effective area depends on the dimensions (e.g. length, width and height) of the building, as well as on the wingspan, flight path angle, heading angle relative to the heading of the building, and the skid length of the aircraft. The effective area is the union of the fly-in area and the skid area. The fly-in area represents the area corresponding to a direct fly-in impact and consists of two parts, the footprint area and the shadow area. The footprint area of a building is the area that an aircraft would hit even if the building height were zero. The shadow area is the building area that an aircraft hits, but which would be missed if the building height were zero.

For simplicity, the building is represented by a bounding rectangle, and the heading of the crashing aircraft with respect to the building is assumed to be perpendicular to the diagonal of the bounding rectangle hereby, as shown in Figure 3-2. These assumptions provide a conservative approximation to the true effective area. The formulas for calculating the skid and fly-in areas for an aircraft crashing into a rectangular building are as follows:

$$A_{eff} = A_f + A_s$$

with:

$$A_f = (WS + R) \cdot H \cdot \cot\theta + \frac{2 \cdot L \cdot W \cdot WS}{R} + L \cdot W$$

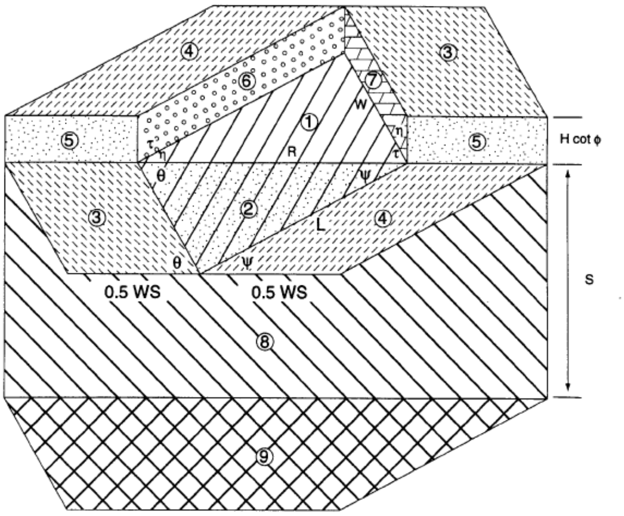
$$A_s = (WS + R) \cdot S$$

where:

A_f	effective fly-in area (m^2),
A_s	effective skid area (m^2),
WS	aircraft wingspan (m),
R	diagonal length of the building (m) (=$\sqrt{L^2 + W^2}$),
H	facility height (m),
cotθ	mean of the cotangent of the aircraft descent angle,
L	length of facility (m),
W	width of facility (m),
S	aircraft skid distance (mean value) (m).

These formulas have been obtained using the sub-regions shown on Figure 3-2 (details can be found in [18]).

Figure 3-2: Rectangular facility effective target area elements [18]



It is noted, that an extension to the aircraft crash hazard assessment methodology of Department of Energy (DOE) Standard 3014 [8] was developed in [18] to assess the effective area of an object of non-uniform construction or one that is shielded in certain directions by surrounding terrain or buildings. The extension is not proposed as a replacement to [8] but rather as an alternate method to cover situations that were not considered.

In summary, an aircraft crash initiating event is an aircraft crash that affects one impact zone by the hit of a certain aircraft type. Consequently, the characterization of initiating events in an aircraft crash PSA covers the description of aircraft crashes according to aircraft categories and the affected impact zone for each category as well as the calculation of crash frequency for each of these events. The impact characteristics of each aircraft category is also identified and assessed for characterizing the initiating events.

3.7 LIMITATIONS AND GAPS IN EXISTING METHODS

3.7.1 EXTERNAL FIRES AND EXPLOSIONS

Several issues should be mentioned here:

- in principle a full QRA study should be performed in order to estimate the frequency of initiating events for PSA; First of all, this can be a complex and time consuming task; secondly the uncertainty is propagated from the initiating events of the QRA, through physical and chemical phenomena descriptions, to the consequence analysis, which is also burdened with some uncertainties; this means that finally, the estimation of the frequency of initiating events for the PSA can be quite rough; therefore a deterministic approach can be as useful as the QRA, for example in the consequence analysis; hence an overestimation of the frequency of initiating events for a PSA can be expected;
- understanding of underlying physical processes for some types of fires and explosions (like vapour cloud evaporating expansion) still needs research; this is, of course, a main source of uncertainty;
- identification of the impact on SSCs of NPP must include not only combinations of different external hazards or combinations of external and internal hazards, but also take into account that some events in the plant can happen simultaneously and independently; this is taken into account by using the internal events model as a basis for the modelling of the external hazards.

3.7.2 AIRCRAFT CRASH

The methodology for assessing the aircraft crash hazard is reasonably well covered in state-of-the-art guidance documents, standards as well as technical publications. This step of the aircraft crash PSA is more mature than most of the other steps, such as plant response analysis, HRA (which in fact is still under development for extreme situations), etc. However, some specific analysis tasks need further developmental efforts in hazard assessment too, including the following in particular:

- the methodology for the assessment of impact mass and velocity distributions for each aircraft type is not complete at all points; appropriate input data with a description of distribution types and values of distribution parameters should be developed, and applicable data sources need to be identified and described in detail; also, the methods of determining correlation between mass and velocity should be presented in detail in updated guides; similarly, comprehensive international databases are needed on characterizing the impact parameters for each aircraft type to ensure adequate input data for hazard assessment.
- there is no definite consensus on how to practically model the secondary effects of an aircraft crash in PSA; available guides suggest an exhaustive listing of all possible secondary effects, however, guidance on applicable modelling assumptions are not given and detailed evaluation methods are not elaborated in detail either.
- the identification of potential impact zones is usually based on the similarities in primary impacts of different aircraft crashes; consequently, safety related buildings are usually considered impact zones; further developmental work is needed to give appropriate considerations to secondary effects in defining impact zones; moreover, the existing methodology should be refined to enable the identification of those impact zones that are hit by an aircraft having only secondary (hence no primary) effects on safety related SSCs; specifically for each representative aircraft or aviation categories the following tasks need to be done:

  - estimation of fire effects distances based on the amount of fuel and other combustibles loads (cable, seats, luggage, etc.) of aircraft;
  - estimation of fuel quantity penetrating into a building after an aircraft impact;
  - estimation of the effects distances of missiles based to statistical analysis of past accidents.
- state-of-the-art guidance documents do not propose any methodology on how to avoid the double counting of crashes when both the background crash rate and the airway related crash rates are assessed and summed up; this analysis area also needs further development.
- more detailed guidance is needed on how to perform trend analysis and qualitative evaluation of future changes.
- uncertainty issues mentioned in previous chapters.

4 HAZARDS COMBINATIONS

4.1 EXTERNAL EXPLOSIONS

4.1.1 EXPLOSION HAZARD CORRELATIONS

External man-made hazards are generally characterized by a relatively large number of cross-correlated phenomena. The correlations between hazards can lead to the following categories:

- *Causally connected hazards* where one hazard may cause another hazard; or where one hazard is a prerequisite for a correlated hazard;
- *Associated hazards* which are probable to occur at the same time due to a common root cause.

In case of explosion, the causality dependence can be divided into 2 categories:

- Causality dependence between explosion and external natural hazards;
- Causality dependence of explosions and other man-made hazards.

A correlation map for the external hazards was developed in D21.2 (List of external hazards to be considered in ASAMPSA_E) WP21 of the ASAMPSA_E project [19].The analysis of the map has led to the following remarks.

As already mentioned the combination of external fire and explosion hazards can be classified in the following categories:

- industrial fire/explosion;
- military fire/explosion;
- transportation fire/explosion;
- pipeline fire/explosion;
- forest fire;
- lightning fire/explosion or lightning/explosion without fire.

All the above categories of fires and explosions can be induced by the following hazards: vibratory ground motion; induced vibratory ground motion; fault capability; liquefaction; tsunami; slope instability; meteorite fall; volcanic hazard. Industrial and military explosions can be induced also by lightning, tornado, windblown debris and snow avalanche. Transportation explosions can be induced also by tornado and snow avalanche. Industrial explosion, transportation explosion and pipeline explosion may induce the occurrence of forest fire.

Regarding the dependence between explosions and other man-made hazards, the following aspects may be specified [19]:

- chemical (toxic) releases can be induced in case of explosions;
- ground transportation – direct impact may induce transportation and pipeline explosions;
- transportation explosions can induce industrial pipeline explosions;
- pipeline explosion can induce industrial explosions, and vice versa;
- military activities can induce transportation explosions, industrial and pipeline explosions.

4.1.2 COMBINATIONS OF EXPLOSION AND OTHER EXTERNAL HAZARDS

The external hazards combinations can threaten simultaneously (with buildings, facilities) diverse safety systems, and screening out external hazards without consideration of dependencies can lead to an underestimation of the associated risk. The international experience shows that the combinations of external hazards are considered only if the hazards are correlated [20]. In practice, the selected combinations of correlated external hazards are strongly dependent on local conditions.

The analysis of possible correlations (dependency) between events can be made by assessing the physical bases of the phenomena, observed data, actual events and general knowledge of local conditions. The identification of potential combined external events depends to some extent on engineering judgment, and there is no evident best method for performing the identification.

Correlated external events are modelled as combined events in an External Events PSA. For example, an explosion may damage the external power grid and can induce fires at the same time. This can be modelled as a combined event “loss of off-site power and fire”.

In any case, the initiating events should be identified by expert judgment taking into account insights gained from analysis and operating experience.

4.1.3 SCREENING OF EXPLOSIONS AND HAZARDS COMBINATIONS WITH EXPLOSIONS

A general approach of the screening process is described in D30.3 “Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA” [3]. The following methodology, consisting of the four major steps, has been proposed:

1. Comprehensive identification of events and hazards and their respective combinations applicable to the plant and site;
2. Initial frequency claims for events and hazards and their respective combinations applicable to the plant and the site;
3. Impact analysis and bounding assessment for all applicable events and scenarios. Events are either screened out from further more detailed analysis, or are assigned to a bounding event (group), or are retained for detailed analysis;
4. Probabilistic analysis of all retained (bounding) events at the appropriate level of detail.

In this chapter specific elements related to explosions are described.

An explosion should be screened out from further analysis; if at least, one of the following site related selection criteria is satisfied [21]:

- *Distance* - the potential explosion cannot occur close enough to the plant to affect it.
- *Inclusion* - the event is included into another (enveloping) event or is included in a combined event (it causes risk increase in connection with some other event).
- *Severity* - the effects of the event are not severe enough to damage the plant, since it has been designed for other loads with similar or higher strength.

Since the explosions are untimely and unexpected phenomena, the warning criterion (time available to impact) is not applicable for screening.

For combinations of hazards, in addition to the above, the following criteria for screening in might be used [21]:

- *Different plant safety functions affected*
  If two external events are dependent and one affects the offsite power while the other one affects the ultimate heat sink, this would be a relevant combination;
- *Degree of impact on plant safety functions*
  If two dependent external events affect the same safety function, they may still be a relevant combination, provided that their combined effect is greater that the effect from any of the single events involved. It should be noted that it is possible that two single hazards could be screened out on consequences, but their combination not. This means that for combinations, in principle, all non-screened list should be used. On the other hand random combinations can be almost always screened on frequency.

It should be mentioned that in the screening process the impact on the plant and the consequences of explosions should be assessed. This concerns the following aspects:

- collapse of structures or components, disruptions of systems or equipment due to pressure waves (characterized by the local overpressure at the plant as a function of time);
- penetration, perforation, spalling or collapse of structures or disruption of systems and components caused by projectiles; false signals in equipment induced by vibration;
- impaired habitability of control room, disruption of systems or components, ignition of combustibles caused by heat (characterized by maximum heat flux and duration);
- blockage of intake filters, impaired habitability of control room and other important plant areas due to smoke (characterized by concentration and quantity as a function of time).

The effects of explosions which are generally of concern when analysing structural response to the blast are:

- incident and reflected pressure;
- time dependence of overpressure and drag pressure;
- blast-generated missiles;
- blast-induced ground motion.

The relative importance of these effects depends mainly on the quantity and type of the explosive materials, the distance of the structure being considered from the source of the explosion, and the details of the geometry and spatial arrangements of the structures.

For the overpressure range less than 0.5 bars, overpressures exceed drag pressures by a sufficient amount so that drag pressures can generally be neglected (the expected low levels of drag pressures are generally accommodated by the usual design for wind loads). However, for the case of a wall vulnerable to negative pressure, or for elastic response of walls subjected to detonation of solid substances with TNT equivalents less than about 500 kg at distances less than about 50 m, the negative pressure may also be important [22] (see also [2] for application of TNT equivalent mass method for calculating minimum safe distance).

It is unlikely that any considerable number of large, hard blown objects will be thrown away for significant distances as a result of an explosion. If the plant has been designed to accommodate the effects of externally generated missiles resulting from other events such as hurricanes, tornadoes or aircraft crash, the effects of missiles generated by an explosion may already have been accounted for [22].

The intensity of blast-induced ground motion to be expected from above-ground detonations at overpressures less than 0.5 bar can generally be accommodated [22].

When calculating distances required for protection by means of separation, use can be made of the attenuation of peak overpressure as a function of distance from the explosion source. The data available for TNT can reasonably be used for other solid substances.

The adequacy of the protection afforded should be evaluated carefully when the location of the explosion can vary, as is the case in transport accidents. Since explosions of gas clouds can affect the entire plant area, the postulated gas cloud should be the most severe credible gas cloud relevant to the site. An analysis of the ability of plant structures to resist the effects of gas cloud explosion can normally be limited to an examination of their capacity to withstand the overpressure loading (primary effect). The pressure developed is a function of the energy release rate, as well as of the total energy release.

It should be noted that the overpressure-time history for a particular structure is heavily dependent on the layout of the surrounding buildings.

A recommendation from ASAMPSA_E report D30.2 [23] is to use appropriate L2 PSA risk measures for events screening. This recommendation targets the identification of low frequency events with potentially large consequences, as in the case of explosion and aircraft crash.

4.2 EXTERNAL FIRES

Fires are one of the most frequently occurring hazards and with heavy consequences risk events with technogenic character. For instance the annual frequency of all types of fires is 30-40x10^3 in Bulgaria [24]. The fire (particularly internal) hazard risk in nuclear power plants is extremely important because it may lead to a nuclear accident. Thus, the use of probability and deterministic approaches in the evaluation of fire hazard is important to manage potential fires and to ensure safety of NPPs. For example, as a good practice, both approaches are applied in Kozloduy NPP in Bulgaria for the analysis and the management of fire risk, with the evaluation of the qualification of the preventive and protective measures against fire and the quantification of the associated risk [25].

Of course fires are also extremely important for the safety of people in different aspects, including the toxic air pollutants impact on the human health. The assessment of safe time periods of people's stay in fire zones [26] is practically important and should be under consideration in an extended PSA.

Taking account already existing guidance on the implementation of External Hazards in extended L1 PSA, the fire hazard should be considered in the all three major types of hazard combination categories [27]:

- causally connected hazards – correlated hazards;
- associated hazards;

- combination of independent hazards (coincident hazards).

4.2.1 CAUSALLY CONNECTED FIRE HAZARDS – CORRELATED FIRE HAZARDS

As correlated fire hazards, the external fire hazard occurring close to the NPP site and inducing, in almost all cases, internal fires hazards in different parts of the plant site should be considered as well as loss of off-site power. Of course the different possible types of external fires have to be included:

- Forest fires;
- Industrial fires in neighbourhood plants to the NPP site;
- Transport fires in the roads located nearby to the NPP site, etc.;
- Possibly agriculture (stubble, bale of hay, feeds, etc.) fires.

These types of fire should be categorized depending on the source and cause of the fire as follows:

1. Fires without human intervention:
    - natural occurring fires – extremely high/sharp increased ambient temperatures, lightning;
    - technological reasons, accidents caused by failure of equipment, industrial accidents, failures of vehicles, fuel leaks, fuel spills, etc.
2. Fires with human intervention:
    - fires due to human negligence, low safety culture, lack of knowledge, failure to comply with rules and instructions, etc.
    - intentional fires - related sabotages, because of terrorist motives or other – these are in general not a part of a PSA.

All of these subcategories of external fire should be considered in the L1 PSA correlated with different internal fire(s) depending on their locations on the NPP' site. Even further, a matrix "External-Internal fire correlated hazards" could be defined at least for quality assessment of the correlated hazards, and maybe to quantify the probability of their occurrence.

There are a lot of examples in almost all European countries (but the data are not always available). The selected in Bulgaria 27 external fires (19 of which are human-induced external fires) - significant as hazards for different types of installations, have been registered by specialized institutions in the last 20 years. They occurred in regions distant from Kozloduy NPP and did not induce any internal fires on the plant site. But for an extended PSA, such cases of external fire should be considered by answering the following question - what would happen if they arise nearby, close to some NPP site? This is a concern for the safety of NPPs and potential external internal fire correlated hazards have to be considered probabilistically.

Apart from the above mentioned events, one can also consider some internal events arising as consequences of the "external and internal fire events". As they occur as consequences of fires, they are not treated as associated hazards but causally connected - they can last further simultaneously with fire. In this respect the following internal events could be listed:

- endangered buildings and constructions;
- damages to the main and auxiliary equipment;
- failure of interrupted power supply and/or water supply;
- interrupted communications and partial impaired technological control and management;

- hampered or impaired the possibility of applying SAM procedures where necessary;
- outbreak of hazardous gases;
- radioactive releases.

Some of the above mentioned internal events could have high impact on the safety of NPPs (degraded or lost functions of safety systems), for instance the failure of power supply and/or water supply in parts of the site. Also, for instance the outbreak of hazardous gases can be highly safety significant for the staff of the plant and perhaps for people outside of the plant.

4.2.2 ASSOCIATED FIRE HAZARDS

In this chapter, the associated external and internal fire hazards and internal events are discussed.

Events associated to external fire due to a common cause and occurring at the same time as the external fire, or due to the superposition of the consequences of events should be discussed.

An example of associated events that could be considered in an extended PSA is an external fire hazard (forest or industrial or other) due the impact of lightning combined with an induced overvoltage of the switchgear of the NPP also due to lightning.

Possibly the following events can be also considered:

- accidents and/or local fires as results of technological reasons or damaged equipment, for instance in the turbine hall, accumulator stations, charging systems and compartments, diesel-generator stations, cable corridors, channels and shafts, circulation pump stations, heavy oil and oil farms, chemical departments/workshops, nitrogen-oxygen stations, auto fleets of the NPP, etc.;
- accidents in heating, ventilation and air conditioning installations, departmental petrol and gas stations;
- local fires in warehouses due to improper storage of inflammable materials, welding, etc.

All of the listed internal events are considered as potential events in previous studies and analysis as EIA of the Kozloduy NPP [28] and L1 PSA for Units 5 and 6 of the NPP Kozloduy [29]. Also, the experience in other countries showed the necessity to have in-depth discussions on associated events with external and internal fire hazards in the extended PSA.

Finally one should mentioned combination of independent hazards (i.e. coincident hazards) – in most cases they can be screened out because of low frequency, but the potential cumulative impact should be careful considered.

4.2.3 SCREENING OF FIRE

A general approach to screening process is described in D30.3 Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA [3]. In this chapter the approach for fire hazards is described.

In principle this approach can be similar to the screening process used for explosions described in chapter 4.1.3. This means that fire can be screened out from further analysis basing on the criteria related to: distance, taking into account however, possibility of the spread of the fire caused by meteorological conditions, inclusion and severity. For combination of hazards additionally criteria are the same as for the explosions.

In the frame of extended PSA, external fire hazards might have a significant impact on the plant and have to be considered further if they are connected to other correlated or associated hazards, like internal fire, consequences of radiation heat (high temperatures), smoke effects, toxic effects, explosions (both external and internal) and their consequences. Thus the external fire can lead to a number of sequences with various events, where each event can have impact either on the same or different SSC, simultaneously or happening one after another. Hence various effects should be examined like loss of off-site power, for example due to the damage of external power grid caused either directly by external fire or as a fire consequence (for instance explosion) or all of them caused by lightning. Such situations can be often modelled as a combined event.

Therefore the screening process may be quite complex and a two-step approach can be used for screening (to some extent similar to the one used for internal fires):

1. Qualitative screening
2. Quantitative screening.

First, the qualitative screening consists in screening fire events depending on their impact based on identifying those fire zones where the expected risk of fire and associated events as well as their consequences is relatively low or negligible compared to others. In these zones, an external fire (or its consequences) causing a transient/initiating event and stopping the unit is unlikely, i.e. the risk caused by external fire is low and can be controlled with planned shutdown of some equipment or systems and other measures for prevention, and no other PSA components modelled in the PSA are affected.

Other indicators should be applied, as for instance:

- Existence of safety related equipment and cables related in the areas addressed in the external fire scenario;
- Identified external fire and associated event load areas;
- Effectiveness of the barriers between the fire zones, and other.

Two different fire situations should be studied:

- Fire within only one fire zone, and;
- Fire in more than one area – “multi-zones” (similar to "multi-compartment fires" considered in case of internal fire).

It should be stressed that in case of large external fire, multi-zones occurrence can be more probable than one zone. Additionally indirect consequences of external fire described by the sequence of various events should be practically examined almost always assuming fire effects in many zones.

Following the qualitative screening, the zones should be divided in two groups: one group for screened-out zones for which the analysis is terminated and one group for fire zones subjected to further analysis and the next stages of screening.

Then, following the qualitative screening, the second phase is the quantitative screening which is performed by establishing frequencies of fire events and sequences of events initiated by external fire, occurring in fire zones and complexes remaining after the qualitative screening analysis. In the frame of an extended PSA, the conditional core damage probability determined in the existing internal events PSA model can be used.

For the preliminary quantitative screening, the frequencies of fire scenarios at power operation, low power and shutdown should be presented. In case of fires of the type of "multi-compartment" in the extended PSA, the frequency of occurrence of fire and possible damage to equipment in "multi-zones" should be based on probability of failure of fire barriers data recommended in IAEA-TECDOC-1134 [30]. The generalized probabilities of failure of barriers from NUREG/CR-6850 [31] can be used only if technical problems on fire barriers in the NPP are not identified from the fire protection staff. According to the procedure NUREG/CR-6850 [31], the criterion for preliminary analysis of frequency of core damage is based on the assumption that the overall frequency of core damage is usually, for most stations, in the range of 1.0×10^{-5} per year or has a greater value. If another assumption is used for the analysis, the frequency of core damage should be redefined.

4.2.4 EXAMPLES OF HAZARD COMBINATIONS

In this chapter of the report, the typical or most important hazard combinations with external fire are listed.

First, the link between fire and explosion hazard should be considered. Different studies, such as the retrospective explosion and fire risk management analysis concerning the transport of liquid fuels, have shown immediate connection between both hazards, requiring mutual consideration in assessing risk for sites, facilities and equipment [32]. Highly probable combinations can exist between external fire and all the categories of explosion listed in 4.1.1:

- industrial explosion;
- military explosion;
- transportation explosion;
- pipeline explosion.

The hazard combination of a correlated external fire and an internal fire with explosion(s) on the NPP' site is also possible.

Other combinations for consideration are:

- lightning and fires;
- fires and hazardous gases;
- extreme high ambient temperature and fire;
- wind and fires;
- intentional or unintentional man-made actions and fires, and other.

As an example of such combination one can mention an external fire hazard (forest or industrial or other) due the impact of lightning combined with an induced overvoltage of the switchgear of the NPP also due to lightning, as pointed out in 4.2.2.

4.2.5 ASSESSMENT OF COINCIDENT HAZARDS BASED ON ESTIMATES OF DURATION TIME OF HAZARD

Recommendation No. 8 of the End Users workshop [1] categorized B/C[2] mentions that the combinations/correlations/dependencies of fire hazards should be discussed in an extended PSA depending on the time frame (for example, addition of independent fire hazards may be considered for a long lasting accident), and that, if appropriate, specific rules should be defined in the guidance. This seems reasonable. However, this recommendation should be applied depending on the frequency of the other hazards and on the differences of their impact, e.g. if the plant situation after the external fire is not worsened with an additional hazard impact, there is no need to analyse this combination further and in detail.

4.2.6 WORST CASE HAZARD COMBINATIONS

The worst case hazard combinations can be found, practically basing on the consequence analysis. Typical candidates are the following:

- the combination of an external fire hazard (forest or industrial or other) due to the impact of lightning combined with an induced overvoltage of the switchgear of the NPP also due to lightning and/or loss of off-site power (i.e. station blackout combined with fire);
- external fire, explosion and hazard gases;
- lightning and fire depending on the objects affected by lightning.

Recommendation No. 29 of the end users [1] categorized A, mentions that the effects of climate changes should be considered in two aspects:

1. The effects of climate changes (global warming) as reason for an increase of the probabilities/frequencies of occurrence of external fires, especially forest fires and agricultural fires.
2. The influence of the external fires on the greenhouse gases, especially forest fires in very larger areas lasting days and weeks, contributing to the global warming.

The last point is not directly related to fire impact on NPP, and in general, is difficult to realize taking into account the current knowledge of climate modelling, lots of uncertainties and therefore not enough credible results of modelling.

The above mentioned potential worst case hazard combinations have to be considered in further detail in the extended PSA.

4.3 AIRCRAFT CRASH

The objective of this chapter is to present and evaluate the possible hazard combinations concerning aircraft crash. Report [19] served as the most important basis of the discussion in this chapter. A hazard correlation chart was established in [19] taking into consideration all single external hazards. The possible hazard combinations

[2] End user’s categorization: Type A: most important end-users needs; Type B: intermediate needs; Type C: less important needs

were determined based on expert judgement and evaluation of past experience. The aforementioned hazard correlation chart is considered comprehensive; therefore no further hazard combinations are addressed in this chapter.

4.3.1 IDENTIFICATION OF HAZARD COMBINATIONS

Report [19] identifies the following three major types of hazard combination categories:

- causally connected hazards;
- associated hazards;
- combination of independent hazards (coincident hazards).

These three general combination categories were looked at one by one describing all aircraft crash related hazard combinations relevant to these categories.

4.3.2 CAUSALLY CONNECTED HAZARDS

With respect to aircraft crash, the following types of causally connected hazards should be investigated based on the approach outlined in chapter 3.1 of report [19]:

- An external event may induce aircraft crash;
- Aircraft crash may induce another external event;
- An external event is a prerequisite for aircraft crash;
- Aircraft crash is a prerequisite for another external event.

According to the hazard correlation chart, meteorological events, forest fire and external man-made hazards can be causally connected to aircraft crash. In report [19] aircraft crash is split into two classes of external hazards, namely aircraft crash related to airport zone and to air traffic. With respect to the possible hazard combinations, the only difference between these two hazards is that an aircraft crash in the vicinity of an airport can be caused by mist or fog, while air traffic related aircraft crash cannot be induced by this cause.

According to report [19], the following meteorological events may induce aircraft crash:

- Strong wind,
- Tornado,
- Snowstorm, icing
- Sandstorm,
- Wind-blown debris,
- Mist, fog.

Generally, all meteorological hazards causally connected to aircraft crash are events that may induce aircraft crash, and evidently no meteorological events can be induced by an aircraft crash.

Besides meteorological events and forest fire, the following external man-made hazards may be causally connected to aircraft crash:

- Explosion at nearby industrial facilities,
- Chemical release at nearby industrial facilities,

- Explosion and projectiles at nearby military facilities,
- Chemical release at nearby military facilities,
- Military activities,
- Explosion due to a transportation accident,
- Chemical release due to a transportation accident,
- Explosion and/or fire due to pipeline damage,
- Chemical release due to pipeline damage,
- Stability of power grid,
- Fire originated by human/technological activity,
- Intentional or unintentional man-made actions.

External man-made hazards causally connected to aircraft crash are consequences of an aircraft crash with the exception of military activities. Accordingly, military activities are one man-made hazards that can induce aircraft crash. Other could be intentional or unintentional man-made actions not connected with military activities, including sudden health problems, psychological deviations, etc.

In the hazard correlation chart there are no external events that would be a prerequisite for aircraft crash. This means that aircraft crash is not an inevitable consequence of any other external event. On the other hand, it is also stated in report [19] that aircraft crash is not a prerequisite for any other event. In other words, there is no external event which is only the consequence of an aircraft crash, all other events can also occur independently of aircraft crash.

4.3.3 ASSOCIATED HAZARDS

As discussed in chapter 3.2 of report [19], associated hazards refer to events that are probable to occur at the same time due to a common root cause. However, in the hazard correlation chart, there are no associated hazards that include aircraft crash. Theoretically, harsh meteorological conditions (e.g. induced by a hurricane) may induce an aircraft crash and in the same time another external event. In this manner the root cause may be the harsh meteorological condition and the associated hazards are aircraft crash and another consequence of the harsh meteorological conditions. Some examples for associated hazards relevant to aircraft crash induced by harsh weather conditions are:

- Aircraft crash and solid or fluid releases due to a ship accident,
- Aircraft crash and ship collision with water intake / UHS,
- Aircraft crash and direct impact by ground transportation,
- Aircraft crash and salt spray,
- Aircraft crash and external flooding.

4.3.4 COMBINATION OF INDEPENDENT HAZARDS

In general, considerations should also be given to those hazard combinations that include independent hazards without any correlation. Combination of independent hazards should be identified and selected by applying screening methods accompanied with expert judgement. In the absence of screening, a comprehensive list of hazard combinations including aircraft crash could be assembled but this would not be practicable due to the large number of identified combinations.

The frequency of aircraft crash in the vicinity of nuclear power plants is usually very low. Consequently, the frequency of a combination considering aircraft crash and a hazard independent therefore commonly falls below the frequency screening threshold set for single external hazards. Moreover, if a combination of independent hazards cannot be screened out, the intensity of the hazard other than aircraft crash is usually not severe enough to have a significant effect on the plant. Since the occurrence frequency of an aircraft crash on a nuclear power plant is very low, the only case an independent external hazard should be evaluated in combination with aircraft crash is if the impact of an aircraft crash on the plant holds for a long duration of time. The aircraft crash is a sudden, quick proceeding event; therefore the primary impact on the plant and on its vicinity takes a short time. Efficient mitigation actions can also be performed in some days (e.g. fire-fighting, removing the damaged parts of the aircraft), respectively the time needed for successful mitigation against the impact of an aircraft crash can also be considered relatively short (e.g. in contrast to flooding that may take a much prolonged time to cope with).

On the other hand, the static stability of SSCs (especially structures) may be affected by the direct (i.e. parts of the aircraft hurtle into a building) or secondary (i.e. fuel fire, secondary missiles, explosion and shockwaves resulting from the crash, etc.) effects of the aircraft crash and the reinforcement of the relevant structures might take a longer time period. An external hazard having a considerable and mechanical type of impact on structures (e.g. high wind or snow load) can occur during this period, which should be taken into consideration in the identification of event combinations. Furthermore the heating, ventilation and air conditioning (HVAC) system may be also affected by an aircraft crash. The restoration of the damaged HVAC system might take a considerable time, while a hot summer or a cold winter might affect some safety related I&C components, which may lead to plant transients. Thus the damage potential of an aircraft crash on the HVAC system and the consequences of some susceptible components from high or low outside temperatures (especially extreme ones) should be assessed.

4.3.5 EVALUATION OF IDENTIFIED HAZARD COMBINATIONS

As presented in chapter 4.3.1.1., report [19] lists a lot of hazards causally connected to aircraft crash. According to the hazard correlation chart, meteorological events, forest fire and external man-made hazards can be causally connected to aircraft crash.

Meteorological hazards and military activities being causally connected to aircraft crash are events that may induce an aircraft crash. Consequently, these events are a subset of the many root causes that can lead to an aircraft crash. If it can be justified that the contribution of meteorological hazards or military activities to the overall aircraft crash frequency is not significant (which is usually the case), then the frequency of an aircraft crash induced by these hazards may be lower than the screening criteria applied to individual hazards. Respectively, combinations of aircraft crash and meteorological hazards or military activities may be eliminated from the hazard combination list based on their occurrence frequency. Since certain meteorological events (e.g. high winds, hurricanes, tornadoes, snowstorms, mists and fogs) can be forecasted in advance, the risk induced by these events can be decreased by modifying the routes of the aircrafts or delaying their take-offs. Moreover, meteorological conditions at two different locations, i.e. near the plant and at the area where the aircraft was impacted might differ significantly due to the large horizontal or/and vertical distance (e.g. a tornado may affect the aircraft but it does not hit the plant). The same considerations apply to military activities: even if an aircraft crash occurs due to military activities, the chance that the plant is also affected by the military activity unintentionally may be negligible. These aspects should be taken into consideration for screening external events that may induce aircraft crash.

Causally connected external hazards, including aircraft crash and aircraft crash induced external events are also listed in report [19]. Forest fire and several kinds of man-made hazards given in chapter 4.1.1.2 belong to this type of hazard combination. Some of these aircraft crash induced events may occur far away from the plant (e.g. a chemical release at military facilities could reach the plant). Consequently, the probability of an aircraft crash having a primary impact on the plant and also causing such an accident far from the plant that has a significant impact on nuclear safety may fall below the screening threshold. Deterministic impact screening should also be applied to these events. The damage potential of an aircraft crash directly hitting a plant building without having the capability of inducing any other off-site events may be more severe than that of an aircraft crash having a moderate impact on the plant on one hand, and inducing some external event (e.g. forest fire) far away from the plant on the other hand. If an aircraft crash has negligible effects on the buildings of the plants, but it induces another single external event (e.g. loss of off-site power or forest fire), then the frequency of the event combination can be added to the occurrence frequency of the single external event being induced by the aircraft crash. Consequently, it is not necessary to perform a detailed assessment for the hazard combination.

Further risk significant combinations include aircraft crash induced external events which occur directly on the site or in its close vicinity. These induced events are usually explosions, extensive fires, generated missiles or toxic gas clouds due to the damage of conventional industrial facilities on or near the site. For example, if an aircraft hits a safety related building and it also causes an explosion and/or fire by damaging a pipeline, then neither probabilistic nor deterministic considerations can justify the screen out of the combined event from the list of potential hazard combinations. All events that may occur on the site due to an aircraft crash should be identified and evaluated. A detailed assessment should be performed for the screened in hazard combinations. The activities of the firefighters including the probable response time, the available fire mitigation and suppression devices as well as the appropriate headcount may be taken into consideration during screening. The possible consequential events induced by an aircraft crash can be considered secondary effects, covering possible induced internal hazards as well.

Current best practices address to some extent secondary effects as fuel fire, secondary missiles, explosion and shock waves resulting from the crash, hazardous effects induced by an accident on a traditional industrial facility located on the site and internal hazards, e.g. internal fire. These secondary effects together with events related to explosion, fire or missiles induced at the site by the crash impact are the most severe aircraft crash related hazard combinations, which should at least be taken into consideration in the PSA. Nevertheless, best practices usually do not take into consideration aircraft crash hazards in combination with associated and independent hazards. The contributions of external events that may induce aircraft crash are included in the aircraft crash statistics, although the combined impacts on the plant are usually not assessed. All these events should also be evaluated, but usually they have low risk significance and are reasonable to screen out.

5 METHODS FOR THE ASSESSMENT OF HAZARDS COMBINATIONS

5.1 GENERAL DESCRIPTION

IAEA Safety Guide NS-G-1.5 [33] includes the combination of human induced events within the group of the man-made external hazards as a result of a common initiating event, as a product of events (like, e.g. explosion with release of hazardous gases, fire and smoke generation, aircraft crash induced missiles, vibrations or explosions of aircraft fuel). Domino effects shall also be considered (like, e.g. storage tank explosion induced by a pool fire chain car/trucks accident accompanied or caused fire).

IAEA Safety Standard NS-R-1 [34], [35] cautions about the combination of individual events evaluation to ensure some rationale justifying the particular combination: for instance, a random combination of events may represent an extremely unlikely scenario such as to motivate its disregarding in the probabilistic safety analysis.

Probabilistic evaluations should be carried out, for the definition of suitable combinations for the plant design and for the subsequent risk assessment, between external events and internal accidents, addressing both their potential correlation and their resulting probability. In any case, combinations of two or more individual events should be carefully analysed with account taken of the dependence or independence of the events. In an accidental scenario, independent events can be assimilated to simultaneous events (for non-simultaneous events, but occurring before the effects of the previous event completely ceased, sometimes, by simplification, it is conservatively considered that the subsequent events will occur at the worst moment for the facility safety): the probability that the events will occur in such conditions that their effects will be cumulated is related to the duration of each event. The probability that the events occur in combination is equal or less than the product of the probability of each event.

Expert judgement and probabilistic methods can be used for the selection and relative credible estimation of event combinations that should be thoroughly analysed in order to select the anticipated operational occurrences and the mitigation actions to be taken into account in the plant design or to be included in the risk assessment. At present, the technology is not always available for precisely assessing the numerical probabilities that a given level of severity of an effect is exceeded in each separate event or by a combination of events. However, in absence of best estimate methods, conservative values should be estimated for these probabilities.

5.2 DATA NEEDS

The approaches to estimate the frequency of combination of external events are applicable by using explicit site and plant specific data, as well as accident statistics relative to trucks, trains, shipments and aircraft and data on traffic accidents involving fires, explosions and toxic releases. As well, industrial facilities and hazardous material pipes shall be considered.

5.3 INITIATING EVENTS

Combination of external events shall be identified based on a comprehensive hazard analysis. All foreseeable combination of external hazards, including the potential for human induced events to affect directly or indirectly the safety of the plant shall be identified and their effects on relevant SSCs important to nuclear safety shall be evaluated.

The design of a facility shall include due consideration of those natural and human induced external events (i.e. events of origin external to the facility) combinations that have been identified in the site evaluation process. In addition to natural external events (including meteorological, hydrological, geological and seismic events), human induced external events arising from nearby industries and transport routes shall be addressed. The credible combinations to consider have been identified in the previous chapter.

For man-made and aircraft crash hazards, all credible combinations have been identified and they can be categorised in three types of hazards: consequential, correlated and coincidental as described in Chapter 4.

In order to simplify the assessment, it is suggested in [36] to split the combination assessment into three stages. The first stage is to identify the plausible off-site hazard combinations. The second stage is to identify the potentially induced on-site failure/hazards. A final stage is to identify the potential additional induced failures that could be induced by the possible hazards identified in the second phase.

5.4 REFERENCE TO KNOWN METHODS

IAEA includes requirements on combined hazards and safety analysis in [22]: the problem is the lack of detailed guidance on this issue and the fact that combinations of events are frequently screened out from analysis. Expert judgement is used for the identification of extreme hazards combination probability, for instance adopting a matrix method with expert panel aimed on identification of critical combinations for given plant design. Document [37] proposes, in the fashion of qualitative analysis, some risk assessment methods applicable to external hazard combination depending on the frequency, effects on the plant and accident scenario:

- risk assessment based on the hazard frequency or hazard impact analysis: the minimum hazard level which may have impact on the plant is established; the frequency of external hazards combinations which exceeds this level is quantitatively evaluated based on a conservative analysis; if the result indicates that such a frequency is below a reference screening-out value, this combination of hazard shall be determined to pose no significant risk of core damage however, it has to be noted that the severity of combinations of hazards can be higher than the severity of each individual hazard taken separately;
- safety margin evaluation: a safety margin evaluation is performed when it is necessary to take into account all accident scenarios after an external hazard has impacted the plant; when the hazard frequency evaluation is difficult to perform or when the uncertainty associated with the frequency is significantly high, it is considered appropriate to evaluate the safety margin of external hazard against core damage risk ;
- Core Damage Frequency (CDF) evaluation: the Conditional Core Damage Probability (CCDP) of the plant caused by the combination of hazards is quantitatively evaluated by assessing the effects of the combination on the occurrence of the initiating events which may lead to core damage and the effects of the combination on the loss of SSCs requested to mitigate the effects of these initiating events (“fragility” assessment); then, the calculated CCDP is multiplied by the frequency of the external hazard combination exceeding the hazard level at which the plant may be affected to determine the CDF.

Within the OECD Workshop on PSA OF NATURAL EXTERNAL HAZARDS INCLUDING EARTHQUAKE [38], some approaches aimed at the combinations of hazards topic are proposed, which are likely to apply to the present case.

In particular the paper presented by L. Burgazzi, ENEA, entitled "Implementation of PSA models to estimate the probabilities associated with external event combination" shows how, in the light of the Fukushima accident, correlated hazards are of special interest in PSA for external hazards [39]. Thus, a mathematical method for modelling correlations was proposed in the presentation and an illustrative example was presented. The method is based on joint probability distributions and covariance matrices.

A systematic method aimed at identifying important hazard combinations and associated dependencies among PSA initiating events was presented by S. Sperbeck from GRS in his presentation titled "Recent research on natural hazards PSA in Germany and future need" [38]. During the discussion, it was also suggested that, given the multiplicity of potential combinations, such an analysis should be carried out in a systematic manner (e.g. by matrix of possible external events combinations).

Finally the workshop pointed out the identification of correlations between external hazards as another important point. The combinations of simultaneous or successive external hazards may result in increased loadings on SSCs or they may simultaneously endanger diverse safety systems. Formal mathematical methods to treat the probabilities of correlated hazards are available but the quantification of the model parameters is a big challenge, due to the scarcity of data.

The problem of combined hazards has been also perceived in the methodologies developed by IAEA and LRC described shortly below. These methodologies are attempts of developing supporting tools to deal with extreme events and relevant accident scenarios.

IAEA Fault Sequence Analysis (FSA) Methodology

IAEA developed a complementary safety analysis FSA methodology and supporting tool to assist in evaluation of the impact of extreme events on NPPs [40], [41]. This method utilises both probabilistic and deterministic safety assessment methods to gain the insights of robustness of plant protection including impact on SSCs against the extreme external hazards and its combinations. The method also considers combined load conditions resulting from the simultaneous occurrence of these hazards. Fundamentally, the FSA method incorporates 'stress test' principles that have been formulated in Europe after the Fukushima accident. The method considers the sufficiency of 1) defence-in-depth provisions, including various dependencies, 2) safety margins, 3) application of specific design features, 4) cliff edge effects, 5) multiple failures, 6) prolonged loss of support systems and 7) the capability of safety important systems for long term operation [41]

The FSA method and supporting tools have been used at Goesgen-Daeniken NPP, Switzerland and Medzamor NPP, Armenia. The methodology is described in detail in IAEA paper [41].

Extreme Event Analyzer (EEA) Methodology

Lloyd's Register Consulting (LRC), in cooperation with IAEA, has further developed the FSA method [42]. LRC developed a value added tool (ExtremeEventAnalyzer (EEA)) to systematically analyse accident conditions even if they are not explicitly addressed in the design extension conditions using integrated deterministic and probabilistic approaches. The tool has incorporated lesson learned from the FSA methodology developed by IAEA, which has been verified by application on Goesgen-Daeniken NPP (Switzerland) and Medzamor NPP (Armenia) [43].

This method utilises an internal initiating events PSA model for assessing the impact of extreme events, including the consideration of hazard susceptibility limits of SSCs and impact of extreme external hazards. In the EEA method, a number of extreme events (including credible combinations) can be postulated, for example seismic, water levels, extreme temperature, weather conditions etc. The extreme event analysis is linked directly to the PSA model (in RiskSpectrum) to ensure that the whole PSA model is included in the evaluation of the impact of the event or combinations of events. The EEA performs re-quantification of the PSA model including the hazard susceptibility limits of the SSCs. The outcome of the analysis is to [42]:

1. Identify sensitive accident NPPs scenarios coming from extreme events;
2. Analyse simultaneous extreme events;
3. Prove robustness of plant design, for individual components and for buildings.

Below is a list of sequential steps to perform while using the EEA method to identify scenarios sensitive for extreme events [42]:

1. Determine what hazards to include. This is site specific and screening criteria may be applied.
2. Determine the components, buildings that can be susceptible to the hazards. Plant data collection and plant walkdowns are important inputs.
3. Determine initiating events which can be triggered by the hazard.
4. Determine the magnitudes of hazards that will fail the components, the buildings and trigger the initiators.
5. Generate the minimal combinations of events given the occurrence of a hazard or combinations of hazards.

The EEA method and tool is utilised in a benchmarking study “Extreme Event Analysis – an application of RiskSpectrum EEA at Armenian NPP” and is performed in a co-operation project between LRC, Nuclear and Radiation Safety Center (NRSC) and Armenian Nuclear Power Plant (ANPP) [43]. The purpose of the study was to perform a comprehensive and systematic assessment of robustness and vulnerability of NPPs against the impact of extreme events using the EEA method and tool. The EEA method, result and conclusion of this benchmarking study are presented in [43].

5.5 BEST PRACTICES

In general modelling correlation of initiating events due to their combination is an open issue. In any case, it requires the inclusion of the dependencies between the marginal distributions to construct the joint probability distributions for combination of hazards. According to the classification proposed in the previous chapter, the following approaches may be taken into consideration for modelling the respective event combinations:

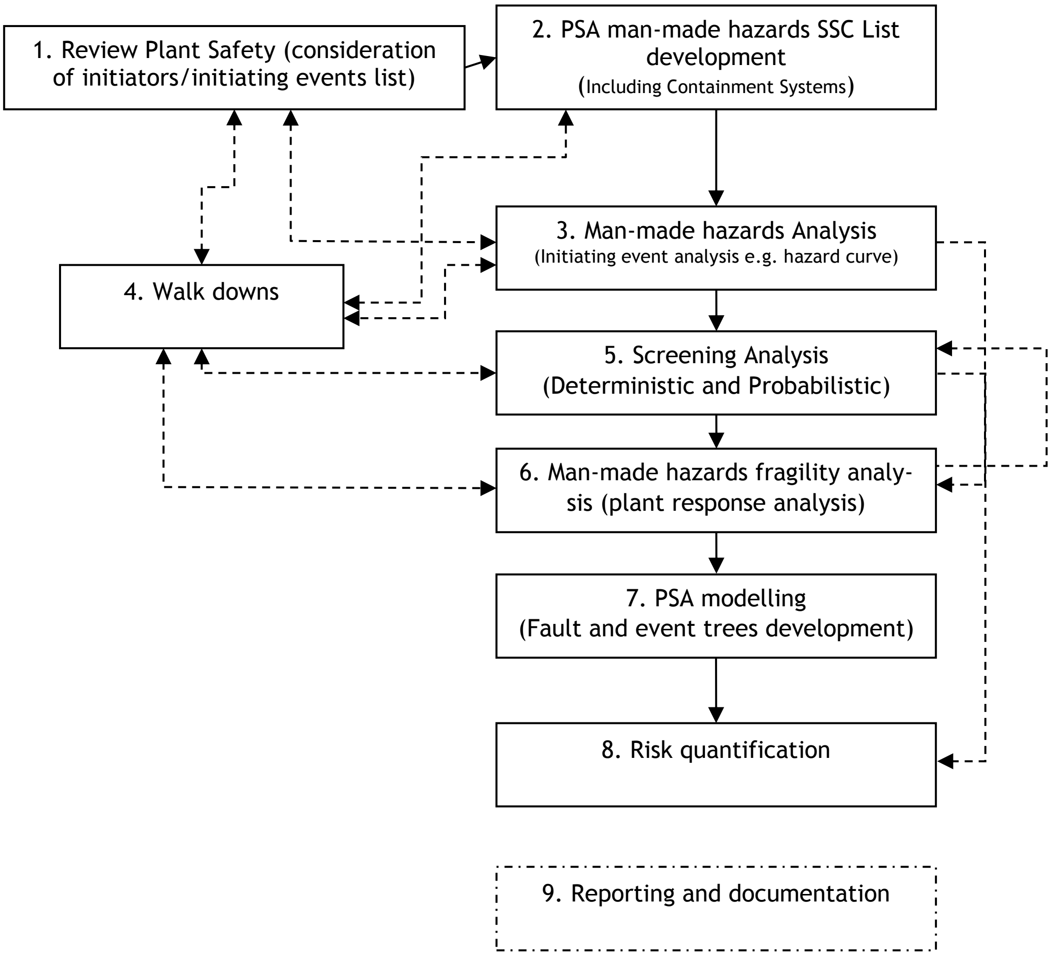
- consequential hazards, potentially induced (e.g. explosion induced events, like pressure wave): the probability of such consequential events A and B would be expressed as the conditional probability of A given B; the approach based on the conditional probabilities concept fits to this category [38] and [39], which allows providing the probabilities of the correlated events occurrence, given a certain frequency for one of them ;
- correlated hazards, may have a certain degree of dependency (e.g. extreme weather condition leading to lightning strikes and to an aircraft crash): the probability of such correlated events A and B would be expressed as the probability of A inter B (A∩ B) with A and B correlated. In this case, the more “classical” joint probability distributions which include the dependencies between the hazards in terms of correlation coefficients are more appropriate;
- coincident hazards, credible independent combinations: the probability of such independent events A and B would be expressed as the probability of A inter B (A∩ B) equal to the product of the two probabilities (P(A) x P(B)) ; in this case, the events are independent and so the relative probabilities, reducing the

problem to the assessment of two or more external events occurring simultaneously so that the overall frequency would be quite straightforward as the product of the single frequencies.

6 STRUCTURE OF MAN-MADE HAZARDS AND AIRCRAFT CRASH PSA

A general flow chart for extended man-made hazards is proposed below, based on the flow chart developed in WP22 for seismic events. It consists of nine steps plus reporting and documentation. The step 4 (Walk downs) is repeated several times during the analysis adding more and more details. Hence it can be regarded as a kind of control part.

Figure 6-1: Flow chart for extended man-made hazards L1 PSA


1. Review Plant Safety (consideration of initiators/initiating events list)
2. PSA man-made hazards SSC List development (Including Containment Systems)
3. Man-made hazards Analysis (Initiating event analysis e.g. hazard curve)
4. Walk downs
5. Screening Analysis (Deterministic and Probabilistic)
6. Man-made hazards fragility analy-sis (plant response analysis)
7. PSA modelling (Fault and event trees development)
8. Risk quantification
9. Reporting and documentation

The first elements of the diagram above are described mostly in Chapters 3 and 4. As far as screening is considered one can mention the SKI report **[21]** where criteria both for single and combinations of hazards are discussed. The ASAMPSA_E report "Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA" **[3]** provides also an analysis of existing practices. As an example the screening criteria for single external events are presented in the table below.

Table 6-1: Screening criteria for single external events [21]

C1/Severity	*C2/ Frequency*	*C3/ Distance*
The event has a damage potential that is less or equal to another event that the plant is already dimensioned for	The event has a considerably lower frequency of occurrence than events with similar uncertainties and cannot result in worse consequences	The event cannot occur close enough to the plant to affect it
C4/ Inclusion	*C5/ Warning*	*C6/ Applicability*
The events can be included in the definition of another event	The event develops at such a slow rate, that there is enough time to initiate counteractions	The event is not applicable to the site

As an example of this method one can mention that aircraft crashes are screened out in Swedish NPPs according to criterion C2 as the frequency of being hit by a crashing aircraft is around 2E-8/year.

Regarding step 6 (plant response analysis) the followings elements have to be taken into account **[21]**:

1. Plant response information needed in deterministic screening;
2. Resistance of relevant buildings and structures against External Event impact ought to be identified;
3. Analysis is highly plant specific;
4. Relevant design characteristics should include:
    - structural characteristics,
    - characteristics of active or passive safety functions,
    - protective / mitigating interactions (safety and operating procedures).

Plant interfaces have to be also considered, e.g.:

- structural integrity,
- main heat sink,
- air supply (cooling, ventilation, combustion, etc.),
- external power supply,
- operating environment of safety related equipment.

Detailed analysis is performed to estimate the frequency of the events identified in step 6. This is described in chapter 3.3.

For external fires and explosions, as it has been already mentioned, in principle QRA-type analysis should provide estimation of the frequency of initiating events.

The next thing to do, following the hazards characterization and the definition and quantification of the initiating events to be modelled in the PSA (see chapters 2 to 5), is to analyse the impact of the man-made hazards or aircraft crash on the plant and the plant response. Often the impact can be grouped into general classes of effects. An example of these general effects is given in [21]:

- **Structure/Pressure**: the external event may affect the structure through pressure which may disable safety functions contained;
- **Structure/Missile**: the external event may affect the structure through missiles, which may disable safety functions contained;
- **Cooling/Ventilation**: the external event may affect the ventilation, which may cause partial or total loss of safety systems relying on air cooling. Alternatively, the event may affect the plant through the ventilation system, e.g., toxic gasses.
- **Cooling/Ultimate heat sink**: the external event may affect the ultimate heat sink which may cause partial or total loss of secondary cooling and other safety systems relying on water cooling;
- **Power Supply**: the external event may affect the external power connection of the plant, and may cause loss of offsite power;
- **External flooding**: the external event may affect the plant by disabling safety systems contained or by undermining the structure;
- **External fire**: the external event may affect the plant by disabling safety systems contained;
- **Electric effects**: the external event has indirect effects on the plant by generating electrical or magnetic fields, which may potentially affect transmission of power supply or control signals to safety systems;
- **Other direct impact**: in a few cases, the event may work in a way that is not covered by the general categories. An example is plant isolation.

For the man-made hazards considered in this report (external fire, external explosion and accidental aircraft crash) mainly the consequences pressure, missiles and external fire are relevant. Based on these effects, combined with the data from the characterization of the hazards (e.g., strength parameters, distance from the plant, propagations paths) the affected plant parts can be determined.

After the identification of the consequences of the man-made hazards, it might be possible to make the link with internal events already modelled in the PSA. If no additional systems are lost compared to the internal event, the hazard may be grouped with the internal event. If additional safety systems are lost or safety functions are degraded, which is often the case for man-made hazards, separate modelling will be required. The modelling can be based on the structure for the internal event, where additional systems are assumed to be lost. The advantage of making the link with the internal events PSA is that consistency is provided.

Example 6.1: internal events analysis as basis for man-made hazard analysis

An external fire might lead to loss of offsite power. If this is the worst imaginable consequence, the hazard may be modelled, with as basis the loss of offsite power of the internal events analysis event tree. However, additional systems may be unavailable, recovery times might change, and procedures might not be applicable.

In general, mainly the SSCs and the operator actions from the internal events PSA need to be adapted to account for the specific plant conditions and plant response in case of man-made hazards or aircraft crash. Basically, some SSCs and failure modes or operator actions should be added or removed or the probabilities of failure should be modified.

In general the following information is required to model the man-made hazards in the PSA:

- **Building and structure mapping**: which SSCs are located in which building? How can failure of these SSCs affect the plant operation? The key steps for generating man-made hazard equipment list are as follows [44]:
    - include all components already considered in the internal-events PSA model.
    - review components that are screened out from the internal events PSA model; due to the hazards, failure modes that were considered negligible in the internal events PSA, could be applicable under the hazard circumstances; for example, spurious actuation might be more relevant;
    - include the passive components, perhaps screened from the internal events model, but whose seismic failure could affect the safety functions modelled in the PSA; e.g. tanks, cabinets, cable trays, HVAC ducting;
    - add the structures which house the PSA and passive components;
    - compare the lists compiled for PSAs at other similar nuclear power plants for completeness.
- **Characterization of the hazard:** this information is already acquired during the identification and screening process (Chapters 3.1, 3.2, 3.4, 3.5, 3.6 and 4). Relevant parameters are as follows:
    - *Strength of the hazard*: identify the effect on SSCs;
    - *Progression of the hazard*: identify short term and long term effects; also, identify whether the hazard can progress to other buildings/SSC's as well;
    - *Environmental impact of the hazard*: will conditions change in such a way that procedures cannot be carried out anymore or are compromised?
- **Qualification of the SSCs**: which SSCs will fail under which circumstances? For the man-made hazards qualifications on, pressure, heat and smoke, might be applicable. Will the effect occur on the long term or the short term? Some SSCs might not be required during the complete accident sequences. Therefore failure modes in the long term might not be applicable for this SSC, however short term failure modes might be relevant.
- **Failure mechanisms**: the man-made hazards can lead to specific failure mechanisms. In Table 6-2 failure mechanism examples for man-made hazards are shown. As can be seen, these failure mechanisms are directly linked to the general effects, mentioned at the beginning of this chapter. If these failure mechanisms lead to distinct failure modes, these need to be added to the model. If these failure mechanisms do not lead to distinct failure modes, they might lead to increased frequency of specific failure modes. This needs to be accounted for in the model for the man-made hazards.
- **Reliability data**: If fragility curves are available for the SSC's then these might be used to estimate the probability that a SSC will fail due to a man-made hazard. Often these fragility curves are not available. In that case a conservative screening process is used: SSCs are either failed or not failed by the man-made hazard.
- **Man-made hazard and initiator specific procedures:**
    - *applicable procedures to prevent consequences of the man-made hazards;*
    - *applicable procedure to mitigate the consequences of the man-made hazards;*
    - *applicable procedures required for mitigation of the initiator; these procedures are the same as for the internal events.*

- **Review of human actions failures:**
  - Conditions, available systems and indications might be altered, as a result of which human error probabilities (HEPs) might change. This is further discussed in chapter 9.

Table 6-2: Examples of failure mechanisms of SSCs in case of man-made hazards

failure mode (FM)		exposure time	remarks, questions, examples
FM	SSC is …		
FM1	Burned	short- to long-term	It is to check if and how a SSC is designed against fire. Is short-term fire of a SSC possible without failure? Assessment of cable and cable connections regarding failure sensitivity against fire or hot temperature they are not designed for.
FM2	Exposed to high temperature	long-term	SSC in hot atmosphere
FM3	Exposed to overpressure, shock waves	long-term	SSC design against overpressure and shock waves
FM4	Unstable	short- to long-term	SSC design against release of gases
FM5	Exposed to missiles	short-term	SSC design against missiles coming from the explosion
FM6	Exposed to smoke	long-term	SSC design against smoke conditions

The objective with the integration of external hazards in the PSA is to use the existing internal events PSA to the extent possible. This means that depending on the hazardous event considered, the same accident sequences, meaning the same operator actions and systems to mitigate the event, as for an internal event already modelled, could be used. This is valid if the impact on the plant and the plant response following the occurrence of the hazard is similar to an internal event already modelled in the PSA. But the probability of failure of the human actions and SSCs credited in the accident sequences might need to be adapted. Thus, the same event trees could be used but some basic events modelling the “normal” probability of failure of the SSCs would have to be exchanged with basic events modelling higher probability of failure.

The system functions need to be reassessed to check that the same success criteria are applicable as for the internal event analysis. If the effect of the hazard can be linked to the internal event analysis, it is most likely that the system function analysis is the same for the hazard analysis and for the internal events analysis.

In that sense, the system reliability analyses for a certain man-made hazard can be very specific and different from the analyses performed in the frame of the internal events PSA. Basically, the functions and SSCs modelled would probably be the same, but the failure modes and the probability of failure would need to be modified.

Depending on the contribution of the man-made hazard to the total ‘Core Damage Frequency’ a more or less detailed modelling is required. This might be the case if the initiating frequency is low, or if the affected systems are not important to plant safety. In that case a screening analysis can be used. Within this screening analysis all SSCs directly or indirectly impacted by the man-made hazards are given a failure probability of 1.

A more detailed analysis would be required if the contribution to the total 'Core Damage Frequency' is unacceptable or if the hazard unnecessarily dominates the results. A less conservative assessment requires detailed fragility analyses of the impacted SSCs to adjust their probability of failure in the PSA according to the severity of the man-made hazard considered. With a more detailed assessment, the link between the hazard characterization and the definition of the initiating events modelled in the PSA can be made with the SSCs of the plant. For a given severity of initiating event, the probability of failure of the SSCs of the plant can be evaluated.

As for other hazards, also for man-made hazards, hazard combination might be applicable. The following selection criteria can be used to obtain a list of combinations of hazards [21]:

1. Definition of events

   A multiple external effects may be included in the definition of a single event, e.g., extreme snow, which includes snowstorm (strong wind AND snow).
2. Dependence of events

   The basis for defining potentially relevant external events, was that the occurrence of the events involved in each group are not independent.

Note: Theoretically, combinations of independent events may be relevant. However, this presupposes a high probability of occurrence of the combination, i.e., a long impact time of the event and/or a high frequency of occurrence. It is assumed that no such cases exist.

3. Different plant safety functions affected

   If criterion 2 is fulfilled, the next condition is that the events must affect different general classes of effect from external events. As an example, if two external events are dependent and one affects offsite power while the other one affects the ultimate heat sink, this would be a relevant combination. If the events affect the same function, an additional check must be made according to "4." below.
4. Degree of impact on plant safety functions

   If two dependent external events affect the same safety function, they may still be a relevant combination, provided the effect they have as a combination is greater than the effect from any of the single events involved.
5. Single external events criteria

   Finally, even if a combined event may be relevant according after having applied the criteria above, the single external event screening criteria should be used also on combined events.

This whole exercise is challenging since there is a lack of experience and input data to define and characterize the considered hazard in sufficient detail and there is also a lack of available test data and numerical values to build the fragility curves. Thus, engineering judgment is also often used and/or conservative approach can be sufficient. This induces large uncertainties and still overestimated contributions to the risk from these external hazards.

Following a rough step-by-step approach is proposed for a site-specific probabilistic analysis of man-made hazards: the fundamental analysis has to be performed regarding the failures modes mentioned above. For that purpose the L1 PSA model for internal events has to be extended systematically, i.e. the fault tree gates describing the failure behaviour of a SSC which can be damaged must be complemented by one or several additional specific failure modes.

7 SOLUTION FOR THE MODELLING OF MAN_MADE HAZARDS AND AIRCRAFT CRASH FOR L1 PSA

7.1 USE OF L1 INTERNAL EVENTS AND HAZARDS PSA

Similarly to most external hazards (as discussed in [22]), the L1 PSA model for internal initiating events is practically always used as a basis for the accident sequence development in aircraft crash, external fire and external explosion PSA. Consequently, the availability of the L1 PSA model for internal events and hazards are a prerequisite for performing a detailed analysis of the man-made hazards. The detailed analysis should be based on realistic models and data, including a comprehensive L1 PSA model that provides the possibility of modelling all phenomena associated with man-made hazards.

In accordance with good practices, preference is given to developing an integrated model for internal and external events (including aircraft crash) in contrast to building separate standalone models for different categories of events. In order to properly address the impact of a man-made hazard, integrated models should also incorporate aspects that are different from internal initiating events. The major impacts of a man-made hazard that could lead to various types of internal initiating events or to core damage directly should be assessed in the selection of the appropriate event sequences from the PSA model for internal initiating events. The probabilities of recoveries and post-initiator human errors should be revised by assessing the impact of a man-made hazard on the credited recoveries and human actions modelled in the L1 PSA for internal initiating events. Also, it may be necessary to include and analyse recovery actions over and above those included in the internal events PSA model.

7.2 STATE OF THE ART METHODOLOGY FOR PSA MODEL DEVELOPMENT

This chapter presents the specificities of PSA model development for man-made hazards by going through the general PSA model development process and the associated analysis steps: characterization of PSA initiating events, development of accident sequence models, fault tree development, human reliability analysis and analysis of input reliability data. Some of these analysis areas are presented in detail in other parts of this document, respectively this chapter focuses on issues that are not discussed elsewhere. To avoid unnecessary overlaps, only the most important aspects are summarized here, and reference is made to the relevant chapter for more details on a given issue.

7.2.1 CONSEQUENCE ANALYSIS OF PSA INITIATING EVENTS

7.2.1.1 Aircraft crash

The first step of PSA model development for external events is the unambiguous definition of PSA initiating events. The identification and characterization of PSA initiating events is performed during hazard assessment, i.e. the output of hazard assessment is the list of PSA initiating events and the relevant characteristics thereof (amongst others their occurrence frequency). Chapter 3 presents hazards assessment for man-made hazards in detail, consequently only PSA model development is discussed hereby.

For the purposes of defining PSA initiating events, aircrafts are classified into different categories relevant to the vicinity of a specific site, because of the different flying characteristics and in the reliability of different aircraft categories. The direct impact of an aircraft crash depends on the descent angle, mass and velocity of an aircraft that differ significantly among aircraft categories. As an example of such detailed analysis of aircraft induced impact on the structure because of vibratory loading can be found in [45]. Similarly safety assessment of reactor building for large commercial aircraft crash is presented in [46]. For initiating event characterization, the impact mass and velocity distributions are also determined as primary information on the hazard. The state of the art methodology does not consider the distribution of descent angle; rather it applies conservative values to assess the effective target areas.

As it has been already stated in chapter 3.6.1 primary and secondary impact areas and related effects have to be analysed basing on the description of initiating events according to aircraft categories and the affected impact zone for each category as well as the calculation of crash frequency for each of these events.

An example of Korean study to assess the risk of NPP against to aircraft crash is illustrated in [47].

Figure 7-1: Example of Technical Roadmap to assess the risk of NPP against to aircraft impacts events [47]

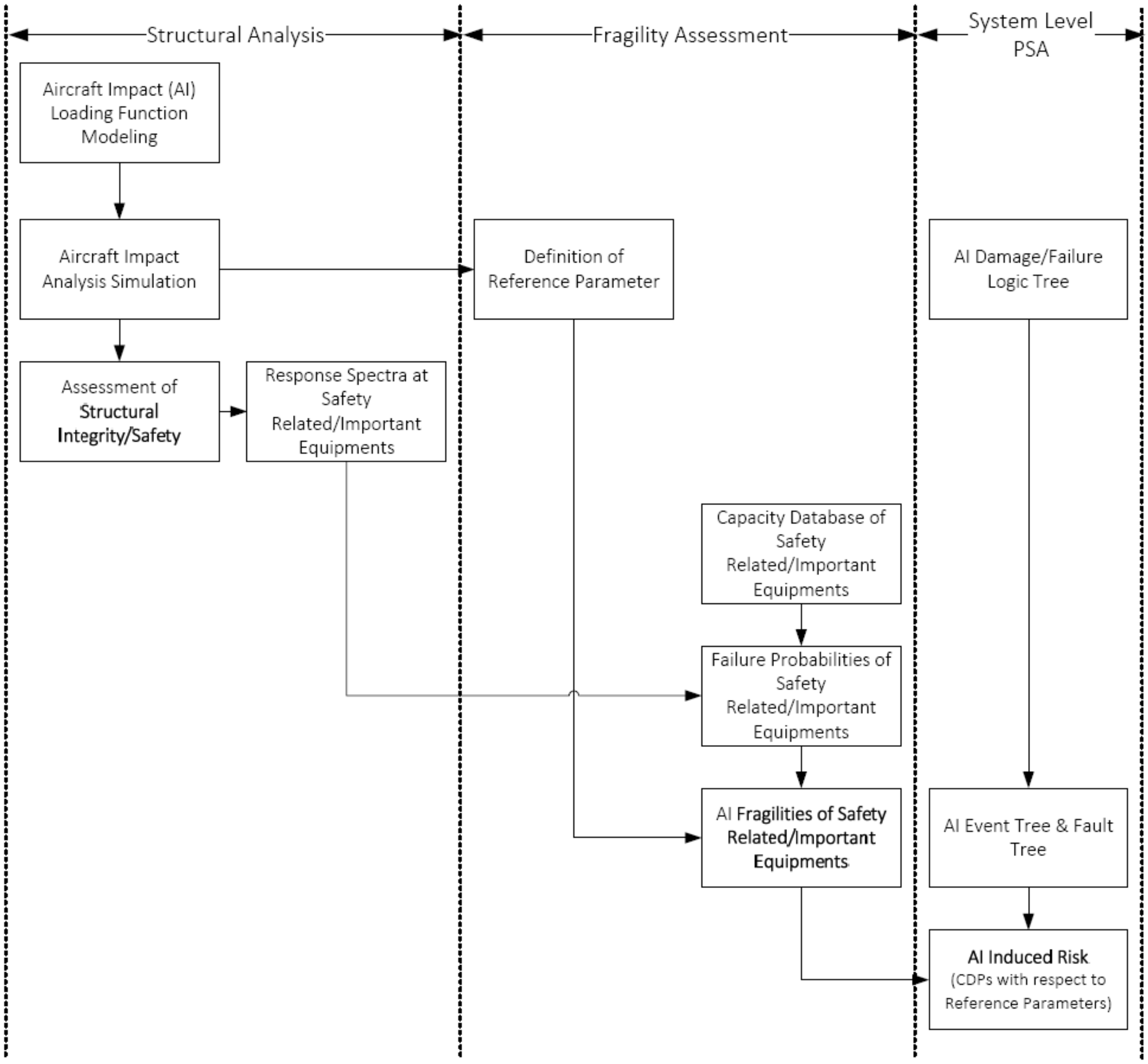

Structural Analysis
Fragility Assessment
System Level PSA
Aircraft Impact (AI) Loading Function Modeling
Aircraft Impact Analysis Simulation
Definition of Reference Parameter
AI Damage/Failure Logic Tree
Assessment of Structural Integrity/Safety
Response Spectra at Safety Related/Important Equipments
Capacity Database of Safety Related/Important Equipments
Failure Probabilities of Safety Related/Important Equipments
AI Fragilities of Safety Related/Important Equipments
AI Event Tree & Fault Tree
AI Induced Risk
(CDPs with respect to Reference Parameters)

Figure 7-1 is a schematic diagram for the assessment procedure of the aircraft impact event induced risk of NPPs. The total procedure composed by three stages; structural analysis to obtain structural responses and evaluate the structural safety, fragility assessment to estimate the aircraft impact fragility functions of safety-related equipment, and system level PSA to quantify the aircraft impact induced risk.

7.2.1.2 External Explosions and Fires

Regardless of the origin of the explosion, its effect can be expressed in terms of the following parameters: impact loads, impulsive loads, thermal loads and vibratory loads. The number of missiles which may be generated and may affect different parts of the plant is as important as their size and velocity.

Similarly the effects of fires are mostly expressed by thermal loads.

The analyses that consider externally induced initiating events in the frame of internal events PSA (e.g., explosions or fires induced losses of off-site power) may not always consider important dependencies (e.g., vibrations induced failures or the smoke caused by fire). Both direct effect of the explosions (e.g., shock-induced collapses or fire destroying elements of electrical system) and the indirect effects (e.g., explosion induced missiles or fire causing blast) are required to be analysed as part of the EE (external events) analysis. It must be decided whether or not the fire or explosion will cause an initiating event in the plant, and which initiating event is the most probable to occur. In most cases the initiating event will be a transient.

The explosions are primarily affecting the structural integrity of buildings or structures. An important consideration in EE PSA is whether the explosion can (depending on design and site-specific details), in addition to disturbing the operation of the plant, also disable or degrade one or more safety functions needed to cope with the initiating event. Similarly fires can affect electrical or power supply systems and the question of degradation of safety functions should be raised. The results of external events PSAs are sensitive to the modelling of dependencies between initiating events and safety system failures as well as between failures of different safety systems. To reflect the degree of protection against the impact by the pressure waves or heat the important areas of the plant could be divided into three classes (A, B and C), the same as for the consideration of aircraft crashes [48]:

- Class A contains systems that induce in case of their damage a hazard state or an initiating event may occur which cannot be controlled by emergency mitigation systems;
- Class B contains systems that may induce in case of their damage an initiating event which is controlled by the emergency mitigation systems;
- Class C contains the safety systems needed for core cooling, consisting of buildings that are structurally designed to withstand external influences, including external events.

Depending on the impact zone, and based on the above classification, the occurrence or not of an initiating event in case of explosions or fires, and the situations where an external influence can cause an initiating event and simultaneously degrade safety systems can be estimated.

The identification of dependencies is based on operating experience, plant walk-downs, interviews of designers and operating and maintenance personnel and systematic analysis of plant systems and components and their design basis.

The assessment of the explosions and fires abilities to impair a mitigating system can be made by the following steps:

- identification of the phenomenological conditions created by the event (e.g., shock wave, missiles, adverse temperatures and thermal effects),
- identification of time-phase dependencies,
- identification of dependence between components,
- identification of the design conditions (trip signals) that will cause a system to fail to start or fail to continue to operate (excessive room temperature).

Not surprisingly, the same considerations as made during the process to screen hazard or hazard combinations out, are valid to assess the impact on SSCs if not screened out. Usually, events such as aircraft crashes and missile strikes have limited impact areas (even when more than one missile is considered), while explosions, fires, ground motions and gas clouds can have plant-wide effects. If the affected area is plant-wide, items important to safety located anywhere in the plant could be affected coincidentally, and necessary safety functions might be affected. Fires resulting from deflagration shall be dealt with on the same basis as fires due to other man-induced impacts [49].

An analysis of the ability of plant structures to resist the effects of a gas cloud explosion can normally be limited to an examination of their capacity to withstand the overpressure (direct and drag) loading. In general, the effects of explosions which are generally of concern when analysing the structural response are [33]:

- incident and reflected pressure (mainly from detonation),
- time dependence of overpressure and drag pressure,
- blast generated missiles,
- blast induced ground motion (mainly from detonation),
- heat or fire.

The relative importance of these effects depends mainly on the quantity and type of the explosive substances, the distance of the structure under consideration from the source of the explosion, and details of the geometry and spatial arrangements of the structures and the explosive.

In case of fire the main concern relates to the duration, the velocity and direction of fire spread (which depends on meteorological conditions) and the location of the source. The extent of the fire and the distance to the structures plays important role.

If the plant has been designed to accommodate the effects of externally generated missiles resulting from other events such as a hurricane, typhoon, tornado or aircraft crash, the effects of missiles generated by an explosion may already have been taken into account. If missiles from an aircraft crash or natural phenomena are not included in the design basis, potential blast generated missiles should be considered [33]. A building designed against deflagration may also withstand a detonation with higher overpressure if the overpressure is of sufficiently short duration in relation to the response period of the structure. The rate of decrease of overpressure with distance differs between deflagration and detonation, having the characteristics influenced by the weather conditions and the topography.

The response of a structure subjected to a blast loading depends upon the time history of the loading as well as the dynamic response characteristics of the structure. An analysis of the ability of plant structures to resist to the effects of explosions can usually be limited to an examination of their capacity to resist the free field or reflected and focused overpressure. In estimating the peak overpressure on a structure, the pressure–distance relationships developed for TNT can be utilized for the detonation of solid substances (by expressing explosive power to equivalent amount of TNT [13]).

If the design of the plant takes into account natural fires (wildfires) then the effects of man-made external fires may have been already incorporated into PSA. The response of the structures (and auxiliary systems) depends on their capabilities for resisting heat load. Analogously the resistance of electrical systems on internal fires is a part of the design, therefore the effects of the heat may be already taken into account – however one should keep in mind that significance of external fire may be higher due to the possibility of additional effects like explosions. In general the heat or fire load from a detonation is not considered a part of the design basis for a target structure (as is considered for a deflagration), this effect should be dealt with on the same basis as fires due to other human induced events. However, particularly in the case of fuel–air mixtures, fire effects associated with a detonation may be significant, and the same provisions should be applied as for deflagrating media.

7.2.2 ACCIDENT SEQUENCES

Ideally the fragilities are used to calculate the frequencies of different event scenarios and this depends on the hazard intensity. Therefore in order to determine frequency (or probability) of the core melt and/or radionuclide release, caused by a sequence of events initiated by a human induced external event, integration over whole range of hazard intensities (or response parameter, in general) has to be performed.

Depending on the type of the hazard, various impacts on the plant have to be considered which is related to different sets of parameters to be analysed. The most important impacts and associated parameters are as follows (according to [50]):

1) Pressure waves, represented by local overpressure in function of time. Possible impact on the plant can be disruption of the systems or collapse of some parts.
2) Heat, represented by heat flux (maximum value) and duration. Limited habitability in the control system, ignition of combustible and fire or damages of the structure or components are typical effects.
3) Projectile, represented by mass, velocity, shape, size, material, structural features and impact angle. The impact on the plant is related to various types of damages of the systems and components (like disruption, spalling, perforation, collapse of the parts), and possible induction of false signal in equipment.
4) Asphyxiant or toxic substances, represented by concentration and quantity in function of time, and corresponding limits. This causes threat to people and can lead to the problems in pursuance of operator’s safety functions.
5) Smoke or dust, represented by composition, concentration and quantity in function of time. The typical impact can be blockage of intake filters and limited habitability in some rooms, including control room (e.g. Regulatory Guide 1.78, “Evaluating the Habitability of a Nuclear Power Plant Control Room During a Postulated Hazardous Chemical Release ”)
6) Corrosive and radiological liquids, gases and aerosols, represented by concentration and quantity in function of time, and corresponding limits, and provenance (sea, land). Corrosion and disruption of the sys-

tems and components on one hand, and possible problems in pursuance of operator's safety functions are typical effects on the plant.

7) Flooding or drought, represented by the level of water in the function of time, and water velocity. This can lead to damages of the structures, systems and components.
8) Ground shaking, represented by response spectrum. Typical effects are mechanical damages.
9) Subsidence, represented by settlement and displacement. The impact on the plant is represented by disruption of the systems and components or collapse of the structure (including underground pipe and cables).
10) Electromagnetic interference, represented by the energy and frequency band. This can produce false signal in electric equipment.
11) Eddy currents into ground, represented by intensity and duration. This can lead to the corrosion of underground elements.
12) Damages to water intake, represented by mass of ship, velocity and area, degree of blockage. The impact can be unavailability of cooling water.

7.2.3 DEVELOPMENT OF ACCIDENT SEQUENCE MODELS

The main objective of developing the accident sequence models is to construct an event tree structure that integrates event sequences developed in the internal events PSA and distinctive man-made hazards induced transients into a generic model that reflects the specifics of man-made hazards initiating events (for details see chapter 7.2.1). There are several approaches appropriate to fulfil this objective. In chapter 0, a series of analysis steps applied by a state of the art methodology is presented, however several, slightly different methods are used in recent PSA studies. According to the presented method, accident sequence models for man-made hazards PSA are developed in the following major steps:

- identification of SSC failure modes that can be caused by a man-made hazard as an initiating event,
- identification of transient initiating failures, mitigation system failures and damage forms that can be the consequence of SSC failure modes identified in the previous step, establishment of a list of transient initiating failures that can be induced by a man-made hazard initiating event,
- development of a generic event tree for modelling plant responses to a man-made hazard initiating event with combinations of single and multiple transient initiating failures.

This method is presented in more details in chapter 0.

7.3 LIMITATIONS AND GAPS IN EXISTING METHODS

The overall procedure, modelling principles and major analysis steps in the development of a L1 PSA model for **aircraft crash hazard** are in good agreement with that of L1 PSA in general. Taking into account a general low impact frequency, a conservative consequence modelling is mostly sufficient. However, apart from already mentioned issues in chapter 3.7.1 some specific analysis tasks can need particular considerations or even further developmental efforts, including especially the following:

- the appropriate definition of failure modes needs to be reviewed with respect to plant response and fragility analysis; in current assessment methodologies the development of fragility curves is not mature enough to take into consideration all the relevant characteristics of an aircraft crash; consequently, no continuous fragility curves are developed, especially not ones that take into account different characteristics of an aircraft crash, e.g. velocity, mass, explosion (see also chapter 8);

- there is a lack of well-established methodology on the definition of correlation among aircraft crash induced failure modes and on the quantification of correlation coefficients, e.g. induced vibrations; this analysis area also needs further development.
- there are limitations with respect to human reliability analysis applicable to an aircraft crash PSA; this aspect is discussed in more details in chapter 9.

As far as **external explosions** are concerned, the usual PSA limitations are applicable, as those induced by the used model (modelling assumptions) and completeness of the analysis (dependencies, initiators). In general, it is difficult to predict the number of generated missiles and this part of analysis will be probably based on expert judgment. Probability of affecting sensitivity target can be obtained by using geometric probability, i.e. likelihood of impact on a particular area will be uniformly distributed. Probability of target damage will be based on extent of damage as evaluated by the use of appropriate empirical formulae.

Physical processes for some types of fires and explosions need very complex models if high accuracy has to be achieved. These limitations, in practically used models, are accommodated by applying a conservative approach.

The design and operating experience have shown that the explosion hazard has effects close to and often enveloped by those of other hazard sources (such as direct impacts and wind) and therefore the use of simplified approaches, such as the TNT equivalent, is usually justified if applied in conservative, first order screening type evaluations.

The quantitative treatment of uncertainties is in general substituted by conservative estimations. The uncertainties in the external event PSA results may be addressed as in the PSA standard (ASME/ANS RA-S-2008) and associated guidance documents (RG 1.174, RG 1.200, and NUREG-1855).

8 SOLUTION TO MODEL THE EQUIPMENT SSCS FOR MAN-MADE HAZARDS AND AIRCRAFT CRASH PSA

In general modelling the SSC for man-made hazards and aircraft PSA should take into account the following basic issues:

1. Modelling of building resistance and tolerance level of the buildings, missile impact, impact on ventilation system and DGs/intakes, long term effects:
    - estimation of the responses of building and components (SSCs), electrical cables and equipment, common pathways (propagation of extreme conditions inside the building, loss of ventilation, air-conditioner, computers and electronics);
    - use of equipment qualification regarding extreme temperature i.e. high, long lasting effects, duration of the fire, vibration, explosion;
    - consequences from a failing SSC on other SSCs;
    - common cause failures.
2. Calculation of fragility or failure probability (if applicable), taking into account human' safety (high temperature, toxic gases), personal protection devices and personnel behaviour;
3. Importance of walk downs and plant specific data;
4. Uncertainty analysis.

In order to obtain the necessary level of detail it is reasonable to organize this process (at least for the first three points above) in an iterative way.

In the following subchapters detailed modelling aspects are considered for an aircraft and man-made PSA.

8.1 DEFINITION OF FAILURE MODES FOR SSCS

For each initiating event from an aircraft crash, external fire or explosion, a comprehensive list of SSCs is developed taking into account the relevant impact characteristics of the event under consideration, as well as all the failures that might have an impact on the plant, i.e. the failure of the SSCs may either induce a plant transient or disable a mitigation system. For plants in operation, a plant walk-down is indispensable to verify and refine the list of SSCs derived from analysis so that the impact of structural failures and spatial system interactions are properly considered during the identification of the relevant SSCs. In fact, for the purposes of identifying all relevant SSCs, fragility analysis and PSA modelling are mutually dependent tasks with a two-way information flow between them. Thus, the failure modes that may be due to an aircraft crash/fire/explosion are defined for each SSC identified earlier.

The identification of the relevant SSCs and their failure modes takes into account all the possible effects of an aircraft crash/fire/explosion. The following potential primary (direct) effects of an aircraft crash on a target are considered [8]:

- local structural damage: an aircraft may hit a target, causing excessive local damage (i.e., penetration and spalling, scrubbing, perforation);

- global structural damage: when subjected to the impact from an aircraft, a target may undergo excessive structural deformation or displacement (without collapse) or may structurally collapse or overturn;
- functional failure of SSCs: when a building structure is impacted, attached SSCs in close proximity to the impact location may be subjected to shock and vibration, resulting in their functional failure.

Direct effects of explosions may be structural damage due to pressure waves (as described above) or generated missiles. In case of fire, apart from possible damages of structures, auxiliary equipment (like electrical systems) can be affected. Special attention should be paid to fires associated with detonations. Their consequences can be either local or global.

With respect to secondary (indirect) effects of an aircraft crash, the following impacts are taken into consideration as a minimum:

- secondary missiles: part of an aircraft and detachment of plant SSCs (e.g. missiles from concrete scrubbing or spalling);
- aircraft fuel fire;
- explosion and shockwaves resulting from the crash;
- hazardous effects induced by an accident on a traditional industrial facility located on the site, e.g. toxic gas cloud, heat flux, pressure wave, vibration and missile impact;
- ground vibrations.

For fires and explosions it is important to realise that a fire (in many but not all cases) may cause an explosion and vice versa, hence separated and combined effects should be taken into consideration.

The most important areas with respect to identification of SSCs and the failure modes thereof are local or global structural damage and equipment failures that can cause or contribute to functional failures. It is also of prime importance to take the impact of shock and vibration on SSCs outdoor and indoor into account in the analysis.

The relevant failure modes may be identified by the use of an inductive or a deductive approach, or the combination thereof. If an inductive approach is used, then all the consequences of external events from a certain category of aircraft, fire and/or explosion, affecting an impact zone are mapped first, and the PSA relevant items are selected afterwards. The deductive approach takes a pre-defined comprehensive list of SSC failure modes as a basis and it tries to determine which might be induced by an aircraft crash initiating event. Typically, the deductive approach is followed with the use of inductive thinking to some extent, i.e.:

- the basis (initial list) is a list of failure events derived from the internal events PSA;
- plant response and fragility analysis, and failure mode identification are performed in combination and in an iterative manner to supplement the list of failure modes with failures that are not included in the original internal events PSA (new initiating events and component failure modes not credited in the internal events PSA because of the low probability of those events due to random internal failures, e.g. simultaneous opening of multiple steam generator safety relief valves in a PWR).

8.2 CATEGORIZATION OF FAILURE MODES AS TRANSIENT INITIATING EVENTS AND FAILURES IN MITIGATION SYSTEMS

In this step of PSA model development, all transient initiating failures and additional system, train or component level failures and damage forms that can be caused by the SSC failure modes identified in the previous step are determined. An illustrative example is the identification of induced plant transients and failures in mitigation systems/components caused by the structural damage of a building. The state of the art methodology assumes that all the equipment installed inside a building fails in case of a global structural damage. All components located within the impact area of a local structural damage (e.g. perforation) are assumed failed. Some guidance documents (e.g. [9]) suggest a conservative approach to assume the guaranteed failure of all the equipment within a building in case of perforation. Similarly, loss of off-site power is often assumed for all aircraft crash initiating events, and the same assumption can be made for fires and explosions (taking into account their localization). External event induced transients, which have not been taken into consideration in the internal events PSA are also defined in this analysis step. To exemplify the typical results of this analysis step Table 8-1 shows those possible failure mode consequences of aircraft crash induced possible global damage of the reactor hall steel structure in a VVER plant that are important to PSA.

Table 8-1: Transient initiating and other failures induced by the damage of reactor hall steel structure in a VVER power plant

GROUP: Reactor Hall Steel Structure
Transient initiating failure(s): • unrecoverable failure of the buffer tank of reactor coolant pump (RCP) intermediate cooling circuit → no water make-up to the RCP intermediate cooling circuit → loss of RCP intermediate cooling circuit
Failure(s): • unrecoverable failure of valves on the feeding headers of the auxiliary emergency feedwater system, rupture of the feeding lines • unrecoverable failure of hermetic isolation valves in various ventilation systems of the hermetic area (failure to close) → containment isolation failure

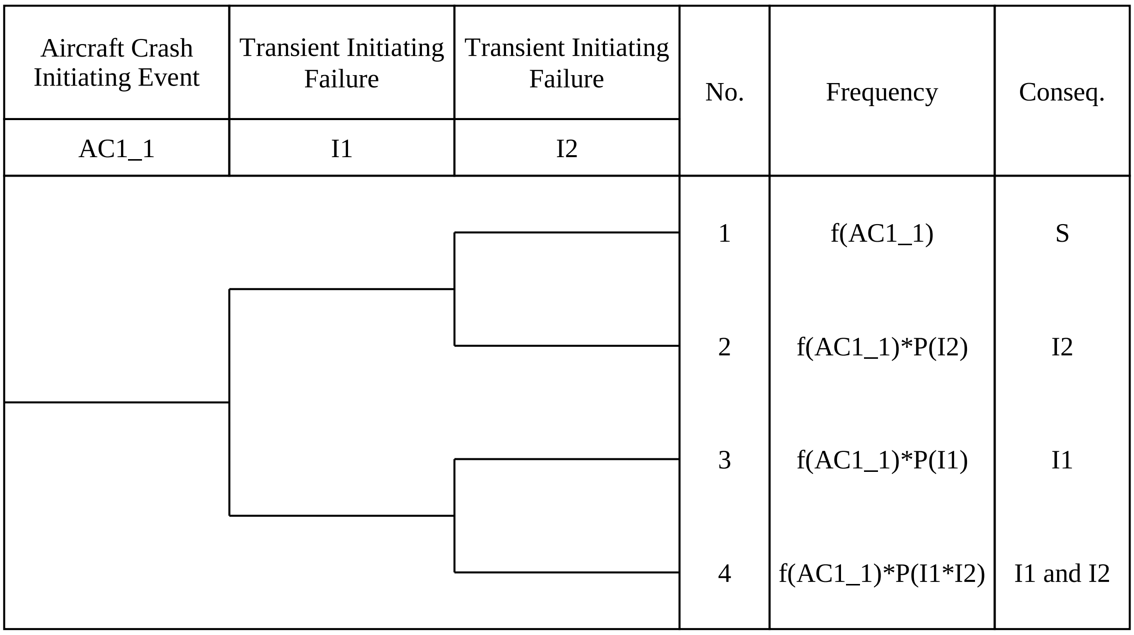
8.3 EVENT TREE CONSTRUCTION

8.3.1 INITIATING EVENTS

The simultaneous occurrence of two or more plant transients (initiating events) is in most cases screened out from a PSA for internal events due to the low frequency of such multiple events as random (not correlated) occurrences. In an aircraft crash or man-made hazard PSA however, multiple transient initiating failures need to be taken into account because such event, as a common cause initiator, may lead to simultaneous occurrences of several accident (transient) initiators. The individual transient initiators that belong to such combinations may or may not already have been considered in the internal events PSA. The systematic identification of each possible combination of impacts and the proper treatment of the correlation among these consequential failures are key elements of the man-made hazard or aircraft crash PSA modelling process. For comparison between the PSA models for external events and internal events, it is convenient to think of each possible combination of aircraft crash, fire or explosion induced failures as functionally equivalent to a distinct initiating event. In comparison to a single transient initiating failure, multiple transient initiating failures (initiators in an internal events PSA) may place different, usually higher demands and challenges on plant systems and personnel concerning accident mitigation. Moreover, the transient initiating failures caused by an aircraft crash, fire or explosion initiating event can, in principle, occur in any combination. For example, if the number of transient initiating failures that an external initiating event can cause is *n*, then the total number of different transient combinations at the onset of the accident sequence development is 2^{n}-1 as determined by the different combinations of simultaneous transient initiating failures. Theoretically, this is the number of event trees that should be built up for each aircraft crash, fire or explosion initiating event. In the state of the art practice the combinations of transient initiating failures are typically modelled by a generic event tree. That generic event tree starts with the external initiating event as initiator and then it branches off for the different transient initiating failures modelled as event tree headers. An example of this event tree structure is depicted in Figure 8-1, where:

- AC1_1 signifies the aircraft crash initiating event which is aircraft crash category 1 hitting impact zone 1;
- I1 and I2 denote the transient initiating failures caused by the aircraft crash initiating event;
- f(AC1_1) is the frequency of event AC1_1;
- P(I1) and P(I2) are the probabilities of transient initiating failures I1 and I2 respectively. It will be clear that these probabilities will have no relation to the normal frequency of the transients;
- consequence S means a state with no transient initiating failures.

Figure 8-1: Example of Modelling Multiple Transient Initiating Failures



Aircraft Crash Initiating Event	Transient Initiating Failure	Transient Initiating Failure	No.	Frequency	Conseq.
AC1_1	I1	I2			
			1	f(AC1_1)	S
			2	f(AC1_1)*P(I2)	I2
			3	f(AC1_1)*P(I1)	I1
			4	f(AC1_1)*P(I1*I2)	I1 and I2

The other consequences represent the occurrence of a single transient initiating failure (sequences No. 2 and 3) or the simultaneous occurrence of I1 and I2 (sequence No. 4).

Depending on the features of the plant design the frequency of simultaneous events I1 and I2 (sequence No. 4) may be much higher than the simple product f(AC1_1)*P(I1)*P(I2). For example, the combined likelihood of these failures may be influenced by such factors as correlation among specific component fragilities, structural failures that damage multiple systems, unique consequential impacts from the first failure, etc. Therefore, the numerical value for P(I1*I2) in sequence No. 4 may be substantially higher than the product of P(I1) and P(I2). The logic structure of the aircraft crash PSA model is developed so that such dependencies are considered explicitly and also quantification of event sequences is performed in view of these dependencies.

If there is a single transient initiating failure, then the functional response of the plant to that event is described in the same way as in the PSA for internal events: once an accident is initiated, the consequences of the transient initiating failure are supposed to be mitigated by ensuring the same functions by appropriate means (response by plant systems and/or personnel) regardless of whether the transient initiating failure is induced by a random failure or by an aircraft crash (see sequences No. 2 and 3 in Figure 8-1). Thus, one would expect that the functional event trees developed for single transient initiating failures in an aircraft crash or man-made hazard PSA are similar, if not identical, to those used in the internal events PSA. This is true, unless there are specific emergency operating procedures, or plant systems and equipment designed to respond differently to an aircraft crash, fire or explosion event as compared to the response to another random initiator. Therefore, transient identification and event tree development are performed in the following steps:

- review of the initiating event list used in the PSA for internal events, selection of initiating events (transient initiating failures) that can be induced by an aircraft crash, fire or explosion initiating event,
- examination of the selected transient initiating failures to determine whether plant responses are designed to be the same for random and for aircraft crash, fire or explosion initiating events or not,
- identification of transient initiating failures that can be induced by an aircraft crash, fire or explosion, but are not included in the PSA for internal events due to their low frequency,
- development of functional event trees for single transient initiating failures,
- development of a generic event tree for modelling plant responses to an aircraft crash, fire or explosion initiating event with combinations of single and multiple transient initiating failures.

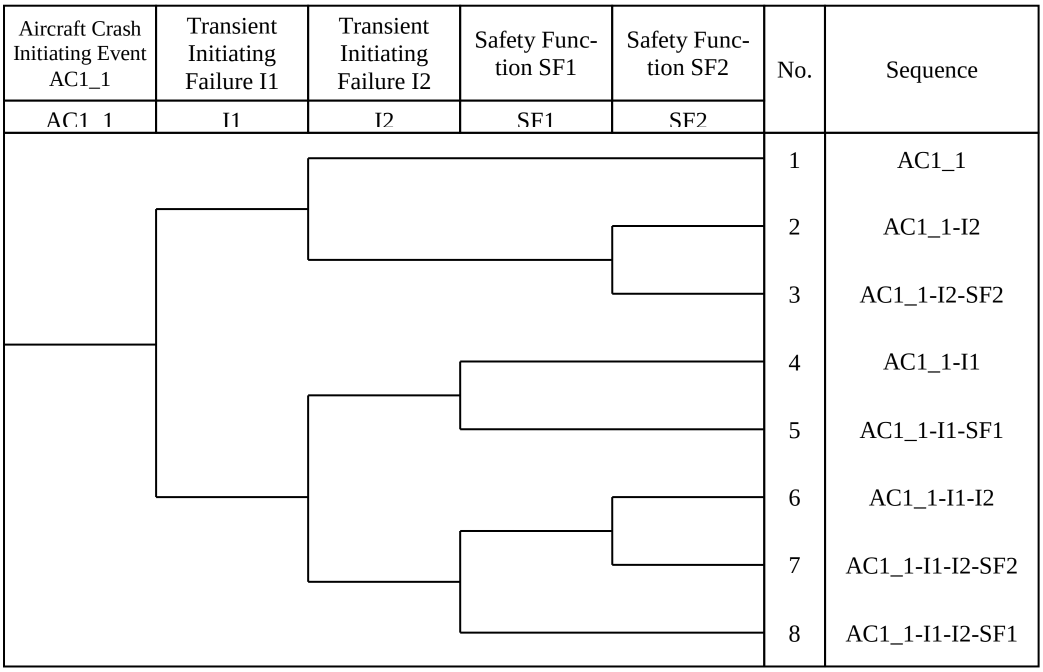
Some transient initiating failures may not be included in the initiating event list of the internal events PSA because of their low frequency of occurrence from random failure causes. Such events become important after an aircraft crash, fire or explosion, if their conditional probability is sufficiently high to give, in combination with the frequency of the external initiating event, a transient initiating failure frequency that is comparable to that of other, screened-in transient initiating failures. These transient initiating failures are also considered in the PSA model for aircraft crash events. It is important to ensure a comprehensive coverage of these and other kinds of aircraft crash specific transient initiating failures. The results of the fragility analysis are used to finalize the list of transient initiating failures in the man-made hazard or aircraft crash PSA. In addition, the importance of making use of findings from a plant walk-down is emphasized for operating plants.

8.3.2 ADDITIONAL SYSTEMS MODELLING

The next step of the analysis process is concerned with the identification of additional systems necessary for ensuring stable core cooling conditions following an external event and with the definition of success criteria for these systems. Also included in this analysis step is the identification of systems that are not safety related but their aircraft crash induced failures might impact on the operation of essential plant systems and equipment through spatial interactions. The system interactions that need to be included in the PSA model are best identified during plant walk-down. If a walk-down is not yet feasible, then design data need to be used. It is also important to identify possible new operator actions that may be required to mitigate the consequences of an aircraft crash event. Typically, these are actions not modelled in the PSA for internal events but may be needed to ensure stable core cooling conditions because of the potential adverse effects of an aircraft crash, fire or explosion. In addition, aircraft crash induced failures (e.g. blockage of access paths, extremely harsh conditions for performing local interactions, etc.) may prohibit or inhibit some operator actions credited in the internal events PSA. These actions are identified in this analysis step too.

A generic event tree (in principle this can be a copy of transient tree) is built up for a range of plant transients (with combinations of multiple transient initiating failures) in the last step of event tree modelling. The approach to developing the generic event tree takes into account the fact that the information about plant responses to multiple transient initiating failures is limited. The scope of safety functions that should be fulfilled following the occurrence of multiple transient initiating failures is assumed to be a union of the safety functions modelled for single transient initiating failures. Consequently, no additional safety functions need to be introduced to delineate the structure of the generic event tree. The generic event tree is then built up in accordance with the illustrative example given in Figure 8-2 (as an extension to the previous example shown in Figure 8-1). This figure includes two safety functions, SF1 and SF2 that need to be ensured following the occurrence of (single) transient initiating failures I1 and I2, respectively.

Figure 8-2: Example of a Generic Event Tree Structure



In practice the approach taken to developing the generic event tree corresponds in principle to the theoretical one described above. For practical reasons, a possible representation of the model is the use of a single generic event tree header as the last header after the headers for the transient initiating failures, as opposed to listing the safety function failures as event tree headers one by one. This last header combines all the core damage event sequences from all the single transient initiating failures. This way the number of sequences in the generic event tree can be reduced significantly, and the logic of the model can be kept unchanged (as compared to the theoretical approach described above) at the same time. Hence, a simple reading of such a generic event tree structure is that the upper branch represents (as usual) the success of an event tree header (the given transient initiating failure does not occur), while the lower branch represents the failure of the given event tree header (occurrence of the given transient initiating failure). The last header combines failures of all the mitigation functions and the associated SSCs as mentioned above.

The development of the generic event tree should not be a mechanistic application of the modelling approach. If the generic event tree is built up mechanistically, then the number of the event sequences would be 2^{K+1}, where K is the number of potential transient initiating failures, and there is one additional (last) header of mitigating systems mentioned above. This may result in a large number of event sequences that are difficult to manage. However, in actual applications there are usually some possibilities to reduce the number of event sequences.

8.4 FAULT TREE DEVELOPMENT

Fault trees are constructed to adequately describe the logical combinations of equipment failures and human errors leading to the failure of safety systems to fulfil their intended functions as well as the occurrence of explicitly defined transient initiating failures. Similarly to the internal events PSA, this is one of the largest efforts in the man-made hazard or aircraft crash PSA too. On one hand logical OR gates combine, in an appropriate logic, those aircraft crash induced failures that result in a transient initiating event specified in chapter 8.2. The system models of the internal events PSA are a good starting point for developing fault trees for the aircraft crash or man-made hazard PSA with respect to availability of the safety functions. The existing system fault trees are extended and modified for the purposes of the aircraft crash analysis. Most importantly, the following tasks are performed to develop system fault trees[3] so that they can be appropriate for use in the aircraft crash/man-made hazard PSA:

- inclusion of induced causes of component failure modes modelled in the PSA for internal events,
- addition of new, externally induced component failure modes that are not included in the PSA models for internal events due to their low probability,
- modelling of dependent failures,
- modelling of induced failures of structures, and failures from spatial system interactions.

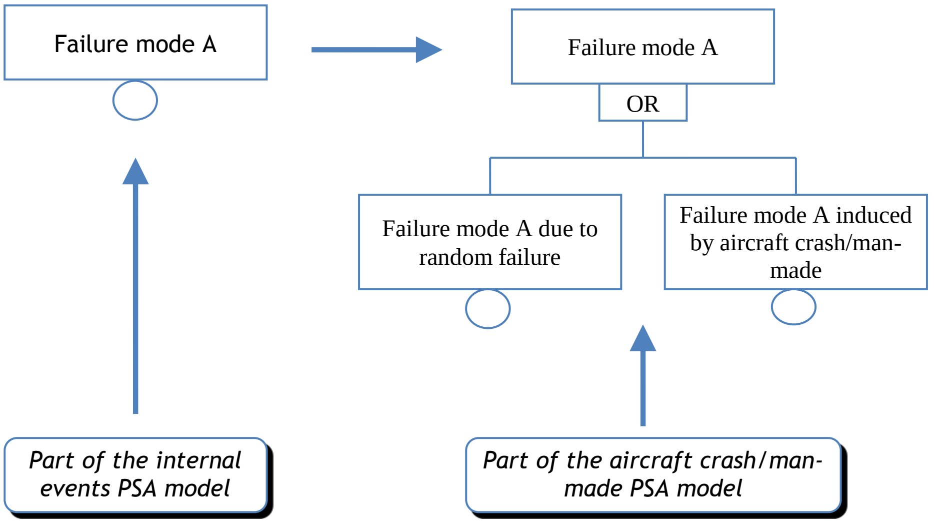
The first two steps above are concerned with supplementing the PSA model with “new” failure events, while the last two ones with modelling of different types of dependencies between equipment failures.

A lot of the failure modes considered in the PSA for internal events can be induced by an aircraft crash, fire or explosion, too. As a first modelling step the failure modes that are susceptible to externally induced failures are listed. Thus a failure mode included in this list can occur as a consequence of an aircraft crash/fire/explosion, or due to random effects independent of the event considered. For these failure modes the basic events in the internal events PSA model are transferred into an OR gate that defines the logical connection between the two types of failure causes (i.e. aircraft crash related or not) for the same failure mode as illustrated in Figure 8-3.

[3] The question whether these tasks are implemented or can be included in available software tools is not considered.

Figure 8-3: Transfer of Failure Modes

to Include Aircraft Crash/Man-made Induced Component Failures


Failure mode A
Failure mode A
OR
Failure mode A due to random failure
Failure mode A induced by aircraft crash/man-made
Part of the internal events PSA model
Part of the aircraft crash/man-made PSA model

This type of modification can, in principle, greatly increase the size of the fault trees through duplicating the number of basic events. Furthermore, the probability of externally induced failure modes changes from one initiating event to another (for example to aircraft category, impact zone), which requires the inclusion of new basic events to represent the same type of induced failures with different failure probabilities for the different external initiating events. Fortunately, not all of the basic events of the internal events PSA have to be duplicated. For example, some basic events describe maintenance errors that are not affected by an aircraft crash, fire or explosion, and thus these entities should not be modelled repeatedly within the list of aircraft crash, fire or explosion induced failures. If there are *N* basic events from the internal events PSA that can be induced by an external event, and the number of initiating events is *M*, then the total number of basic events that are added to the aircraft crash/man-made hazard PSA model is *N*×*M* as given in Table 8-2 (where FMij denotes failure mode *i* in initiating event *j*). However, the number of basic events to actually build into the system fault trees can be just *N*. The so-called exchange events, as a built-in feature of most PSA codes, can be used for replacing a basic event with other basic events that represent the same aircraft crash, fire or explosion induced component failure but with different probabilities of failure for the different initiating events. A boundary condition (house event) is defined for the event tree(s) related to a given initiating event, and the basic events that describe the induced component failures are exchanged by setting the same boundary condition to TRUE. Using the example of Table 8-2 it means that only the failure modes in the first column are built into the fault trees. The failure modes belonging to the other external initiating events are modelled as exchange events to these built-in failure modes set by appropriate boundary conditions. The assumptions made on the dependencies between aircraft crash, fire or explosion induced failures and the results of fragility analysis can also be used to significantly reduce the number of basic events that need to be added to the existing fault tree models - see also a discussion on this issue later in this chapter. Further, it is often possible to add aircraft crash, fire or explosion induced failures at a higher level in the fault trees than the component level basic events. Overall, appropriate considerations to all these factors can substantially reduce the number of new basic events that need to be added to model the aircraft crash, fire or explosion induced failures.

Table 8-2: New Principal Basic Events of the Aircraft Crash/Man-made PSA

		Aircraft crash/man-made initiating event					
		1	2	...	*j*	...	*M*
Failure mode of IEPSA[*] susceptible to aircraft Crash/man-made hazard	1	FM_{11}	FM_{12}	...	FM_{1j}	...	FM_{1M}
	2	FM_{21}	FM_{22}	...	FM_{2j}	...	FM_{2M}
	...	...	...		...		...
	i	FM_{i1}	FM_{i2}	...	FM_{ij}	...	FM_{iM}
	...	...	...		...		...
	N	FM_{N1}	FM_{N2}	...	FM_{Nj}	...	FM_{NM}

[*] - IEPSA = Internal Events PSA

In addition to supplementing the existing failure modes in fault trees of the internal events PSA with similar but aircraft crash, fire or explosion induced failure modes, it is also necessary to incorporate some failure modes that are not at all included in the PSA for internal events. These are failure modes screened out from the internal events PSA because of their negligible probability as random failure events. However, they may become an important contributor to aircraft crash/man-made related risk if caused by the event with a sufficiently high probability. Representative examples are:

- spurious opening of valves that constitute the pressure boundary of a mitigating system,
- spurious closure of a valve on a pipeline that is necessary for the delivery of coolant, and,
- failures of system piping.

The identification of these failure modes requires a complete review of the existing fault tree models. This should be done by considering all basic events representing safety related SSCs and by determining if they may have any additional failure modes due to an aircraft crash, fire or explosion. Moreover, the results of plant response and fragility analysis as well as the observations of plant walk down should be taken into consideration in this analysis step. Newly defined basic events should be incorporated into the model based on this information to all necessary places. The identified new failure modes are subsequently incorporated into the fault trees in appropriate failure logic in accordance with the standard approaches to fault tree development.

Dependent failures are those multiple failure events, whose simultaneous occurrence probability cannot be calculated by simply multiplying the individual event probabilities as in the case of independent events. Several categories of dependent failures are taken into account in the internal events PSA, e.g.:

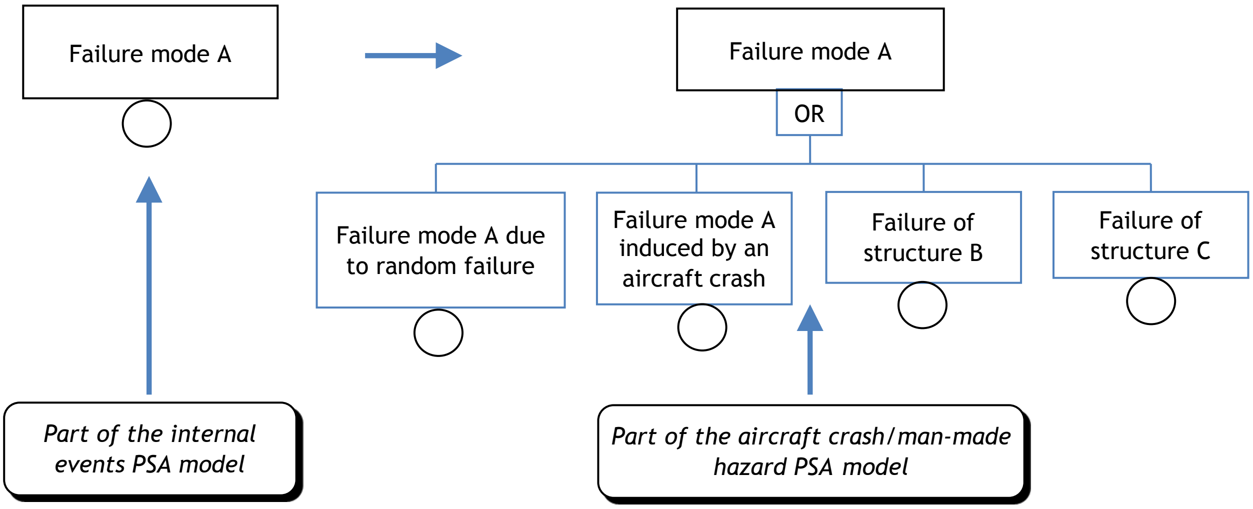
- functional dependencies,
  - time dependent events,
  - structural dependent events,
- physical dependencies,
- human interaction dependencies,
- residual dependencies.

Modelling and quantification of dependencies varies for the different categories of dependent events. Some of them are modelled explicitly, others implicitly. In both cases, commonly used methods and internationally acknowledged guidelines are taken into account. In addition to the dependencies considered in the internal events PSA, two specific types of physical dependence are also taken into account in the aircraft crash/man-made hazard PSA: dependence due to correlated aircraft crash, fire or explosion induced failures, and dependence due to failures of structures or spatial system interactions. These dependencies should be identified by taking into account the results of plant response and fragility analyses, as well as the observations of plant walk downs.

The calculation of cut set probabilities/frequencies presents one of the most fundamental differences between an aircraft crash/man-made hazard PSA and internal events PSA. In an internal events PSA component failures within a minimal cut set are usually treated as independent events. The dependencies among independent events are modelled by an appropriate parametric common cause failure model. Consequently, the probability/frequency of a cut set is evaluated by simply multiplying the random or common cause failure probabilities of each element of that cut set. In an aircraft crash/man-made hazard PSA, the component failures involved in a cut set may be correlated through their respective responses and fragilities. The calculation of the probabilities (frequencies) of cut sets containing correlated events involves multivariate integration of the joint probability distribution function of the cut set elements. This integration tends to increase the complexity of the calculation without sufficient justification of the numerical values of correlation coefficients between the different random variables for aircraft crash, fire or explosion induced failures. In order to avoid such an unnecessarily complex quantification a two phase screening process is usually followed with regards to the treatment of correlated events. Two types of correlation are considered in the first phase: no correlation or complete correlation. Separate basic events are used in the PSA model if no correlation is assumed due to markedly different characteristics of component response and fragility. If events are modelled as fully correlated due to similarity in aircraft crash/fire/explosion related response and fragility, then use is made of exchange events mentioned earlier. The correlated basic events that describe different aircraft crash/fire/explosion induced failures are exchanged by the same boundary condition, so the correlated events are replaced with a single basic event. Using the example of Table 8-2 this means that some failure modes of the first column are exchanged to the same failure mode, so if e.g. failure modes 2 and *i* are (fully) correlated, then events FM_{22} and FM_{i2} should have the same identifier. This approach leads to a reduction in the number of basic events that are multiplied for the different aircraft crash, fire or explosion initiating events. After finishing the first phase of the analysis correlated induced failures that appear to be significant are re-examined, and refined correlation coefficients are assigned to them (if necessary and justifiable) based on the results of fragility analysis. The quantification of multivariate distributions with correlated random variables is performed for these refined correlated events.

Dependence is introduced by the failures of structures and by the effects of spatial system interactions. Such failures are not included in the PSA model for internal events but they may be very important in the aircraft crash/man-made hazard PSA. In addition to design data, use is made of plant walk-downs in operating plants to identify such structural failures and spatial interactions, whereas the probabilities of these effects are determined by fragility analysis. Since these failures usually cause damage to several essential plant components, they represent a very important, often dominant type of dependence. This dependence is very similar to functional dependency (in terms of its consequences). It is often modelled explicitly by assigning a single basic event to all those components that are affected by the dependency under an OR gate. That single basic event represents the failure of a structure or the failure due to a specific spatial interaction. Figure 8-4 is an extension of Figure 8-3, and it shows that the same failure mode can be induced by a number of different causes. In order to model the given dependency correctly the same basic event is assigned to all the basic events affected. It also implies that it is not necessary to actually include the new basic event at the level of each affected component because a logic gate can typically be found at a higher level of the fault tree hierarchy where the required basic event can be placed (although this is not in accordance with normal fault tree development).

Figure 8-4: Scheme for Modelling Specific Aircraft Crash/Man-made Related Dependencies


Failure mode A
Failure mode A
OR
Failure mode A due to random failure
Failure mode A induced by an aircraft crash
Failure of structure B
Failure of structure C
Part of the internal events PSA model
Part of the aircraft crash/man-made hazard PSA model

The analysis of external man-made or accident aircraft events may deal with many different uncertainties. Insufficient understanding of the properties and failure modes of structural materials, imperfect models, and the use of generic data and engineering judgment in the absence of plant specific data are typical sources of uncertainties in the evaluation of component fragilities. One of the methods for propagating uncertainties is an iterative approach consisting of the two elements. In the first one, for each component the best estimate hazard and fragility curves are determined. In the second one, basing on probability distributions of the hazard and fragility curves, samples are generated (perturbation step). These samples are applied again in order to determine the hazard and fragility curves for perturbed data. Analogously the uncertainties can be treated for the frequency of core melt and various types of radiological releases, as well as damages. This approach can be quite expensive, therefore it seems reasonable to make an attempt to identify dominant accident sequences and perform analysis for them. Whatever approach is used in order to quantify uncertainties in hazard analysis and evaluation of component fragility, they should be treated in a consistent way and propagated through all the steps of analysis.

8.5 ANALYSIS OF INPUT RELIABILITY DATA

The numerical input data necessary for quantifying accident sequences consist basically of data needed to calculate the frequencies/probabilities of basic events included in the PSA model. This information need is dependent on the underlying component (basic event) reliability models applied generally as follows:

- Initiating Events
  - a) frequency - f (1/y)
- Independent Component (Hardware) Failures
  - a) time related failure rate - λ (1/h) or
  - b) demand related failure rate or probability of failure per demand – λ_d or Q or P (1/demand)

c) time data on operating hours, test and repair, as appropriate (mission time: T_{mis} (h), repair time: T_{rep} (h), test interval (time between tests): T_{per} (h), test time: T_{test} (h))

d) aircraft crash/fire/explosion induced failures, fragilities – P (failure probability)

- Dependent (Common Cause and Correlated) Component Failures

  a) data on independent failures for each component involved in a common cause failure (CCF) group - see above

  b) parameter values for the fraction of common cause failures in a CCF group in accordance with the underlying parametric CCF model applied (e.g. ß factors, α factors, MGL factors)

  c) correlation coefficients for multiple, correlated failures of SSCs: ρij.

- Human Errors

  a) probability of an human error: HEP.

The frequency of an aircraft crash, fire or explosion initiating event is characterized by the annual frequency of each aircraft type hitting each relevant impact zone. The frequency is characterised by its mean value and by expected frequencies for a range of confidence levels or by a continuous probability distribution. The hazard characteristics are obtained from the aircraft crash, fire or explosion hazard assessment as input information for the aircraft crash/man-made hazard PSA, therefore there is no need to describe the methodology of aircraft crash/fire/explosion hazard assessment in this chapter – see chapter 3 for the details of hazard assessment.

The reliability data for random equipment failures are taken from the PSA for internal events. Additional reliability parameters also need to be estimated for quantifying random failures included in the system fault trees developed newly for the purposes of the aircraft crash/man-made hazard PSA. The method of parameter estimation follows the practice commonly applied in the internal events PSA.

Aircraft crash, fire or explosion induced failures of equipment and structures, including transient initiating failures and mitigating system failures, are modelled by different basic events in the logic model for the different aircraft crash/fire/explosion initiating events. The probabilities of these failures are determined by fragility analysis. The fragility analysis quantifies the likelihood that a component or structure fails, as a function of the aircraft mass and velocity relevant to an investigated aircraft type hitting an impact zone at the plant. Similarly for fires and explosions fragility is estimated in function of strength of the explosion (for example expressed in TNT terms), duration of fire, etc. The fragility analysis explicitly accounts for the effects from randomness of the aircraft crash characteristics and uncertainty in the component response to a particular aircraft crash, fire or explosion initiating event.

With regards to common cause failures of plant equipment the data available in the internal events PSA is used without modification for the purpose of the aircraft crash/man-made hazard PSA. It is important to note that these are common cause failures of random failure events as opposed to dependent failures due to aircraft crash, fire or explosion effects. The approach applied in the internal events PSA is followed to estimate the common cause failure parameters of the random equipment failures modelled newly for the purposes of the aircraft crash/man-made hazard PSA.

The approaches to estimating human error probabilities for different initiating events are summarized in chapter 9.

9 SOLUTION TO MODEL HRA FOR MAN-MADE HAZARDS AND AIRCRAFT CRASH PSA

9.1 BACKGROUND

External events may lead to harsh personnel working conditions, problems in getting external aid and increases in emotional burden (site isolation as consequence of a fire, worrying about the situation of family members, adverse conditions for countermeasures requiring working outdoors). Several documents [20], [27] acknowledge that the effects generated by external hazards could have the potential to adversely impact the plant safety and the response of plant personnel (e.g. the possibility of implementing emergency procedures could be affected; the operator access could be impaired). More detailed information on treatment of HRA and on HRA models is available in case of seismic events or internal fire events. For the other external hazards, the literature with regard to HRA is not well developed [27].

Regarding the assessment of human factors, some general recommendations can be summarized from the related literature [27]:

- HRA should adequately account for the additional influences caused by the external event,
- human failure events adopted from an Internal events PSA should be modified as appropriate to reflect the external hazard effects,
- new human failure events should be included to account for specific hazard related actions that are consistent with plant procedures that were not covered in the Internal Events PSA.

There are several international efforts dedicated to improve HRA methods, such as the International HRA Empirical Study [21], where the human actions performed by operator crews (at the Halden Reactor Project simulator) were analysed using different HRA methods and the results were compared to crew simulator performance in an effort to benchmark HRA methods using empirical data. In Germany, the effects of external events on the reliability of human actions are not explicitly considered in the PSA. However, the HRA takes into account the potentially different environmental conditions affecting the human behaviour in case of an external hazards (EE) [9]. In Slovakia increased human error probabilities are used after occurrence of EE and higher level of dependencies between the human errors are applied [20]. In Chinese Taipei, the human error probabilities used in internal event analysis were increased by factor 3, following a suggestion to take into account for special stress of operating crew and possible damage (or blockage) to the pathway from control room area to other areas where the components are located [20]. In the USA, some of the “second generation” methods (e.g., ATHEANA) place a heavy emphasis on the description of the context for operator actions, and on the potential of challenging situations to increase the likelihood of error [20]. ATHEANA [51] is based on a multidisciplinary framework that considers both the human-centred factors (e.g., human-machine interface, procedures content and format, training) and the conditions of the plant that give rise to the need for actions and create the operational causes for human-system interactions (e .g., misleading indications, equipment unavailability, and other unusual configurations or operational circumstances).

In the existing documentation whether or not the increases in error probabilities are used, besides the general statement that the basis for decision about what error rates to be used should be justified, the basis for determining these increases is not well developed. It may be concluded that the PSA for external hazards should take account the potential for human response to be affected by the external event, and the available time for operator intervention for mitigation of external event effects needs to be considered. The additional stresses that can increase the likelihood of human errors or inattention should be examined, and compared to the likelihood assigned in the internal events HRA, when the same activities are undertaken in non-hazard accident sequences.

9.2 CONSIDERATIONS ON APPLICABILITY OF CURRENT HRA METHODS

After an external initiator two contributions should be considered in HRA: the success of operators to follow related emergency procedures, and the success of improvised recovery actions for human and equipment failures, in opposition with inadvertent and erroneous actions having the potential to worsen the situation. HRA is currently still not capable to model adequately the human ability to adapt, innovate and manage under extreme situations.

No specific methods have been proposed up to now for modelling the impact of external hazards on the quantification of human factor in the EE PSA. The impact of external events on the quantification of human factor in the external events is in general based on the “extension” of the existing Human Reliability Analysis (HRA) methods, with the idea that the assessment of human error probabilities for external hazards should follow the basic assumptions from PSA for internal events that will be tailored on external hazard conditions. As results, more pessimistic factors in the HEP quantification, or rough modification of the quantified HEP is used [20]. To define the human interactions, similar stages as those used in SHARP-1 methodology [52] can be used:

- definition and modelling of human interaction events;
- quantification of human failure events (HFEs);
- recovery analysis;
- review.

Consistent with PSA tasks, the HRA stages are intended to emphasize the integration of the HRA into PSA model, with a special focus on the dependencies that exist between human interactions and other events. The four stages should be performed iterative, rather than in a stepwise manner.

9.2.1 DEFINITION AND MODELLING OF HUMAN INTERACTION EVENTS

The most important objectives of this stage are the following:

- to provide an understanding of the context of human interaction analysis;
- to understand the impact of the human interactions on accident sequence development;
- to incorporate the human interaction events into the plant logic models.

Post-initiator operator response can be divided into four stages: detection of a critical situation, diagnosis of the situation, deciding on the necessary actions, and implementation of these actions.

The human interactions could be very scenario-dependent, related to actions dictated by plant operating procedure or related to recovery of failed equipment, establishing cross-connection within units, repairing the equipment, etc. The human interactions could be incorporated in the PSA model in the definition of initiating event and in accident sequence development. The interaction ways will be a function of the various conditions that can occur, as defined by the development of the PSA accident sequences and associated equipment unavailability and failure modes. Some of the operator actions may be performed immediately and without regard to the specific situation, while others will be dependent on the plant status and cues. Each specific post-initiator HFE should be modelled in PSA to accurately represent the failure of each action identified. This involves: modelling of the HFEs as human-induced unavailability of functions, systems, or components consistent with the level of detail in PSA accident sequences and system models, possible grouping of responses into one HFE, and ensuring that the modelling reflects the specificity of plant and accident sequence.

In conditions of external hazards occurrence, a thorough check and associated adjustment should be performed in relation to recovery actions and probabilities of human errors. All human actions should be revisited, but depending on the time between initiating event and the moment the action has to be performed, it should be examined if the situation is already normalised again. For instance most fires will be extinguished within 1 or 2 hours, which means that smoke will not interfere with actions after about 4 hours, or accessibility could be restored already. In general only actions within a certain time frame need adaption (the time frame depending on the location where the action has to be performed) and adjusted for the specific external hazard conditions. As a minimum, the following induced effects on the operators' performance shaping factors should be taken into account:

- availability of pathways to specific structures, systems and components after an external hazard occurrence;
- increased stress levels; compared to accident scenarios caused by internal initiating events, the operators stress levels and conditions in the plant may differ considerably after an external initiating event;
- failures of indication or false indication;
- failure of communication systems.

Recovery actions that cannot be performed due to the impact of external hazards of certain magnitude should be removed from the Level 1 PSA model or probabilities of failure performing the action should be increased.

9.2.2 QUANTIFICATION OF HUMAN FAILURE EVENTS

This stage provides as output the probabilities of human interaction basic events (HEPs) for each of HFE, the uncertainties of estimations and whatever revisions to the models are needed to properly account for the final definitions of the human actions to be modelled.

The probabilities may be quantitative screening values, or the results of a detailed evaluation. There are likely to be interdependencies between the individual human failures events included in the logic model. Such interdependencies could arise from the use of a common cue or procedural step, incorrect procedures, an incorrect diagnosis or a plan of action in carrying out response actions, etc. Dependencies among human failure events in the same sequence, if any, can significantly increase the human error probability, and they should be identified and quantified in the analysis. Proper consideration of the dependencies among the human actions in the model is necessary to reach the best possible evaluation of both the relative and absolute importance of the human events and related accident sequence equipment failures. Whether it use conservative or detailed estimation of the post-initiator HEPs, the evaluation should include both diagnosis and execution failures. Diagnosis tasks consist of reliance on knowledge and experience to understand existing conditions, planning and prioritizing activities, and determining appropriate courses of action. Criteria for selecting or modifying the HRA models include availability of data, experience of the user with the model, importance of the action being modelled and the correspondence between the key influence factors identified for the human interaction and parameters used as input to the quantification model (e.g. such as the time available to complete the action). Some performance factors may affect the decisions taken, while other influence factors will affect only the value of the human interaction probabilities. If the importance of certain PSFs (performance shaping factors) in not recognized in stage 1, the plant model should be revised to account for additional scenario dependencies on human interactions which were not considered previously.

9.2.3 RECOVERY ANALYSIS

The recovery actions are identified for the scenarios, judged as feasible, explicitly defined and quantified. This action accounts for other reasonable actions the operators might take to avoid severe core damage and/or a large early release that are not already specifically modelled. The failure to successfully perform such actions would subsequently be added to the accident sequence model thereby crediting the actions and further lowering the overall accident sequence frequency because it takes additional failures of these actions before the core is actually damaged. Usually, the possibilities to worsen an accident by the operators, as the possibilities to perform recovery actions unplanned are omitted from the model. The following issues should be considered in defining appropriate recovery actions:

- whether the cues will be clear and provided in time to indicate the need for a recovery action,
- whether the recovery is a repair action of a failed equipment,
- whether sufficient time is available,
- whether sufficient crew resources exist to perform the action,
- whether there is procedure guidance to perform the action,
- whether the crew has trained on the recovery action including the quality and frequency of the training,
- whether the equipment needed to perform the action is still accessible and in a non-threatening environment/ location.

The influence factors may not only increase the time to complete the tasks but also cause unsuccessful recoveries. The possibility to use mobile equipment (pumps, DGs) should be considered. Another important point in modelling equipment restoration is the consideration of shared resources in case of multi units, i.e. management difficulties, sharing of human resources and equipment.

9.2.4 REVISION

This step includes revisiting the validity and completeness of the results obtained in the first stages of the procedure. The authors consider that the general procedure and the major analysis steps in HRA within a PSA for man-made hazards are actually in good agreement with that of HRA in general. However, some specific analysis tasks need particular attention or even further developmental efforts, especially regarding the identification of external performance shaping factors. During the ASAMPSA_E end-user workshop held in Uppsala, it was recommended that the project shall examine how to improve HRA modelling for external hazards conditions to tackle the following issues [27]:

- the high stress for NPP staff,
- the number of tasks to be executed by the NPP staff,
- the impossibility, for rare events, to generate experience or training for operator actions (no observation of success/failure probability (e.g. simulator)),

- the possible lack of written operating procedures,
- the possible wrong information in the MCR or maybe the destruction of the MCR,
- the methodologies applicable to model mobile barrier installation (for slow developing events),
- the methodologies available to model the use of mobile equipment (pumps, DGs) and conditional failure probability (human and equipment),
- the methodologies applicable to model equipment restoration (long term accident sequences, specific case of multi-units accidents).

In the following chapters, the authors discuss the analysis areas that need specific attention, and the challenges in treating the topic.

9.3 SPECIFIC ANALYSIS TASKS

9.3.1 OVERVIEW OF TASKS

As presented in 9.2, the general procedure, modelling principles and major analysis steps in HRA within a PSA for man-made hazards are actually in good agreement with that of HRA in general. Specific analysis tasks that need particular considerations or even further developmental efforts are presented in this chapter by going through the major analysis steps one by one. This chapter is structured according to the two main tasks of HRA: 1) identification of human failure events (HFEs) and 2) quantification thereof. In addition, qualitative analysis is discussed in a stand-alone sub-chapter. Qualitative analysis is an essential part of HRA, although not always explicitly described as a separate step in the HRA process since it belongs to both identification and quantification of HFEs. However, special attention is paid to the qualitative analysis in this report due to its importance in HRA for man-made hazards.

The aim of this chapter is to discuss the specificities of the state-of-the-art concerning HRA in a man-made hazard PSA. Existing guidance documents on HRA were reviewed to select the ones considered most appropriate for the purposes of HRA for man-made hazards. It was concluded, that there is no guidance in place specifically on HRA for man-made hazards. However, the guidelines on fire human reliability analysis (NUREG-1921, [53]) developed by cooperation of the Electric Power Research Institute (EPRI) and the U. S. Nuclear Regulatory Commission (U.S. NRC) were found to be a suitable basis for man-made hazards HRA. A practical approach to HRA for man-made hazards, which primarily adapts the methodology presented in [53] for fire events, considered appropriate and practical to follow, is proposed in this chapter. The guiding methodology has been customized to take a good account of the unique characteristics of human induced external events that need to be considered in the specific area of HRA. It should be noted, that the proposed approach is regarded relevant to man-made hazards in general, although hazard specific characteristics have to be considered in the application of the proposed methodology to certain hazards (i.e. external fire and explosion and aircraft crash).

9.3.2 SELECTION OF HUMAN FAILURE EVENTS (HFES)

9.3.2.1 HFEs to consider

The aim of this chapter is to describe the formulation of high level HFEs as typically represented in a PSA model rather than a decomposition of PSA events into lower level human failures. In this sense the selection of HFEs is concerned with:

- the identification of operator actions and associated instrumentation necessary for the successful mitigation of accident sequences induced by a man-made external event, and,
- the definition of HFEs at an appropriate level of detail,

so that a meaningful qualitative analysis and subsequent quantification can be performed.

The identification of post-initiator HFEs in man-made hazards HRA is primarily based on the instructions in normal emergency operating procedures (EOPs) and/or abnormal operating procedures (AOPs) as well as in specific emergency procedures applied specifically to respond to (man-made) external events as compared to the responses to other (typically internal) initiators and plant disturbances. Although the latter ones are not always in place, the methodological description presented here assumes and accounts for the availability of such a procedure. (If such procedures are not in use, then the proposed approach should be used with appropriate considerations to this fact.)

The following three types of man-made hazard related post-initiator operator actions are considered and discussed in this chapter:

- internal events operator actions,
- operator actions in response to man-made hazards,
- undesired operator responses.

After the operator actions have been identified and the HFEs defined, it needs to be determined which operator action is feasible. This is considered as preliminary qualitative screening that is also part of the selection process (see chapter 9.3.2.5).

9.3.2.2 Selection of Operator Actions from Internal Events PSA

Several HFEs are already defined and included in the internal events PSA, so it is not necessary to repeat this selection step. In the man-made hazards HRA, all those HFEs that can occur after a human induced external event are determined. This is done by considering the plant transients triggered by the external event and the corresponding fault trees and event trees from the internal events PSA. The following steps are taken to select all relevant operator actions from the internal events PSA:

- identify all operator actions included in the internal events PSA;
  (this is generally a data extraction from internal events PSA based on basic event IDs or descriptions)
- screen out HFEs not related to man-made hazards;
  (as a first step all pre-initiator events are eliminated from further evaluation; moreover, HFEs not related to mitigation of man-made hazards induced transients are excluded from detailed assessment; this task is based on the results of plant response and fragility analysis, as well as on the decomposition of man-made hazard induced failure modes into transient initiating events and failures in mitigation systems)
- review man-made hazards related fault trees and event trees;

(it is assumed that the internal events PSA model is comprehensive and is in agreement with state-of-the-art methodologies and good practices; a review of the man-made hazards related fault trees and event trees is needed to ensure that internal events actions are still modelled appropriately; this review may identify actions that are not modelled in the internal events PSA but are needed for the man-made hazards PSA; these are procedural actions that were not considered important for the internal events model because of a low probability of associated component failures)

- define each internal events HFE for use in man-made hazards PSA;
(the human failures in response to a man-made hazard are defined to represent the impact of the human failures at the function, system, train, or component level as appropriate).

9.3.2.3 Identification of Operator Actions in Response to Man-made Hazards

Operator actions in response to man-made hazards are new post-initiator operator actions required to mitigate the consequences of a human induced external event. These actions can either be directed by the normal EOPs or by procedures related to external (man-made) hazards. Such operator actions are identified by a systematic review of the procedure(s) used under the circumstances of a man-made external event. To understand which response actions are desired in the man-made hazards PSA, it is necessary to first understand the scenarios, which may require modelling of the impacts of a man-made hazard on equipment and instrumentation in the PSA.
The following different types of response actions are distinguished based on their function in the man-made hazards PSA:

- actions to mitigate the expected consequences of equipment damage induced by man-made hazards;
These actions are intended to mitigate the effects of equipment damaged or degraded due to man-made hazards; each part of the plant that is affected by a man-made hazard is first analysed to identify all equipment in that area that are potentially damaged by the external event; this analysis step actually belongs to the plant response analysis in man-made hazards PSA; given equipment damage due to a man-made hazard is identified, the EOPs applicable to the relevant scenario(s) are reviewed to identify any response actions that can be credited for mitigation; an example for these kinds of actions is the opening of a level control valve using a local hand wheel after the man-made hazard has caused remote control unavailability.
- pre-emptive actions to prevent man-made hazards induced damage to equipment (protect equipment) relevant to PSA;
Most pre-emptive man-made hazards related HFEs involve failures to de-energize power supplies or disable control systems in order to prevent spurious actuations; these actions are typically performed following either the detection of a man-made hazard (e.g. an alarm goes off) or the confirmation of an accident locally (e.g. the operator sees flame or significant smoke), depending on the procedure; as such, the action is intended to occur prior to significant damage; as an example for the case of fault clearance, operator actions may be required within the special EOPs to manually check or position valves by “resetting” all electrically controlled valves and then manually “realigning” selected valves in a single cooling train; operator errors during either the reset or realignment steps are assumed to leave key valves and components modelled in the PSA in the wrong position and are therefore included as HFEs.

- actions recovering PSA sequences or cut sets;
  For scenarios in which the internal events operator actions are assumed failed because of impacts from man-made hazards on the instrumentation or equipment, additional actions may be credited in the analysis; these actions could also be procedural in some relevant procedures; however, non-procedural actions can also be taken into consideration if justifiable by operator training, crew knowledge and experience, availability of additional human resources or any other factors that can favourably influence the recovery potential; recovery actions may include replacement or modification of components.
- main control room (MCR) abandonment actions;
  A man-made hazard may induce such conditions at the plant, that operators are forced to abandon the MCR; generally, there are two criteria for MCR abandonment: the MCR is inhabitable (because of toxic gas, smoke, heat, etc.) or the plant cannot be controlled from the MCR (e.g. due to missile impact or direct fire damage); the same identification process applies as that for other response actions discussed earlier, but the procedure review would be limited to the EOPs that apply to
  - the decision to abandon the MCR;
  - establishing control outside of the MCR, and;
  - performing both command and control functions and actions taken outside of the MCR.

9.3.2.4 Identification of Undesired Operator Responses

For man-made hazards HRA, an undesired action is defined as a thoughtful intentional operator action that is inappropriate for a specific context and that unintentionally aggravates the scenario (i.e., an error of commission). In principle, aggravation is measured by an increase in the conditional probability of a severe accident (core damage) due to the given response in comparison to not taking action. Undesired responses consist primarily of shutting down or changing the state of mitigating equipment in a way that increases the need for safe shutdown systems, structures, and components (SSCs). The key criterion in identifying undesired operator actions is that the action leads to a worsened plant state (e.g. the operators conclude, from false indications or any other cues, that the safety injection (SI) termination criteria are met and then shut down SI when it is inappropriate to do so).

One of the two most relevant root cause categories of errors of commission for man-made hazard scenarios are induced cable failures or electrical faults that cause a spurious alarm or an indication failure. These failures and faults may lead the operator to take an action that would make the plant response worse. All the potential spurious alarm or indication failures that may be triggered by man-made hazards induced cable failures and electrical faults and are relevant to the safety of the plant are defined. These failures are for example relevant to the aircraft crash hazard that may have secondary effects (i.e. fuel fire, secondary missiles, explosion and shockwaves resulting from the crash, internal fires, etc.) having the potential to induce cable failures and electrical faults. After induced failures of alarms and indications are identified, the procedures and specific procedural steps related to responses to be based on the affected alarms and indications are studied and evaluated to assess the potential for errors of commission. The impact of spurious cues on procedure based operator actions are analysed and evaluated for the purposes of identifying errors of commission. Harsh ambient conditions and external stressors (see more details in chapter 9.3.3) also have the potential to induce errors of commission without having any spurious signals. The EOPs and other relevant procedures followed in response to man-made hazards are to be systematically reviewed to identify all steps in which an undesired operator action may be likely to be taken in view of the harsh conditions induced by the hazards. Each step in the procedure that contains some decision logic is to be considered for the potential to cause an undesired operator action if the decision associated with the step in question is inadequate.

9.3.2.5 Preliminary Feasibility Assessment

The feasibility check ensures that the man-made hazards PSA is not crediting an operator action that may not be possible. During the selection of HFEs, the initial feasibility assessment is conducted primarily based on information obtained during the HFE definition and supplemented by any additional information that may be known about the particular action or PSA scenario. The process is iterative, so result of the feasibility assessment is reviewed periodically as the HRA is further developed and refined. If an operator action is considered not feasible, the human error probability (HEP) is set to 1.0. Additional analysis may be needed to reassess actions that were previously considered not feasible and are risk significant according to the PSA results. This justifies the choice of setting HEPs for non-feasible actions to 1.0 as opposed to not giving credit to the HFEs.

An operator action is recognized as a not feasible action in the man-made hazards PSA, if any of the following criteria is met:

- there is no sufficient time available to complete the action;
- the location where the action is to be accomplished is not accessible;
- not enough crew members are available to complete the action;
- the equipment manipulated during the operator response is damaged or degraded due to the man-made hazard (and recovery cannot be credited).

9.3.3 QUALITATIVE ANALYSIS

The objectives of the qualitative analysis in general are to understand the modelled PSA context for the HFE, understand the actual "as-built, as-operated" response of the operators and plant, and translate this information into factors, data, and elements used in the quantification of human error probabilities. The results of qualitative analysis are needed for two of the key HRA process steps: the identification and definition of HFEs and the development of human error probabilities for HFEs. Consequently, qualitative analysis is not always explicitly identified as a separate step in the HRA process, but is incorporated partly into the identification as well as into the quantification process. This analysis ensures an overview of the issues to be considered, qualitatively, in performing an HRA. Only the issues specific to man-made hazards analysis are discussed hereby. Qualitative analysis starts with a collection and review of information supporting the development of the modelled HFEs. The information comes from three general sources: the PSA, the plant, and the existing HRA. The following types of data are useful to be collected for each source:

- PSA information needed to understand the modelled context for each HFE:
  - ○ hazard assessment for the man-made external hazard in question, with respect to hazard characteristics at the location of the source as well as at the plant;
  - ○ plant response and fragility analysis, regarding all safety related plant areas affected by the external event in question and deterministic analyses on the tolerability of protective measures (e.g. capacity of air filtration and cleaning systems);
  - ○ PSA model consisting of plant transients induced by the man-made hazard, event sequences for plant response/failure, fault trees for systems response/failure, and data and results (such as for accident sequences and important contributors);

  - success criteria analyses providing the basis for the accident progression modelling and times to component damage;
  - timing information such as from thermal-hydraulic calculations.
- Plant information needed to understand the actual "as-built, as-operated" plant response:
  - procedures including EOPs, abnormal operating procedures, and other, external (man-made) hazards related procedures;
  - alarms and instrumentation associated with operator response to man-made external hazards;
  - system descriptions for systems credited in the man-made hazards PSA;
  - operator training information such as the scope, types and frequency of training associated with man-made hazards and the associated plant transients that may be induced;
  - location and plant layout information;
  - plant staffing and roles following the occurrence of a man-made external event;
  - man-made hazard specific protection evaluations of the feasibility of manual operator actions (e.g. evaluation of air filtration and cleaning systems, individual protective clothing and devices (e.g. masks), sufficient prophylaxis, etc.).
- HRA-specific information needed to understand existing HRA methods and data sources:
  - HRA from the internal events PSA providing qualitative and quantitative data and analyses;
  - Interview notes from discussions and talk-through with operators and/or operator trainers;
  - Simulator observations and walk-down data.

As part of the qualitative analysis, the feasibility assessment in the HRA assesses whether an operator action can be accomplished in the context associated with the response to a man-made hazard related initiating event. Feasibility assessment is discussed to some extent in chapter 9.3.2.5. Important additional aspects of this analysis step are addressed hereby.

The most important factors influencing whether an action can succeed are the effects of a man-made hazard on plant personnel working out-side at a nuclear site as well as the habitability within building enclosures of a nuclear power plant by considering toxic gases, smoke, heat flux or major damage of building structures.

The accessibility of the plant as well as the conditions and the allowable time for working out-side at the site should be evaluated for most man-made hazards. In general, protective measures are applied to reduce harmful effects on the plant personnel. These measures are taken into consideration and the effectiveness of the measures is assessed during the feasibility analysis. For that purpose the design basis loads of the protective measures are compared with the loads induced by the given external event. First, considerations to existing (or potential) protective measures to ensure tolerable working conditions open air are described shortly on the example of man-made hazards resulting in toxic gas releases in the following. Then protective measures used within building enclosures are discussed.

A considerable reduction in harmful toxic consequences can be achieved by using individual protective clothing and devices (e.g. masks) or sufficient prophylaxis of the equipment. Suitable decontamination technologies and special transport vehicles can be used to reduce the effects of ground contamination below a tolerable level. Application of appropriate safety distances is also a good means to reduce the dose from inhalation consequences. Furthermore, the exposure time of the operating personnel can be limited by strictly controlling the allowable time for working open air with considerations to the dose rate anticipated.

The consequences of accidents with toxic effects or heat flux should be taken into consideration in order to ensure the habitability of vital service areas within the building enclosures needed to maintain the safe conditions of the nuclear power plant. A significant reduction in health effects can be achieved by using sufficient air filtration and cleaning systems. Therefore, appropriate positioning and orientation of the air filtration equipment also helps to limit the health effects from inhalation within the plant buildings. Furthermore, the exposure time of the operating personnel can be limited by strictly controlling the allowable time at work.

The most challenging HRA task in man-made hazards PSA is the identification of all relevant performance shaping factors (PSFs) and the appropriate characterization thereof. The authors consider the following factors as the most relevant ones with respect to HRA for man-made hazards:

- <u>bans or allusive signs and indications</u>

  For both in-control room and local actions, signs and indications are necessary since all required operator actions are predicated on them; without signs or indications, the operators have no prompts that some action is required, and therefore no operator action can be credited; for man-made hazards the following aspects are of great importance:

  - man-made hazards may result in a large number of and also simultaneously changing signs and indications, that may inhibit the identification of the relevant cues and indications in time;
  - operator action credited in response to certain indications in the internal events PSA may not still be credible if the indications are impacted by the man-made hazard;
  - signs and indications may be inadequate (in contrary to assumptions of internal events PSAs) in scenarios in which redundancy and/or diversity could be impacted;
  - spurious indications can cause confusion or even prompt the operators to take an inappropriate action;
  - for MCR abandonment actions, the crew will likely have limited familiarity with the ex-control room panels and the way in which cues for actions are presented; furthermore, the human-machine interface of these panels may not be as good as that in the MCR),

- <u>available time</u>

  The available time refers to the amount of time that an operator or a crew has to diagnose and act upon an abnormal event [54]. Timing analysis is usually based on delineation of a timeline that is composed of several elements to capture the various aspects of time during the progression from the initiating event until the time at which the action will no longer succeed. This approach is applicable to man-made hazards HRA too. A shortage of time can affect the operator's ability to think clearly, to consider alternatives and to perform the required tasks. The time pressure imposes heavy task load situations (task complexity) and high or extremely high stress level. It is important that the time available and the time needed to perform the action are considered together with many of the other PSFs and the demands of the accident sequence.

  For the purposes of man-made hazards HRA the following examples on special considerations can be identified:

  - use of less familiar or otherwise different procedure steps and sequencing could change the anticipated timing of actions in response to a man-made hazard;
  - interfacing with other organizations (e.g. fire brigade) working in the vicinity or on the site may delay performing some actions;
  - accessibility issues, harsher environments, and/or the need for other special tools may impact the overall timeline of how quickly actions normally addressed in response to internal events can be performed under the conditions imposed by man-made hazards;

  - for rooms outside of the control room local actions after a man-made external event, the available resources, the number and locations of the necessary actions and the overall complexity of the actions that must be taken may have a most significant impact on the time required to perform the actions.

- <u>procedures and training</u>
  Operator response to events in complex situations is improved by having procedures available, moreover complex situations may slow the typical response to procedures or may lead to the selection of the wrong procedure, especially for scenarios in which instrumentation is affected or when training does not cover the specific situation. Depending on the man-made hazard, the operators may need to use procedures or controls other than EOPs typically used in response to internal events. Implementing unfamiliar or multiple procedures simultaneously could lead to confusion. In some cases, especially for some ex-control room actions, procedures might not exist or be readily retrievable or might be ambiguous in some situations. The analysis should include a review of the adequacy and availability of these other procedures that would be needed to address the man-made hazards modelled in the external events PSA. The amount and types of training the crews receive on implementing the procedures and the degree of realism are a critical factor. If any response actions are required that are not procedural, the man-made hazards HRA does not take credit for them as a first approximation. Non-procedural recovery actions are to be credited on an as-needed basis in subsequent phases of the PSA development. A particularly important concern is the decision of “if and when” to leave the MCR. The procedural guidance, training received, and the explicitness and clarity of the criteria for abandoning the MCR are considered. This concern is an area of uncertainty because there may not be clear decision criteria for abandonment; it may be at the discretion of the shift supervisor. Problems leading to a higher likelihood of failure in transient mitigation can arise if the crew delays too long in leaving or if they leave too quickly.
- <u>task complexity</u>
  The PSF reflecting task complexity attempts to measure the overall complexity involved for the situation after a man-made hazard and for the action itself. Many other PSFs affect the overall complexity, such as the need to analyse numerous indications and alarms, the presence of many complicated steps in a procedure, or poor HMI. Most man-made hazard related scenarios may be considered as complex tasks due to multiple induced transients, unavailability of multiple equipment, large number of actions required, misleading or absence of indications, transitioning between multiple procedures and large amount of communication required. Moreover for local and MCR abandonment actions, the crew may be required to visit various locations that may increase the complexity of the situation. All these features should be addressed.
- <u>workload, pressure and stress</u>
  Although workload, pressure, and stress are often associated with complexity, the emphasis here is on the amount of work that a crew or individual has to accomplish in the available time (e.g. task load) along with their overall sense of being pressured and/or threatened in some way with respect to what they are trying to accomplish. In this sense, this PSF is largely associated with “available time” too. Human induced external events may cause multiple transients with simultaneous degradation of mitigation systems. Consequently, the activities involved in restoring the normal status impose a high level of task load and pressure on operators, corresponding to a high level of stress and the possibility to lose control. Especially for local and MCR abandonment actions, there is the potential for high time pressure to reach the necessary locations and perform the appropriate actions. An important consideration in the performance of these actions is the extent to which multiple actions need to be coordinated or sequentially performed

and the available time as perceived by the operators. The stress variable can be represented with different levels of stress in a situation after a human induced external event, e.g.: nominal (not higher than that assumed in the internal events PSA), high (moderately disruptive), and extremely high (very disruptive), depending on the impact area location and dimensions.

- <u>human-machine interface</u>
  For man-made external hazards, the human machine interface can have potentially large impacts on operator performance during local and other ex-MCR actions, although control room actions are influenced similarly to responses to internal initiating events. Local actions may involve more varied layouts (and not particularly subjected to human-factors engineering) and require operators to take actions in much less familiar surroundings and situations. Therefore, any problematic human-machine interfaces can be an important negative factor on operator success. For control room abandonment or alternate shutdown actions, the adequacy of the remote shutdown and local panels needs to be verified. In addition, the operators are not as familiar with the panel layout as they are in control room scenarios. This PSF partially overlaps with “cues and indications” discussed above.
- <u>environment</u>
  Environmental factors may significantly influence whether an operator action can succeed. The effects of man-made hazards on plant personnel working open air at a nuclear site as well as the habitability within building enclosures of a nuclear power plant due to toxic gases, smoke or heat flux are to be analysed and evaluated for characterizing this performance shaping factor. The accessibility of the plant as well as the conditions and the allowable time for working open air at the site should be evaluated for certain man-made hazards. In general, protective measures are applied to reduce harmful effects on the plant personnel (see details earlier in Sub-chapter 9.3.2.5 on feasibility assessment). After a human induced external event, the potential exists that the crew’s travel path (expected by design) to the action location will be blocked and lead to a delay or inability to reach the action location. Where alternative routes are possible, the demands associated with identifying such routes and any extra time associated with using the alternative routes should be factored into the analysis. This can also be taken into consideration as a stand-alone performance shaping factor, i.e. accessibility (of equipment to be manipulated). Moreover, structural damage may adversely impact on the environmental conditions for local actions (difficulty to operate equipment, use tools, etc.).
- <u>special equipment</u>
  Due to the harsh ambient conditions after a man-made external event, the crew may require the use of special equipment. Primarily these items include protective clothing and devices (e.g. masks), as well as special transport vehicles. Keys, ladders, hoses, flashlights and self-contained breathing apparatus (SCBAs) are also considered as special equipment applied after a man-made hazard. The availability and accessibility of these tools need to be checked to ensure that they can be located and would be accessible during the harsh environmental conditions. Furthermore, the level of familiarity and training on these special tools needs to be assessed. Special equipment tends to be more important for the success of local actions than control room actions.
- <u>special preparedness needs</u>
  Man-made hazards may induce the need to consider actions not included in the internal events PSA or changes to how previously considered actions are performed. Examples of unique preparedness needs include the following:
  - having to climb up or over equipment to reach a device because the external event has caused the proper travel path to be blocked;

  - needing to move and connect hoses, especially if using a heavy or awkward tool;
  - using SCBA, which can be physically demanding and hinder communication.
- personnel communication, staffing and dynamics
  Personnel dynamics and characteristics are essential to understand how and where the early responses to an event occur and the overall strategy for dealing with the event as it develops. In particular, the structure of the applicable procedures, scope of training as well as the organizational and administrative environment can affect overall crew performance. For man-made hazards HRA, the typical internal events crew dynamics may change as a result of responding to an external hazard and need to be reconsidered. For instance, the man-made hazard may create new or unique hazard-related responsibilities that have to be handled by a personnel member. The use of plant status discussions by the personnel may be delayed or performed less frequently, allowing fewer opportunities to recover from previous mistakes. A man-made hazard can introduce additional demands for staffing resources beyond what are typically assumed for handling internal events. These demands can take the form of using multiple procedures in parallel or needing to use and coordinate with additional personnel to perform certain local actions and with the fire brigade and/or local fire department personnel. For control room actions, communication among crew members should be verified. It is expected that communication within the crew will not be a problem in a situation following a man-made hazard; however, any potential communication problems (such as having to talk while wearing SCBA in the control room) should be accounted for if they exist. For local actions, communication may be much more important because of the possibility of a less-than-ideal environment or situation. The way in which equipment faults caused by the man-made hazard could affect the ability of operators to communicate as necessary to perform the desired act(s) should be understood. Following MCR abandonment, the ability to communicate from different places (e.g. the location of remote and alternate shutdown panels) should be considered and addressed. Furthermore, if SCBA is required to be worn, the apparatus might interfere with clarity in communications among team members. In evaluating communication between actors of different crews (e.g. communication between MCR personnel and local operators) the impact of the man-made event on communication channels and modes should be assessed too.

9.3.4 QUANTIFICATION

9.3.4.1 Approaches

Three main approaches are proposed in [53] to quantify all relevant HFEs in a fire PSA. The authors find these approaches (with some modifications) relevant to and appropriate for the purposes of man-made hazards HRA assessment as well. Therefore the quantification of HFEs is discussed in the following breakdown:

- screening HRA quantification;
- scoping HRA quantification;
- detailed HRA quantification modified for application in man-made hazards HRA.

9.3.4.2 Screening HRA Quantification

The aim of screening in the HRA is to assign initial screening HEPs to HFEs to ensure simplification and refinement in the PSA model to help focus the analysis on risk-significant transient scenarios induced by man-made hazards, associated equipment failures, and operator actions. During screening process quantitative screening values are used for the HFEs modelled in the man-made hazards PSA by addressing the unique conditions created by the external event in question. For quantification reasons, all HFEs are matched to a set of criteria. Because of the unique conditions created by man-made hazards, some level of analysis is needed to determine which screening "set" is applicable. The HEPs assigned in this manner are conservative and may not be acceptable as a final HEP for a given HFE (i.e., a more realistic HEP is needed). The screening method should support the assignment of screening values by addressing the conditions that can influence crew performance during responses to a human induced external event, ensuring that the time available to perform the necessary action is appropriately considered (given the other ongoing activities in the accident sequence) and that potential dependencies among HFEs modelled in a given accident sequence are addressed. For a particular HFE, if an appropriate set of criteria cannot be identified or met, no screening value should be used (i.e., a 1.0 failure probability should be assigned initially and/or a more detailed analysis be performed, depending on whether the HFE becomes important after initial model quantification). In addition, because the screening approach assigns a screening value of 1.0 for alternate shutdown actions (including MCR abandonment as a result of habitability), a possible next step and conservative approach should be provided at the end of the screening chapter. This approach may allow the assignment of a single overall failure probability value (e.g. 0.1) to represent the failure of reaching safe shutdown using alternate means (including MCR abandonment) if certain minimal criteria are met. One example of the screening set categories for man-made hazards can be given on the basis of the criteria proposed in [31]:

- set 1 criteria: a goal here can be to determine whether the conditions due to the man-made hazard are such that a HEP of an HFE modelled in the man-made hazards PSA can simply be originated (and to some extent modified with a certain multiplication factor) by the value used in the internal events PSA for the similar HFE;
- set 2 criteria: this set of criteria may address a special case for HFEs modelled in related scenarios in the internal events PSA but that did not meet the Set 1 criteria;
- set 3 criteria: this set may address new HFEs added to the man-made hazards PSA to account for hazard-specific effects and prior internal events PSA HFEs that had to be significantly altered or modified during the identification and definition step (see Chapter 9.3.1) to reflect man-made hazard induced effects;
- set 4 criteria: this set may address actions involved with MCR abandonment and the abandonment decision.

9.3.4.3 Scoping HRA quantification

An alternative approach (i.e. scoping method) to screening may be applied in man-made hazards HRA quantification to reduce some of the conservatism of the screening approach and may be used instead if potentially less conservative initial HEPs are desired. The scoping method relevant to man-made hazards is adapted from the scoping fire HRA approach developed specifically for report [53]. It is a simplified quantification approach that addresses only a few performance shaping factors specific to man-made hazards. The scoping analysis uses decision-tree logic and descriptive text to guide the analyst to the appropriate HEP value. Although it has similarities to screening approach, the scoping quantification process requires a somewhat more detailed analysis of the scenarios in the man-made hazards PSA and the associated plant conditions as well as a good understanding of several factors likely to influence the behaviour of the operators in taking response to a hazard scenario. Given such an analysis, it is expected that the flowcharts provided below can be used to perform quantification for many of the HFEs being modelled. However, it is expected that some actions will not meet some of the criteria and result in an HEP of 1.0. Furthermore, the HEPs developed using this method may be conservative compared to those that could be derived if a more detailed and time-consuming HRA was performed. A minimum criterion has to be satisfied to use the scoping HRA approach. If the criteria covered within this scoping procedure are not met, a more detailed HRA should be performed. The minimum criterion has to be determined based on the specificities of the man-made hazard in question.

Applicable minimum criteria for most of the hazards are as follows:

- procedures: there should be plant procedures (e.g. EOPs, AOPs and special procedures related to external (man-made) hazards) covering each operator action being modelled; the procedures should support both the diagnosis and execution of the action, unless the execution of the action can be demonstrated as skill of the craft;
- training: operators should have received training on the procedures being used and the actions being performed; the training should establish familiarity with the procedures, the equipment needed to perform the desired actions, and the steps required to successfully execute the action; training should cover initial and continuing (refresher) training as well;
- availability and accessibility of equipment: all equipment and tools needed to perform the modelled human actions should be readily available and accessible.

One of the key inputs to the scoping approach is time margin. To assess the time margin, the difference between the total available time and the time required (i.e. the extra time available) should be divided by the time required, that is used to represent a continued emphasis on sufficient time for operator action and other factors not addressed in the feasibility assessment. In addition to addressing the timing issues, decisions must be made regarding particular conditions and PSFs that could affect the performance of the actions. In general, the following conditions and PSFs are important to the scoping flowchart delineation for man-made hazards:

- existence of procedures with respect to the scenario in question;
- response execution complexity;
- single-step actions;
- multiple step actions;
- multiple crew members performing coordinated steps;
- multiple location steps;
- multiple functions;
- accessibility of location or tools;
- timing of cues for the action relative to expected termination of harmful effects;
- time available for action;
- concentration of toxic gas and other hazardous elements and any other harsh environmental conditions in action areas.

In the scoping HRA quantification approach for man-made hazards, a unique selection scheme and associated following flowcharts need to be developed for each man-made hazard. A good general approach may be to treat HFEs based on conditions within the MCR, the location of the diagnosis and execution of the actions associated with the HFE (MCR or ex-control room), and the condition of relevant instrumentation. The selection scheme uses a series of questions to determine which action is being quantified and to direct the analyst to one of the following flowcharts that is appropriate for quantification: MCR action, ex-control room or local action, alternate shutdown, or recovery of error resulting from spurious actuation due to instrumentation failure. In some instances, the HFE may be quantified within the selection scheme. An example for the selection scheme is given in Figure 9-1, where

FC denotes Flowchart. Furthermore, Figure 9-2 shows a following flowchart for man-made hazards HRA in general on the example of in-MCR actions. The flowchart may be applicable e.g. to an accident at a nearby industrial facility. The flowchart walks through the steps of assigning scoping HEPs to HFEs within the MCR. HEP values should be selected in advance of HFEs quantification based mainly on experience with the range of values traditionally used and accepted in HRA performed for nuclear power plants by licensees and regulatory bodies, and experience in applying a range of HRA methods and the values associated with those methods. The values should be selected with the goal of being moderately conservative while crediting reasonable time margins and other PSFs. Please note that 'Smoke in the MCR' in the flowchart refers to all hazardous effects in the main control room, that may be caused by a man-made hazard, i.e. toxic gas, smoke, heat flux, missile impact, other hazardous elements.

Figure 9-1: An exemplary selection scheme for scoping quantification of HFEs in man-made hazards HRA (A negative ('No') answer should also be given, if there are no procedures for executing the required MCR actions, unless those are skill-of-the-craft)

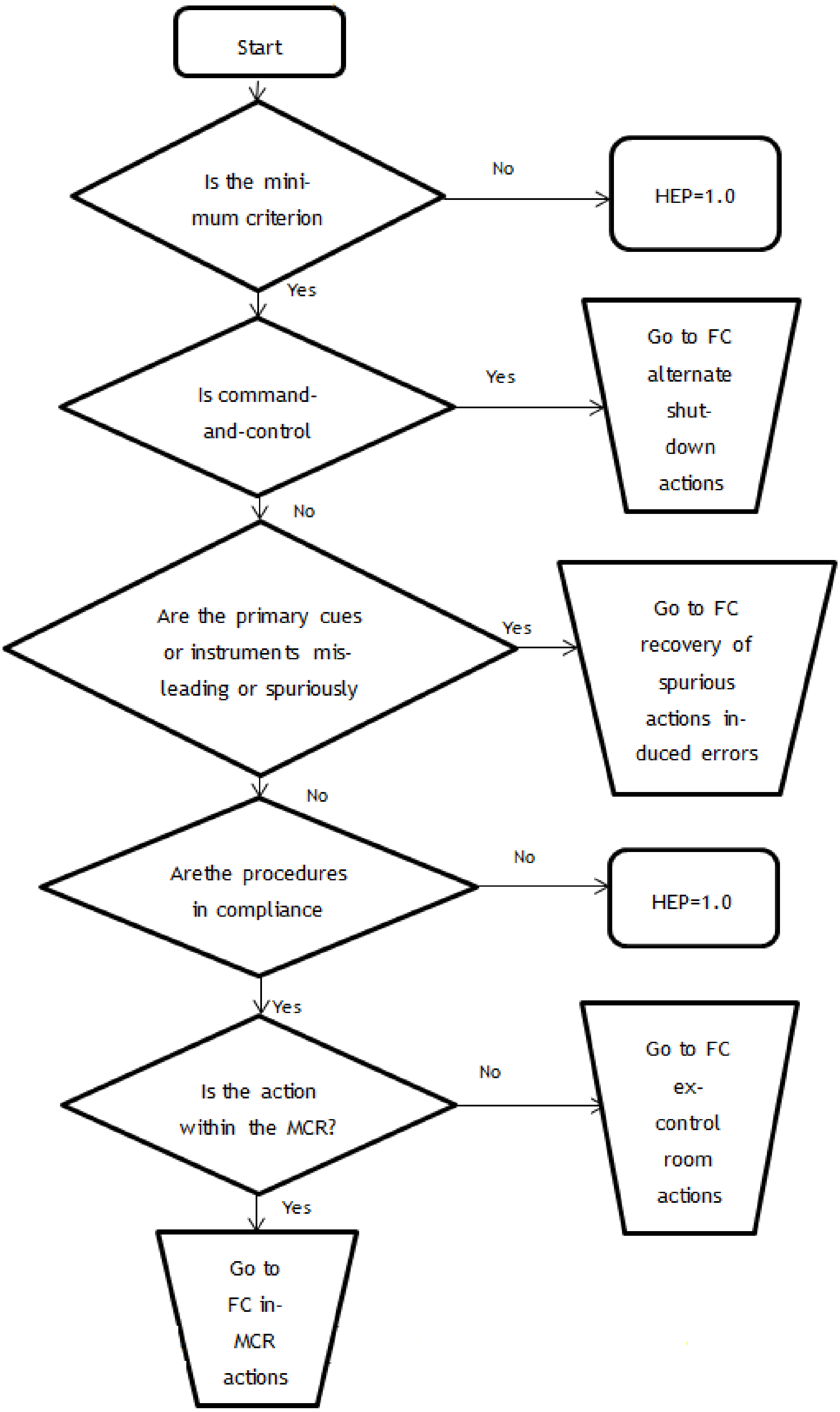
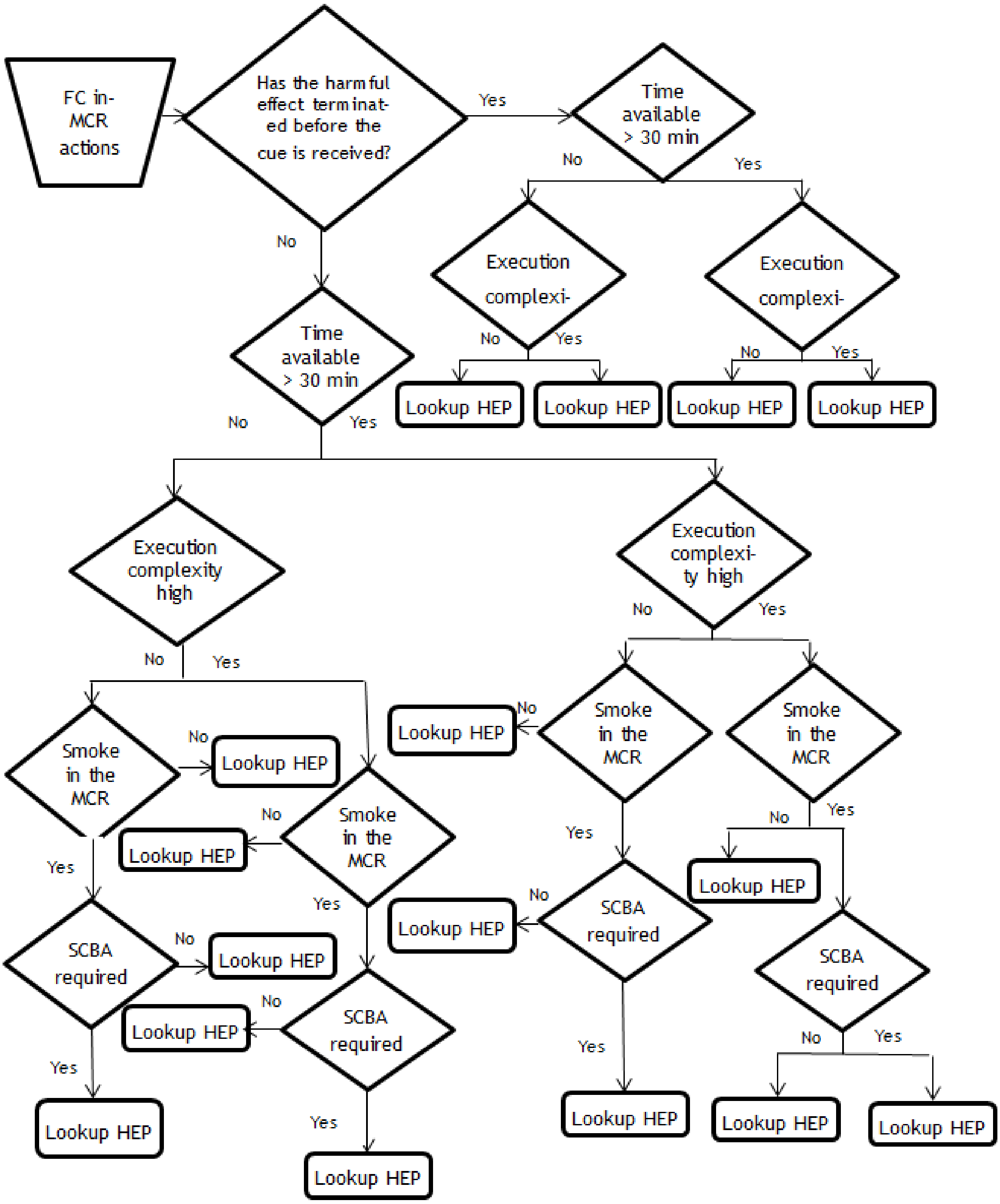

Start
Is the minimum criterion
No
HEP=1.0
Yes
Is command-and-control
Yes
Go to FC alternate shut-down actions
No
Are the primary cues or instruments misleading or spuriously
Yes
Go to FC recovery of spurious actions induced errors
No
Arethe procedures in compliance
No
HEP=1.0
Yes
Is the action within the MCR?
No
Go to FC ex-control room actions
Yes
Go to FC in-MCR actions

Figure 9-2: An exemplary scoping flowchart for in-MCR actions relevant to man-made hazard related HFEs[4]



Before quantifying an HFE, the feasibility criteria of the operator action(s) associated with that HFE must be applied (see chapter 9.3.2.5). Although the feasibility assessment process begins at the identification and definition

[4] Lookup HEP values are not given in the sample flowchart because they are dependent on the man-made hazard being (and the plant design) analysed and thus indication of any specific values would be misleading.

stage and is a key part of the initial qualitative analysis, new information may be available during the quantification process that would require the feasibility to be reassessed. Therefore, feasibility assessment is a continuous process throughout the man-made hazards HRA. As discussed earlier, it is expected that some actions will not meet the criteria in the scoping HRA approach and result in an HEP of 1.0. Furthermore, the HEPs developed using the scoping approach may be fairly conservative compared to those that could be developed using a detailed HRA. There are numerous methods available for detailed HRA and quantification of HFEs. It is not the purpose of this chapter to present an exhaustive listing of all the methods that could be a candidate for use in detailed HRA quantification. However, reference is made to report [55] that evaluates a number of available HRA methods against pre-defined quality measures of good practices in HRA. In addition, a more recent study of the OECD-NEA [56] also evaluates a range of methods against desirable attributes of contemporary human reliability assessment. All the methods listed and evaluated in these reports can, to a smaller or larger extent, be used for quantifying HFEs in man-made hazards HRA. Preference should be given to those methods that are capable of explicitly describing the relationship between an HEP and the context (in which an error is made) for a wide range of contextual conditions. This is particularly important for external events PSA (including PSA for man-made hazards) because of the specificities of contexts that characterize the accident sequences induced by such events. In other words, the method should be applicable to address man-made hazard specific issues and PSF impacts with appropriate considerations to the man-made hazard scenarios as described in Chapter 9.3.3. To that end, it is noted that none of the existing HRA methods has actually been evaluated for use specifically in man-made hazards PSA. Although HRA methods should, by their nature, be general enough to enable their use in different PSA areas, there is evidently a need to examine and assess the capabilities and limitations of current HRA methods for use purposefully in man-made hazards HRA. Some of the existing methods were experimented for application to fire PSA/HRA in [53] and the insights gained are also useful for man-made hazards HRA because of the various kinds of similarity between the two types of analysis (fire PSA and man-made hazards PSA). However, this in itself does not fill in the gap that exists in the evaluation of the methods for use in man-made hazards HRA. It is recommended, that the detailed HRA quantification process should assess, as a first step, which basic inputs used for the internal events PSA are still applicable in an external event situation. This should be followed by an assessment and description of the hazard impact in terms of its manifestation in the PSFs that are important to characterizing the context and determining the HEP. Data collected during qualitative analysis can be used in this step. It is expected that this approach will lead to an increase in the error probabilities used for internal events PSA.

9.3.4.4 Dependence

Dependence should be assessed for HFEs potentially dependent on the effects of man-made hazards as well as for HFEs newly introduced into the model to ensure that dependence is accounted for in the man-made hazards PSA. If new HFEs related to a man-made hazard have been added to the model, these new actions should be shown to not create new dependence among the HFEs in the accident sequence. In addition, any likely strong dependence should be shown to be accounted for during the screening so that accident sequences/cutsets are not artificially removed because of multiplying many supposedly independent HEPs. In comparison to internal events PSA, more significant dependence might be applicable to HFEs related to man-made hazards due to the impact of the hazards on some PSFs. Influences of success or failure on parallel and subsequent human actions and system performance should include at least the following:

- time margins;
- common causes (e.g., common instrumentation or procedures, an inappropriate understanding or mind-set as reflected by the failure of a preceding HFE, and increased stress);

- resource availability (e.g., crew members and other plant personnel to support the performance of ex-control room actions).

9.3.4.5 Uncertainty

Uncertainties in HRA play an outstanding role in the overall uncertainty assessment within man-made hazards PSA. Hence uncertainties should be described beside the point values defined for each HFE. Examples on potential sources of uncertainty in man-made hazards HRA modelling are:

- timing, e.g. timing data inputs, ex-control room action travel path changes as a result of the impact of the man-made hazard;
- dependence, e.g. common cognitive impact;
- stress, nervous tension;
- workload;
- communications, i.e. damage of normal communications systems and processes as well as availability of backup radios;
- training, lack of gaps of training;
- procedures.

9.4 CHALLENGES AND OPEN ISSUES

Based on the above chapter 9, the following challenges were identified in relation to man-made hazards HRA:

- **Lack of explicit detailed guidance** document on how to address the specific needs of man-made hazards HRA when applying current (general) human reliability assessment methods. This generates the need to investigate the capabilities and limitations of current human reliability analysis methods for use purposefully in man-made hazards HRA.
- Limitations and uncertainties in both identification and quantification of HFEs due to **the limited availability (very often lack) of procedures, training and experience** relevant to man-made hazards.
- Plant response assessment is often based on **simplified assumptions** and scarce data sets; hence HRA based on this information is also limited.
- Excessive reliance on expert judgement due to scarcity of observations (on the simulator or in the field) induces **a high level of subjectivity**.
- The basis for **determining and estimating increases in error probabilities** in PSA in conditions of external hazards occurrence are not well developed.
- Some PSFs need detailed investigations **to reflect the effects of man-made hazards** in an appropriate manner, e.g. environment, special equipment, task complexity, etc. For instance, there is a strong possibility for bad or inadequate communications in external hazard conditions, i.e. damage of normal communications systems and processes as well as availability of backup radios, and the influence induced by the level of communication on the event progression should be investigated. There is the possibility to have and to use wrong information for decisions, as result of external hazards impact, but the measures to establish this require some back-up indications.
- A special attention should be paid for **recovery actions**, and for necessary actions to use the **mobile equipment**.

- There is a limited accounting for **dependencies among actions**. In comparison to internal events PSA, more significant dependence might be applicable to HFEs related to man-made hazards due to the impact of the hazards on some PSFs.
- Is difficult for rare events, **to generate experience or training for operators actions** (e.g. simulator) and this may generate a high probability of failure for actions.
- Compared to accident scenarios caused by internal initiating events, the **operators stress levels and conditions in the plant** may differ considerably after an external initiating event; the stress variable can be represented with several levels of stress: nominal, high (moderately disruptive), and extremely high (very disruptive), depending on the impact area location and dimensions. But there is a lack of methodology to actually assess the stress level as a manifestation of the underlying stressors and to justify this assessment.
- There is a lack of adequate identification, explicit representation, and quantification of **actions with potential adverse effects on plant conditions (errors of commission)**. The errors of commission are considered to be largely the result of problems in the plant information/operating crew interface (wrong or inadequate information, or the information can be easily misinterpreted) or in the procedure-training/operating crew interface (procedures/training do not cover the actual plant situation very well because they provide ambiguous guidance, or no guidance for the actual situation that may have evolved in a some unexpected way). In either case, significant mismatches can occur between the scenario conditions and the understanding of those conditions, and their potential for leading to commission errors should be examined.
- There is no explicit account for **the impact of organisational and management aspects**, that may have a significant influence on operator actions. Also there is no explicit account for influence of multiple decision makers, which may not always have a positive influence on the accident progression.

10 SOLUTION TO MODEL ADDITIONAL EMERGENCY RESPONSE

The emergency response to the hazard events may significantly affect their progression time and severity (in terms of potential effect on plant systems, structures and components) by preventing their progression to a safety significant initiating events and mitigating their consequences. Thus, for example, more than 70% of NPP fire events reported in OECD FIRE Database were extinguished by on-site fire brigade or plant personnel, and ~12% of these events involved external fire brigade participation (see chapter 4.3 and Figure 11 of [57]). Therefore, incorporation of emergency response (ER) actions in probabilistic safety analyses is needed in order to obtain more realistic estimates of plant response to the hazards, to assess adequacy of existing emergency response plans and procedures, and to provide insights for their improvement. An approach for modelling of emergency response actions in PSA is based on estimation of likelihood that time of successful response (e.g., fire detection and suppression, establishing water supply from mobile pump) is greater than available time to prevent damage of particular SSC (e.g., failure of particular component caused by fire) affected in a given hazard progression scenario.

10.1 MOBILE EQUIPMENT AND HELP FROM OUTSIDE THE PLANT SITE

Basic information on emergency response requirements and rules can be found in GS-R-2 [58], national legislation, correspondent governmental body or organization regulations and guides. Other valuable sources of information on emergency response organization, infrastructure and capabilities at the on-site, local, regional and national levels include the plans and procedures of the on-site and off-site emergency response teams including the ones of the utility of NPP under evaluation, and of fire brigades. These documents allow identifying:

- a list of organizations and institutions involved, their responsibilities and subordination in the emergency conditions;
- the types of support that could be expected (e.g., firefighting, repair activities, transportation, mobile equipment and fuel supply, etc.);
- the conditions for identification of transfer from normal to an emergency operation and declaration of the emergency;
- the notification, communication and reporting lines and procedures;
- the emergency teams activation, arrival and response procedures;
- the technological risks that may be imposed in case of some actions;
- the technologically defined maximal times to take mitigation measures;
- the sequence of actions;
- the prescribed timeframes.

While familiarization with the national and regional ER documents is useful for understanding the overall response structure and organization, it is practical to focus further studies primarily on the on-site, the particular facility, its technological structure and local emergency response actions. On the necessity the analysis may be extended to take into account other off-site response. The data to be collected include[5]:

- the type of the emergency response facilities;

[5] It is assumed that data specific to a particular hazard source, magnitude, etc. are collected as a part of hazard analysis task

- the quantitative resource of the emergency response facilities (quantitative estimation of the emergency response facilities in respect to the respective nuclear facility size: number of units, spent fuel storages, other);
- location of emergency response facilities (e.g., fire station, mobile equipment hangars);
- transportation routes that will be used;
- emergency response team organization and capabilities (staff number, training, specialized emergency equipment and machinery availability and readiness, etc.);
- emergency response procedures;
- emergency response staff preparedness to cope with any situation that may occur;
- 24h availability of the emergency response staff, availability of second shift;
- communication organization and means;
- notification processing and arrival time;
- location and inventory of water, special firefighting means, and fuel sources to be used, location of fire water stand pipes and mobile equipment connecting points.

The general guidance on modelling the emergency response to a fire is provided in NUREG/CR-6850 [31]. The probability of fire brigade failing to suppress the fire is estimated using the following formulae:

$$\Pr(t_{supp} > t) = e^{-\lambda t},$$

where t_{supp} – fire suppression time;

t – time available for fire suppression prior to target damage;

λ – fire suppression rate.

The time of target damage can be estimated using engineering calculations or dedicated fire modelling tools. NUREG-1805 [59] provides information on methods, correlations and data for engineering calculations of such characteristics of room and open fires (including liquid pool fires) as heat release rate, burning duration, flame height, temperature, flux to a target, ignition time of a target fuel, etc., that can be used to evaluate particular fire progression scenario. Discussion on application of fire modelling tools can be found in [60]. To calculate fire suppression rate the reported suppression time data from actual fire events (excluding self-extinguished fires, supervised burnouts and fires extinguished with automatic systems) are used. Table 14-3 of NUREG/CR-6850 Supplement 1 provides the list of fire events at U.S.NPPs and correspondent fire suppression time. Based on these data the mean values of fire suppression rates for 11 fire types (e.g., fire of transformer yard, flammable gases fire, etc.) as well as for all considered fire events are calculated (see Table 14-2 of Supplement 1 [31]). It shall be noted that original approach presented in Appendix P of NUREG/CR-6850 treated the fire suppression by plant personnel and by on-site fire brigade separately, and required to consider the fire brigade response time which by itself represent the uncertain value that varies from fire to fire. In this approach the available time for fire suppression (in minutes) t = t_{damage} - t_{fb} - t_{det}, where t_{damage} is the time to target damage, t_{fb} is the fire brigade response time, and t_{det} is the time to detection. The difficulty in application of this approach is caused by the necessity to distinguish the fire brigade role in suppression of particular fire, while this information in the actual fire data records may be missing or ambiguous.

The updated method described in Supplement 1 of NUREG/CR-6850 [31] considers the fire suppression as a continuous activity implemented by plant personnel and the on-site fire brigade and utilizes a more consistent approach in processing of recorded fire events data. For this approach $t = C_s \times (t_{damage} - t_{det})$, where C_s is a scenario-specific adjustment factor to account for cases where the fire brigade response time is expected to differ significantly from the typical response time:

$$C_s = 1 - \left(\frac{\langle T_{fb-s}\rangle - \langle T_{fb-t}\rangle}{\langle T_{fb-s}\rangle + \langle T_{fb-t}\rangle}\right),$$

where $\langle T_{fb-t}\rangle$ and $\langle T_{fb-s}\rangle$ are the mean typical and scenario-specific fire brigade response times, respectively. Corresponding data can be obtained from plant training records.

Detection time depends on the availability of automatic fire detection systems, their characteristics (location, type, actuation set point, etc.) and alarm processing procedure (i.e., necessity of alarm confirmation by plant personnel). Automatic detectors actuation time can be estimated using engineering calculations (see NUREG-1805 [59]) or dedicated fire modelling tools. If automatic detection is not available, the manual detection is considered. In this case the detection time depends on whether the particular compartment or area is occupied, entered or monitored constantly or periodically. The hazard progression scenario under evaluation may impose restricting conditions which affect the firefighting response resulting in longer fire durations. Examples of these conditions include roads and emergency access blockage, structural damage, accessibility of fire water stand pipes, multiple fire locations, etc. The results of plant walk-downs and engineering judgment are used in estimating how these conditions influence the fire brigade response time. In fire scenarios multiple sources of inflammable / explosive media shall be taken in account: for example turbine bearing lubrication oil in combination with hydrogen.

Several topics for improvement related to modelling of fire brigade response were identified in previously conducted PSAs (see ch.3.3.2.3 of NUREG/CR-5042 [61]) that need to be addressed, i.e.:

- potential spread of smoke and heat through the access doors that may result in a damage of equipment and ignition of fire sources located therein or propagation of fire to adjacent area in the case of suppression failure;
- potential damage of equipment caused by spreading of fire suppression substances;
- influence of smoke on fire suppression effectiveness[6].

It is recognized that organization and capabilities of fire brigades at NPP under evaluation may vary from those accounted in NUREG/CR-6850, and applicability of suppression rate data from NUREG/CR-6850 may be questioned. Earlier analyses which took into account fire brigade response, utilized plant specific fire drill data to estimate the fire suppression probability assuming that the time to detect, respond, and extinguish the fire are equivalent to those observed in the drills. This simplified approach may lead to underestimation of the time to extinguish a fire especially for the plant areas where substantial smoke build-up is possible prior to arrival of the fire brigade (see ch.V-2 of IAEA-TECDOC-1134 [30]). Therefore, the application of domestic or applicable international data on fire brigades response to actual NPP fire events to estimate fire suppression probability is more preferable. If existing data are insufficient for obtaining representative estimates, the review of fire brigade practices, interviews of fire department personnel and plant walk-downs may be used (see [62] and ch.V-2 of IAEA-TECDOC-1134 [30]). Alter-

[6] According to B.8 of [79], the issue is accounted by application of industry experience data and high no-suppression probabilities numbers for cable fires that are more likely to introduce smoke filled environment.

natively, the plant-specific information from actual fire events can be compared with NUREG/CR-6850 data, and appropriate adjustment method introduced if deemed necessary. Usage of Boolean/discrete representation of ER success or failure instead of variable probability distribution also may be found applicable (especially at the initial stages of analysis).

Aircraft crash fires represent a significantly higher threat to the plant SSCs as compared to "conventional" fires because of the larger fuel quantities involved, the very rapid rate of fire development, the combination with structural damages as impact result, and the necessity to use special firefighting equipment (e.g., foam generators), suppression agents and specific firefighting operations. The effects associated with aircraft crash fires include (see ch.4.23 of IAEA NS-G-1.5 [33], 5.16 of NS-G-3.1 [50]):

- burning of aircraft fuel outdoors causing damage to exterior plant components important to safety;
- explosion of part or the whole aircraft fuel externally to buildings;
- entry of combustion products into ventilation or air supply systems, thereby affecting personnel or causing plant malfunctions such as electrical faults or failures in emergency diesel generators;
- spreading of aircraft fuel to the compartments through normal openings, through holes/cracks which may have resulted from the crash or as a vapour or aerosol through air intake ducts, leading to subsequent fires or explosions.

The spill of aircraft fuel on large area shall be taken into account. Such fire can cause smoke curtain in the area of the accident and obstacle the initial visual estimations of the accident consequences.
Combination of aircraft fuel fire with affected equipment on the ground must be taken in account:

- transformer oil in unit / auxiliary transformers;
- compressed air receivers /tanks/ (for example for DG starting system, etc.);
- diesel fuel tanks;
- compressed hydrogen receivers /tanks/ (for example for generator filling system);
- other storages for inflammable / explosive media.

There is no experience with damage induced by aircraft falling on nuclear islands. Therefore evaluation of fire brigades capabilities to cope with the fires induced by an aircraft crash is based mainly on engineering judgment, interviews of fire department personnel, and large pool fire estimates and experience. Some recommendations on estimation of fuel quantity penetrating into a building in the case of aircraft impact, pool fire size, and simulation of fire effects can be found in [63]. The time and means needed for emergency response can be estimated mainly on the experience of fire brigades with the fires of similar scale.

Appendix 4 contains additional material relevant to emergency response related to aircraft crash hazards.

The guidance on modelling the emergency response to a fire can be adopted for modelling of mobile equipment usage (e.g., mobile pumps for steam generators feed and service water supply, mobile diesel generators). For this case time available for emergency response is determined based on the results of thermal-hydraulic accident analyses, and typical response time is estimated from emergency drills records. As in the fire response evaluation the restricting conditions imposed by the hazard progression scenario need to be taken into account in estimating the scenario-specific timing. Criteria and considerations given in NUREG-1852 [64] may be applied as a guidance for evaluating and demonstrating the correctness of assumptions on scenario-specific timing estimate. Sufficiency of the water sources inventory and fuel supply available for mobile equipment operation need to be evaluated considering the consumption rate in particular scenario and potential dependencies between water inventory discharged for fire suppression and for supply by mobile equipment if sharing of same water sources is permitted for both purposes.

Incorporation of emergency response to a PSA model involves:

- introduction of additional top event(s) to the event trees representing plant response to a particular hazard (hazard event tree);
- identification of end states for successful or unsuccessful ER sequences (with or without transfer to the internal initiators Level 1 PSA event trees);
- modification of correspondent event and/or fault trees of basic Level 1 PSA model.

Depending on the specific features of software used to construct PSA model, the modifications of system or functional fault trees may be implemented either by incorporation of additional house events allowing to change fault tree logic for different accident sequences or by exchange events. It shall be noted that incorporation of several top events to the hazard event tree may be required depending on the complexity of potential hazard development and its consequences. Depending on the nature of the hazard and of its secondary effects, their progression, timing/effectiveness of emergency response, the following consequences may be distinguished:

A. The hazard and its secondary effects do not affect safety-related SSCs directly or due to their progression. In this case the end state of correspondent sequence in the hazard event tree is OK (see Figure 10-1, sequence #1).

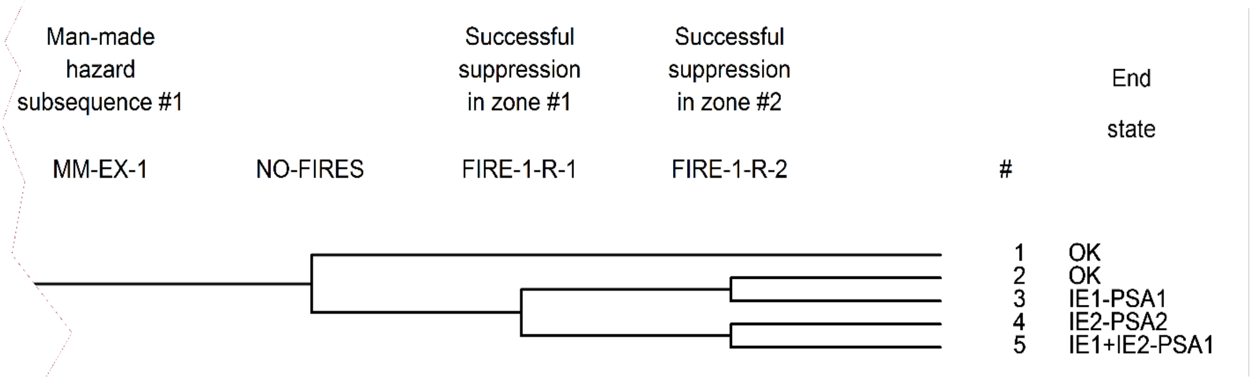
B. Hazard or its secondary effects may affect safety-related SSCs either directly or due to their progression, but cannot lead to initiating event. Emergency response can either prevent failure of safety-related SSCs or minimize number of failed SSCs. Similar to the above case the end state of correspondent sequence in the hazard event tree is OK (see Figure 10-1, sequence #2).

C. Hazard or its secondary effects either directly or due to their progression may cause an occurrence of IE accounted in the internal initiators L1 PSA if emergency response actions are not successful. Then unsuccessful emergency response sequence in the hazard event tree ends with a transfer to IE considered in L1 PSA (see Figure 10-1, sequences #3, 4). To reflect failures of equipment caused by the hazard (and, potentially, by emergency response) event tree and/or fault trees of basic L1 PSA model are modified.

D. Emergency response does not allow to preclude an occurrence of IE accounted in the internal initiators L1 PSA, but changes number/nomenclature of failed safety-related SSCs or provides additional means (e.g., mobile equipment or failed equipment recovery) to cope with the accident. Both sequences are accounted similar to unsuccessful ER path of case C, above. Additional means are accounted by incorporation of correspondent top event(s) representing new possibilities to perform the safety function to the L1 PSA ET. Probabilities of mobile equipment failure are accounted in the fault tree linked to this top event.

E. Hazard produces more severe consequences than initiating events accounted in L1 PSA for the internal initiators. In this case a representative IE from L1 PSA is selected as the end state of hazard event tree, and additional failures are reflected in correspondent event and/or fault trees (see Figure 10-1, sequence #5).

Figure 10-1: Sample hazard event tree with fire brigade response modelled


Man-made hazard subsequence #1
Successful suppression in zone #1
Successful suppression in zone #2
End state
MM-EX-1
NO-FIRES
FIRE-1-R-1
FIRE-1-R-2
#
1 OK
2 OK
3 IE1-PSA1
4 IE2-PSA2
5 IE1+IE2-PSA1

In emergency response evaluation and modelling the number of difficulties and uncertainties may arise that need to be resolved. Generally these are associated with multiple hazard consequences (e.g., multiple fires requiring to assume particular fire suppression sequence), uncertainty in their number and severity (e.g., fuel quantity spilled outside and inside the building affected by aircraft impact), unavailability of representative data to estimate emergency response success, assessing coordinated emergency response to the hazard consequences that requires sharing of available resources (e.g., necessity to address both off-site and on-site hazard consequences), etc. Resolution of these difficulties involves introduction of bounding assumptions that allow limiting the number of potential scenarios to be evaluated.

10.2 SPECIAL PROVISIONS

There are additional means that can be undertaken in order to be better prepared in case of emergency caused by external fire, explosion or aircraft crash. It concerns the following issues:

1. Emergency preparedness and response should also take into account accidents induced by external events; in particular the procedures and means should be predicted at the early phase of the development of emergency situation. In this respect layer of protection analysis (LOPA) is one of the possible techniques for risk assessment and optimization of emergency response.
2. Proper localization of standard emergency equipment should be carefully analysed in order to minimize the possibility of the occurrence of common cause failures and further development of emergency situation.
3. Early detection of external fire may be a key factor for successful response. Therefore fire monitoring and protection systems have to be designed, built and maintained in such a way that detection of fire should be as fast as possible. For existing NPP appropriate improvements of existing systems can be made after careful inspection.
4. As external fires and explosions can be mostly caused by transportation accidents the risk coming from such events can be minimized by undertaking decisions on the prohibition of transport of dangerous materials in the vicinity of NPP.

10.3 PREVENTIVE MEASURES

Based on the results of the hazards scenarios analyses and the evaluation of emergency response actions the preventive measures may be identified and implemented as deemed practical. This is especially important for the scenarios for which emergency actions are insufficient or cannot be implemented in timely manner to reduce the consequences below the acceptable level. Some examples of preventive measures are listed below [65]:

- optimization of the mobile equipment location and storage protection features;
- arrangement of additional passageways to the plant site in order to reduce arrival time of mobile equipment;
- preventive arrival and set up of mobile equipment (in the case of slow progressing external hazards);
- reduction of combustible materials adjacent to or on the nuclear site (see chapter 2.37 of NS-G-1.5 [33]), arrangement of exclusion zones in close proximity to the plant and along the electrical transmitting lines to prevent external fires propagation;
- isolation of the air intake of the main control room in the event of toxic clouds (see chapter 3.18 of NS-G-1.5 [33]);
- reinforcing the elements and structures that can cause seismic induced fires or block important access paths due to local structural collapse.

11 SOLUTION TO MODEL MULTI-UNIT FOR MAN-MADE HAZARDS AND AIRCRAFT CRASH PSA

11.1 ACCIDENT SEQUENCES

Man-made hazards and aircraft crash accidental events can simultaneously affect all the units at a site: this requires appropriate interface arrangements to deal with as well as with the potential domino effects (as explosions resulting in pressure or shock wave propagating from one unit to another). These site initiating events create the potential for similar accident sequences due to the failure of common or shared mitigation systems as well as the potential for common cause failure of identical components across units or inter-unit common cause failures. In addition, a single-unit event can trigger a cascade sequence to impact the other units: for units with shared or connected structures, internal fires, for instance consequential to an aircraft crash, can propagate from the first-impacted unit to affect the second unit.

11.2 CCF

The first step within the approach to assessing site integrated risk consists in the identification of the interactions between the units because of specific design features, operating practices, safety features and culture, economic considerations and construction layout: the multi-unit dependencies must be identified, accounted for and modelled within the PSA model of the site. These include principally the common elements shared by units in the site, including:

- common physical location (that is, single site or regional site),
- common or shared systems; examples of common or shared systems include e.g. switchyard, fire protection pumps/tanks, ultimate heat sink, where the risk issue is related to system failure impacting all the units and the system resources directed to one unit, not available to the second unit for instance,
- proximity dependencies, where a common environment has the potential to affect multiple units: these apply to common or connected structures (like turbine building, auxiliary building, main control room); if there was an explosion with consequences on the site and two units were located very close together, the same explosion could affect both units,
- human and organizational dependencies, addressing shared staff resources, like the shared operators and FLEX equipment, whose action can be challenged by the event occurrence,
- unit interconnections in the form of cross-tie systems and swing equipment, such as emergency diesel generators,
- identical components (that is components with same design and operation) with the potential of cross-unit common cause failures.

These dependencies are to be modelled somehow in the site PSA framework. In order to accomplish the task, for instance, the dependencies of all front-line systems are to be defined in a dependency matrix. This approach is already typically performed for single-unit PSAs and includes only hard physical connections, such as a motor-operated valve needing to have power from a predefined source. These matrices allow the PSA model developer to know what to consider when creating the system fault tree. Using the base PSA, the initiating events, shared connections, and identical components would be developed. As regards human and organizational dependencies, one can resort to human reliability analysis.

11.3 MULTIPLE INITIATORS

In the multi-unit context, an external hazard can induce initiating events which can impact only one unit (single unit IE) or more than one unit (multi-unit IE). Most of the external hazards may affect more than one unit, but not always a multi-unit IE is induced, due to inherent existing differences between the site units (position, design).

Between the causes that could induce multiple IE, the following should be analysed [66]:

- *Shared Connections* - Links that physically connect SSCs of multiple units (spent fuel pool cooling system, circulating water system, reactor component cooling water system, high, medium and low voltage AC distribution systems);
- *Shared vulnerabilities* in case of external hazards - shared SSCs, shared instrumentation and controls.

A shared system means multiple initiation points for the sequence of events, but the interactions can affect the entire sequence (not just the initiator). The unavailability of site shared fire protection could occur, along with the ventilations vulnerability in case of external explosion.

- *Proximity Dependencies* - A single environment has the potential to affect multiple units (ultimate heat sink, containment, non-safety DC electrical and essential AC distribution system, control room HVAC). This is applicable to common or connected structures (like turbine building, auxiliary building, main control room); for instance, an explosion could impact two units located very close.
- *Human and Organizational Dependencies* - Shared control room, operator staffing more than one reactor, same emergency organization staff, decision-maker overseeing more than one reactor or more than one operator.

According to their impact on the multi-unit context, the hazards could be categorized in two large classes:

- Hazards that will always affect multiple units (direct impact): seismic events; strong wind; tsunami; external floods; external fires; freezing rain; low/high air temperature; humidity; thunderstorm; extreme precipitation (rain, snow), truck crash in switchyard;
- Hazards that will affect multiple units only under certain conditions: aircraft crash; offsite explosions, biological fouling.

The external fires could have the capacity to affect multiple units when occurring. Aircraft crash and external explosions can affect multiple units under specific conditions, like in the case of proximity dependencies.

Some hazards affect multiple units simultaneously, but we have also cases when an accident that initially impact only one unit can cascade or propagate to others on the site. The analysis need to consider whether the external hazard affects all the units of a site, and in case of a positive answer, if the magnitude of the hazard varies with the units. From the IE grouping point of view, events which affect one unit or multiple units should not be grouped together. Events which may be propagated from other units (including cascading events) (directly or via shared systems - as missile from one unit affecting the other units, fire spreading) should be considered, so given the unit IE, the conditional probability to face a multiple unit IE needs to be estimated.

The existing L1 PSAs for multi-unit stations are mostly developed on a single unit basis, where one unit is selected as the representative reference model unit. However, in some cases, the initiating events that can affect the selected model unit include events that originate outside of the selected reference model unit [66], [67].

11.4 CROSS CONNECTION BETWEEN DIFFERENT UNITS

For sites with multiple units, their appropriate independence should be ensured. The possibility of one unit supporting another could be considered as far as this is not detrimental for safety [68] [69].

One of the post-Fukushima requirements was related to the use of alternative systems and cross-connections between units [23]. Sharing systems between units is influenced by four factors: safety, operability, costs, and licensing considerations. There are different types of sharing, as follows [70]:

- a single system supports both units simultaneously (a single station-blackout diesel generator, or a fire protection system shared between units);
- full capacity, independent systems at each unit that can be cross-connected to support the other unit if necessary; an example of this type of sharing is the standby coolant supply system that provides the capability to cross-tie selected portions of the residual heat removal (RHR) systems between units.

A similar case is when full capacity, independent systems at each unit share standby or spare equipment (an installed spare pump that is shared between units).

Even if the actual issue was to reduce costs, while maintaining the safety, many plants have found that providing additional capabilities to cross-tie and back-up systems can be beneficial, particularly for systems like electric power (capability to cross-tie ac and/or dc power supplies) and cooling systems. For example, crediting the use of a cross-connection between the units' service water systems (additional protection when the service water cooling was lost at one unit) resulted in a 25% reduction in the CDF for each unit; provision of a cross-tie capability between the 4kV electrical safety buses at two units resulted in a 35% reduction in CDF [70]. In Japan "cross-tie of electric power supplies" among units at the multi-unit sites is taken into account in the internal events PSA because the cross-tie is one of the accident management measures. Based on the above mentioned, cross-connection of EDGs between units could be beneficial and worthy to be examined for a multi-unit site (as an accident management measure).

A system could be shared:

- via a cross-tie;
- having a common supply header (service water systems);
- having shared components.

Within a multi-unit, many systems, functions, and physical facilities are shared, including the control room, fuel handling system, fuel pool cooling and clean-up system, pump houses, radioactive waste treatment systems, fire protection system, potable and sanitary water system and switchyard. In case of systems sharing, there is the potential for inadequate operations when they are shared (the potential to have an inadequate number of available components or inadequate flow rates when are shared) [70].

11.5 CONSIDERATIONS

Most of the existing PSAs already account for shared equipment and systems, as well as cross-tie capability (including manual cross-tie from the unaffected unit) as allowed by design and procedures. If multi-unit considerations are taken into account in the PSA, and if a shared part has the capacity to support only one plant at a time, then a shared availability factor should be incorporated into the system fault tree, reflecting the probability that the other plant will not need the asset in order to meet minimal functional success criteria. The shared availability factor should include the human error probabilities of implementing the actions, and hardware failure probabilities. For the events that involve more than a single unit, the mitigating functions in the L1 PSAs could be modelled for the selected reference model unit, but it should reflect also the impact of the event on the other units. For example, the success criteria for common systems such as emergency power and water should reflect the demand requirements on the system following a common mode event that affects all units. The reduced availability of shared systems (or through inter-unit ties for specific systems) following events that could affect the supplying unit should be considered. It is necessary to review relevant system fault trees where operator action to cross-tie units is credited and to ensure the adequacy of actual plant and operator response to an event (e.g., time available for operator response vs. feasibility of recovery actions under changing environmental conditions). On the other hand the effect of options for backup power/water supply should be considered.

11.6 CONNECTIONS WITH OTHER FACILITIES OUTSIDE THE PLANT

The framework for site assessment should include as well the “site configuration” with other facilities, as a multiple source area, which prompts new scenarios by the interaction between/among units and the other facilities, which are as well radioactive sources on the site, like the irradiated fuel in the spent fuel pool. These interactions can create more challenging accident sequences than sequences evaluated for a single plant, increasing the site risk, particularly in terms of radioactive releases (i.e. LRF) and health effects. This is the case, for instance, of a multi-unit configuration for a two units site with a common spent fuel pool, taken as an illustrative example. Clearly the spent fuel state is dependent on the configuration of the two units, which is whether both units are in operation or one in operation and the other in a refuelling outage or maintenance outage.

12 L1 PSA QUANTIFICATION

The L1 PSA models for man-made hazards shall encompass dangerous phenomena linked to the industrial environment, the dangerous goods transportation (by road, by rail or by ship) and the aircraft crash. Hazards such as fire, explosion or toxic release can then occur and have to be assessed regarding the nuclear facility safety objectives. However, physical processes for same types of fires and explosions needs very complex model if high accuracy has to be achieved. Moreover, the results of external events PSA are sensitive to the modelling of dependencies between initiating events and safety system failures as well as between failures of different safety systems which was described in chapter 8 of this report. It makes quantification of the man-made hazard or aircraft crash PSA much more challenging when compared to the internal events L1 PSA and some additional considerations must be given to achieve the usable results.

First of all, in the aircraft crash/man-made hazard PSA the multiple transients initiating failures should be taken into account which does not apply to the internal L1 PSA. These failures may place different, usually higher demands and challenges on plant systems and personnel concerning accident mitigation. Moreover, depending on the features of the plant designing the frequency of two simultaneous events may be much higher than the simple product of their particular frequencies. The calculation of the probabilities of cut sets containing correlated events involves multivariate integration of the joint probability distribution function of the cut set elements. This tends to increase the complexity of the calculation without sufficient justification of the numerical values of correlation coefficients between the different random variables for external induced failures.

Another issue is that the external events may lead to harsh personnel working conditions, problems in getting external aid and increases in emotional burden (site isolation as consequence of a fire, worrying about the situation of family members, adverse conditions for countermeasures requiring working outdoors). Sometimes, there are also specific emergency operating procedures, or plant systems and equipment designed for responding differently to an aircraft crash, fire or explosion event as compared to the response to other random initiators. Thus, the PSA for external hazards should take to account the potential for human response to be affected by the external event, and the available time for operator intervention for mitigation of external event effects needs to be considered. A shortage of time can affect the operator’s ability to think clearly, to consider alternatives and to perform the required tasks. The time pressure imposes heavy task load situations (task complexity) and high or extremely high stress level. It is important that the time available and the time needed to perform the action are considered together with many of the other PSFs and the demands of the accident sequence. The difference between the total available time and the time required (i.e. the extra time available) should be divided by the time required to assess the available time margin which is the key factor for the feasibility assessment.

The extension of mission time is especially important for the assessment of the feasibility of the recovery and repair actions. The failure to successfully perform such actions should be added to the accident sequence model thereby crediting the actions and further lowering the overall accident sequence frequency because it takes additional failures of these actions before the core is actually damaged. However, the influence of external event may not only increase the time to complete the tasks but also cause unsuccessful recoveries. Recovery actions that cannot be performed due to the impact of external hazards of certain magnitude should be removed from the L1 PSA model. Special attention should be paid to recovery actions, and to necessary actions to use the mobile equipment (pumps, DGs, etc.), especially when this equipment is shared between two or more units. The availability of site shared fire protection systems, mobile equipment and cars may be limited when the external event affects more than one unit.

The results of man-made hazards PSA should be presented and analysed in the form of probability/frequency distributions rather than point values. This requires an analysis of uncertainty to be performed. The outstanding role in the overall uncertainty assessment within aircraft crash/man-made hazards PSA play the uncertainties of HRA. The potential sources of these uncertainties are: dependences (e.g. common cognitive impact); stress; workload; communications, etc. The aircraft crash/man-made hazards PSA results should be interpreted in the context of internal L1 PSA to achieve the impact of external events on the overall risk associated with the facility operation. Based on the results of hazards scenarios analyses and evaluation of emergency response actions the preventive measures may be identified and implemented as deemed practical. This is especially important for the scenarios for which emergency actions are insufficient or cannot be implemented in timely manner to reduce the consequences below the acceptable level. Results of the aircraft crash/man-made hazards PSA may be used in optimization of mobile equipment location and storage protection features; arrangement of additional passageways to the plant site in order to reduce arrival time of mobile equipment; preventive arrival and set up of mobile equipment; reduction of fire loading materials adjacent to or on the nuclear site, arrangement of exclusion zones in close proximity to the plant and along the electrical transmitting lines to prevent external fires propagation; isolation of the air intake of the main control room in the event of toxic clouds; reinforcing the elements and structures that can cause seismic induced fires or block important access paths due to local structural collapse.

A very important issue is the comparison of existing experience in this area between partners having already developed such PSA, especially for long term accident sequences. This comparison should include the input data analysis and methods for the data collection, as well as assumptions, models and results of the man-made hazards PSA. Such a process could be carried out in the form of workshop and be focused on solving real problems. During this workshop one partner could present how the particular problem has been solved and the other participants might suggest some modifications. This approach allows for greater involvement of partners than only theoretical discussions.

13 CONCLUSION AND RECOMMENDATIONS

13.1 FEASIBILITY AND PRAGMATIC APPROACH

There are few basic questions that should be answered before performing a man-made hazard and aircraft crash PSA:

1. are there any connections between aircraft crash/man-made hazards and other external events, like seismic events, wildfires, etc.?
2. what are the connections and possible combinations between man-made hazards/aircraft crash PSA and internal event PSA?
3. how to take advantage from internal event PSA already done?
4. can man-made/aircraft crash initiating events be reduced to internal initiating event or other type of external initiating events already analysed?

An important feature of man-made and aircraft crash hazards is the fact that often either they can induce or they can be associated with other hazards. This leads to the type of analysis when the events under consideration are not independent. Therefore calculation of the probabilities (or frequencies) in L1 PSA, formally should be based on joint probability distribution functions, what gives additional complexity, as estimation of correlations is not straightforward. From a practical point of view, some techniques, allowing a reduction of the number of basic events, that should be considered (as described in Chapter 8) can be useful.

It should be also kept in mind that estimation of frequencies of man-made and aircraft hazards can be afflicted with big uncertainties. In particular for man-made hazards, in principle full quantitative risk assessment (QRA) studies should be done to obtain quite reasonable results. This concerns both frequencies of the occurrence of external man-made hazards (fires, explosions, toxic releases), and the analysis of possible consequences of such events. Therefore, for the latter, in practice a deterministic approach can be utilized to perform the important step of the analysis: from hazard to initiating event.

13.2 RECOMMENDATIONS

There is no doubt that the man-made hazards should be considered as part of standard PSA study for external initiating events. In order to perform the study effectively, as much as possible, the results of internal events PSA (or other external) should be utilized.

The need to incorporate external man-made hazards, like accidents with flammable, explosive or toxic substances strongly and aircraft crash depends on the location of the NPP and preventive measures taken. Occasionally, a major accident in a stationary chemical plant in the region may induce other initiating event (like wildfire), however this is a rather rare situation and appropriate planning can also minimize such a risk. The most dangerous are, obviously, combinations of hazards (like fire and explosion, especially as combination of external and internal hazards) that impact the plant more severely than each of the single hazards. Also these analyses should be performed, if possible using the internal events (including internal hazards) PSA studies already done.

It should be mentioned, that the hazards related to aircraft crash and transportation accidents with dangerous substances can be also considered from a security perspective, and if such type of analysis (like a security vulnerability analysis) has been performed, the results can be reflected in PSA studies.

14 LIST OF OPEN ISSUES

In this chapter, some issues that need more research or experience from application are mentioned:

- the practical modelling in PSA of the secondary (indirect) effects of an aircraft crash,
- more accurate models predicting the number of generated missiles and their dispersal in case of explosions,
- methodology on how to avoid double counting of aircraft crashes when both the background aircraft crash rate and the airway related crash rates are assessed and summed up,
- methodology for the assessment of impact mass and impact velocity distributions for each aircraft type,
- methodology to identify those impact zones that are hit by an aircraft having only secondary (hence no primary) effects on safety related SSCs,
- guidance for each representative aircraft or aviation category on the way to estimate:
    - fire effects distances based on the amount of fuel and other combustibles loads (cable, seats, luggage, etc.) of aircraft;
    - fuel quantity penetrating a building after an aircraft impact;
    - the effects distances of missiles based on statistical analysis of past accidents and tests.
- methodology on the definition of correlation among aircraft crash/man-made induced failure modes and on the quantification of correlation coefficients,
- methodology to take into account intended actions related to aircraft accidents as potential risk for NPP,
- methodology for the modelling and assessment of complex cases of superposition of the various impacts of the man-made and other types of hazards (or their combinations),
- specific open issues related to HRA are mentioned in chapter 9.4.

15 LIST OF REFERENCES

[1] IRSN and FKA, "Minutes and recommendations of the ASAMPSA_E Uppsala End-Users workshop (26-28/05/2014), IRSN PSN-RES/SAG/2014-00335," IRSN, 2014.

[2] NRC, "Regulatory Guide 1.91, Evaluations of Explosions Postulated to occur on Transportation Routes Near Nuclear Power Plants," NRC.

[3] A. Wielenberg (GRS) et al, "Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA," Reference IRSN PSN-RES/SAG/2017-00017, Technical report ASAMPSA_E/WP30/D30.7/2017-31 volume 2.

[4] IAEA, "Tecdoc draft: Assessment of Vulnerabilities of operating nuclear power plants to extreme external events, R0D6," Vienna Austria, 10 August 2015.

[5] J. M. a. K. WERTS, "The use of overpressure exceedance curves in building siting," in *Spring Meeting & 7th Global Congress on Process Safety*, Chicago IL, 2011.

[6] Center for Chemical Process Safety, "Guidelines for Chemical Transportation Safety, Security, and Risk Management," 2008.

[7] J. Byrne, "The calculation of aircraft crash in the UK, AEA Technology plc Contract Research Report 150/1997," 1997.

[8] U.S. Department of Energy, "Accident analysis for aircraft crash into hazardous facilities, DOE-STD-3014-2006," Washington, DC, 2006 May.

[9] Swiss Federal Nuclear Safety Inspectorate, "Probabilistic Safety Analysis (PSA): Quality and Scope, Guideline for Swiss Nuclear Installations, ENSI-A05/e," 2009 March.

[10] BULATOM, "“Risk Assessment and Development of Protection Capacity for Critical Infrastructures due to Air-craft Attack," in *” RISK PROTEC CI, Results of a European R&D Project, edited by F.O. Henkel and M. Kostov*, Sofia, 2104.

[11] Center for Chemical Process Safety, American Institute of Chemical Engineers, "Guidelines for Chemical Process Quantitative Risk Analysis, Second Edition," New York, 2000.

[12] Center for Chemical Process Safety, American Institute of Chemical Engineers, "Guidelines for Chemical Transportation Risk Analysis," New York, 1995.

[13] TNO Yellow Book, "Guidelines for Quantitative Risk Assessment," 1999.

[14] TNO Red Book, Methods for determining and processing probabilities, 2005.

[15] Safety, Center for Chemical Process, "Guidelines for consequence analysis of chemical releases, Table 1.2," 1999.

[16] R. Alzbutas, J. Augutis, R. Krikštolaitis and E. Ušpura s, "Uncertainty and Sensitivity Analysis in Aircraft Crash Modelling, ISSN 1642-9311, Proc. of The 3-rd Safety and Reliability International Conference KONBiN‘03, V2, p. 267–274," Gdynia, Poland, 2003.

[17] E. Hofer, "Sensitivity analysis in the context of uncertainty analysis for computationally intensive models, Computer Physics Communications, 117, p. 21-34," Elsevier Science, 1999.

[18] C. Kimura, D. Sanzo and M. Sharirli, "An Approach to Estimate the Localized Effects of an Aircraft Crash on a Facility, Energy Facility Contractors Group (EFCOG) Safety Analysis Workshop," San Fancisco Bay Area,

California, May 1-6, 2004.

[19] K. Decker and H. Brinkman, "List of external hazards to be considered in ASAMPSA_E, reference ASAMPSA_E/WP21/D21.2/2017-41, report IRSN IRSN PSN-RES/SAG/2017-00011," 2017.

[20] OECD/NEA, "PROBABILISTIC SAFETY ANALYSIS (PSA) OF OTHER EXTERNAL EVENTS THAN EARTHQUAKE, NEA/CSNI/R(2009)4," March 2009.

[21] M. Knochenhauer and P. Louko, "SKI Report 02:27, Guidance for External Events Analysis," February 2003.

[22] IAEA, "IAEA SAFETY STANDARDS SERIES No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants," Vienna, 2010.

[23] Kumar M, "Lessons of the Fukushima Dai-ichi accident for PSA, reference ASAMPSA_E/WP30/D30.2/2017-32, IRSN PSN-RES/SAG/2017-00021".

[24] B. G., "Risks disasters and accidents in key infrastructure, Scientific-practical Conference “Risk management in energetics, infrastructure and utilities”," Blagoevgrad, 26th Nov 2006.

[25] B. G. and K. J. J., "Comparative evaluation of two approaches to the fire hazard risk management in the nuclear power plant Kozloduy, Bulgaria. Balkan Environmental Association.," 2001.

[26] B. G. and K. J., "Determination of Combined effect on the Human Health of Toxic Air Pollutants Formatted During Fires in Bulgaria, 4th International conference of the Balkan Environmental Association “Transboundary Pollution”," Edirne, Turkey, 18-21 October 2001.

[27] ASAMPSA_E, "D22.1 Summary report of already existing guidance on the implementation of External Hazards in extended Level 1 PSA," 2015.

[28] I. Ivanov et al, "Environmental Impact Assessment Report of Kozloduy NPP, NEK," Sofia, 2000.

[29] "Risk analysis of internal fires. Update of existing PSA level 1 for Units 5 and 6 NPP "Kozloduy", Risk Engineering".

[30] IAEA, "IAEA-TECDOC-1134, Use of operational experience in fire safety assessment of nuclear power plants," Vienna, 2000.

[31] EPRI/NRC, "NUREG/CR-6850, EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, EPRI 1011989," September 2005.

[32] B. G. and K. J., "Retrospective Fire and Explosion Risks Management of Crude oil Carriers, 8th International Conference on stability and handling of liquid fuels (IASH)," USA, Colorado, Steamboat Springs, September 14-19, 2003.

[33] IAEA, "IAEA Safety Guide No. NS-G-1.5, External events excluding earthquake in the design of Nuclear Power Plants".

[34] IAEA, "IAEA Safety Standard No. NS-R-1, Safety of Nuclear Power Plants: Design".

[35] IAEA SSR2/1 Rev 1, "Safety of Nuclear Power Plants," 2012.

[36] P. Bester, "Implications of The Fukushima Daiichi Accident on the Regulatory Framework in South Africa, IAEA Technical Meeting on Developing Methodologies for Complementary Assessment of Nuclear Power Plants' Robustness against the Impact of Extreme Events," Vienna, 7-11 July 2014.

[37] T. K. e. al., "Development of Implementation Standard Concerning the Risk Evaluation Methodology Selection for the External Hazards, The Probabilistic Safety Assessment & Management conference Honolulu," Hawaii, June 22-27, 2014.

[38] "NEA/CSNI/R(2014)9 Proceedings of the OECD Workshop on PSA OF NATURAL EXTERNAL HAZARDS INCLUDING EARTHQUAKE," Prague, Czech Republic, June 17-20 2013.

[39] L. Burgazzi, "Implementation of External Event Modelling in Advanced PSA Studies, International Experts' Meeting on Strengthening Research and Development Effectiveness in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA Headquarters," Vienna, 16-20 February 2015.

[40] L. A. E.-S. M. Kuzmina I., "An Approach for Systematic Review of the Nuclear Facilities Protection against the Impact of Extreme Events," in *(Proceedings of the Nordic PSA Conference - Castle Meeting 2011, 5-6 September 2011, Stockholm, Sweden*, 2011.

[41] L. A. H. P. K. J. K. T. S. V. Kuzmina I., "The Fault Sequence Analysis Method to Assist in Evaluation of the Impact of Extreme Events on NPPs," in *Proceedings of the Nordic PSA Conference - Castle Meeting 2013, 10-12 Apr*, Stockholm, 2013.

[42] B. O. Y. L. K. I. L. A. E.-S. M. Sörman J., "Method for analysing extreme events," in *PSAM 12, June 2014*, Honolulu Hawaii, 2014.

[43] K. M. e. al., " Extreme Event Analysis – A benchmaking study at Armenian Nuclear Power Plant to examine plant robustness against the impacts of Extreme Events," in *13th International conference on PSAM 13* , Seoul Korea, 2016.

[44] EPRI, "EPRI-1002989".

[45] K. A. D. S. M. K. A. Andonov, "Parametric Study on the Floor Response Spectra and the Damage Potential of Aircraft Impact Induced Vibratory Loading," *Journal Of Disaster Research vol. 5. No. 4,* pp. 417-425, 2010.

[46] F. A. A. M. Kostov, "Safety assessment of A92 reacotr building for large commercial aircraft crash," in *ransactions, SMiRT 21, 6-11 Nov. 2011*, New Delhi, India, 2011.

[47] D. Halm et. al., "Preliminary assessment of the probabilistic risk of nuclear power plant against to the aircraft impact loading,," in *Probabilistic Safety Assessment and Management PSAM 12,*, Honolulu, Hawaii, June 2014,.

[48] J. Hauschild and H.-P. Berg, "HOW TO ASSESS EXTERNAL EXPLOSION PRESSURE WAVES, RT&A # 01 (24), (Vol.1)," March 2012.

[49] IAEA, "IAEA Safety series No. 50-P-7, Treatment of external hazards in probabilistic safety assessment for nuclear power plants," Vienna , 1995.

[50] IAEA, "IAEA Safety standards series No. NS-G-3.1, External human induced events in site evaluation for nuclear power plants," IAEA, Vienna, 2002.

[51] U.S. Nuclear Regulatory Commission, "NUREG/CR-6350, A Technique for Human Error Analysis (ATHEANA)," July 1996.

[52] EPRI, "EPRI TR 101711, SHARP1- A Revised Systematic Human Action Reliability Procedure," December 1992.

[53] U.S. Nuclear Regulatory Commission, "NUREG/CR-1921, Fire Human Reliability Analysis Guidelines, EPRI 1023001, EPRI/NRC-RES," July 2012.

[54] D. Gertman, H. Blackman, J. Marble, J.Byers and C. Smith, "NUREG/CR-6883, The SPAR-H Human Reliability Analysis Method," August 2005.

[55] U.S. Nuclear Regulatory Commission, "NUREG-1842, Evaluation of Human Reliability Analysis Methods Against Good Practices," September 2006.

[56] "NEA/CSNI/R(2015)1, Establishing the Appropriate Attributes in Current Human Reliability Assessment

Techniques for Nuclear Safety," March 2015.

[57] "NEA/CSNI/R(2009)6, FIRE Project Report: "Collection and Analysis of Fire Events (2002-2008) - First Applications and Expected Further Developments”".

[58] IAEA, "GS—R 2. Preparedness and response for a nuclear or radiological emergency, IAEA safety guide," Vienna, 2002.

[59] "NUREG 1805, Fire Dynamics Tools (FDTs): Quantitative Fire Hazard Analysis Methods for the U.S. Nuclear Regulatory Commission Fire Protection Inspection Program Final Report," 2004.

[60] "NUREG-1934, Nuclear Power Plant Fire Modeling Application Guide (NPP FIRE MAG), Final Report," 2012.

[61] "NUREG/CR-5042, Evaluation of External Hazards to Nuclear Power Plants in the United States," 2000.

[62] N.Fritze and H.P.Berg, "First experiences from international databases on nuclear power plant fire brigade activities, SMiRT21 12th International seminar on fire safety in nuclear power plants and installations, GRS-A-3651, p.268-277," München, Germany, September 13-15, 2011.

[63] P.Contri, A.Gürpinar and U. Schneider, "Large fire scenarios in relation to sabotage of nuclear installations, 18th International Conference on Structural Mechanics in Reactor Technology (SMiRT 18), SMiRT18-J03-4," Beijing, China, August 7-12, 2005.

[64] "NUREG-1852, Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire," 2007.

[65] D. Bogdanov, "Nuclear power plant station blackout – causes, risks, options to mitigate the consequences. Proceedings of the IVth conference of the faculty of electrical engineering of TU-Sofia, Sozopol, Bulgaria, 2012.," 2012.

[66] "International Workshop on Multi-unit Probabilistic Safety Assessment (PSA)," Ottawa, Canada, November 17-20, 2014.

[67] "COG-13-9034 report, “Development of a Whole-Site PSA Methodology”," February 2014.

[68] "WENRA Reference level demands, Issue E – Design Basis Envelope for Existing reactors, Chapter 9 “Design of safety functions”".

[69] IAEA, "IAEA Specific Safety Requirements No SSR 2/1 Other design considerations - Requirement 33 “Sharing of safety systems between multiple units of a nuclear power plant”".

[70] M. D. Muhlheim and R. T. Wood, "ORNL/LTR/INERI-BRAZIL/06-01, Design Strategies and Evaluation for Sharing Systems at Multi-Unit Plants Phase I," August 2007.

[71] R. (. E. I. Alzbutas, "New NPP Risk Zoning in Relation to PSA and Risk of External Events (Application to Iris Design), IAEA Technical Meeting on Probabilistic Safety Assessment for New NPPs’ Design," IAEA, Vienna, Austria, October 1-5 2012.

[72] US Nuclear Regulatory Commission NUREG 0800, "Standard Reveiw Plan," 2010.

[73] NUREG/CR-4550 , "Analysis of Core Damage Frequency, Surry Power Station, Unit 1, External Events, Sandia National Laboratories, SAND86-2084," 1986.

[74] H.-P. Berg, "Risk Assessment of Aircraft crash onto a nuclear power plant," *Reliability & Risk Analysis: Theory and Applications # 01 (20) Vol.2*, pp. 38-51, March 2011.

[75] D. Bogdanov, "Aspects of the defence in depth of the nuclear power plant in respect to some external events," Proc. of the VIth Conference of the Faculty of Eletrical Engineering of TU SOfia, Sozopol, Bulgaria, 2014.

[76] EASA, " Regulation – Amendment of Implementing Rule 2042/2003, Dated: 13/01/2012, Version 1.," 2012.

[77] L. R. Consulting, "RiskSpectrum HazardLite, User guide version 1.1.0, ,," Lloyd's Register Consulting, Sweden, 26th February 2015.

[78] "NUREG/IA-0216, VOLUME 1, INTERNATIONAL HRA EMPIRICAL STUDY – PHASE 1 REPORT".

[79] "NUREG-1742, Perspectives Gained From The Individual Plant Examination of External Events (IPEEE) Program," 2001.

[80] I. I. e. al., "Environmental Impact Assessment Report of Kozloduy NPP, NEK," Sofia, 2000.

[81] D. Bogdanov, " Nuclear power plant station blackout – causes, risks, options to mitigate the consequences. Proceedings of the conference of the faculty of electrical engineering of TU-Sofia, Sozopol, Bulgaria, 2012.," 2012.

16 LIST OF TABLES

17 LIST OF FIGURES

APPENDIX 1 – INTERFACE LEVEL 1 – LEVEL 2 FOR MAN- MADE HAZARDS

This appendix provides recommendations regarding the definition of Plant Damage States (PDSs), which are used as boundary conditions in the L2 analyses, for the man-made external hazards initiators groups that have been identified to be of most interest by the end-users groups after collection and discussion of results from the ASAMPSA_E end-users survey [A1]. The general discussion on definition of PDSs and protocols and recommendations for performing PSA are to be found in the ASAMPSA2 guidelines ([A2] and [A3]).

Most of the discussion is the same for each of the external events initiator groups, according to experience gained from performing and/or reviewing complete and integrated analyses, and therefore the sections are given for completeness and to make the discussion self-contained for each initiator group and with small variations from each other, according to initiator group expected consequences. The only exception is for the “biological infestation” group, for which no specific analysis has been performed to date. For this group, guesses are given, on the basis of potential (or known) infestation incidents.

Definition of Plant Damage States (PDS) for external explosion, external fire, and aircraft crash INITIATING EVENTS

The discussion for external explosion, external fire and aircraft crash initiating events is based on analyses that considered all these potential initiating events, including impact of large commercial aircraft, civilian aircraft, and military plane crashes. The resulting consequences varied from “localized” (as for internal fires) to widespread and catastrophic.

Since the definition of, and collection of data for the PDSs are tasks that may fall upon different teams that perform the analyses (L1 and L2 teams), this section is intended primarily for L2 experts.

It must be stressed, as was done for analyses of internal events ([A2] and [A3]), that this task involves close interaction between the teams performing the analyses. L2 PSA personnel has knowledge about what boundary conditions are necessary for characterization of accidents after core damage, and L1 personnel knows how accidents progressed up to that point and why core damage occurred. Therefore, this part of the works profits from feedback and potentially iterative work between the two teams in the course of defining the PDSs.

To this point, it is recommended that the L2 team in general takes cognizance and understands thoroughly the definition of systems success criteria used in the L1 study, and in particular for accidents initiated by external explosion, external fire and aircraft crash events, what are the potential initiator-dependent systems failures (failure of systems that occurred as a direct impact from the initiator) and –independent failures (failure of systems that may have occurred after accident initiation, at a time that for the most part cannot be specified by L1 analyses).

It is also strongly recommended that the L2 team familiarizes themselves with the results of L1 in terms of individual accident sequences or Minimal CutSets (MCSs) that show the chain of failures (initiator, dependent systems failures, component failures, and operator errors) that ended in core damage. Operator errors in L1 are of particular importance for L2 analyses if operator interventions that could be considered as part of SAMGs are introduced in L1 in conjunction with interventions that are part of EOPs. This is the case for instance for containment venting, initiation of containment sprays, or initiation of firewater (or equivalent emergency system) injection in the RCS prior to core damage in BWR plants. The danger is that these systems may be over-credited in L2, if accident progression to the time of core damage is not thoroughly understood by the L2 teams.

In addition, it is also strongly recommended that the L2 team responsible for the definition of PDSs understand the role of auxiliary systems (such as compressed air, auxiliary and component cooling water systems) in the process of preventing core damage in particular accident scenarios, since these systems may fail as dependent on the initiator, without immediate failure of the primary safety systems.

The definition of PDSs that has been used for the internal events analysis has to be verified for applicability to Level 1 accident sequences that are initiated by external explosions, external fires and aircraft crash events. The combination of dependent and independent systems failures due to external explosion, external fire and aircraft crash events-induced sequences may require the definition of additional PDSs that were not considered possible for internal events. Finally, operators may be required to perform actions (such as venting of the containment prior to core damage) that would not be considered under accidents initiated by internal events and that change the status of the containment before the beginning of L2 analyses.

Preliminary discussion of this topic within WP40 has led to the conclusion that for the purpose of “presentation of results” and “analysis of results” (especially for importance analysis) it is strongly suggested to include one additional characteristic in the definition of PDSs that describes the group of initiators. Apart from this additional information, the traditional PDS characteristics seem to be suitable also for external explosion, external fire and aircraft crash events characterization.

Additional characteristics with particular importance for L2 PSA do not seem to be needed. Any example we could think of would be an accident with somehow catastrophic consequences in L1 (everything fails), so that any issue impacting L2 would be “mute”.

As a preliminary conclusion of the present document it seems that – apart from the initiating event itself – no additional PDS characteristics are needed.

References

[A1] Minutes of the ASAMPSA_E WP10 WP 21 WP22 WP30 technical meetings 8th-12th September 2014 Hosted by Vienna University in Vienna, Austria, WP5/2014-06.

[A2] Best-Practices Guidelines for L2PSA Development and Applications, Volume 1 - General, Reference ASAMPSA2, Technical report ASAMPSA2/WP2&3/ 2010-28, Reference IRSN - Rapport DSR/SAGR/2010-193, dated 19.09.2011.

[A3] Best-Practices Guidelines for L2PSA Development and Applications, Volume 2 - Best practices for the Gen II PWR, Gen II BWR L2PSAs, Extension to Gen III reactors, Technical report ASAMPSA2/D3.3/2013-XX, Reference IRSN - Rapport PSN-RES/SAG/2013-XX, dated 05.01.2013.

APPENDIX 2 – EXAMPLES OF NATIONAL EXPERIENCES ON MAN-MADE HAZARDS

ANNEX 2.1 EXAMPLE OF FRENCH APPROACH

The French Order [B1] requests that the external hazards to be considered in the demonstration of nuclear safety include:

- the risks induced by the industrial activities and communication routes, including explosions, hazardous substance emissions and aircraft crashes;
- earthquakes;
- lightning and electromagnetic interference;
- extreme meteorological or climatic conditions;
- fire;
- floods originating outside the perimeter of the basic nuclear installation, including their dynamic effect;
- malevolent acts;
- any other external hazard identified by the licensee or, if appropriate, that ASN considers must be taken into account;
- plausible combinations of the above hazards."

In practice, the French basic safety rules [B2] and [B3] are applied by the utility. They include the requirements described hereafter.

Man-made hazards shall encompass dangerous phenomena linked to the industrial environment, the dangerous goods transportation (by road, by rail or by ship) and the aircraft crash. Hazards such as fire, explosion or toxic release can then occur and have to be assessed regarding the nuclear facility safety objectives.

Spreading and ignition of flammable liquid towards the NPP and other possible propagation possibilities shall be considered, as well as effects of smokes on equipment or people.

These hazards are not supposed to challenge the following safety functions:

- emergency shutdown and evacuation of residual heat;
- spent fuel pool;
- treatment and confinement of radioactive waste.

Regarding industrial environment and dangerous goods transportation hazards, the French basic safety rules (RFS I.2.d) [B2] gives target thresholds for the probability of external hazards to lead to unacceptable radioactive releases for NPPs:

- the overall probability that, due to the man-made hazards, the premises may be the cause of unacceptable radioactive releases shall not exceed about 10^{-6} per year[7];
- specific objective for each of the three families of hazard (industrial facilities, pipes and dangerous goods transportation): the probability of unacceptable releases shall not exceed about 10^{-7} per year[1].

[7] Order of magnitude.

Regarding external hazards that may induce an overpressure, all French NPPs include a minimum safety design criteria: the nuclear island buildings is designed to withstand an incident overpressure of 50 mbar/300 ms.

An oil slick drifting to the NPP pumping stations is a specific hazard that has to be assessed. In this situation, the loss of the cooling source can occur:

- by clogging the filtering systems, which lead to a water flow depletion at the cooling pump inlets;
- by reducing the efficiency of heat exchangers.

This hazard is essentially mitigated by human actions and floating barriers.

For the aircraft crash assessment, a probabilistic approach is also implemented. French basic safety rule (RFS I.2.a) [B3] gives target thresholds for the probability of an aircraft crash to lead to unacceptable radioactive releases:

- the overall probability that, due to an aircraft crash, the premises may be the cause of unacceptable radioactive releases shall not exceed about 10^{-6} per year[1];
- specific objective for each of the three aircraft families (general aviation i.e. civil aircrafts under 5.7 tons, commercial aviation and military aviation): the probability of unacceptable releases shall not exceed about 10^{-7} per year[1].

Regarding aircraft crash hazards, French NPPs have a minimum safety design criteria. The nuclear island buildings are designed to withstand the crash of a CESSNA 210 (single-engine aircraft of 1.5 tons) and a LEARJET 23 (twin-engine aircraft of 5.7 tons). The crash speed is assumed to be 100 m/s.

In addition, each 10 years (periodical safety assessment), external hazards have to be reassessed. The same probabilistic thresholds are used, considering the frequency of each type of transport, accident data, the intensity of the different effects in case of accident (fire, explosion or toxicity) and the length of route onto which the accident could lead to significant effects on the facility. For the aircraft crash, the traffic and the accident data shall be updated.

The methodology to assess man-made hazards such as fires, explosions or toxic releases due to the industrial environment or the dangerous goods transport as well as the aircraft crash consists of the following steps:

- identification of external hazard sources and resulting hazardous phenomena;
- identification of safety targets that have to be protected;
- deterministic approach to establish scenarios that may affect these targets and estimation of consequences on nuclear safety;
- probabilistic approach for each accident scenario and compliancy with the safety requirements of the basic safety rules RFS I.2.d (industrial environment and dangerous goods transport) or RFS I.2.a (aircraft crash).

The annual probability P to have an inacceptable radioactive release due to an external man-made hazard is calculated with the formula:

$$P = P1 \times P2 \times P3$$

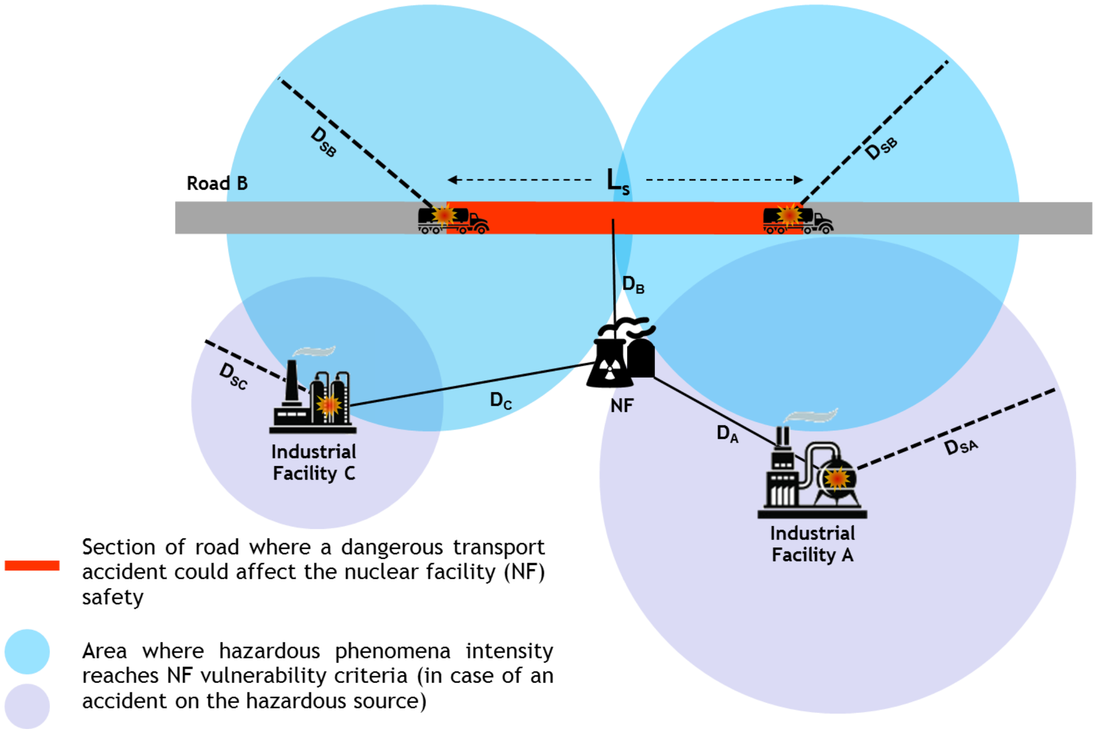
Where:

- P1: probability that an external hazard due to human activities affects the nuclear plant;

- P2: conditional probability of the unavailability of a function important for the safety. P2 = 0 if not any function important for the safety is affected by the external hazard;
- P3: conditional probability of an inacceptable radioactive release. P3 = 0 if the consequences of the radioactive release are acceptable.

In practice, if the deterministic approach concludes that safety targets are affected, the probabilities P2 and P3 are considered equal to 1 (and in this case, P = P1).

For example, consider a nuclear facility (NF), with a design withstanding an overpressure of 50 mbar, a nearby road B (on which mobile sources of hazards can be present) and two industrial facilities A and C (stationary sources of hazards). The nuclear facility and these external hazard sources are separated respectively by distances D_B, D_A and D_C (see figure below). Concerning the explosion risk assessment, the first step is to identify the hazard sources that generate, if an accident occurs, an overpressure greater than 50 mbar: in this case, only the industrial facility A and the road B could affect the safety of the nuclear facility (see figure below).


Road B
D_{SB}
L_S
D_{SB}
D_B
D_{SC}
D_C
NF
D_A
D_{SA}
Industrial Facility C
Industrial Facility A
🟥 Section of road where a dangerous transport accident could affect the nuclear facility (NF) safety
● Area where hazardous phenomena intensity reaches NF vulnerability criteria (in case of an accident on the hazardous source)

The different accident scenarios (unconfined vapour cloud explosion, pool fire...) with consequences on safety targets are assessed by a deterministic approach. For each scenario, the result of this step is the determination of the distance D_s where the hazardous phenomena intensity reaches the target vulnerability value (in this example, it's the maximal distance for an overpressure of 50 mbar). For the road B, the length of dangerous section L_s, for which the safety of the nuclear facility would be affected if an explosion scenario would occur, is calculated by the formula:

$$L_S = 2\sqrt{(D_{SB}{}^2 - D_B{}^2)} \quad \text{if } D_{SB} > D_B, \quad L_S = 0 \quad \text{if } D_{SB} \leq D_B$$

The probabilistic approach is based on the LANNOY simplified probabilistic model for mobile sources proposed in the document [B4] – an abstract of this book is given below. The annual probability P_{1x} for a road accident with scenario x is determined by the formula:

$$P_{1x} = P_a \times P_e \times S \times F \times P_{Sx} \times E_i \times L_S$$

where:

- P_a: frequency of an accident involving a dangerous good transport [accident/(vehicle x km)];
- P_e: probability to have a dangerous phenomenon (fire, explosion…) when an accident occurs [-];
- S: corrective factor to take into account the different types of route (highway, B-road…);
- F: annual number of dangerous goods transports [vehicle/year];
- P_{Sx}: probability that the scenario x occurs (leak size, drifting cloud…) [-];
- E_i: probability of unfavourable meteorological conditions [-];
- L_s: length of dangerous section [km].

In the above formula the last three items strongly depend on the scenario type and possible consequences. For example for fire, direct and delayed ignitions should be considered separately. Weather conditions influence the dispersion of the cloud but not the height of overpressure in case of direct ignition. This means that the selections of the scenarios should reflect such distinctions.

In the same manner, for a stationary source, the annual probability P_{1x} for an industrial facility with scenario x is determined by the formula:

$$P_{1x} = P_a \times P_e \times n \times P_{Sx} \times E_i \times U_{IS}(D_{SA} - D_A)$$

where:

- P_a: frequency of an accident implying a specific of dangerous good contain in an hazardous source (tank, storages, process…) [accident/year];
- P_e: probability to have a dangerous phenomenon (fire, explosion…) when an accident occurs [-];
- n: number of facility hazardous sources [-];
- P_{Sx}: probability that the scenario x occurs (leak size, drifting cloud…) [-];
- E_i: probability of unfavourable meteorological conditions [-];
- UIS: unit step function [-] with UIS = 1 if DSA ≥ DA and UIS = 0 if DSA < DA.

Abstract: *Analysis of unconfined air-hydrocarbon explosions - Deterministic and probabilistic studies of the accident scenario - Prediction of the overpressure effects (A. LANNOY, 1984) [B4].*

Among the potential hazards of industrial activity in the environment of nuclear sites, particular attention must be paid to fires and explosions of hazardous materials. Indeed, thermal radiation from such a fire close to the site could endanger the structures of the plant.

Similarly, an accidental explosion would cause an overpressure wave that could affect the buildings behaviour. This paper outlines a procedure that may be adopted for evaluating the consequences of accidents occurring:

- in industrial installations: refineries, chemical and petrochemical plants, storage areas, gas and pipe-lines containing liquid, gaseous or liquefied products;

- on means of communication (roads, railways, rivers and canals) carrying dangerous products (solid explosives, liquid, gaseous or liquefied hydrocarbons).

Among these dangers, the explosion of a gas cloud caused by the accidental release of a volatile product is an essential problem that may be encountered for protecting installations. To ensure safety, it is necessary to predict maximal overloads and design the installation accordingly, and for these purposes overpressure effects of a possible explosion must be quantified.

A posteriori analysis of accidental explosions that have actually occurred, taking as a basis a “total explosion yield“ defined from the damage observed and the potential energy of the explosive mixture, allows to evaluate the associated risks.

From analysis of actual accident statistics, probabilistic assessment methods have been developed (in particular for risks associated with means of communication), and typical accident scenarios in realistic and representative form have been established. Five main sequences have been pointed out:

- the formation of a fluid jet at the point of breakage,
- vaporization of the product and possibly formation of a liquid pool,
- atmospheric dispersion and drift of a gaseous cloud,
- thermal radiation from fire,
- unconfined explosion of the gaseous cloud.

The theoretical approach comes up against serious difficulties with the “explosion” event. This is because the present knowledge of the deflagration of gas clouds is not sufficient to permit development of methods that are conservative enough for safely calculations. Furthermore, it is unrealistic to take into consideration the case of ideal detonation of a gas cloud, which would lead to unnecessarily large overdesigning of the installations. The method adopted is thus based on analysis of actual accidents, and the TNT equivalent of these explosions is deduced from analysis of the damage.

These methods permit a coherent and realistic approach to an estimate of risks arising from industrial activities. Typical examples are given to illustrate the proposed method as a whole.

References:

[B1] Order of 7 February 2012 setting the general rules relative to basic nuclear installations - JORF (Official Journal of the French Republic) No. 0033 of 8 February 2012, page 2231 - Text No. 12

[B2] RFS I.2.d (7 May 1982) - REP - Principes généraux relatifs à la protection contre les agressions externes - Prise en compte des risques liés à l'environnement industriel et aux voies de communication (no English version available: NPP – General principles for protection against external hazards – assessment of industrial environment and dangerous goods transportation hazards)

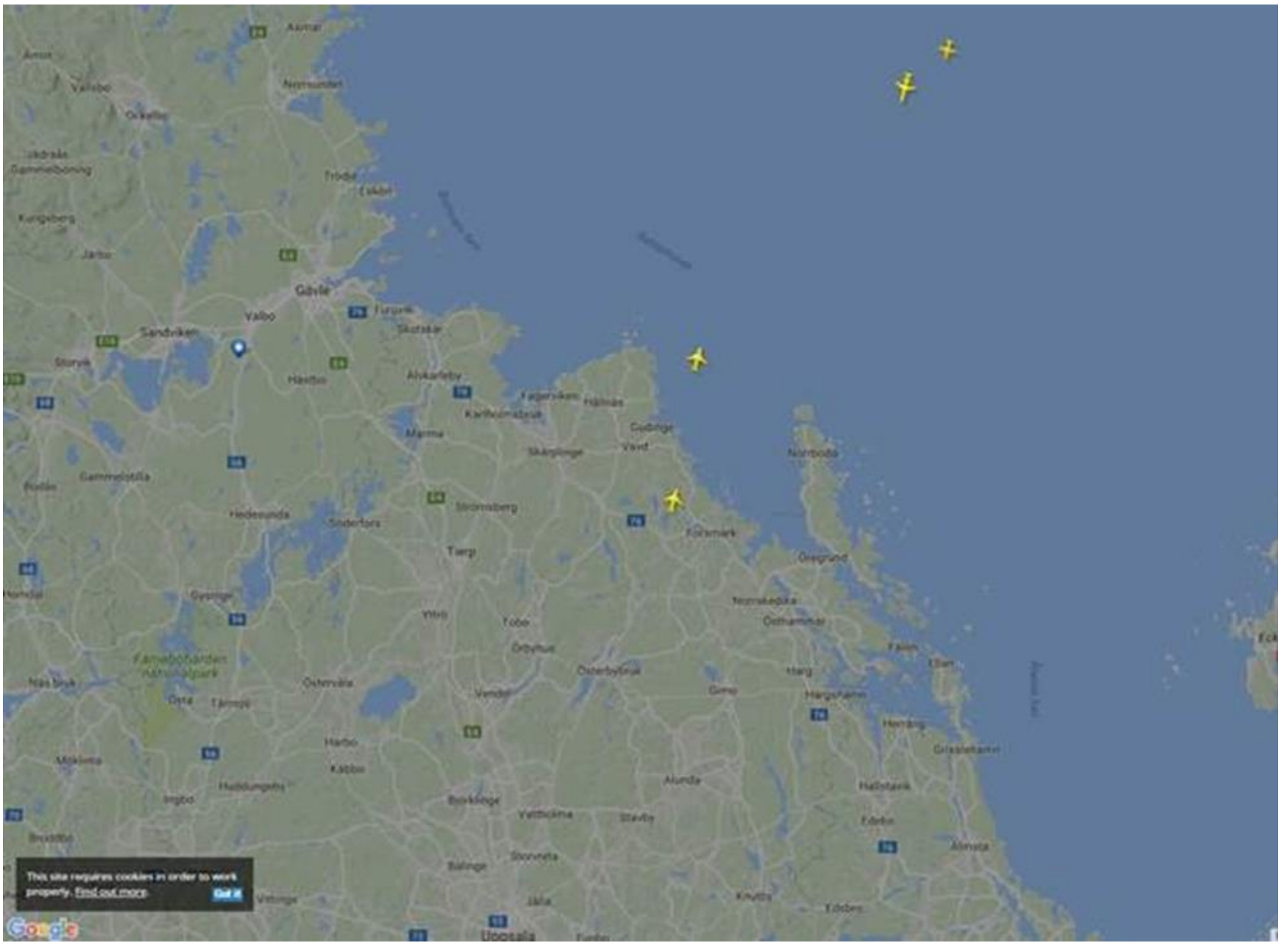
[B3] RFS I.2.a (5 August 1980) - REP - Principes généraux relatifs à la protection contre les agressions externes - Prise en compte des risques liés à la chute d’avion (no English version available: NPP – General principles for protection against external hazards – assessment of aircraft crash hazards)

[B4] André Lannoy – Analyse des explosions air-hydrocarbure en milieu libre – Etudes déterministe et probabiliste du scénario d’accident - Prévision des effets – EDF – 1984 (in French)

ANNEX 2.2 EXAMPLE OF SWEDISH EXPERIENCE

At Forsmark NPP the nearest commercial airport is Stockholm Arlanda Airport approximately 100 km southwest of Forsmark. Flights to northern Sweden and Finland pass over Forsmark, but at high altitude and the number of aircraft are relative small. Over for example Olkiluoto NPP in western Finland there is likely even less air traffic. In relatively sparsely populated countries like Sweden and Finland, there is no absolute demand to model aircraft crash in a standard PSA. A discussion why it is screened out may be sufficient in areas with little air traffic.

Below the differences in air traffic is illustrated by two pictures from www.flightradar24.com obtained a few minutes before 9 a.m. on August 4, 2016. The first picture is the area around Forsmark, while the second picture below is a comparison with the area around London, United Kingdom. Both maps have the same scale.



Towcester
Bedford
Banbury
Milton Keynes
Bletchley
Buckingham
Biggleswade
Letchworth Garden City
Saffron Walden
Haverhill
Sudbury
Ipswich
Dedham Vale AONB
Felixstowe
Harwich
Colchester
Braintree
Bicester
Luton
Bishop's Stortford
Witham
Clacton-on-Sea
Aylesbury
Oxford
Witney
St Albans
Harlow
Chelmsford
Maldon
Abingdon
Chiltern AONB
High Wycombe
Didcot
Wantage
Basildon
Southend-on-Sea
Canvey Island
Maidenhead
London
Ilford
Windsor
Reading
Bracknell
North Wessex Downs AONB
Thatcham
Dartford
Grays
Croydon
Rochester
Isle of Sheppey
Whitstable
Margate
Broadstairs
Camberley
Woking
Epsom
Farnborough
Sevenoaks
Maidstone
Faversham
Canterbury
Basingstoke
Guildford
Surrey Hills
Andover
Whitchurch
Tonbridge
Royal Tunbridge Wells
Deal
Alton
Crawley
Kent Downs AONB
Dover
Haslemere
Winchester
Horsham
High Weald AONB
Tenterden
Folkestone
Haywards Heath
South Downs National Park
Eastleigh
Southampton
New Romney
Rye
Battle
Fareham
Havant
Chichester
Arundel
Worthing
Brighton
Lewes
Hailsham
Hastings
Portsmouth
Bognor Regis
Newhaven
Eastbourne
Isle of Wight
This site requires cookies in order to work properly. Find out more.
Got it
Google
Map data ©2016

At Swedish NPPs, to perform the detailed aircraft crash analysis data on location and volumes of air traffic in the region is obtained. The methodology used is based on 'German Risk Study'. Aircraft crash frequencies from a number of sources are reviewed. Frequency of being hit by a crashing airplane is around 2E-8/year; hence the event is screened out using the SKI 02-27 screening approach (criterion C2 frequency).

APPENDIX 3 – METHODOLOGIES FOR ESTIMATING FREQUENCIES OF AIRCRAFT CRASH RATES

The approach discussed here uses the methodologies of [7] and [8] as a basis and supplements it with other related documents as well as with additional considerations to ensure the applicability of the method in a PSA context.

According to [7], the quantification of the background crash rate may be based on the assumption that the number of aircraft crashes follows a homogeneous Poisson process, where the crash rate is the constant, stationary parameter of the process. However, it should be justified by hypothesis testing, whether the Poisson distribution is an appropriate approximation. To ensure that: 1) the process is stationary and there is also an appropriate amount of data available to statistical calculations, and 2) the input data reflects the most up-to-date aerial activity, flying patterns and relatively modern aircraft types, at least a 10-year period of data is recommended to be taken into consideration for the hazard assessment. The application of the Poisson process for quantifying the background crash rate enables the use of the x^2 (chi-squared) distribution to determine the estimated crash rate at any predefined level of confidence. It is recommended to assess primarily the crash rate related to a=0.5 exceedance probability as the best estimate value. Besides, the crash rate with a=0.05 exceedance probability is reasonable for characterizing uncertainty. The background crash rate can be computed by using the following formula [8]:

$$F_B = \frac{\chi^2_{1-\alpha,2(r+1)}}{2 \cdot T \cdot A}$$

where:

F_B	background crash rate specific to a unit ground area (relevant to a specific aircraft category) [event/year/unit area],
x^2	chi-squared distribution for (1-a) confidence level,
a	exceedance probability,
r	number of crashes occurring in time period T on the area A [event],
T	time period taken into consideration [year],
A	area taken into consideration [km^2].

On one hand the background crash rate can be assessed by taking into account all crashes occurred in the region/country assuming that crashes are equally distributed over the area considered, that is called homogenous background crash rate. On the other hand inhomogeneous background crash rates may be determined by considering aerial features (e.g. restricted or prohibited airspace, short or long distance from airports) specific to a site and its vicinity. Special aerial features may only be credited if their assumed impact on the crash rate can be justified.

A large number of aircaft crashes occur in the vicinity of airports. Consequently, the additional risk due to airports in the vicinity of the site has to be quantified. As a first step, airports having a negligible effect on site specific crash rate due to large distance should be screened out from detailed assessment. A commonly applied screening approach described in [50] in detail is as follows. The potential hazards arising from aircraft crashes are taken into account if airports are located within 10 km of the site for all but the biggest airports. Large airports can be screened out, if the distance d in kilometres to the site in question is less than 16 km and the number of projected yearly flight operations is less than 500d^2. Where the distance d is greater than 16 km, the hazard should only be considered if the number of projected yearly flight operations is greater than 1000d^2. For military installations or air space usage such as training bombing, targeting or firing ranges, which might pose a hazard to the site, the hazard should be considered if there are such installations within at least 30 km of the site. The range of the respective means (arms, firing equipment, launching systems) must be estimated in order to be correctly taken into account. Long-range artillery, missiles launching systems may need a distance more than 30 km.

It is appropriate to assume that operations at each runway is equally distributed among take-offs and landings (i.e. 50% of runway operations is due to take-off and 50% due to landing) [7]. Several empirical formulas have been developed to calculate the crash rate in the vicinity of airports taking into account mostly the number of take-offs and landings (*N*), the crash probability per movement of a landing or take-off accident (P_A) as well as the site position relative to the runway (*R, θ*). The straightforward, easy to use approach of [7] is given hereby, although more complex and precise models are also discussed in [7].

$$F_A = N \cdot P_A \cdot \left(\beta_1 \cdot e^{-R/\beta_2} e^{-\theta/\beta_3}\right)$$

where:

F_A crash rate due to a specific runway (relevant to a specific aircraft category) [event/year/unit area],

N runway movements per year [event/year],

P_A accident probability per movement of a take-off or landing [-],

R distance from the runway threshold to the site [km],

θ angle between the extended runway centreline and a vector from the site to the runway threshold [°],

β_i constant, dependent on aircraft category, e.g. (according to [7]):
for light civil aircrafts: β_1 = 0.08; β_2 = 2.5; β_3 = 60;
for small and large transport aircrafts as well as military combats and jet trainers: β_1 = 0.23; β_2 = 5; β_3 = 5.

Helicopter accidents occur mostly in the close vicinity (i.e. 200 m radius) of the helipad. The accident frequency relevant to this small circular area can be assessed by using the following formula [7]:

$$F_A = N \cdot P_A \cdot \beta_1$$

According to [7], 93 % of the helicopter accidents occur within 100 m of the helipad, and 7 % occur between 100-200 m. Consequently, for distances between 0-100 m β_1 = 29.6 and for the range 100-200 m β_1 = 0.74 is applicable for helicopters [7]. In practise, generally there are no helipads in a 200 m radius of the sites; therefore this category may be excluded from further assessment (unless helicopters can be used for transportation of equipment/personnel/rescue teams).

For the characterization of airport related hazard, F_A has to be assessed first for each aircraft category by considering each and every runway. Then the crash rates relevant to an aircraft category should be summed up for all the airports.

Besides airport related and background crash rates, the risk due to predetermined airways needs to be assessed for hazard characterization. According to [50], those addends of the aircraft crash rates that may arise additionally from airways can be screened out, if no airways and no airport approaches pass within 4 km of the site. An initiative and action of the European Route Network Improvement Plan (ERNIP) is in progress to implement full free route operations across European airspace till January 2022. Significant changes have been made in some countries (e.g. Hungary) as a result of this initiative, where regulations already enable to use airfields freely, that is, as a result of recent changes in airfield regulations, there are no assigned airways. However, there may be preferred routes that should be considered as airways during hazard assessment for PSA. In general, the airway related crash rate is not a dominant contributor to the overall aircraft crash frequency. Moreover, special care should be taken to avoid double counting crashes when both the background crash rate and the airway related crash rate are summed up [7]. A methodology to determine the airway related crash rates is given hereby for completeness. However, such calculations may be unnecessary for a lot of sites. Document [71] [16] proposes the following formula to assess the airway related crash frequency in a unit area:

$$F_W = N_F \cdot P_w \cdot \frac{g}{2} \cdot e^{-g \cdot s}$$

where:

F_W crash rate due to a specific airway (relevant to a specific aircraft category) [event/year/unit area],

N_F number of flights along the airway per year [1/year],

P_W aircraft crash probability per flight kilometre (in-flight reliability) [event/km],

g constant, dependent on aircraft category, that characterizes the likelihood of a close crash, e.g. for civil aircrafts: $g = 0.23$; for military aircrafts $g = 0.63$,

s distance between the flying route and the site [km].

To precisely assess the site specific airway related crash frequency, the site area should be divided into finite elements and the formula above should be applied to each of these elements. By summing up the crash frequencies determined this way, an airway related crash frequency can be obtained.
It should be mentioned that there are other formulas, that can be applied – for example, according to NUREG-0800 [72] one can calculate the frequency of aircraft crashing into the plant by the following formula:

$$P_{FA} = C \times N \times A/w$$

where:

C in-flight crash rate per mile (or km) for aircraft using airway,

N number of flights per year along the airway,

A effective area of plant in square miles (or square km),

w width of airway (plus twice the distance from airway edge to the site when the site is outside the airway) in miles (or km).

When there are no airports in the surroundings of the NPP, then according to [73], the aircraft crash probability per year can be estimated as:

$$P = P_l \times N_c \times A \times F$$

where:

P estimation of aircraft crash probability per year, [1/year];

P_l aircraft accident frequency per flight kilometre, [1/km];

N_c number of flights per year, [1/year];

A target area, [km^2];

F function of deviation per flight kilometre from initial flight route during an accident, [1/km].

As a consequence [71] [16], the general aircraft crash probability per year on territory of radius *r* around a NPP can be expressed by the following formula:

$$P = P_c N_c r^2 g(e^{-yg} - e^{-s\sqrt{D^2+y^2}})$$

where:

y	distance to the corridor, [km]
D	segment of the corridor, and
g	a constant depending on the type of aircraft (as shown earlier).

Some authors propose calculating frequencies starting from the global frequencies of aircraft crashes, depending on the weights of the aircraft. This type of statistics is available for different phases of flights – typically: the landing and take-off phase, the air lane traffic and waiting loop traffic, and the free air traffic. Basing on the number of yearly flying operations (take-offs and landings) of the airport to be considered, the number of the yearly crashes H_{ij} can be calculated for an impact area of the plant in a given annulus [74]:

$$H_{i,j} = h_{i,j} \cdot \frac{d_i}{d_{global,i} \cdot \Delta t} \cdot \frac{F_{NPP}}{F_{\alpha i}}$$

where:

h_{ij}	number of crashes within definite angular segment j and some distance and weight class
d_i	number of flying operations per year at the airport considered
$d_{global,i}$	number of global flying operations per year
FNPP/$F_{\alpha i}$	area of NPP annular segment
i,j	weight class, annular segment
Δt	time span analysed
H_{ij}	number of theoretical yearly crashes within NPP area.

The hazard assessment should include the evaluation of the current status of as well as the changes in air traffic, moreover the anticipated characteristics of aviation technology in the near future. Short- and mid-term trend analysis should be performed for crash rates based on the evaluation of past and recent air traffic data. The overall air traffic in a specific region reflects the transit, departure as well as arrival related air traffic. Consequently, the yearly data on each of these categories should be assessed and evaluated separately to fit a trend line thereon. To characterize the changes in the nature of air traffic, a qualitative characterization should also be performed with respect to the forecasted changes taking into consideration the impacts attributable to the current local, regional as well as global air traffic trends. This should be based on the data and trend line assessed earlier. The forecasted regional changes in the uses of airfields and airways should also be considered in this assessment.

APPENDIX 4 – ADDITIONAL ISSUES FOR EMERGENCY RESPONSE RELATED TO AIRCRAFT CRASH HAZARDS

In case of NPP some measures can be undertaken to minimize the risk of aircraft approaching the vicinity of particular site, and improve the site to better withstand such an event [75]. In relation to these concerns, the DiD concept for NPP has to be estimated for plants in operation and for these to be constructed future, in relation to the risks of aircraft impact:

- (1) primary risk: reactor building external wall damage;
- (2) primary risk: reactor containment damage;
- (3) primary risk: kerosene spill fire – if penetration of aircraft tank in the containment is assumed, the worst case is fire in the zone of cavity between the reactor building external wall and containment wall (if such zone exist);
- (4) secondary risk: blackout on site;
- (5) secondary risk: damage of non-safety related systems which may initiate a critical scenario for safe operation;
- (6) reactions of panicked personnel / inadequate response.

In order to mitigate such risks, the reactor building walls could be “hidden” as much as possible behind other structures of facilities. Wrapping of safety trains from two or three sides around the reactor building and one side wall protected by turbine hall can be assumed as option for feasible design.

Another option is to “dig down” part of the reactor containment below elevation “zero” for the site. This may seem a step back in respect to modern NPP projects, but can assure protection of impact of aircraft or other flying object.

An option for reactor building side area protection is the construction of buffer structure rooms in the periphery of the building, eventually filled with appropriate material: wafer of mineral wool and metal sheets, gravel etc. Such zones may have the effect to disperse the impact energy and reduce penetrating speed of external objects. General impact prevention of the site can be coordinated if water cooling towers exist. Such structures may by appropriate positioning help to coordinate the site protection in particular for the rector building.

In relation to air traffic risks imposed on the design of NPP, general requirements should be defined in related regulatory documents and these requirements should be imposed to NPP structures to withstand the impact of aircrafts under particular conditions. This topic can be quite delicate as the sizes of aircrafts vary in wide spectrum, but some basic levels of feasibility shall be required. In the regulations for design of NPP structures – in particular of containment buildings – it should be indicated what size of aircrafts can impact them without sustainable damage and technological risk of radioactive pollution.

As already mentioned probability of impact of aircraft with sizes classified in accordance to the standards is to be estimated first. The variety of sizes of aircraft, respectively their speed and weight shall be counted in impact effect calculations - categorization of aircrafts according to their weights has been defined both by the European Aviation Safety Agency (EASA) and US Federal Aviation Administration [76]. Impact model results can indicate if the aircraft could penetrate areas of the facility. In the worst case – if the containment area can be penetrated, this shall be regarded as weakness in the basic design of the facility.

APPENDIX 5 – HAZARD RISK ASSESSMENT AND PSA TOOL EXAMPLE

RiskSpectrum® HazardLite [77] (hereafter called ***HazardLite***) is a light tool for assessing hazard risks, e.g. earthquake, tsunami, extreme weather etc. The input to ***HazardLite*** includes definition of initiating events ranges, hazard curves and fragilities. The output is an excel workbook containing the results in form of Basic Events. This excel file can be imported into RiskSpectrum® PSA for further analysis. In addition, if the Monte Carlo method is selected in the analysis, a series of text files will also be generated for uncertainty analysis in RiskSpectrum® PSA.

A probabilistic safety assessment of an external hazard is different from analysis of internal events e.g. seismic hazards. The differences are mainly that:

- The hazard (the initiator of the sequence) spans over a continuous range
- There is relation between the hazard and the failure of equipment (fragility). The stronger the external hazard e.g. earthquake, the more likely the equipment will fail.
- This is relevant also for other types of hazards, e.g. tsunami, extreme weather hazards, man-made hazards.

HazardLite uses an EXCEL workbook to store the input necessary for fragility calculations of components over discreet ranges of peak ground accelerations, which are considered to be the initiating events. To capture the full uncertainty inherent in our knowledge, families of both hazard curves and fragility curves are used.

To capture the uncertainty of hazard curves, several hazards curves may be entered and each curve is given a probability, or weight, that it is the actual hazard curve. To capture the uncertainty of the fragility curve for each component, the user must enter the median acceleration where the component is expected to fail (called Am), the logarithmic standard deviation (called β_R) which represents the random variability of the fragility, and the logarithmic standard deviation (called β_U) which represents the uncertainty in the actual shape of the fragility curve. Fragility curves are modelled as lognormal probability distributions.

The hazard curves (and the fragility curves) are divided into discrete intervals by the analyst. In the PSA model, each of these intervals needs to be represented. ***HazardLite*** will generate the input necessary, with regard to hazard frequencies within each interval and fragilities to be used within each interval. These basic events are intended to be used as initiating events (frequency events) and as component failure in the PSA model (normal basic events in the fault tree structure).

It shall be noticed that fragilities may be grouped and combined. Grouping of equipment is performed to reduce the amount of necessary seismic fragility events and it represents OR-structures of components that need to be treated as fragilities. Combinations may be relevant when several fragility events are found in the same MCS. The reason for this is that the convolution approach used in ***HazardLite*** is more exact if the convolution is performed for the events together, rather than performing the convolution individually and then combining them in a MCS.

In the quantification, each of the defined intervals is subdivided into a number of sub-intervals. The chosen amount of subintervals is 100 in ***HazardLite***.

Within each interval the hazard frequency, as well as the fragility for each component is calculated. The calculation of the fragility is convoluted with the frequency, to account for differences in the interval (both the hazard curves and the fragility curve will change value within the interval).

The quantification algorithm is described by following:

- Point estimate calculation
- Quantification of the hazard frequency, the initiating events
- Fragility
- Calculation of fragility for group of events
- Calculation of fragility for combination of events
- Uncertainty calculation
- Quantification of hazard
- Quantification of fragility

Quantification of hazard, initiating events, point estimate calculation

HazardLite is calculating the frequency for the hazard by calculating the average frequency taking into account the weight of the hazard curve. The hazard frequencies are calculated by subtracting the exceedance frequency at the upper hazard boundary from the exceedance frequency corresponding to the lower boundary. Thereby a frequency within each interval is calculated. The calculation of hazard frequency is also performed for each sub-interval, since these frequencies are required for the convolution of hazard and fragility. Logarithmic interpolation is used when the definition of the interval does not match the user defined input data for the hazard curve.

Fragility

The HazardLite is used earthquakes as an example to illustrate how it works.

The fragility calculation is based upon following formula [1]:

$$f' \quad = \Phi\left(\frac{ln\left(\frac{a}{A_m}\right)+\beta_U\cdot\Phi^{-1}(Q)}{\beta_R}\right) \tag{1}$$

Where:

Φ() is the standard Gaussian cumulative distribution

a is the PGA

A$_m$ is the median capacity of the component

ß$_R$ is the random variability (the randomness wrt the earthquake)

ß$_u$ is the state of knowledge uncertainty (uncertainty of fragility curve shape)

Q is the confidence that the conditional probability of failure, f, is less than f´ for a given peak acceleration a.

A mean fragility curve can be calculated by replacing ß$_R$ by following

$$\beta_C = \sqrt{\beta_R^2 + \beta_U^2} \tag{2}$$

in the equation above and to set ß$_U$ to zero [1]. Then following equation can be defined:

$$f = \Phi\left(\frac{ln\left(\frac{a}{A_m}\right)}{\beta_C}\right) \tag{3}$$

This equation is used in ***HazardLite*** to calculate the mean fragility (e.g. at a given PGA a).

Since the fragility is representing a range of PGAs, and over this range the hazard frequency is also changing, and the cut sets including fragilities will always include one hazard and at least one fragility, the proper calculation would be to integrate them over the interval (over which the hazard is defined). However, the calculation in RiskSpectrum PSA/RSAT does not allow for such evaluations and thereby the calculation of the fragility must take this into consideration. The calculation of the individual component fragility convolution is described below, and the calculation of groups and combinations is described in a separate section.

Assume following cut set

H_1, F_1, B

Where H_1 is the frequency in an interval, F_1 is the failure probability of a component in the same interval, and B is an independent failure probability.

If H_1 and F_1 are calculated independently with regard to the frequency and probability within the interval, this will not necessarily yield the same result as the mean value computed by

$$\frac{1}{x}\int_0^x h(x) \quad \cdot f(x) \quad dx \qquad (4)$$

And the mean value from the integral above is the correct mean value. Therefore ***HazardLite*** does the convolution through a numerical integration, and then divides it by the frequency in the interval. In this way a weighted fragility estimate is calculated, and when it is multiplied with the hazard frequency in the MCS again, it will yield the same result as if the integration would have been performed for the MCS itself.

To put it in formula, F_i the failure probability of the component due to seismic fragility in interval i is calculated by:

$$F_{i,h_k} = \frac{\sum_{j=1}^{100}(h_{ij} \cdot f_{ij})}{\sum_{j=1}^{100} h_{ij}} \qquad (5)$$

Where:

$F_{i,hk}$ is the fragility calculated for interval i based on hazard curve k

h_{ij} is the hazard frequency for interval i, sub-interval j

f_{ij} is the fragility calculated for the interval i, sub-interval j

The value of the fragility f_{ij} is calculated at the upper end of the sub-interval, which is a slightly conservative approach taken. The probability is calculated by formula (3).

The fragility (failure probability) is calculated for each individual hazard curve as basis, and then the fragility (failure probability) results to be used in the PSA for the interval are calculated by multiplying the weight of the hazard curve with the $F_{i,hk}$ of that specific curve. The raw data are the hazard curves, and thereby these should be used as the basis for the convolution. The fragility (failure probability) for the component is calculated by:

$$F_i = \sum_{k=1}^{n} F_{i,h_k} \cdot W_{h_k}$$

Where:

W_{hk} is the weight of hazard curve k

$F_{i,\ hk}$ is the fragility in segment I for hazard curve hk

Component groups and combinations

A component groups is defined as a set of components that are grouped together and instead of representing them individually, they are represented as a group. These events could be considered to be represented under an OR-gate.

The quantification of the fragility for each component is according to the methodology above, but instead of representing each value in the PSA model by a basic event, they are combined according to following formula:

$$F_{Group} = 1 - \prod_{i=1}^{n}(1 - F_i)$$

Combination

A combination is defined as a set of basic events that are found in the same MCS. The process described above for components and groups of components generates a convolution of the hazard and the fragilities over the hazard range. This process is used to, as accurately as possible, calculate the values that should be produced by the MCS analysis whenever the cut set includes the hazard (which it should always do in the hazard analysis) and a fragility. However, when a cut set contains more than one fragility the convolution is no longer correct.

HazardLite gives the user the possibility to specify combination of events. There can be a prohibitively large number of combinations, so the process is intended to be used for the events that may have impact on the results.

The combinations defined are calculated simultaneously as the individual basic events, to ensure consistency of values used (e.g. with regard to uncertainty simulations – same value must be used for $fA(i)$ (failure probability A in internal i) both when the individual basic event is computed and the combination event).
The combinations are intended to be included in the analysis using MCS post processing, replacing the events in the cut set by the combinations. The difference in results when applying combinations and not for individual MCS may be significant, and hence it is recommended to use the combinations for event combinations of importance.

Uncertainty calculation

The uncertainty calculation is built by the same methods as presented above. The equations are slightly different, when it is no longer the mean value that is computed.
The method is:

- Randomly select one of the hazard curves (according to its weight)
- Randomly select one of the fragility curves in the group of fragility curves (for each component)
- Calculate the hazard frequencies for all defined intervals
- Calculate the fragilities for all intervals, under the condition of the selected hazard curve (convolute with the selected hazard curve only)
- Calculate Component groups and combinations
- Perform next sampling