Ref. Ares(2019)5560453 - 04/09/2019

NARSIS

New Approach to Reactor Safety Improvements

WP5: Supporting Tool for Severe Accident Management

D5.3 - Definition of Hazard-Induced Damage States and Development of State-Specific APETs for Demonstration Purposes

This project has received funding from the Euratom research and training programme 2014-2018 under Grant Agreement No. 755439.

Project Acronym:	NARSIS
Project Title:	New Approach to Reactor Safety Improvements
Deliverable:	D5.3 - Definition of Hazard-Induced Damage States and Development of State-Specific APETs for Demonstration Purposes
Month Due:	24 **Month delivered:** 24
Leading Partner:	APOSS
Version:	V0

Primary Authors: Ivan Vrbanić, Ivica Bašić (APOSS)

Other contributors:

- GEN: Luka Štrubelj, Klemen Debelak
- JSI: Marko Bohanec

Deliverable Review:

- **Reviewer #1:** Jože Špiler, GEN **Date:** 09/08/2019
- **Reviewer #2:** Maciej Skrzypek, NCBJ **Date:** 01/08/2019

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of contents

1 Introduction 8
1.1 Purpose 8
1.2 Scope 8
2 Accident Progression Logic Model 9
2.1 Background for Accident Progression Logic Modeling 9
2.2 Introductory Considerations of Hazard Damage States 11
2.3 Characterization of Hazard Damage States for This Study 18
2.4 Main Plant Systems and Functions Related to HDS 21
2.4.1 RCS Depressurization 22
2.4.2 LP ECCS Injection (Transport of RWST Inventory) 22
2.4.3 LP ECCS Recirculation 24
2.4.4 Containment Spray Injection 24
2.4.5 Containment Spray Recirculation 25
2.4.6 Reactor Containment Fan Coolers 25
2.5 Accident Progression Logic Model Structure 26
2.5.1 Plant Status Questions and Phenomenological Questions 26
2.5.2 APET Logic Structure 30
2.5.3 Probability Model for Answers to Plant Status Questions 38
3 Types of Decisions and Actions in Severe Accident Management 41
3.1 Types of Procedures/Guidelines under Accident Management Program 41
3.2 Severe Accident Progression and Degrees of Severity 42
3.3 Plant Damage Condition Diagnosis as used in SAMG 45
3.4 SAMG Strategies and Decision Making Process 51
4 Attributes for Use in Decision-Making 61
5 Concept for the Use of the Tool 64
6 Summary 65
7 References 66

List of Figures

Figure 1: Outline of Logic Model for Severe Accident Sequences in PSA (Taken from the IAEA's SSG-4, [IAEA,10b]) 10
Figure 2: Outline of Logic Model for Seismically Induced Initiating Events 11
Figure 3: Example Logic Model for Seismically Induced HP and LP Sequence 12
Figure 4: Outline of Complete Logic Modeling Framework for Hazard-Induced Severe Accident Sequences 14
Figure 5: Example: Input by Assessor for Alternative #1 and Alternative #2 29
Figure 6: Overall APET structure 33
Figure 7: Main Tree 34
Figure 8: Sub-Tree SUB1 35
Figure 9: Sub-Tree SUB2 36
Figure 10: Concept of General Phenomenological Tree 37
Figure 11: Different Time-Dependent Probability Profiles Established by Lognormal Distribution 40
Figure 12: Examples of Adjusted Probabilities for Establishing or Recovering a Function 41
Figure 13: Illustration of Accident Management Program 42
Figure 14: Severe Accident Progression Diagram 44
Figure 15: Core Damage Conditions Status Tree (example) 48
Figure 16: Containment Condition Status Tree (example) 48
Figure 18: SAMG Package 54
Figure 19: SAMG Decision Making Process 59
Figure 20: Determination the availability of equipment to perform the strategies in the guideline SAG-1 (Inject to SGs) 60
Figure 21: Form of the Results from Quantification of Particular Alternative 62
Figure 22: Illustration of Comparison of Two Alternatives 63
Figure 23: Conceptual Diagram for Use of the Tool 64

List of Tables

Table 1: Set of Plant Status Questions 27
Table 2: Phenomenological Questions 30
Table 3: RCS Damage Condition Descriptors and Possible Symptoms 45
Table 4: Containment Damage Condition Descriptors and Possible Symptoms 46
Table 5: Summary of Reactor Core, RCS and Containment States 50
Table 6: Example of CHLA inject into RCS effects and consideration 52
Table 7: Monitored Plant Parameters used for demonstration of SAMG decision making process 56

List of Abbreviations

AOP	Abnormal Operating Procedure
APET	Accident Progression Event Tree
ARP	Alarm Response Procedure
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient without Scram
B	Containment Damage Status: Bypassed Containment
CA	Computational Aid
CC	Containment Damage Status: Closed and Cooled
CD	Core Damage Status: Core Damage
CET	Core Exit Thermocouples
CHLA	Candidate for High Level Action
CHR	Containment Heat Removal
CX	Containment Damage Status: Challenged Containment
DB	Design Basis
DCH	Direct Containment Heating
DEC	Design Extension Condition
DFC	Diagnostic Flow Chart
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EX	Core Damage Status: Corium Ex-vessel
EDMG	Extensive Damage Management Guidelines
EOP	Emergency Operating Procedure
ESF	Engineered Safety Features
HDS	Hazard Damage State
HP	High Pressure
HPME	High Pressure Melt Ejection
IAEA	International Atomic Energy Agency
I	Containment Damage Status: Impaired Containment
ID	Identifier
IE	Initiating Event
IVR	In-Vessel Recovery
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LP	Low Pressure
MCCI	Molten Corium Concrete Interaction
MCR	Main Control Room
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OK	Core Damage Status: No Core Damage

OX	Core Damage Status: Core Cladding Oxidation
PORV	Power Operated Relief Valve
PSA	Probabilistic Safety Analysis / Assessment
PWROG	Pressurized Water Reactor Owners Group
RC	Release Category
RCFC	Reactor Containment Fan Coolers
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RPV	Reactor Pressure Vessel
RVF	Reactor Vessel Failure
RWST	Refueling Water Storage Tank
SACRG	Severe Accident Control Room Guideline
SAG	Severe Accident Guideline
SAEG	Severe Accident Exit Guideline
SAMG	Severe Accident Management Guideline
SBO	Station Blackout
SCG	Severe Challenge Guideline
SCST	Severe Challenge Status Tree
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SIET	Seismic Initiating Event Tree
SSC	Structures, Systems and Components
TSC	Technical Support Centre

1 Introduction

1.1 Purpose

External or internal hazard occurring at particular nuclear power plant (NPP) can have a twofold major impact on NPP's structures, systems or components (SSC):

- It can cause direct damage to plant's SSCs; and
- It can, at the same time, induce an initiating event such as loss of coolant accident (LOCA) or transient which can develop into accident sequence leading to reactor core damage.

The combined impact of direct damage and of triggered severe accident which resulted with reactor core damage or degradation can be referred to as a "hazard damage state" (HDS). Particular HDS can, depending on the accident progression, phenomena and response of the containment, lead into release of radioactivity into the environment. It is the role of severe accident management and corresponding guidelines (severe accident management guidelines - SAMGs) to prevent or mitigate this kind of development. In Work Package 5, [NARS,17], a supporting tool is developed, for demonstration purposes, which may support severe accident management. The tool would reflect the SAMG framework existing today, as well as quantitative risk assessment techniques used in probabilistic safety analyses (PSAs).

The purpose of this report, developed under the Task 5.3, is to establish the hazard damage states and the logic model for accident progression, to be used as a basis for the mentioned supporting tool, which will be developed under the Task 5.4.

Definition of the hazard damage states as well as development of logic model for severe accident progression reflect the type of the plant design and the type of the emergency operating procedures (EOP), extensive damage management guidelines (EDMG) and SAMGs described in the reports developed under the Task 5.1 and Task 5.2, i.e. [NARS,18a] and [NARS,18b].

1.2 Scope

Implementation of the Task 5.3 was divided into the following three main activities, which are described in this report:

- Identifying and defining the hazard damage states and developing the accident progression logic structure (in the form of event trees and similar techniques such as event sequence diagrams) for the postulated set of hazard damage states. This is addressed in section 2 of the report.
- Identifying and characterizing types of decisions and actions to be made under the severe accident management, to be considered by the supporting tool. This is addressed in section 3 of the report.
- Defining the attributes with regard to which the available options / alternatives would be evaluated. This is addressed in section 4 of the report.

2 Accident Progression Logic Model

2.1 Background for Accident Progression Logic Modeling

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

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

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

Probabilistic safety assessment (PSA) for nuclear power plants is an attempt to put all possible accident sequences into a logic system which is manageable for practical purposes concerning plant safe design and operation. PSA, as defined and known today, is considered to be the best method currently for the purpose of accident progression logic modeling. Here, the term “as defined and known today” refers to PSA attributes and uses established in accordance with internationally recognized standards and technical guiding documents, such as safety guides and technical documents [IAEA,10a], [IAEA,10b], [IAEA,16] and other PSA-related documents of International Atomic Energy Agency (IAEA); PSA standards [ASME,13] and [ASME,14] of American Society of Mechanical Engineers (ASME); regulatory guides [NRC,11], [NRC,09], and others of U.S. Nuclear Regulatory Commission (NRC); as well as a number of other internationally known guidelines from the side of regulators, industry or utilities.

The complexity of the logic model of severe accident sequences, as well as their very large numbers to be dealt with, can be appropriately illustrated as in Figure 1, which is taken from the IAEA’s SSG-4, [IAEA,10b]. The set of all possible (imaginable) initiators is usually partitioned in two major categories: loss of coolant accidents (LOCA) and transients. (“Transient” category, in this context, represents anything that remains after all the LOCA-type events (direct or consequential) are addressed). They are usually further divided into a number of initiating event (IE) categories. Each IE category is “passed” through appropriately developed “event tree”, resulting in a number of accident sequences leading to end states involving some degree of reactor core damage. These sequences are usually referred to as “core damage” (CD) sequences. This is in Figure 1 represented by the first box on the left side, “Level 1 PSA”. A Level 1 PSA for a nuclear power plant (which are currently operating around the world) would have hundreds if not thousands of CD sequences explicitly modeled.

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

represents a group of accident sequences resulting with similar response of plant systems / ESFs, similar damage to the reactor core and similar challenge to the containment.

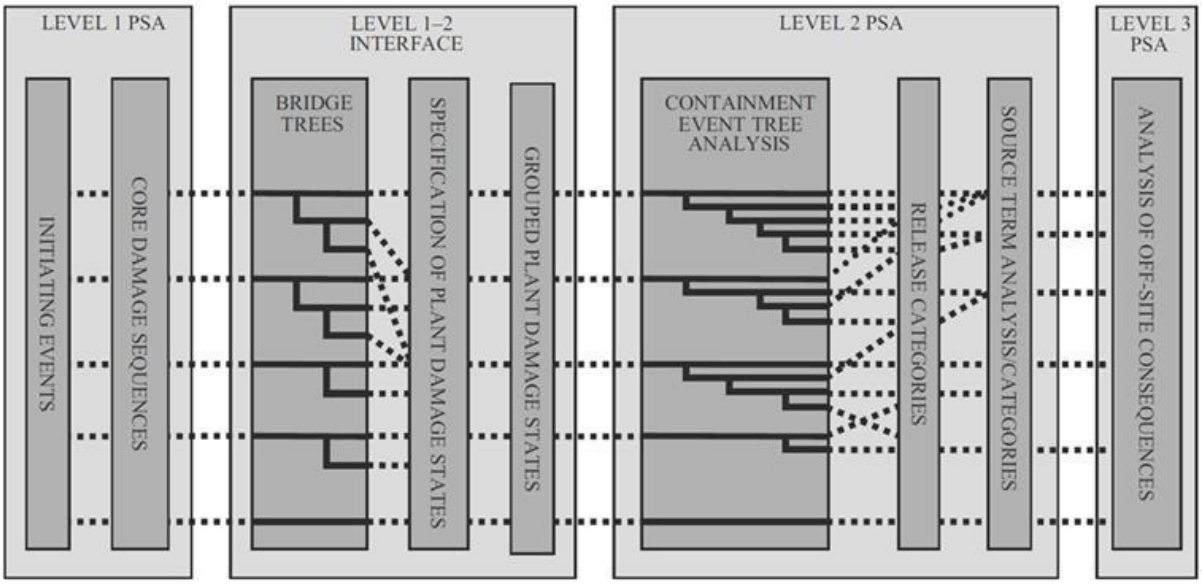

Figure 1: Outline of Logic Model for Severe Accident Sequences in PSA (Taken from the IAEA's SSG-4, *[IAEA,10b]*)

Particular plant damage states need then to be "passed" through the event tree which represents a logic model of severe accident phenomena taking place inside the reactor vessel and primary system (many times referred to as "in-vessel" phenomena) as well as outside of the vessel / primary system (usually referred to as "ex-vessel" phenomena). This event tree is usually referred to as a "containment event tree" (as in Figure 1) or as an "accident progression event tree". In this document the second term will be used (accident progression event tree), since the abbreviation for the first term is the same as for the "core exit thermocouples" (CET), which is one of the key terms in the frame of Work Package 5.

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

The end states of the accident progression event tree represent states with different releases of radioactivity into the environment, depending on the accident phenomena and containment failure modes. They are, in most of the cases, grouped into categories which are usually referred to as "release categories" (which is also the case in Figure 1). Many times, a Level 2 PSA model would have about 10 to 20 release categories.

For each release category a "source term" is usually calculated, including the inventories, amounts and timing of radioactivity releases. The whole model is, eventually, extended to the so-called Level 3 PSA, which represents the analysis of the offsite consequences. The source term analysis and offsite consequences analysis are, in principle, considered not to be relevant for Work Package 5, as the focus is on preserving the containment integrity (avoid large releases), rather than response to large releases (e.g. emergency planning).

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

purposes and for investigating of the feasibility of this kind of accident management supporting tool.

2.2 Introductory Considerations of Hazard Damage States

The initiating events, discussed in the previous section, are related, in principle, to internal events due to random causes, e.g. LOCA due to random rupture of a pipe or loss of main feedwater due to random failures. On the other hand, in the case of a hazard, the initiators would be induced by occurrence of an event from the considered hazard category (or, in some cases, by a combination of induced and random failures). Thus, in the case of seismic event, the main categories of the initiators would be seismically-induced LOCAs (e.g. LOCA due to seismically induced rupture of a primary system pipe or seismically induced loss of main feedwater or seismically induced loss of offsite power).

Seismic hazard will be taken as an example to illustrate the concept of logic modelling of hazard-induced accident sequences, continuing from the logic model outlined in the previous section. Seismic hazard is a good example, since it simultaneously challenges all relevant systems, structures and components (SSCs), unlike some other hazards which may challenge only the external structures or the internal SSCs located in particular area. However, it should be noticed that the principles discussed below can be applied to basically any hazard or to a combination of hazards (multi-hazards).

Figure 2 outlines the principles for the identification and logic modeling of seismically induced initiating events, which are, many times, used in seismic PSAs. This kind of logic model is many times referred to as “seismic master event tree” or “seismic initiating event tree” (SIET).

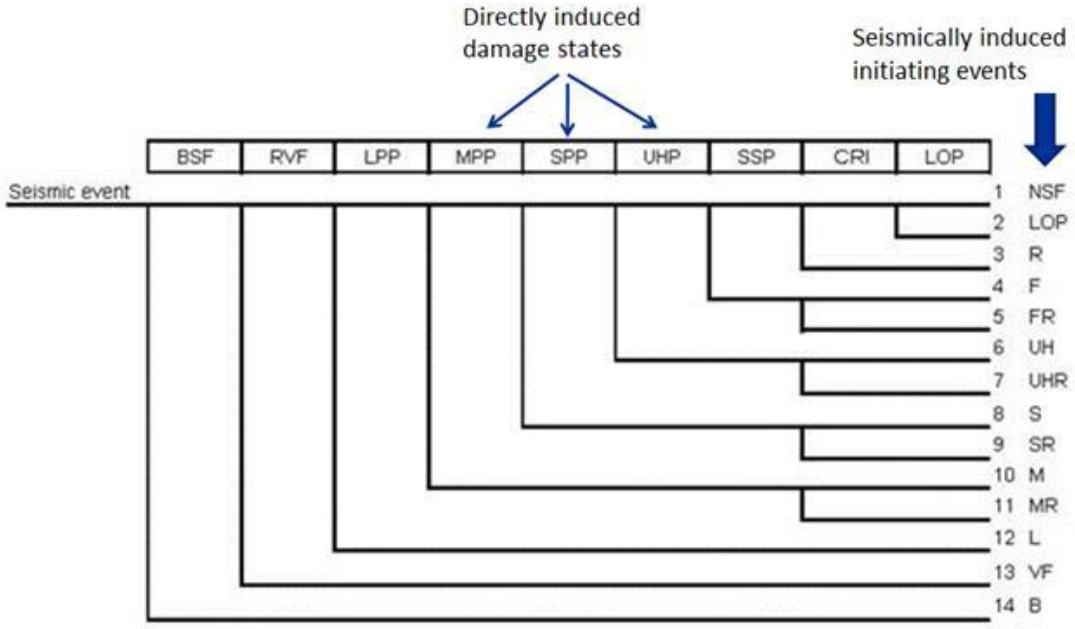

Figure 2: Outline of Logic Model for Seismically Induced Initiating Events

Basic principles of SIET outlined in Figure 2 are:

- Seismic event (which is input or main initiator) can cause direct damage to plant structures, systems or/and components;
- In turn, direct damage can, depending on the SSCs affected, induce different initiator categories.

Thus, the SIET has different directly induced damage states as its function events (headings) and induced initiating event categories as its end states.

Examples of function events / direct damage states may include: structural failures of buildings; seismic failures of large primary components leading to beyond design basis LOCA events; seismic failures of primary or secondary piping, etc. Examples of induced IE categories may include, from the worst to the least severe: beyond design basis event caused by building's structural failure leading to a direct CD and direct release; beyond design basis LOCA leading to a direct CD (without directly compromising the containment integrity); induced design basis LOCA etc. The least severe initiator induced by a strong earthquake can be represented by a transient (e.g. manually implemented reactor trip) in the absence of any seismically induced failure.

Usually, the direct damage states are defined in a way and ordered by certain hierarchy and rules which enable establishing a set of mutually exclusive induced initiator categories.

As already identified under the previous Project's activities, the severe accident sequences (postulated initiating events resulting with significant core degradation) can be generally grouped into two major sequence categories, based on the reactor coolant system (RCS) pressure at which the reactor pressure vessel (RPV) fails and dynamic effects on containment structures:

- High pressure (HP) sequence; and
- Low pressure (LP) sequence.

These categories are briefly described in [NARS,18b]. Logical modeling (in terms of) of these two sequence types is further addressed in the sections below, including the damage states to which they can lead.

To put these two sequence types in the context of the hazard-induced initiators, the logic model from Figure 3 can be used. An example of each of the two sequence types, as possibility triggered by a seismic event, is shown by Figure 3.

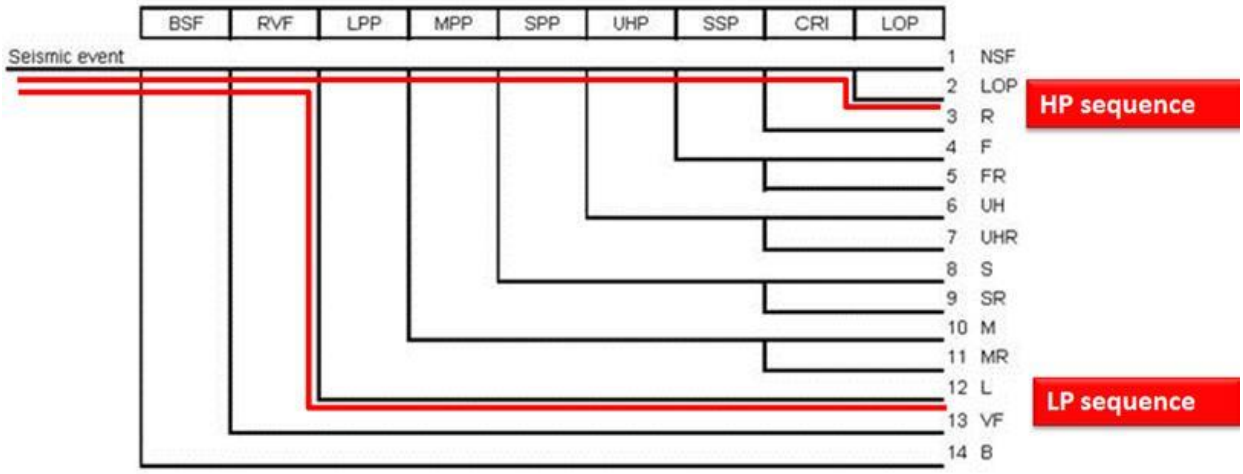

Figure 3: Example Logic Model for Seismically Induced HP and LP Sequence

In this example, function "BSF" refers to structural failure of buildings; function "RVF" refers to seismic failure of a large primary component; "function "LPP" refers to seismic failure of large primary pipe; the last function among the headings, "LOP" refers to seismically induced loss of offsite power (LOOP). It should be noted that the above SIET figure is provided only for illustration of the principles. The remaining functions represent seismic failures of other primary piping (medium and small size), secondary piping and other relevant high-level plant functions.

One seismically induced LP sequence can be represented by success of (no damage to) buildings and large primary components, coincident with failure of large primary piping. This would lead to a large LOCA initiator, induced by a seismic event. It should be noted that status of medium and small size primary piping is not relevant once the large piping has failed, because it would only increase the size of the break but would not change the nature of the initiator or the sequence type. Depending on the status of other design basis (DB) mitigating systems, this large LOCA may be mitigated by the DB systems or may require (in the case of failure of DB systems) additional systems for mitigation (e.g. systems foreseen for design extension conditions, DEC).

In the similar manner, if a failure of large component occurs (i.e. “RVF” function fails), the status of large or other primary piping is not relevant, because this is already a beyond-DB LOCA event. Thus, both sequence #13 and #12 are LP sequences. However, these two initiators differ with regard to mitigation status: in the case of sequence #13 there is no mitigation, by definition, and sequence leads to core damage; on the other hand, sequence #12 can be mitigated and core damage prevented, depending on the status of DB and DEC systems.

Sequence #2 presents a possible example of HP sequences. In this sequence there are no seismically induced breaks, primary or secondary. However, it involves seismically induced LOOP. If this is combined with a failure (seismic or random) of the emergency diesel generators (EDG), the sequence results with station blackout (SBO) condition. If not mitigated, SBO would lead to a sequence with HP core damage and (likely) HP vessel failure.

Complete logic modeling framework for hazard-induced severe accident sequences can be presented by putting the SIET (or corresponding initiating event tree for any other hazard) in front of the Level 1 event trees discussed in the previous section. The end states of the SIET (hazard-induced initiators) would then be mapped (and linked) to the corresponding random-failure (internal) initiator categories such as LOCAs and transients, with addition of some hazard-specific sequences which usually lead to a direct CD, as indicated in Figure 4.

One of the key points in developing the platform for the mentioned accident management supporting tool is in establishing a reasonably complete and, on the other hand, a reasonably small set of hazard damage states (HDS) which would serve as a basis for predicting the risk and for putting it into some quantitative terms. In this sense, particular HDS can be seen as:

- Combination of damage to SSCs and reactor caused (induced) directly by a hazard itself, as well as damage caused by triggered accident sequence; and
- Impact of this combined damage on plant’s systems, functions and mitigation capability.

Plant damage states used in the current state-of-the-art PSAs for the operating nuclear power plants can be considered as a basis for establishing such a set of HDSs. The role of plant damage states in a current PSA was briefly discussed in the previous section. Following is a somewhat more elaborated discussion.

Plant damage states used in a PSA are functional groupings of Level 1 core damage sequences extended to but not including reactor vessel failure, for use in the Level 2 PSA analysis. The sequences in a particular damage state typically provide similar input to evaluate containment response. A particular plant damage state contains delineation (characterization) of Level 1 sequences up to vessel failure, including the case where core damage occurs but in-vessel recovery (IVR) may take place (i.e. reactor vessel failure may be avoided).

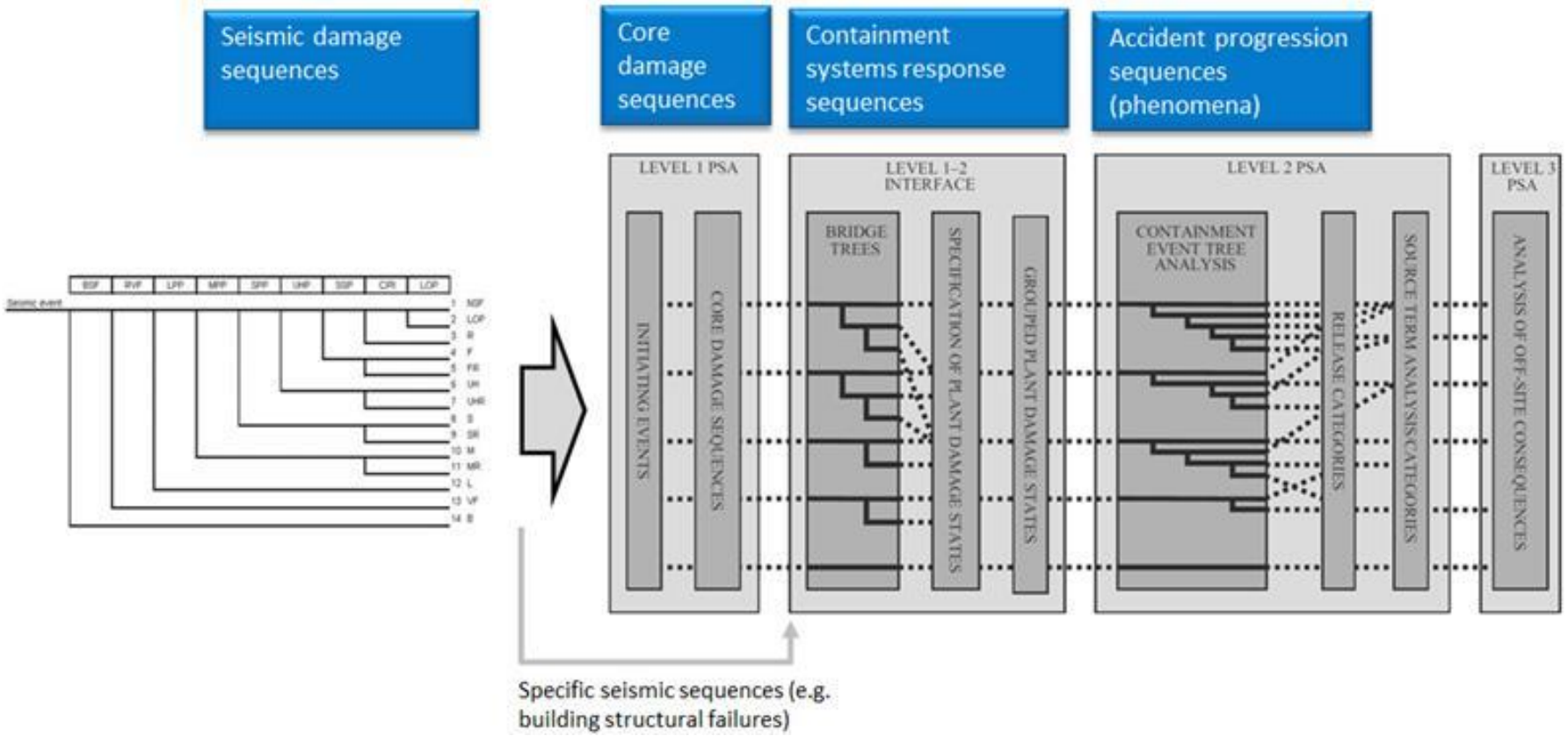

Figure 4: Outline of Complete Logic Modeling Framework for Hazard-Induced Severe Accident Sequences

The plant damage state provides extended characterization of status of the plant as compared to the respective group of Level 1 core damage sequences. The status characterized by a core damage sequence from the Level 1 event tree is focused on the reactor core and plant systems related to the safety of the reactor core (e.g. secondary heat sink or emergency core cooling system (ECCS)). The plant damage state extends this characterization by providing additional information which includes the status of relevant containment systems.

It is, thus, a function of specific plant characteristics important to containment performance (containment response to core damage event).

In a PSA, the plant damage states (induced by a hazard / initiator or by progression of triggered accident sequence) are typically characterized by a set of attributes. Those attributes usually include:

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

Each of these functional characteristics (attributes) can significantly influence the progression of a severe accident (pre- and/or post- core damage) and, thus, the resulting performance of the containment.

What is in a PSA referred to as a “plant damage state” is a particular combination of states defined for such pre-established attributes.

Some further discussion is provided below for each of the above mentioned attributes.

Initiating Event Type

Core damage prevention depends on the ability to maintain water inventory for decay heat removal. This ability depends on the rate at which water enters the vessel versus the rate at which water exits. The initiating event type defines the means by which a break in the primary system would occur and thus the rate at which water would exit. Additionally, the initiating event type may directly influence the status of the containment (e.g. containment bypass).

Thus, the initiating event type for characterizing the plant damage state is usually defined in a way to make a distinction between:

- Large / medium LOCA, characterized by rapid decompression of the RCS and core uncovering;
- Small LOCA, under which, depending on the break size, the RCS decompression can slow down or even remain at relatively high pressure levels;
- Transient (“non-LOCA”), characterized by release of primary coolant through the pressurizer relief and safety valves; the RCS pressure may or may not drop, depending on development of the accident sequence;
- Initiators with potential for containment bypass, such as interfacing systems LOCA or steam generator tube rupture (SGTR); in the context of external hazards, this type can also include, for example, seismically induced structural failures of containment integrity.

Time of Core Damage

Timing of core damage following accident initiation can be important from a perspective of implementing accident management strategies. Many times, two periods are considered, “early” (within several hours) and “late”. In the early time period most activities are dominated by automatic actuations and diagnostic evaluations. Emergency operating procedures would govern the direction the plant staff would take during this time period. In the late phase the implementation of accident management strategies become feasible. From the perspective of the risk quantification as done in a typical PSA it can be useful to classify the plant damage states in this way. The assignment of the state (“early” versus “late”) depends, in principle, on the rate of primary depletion (break size) and on whether the core damage occurs during the direct injection phase or the recirculation phase of ECCS.

Late core damage also allows for the decay of some fission product radioisotopes. This effect is however not very important as it concerns mostly the noble gasses with half-lives of the order of hours, while the other volatile and non-volatile fission products have half-lives ranging from days to years.

Pressure at Reactor Vessel Failure

This attribute can be used to make distinction amongst those sequences that lead to core damage, but for which vessel failure does not occur (i.e. in-vessel recovery (IVR) is achieved) and those leading to vessel failure at high or low pressure. For example, in-vessel recovery is, possible when primary depressurization is performed using the EOPs or SAMGs after the failure of high pressure ECCS has caused core damage. The depressurization allows the low pressure ECCS to be effective in arresting the core damage. (Note, however, that while the depressurization is a prerequisite for the IVR it is, by itself not sufficient to ensure the IVR.)

The primary system pressure at the time of vessel failure dictates the distribution of the molten core outside the vessel. For high pressure sequences the potential for direct containment heating (DCH) or the entrainment of the corium through the cavity and instrumentation channel into the annular compartment become significant. DCH is a phenomenon that could lead to containment failure at vessel failure and it requires a high pressure ejection of the debris into the containment atmosphere. For low pressure vessel failures the molten core will remain in the cavity resulting in a deep debris bed in the cavity and a greater degree of concrete ablation, producing non-condensable gases and a larger release of non-volatile fission products.

Status of ECCS

Core damage occurs when it is no longer possible to maintain water inventory, implying the rate at which water exits the vessel exceeds the rate at which it is being injected. The "initiating event type" attribute defines the mechanism by which water will leave the vessel and this attribute "ECCS status" addresses the mechanism by which water can enter the vessel.

The ECCS typically consists of high and low pressure injection along with alignment for recirculation. The combination of these injection sources dictates the plant damage state for the ECCS status.

This attribute, ECCS status, can be defined in way to distinguish three different situations:

- Injection before reactor vessel failure;
- Injection after reactor vessel failure;
- No injection.

They are further discussion below.

Injection before Reactor Vessel Failure

This situation is in most cases characterized by a failure of ECCS recirculation after ECCS injection has succeeded. Usually, high or low pressure injection succeeds early in the accident. Core damage followed by vessel failure occurs when recirculation fails and the RWST inventory is depleted.

Injection after Reactor Vessel Failure

This situation usually represents the case where the primary pressure remains above the shut-off head of ECCS injection leading to a high pressure vessel failure. This normally refers to low head ECCS, but for special cases, such as for some small LOCAs or transient sequences (including anticipated transient without scram, ATWS), the pressure may remain above the shut-off head of the high head ECCS.

After vessel failure the RCS pressure drops and ECCS injection injects the RWST inventory into the failed reactor vessel and, thus, into the containment. Transport of the content of the RWST into the containment is important for debris cooling and fission product scrubbing.

Successful post vessel failure injection may or may not be followed by successful recirculation. The RHR heat exchanger is included in the definition of the successful recirculation. Failure of low pressure injection would also normally imply failure of low pressure recirculation.

No Injection.

In this case there is no ECCS injection or recirculation. The failure of injection normally implies the failure of recirculation. The failure of all ECCS injection means that there will be no RWST inventory injected to the containment unless containment spray injection (discussed under the next attribute) is successful. The water inventory available for debris cooling and fission product scrubbing will be limited to the reactor coolant system inventory (possibly also the accumulator inventories) that enters the containment through the failed vessel.

When establishing the ECCS status certain dependencies among the mentioned functions need to be considered. Thus, for example, a failure of high pressure injection normally implies a failure of high pressure recirculation. Likewise, a failure of low pressure injection implies a failure of low pressure recirculation. Also, the failure of high pressure recirculation can be considered to imply (with high likelihood) the failure of the low pressure recirculation because of the high level of dependency between the two modes of operation (as both of them rely on LP ECCS pumps). Additionally, there are dependencies between the ECCS and the containment spray system which are pointed out under the CHR status discussed below.

Status of Containment Heat Removal

For the considered plant design, the reactor containment fan coolers (RCFC) and containment spray system are the primary mechanisms for the CHR. During the spray recirculation phase, the spray system functions in conjunction with the low pressure ECCS recirculation to remove the heat from the containment via the RHR heat exchangers.

This attribute is usually defined to in a way to simply make a distinction between plant damage states with successful containment heat removal and those with failure of containment heat removal.

As noted above, the success criterion for the containment heat removal function is defined as: success of “RCFC” or (success of spray recirculation and success of LP ECCS (RHR) recirculation).

Similarly to the previous attribute, there are function dependencies which need to be considered. Thus, a failure of spray injection normally implies a failure of spray recirculation. Also, in certain sequences the ECCS pumps may empty the RWST before the containment spray is actuated. Therefore, no spray injection is performed. However, the spray recirculation function can still be initiated and performed.

Status of Containment Integrity

The last among the above mentioned attributes is related to the containment integrity status. The containment may be initially intact, the containment isolation may have failed, or the containment may be bypassed. These three different states are usually reflected in this attribute. Containment bypass state usually represents the core damage sequences resulting from interfacing system LOCA and core damage sequences from SGTR with stuck-open SG relief valve. In the context of external hazards, this state can also include, for example, seismically induced structural failures of containment integrity.

2.3 Characterization of Hazard Damage States for This Study

A set of hazard damage states (HDS) is, for the stated purpose of this study, established by considering the PSA-based plant damage state framework discussed in the previous section. Discussed below are further considerations which were applied in the process.

The considered accident management supporting tool is to be “activated” at the time when certain CD condition either already exist or is about to commence. Therefore, for its purpose the sequence “begins” with core damage or it can be said that the initial condition involves core damage (or at least some core degradation - not necessarily physical damage). The type of the actual event which initially triggered the sequence leading to the point of this CD condition is, from the perspective of the tool (or tool’s user) not relevant, in principle. The type of the initiator would reflect in the CD conditions, e.g. high or low pressure at the time of core degradation.

The time which has passed between onset of the initiator and start of core degradation can be considered not to be relevant, in principle, for similar reasons.

Thus, the first two attributes of those discussed in the previous section are considered not to be relevant for the purpose of this study (which is to provide a framework for the status-oriented quantitative risk assessment for a demonstration-level supporting accident management tool).

Furthermore, the following considerations are applied to the containment bypass sequences and sequences with failure of containment isolation:

- This type of accident sequence is not in focus of the study because it is not suitable for the demonstration purposes of an accident management decision-making tool. The reason for this is that this kind of a sequence would result with immediate radioactivity releases. Therefore, the actions to be taken would be predetermined, i.e. based on the existing emergency plan. There would be no decision-making (or at least not of the kind that is subject to the considered supporting tool).
- Focus of the decision-making supported by the considered tool is to preserve the integrity of containment, i.e. decisions are favored or non-favored with regard how they affect the containment integrity. The best decision course, in principle, is the one which leaves the best chance to preserve the containment integrity.

Therefore, the initial conditions (status) for the purpose of this study will include:

1) Onset of core degradation, or core degradation is about to start; (the parameters by which this condition is recognized are discussed in section 3); there is no particular consideration of the type of initiator or the time which has passed since it had occurred;

2) No containment bypass; the accident sequence which leads to the above condition (core degradation) is not such that it would include containment bypass; the sequence is not an interfacing LOCA sequence; the sequence is not so-called V-sequence (SGTR with stuck open SG PORV); the sequence is not initiated by hazard which could compromise structural integrity of the containment (e.g. seismic event so strong that it may fail containment structure).

   The exception, however, is containment bypass which may be caused by the creep rupture of the SG tubes. This kind of bypass, which is a phenomenological issue and a part of accident progression, needs to be explicitly addressed.

3) Successful containment isolation; the sequence did not involve failure of Phase A Isolation or failure of Containment Ventilation Isolation or failure of Containment Phase B Isolation ([NARS,18a], [NARS,18b]), or any other failure relevant for the success of containment isolation (e.g. status penetrations or personnel / equipment access hatches).

In short, the initial condition for the purpose of the study is start of core damage with (initially) intact containment.

Hazard damage state (HDS) can, under such conditions and having in mind the framework from the previous section, be characterized by the three main attributes which are described below.

At this point it is important to note that particular HDS does not determine the containment status (i.e. whether integrity is preserved or compromised). However, it can be related to the containment failure likelihood (based on PSAs and severe accident analyses). Thus, it can provide a meaningful basis for the quantitative assessment of risk from containment failure by the considered tool, which can then be used to quantitatively compare different available decision paths.

Attribute 1: Pressure at Reactor Vessel Failure (RVF)

The first attribute can be assigned one of the three mutually exclusive states:

H = Reactor Vessel fails at high pressure;

The “high pressure” is, for the purpose, approximated as pressure above the shutoff head of the LP ECCS pumps. This pressure prevents injection and recirculation by the LP ECCS. At the same time, the reactor vessel failure at this kind of pressure is considered to have a potential to result with dynamic phenomena under HPME, such as DCH.

L = Reactor Vessel fails at low pressure;

Analogously, the “low pressure” is approximated as pressure below the shutoff head of LP ECCS pumps. This state is defined as follows: the pressure was reduced below the pumps shutoff head before the reactor vessel failure. However, the LP ECCS pumps (or any alternative means) are not available to perform injection and recirculation.

R = Pre-requisites for in-vessel recovery (IVR);

This third state is a complement to the above two: RCS was depressurized below the shutoff head of the LP ECCS pumps and the LP ECCS pumps are available for (injection and) recirculation. This creates necessary pre-requisites for the in-vessel recovery. (However, the pre-requisites do not guarantee the IVR. The success of IVR further depends on whether the degraded core geometry is actually coolable.)

Attribute 2: ECCS status

This attribute can achieve three mutually exclusive states. They are defined with regard to the injection and transport of the RWST water inventory (from the tank into the RCS / containment).

B = RWST inventory transported into the RCS / containment before RVF;

Typical example of accident sequence which would lead to this state is a large LOCA with successful LP ECCS injection followed by failed recirculation. The RWST inventory was transported into the RCS / containment sump before core damage and before RVF.

A = RWST transported after RVF;

Typical example of accident sequence which would lead to this state is a small LOCA with failure of HP ECCS and failure to depressurize the RCS in order to enable LP ECCS injection. This would lead to core damage and to reactor vessel failure at pressure above the LP ECCS shutoff head. After the RVF the pressure would, however, drop, which would enable LP ECCS injection and transport of the RWST inventory into the containment.

N = RWST not transported;

This is a state resulting from the failure of all ECCS (HP and LP).

The DB systems which are credited for the injection and RWST inventory transport before the reactor vessel failure:

- HP ECCS;
    - In principle, the HP ECCS is credited only if the injection was a part of the sequence before CD. The example of a sequence would be a small LOCA with successful HP injection followed by failed HP recirculation. Absence of core cooling upon completed injection would lead to core damage. However, the RWST inventory would be transported into the RCS / containment before the CD.
- LP ECCS or Containment Spray Pumps.

Additionally, any other alternative systems such as DEC or flexible equipment can be considered for this purpose as a part of severe accident management strategies.

Attribute 3. Containment Heat Removal (CHR)

This attribute can be assigned one of the two mutually exclusive states:

Y = Yes (CHR available);

In accordance with discussion in the previous section, the CHR can be implemented by the Reactor Containment Fan Coolers (RCFC) or by the Containment Spray recirculation in conjunction with LP ECCS recirculation through the RHR heat exchangers.

N = No (CHR not available);

This is complementary state to the first one. The RCFC system is not available. Additionally, the Containment Spray recirculation or/and LP ECCS recirculation through the RHR heat exchangers is not available.

Example of a Hazard Damage State

Let hazard damage state "HAN" be considered as an example of a damage state defined by the above established scheme. (The abbreviation corresponds to the values of the three attributes described above.) This HDS is defined as:

- Reactor vessel failure occurs at high pressure (H);
- RWST inventory is transported into the containment after the reactor vessel failure (A);
- Containment heat removal is not available (N).

Main points of this HDS can be summarized as:

- With RVF at HP the containment can be severely challenged already at the time of the RVF or shortly afterwards, due to dynamic phenomena associated with RVF at HP;
- If containment survives the RVF, corium would be dispersed to some extent rather than piled up and subsequent transport of the RWST inventory would facilitate initial corium quenching; however, without CHR available corium would not dry out; also, pressure and temperature in the containment atmosphere would build up leading to severe containment challenge within some intermediate time window.

This kind of HDS would be related to considerable likelihood of containment failure in the short or intermediate term and should, in principle, be avoided.

Particular HDS, as considered here, is, in principle, related to the response and status of a set of plant systems and functions which are discussed in the next section.

2.4 Main Plant Systems and Functions Related to HDS

Particular core degradation / damage condition would propagate to one among the HDSs depending on the response of plant systems and functions relevant for in-vessel behavior and for the containment status. Based on the discussions in the previous two sections the main plant systems and functions (for the type of plant design and EOP / SAMG framework described in [NARS,18a] and [NARS,18b]) which would determine propagation of CD to HDS can already be identified as:

- RCS depressurization from primary or secondary side;
- LP ECCS injection (transport of RWST inventory into the RCS / containment)

  - Note: This also include the injection of RWST inventory which may have been implemented by either HP ECCS or LP ECCS before core damage. Refer to the discussion in the previous section.
- Low pressure recirculation (in the case of successful low pressure injection);
- Containment spray injection;
- Containment spray recirculation (in the case of successful spray injection);
- Reactor containment fan coolers;

These functions and underlying systems are further described in separate subsections below.

2.4.1 RCS Depressurization

The success of this function would lead to one of two types of outcomes. The first is the possibility of avoiding vessel failure after core damage has already occurred. The second is to change a high pressure vessel failure into a low pressure vessel failure. Either outcome may be achieved with the successful implementation of this function which can be governed by a function restoration procedure or by a SAMG. This function is important for the sequences resulting with high pressure core damage. This could occur due to, for example, the failure of high pressure injection or recirculation along with the failure of actions by the operator to reduce the pressure in order to enable LP ECCS injection before core degradation starts (i.e. the primary pressure remains above the low pressure ECCS shut-off head and core damage occurs). If the operator then succeeds to perform the RCS depressurization, based on the function restoration procedures or SAMGs, it would enable depressurizing the primary system and allowing low head injection and recirculation and, possibly, recovery before vessel failure.

The success criterion for this top event is to depressurize the primary system to below the low head safety injection system shut-off head before vessel failure. It may be formulated as rapid secondary depressurization (in which case emergency feedwater to SGs should, in principle, be available) or opening Pressurizer PORVs.

The limiting time in which the depressurization must be performed can be determined by the accumulator injection setpoint. In principle, this pressure must be reached before vessel failure. Once this pressure is reached the accumulators would inject and the depressurization can be completed (assuming the injection of the accumulators would prevent the vessel failure for the time being). For the considered type of plant design, this time window can be relatively short (e.g. some ten minutes can be indicated for HP transient sequences, but the time estimate would need to be established by severe accident analyses.)

This function event is not relevant for those sequences leading to low pressure CD.

2.4.2 LP ECCS Injection (Transport of RWST Inventory)

In the case where this function follows the success of the RCS depressurization it checks whether the low pressure safety injection system succeeds upon primary depressurization. Success of the LP ECCS in such a case may allow for in-vessel recovery (IVR), while its failure is consistent with low pressure vessel failure. (Note: The success of the low pressure injection / recirculation following the success of the RCS depressurization function is a prerequisite for the IVR. However, it is not by itself sufficient for the successful IVR. Successful IVR additionally requires coolable core geometry which is, as a phenomenological event, addressed in the PSA as a part of the accident progression event tree logic.)

When this function follows the failure of the RCS depressurization it checks whether RWST water is injected after vessel failure. In most cases this refers to low pressure injection. For some of the small LOCA core damage states the special situation exists that vessel failure occurs in spite of the success of high pressure safety injection (i.e. the primary pressure remains above the shut-off head of the high pressure injection system until vessel failure). Thus for these events the RWST content is injected by either the high or the low pressure injection system. Either of the two systems would have the desired effect and the difference in the injection rates do not significantly affect the results. This function is probably not significant in low pressure sequences as low pressure injection would have been initiated prior to core damage. Care must be taken to consider the cases where the RWST has been depleted / injected prior to core damage (i.e. the injection phase succeeded, but failure of recirculation lead to the core damage).

Thus, water injected before vessel failure could lead to the arrest of the core damage and recovery in-vessel. Water injected after vessel failure would spill into the cavity through the failure in the RPV lower head and play a role in the quenching of the debris in the cavity.

The success criterion for this function (for the type of plant design considered) is that 1 out of 2 low pressure safety injection trains succeed upon vessel depressurization (or that the RWST inventory was injected prior to CD).

The time window for operator response in the context of the RCS depressurization is limited from the perspective of preventing vessel failure. This function would be initiated after core uncovering has already occurred. In principle, the operator would be instructed to verify or initiate RHR in a function restoration procedure.

However, the injection of the RWST is also a longer term containment challenge issue. To use, for consideration of containment integrity, a time window as limited by the RCS depressurization context would be overly conservative.

It is, therefore, of interest to consider two time windows for establishing the LP ECCS injection: the first one concerning the possibility for the in-vessel recovery (IVR) and the second one for avoiding containment failure from pressure buildup.

The first one can be established as the time from the accumulator injection (following the success of the RCS depressurization) to vessel failure for the relevant transient and LOCA sequences. The time from core uncovering to vessel failure can be relatively short (e.g. 10 to 20 minutes, for indication; however, the actual time window would need to be established by severe accident analyses.). The question of whether the LP ECCS injection success (following the RCS depressurization success) could prevent vessel failure is finally addressed in the accident progression event tree logic, based on whether the core geometry remains coolable or not.

The second time window is applied in the case that RCS depressurization is not successful. In this case the injection of the RWST is important for containment heat removal. In this case the time window is much longer and is determined by the pressure buildup to the values which can threaten the containment integrity. The weakest point in the containment structure, together with containment pressure at which structural failure can be expected to occur, are subject to containment pressure fragility analysis. Different studies performed to this date have shown that there is a considerable margin in containment structural strength and that failure pressure is expected to be by a factor higher than the design basis pressure. For example, NUREG/CR-6906 shows that, taking out the obvious outliers, median of the fragility curve for Large Dry Pre-stressed Containments is within 2 to 3 times the design basis pressure, [NUR,06].

For the considered type of plant design a one day period can be considered, for indication, to reach this kind of pressure, but the actual estimate would need to be obtained from the severe accident analyses.

Alternative means, e.g. DEC or flexible equipment, included in the EOPs or SAMGs can also be considered.

2.4.3 LP ECCS Recirculation

This function refers to low pressure recirculation before or after vessel failure (as applicable, and depending on the status IVR). Water injected into the vessel would be transported into the cavity through the break in the system or the failure in the reactor vessel lower head. This function event refers to high pressure sequences where low pressure recirculation is available, but it cannot be initiated because the reactor vessel pressure is above the low pressure injection pumps shut-off until vessel failure. It also refers to the sequences with successful depressurization.

After vessel failure, low pressure recirculation would quench the debris in the cavity. If the RHR heat exchanger is available, debris cooling and containment heat removal are established. Therefore, RHR heat exchanger availability is included as part of this function event.

Success of this top event is one of two low pressure trains in the recirculation mode with an RHR heat exchanger available to remove decay heat.

The switchover from the low pressure injection to recirculation is implemented by the control room operator upon RWST low-low level alarm in accordance with the applicable procedure.

Time window for implementation of switchover is from the time of low RWST level alarm (instruction for operator action to switchover to recirculation) to the time of low-low RWST level (caution to stop the pumps to prevent damage). This time depends on the depletion rate and is considered for two different cases.

First case is when the low pressure injection was initiated after successful implementation of RCS depressurization in order to prevent vessel failure (after core damage has already occurred). This is a kind of sequence representative of a situation where one or two primary PORVs are open which may correspond to a medium LOCA. The time window for injecting the RWST to the level when the switchover to recirculation is needed may be indicated at couple to several hours. However, the actual estimate would need to be obtained by the severe accident analysis.

Second case considers the importance of low pressure injection / recirculation from a containment failure perspective (decay heat removal) for sequences where vessel failure has already occurred. In this case, the time window for starting the injection (and then switching over to recirculation upon depleting the RWST to low level alarm for recirculation) would be considerably longer than in the first case: as discussed under the LP ECCS injection above, a one day time period can be indicated, but the actual time would need to be established by the severe accident analysis.

Consideration should also be given to the time window for the switchover itself (i.e. from low RWST to low-low RWST) as well as to the tripping of the LP injection pumps on the emptying of the RWST (and avoid possible damage).

Alternative means, e.g. DEC or flexible equipment, included in the EOPs or SAMGs can also be considered.

2.4.4 Containment Spray Injection

Under the considered type of plant design, [NARS,18a], the containment spray system contains two separate trains of equal capacity, each capable of meeting the design bases. It consists of two pumps, spray ring headers and nozzles, valves, connecting piping, containment recirculation sump, and spray chemical additive tank. Initially, water from the RWST is used for containment spray. When spray injection is completed, containment spray is continued using recirculated water from the containment sump. Each train of containment

spray receives electrical power from separate and redundant electrical power train and receives an actuation signal from separate and redundant actuation train.

The actuation is either by the automatic containment pressure signal or by the control room operator (according to the EOP in charge). The switchover to recirculation is implemented by the control room operator, in accordance with the applicable EOP.

This function refers to spray injection before or after vessel failure. If sprays are initiated before vessel failure, they affect the vessel failure timing by draining the RWST and injecting its inventory into the containment. If the spray pressure set point is not reached before vessel failure, it will be reached at vessel failure resulting in the initiation of containment spray. In this case the core damage timing is not affected by the spray injection, but the sprays play an important role in containment performance. Spray injection reduces the mass fraction of steam in the containment, as steam condenses on the subcooled spray droplets. The containment pressure is reduced and the containment atmosphere is scrubbed of fission products (The containment is also de-inerted).

The success criterion for this event requires one out of two containment spray trains injecting RWST inventory through the ring header and nozzles into the containment.

Concerning the time window, the same discussion applies as under the LP ECCS injection above: a one day time period can be indicated, but the actual time would need to be established by the severe accident analysis.

Alternative means, e.g. DEC or flexible equipment, included in the EOPs or SAMGs can also be considered.

2.4.5 Containment Spray Recirculation

The main function of spray recirculation considered here is the containment heat removal if the sump water is cooled by the RHR heat exchangers. Although the containment spray takes suction from the containment sump, containment heat removal by fan coolers or RHR heat exchangers is required to keep the sump water subcooled. Containment spray recirculation alone does not provide containment heat removal.

The instructions to the operator concerning switchover to spray recirculation are provided in the EOPs / function restoration procedures and are primarily based on containment pressure. Concerning the time window, discussion under the LP ECCS recirculation above applies. One day time period can be indicated, but the actual time would need to be established by the severe accident analysis.

Consideration should also be given to the time window for the switchover itself (i.e. from low RWST to empty RWST) as well as to the tripping of the spray pumps on the emptying of the RWST (and avoiding possible damage).

The success of this function requires one out of two trains of the containment spray system operating in recirculation mode. The containment spray recirculation is activated by the control room operator when the RWST low-low level alarm is generated.

Alternative means, e.g. DEC or flexible equipment, included in the EOPs or SAMGs can also be considered.

2.4.6 Reactor Containment Fan Coolers

The fan coolers serve as containment heat removal and to maintain containment pressure below failure levels. If the containment is isolated the fan coolers prevent its failure due to over-pressure/over-temperature, but do not mitigate molten core-concrete interaction. Fan coolers prevent over-pressure by condensing steam from the containment atmosphere, but

can also de-inert the containment. The operator is required by EOPs to verify that the fan coolers are running in slow speed and to manually start them if necessary.

In the considered type of the plant design, [NARS,18a], the RCFC consists of four fan coolers of equal capacity. The RCFCs utilize component cooling water.

The success criterion for the containment air cooling system, for the considered plant design, requires the operation of at least 2 out of 4 fan coolers at full flow in low speed.

Concerning the time window, the same discussion applies as under the LP ECCS injection above: a one day time period can be indicated, but the actual time would need to be established by the severe accident analysis.

Alternative means, e.g. DEC or flexible equipment, included in the EOPs or SAMGs can also be considered.

2.5 Accident Progression Logic Model Structure

2.5.1 Plant Status Questions and Phenomenological Questions

Previous section identified main plant systems and functions which would determine the HDSs induced by the considered hazard. The status of those systems and functions need to be directly incorporated into the accident progression logic model of the supporting tool.

Additionally, to the status of plant systems / functions there are phenomenological issues which define accident progression. Those also need to be incorporated into the accident progression logic for the considered tool. Here, one of the particularly important issues for accident management is containment bypass (mentioned in section 2.3 above) which may be caused by the creep rupture of the SG tubes in certain type of accident sequences.

In the concept for accident progression logic model structure described below, the plant systems / functions status and accident phenomenology are addressed through two types of questions:

- Plant status questions; these are to be answered by the assessor, i.e. the user of the tool; and
- Phenomenological questions; these are not meant to be answered by the assessor, i.e. tool user; their answers are to be incorporated into the tool's logic.

The first type, plant status questions to be answered by the evaluator assessor, relates to the status of primary system, secondary system, ECCS and containment. In particular, the assessor would need to define the status of the following systems / functions:

- Primary system:
  - Pressure (HP vs. LP);
  - Pressurizer PORVs;
- Secondary system:
  - SG injection systems before RVF;
  - SG PORVs;
- ECCS:
  - RWST injection in short term (before RVF);
  - LP recirculation in short term (before RVF);
  - LP recirculation in longer term (before containment challenge);
- Containment:

- Containment spray;
- RCFC.

The set of nine plant status questions to be answered by the assessor (user of the tool) is presented in Table 1. Each question has its identifier (ID) which is used in the diagrams representing the accident progression logic model.

Table 1: Set of Plant Status Questions

	ID	Question	Answer Type
Primary	HP	Is RCS pressure above the LP ECCS shutoff head? (Question differentiates between HP and LP sequence.)	Y/N (0/1)
	PRZR	If HP: Is it possible to depressurize RCS by Pressurizer PORVs before reactor vessel failure?	Y/N (0/1) Probability
Secondary	SGFW	If HP: Is it possible to inject into SG and cooldown / depressurize RCS before reactor vessel failure, using also SG PORVs as needed?	Y/N (0/1) Probability
	SGRV	If HP: Is it possible to depressurize RCS before reactor vessel failure, using only SG PORVs?	Y/N (0/1) Probability
ECCS	RWST	Can RWST be injected before reactor vessel failure? (HP ECCS, LP ECCS or alternatives)	Y/N (0/1) Probability
	LRV	Is LP recirculation available or can be established before reactor vessel failure? (LP ECCS or alternatives)	Y/N (0/1) Probability
	LRC	Is LP recirculation available or can it be established before containment failure? (LP ECCS or alternatives)	Y/N (0/1) Probability
Containment	SP	Is Spray available Or can Spray injection and recirculation be established before containment failure? (Alternatives included.)	Y/N (0/1) Probability
	RCFC	Is RCFC available Or can be established before containment failure?	Y/N (0/1) Probability

The answers to the plant status questions from Table 1 are in the form of “Yes/No” (Y/N) or in the form of probability. (The only exception is the first question (“HP”) to which the answer is of the type “Y/N” only.) Actually, all the answers can be interpreted in terms of probabilities where “Yes” would mean probability of 1 and “No” would mean probability of 0. (See example below.) In this way the input would be numerical (quantitative) only.

In some cases, the answer would readily be “Yes” / “No” while in some other it would need to be provided as probability. (Here, it needs to be considered that the questions would be answered in a repeating manner, i.e. in cycles.)

For example, taking the question “RWST”:

- Assuming that, at the time the question is asked, RWST injection has been completed and monitored parameters show that vessel is not ruptured (e.g. core water level and / or RCS pressure) the answer is clearly “Yes” (1);
- Assuming that, at the time the question is asked, vessel is known to be failed and RWST is full, the answer is clearly “No” (0).
- For other cases, i.e. vessel is not failed and RWST is not injected, probability may be assigned, based on the availability of injection systems or on probability to restore / establish them.

The alternatives between which a decision is to be made would then be expressed as vectors of answers (vectors of probabilities).

To illustrate the concept, the following simple example is provided:

Example: Assume that there is a HP core degradation sequence with loss of DB Emergency Feedwater and ECCS. Assume that the following two alternatives are being considered, for which a mobile pump can be used (either for the first or for the second):

Alternative #1: By a mobile pump inject to SG;

Alternative #2: By mobile pump inject RWST into containment (no HP pump to enable injection into RCS) and depressurize the RCS by Pressurizer PORVs.

Possible inputs by the assessor into the tool for the Alternative #1 (left side) and the Alternative #2 (right side) are, just for illustration, shown in Figure 5.

The two inputs are briefly explained as follows:

Alternative #1:

HP = 1;	RCS pressure has been read to be above the LP ECCS shutoff head; therefore, the answers for PRZR, SGFW and SGRV need to be provided;
PRZR = 1;	Pressurizer PORVs are confirmed operable; user is confident that RCS can be successfully depressurized before reactor vessel failure with Pressurizer PORVs; (see note below);
SGFW = 0.8;	User assesses that there is 80% of a chance to inject into SG by the mobile pump and succeed to cooldown / depressurize RCS before reactor vessel failure, using also the SG PORVs; (see note below);
SGRV = 1;	SG PORVs are confirmed operable; user is confident that RCS can be successfully depressurized before reactor vessel failure using only SG PORVs; (see note below);
RWST = 0;	Since the mobile pump would be used to inject into the SG, there is no way that RWST is injected before reactor vessel failure;
LRV = 0;	LP recirculation is not available and there is no way to establish it before reactor vessel failure;

LRC = 1; LP recirculation is not available, but the user is confident (based on the available information) that it can be established before containment challenge; (time window in the range of one day);

SP = 1; Containment Spray is confirmed available;

RCFC = 1; RCFC is confirmed available.

Note concerning the depressurization by PRZR, SGFW or SGRV: It is important to recognize that probability of SG tube creep rupture (and, hence, containment bypass) is different for the three techniques. Preferable technique for depressurization should be SGFW, because it keeps the SG tubes wet and reduces to minimum the probability of having the SG tube creep rupture. The user assesses only feasibility of technique (whether it can be implemented or not), not the probability of having the SG tube creep rupture along its implementation. This probability is to be incorporated into the tool. Thus, even if user assesses that depressurization by SGFW can be implemented only with 80% chance and by other two techniques with 100% chance, it does not mean that other two are better. This is to be decided (recommended by the tool).

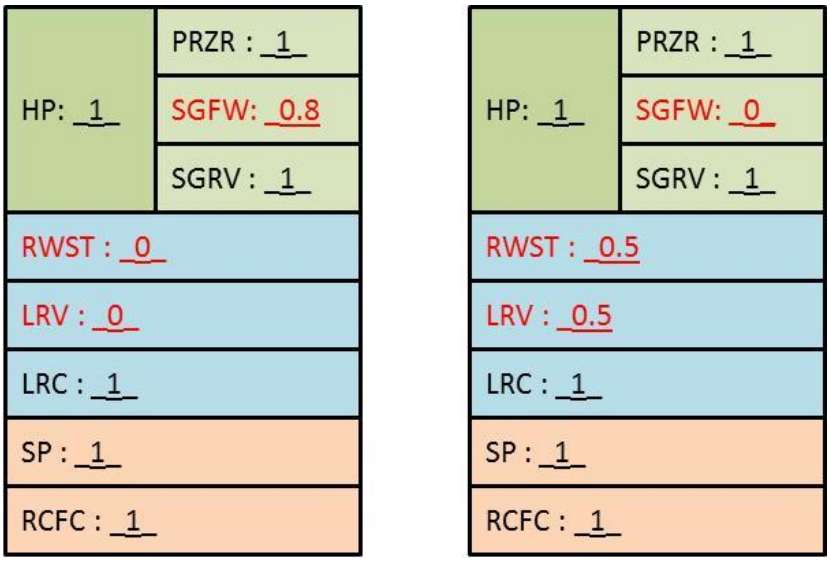

Figure 5: Example: Input by Assessor for Alternative #1 and Alternative #2

Alternative #2:

HP = 1; RCS pressure has been read to be above the LP ECCS shutoff head; therefore, the answers for PRZR, SGFW and SGRV need to be provided;

PRZR = 1; Pressurizer PORVs are confirmed operable; user is confident that RCS can be successfully depressurized before reactor vessel failure with Pressurizer PORVs; (see note above);

SGFW = 0; Mobile pump would be used for injecting the RWST into the containment; there is no way to inject into SGs; (see note above);

SGRV = 1; SG PORVs are confirmed operable; user is confident that RCS can be successfully depressurized before reactor vessel failure using only SG PORVs; (see note above);

RWST = 0.5; User assesses that there is 50% of chance to establish injection by the mobile pump from the RWST to the RCS (to be depressurized by PRZR or

SGRV) and to inject / recirculate before reactor vessel failure (and avoid reactor vessel failure);

LRV = 0.5; See under RWST above;

LRC = 1; User is confident that LP injection / recirculation can be established before containment challenge; (time window in the range of one day);

SP = 1; Containment Spray is confirmed available;

RCFC = 1; RCFC is confirmed available.

Beside plant status questions there are also phenomenological questions. The questions related to creep rupture of the SG tubes are presented by Table 2. Each of these questions is assigned an identifier (ID) which is used in the logic model structure. These questions are not meant to be answered by the evaluator. The answers (probabilities) will be elaborated in Task 5.4 and incorporated in the logic structure of the tool.

Other phenomenological issues will be quantified by means of phenomenological trees which will be incorporated into the tool in the form of a matrix which converts the HDS likelihoods into the release category (RC) likelihoods.

Table 2: Phenomenological Questions

ID	Question
CRSGFW	What is the probability of creep rupture of SG tubes before other RCS creep rupture and before the vessel failure, assuming SG injection established and keeping SG tubes wet?
CRSGSR	What is the probability of creep rupture of SG tubes before other RCS creep rupture and before the vessel failure, assuming RCS depressurization by SG PORVs (no SG injection)?
CRSGPR	What is the probability of creep rupture of SG tubes before other RCS creep rupture and before the vessel failure, assuming RCS depressurization by the Pressurizer PORVs?
CRSG	What is the probability of creep rupture of SG tubes before other RCS creep rupture and before the vessel failure, assuming no RCS depressurization?

2.5.2 APET Logic Structure

Based on the discussions in sections 2.2, 2.3 and 2.4 above the core damage sequences can, depending on the pressure at which core degradation starts and on the implementation of the RCS depressurization, be broadly divided into three major categories:

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

In the overall accident progression event tree (APET) structure the sequences from the first group will be presented by a sub-tree referred to as “SUB1”. The sequences from the second group will be presented by a sub-tree named “SUB2”. The sequences from the third group will be presented by a direct path (sequence) leading to early releases.

A diagram representing the overall APET structure is shown in Figure 6. As shown, the APET structure to be incorporated into the tool would consist of three main parts:

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

The main tree is shown in Figure 7. It is provided in the form of a sequence diagram with boxes containing the statements which correspond to the questions from Table 1 or Table 2. Each statement is linked by identifier to the corresponding question in Table 1 or Table 2 (column “ID”). Each box with a statement / question has one input (at the right side or at the upper side) and two outputs: one at the right side and one going downward. The output going to the right side (horizontally) represents the branch with “statement is true” (answer is “yes”). The output going downward (vertically) represents the branch with “statement is false” (answer is “no”).

The main tree contains the logic which distinguishes between the LP CD sequences and the HP CD sequences. The LP CD sequences are sent to the SUB1 sub-tree mentioned above. The HP CD sequences are further divided into those in which creep rupture occurs at the SG tubes and all other HP CD sequences. The sequences with SG tube creep rupture are sent directly to early release. (The release categories shown in Figure 6 are explained in section 4.) All other HP CD sequences are sent to the SUB2 sub-tree mentioned above.

The sub-tree SUB1 is shown in Figure 8. It is provided in the same form as the main tree. Each statement in SUB1 sub-tree is linked by identifier to the corresponding question in Table 1 (column “ID”). The end states of the SUB1 sub-tree are the HDSs of the type “Rxx” or “Lxx” which comes from the definition of the SUB1 sub-tree. (For definition of these HDSs, e.g. RBY, RBN, LBY etc, refer to section 2.3.)

The sub-tree SUB2 is shown in Figure 9. It is provided in the same form as the main tree and SUB1. Each statement is linked by identifier to the corresponding question in Table 1 (column “ID”). The end states of the SUB2 sub-tree are the HDSs of the type “Hxx” which comes from its definition.

The phenomenological tree can be thought of as a logic model used to map the HDSs into the RCs. A concept for the general phenomenological tree (to cover all HDS-specific phenomenological trees) is shown in Figure 10. This concept is based on the four time windows during severe accident progression which are many times considered in Level 2 PSAs:

- Time window covering the time up to the reactor vessel failure (TW1);
- Time window following the reactor vessel failure and covering the dynamic phenomena associated with ex-vessel phase (TW2);
- Time window following the end of the dynamic phenomena and covering a specified period of time, such as one day or similar (TW3);
- Longer term time window (TW4).

The key issue in all time windows is containment integrity and a part of it (although not all of it) is the issue of hydrogen burn. These issues are, directly or indirectly, questioned in all time windows.

Other main key issues in TW1 are the IVR and creep rupture, as discussed above. In TW2 other main key issues are the dispersion of the corium and quenching of the debris. In TW3 the main other key issue is dry-out of the quenched debris. Based on the initial quenching and longer term prevention of the dry-out, the sequences and their corresponding logic trees are divided into “wet case” and “dry case”. In TW4 the important other issue is, in the dry case, the integrity of the basemat. The presentation of the tree logic is conceptual. Nevertheless, the downward path generally indicates that a statement is false (e.g. there is no containment integrity; there is no debris quench…). The outcomes (end-states) of the phenomenological tree are different release categories. Explicitly shown in the diagrams are sequences with failure of containment integrity in TW2. Those are failures of containment associated with dynamic phenomena (resulting from HPME). Those failures, as well as any failures in TW1 (not explicitly shown in the diagram) are considered to lead to early releases.

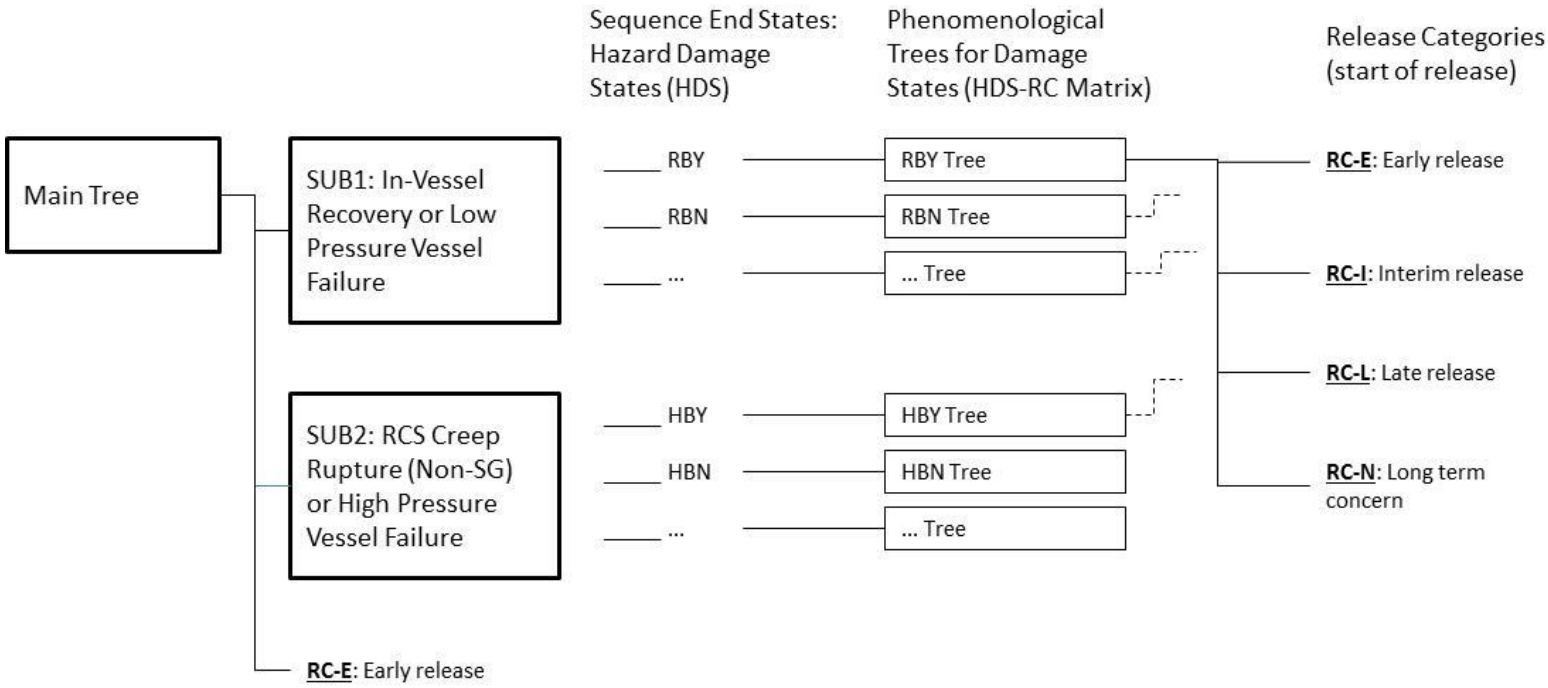

Figure 6: Overall APET structure

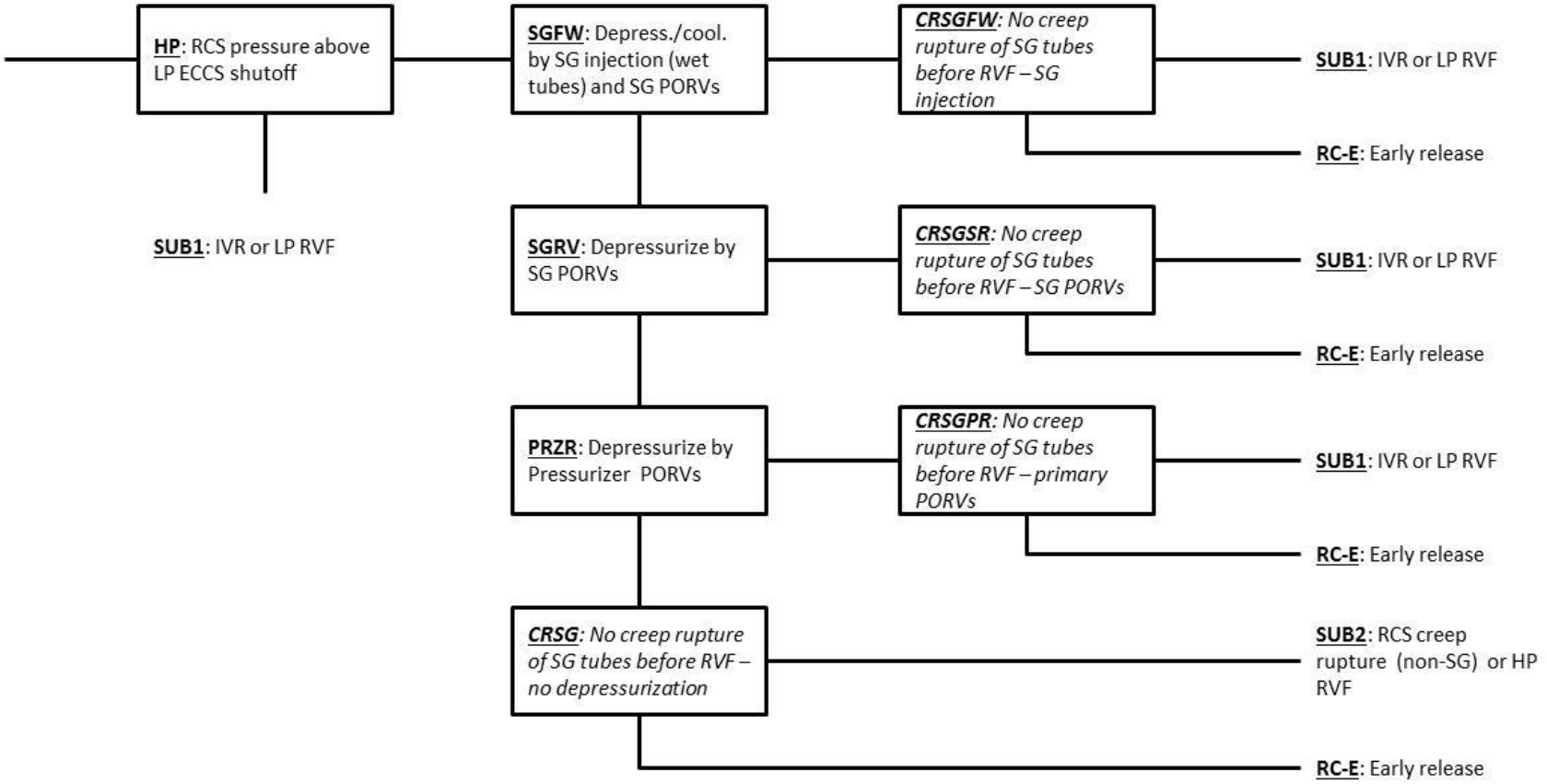

Figure 7: Main Tree

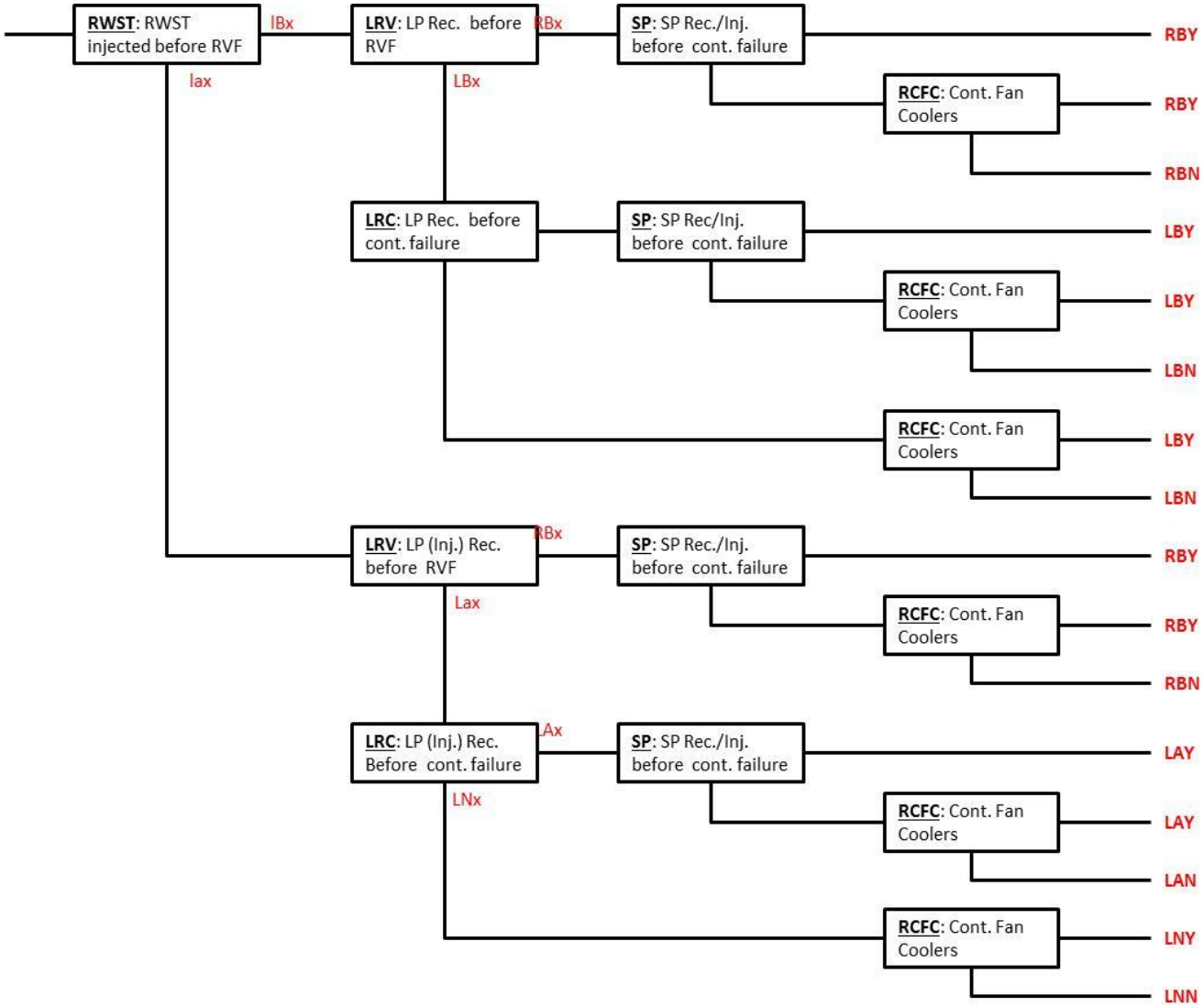

Figure 8: Sub-Tree SUB1

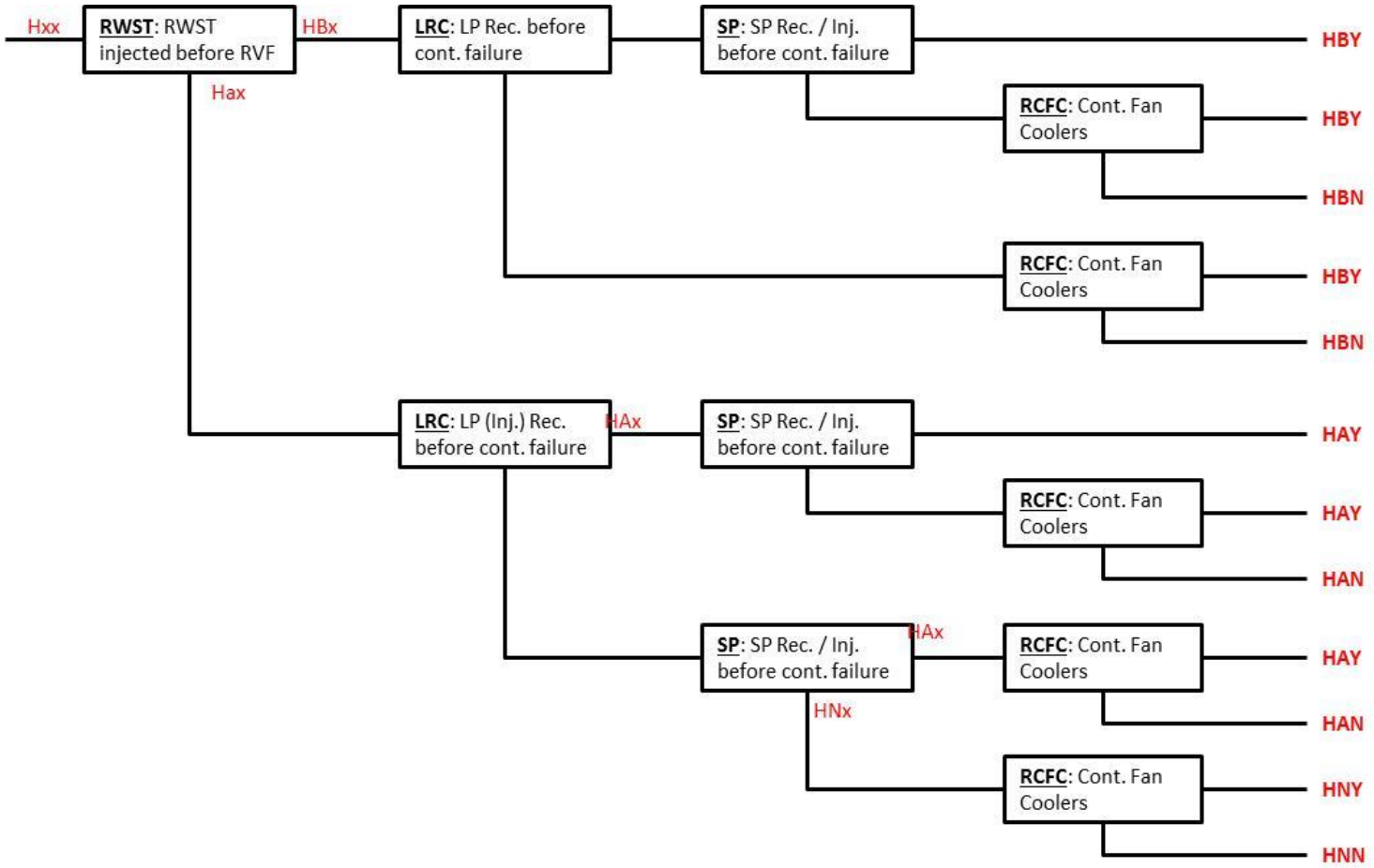

Figure 9: Sub-Tree SUB2

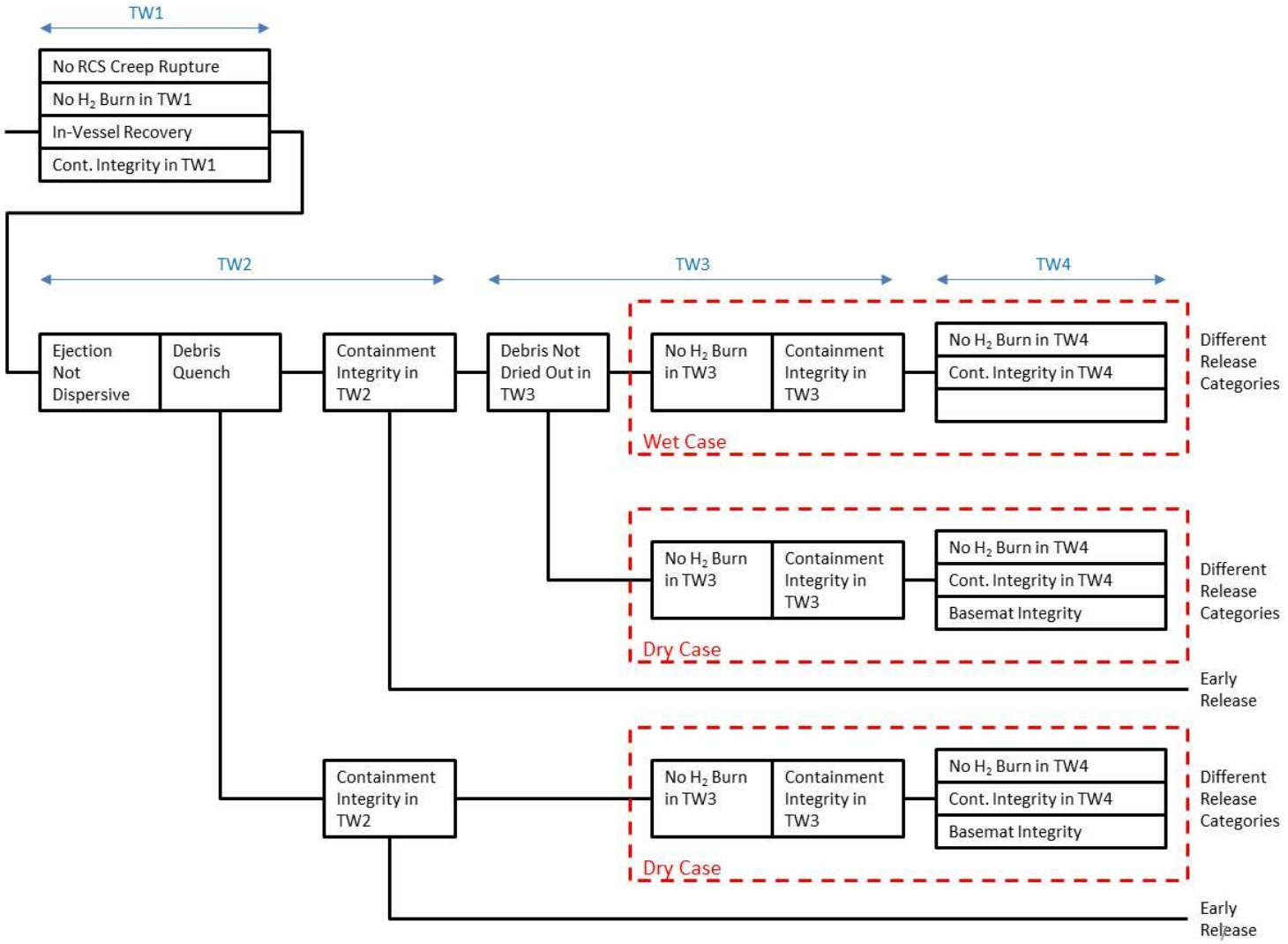

Figure 10: Concept of General Phenomenological Tree

In the considered tool each HDS-specific phenomenological tree will be incorporated as a vector of split fractions which maps the HDS probability into the set of RC probabilities. The set of phenomenological trees indicated in Figure 6 will, thus, be in the tool presented as a "HDS-RC" matrix which translates a set of HDS probabilities into a set of RC probabilities. This matrix will be populated with conditional probabilities obtained on the basis of knowledge from the Level 2 PSAs and on the basis of the severe accidents performed within the Project. It will be further elaborated in the report developed under the Task 5.4.

2.5.3 Probability Model for Answers to Plant Status Questions

The plant status questions which would need to be answered by the assessor (i.e. tool user) are presented in Table 1. The answers to these questions (i.e. user's input to the tool) are provided in terms of probabilities (where probability of 1 represents "Yes" and probability of 0 means "No"). The probabilities may be based on judgement which relies on the available information on the plant status and on the knowledge. However, it may be helpful to develop a model for establishing particular probability which would put some formalism into assignment of the probabilities and avoid or at least reduce the possibility that probabilities may be assigned completely subjectively or arbitrarily. Probability model will be elaborated in the report under the Task 5.4.

It would need to be success-oriented, because questions are success-oriented. It can be established as a product of time-dependent term $Q_{ph}(t)$ and shaping factor c:

$$Q = Q_{ph}(t)\, c \quad ; \quad 0 \leq Q \leq 1 \qquad \text{(Equation 1)}$$

The term $Q_{ph}(t)$ would represent phenomenological ("theoretical") probability of successful implementation of considered function under the assumptions that:

- Implementation is initiated at time t; and
- It is done by (phenomenologically) fully adequate equipment / system (i.e. by the equipment / system which were proven by test or analysis to be able to adequately perform the function).

This term can be presented by inverse cumulative function of lognormal distribution:

$$Q_{ph}(t) = 1 - F(t) = 1 - \Phi\left(\frac{\ln t - \mu}{\sigma}\right) \qquad \text{(Equation 2)}$$

In the above equation $F(t)$ represents cumulative function of lognormal distribution, $\phi(\ \ )$. Represents cumulative function of standard normal distribution, while the terms μ and σ represent mean and standard deviation of the underlying normal distribution.

The lognormal distribution was found useful many times in risk assessments, especially when a probability is to be established on the basis of assessed low and high values (or a mean value and low / high value).

For example, in a number of problems two time windows can be assessed by severe accident analyses:

- Minimum time during which a function would need to be established in order to be successful with high likelihood (or unsuccessful with low likelihood);
- Maximum time during which a function would need to be established in order not to be unsuccessful with high likelihood.

The first time (minimum) can be, for example, established as 5th percentile, $t_{0.05}$: if the action is performed (function established) sooner than this time, the chance of its success is considered to be higher than 95% (less than 5% chance of failure).

The second time (maximum) can then be established as 95th percentile, $t_{0.95}$: if the action is performed (function established) sooner than this time, the chance of its failure is considered to be smaller than 95% (still more than 5% chance of success).

Assuming these two time windows are known, it can be shown that the parameters of the distribution can be calculated as:

$$\sigma = \frac{\sqrt{\frac{t_{0.95}}{t_{0.05}}}}{\Phi^{-1}(0.95)} \quad \text{(Equation 3)}$$

$$\mu = \ln\sqrt{t_{0.05}t_{0.95}} = \ln t_{0.50} \quad \text{(Equation 4)}$$

The model based on the lognormal distribution can provide different time profiles for probability of success, depending on the nature of the function being established. This is illustrated by Figure 11. Upper part of the figure shows the profiles for the actions (functions which need to be initiated on “the sooner the better” principle. The lower part of the figure shows two profiles for the actions which are delayed but once the time comes they need to be started / implemented rather quickly.

Second term in Equation 1 above, the shaping factor c (c≤1), would be used to adjust, as necessary, the “phenomenological” probability $Q_{ph}(t)$. For example, it may be used to reduce the success probability due to non-confirmed or questionable adequacy of the substitute equipment (e.g. flexible equipment) which may need to be used in the case of unavailability of verified design basis or DEC equipment.

Some examples of how the discussed model can be used to adjust the probability of successful establishing or recovery of a function (system or equipment) are indicated by Figure 12. The figure shows three different probabilities established by the model for three different conditions or situations:

A. Equipment to implement the function is considered adequate and is available now.

B. Equipment to implement the function is considered adequate, but is not available now. Assessor is confident that it will be available in less than 2 hours.

C. Equipment is to be available in less than 2 hours, but it may or may not be really adequate (e.g. 50% confidence).

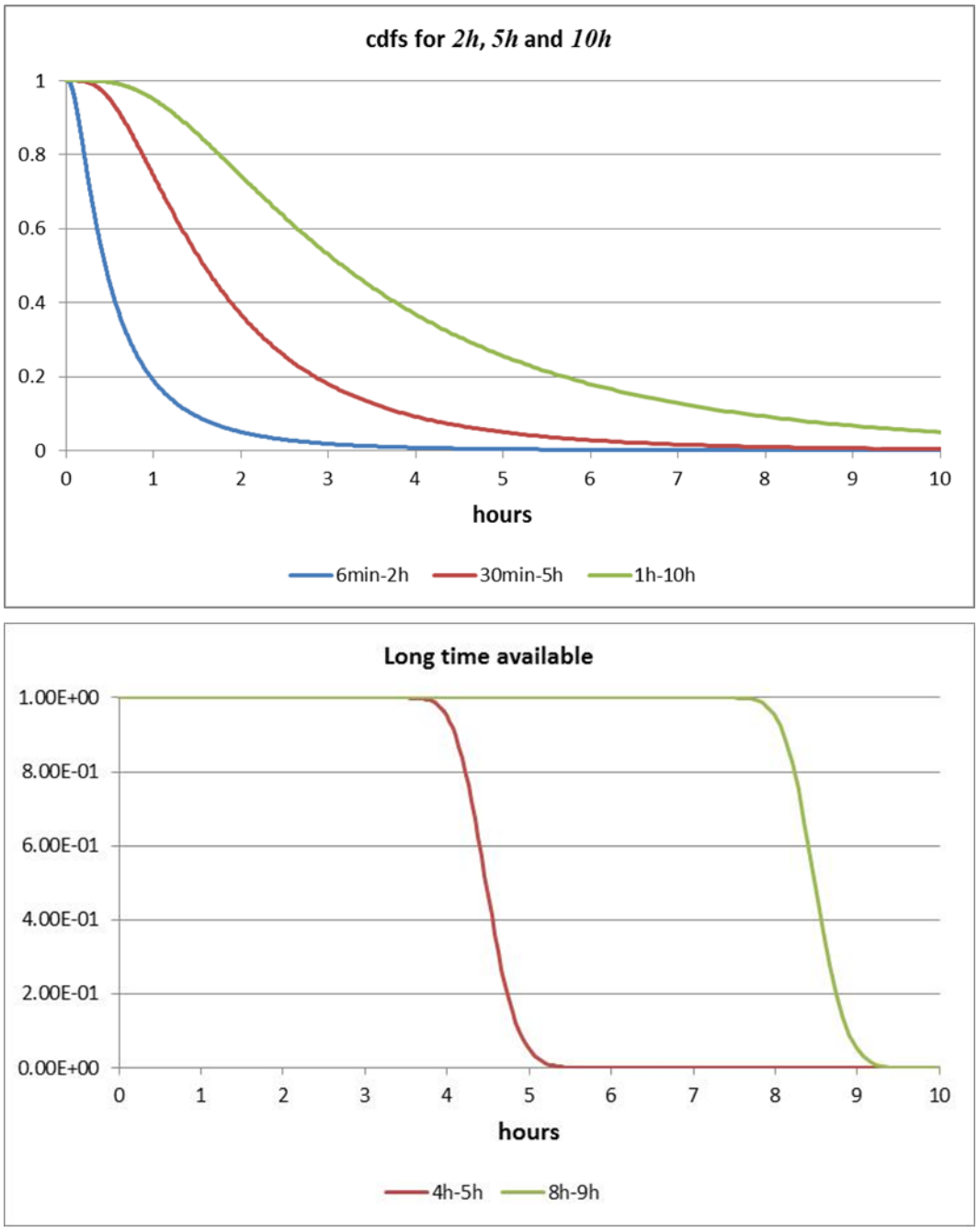

Figure 11: Different Time-Dependent Probability Profiles Established by Lognormal Distribution

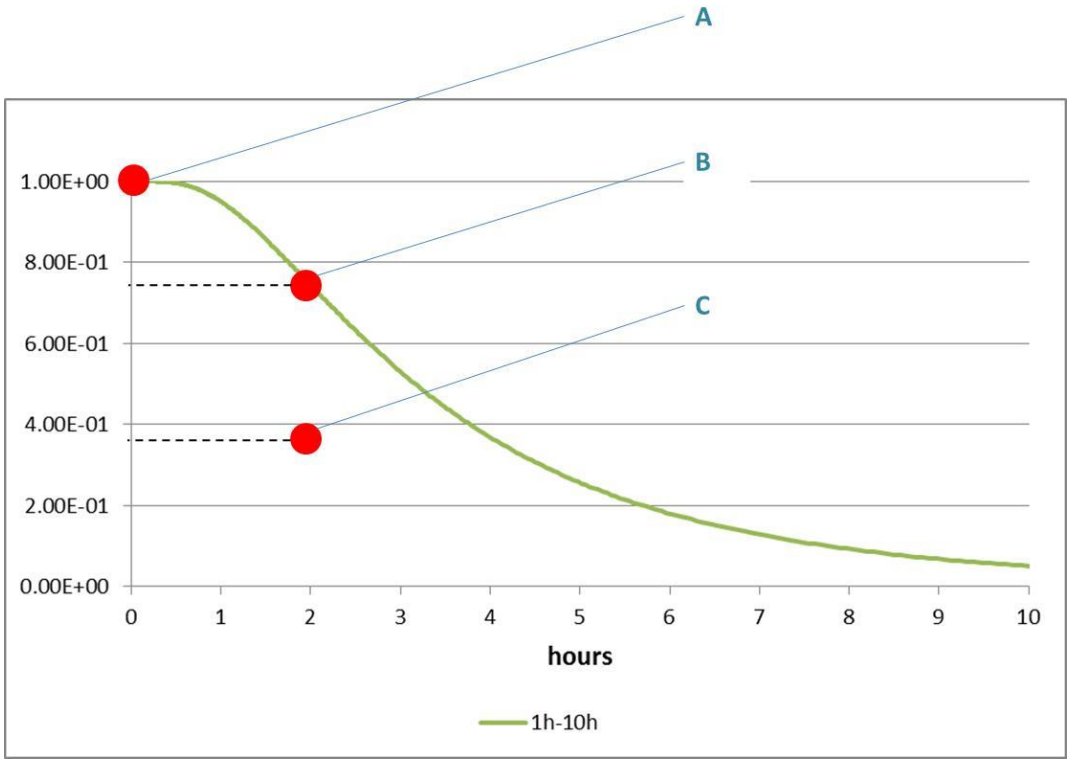

Figure 12: Examples of Adjusted Probabilities for Establishing or Recovering a Function

3 Types of Decisions and Actions in Severe Accident Management

3.1 Types of Procedures/Guidelines under Accident Management Program

Depending on the level of defense in depth breached, the following are the four main objectives of accident management ([IAEA,04], [IAEA,19]):

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

The NARSIS report 5.2 [NARS,18b] describes a general concept of Emergency Operating Procedures (EOP), Extreme Damage Management Guidelines (EDMG) and Severe Accident Management Guidelines (SAMG) typically used in the second generation operating nuclear power plant, representing the European fleet. EDMGs are not part of consideration for this project but cover the execution of SAMG for certain scenarios. Accordingly to the reference [IAEA,04], in the case of deviation of certain plant parameters measured in an NPP, alarm goes off in main control room and the operators use alarm response procedures (ARP) to respond to alarms. If they are not able to successfully correct the situation, they use the Abnormal Operating Procedures (AOP). If the problems still persists, the reactor trip may be actuated and, the design basis accident might be occurring and then the Emergency Operating Procedures (EOP) are used by MCR staff to assess the plant and equipment status and initiate critical safety functions monitoring and activate engineering safety equipment or perform operator other actions if necessary. If operators' actions from EOPs

are not successful, the core starts to heat up due to decay heat. If core becomes uncovered and overheated during the longer period the severe accident with significant core degradation can occur. If the restorative actions in the EOP domain fail to achieve the desired objectives, core damage is expected to occur. Priority now shifts to severe accident management.

Once MCR staff indicates the inadequate core cooling (by monitoring core exit temperature above certain level) and there is no available systems and equipment to establish it, MCR staff exits the EOP and enter to Severe Accident Control Room Guidelines (SACRGs) till notified that TSC is operable. Since the usage of EOPs is intended to prevent the core damage ("Preventive Core Damage Actions"), the usage of SAMG Package is intended to ultimately protect the containment as the last fission product barrier and mitigate the fission products release ("Mitigating Core Damage Actions").

The responsibility for accident management of NPP is transferred from operators in MCR to TSC once TSC declared their operability (declared to be able to recommend the first action to the MCR staff). In order to manage severe accidents, the SAMGs are used by TSC staff. In the contrast to previously used procedures (e.g. ARPs, AOPs, EOPs), where operators followed the procedures line by line with prescribed way of assessment of plant indications or/and critical safety functions, the TSC staff through the usage of SAMGs need to evaluate the different strategies including potential positive and negative impacts of any Candidate for High Level Mitigating actions (CHLAs) before making decisions.

Figure 13 illustrates the different Accident Management Program procedures and guidelines related to plant conditions and responsibility for decision making process.

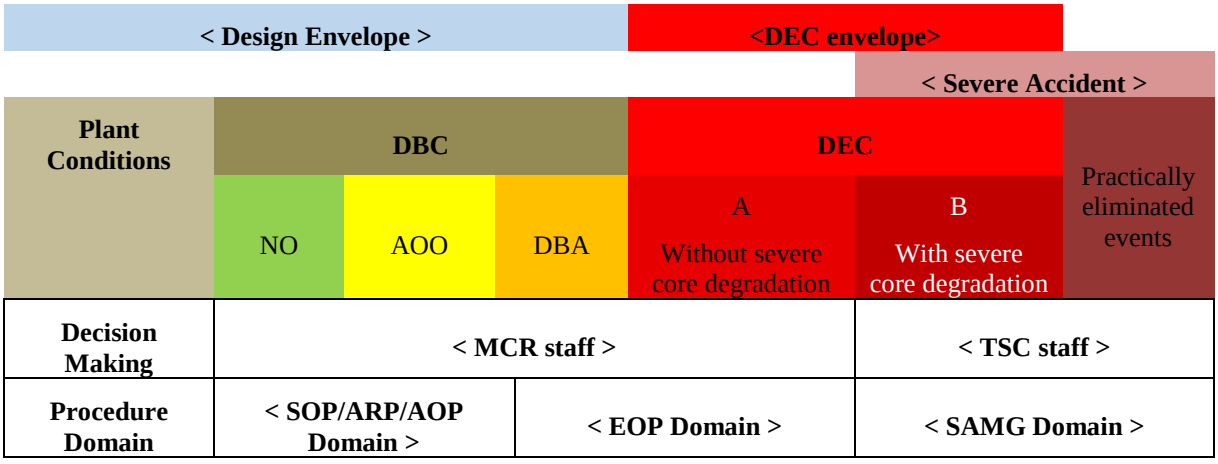

Figure 13: Illustration of Accident Management Program

3.2 Severe Accident Progression and Degrees of Severity

As it was identified in 2.2, in a PSA, the plant damage states (induced by a hazard / initiator or by progression of triggered accident sequence) are typically characterized by a set of attributes. From deterministic point of view and SAMG approach ([IAEA,04], [EPRI,12a], [EPRI,12b]), for development of decision making tool it is necessary to compare analytically available plant response (critical parameters - plant specific calculated by severe accident analysis codes or generic response discussed in [EPRI,12a] and [EPRI,12b]) with actual plant information to evaluate possible accident progression and time window for proper TSC/MCR staff actions. Especially, factorization of different accident progression paths is needed if performed SAMG actions are not efficient *or* there are no any actions performed during observed time at all.

In the case of an accident sequence with sustained loss of core cooling, the accident progression can involve two phases, with fundamental differences in the challenges to safety functions and the source term: the in-vessel phase and the ex-vessel phase. An example of the sequence ([IAEA,04], [EPRI,12b]) of in-vessel phenomena follows:

a) Overheating of fuel and cladding;

b) Onset of exothermic oxidation of the cladding, accompanied by production of hydrogen;

c) Damage of the fuel cladding;

d) Rapid increase in hydrogen production, with a possible challenge to containment integrity due to deflagration/detonation;

e) Melting of the cladding, fuel and core materials and downward relocation of the corium;

f) Interaction of the molten corium with the residual water in the RPV;

g) Potential steam explosions caused by a molten corium–water reaction;

h) Heating of the RPV by the molten corium.

At the last stage the possibility of RPV failure must be seriously considered. Cooling of the lower head of the RPV may be restored by flooding the core in-vessel or by using water to cool the lower head from the outside. If attempts to stop the accident progression at this point are not successful, vessel melt-through will occur and the ex-vessel phase of the accident will commence. During this phase a variety of phenomena challenge the containment integrity. They may include:

a) Damage to the containment due to high pressure expulsion of the corium (high pressure melt ejection (HPME) and direct containment heating (DCH)).

b) Hydrogen combustion (deflagration/detonation), with hydrogen produced during the in-vessel phase and later during the ex-vessel phase by core–concrete interaction (which may also produce carbon monoxide, which is also combustible) or a molten corium–water reaction; apart from the threat of global combustion there is a danger of local deflagrations/ detonations which can generate missiles that may challenge the containment integrity.

c) Core–concrete interactions which directly jeopardize the integrity of the containment through concrete basement melt-through (Molten Corium Concrete Interaction (MCCI)).

d) Long term pressurization and/or temperature increase, ultimately leading to failure of the containment.

e) Bypass of the containment, e.g. through a damaged steam generator (SG) due to tube creep rupture, or through some other pathway, e.g. an interfacing system LOCA.

Figure 14 illustrates the severe accident progression diagram with typical times (from various severe accident analyses) of phenomenologically critical events (e.g. core uncovering, starting of fuel cladding oxidation (hydrogen production), reactor pressure vessel failure and containment failure) for the reference plant (2000 MWth). Also, Figure 14 illustrates severe accident progression for two major groups of initiating events/sequences grouped based on RCS pressure (low pressure (LP) or high pressure (HP) sequences) at time when reactor pressure vessel (RPV) fails. RPV failure at high pressure can challenge the containment structure almost instantaneously (see 2.4.1, 2.5 and Figure 10 above) due to stronger dynamic phenomena (related to High Pressure Melt Ejection (HPME) and Direct Containment Heating (DHC)). Brief description of LP and HP sequences are given in section 1.3.1 and 1.3.2 of [NARS,18b].

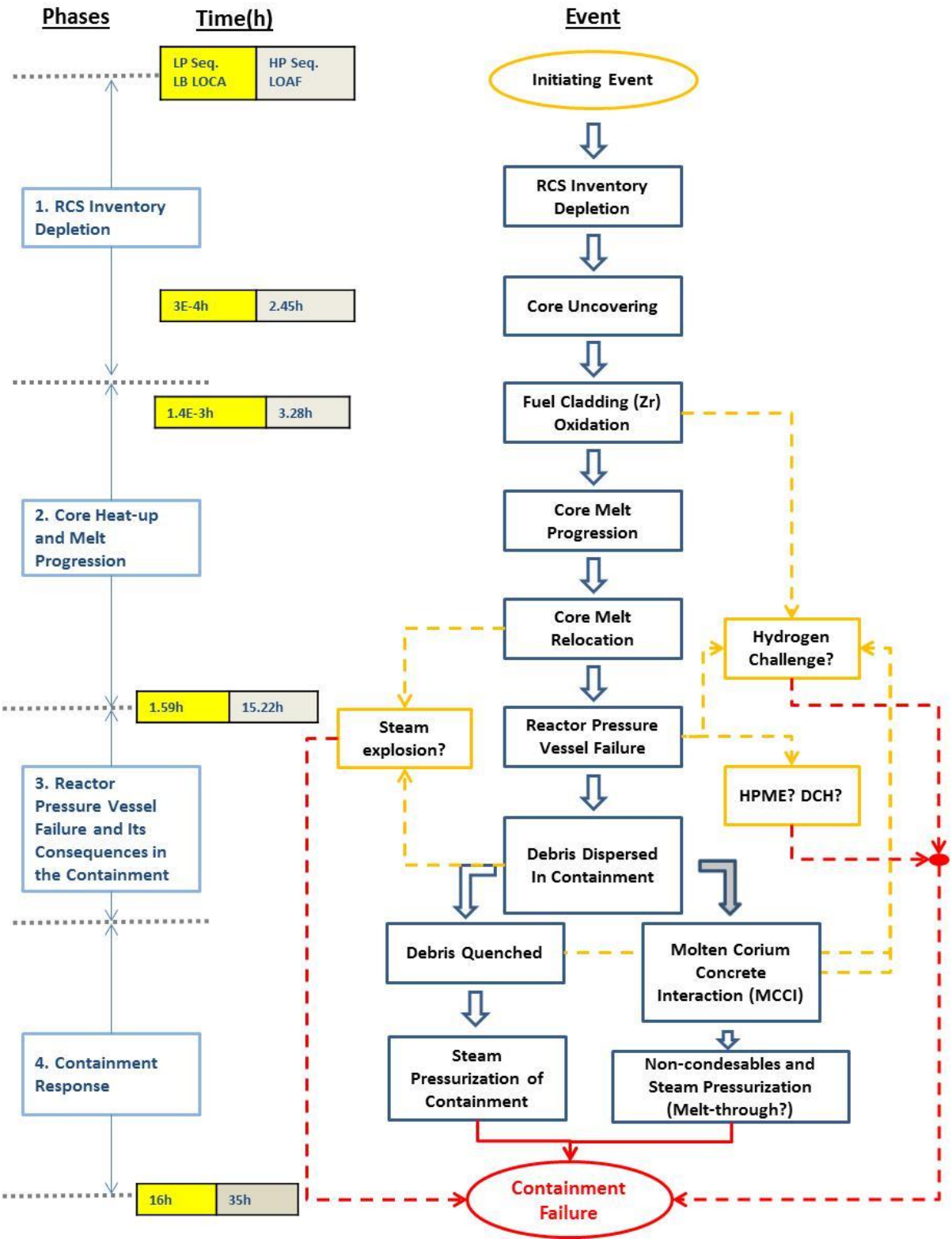

Figure 14: Severe Accident Progression Diagram

3.3 Plant Damage Condition Diagnosis as used in SAMG

Section 2.2 in this report discusses the Hazard Damage States (HDS) from PSA standpoint. In a PSA, the plant damage states (induced by a hazard / initiator or by progression of triggered accident sequence) are typically characterized by a set of attributes. Both references ([IAEA,04], [EPRI,12a]) used for preparation of generic SAMGs provide a structure to define a limited number of plant damage states mainly from DSA (deterministic safety analysis) point of view. A severe accident is defined as any accident that results in significant degradation of fuel in a reactor core or stored in a spent fuel pool so that there is the potential for a substantial release of fission products from the affected fuel assemblies. Such an accident results from a mismatch between the rate of heat generation within the fuel and the rate of heat removal at the surface of the fuel cladding assuming a combination of SSCs failures caused (induced) directly by a hazard itself, as well as damage caused by triggered accident sequence; and impact of this combined damage on plant's systems, functions and mitigation capability.

Report [EPRI,12a] discusses the potential plant damage conditions mainly from deterministic point of view, correlating the results of deterministic safety analyses (performed by the MAAP code) with barriers conditions and recognitions of possible symptoms as seen from available parameters in MCR or TSC. It has to be understood that MCR/TSC staff is limited with number of installed and qualified instrumentations used for diagnostics ([EPRI,93b]). Assumed usage of instrumentation for severe accident management decision making process (through Diagnostic Flowchart (DFC) and Severe Status Challenge Tree (SCST) is described in section 3.2 of [NARS,18b].Table 3 summarizes the major symptoms with respect to core and RCS damage states. Table 4 summarizes the major symptoms with respect to containment damage states. It should be noted that MCR/TSC staff does not evaluate through DFC and SCST either core or containment damage states but they are focused on entrance to applicable SAGs or SCGs (implementation of SAMG strategies) based on plant parameter trigger (setpoint). Understanding of plant damage state is necessary for assessment of positive and negative impacts in the future SAMG Decision Making Tool. Such tool should evaluate the plant status based on the measured plant values in comparison with performed operator actions (or without) and possible accident progression (and associated probabilities, see 2.5 above).

Table 3: RCS Damage Condition Descriptors and Possible Symptoms

Designator	Damage Condition Descriptors	Possible Symptoms [Note1]
OX	Core significantly oxidized but intact (cladding ballooning or collapse might have occurred, but none of the core structural materials—fuel, clad, or steel—are molten)	• Limited radiation in containment, perhaps due to primary coolant activity and the release of fission product gases from fuel cladding gap, as well as limited diffusion from the fuel matrix. • Core outlet temperature (where appropriate) > 650°C. • Considerable superheat (>100°C) measured at the hot leg thermocouples (where appropriate for the NSSS system and the instrumentation). • Core water level: collapsed water height at or below core mid-plane. • Inference of elevated core temperatures by a combination of parameters. • Loss of pressurizer level (for PWRs without a loop seal). • External core power monitors increasing. • Some or increasing hydrogen measured in containment
CD	Core significantly oxidized and not intact (core structural components have melted and relocated downward)	• High radiation in containment. • Increasing hydrogen measured in containment. • Core outlet temperatures (where appropriate) > 1093°C.

Designator	Damage Condition Descriptors	Possible Symptoms [Note1]
		• Loss of pressurizer level (for PWRs without a loop seal). • External core power monitors increasing. • Collapsed water level at or below 40% core height for 10 minutes or longer. • Inference of elevated core temperatures by a combination of parameters.
EX	Core debris relocated to the primary containment (RPV failed)	**There is no unambiguous symptom for condition EX.** Some related symptoms include the following: • High radiation in containment. • Substantial hydrogen measured in the containment (equivalent to more than 20% of the active fuel cladding reacted). • Given damage condition CD (Core Damage), the RCS is depressurized to essentially the containment pressure. • Pressurization of the containment combined with RPV depressurization. • Rapid increase in radiation level in containment (radiation monitors must be less than saturation values). • Rapidly increasing and sustained containment temperatures (more than the saturation temperature). • A sudden increase in hydrogen concentration in containment combined with a depressurization of the RPV. • Sudden loss of water level in the RPV and RPV is depressurized.

Notes for Table 3:

1. This is a list of possible symptoms, some of which might have occurred in advance of the RCS damage condition. Nonetheless, when combined with other symptoms, these are indicators of the accident condition. Also, some of these symptoms might not be observable due to sequence-specific conditions.

Table 4: Containment Damage Condition Descriptors and Possible Symptoms

Designator	Damage Condition Descriptors	Possible Symptoms[Note1]
CH	Containment is closed but challenged	• Given RCS damage condition BD, the combination of a high RCS pressure and dry steam generators would indicate a potential challenge to the steam generator tube integrity. • Significant hydrogen concentration and increasing. • CO and/or CO2 measured in containment and increasing. • A pressure increase caused by a complete burning of the measured combustible gases could result in a pressure sufficient to challenge containment integrity.
I	Containment boundary is impaired (containment isolation function not complete)	• Isolation not complete. • Steam release detected outside containment. • High radiation detected outside containment. • A decrease in containment pressure in the absence of containment heat removal.
B	Containment bypassed (RCS isolation function not complete)	• High pressure or ruptured disk in the pressurized quench tank (for systems with relief valves on the low-pressure systems piped to the quench tank).

Designator	Damage Condition Descriptors	Possible Symptoms[Note1]
		• High humidity detected in the secondary containment/auxiliary building. • High temperatures detected in the secondary containment/auxiliary building. • High radiation detected outside containment. • For PWRs, high RCS pressure (near nominal operating condition) and condition BD. • Water accumulation[Note2] detected in the secondary containment/auxiliary building. • Activation of fire suppression system or isolation dampers in secondary containment/auxiliary building. • High radiation detected in the standby gas treatment system. • High radiation detected in the steam generators.

Notes for Table 4:

1. This is a list of possible symptoms, some of which might have occurred in advance of core damage. Nonetheless, when combined with other symptoms, these are indicators of the accident condition. Also, some of these symptoms might not apply to some accident conditions, and some might not be observable due to sequence specific conditions.
2. The ability to determine the water level in various containment compartments is likely accident sequence and plant specific.

To help the development of the SAMG supporting tool for demonstration purposes (subject to the NARSIS project) the examples for core and containment status trees [EPRI,93b] are used. These status trees were developed from core and containment severe accident phenomena identified in [EPRI,12a]. They provide the general insights into types and representative values of information that might be used the SAMG supporting tool to determine plant status. It should be noted that MCR/TSC staff does not have instrumentation which measures all parameters which can be obtain from detailed severe accident analyses by the tools such as MAAP or MELCOR (e.g. fuel cladding and fuel centerline temperatures are not measured, hydrogen production in the core is not measured, etc.). These information sources are used to characterize the types of information and general ranges of parameters that most likely would be used for severe accident management purposes. The general idea is to merge the possible core and containment damage descriptors (Table 3 and Table 4) with available plant measurements and indications. Figure 15 and Figure 16 present the Core Damage Conditions Status Tree and Containment Condition Status Tree modified for supporting tool usage.

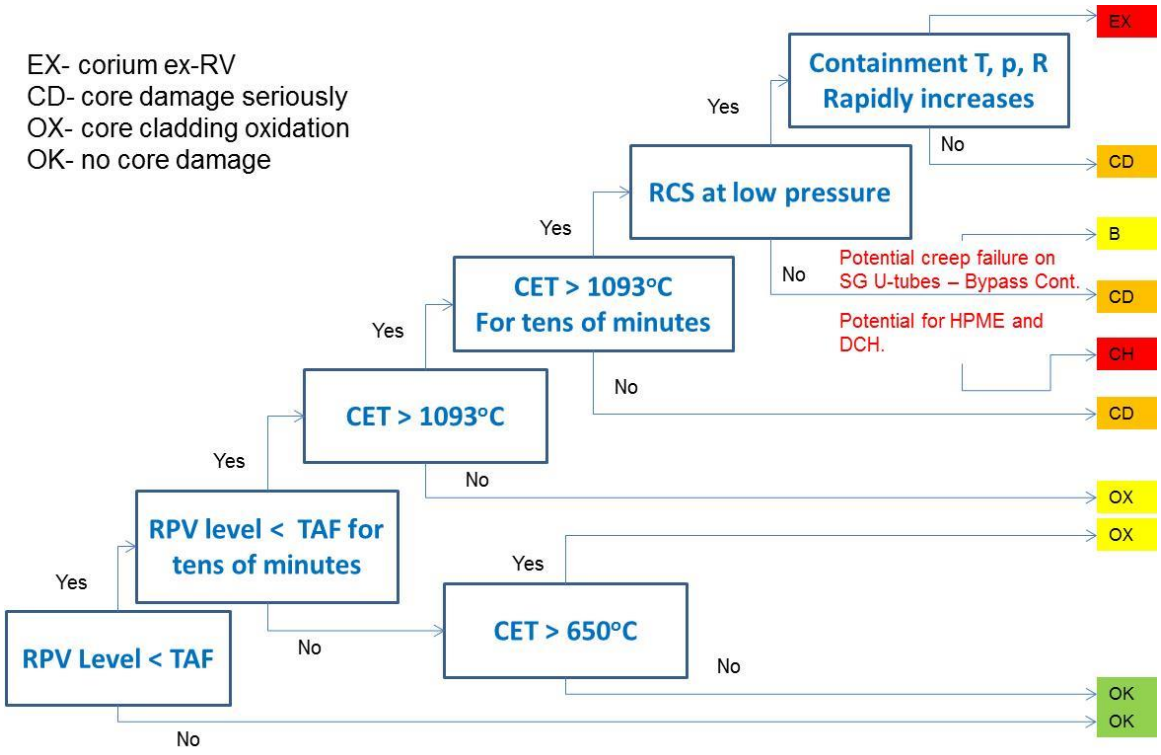

Figure 15: Core Damage Conditions Status Tree (example)

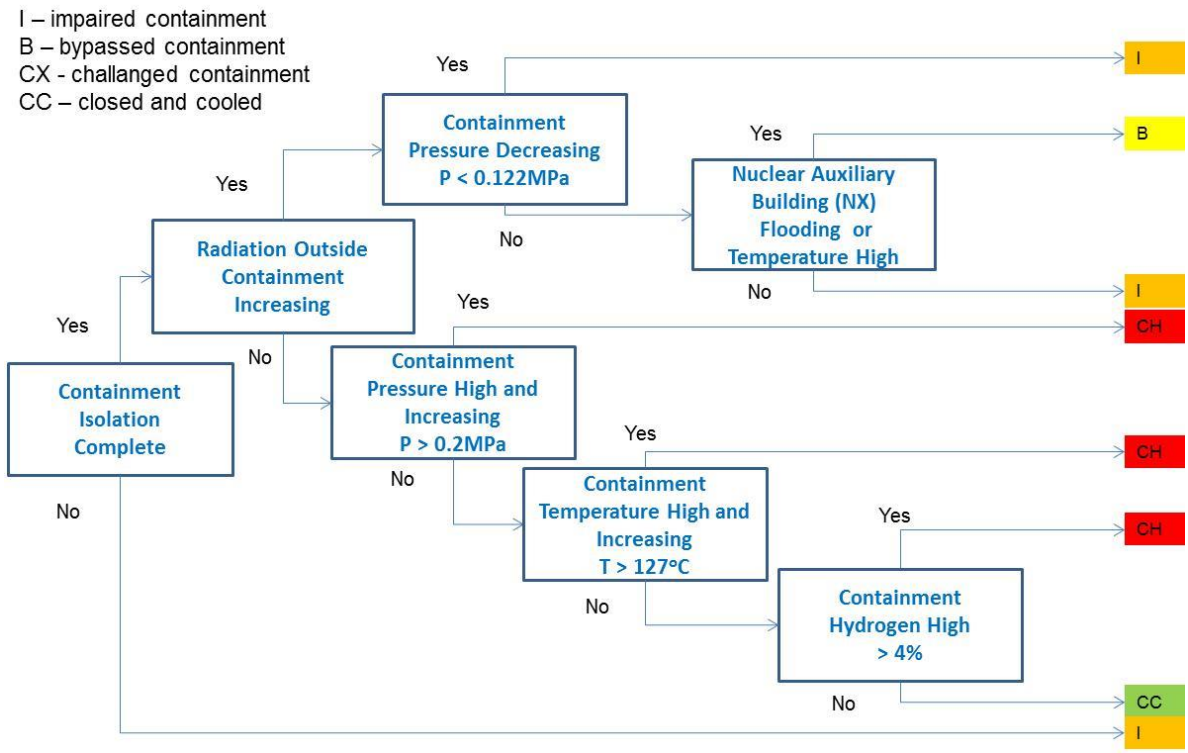

Figure 16: Containment Condition Status Tree (example)

Combining the assessment of plant damage states as described by Table 3, Table 4 and illustrated by Figure 15 and Figure 16, the severe accident progression (without assumed efficient operator actions) can be simplified for discretization of plant status in the future SAMG supporting tool.

Table 6 summarizes reactor core, RCS and containment states. Codes used in Table 6 have the following meaning:

BAF – Bottom of Active Fuel;

CET – Core Exit Thermocouples;

CH – Containment Challenge;

DCH – Direct Containment Heating;

HPME – High Pressure Melt Ejection;

MCCI – Molten Core Concrete Interaction;

Pcont – containment pressure;

Prcs - RCS pressure;

RPVL – Reactor Pressure Vessel Level;

TAF – Top of Active Fuel;

Tcont – Containment Temperature.

Table 5: Summary of Reactor Core, RCS and Containment States

CORE DAMAGE STATES

State	Condition	Accident Progression without operator action
OX (cladding oxidation)	CET > 650degC for 10 minutes RPVL < TAF	CD CH (hydrogen burn)
CD (Core Damage)	CET > 1093degC for tens of minutes RPVL < TAF	RPV melt-through (CH depend on RCS pressure) CH (hydrogen burn)
OK	CET < 354degC, quenched, cooled	

RCS STATES

State	Condition	Accident Progression without operator action
Intact: Pressurized	CET > 650degC for 10minutes OR 1093degC Prcs > 15.7MPa	RCS sudden depressurization: • SG U-tubes creep Failure (containment bypassed B) • HL creep failure (CH for containment) • RPV failure with HPME (CH – DCH, pressure, temperature, hydrogen)
Intact/Failed: Depressurized	CET > 650degC for 10minutes OR 1093degC Prcs < 0.3MPa RPVL < BAF	RPV melt-through (CH – hydrogen burn, MCCI)
OK	CET < 354degC, quenched, cooled	

CONTAINMENT STATES

State	Condition	Accident Progression without operator action
Intact	Pcont > 0.2MPa, not-cooled Design Basis Leakage	CH Environmental impact
Bypassed	Pcont <0.2MPa Design Basis Leakage or more	Environment Impact
CH (Containment Challenge)	0.6 MPa > Pcont >0.3MPa Tcont > 127degC Hydrogen >4% and Pcont < 0.15MPa	Containment Failure • Overpressure • Over temperature • DCH (steam explosion potential) • MCCI (potential containment basement melt-through) Environment Impact
OK	Pcont < 0.3MPa, cooled Hydrogen < 4% Design Basis Leakage	

3.4 SAMG Strategies and Decision Making Process

The term "strategy" is often used without explicitly being defined, and therefore it has slightly different connotations for different organizations throughout the nuclear industry that are involved in severe accident management. Generally, a strategy is a method that can be used to recover from or mitigate a specific challenge during a core damage accident. For the SAMG development, the term strategy was further refined to include three elements:

- An action (or set of actions) to be taken (plant specific Candidate High Level Actions (CHLAs) referred to generic from [EPRI,12a] and [IAEA,19]),
- A challenge that is to be mitigated ([EPRI,12a] and [EPRI,12b]), and
- Equipment that will be used (plant specific).

Many different types of accident event sequences can progress to severe core damage. The aim of the SAMGs ([IAEA,04], [EPRI,12a]) is not to identify specific strategies to mitigate each event sequence. The goal of plant specific SAMGs is to identify a limited set of strategies that are capable of mitigating a severe accident, independent of the specific event sequence. These strategies are intended to minimize the degree to which severe-accident phenomena can jeopardize the integrity of various fission product barriers. These barriers are the fuel, reactor, or containment structures that serve to limit the potential for offsite radiological releases. To preserve these barriers, the following objectives should be achieved:

- Remove heat from the overheated fuel debris to stop further fuel degradation, thereby protecting reactor and containment structures in contact with the debris;
- Control the atmospheric conditions in containment to prevent or limit the extent of challenge to the integrity of the containment;
- Minimize the release of fission products into the primary and secondary containment atmospheres, as well as to the environment.

For conditions leading to a severe-accident state, most or all of the safety systems considered in the EOPs would be lost for a sufficient time to uncover the core and result in the overheating of the fuel and cladding sufficient to cause extensive cladding oxidation.

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

- Design basis SSCs (addressed in 2.5.3 as equipment to implement the function, which is considered adequate and is available now or in near future),
- Alternate SSCs (addressed in 2.5.3 as equipment to implement the function which is considered adequate, but is not available immediately. Assessor considers that it will be available in less than 2 hours), and
- Mobile (or sometimes called “FLEX”) (addressed in 2.5.3 as equipment is to be available in less than 2 hours, but it may or may not be really adequate (e.g. 50% confidence)).

In accordance with [IAEA,04] and [EPRI,12a], the following is a list of generic CHLAs, as used in PWR SAMGs:

- Control RCS/core conditions:
  a. Injection to the RCS,
  b. Injection into (feed) SGs,
  c. Depressurization of the SGs,

d. Depressurization of the RCS,

e. Depressurize the SGs.

- Control Containment conditions:
  a. Flooding of the reactor cavity (injection into containment),
  b. Spray into the containment,
  c. Operate fan coolers,
  e. Operate hydrogen recombiners,
  f. Inert the containment with non-condensables,
  g. Vent the containment

For each of CHLA the reference [EPRI,12a] discusses the potential effects of performed actions depending of damage conditions. Table 6 illustrates potential positive and negative effects of SAMG action inject to RCS depending to damage condition. The abbreviations (damage conditions) are the same ones which were used in Figure 15, Figure 16, and Table 5**Erreur ! Source du renvoi introuvable.** above.

Table 6: Example of CHLA inject into RCS effects and consideration

Damage Condition	Effects of the performed CHLA
OX	a. Water added at rates much greater than values from Computational Aid CA-1 would rapidly quench the overheated core material, producing steam in the process. b. Water added at rates of approximately CA-1 flow would cool the intact fuel rods and terminate the accident progression. Some additional hydrogen would be generated if hot, unreacting cladding was available and embrittled fuel pin clad and fuel pellets could be shattered causing a transition to RCS damage condition BD. c. Water added at flow rates below CA-1 would likely stop the accident progression but would take a long time to recover the core. Essentially all of the flow rates would be vaporized, and embrittled cladding and fuel pellets could shatter. Substantial hydrogen is likely to be produced, and this could result in a progression to RCS damage condition BD before the accident progression would be terminated. d. Water addition rates much less than CA-1 would increase the hydrogen generation rate, thereby increasing the rate of accident progression to RCS damage condition BD. e. In the absence of sufficient control material or adequately borated water in regions of the core, there is the potential for an arrangement of fuel in the reactor to become critical after the injection of cold water. Etc.
BD	Items *a* to *e* similar as for OX, above. Accumulation of RCS injection water in the containment sufficient to submerge the RPV lower head would prevent high temperatures through the part of the reactor vessel wall that is submerged in water. This could delay or prevent failure of the vessel wall and would remove 25% or more of the decay heat for the core debris accumulated in the lower. Deeper submergence of the vessel could remove more of the decay heat. At submergence depths approaching the top of the core, all the decay heat could be removed through the RPV walls.
EX	Any water injected into the RCS/RPV and lost through the failed vessel would help cool debris in containment and limit the containment gas temperatures. Whether the debris would be quenched would depend on the water flow rate and the configuration (geometry) of the debris.

In the process of preparation of the plant specific SAMG, all generic CHLA [EPRI,12a] were assessed and grouped in associated SAMGs. The [NARS,18b] describes the proposed SAMGs guidelines applicable to selected sequences necessary for developing and testing the SAMG decision making tool. Evaluation of potentially positive and negative effects for each SAMG strategy in [NARS,18b] is conservatively given based on certain plant indication but without direct consideration of damage conditions.

Figure 17 illustrates the whole implementation of generic PWROG SAMG package to the reference plant as described in [NARS,18b]. It should be noted that some SAGs (e.g. SAG-7) and Computational Aids (e.g. CA-3 and 7) are removed from PWROG generic package due to implementation of passive hydrogen recombiners (Passive Hydrogen Recombines) in referenced plant.

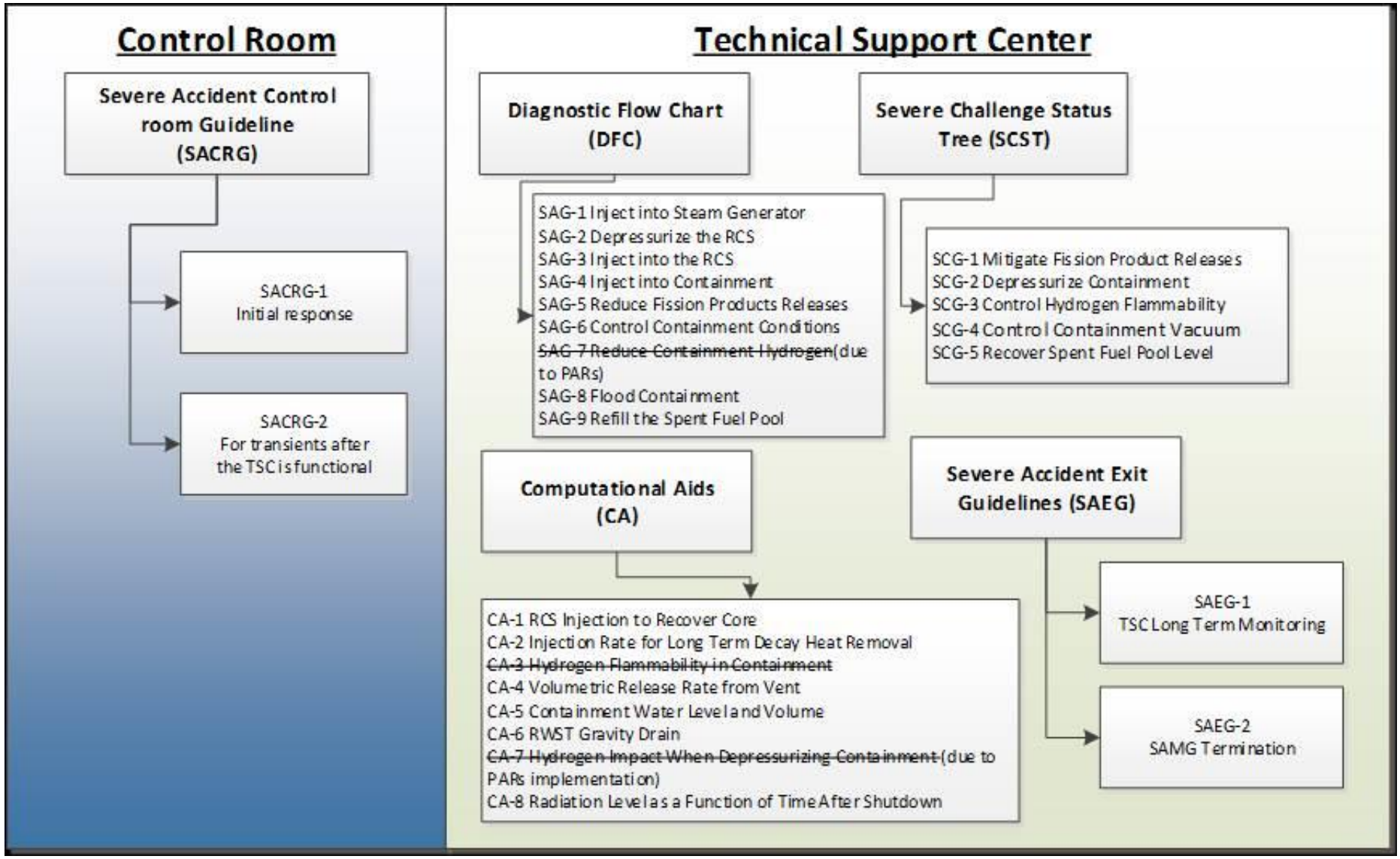

Figure 17: SAMG Package

After entering the SAMGs, TSC team monitors the DFC (diagnostic flow chart) and SCST(severe challenge status tree):

- DFC provides a method for the TSC to diagnose the plant conditions during a severe accident and to select the appropriate Severe Accident Guidelines (SAGs) for implementation.

  NOTE:

  Table 7**Erreur ! Source du renvoi introuvable.** summarizes the monitored plant parameters which will be used for demonstration of SAMG decision making process. Severity is assumed based on the potential Plant Damage States and DFC set points for selection of appropriate SAG based on Figure 2 [NARS,18b]. Successfully implementation of strategies from particular SAG should decrease severity and change the color of the monitored parameters.

- SCST provides a method for the TSC to diagnose the severe challenges to the containment fission product boundaries during a severe accident and to select the appropriate Severe Challenge Guidelines (SCG) for implementation.

Table 7: Monitored Plant Parameters used for demonstration of SAMG decision making process

Monitored Parameters		**Range**	**Severity based on potential Plant Damage States**			
Abbreviation	**Description**		**RED**[Note 3]	**ORANGE**	**YELLOW**	**GREEN**
SGL	SG level (1 and 2)	0 to 100%		0% < SGL < 70% **Enter SAG-1**	> 50% after SAG-1 implementation	> 70%
Prcs	Reactor Coolant System Pressure (gauge)	0 to 21 MPa		> 3.5MPa **Enter SAG-2**	2 MPa < Prcs < 3.5MPa	1.14 MPa < Prcs < 2MPa
CET	Core Exit Thermocouple	0 to 1260degC		> 650degC **Enter DFC/SCST and SAG-3**	354degC < CET< 650degC, decreases after SAG-3 implemented	CET < 354degC
RPVL[Note 2]	Reactor Pressure Vessel Level	0 to 120%		0%	0% < RPVL < 100%	> 100%
Pcont	Containment Pressure (gauge)	0MPa to 0.6MPa	> 0.4MPa	> 0.03MPa **Enter SAG-6**[Note 1]	<0.3MPa after application strategies from SAG-6	0 MPa < Pcont < 0.03MPa
Tcont[Note 2]	Containment Temperature	0 to 120degC	> 127 degC	127degC> Tcont >90degC	90degC> Tcont >50degC	< 50degC
Lcont	Containment Water Level	0 to 6m		< 3.9m **Enter SAG-4**	4m< Lcont < 6m **Enter SAG-8**[Note 1]	> 4m
H2[Note 2]	Hydrogen	0 to 10%	> 4% and Pcont< 0.15MPa(gauge)	< 4 %	4% > H2 >3%	< 3%

Notes:

1) SAG-5, SAG-6 and SAG-8 are not in scope of SAMG decision making demonstration;
2) Measurements not monitored by DCF or SCST but used for internal determination of plant damage state in SAMG decision making demonstration;
3) RED conditions are reserved for SCGs (already prioritized and out of the project scope);

Severe Accident Guideline (SAG)

As it is mentioned above, each of the parameters in the DFC provided in Figure 2 in [NARS,18b] specifies one Severe Accident Guideline (SAG) to be used when the parameter setpoint is exceeded. The SAGs are used to:

a. determine the availability of equipment to perform the strategies in the guideline (Figure 19 illustrates the equipment determination process on SAG-1 example (inject to SGs)).

b. determine the positive and negative impacts associated with implementation of each of the available strategies (illustrated in Table 6 and details given in [NARS,18b] for SAGs particularly subjected by NARSIS project),

c. determine the limitations dictated by plant conditions associated with implementation of a strategy,

d. determine the impact of not implementing any of the strategies (simplified summary presented on Table 6**Erreur ! Source du renvoi introuvable.**),

e. determine the short term and long term plant response after strategy implementation, and

f. determine if an implemented strategy should be stopped due to excessive negative impacts (in other words if relevant monitored parameters change colors as suggested by Table 7**Erreur ! Source du renvoi introuvable.**).

The use of the SAMG requires that certain information be available as the basis for decision making. For the TSC guidance, it has been assumed that the plant instrumentation will be available. However, any information that is used as the basis for taking actions during a severe accident should be verified by an alternate information source if available. A table of primary and alternate instrumentation for each of the key decision parameters is provided in Table 2 of [NARS,18b].

Although TSC evaluations of the different aspects of the strategies in particular SAG may proceed in parallel, the order for decision making purposes should be that specified in the guideline. The guideline steps specify when and how the guideline is exited. The guideline may be exited prior to the DFC parameter changing status with respect to the DFC setpoint for that parameter. For example if RCS depressurization is initiated from SAG-2, SAG-2 may be exited prior to the RCS pressure reaching the DFC setpoint.

When the TSC is referred to another guideline (SAG) to evaluate the benefits and negative impacts of implementing a set of actions, work in the present guideline should stop until the evaluation in the new guideline is completed. At that point, the exit from the second guideline would send the TSC back to the original guideline and the evaluations in that guideline would then be completed. Since the SAMG are guidelines and strict compliance with each guideline step is not required, it is especially important to evaluate negative impacts before reaching a decision on the implementation of a strategy. The evaluation of negative impacts in SAMG space should be considered a "good practice". Each of the SAGs has an exit which directs the user to either the DFC or the guideline and step in effect, as appropriate. Just prior to exiting particular SAG, the TSC is instructed to refer to the "long term concerns" attachment to that guideline. Here, the TSC would determine the long term concerns that are applicable to the strategy implemented from the SAG and attach the worksheet to the SAEG-1 guideline.

Severe Challenge Guidelines (SCGs)

Based on the rule of usage, the SCGs are similar to the SAGs except that the evaluation of the positive and negative impacts of implementing strategies is not done in the SCGs. The negative impact of not implementing a strategy, assuming the equipment is available, would

be loss of a containment fission product boundary; **this dictates that a strategy must be implemented.** Although TSC evaluations of the different aspects of the strategies in the SCGs may proceed in parallel, the order for decision making purposes should be that specified in the SCST.

Taking into account that SCGs are already prioritized our focus for development off SAMG Decision Making Tools are usage of DFC and corresponding SAGs because SAGs strategies can be assessed in parallel. Taking into account relative short time for assessment of strategies in SAGs (negative and positive effect) in comparison with analytical uncertainties of executed strategies success, this area is interesting for further research. Figure 18 illustrates the framework and context for the SAMG decision making.

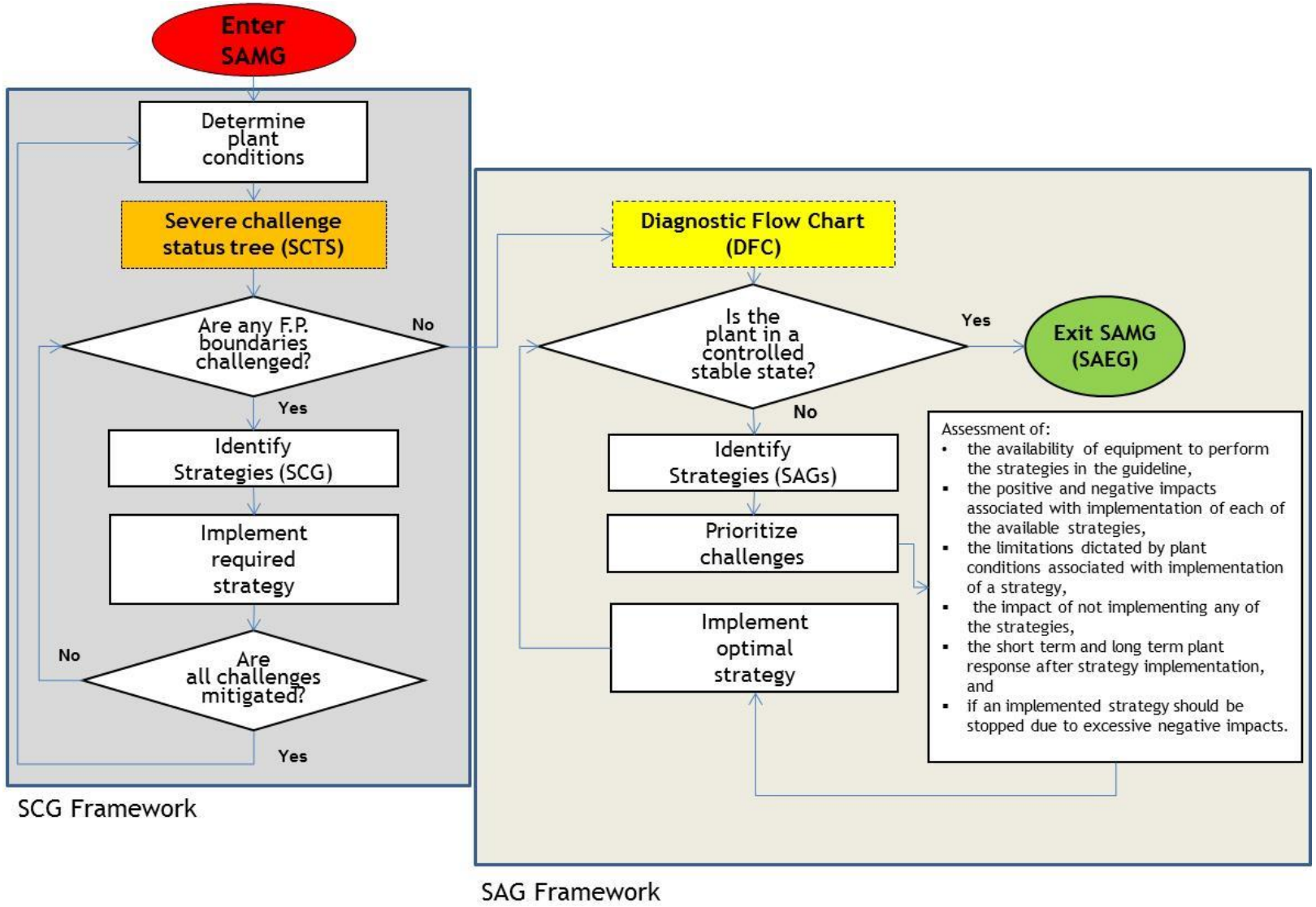

Figure 18: SAMG Decision Making Process

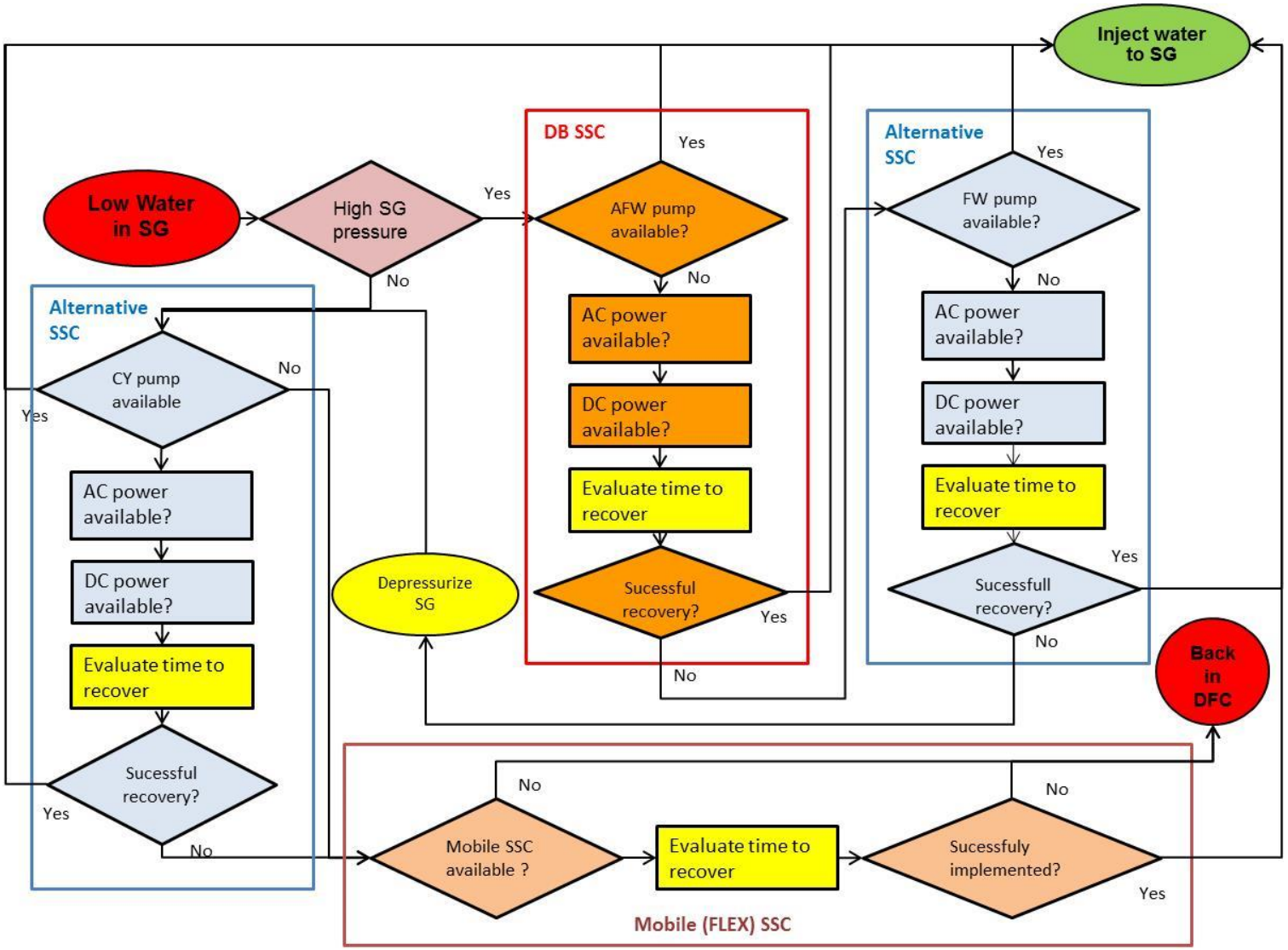

Figure 19: Determination the availability of equipment to perform the strategies in the guideline SAG-1 (Inject to SGs)

The report [NARS,18b] provides the detailed description and major steps of representative SAMG Diagnostic Flowchart (DFC) and the major four SAGs used for demonstration of SAMG diagnostic through two chosen scenarios (severe accident scenario with high RCS pressure at RPV failure and severe accident scenario with low RCS pressure at RPV failure).

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

4 Attributes for Use in Decision-Making

The attributes presenting quantitative risk for comparing different alternatives will be the likelihood of containment failure and time frame at which the failure is expected to occur. They will be expressed through the four categories of radioactivity release which were included in Figure 6:

RC-E: Containment failure with significant release of radioactivity is expected within several hours.

RC-I: Significant release of radioactivity (containment failure) is not expected within several hours. However, it can be expected to start within several days.

RC-L: Significant release of radioactivity (containment failure) is not expected within several days.

RC-N: Long term concern (in-vessel recovery and/or intact containment).

The process of quantification of particular alternative can be summarized in the following steps (referring to section 2.5.1 and Figure 6):

- Provide the answers to the plant status questions, i.e. assess the set of corresponding probabilities. This is done by the user and is provided as user's input into the tool. The remaining steps below are done by the tool.
- Calculate probabilities of hazard damage states (HDS);
- Map HDS probabilities into release category (RC) probabilities by means of HDS-RC matrix (incorporated into the tool);

Result of the quantification is obtained in the form of probabilities of four RCs discussed above. Form of the results is illustrated by Figure 20. It should be noted that the RC probabilities sum to 1.

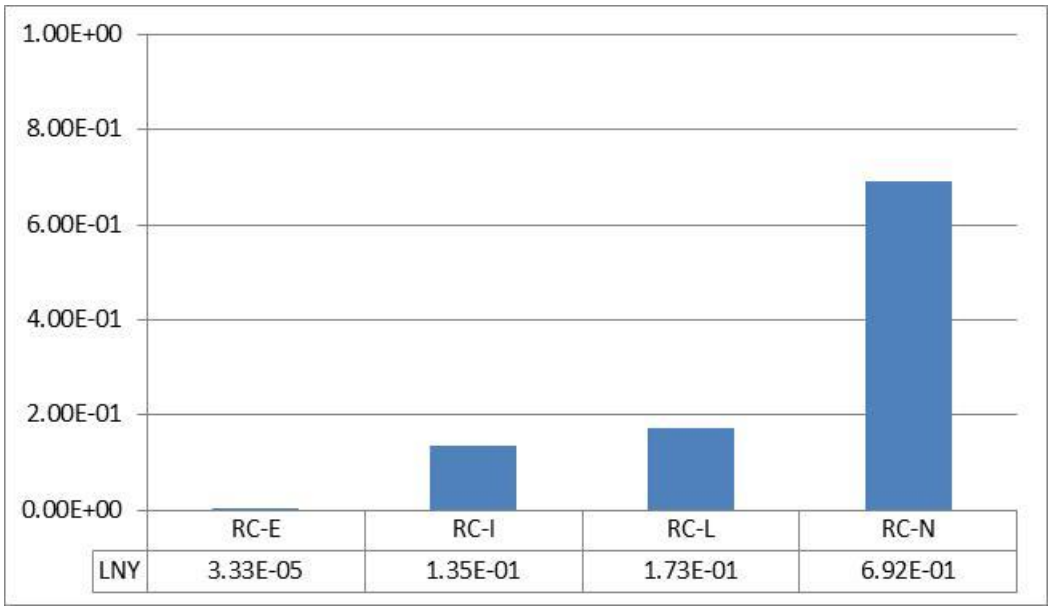

Figure 20: Form of the Results from Quantification of Particular Alternative

Comparison of alternatives is illustrated by a simple exercise shown in Figure 21. It is based on the example with Alternative #1 and Alternative #2 from section 2.5.1 above. (For description of the alternatives and corresponding inputs refer to the mentioned section.) The results shown were obtained by "tentatively" populated HDS-RC matrix and are given here for illustration purposes only.

It should be clear that, even if the form of the results is simple, interpretation of the results would require a due care and some background knowledge concerning the severe accidents and understanding of risk.

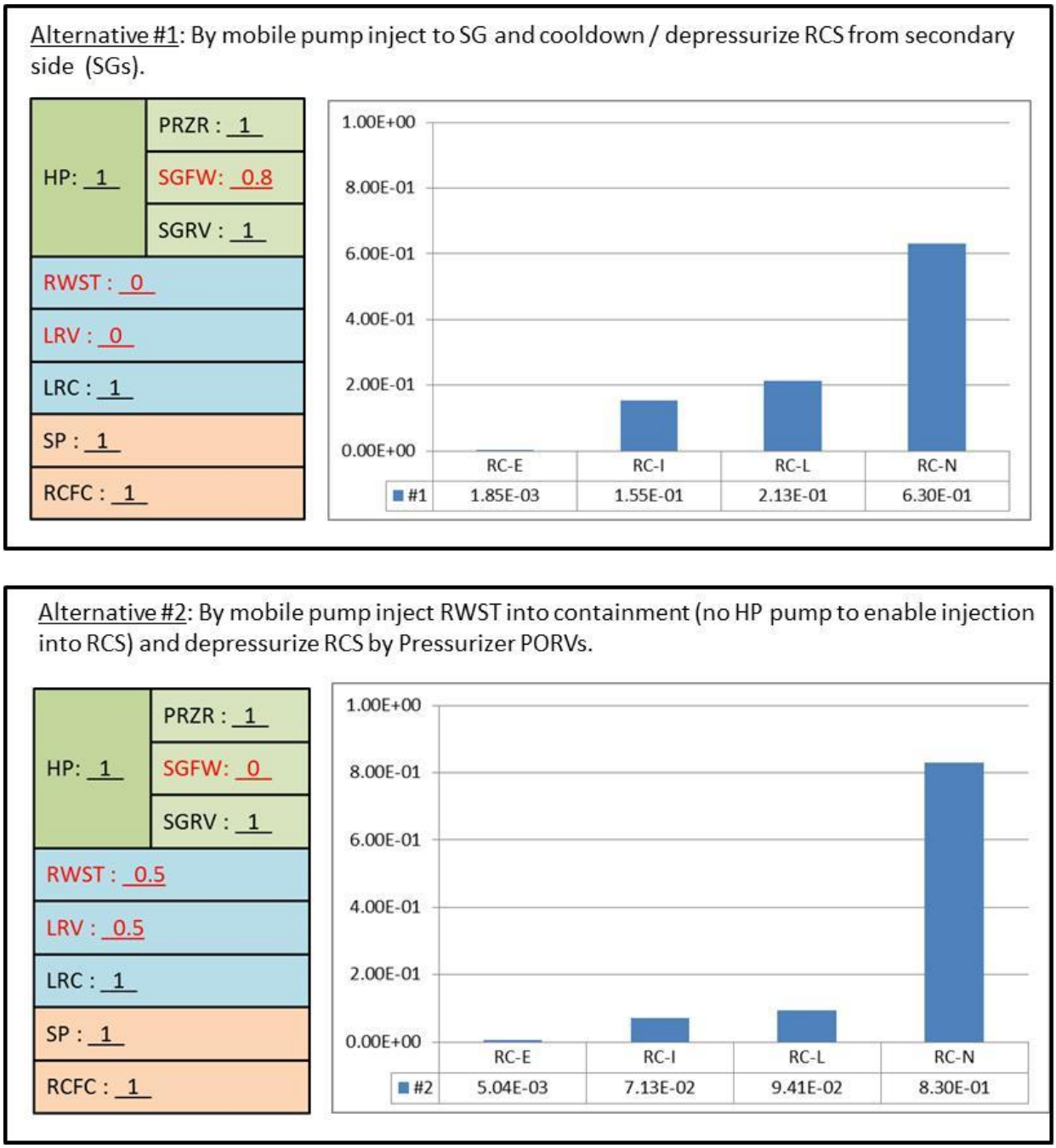

Figure 21: Illustration of Comparison of Two Alternatives

Thus, for example, at quick glance (without reading numbers), it may be concluded that Alternative #2 is better because the bulk of probability moves to no releases. The first point is that the explanation of these graphics is not obtainable without understanding severe accident progression incorporated into the logic model to be used by the tool. In this particular example the explanation can be summarized as follows:

- Alternative #1 is focused on injection to SGs in order to prevent SG tube creep rupture. It gives up establishing the reactor injection / recirculation before vessel failure (RWST = 0; LRV = 0). Therefore, it gives up the in-vessel recovery (IVR).
- Alternative #2, on the other hand, focuses on the reactor injection and gives up SG injection. It increases the IVR potential and that is why it increases the no-release probability.

However, the Alternative #2 also increases the potential for SG tube creep rupture and, thus, early releases. It should be noted that the probability of the RC-E category is almost three times higher than in the case of the Alternative #1. (However, the probabilities of RC-E are so small that their corresponding bars are not visible beside those for the remaining releases).

Apparently, some issues may be expected concerning how to compare (combine) the changes in probability of early release with changes in probability of late/no release. (Note: If the decision is based only on early release probability (like with many Level 2 PSAs) then the conclusion would be the opposite than the above: better is the Alternative #1. However, this kind of issue (comparing / combining low likelihood - high consequence with high likelihood - low consequence) is as old as any risk consideration or any decision-making. Further elaboration on this will be done under Task 5.4.

5 Concept for the Use of the Tool

This section briefly introduces a concept for the use of the tool, which will be further elaborated in the Task 5.4. It is shown by a simple diagram in Figure 22. Repeated use of the tool can be foreseen in intervals not shorter than 15 minutes or so (due to constraints in availability of new relevant information). Establishing the basis for and selecting the most proper interval will be done in the Task 5.4.

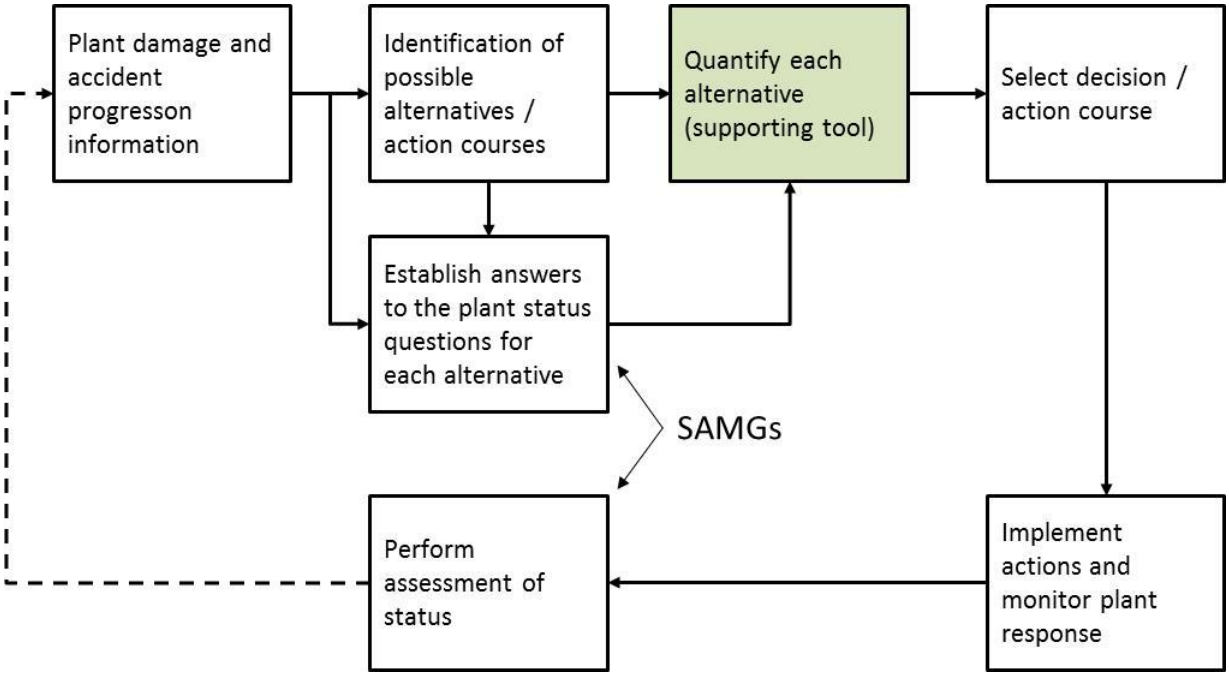

Figure 22: Conceptual Diagram for Use of the Tool

Sequence of main steps in such cyclical use of the tool can be summarized as:

- Monitor and assess plant status; this would include monitoring and assessment of relevant parameters (e.g. primary system or containment) as well as of the availability and performance of plant systems; for example, systems which were initially unavailable may have been repaired; alternative systems may have been established or mobile equipment brought to site etc.;
- Based on monitoring and assessment collect the information concerning the current status of plant damage and accident progression; e.g.: which barriers are challenged

or soon may be, which functions are not available; in principle, this is normally done through the use of the SAMGs, which is also indicated in Figure 22;

- Identify possible alternatives (action courses) based on this information; identified action courses should include the actions which are required by the SAMGs (e.g. in the case of severe challenges) and should consider the availability of plant systems / functions; (it may not be possible to implement certain actions because equipment needed is not available);
- For each identified alternative establish the answers to the set of plant status questions, i.e. establish the input for the tool for each alternative;
- Quantify each alternative by the tool and obtain the results discussed in the previous section;
- Compare the alternatives based on the results from the tool and select the option / alternative to proceed with; selection should consider the requirements from the SAMGs;
    - It should be recognized here that there may be situations when there is only one possible action course (i.e. no multiple alternatives). There may also be situations when SAMG requirements may be in conflict with preferences obtained by the tool (although this kind of issues should be resolved before the tool would be put in actual use).
- Implement the selected actions and observe plant's response;
- Monitor and assess plant status; etc.

6 Summary

The purpose of this report, developed under the Task 5.3, is to establish the hazard damage states and the logic model for accident progression, to be used as a basis for the accident management supporting tool for demonstration purposes.

The report provides background for hazard-induced damage states and for accident progression logic modeling by means of event trees and similar techniques such as sequence diagrams, based on the probabilistic safety analyses for the nuclear power plants. A set of hazard damage states for the purpose of development of demonstration-grade supporting tool was identified and defined. Main plant systems and functions related to hazard damage states which need to be reflected in the accident progression logic model were identified and described. Based on those, a set of plant status questions was established. Answers to those questions would provide a characterization for particular alternative, which would be provided as input to the tool for each considered alternative.

Accident progression logic model structure was established and described. It is based on event sequence diagrams (which is a technique similar to event trees) and would be used to quantify each considered alternative with regard to risk from containment failure.

The definitions of the hazard damage states as well as development of logic model for severe accident progression reflect the type of the plant design and the type of the emergency operating procedures (EOP), damage guidelines and SAMGs described in the reports developed under the Task 5.1 and Task 5.2, i.e. [NARS,18a] and [NARS,18b].

Types of decisions and actions in severe accident management have been identified and characterized, forming the basis for establishing the available alternatives for accident management.

The attributes for use in decision-making with regard to selecting among, making quantitative comparisons of the available alternatives, have been established. They present the likelihood

of containment failure and time frame at which the failure is expected to occur and they would be expressed through the major categories of radioactivity release. An example on comparison of two alternatives was provided and discussed. A general concept for the use of the supporting tool has been also described.

7 References

[ASME,13] ASME/ANS RA-Sb-2013, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addendum B, ASME/ANS, New York, 2013;

[ASME,14] ASME/ANS RA-S-1.2-2014, Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), ASME/ANS, 2014;

[IAEA,04] IAEA Safety Reports Series No. 32, Implementation of Accident Management Programmes in Nuclear Power Plants, 2004;

[IAEA,10a] IAEA Specific Safety Guide No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, 2010;

[IAEA,10b] IAEA Specific Safety Guide No. SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, Vienna, 2010

[IAEA,16] IAEA-TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA, Vienna, 2016

[IAEA,19] IAEA Draft Specific Safety Guide (DS483), Severe Accident Management Programmes for Nuclear power Plants, 2019;

[EPRI,12a] EPRI TR-1025295-V1, Severe Accident Management Guidance Technical Basis Report (TBR), Volume 1: Candidate High-Level Action and Their Effects, 2012;

[EPRI,12b] EPRI TR-1025295-V2, Severe Accident Management Guidance Technical Basis Report (TBR), Volume 2: The Physics of Accident Progression, 2012;

[EPRI,93a] EPRI TR-102371, Instrument Performance under Severe Accident Conditions, 1993;

[EPRI,93b] EPRI TR-103412, Assessment of Existing Plant Instrumentation for Severe Accident Management, 1993;

[NARS,17] European Commission Directorate-General Research and Innovation, Grant Agreement number: 755439 — NARSIS — NFRP-2016-2017/NFRP-2016-2017-1, ANNEX 1 (part A), Research and Innovation action

[NARS,18a] Characterization of the Referential NPP for Severe Accident Management Analyses, NARSIS Deliverable D5.1, 2018

[NARS,18b] Report on Characterized EOP/EDMG/SAMG, NARSIS Deliverable D5.2, 2018

[NUR,06] NUREG/CR-6906, Containment Integrity Research at Sandia National Labortories, U.S. NRC, 2006

[NRC,11] U.S. NRC Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis, Revision 2, U.S. NRC, 2011

[NRC,09] U.S. NRC Regulatory Guide 1.200, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, Revision 2, U.S. NRC, 2009