Mat-2.4108
Independent Research Project in Applied Mathematics

Reliability analysis for passive systems – A case study on a passive containment cooling system

Author: Taneli Silvonen
Date: 16.9.2011

Aalto University
School of Science
Department of Mathematics and Systems Analysis
Systems Analysis Laboratory

Table of Contents

List of abbreviations

BWR	Boiling water reactor
CET	Containment event tree
ECCS	Emergency core cooling system
ESBWR	Economic simplified boiling water reactor
FMEA	Failure modes and effects analysis
GDCS	Gravity driven cooling system
GE	General Electric
HEX	Heat exchanger
IAEA	International atomic energy agency
LOCA	Loss of coolant accident
NPP	Nuclear power plant
NRC	The U.S. Nuclear Regulatory Commission
OL1	Olkiluoto 1
PCCS	Passive containment cooling system
PSA	Probabilistic safety analysis
RMPS	Reliability methods for passive safety
RPV	Reactor pressure vessel
SBO	Station blackout
SBWR	Simplified boiling water reactor
T-H	Thermal-hydraulic
TVO	Teollisuuden Voima Oyj

1. Introduction

Passive safety systems in nuclear power plants do not need any external input to operate unlike active ones. Instead, they depend on natural phenomena like gravity. In future plant designs, passive systems are used increasingly because they are regarded more reliable and simpler than their active counterparts. It is also advantageous that the need for human interaction and external signals is reduced. Safety systems of a modern nuclear plant are implemented so that they combine both passive and active safety features.

The passive containment cooling system (PCCS) is investigated in more detail in this study. It is designed to provide steam suppression in the drywell in the event of loss of coolant accident (LOCA). PCCS relates generally to protection systems for shutting down a boiling water reactor (BWR) and maintaining it in a safe condition in the event of a system transient. PCCS is a passive system without power actuated valves or any other components that must actively function. It is a thermal-hydraulic (T-H) system, which contains moving working fluids and relies on natural circulation.

The reliability assessment of the PCCS, or any other passive thermal-hydraulic system, necessarily differs from classical component reliability based approach. The significant uncertainty related to thermal-hydraulic system operation is complicating reliability analysis. However, also methods which apply classical reliability assessment techniques have been developed. Many other techniques rely on computer programs, which simulate the thermal-hydraulic physical phenomena related to the system under investigation. When the failure criteria have been defined, it is possible to provide a reliability estimate for the passive safety system according to the simulations. The assessment may also be purely qualitative without giving any numerical values to evaluate the reliability.

MELCOR is software to model the progression of severe accidents in light water reactor nuclear power plants. It is being developed at Sandia National Laboratories for the U.S. Nuclear Regulatory Commission (NRC). In this study MELCOR is used to evaluate the performance of the PCCS in different conditions from the reliability point of view. MELCOR has its own condenser package which is used in this study. Also a self-implemented MELCOR model is experimented in order to validate the results obtained with the condenser package. The accident scenario the plant is exposed to is a station blackout (SBO), although a little different scenario is experimented as well. The MELCOR input file has originally been created for Olkiluoto 1 (OL1) BWR design in Finland. Because the PCCS is added to the input, the simulations cannot be considered plant-specific anymore, but hypothetical instead.

In section 2, the essential concepts in passive nuclear safety are dealt with. The categorization of passive safety systems is introduced and the uncertainties which complicate reliability assessment are examined. Also an overview on the methodologies for passive system reliability analysis discussed in literature is given. Section 3 concentrates on technical implementation of the PCCS and presents the factors which affect the performance of the system. In section 4 failure modes and effects analysis (FMEA) and fault tree analysis for PCCS are conducted, thus introducing a way to apply classical reliability methods to thermal-hydraulic passive system assessment. MELCOR simulation scenario and results for PCCS performance in different situations are discussed in section 5 along with the simulations' interface with reliability analysis.

2. Passive safety systems for nuclear power plants

In order to provide nuclear power plant (NPP) with safety, combinations of inherent/intrinsic safety characteristics and engineered safety systems, whose function may be active or passive, are used. If an inherent hazard can be eliminated through the design or material choices made for the nuclear plant, the plant is said to be inherently safe with respect to this eliminated hazard. Inherent hazards include e.g. fission products and their associated decay heat or high pressures. Inherent safety characteristic is not subject to failure of any kind and represents deterministic, not probabilistic, safety. When an inherent hazard has not been eliminated, engineered safety systems are provided. They generally aim to prevent potential accidents, but remain in principle subject to failure, although preferably with low probability.

The concepts of active and passive safety are used to describe the functioning of the engineered safety system, structure or component. These two terms are distinguished from each other by determining whether there exists any reliance on external mechanical or electrical power, signals or forces. Passive safety features are independent from such external factors and are instead reliant on natural laws, material properties and internally stored energy. This results in elimination of failures caused by human action or power failures. However, passive safety devices remain subject to failures due to mechanical or structural defects and they are not synonymous to absolute reliability

A safety system is basically composed of safety components, which are defined (by the IAEA) passive if they do not need any external input to operate [1]. If a component is not passive, it is necessarily an active one. This applies to whole safety systems as well: A passive system consists of passive components only, otherwise it is defined active. However, if a system uses active components in a very limited way, it can be labelled passive.

The concept of passivity can be considered in terms of several categories. Higher categories are at issue when all components in a safety system can be classified as passive. A system can have passive and active characteristics at different times. For example the active opening of a valve initiates subsequent passive operation by natural convection. There are four categories in total and they are characterized as follows [1]:

- Category A
  - No signal inputs, external power sources or forces.
  - No moving mechanical parts.
  - No moving working fluids
    - For example physical barriers against the release of fission products.
- Category B
  - No signal inputs, external power sources or forces.

  - No moving mechanical parts.
  - Moving working fluids, which are due to thermal-hydraulic (T-H) conditions occurring when the safety function is activated.
    - For example emergency cooling systems based on air or water natural circulation in heat exchangers (HEX) immersed in water pools.
- Category C
  - No signal inputs, external power sources or forces.
  - Moving mechanical parts, whether or not moving working fluids are also present. Mechanical movements are because of e.g. static pressure in valves.
    - For example check valves and spring-loaded relief valves.
- Category D
  - Intermediary zone between active and passive. Execution of the safety function is made through passive methods.
  - External signal is permitted to trigger the passive process.
  - "Passive execution/active initiation".
  - Energy only from stored sources.
  - Active components limited to controls, instruments and valves.
    - For example emergency core cooling systems based on gravity-driven flow of water, activated by valves which break open on demand.

Innovative reactor concepts make use of passive safety features to a large extent and they are combined with active safety systems. Advantages of passive systems are simplicity, reduction of the need of human interaction and reduction of external electric power, to name a few. Passive systems also have a higher reliability with respect to active ones, because the risk for hardware failure or human error is mitigated. The unavailability of a passive system is usually related to some physical phenomena or natural forces, such as gravity or natural convection. This is true especially for category B systems, which are also called thermal-hydraulic passive systems.

The T-H passive systems i.e. natural circulation systems pose probably the most relevant challenges regarding reliability assessment [2]. Hence a rather large portion of literature deals with these kinds of passive systems. T-H passive systems are under investigation also in this study which takes a closer look of the Passive Containment Cooling System (PCCS).

2.1. Uncertainties related to passive systems

There are challenges regarding passive systems. There can be a lack of data on some significant phenomena affecting the operation of a passive system. Also shortage of operating experience over wide range of conditions can be a problem and passive systems are also usually less effective than their active counterparts. These factors, among others, make reliability assessment of passive safety systems somewhat more complicated than assessment of active systems. The following discussion relates particularly to T-H systems.

It is useful to separate two kinds of uncertainties, which are called aleatory and epistemic uncertainties. The former one refers to events or phenomena which take place in a stochastic way, thus requiring probabilistic modelling. The latter one is linked to the knowledge possessed on the system and its behaviour and it is sometimes referred as state-of-knowledge uncertainty. The better the model is believed to represent the actual system, the smaller is epistemic uncertainty. Epistemic uncertainty can be further reduced by acquiring more information about the system. Both uncertainties mentioned above complicate the reliability analysis of a passive system.

Uncertainties, both of aleatory and epistemic kind, affecting T-H passive system operation have been identified in reference [3] and adopted here from [4]. The uncertainties can be summarized to include

- Aleatory uncertainties
  - Geometrical properties
  - Material properties
  - Initial/boundary conditions (design parameters)
- Epistemic uncertainties
  - T-H analysis
    - Model
    - Parameters
  - System failure analysis
    - Failure criteria and failure modes

Aleatory uncertainties concern the variability in geometrical and material properties e.g. undetected leakage in piping. Also the initial/boundary conditions of operation, such as pressure in reactor pressure vessel (RPV), can have some random or stochastic behaviour. Epistemic uncertainties arise from the lack of knowledge about e.g. natural circulation and this leads to ambiguity in model and its parameter values. The estimation of failure probabilities can be very sensitive to uncertainties in modelling and parameters, partly because some specific reactor parameter can be chosen to serve as a failure criterion.

2.2. Reliability assessment for a passive system

A number of methodologies have been developed in order to investigate the reliability of T-H passive systems. These include approaches based on independent failure modes, failure modes of passive system hardware components, functional failure, and the reliability methods for passive safety functions (RMPS) [4].

In the approach based on independent failure modes, the reliability is seen from the perspectives of system/component reliability and physical phenomena reliability. The first contribution calls for engineered passive components and it is treated in the classical way, i.e. in terms of failures of components. The latter is concerned with the way the natural physical phenomena operate. The failure probability is evaluated as the probability of occurrence of the different failure modes which are considered independent. Failure causes are seen in terms of critical parameters for the natural circulation performance or stability. Difficulties arise for example when identifying probability density functions for the states of important parameters.

Difficulties in independent failure modes approach can be overcome by associating each physical failure mode to a failure mode of a hardware component designed to ensure the conditions for successful system performance. Thus the probabilities of physical failures are reduced to unreliabilities of the components whose failures complicate the successful passive system operation. For example some problems in a heat transfer process can simply be seen as a failure of heat exchangers.

The functional failure approach exploits the concept of functional failure to define the probability of failing to carry out a given safety function. The idea is adopted from the resistance-stress ($R - S$) interference model from fracture mechanics. For T-H passive systems reliability assessment, R expresses safety functional requirement on a physical parameter and S expresses system state. R can be for example a minimum required value for water mass flow, whereas S could represent the actual value of mass flow. Probability distributions are assigned to both R and S and failure probability is computed as the probability that S is greater than R. Hence the states of the system are divided into the failed and the safe states. Some further discussion can be seen in [4].

The reliability methods for passive safety (RMPS) functions is a research and development framework programme supported by the European Union. The RMPS functions addresses issues such as

- Definition of failure criteria of the passive system.
- Identification and quantification of the sources of uncertainty and determination of the most important ones.
- Propagation of the uncertainties through T-H modelling.
- Evaluation of the passive system unreliability.

The RMPS methodology consists of several steps which are shown in Figure 1. It starts with the identification and characterization of the accident scenario and ends up with the reliability evaluation of the system in question. Further reading and information on the RMPS topic is available for example in references [4], [5] and [6].

The reliance of passive systems on inherent physical principles makes the reliability assessment quite difficult to accomplish in comparison to classical system reliability analysis. The current knowledge of passive reliability contains large uncertainties, especially in the area of thermal-hydraulics. The assessment of reliability of the passive T-H systems is a crucial issue because they are increasingly used in future NPPs. By developing solid methods to beat uncertainties relating to reliability assessment of T-H passive systems, also the public acceptance for future reactor systems may increase.

It is essential to be aware of the fundamental differences between the analysis of passive and active safety systems. Reliability assessment for an active system can even be regarded as a somewhat mechanical and straightforward procedure whereas issues relating passive systems are of higher complexity containing more uncertainties. In active systems the number of components is usually higher than in their passive counterparts, and in active systems dependencies within the system can be considered mainly functional, whilst passive systems rely on physical or phenomenal principles and are more difficult to model.

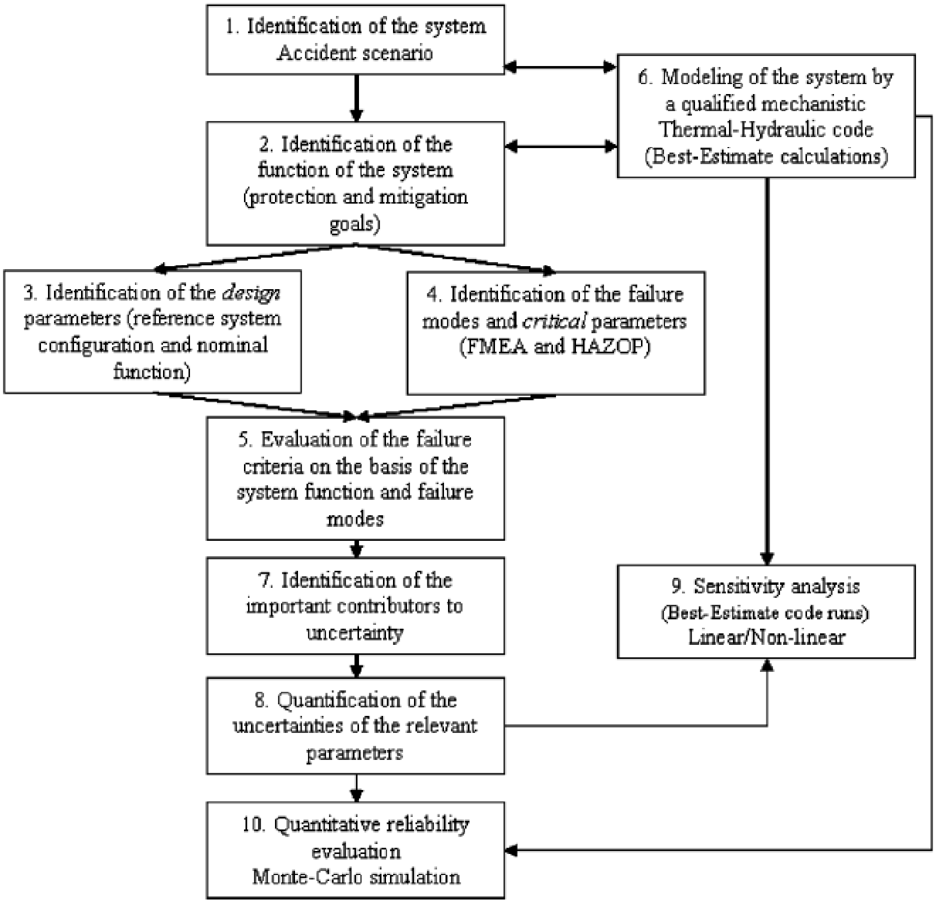

Figure 1: The Reliability Methods for Passive Safety (RMPS) methodology roadmap [5].

For active systems it is often easy to identify the failure modes, which are typically discrete and few in number. The system either works or does not work. For passive systems the measures which determine failure states can be continuous instead, and the failure criterion can be defined to be e.g. some percentage value of the performance in nominal conditions. Also there is normally more information and reliability data available on active systems. Knowledge of passive systems rely more on expert judgements and simulations.

3. Passive Containment Cooling System

Passive containment cooling system (PCCS) is a passive engineered safety feature first utilized in simplified boiling water reactors (SBWR), by General Electric (GE), to provide steam suppression in the drywell in the event of loss of coolant accident (LOCA). SBWRs have been designed with passive safety features in order to provide more resistance to human error. PCCS relates generally to protection systems for shutting down a boiling water reactor (BWR) and maintaining it in a safe condition in the event of a system transient. In particular, PCCS relates to emergency core cooling systems (ECCS) for supplying water to the reactor core and containment systems in the event of a LOCA. [7]

GE's latest evolution of BWR technology is the economic boiling water reactor (ESBWR), which is built on innovations developed for the company's earlier reactor types. The ESBWR design relies on natural circulation and passive safety functions, which enhance plant performance and simplify the design. Natural circulation enables the elimination of several systems, including recirculation pumps, safety system pumps and safety diesel generators. Passive safety systems make safety-grade pumps and AC power needless. The passive safety systems of the ESBWR are shown in Figure 2. The ESBWR utilizes PCCS, which is implemented in six independent loops, each containing a heat exchanger (HEX). Thus the requirement of redundancy in safety systems is fulfilled. In this study, PCCS is considered in the light of the ESBWR design. [8]

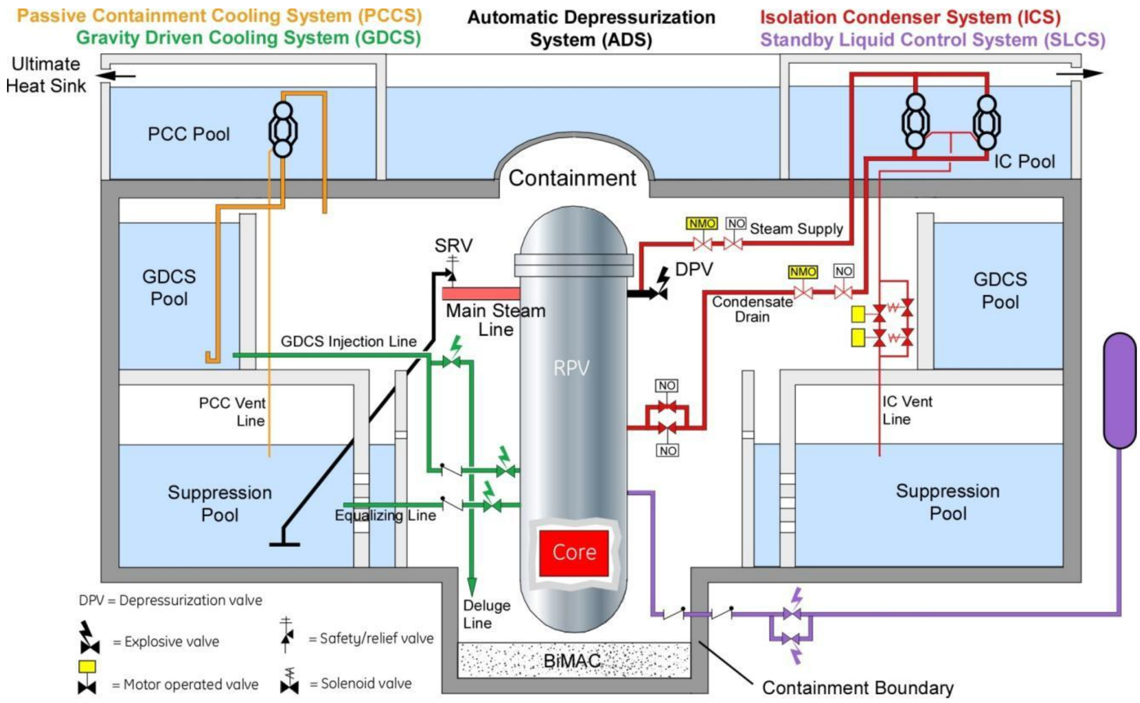

Figure 2: The passive safety systems of the ESBWR. [9]

The PCCS removes the core decay heat rejected to the containment after a LOCA and provides containment cooling for a minimum of 72 hours post-LOCA. It is a passive system without power actuated valves or any other components that must actively function. The absence of valves of any kind also implies that the system should always be available. Each PCCS condenser is designed for 11 MW_t nominal heat transfer capacity and they are located in a large pool positioned above, and outside, the ESBWR containment. HEXs condense steam and transfer heat in the pool, which is vented to atmosphere.

The PCCS operates by natural circulation and its operation is initiated by the difference in pressure between the drywell and the wetwell. The PCCS condenser receives a steam-gas mixture supply directly from the drywell. In HEXs the gases are cooled and some or all of the steam vapour is condensed. The condensed steam is drained to the gravity driven cooling system (GDCS) pool and the noncondensible gases are vented through the vent line, which is submerged in the pressure suppression pool. The vent line functions whenever the drywell-wetwell pressure differential is sufficient to clear the water from the vent line terminus within the pressure suppression pool. A schematic picture of the PCCS is shown in Figure 3. [10]

3.1. General PCCS performance and implementation in MELCOR

The PCCS model in MELCOR has some basic attributes affecting heat transfer capacity in order to properly describe the system at issue. A change in current conditions causes variation in PCCS performance and this is taken into account in the model. Tabular inputs are required in the MELCOR input file for determining the effects of changes in conditions to PCCS performance. Tables for performance variation shown in this section have been used in example calculations in [11] and they are adopted here as well, as they seem feasible.

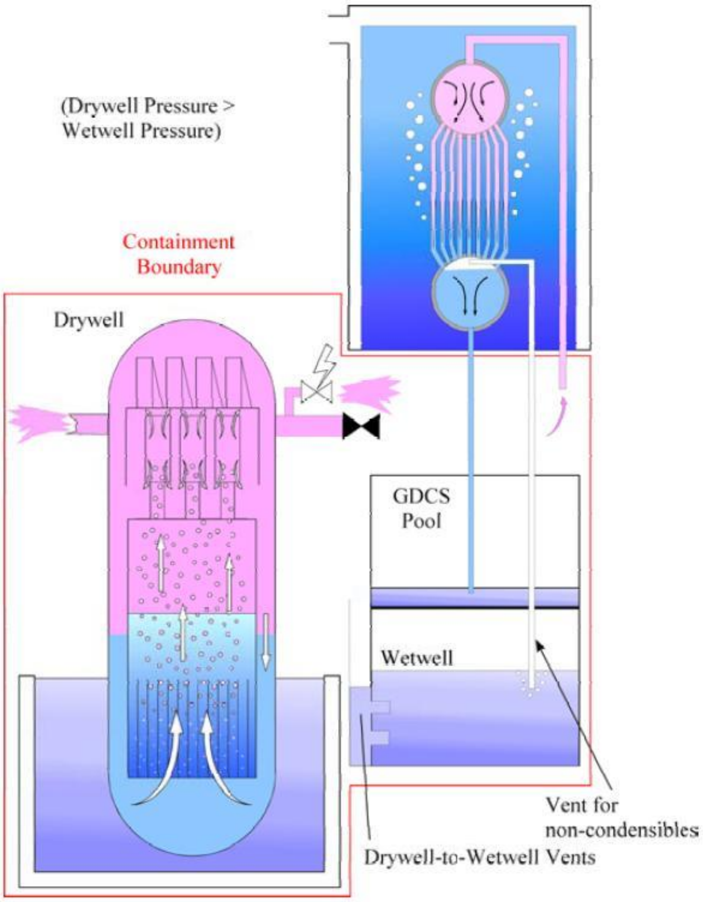

Figure 3: A schematic picture of the passive containment cooling system for ESBWR. [9]

The capacity is limited to gravity drainage of steam condensing in the tubes until drywell pressure exceeds suppression chamber pressure by a margin sufficient to overcome PCCS vent line submergence. Capacity increases as the drywell-to-suppression pool pressure differential increases, according to Table 1. The drywell-to-wetwell differential pressure affects the heat exchanger performance because it determines velocity within the heat exchanger tubes. The velocity, in turn, affects the heat transfer coefficient at the inner surface of the tubes.

Table 1: Variation in PCCS performance due to pressure difference between the drywell and the wetwell. [11]

Differential Pressure [Pa]	Variation factor
0.0	1.000
7239.5	1.000
8618.5	1.072
10342.1	1.153
12065.8	1.227
13789.5	1.294
15423.6	1.353

The capacity decreases when the partial pressure of noncondensible gases increase in the upper drywell because they interfere heat transfer within the PCCS tubes. When the pressure differential between drywell and wetwell is not sufficient to maintain vent line flow, the PCCS HEX-condenser fills with noncondensible gases. The condensing steam is replaced with a mixture of steam and noncondensible gases from drywell, which is the source volume for the PCCS. The PCCS is said to be "bound", when it contains only cool noncondensible gas. In that case, no heat exchange or condensing operation exists, as can be read from Table 2. Noncondensible gas mole fraction has the most substantial effect on the performance compared to other factors.

Table 2: Variation in PCCS performance due to noncondensible gas fraction in the drywell. [11]

Noncondensible gas mole fraction	Variation factor
1.00	0.00
0.10	0.60
0.05	0.82
0.02	0.90
0.01	0.96
0.00	1.00

Also the drywell pressure alone affects the capacity of the PCCS. The effects are shown in Table 3. A pressure drop in the drywell results in a drop of temperature of steam and its condensate. Thereby heat transfer between the condenser wall and the steam lowers. The base operating condition for the PCCS is at 0.3 MPa with a variation factor 1.0. The heat transfer is determined with help of a heat transfer coefficient for condensing steam.

Changes in the PCCS pool temperature are assumed to have no effect upon the PCCS system performance, because the pool is sufficiently large. The detailed description of the MELCOR PCCS model operation with required steps and algorithms is given in [11].

In MELCOR, the PCCS input requires definition of volumes that represent the heat sink for the heat exchangers (PCCS pool), the volume from which material is removed (drywell), the volume containing the vent (wetwell), and the volume containing the drain (GDCS pool). The data for the variation in capacity, discussed above, is required in tabular functions. Also a geometric input for the vent line and a PCCS unit description are required. MELCOR allows only three PCCS units, according to SBWR design, whereas in ESBWR there are six units. However, heat transfer capacity of six units can be achieved e.g. by installing three units with doubled capacity.

Table 3: Variation in PCCS performance due to pressure in the drywell. [11]

Pressure [10^5 Pa]	Variation factor
0.000	0.0000
1.000	0.0000
1.500	0.4250
2.000	0.6660
2.500	0.8495
3.000	1.0000
3.500	1.1289
4.000	1.2425
4.500	1.3450
5.000	1.4386
6.500	1.6807
7.000	1.7518

4. Reliability analysis for PCCS

In accordance to discussion in chapter 2, PCCS is classified as a type B passive system, i.e. it relies on natural circulation. Furthermore, referring to section 2.2, one approach for the reliability assessment of such systems consists of two parts: The first part includes the classical reliability analysis of components and the second part concerns the passive function, in this case, natural circulation. Quantification of a thermal-hydraulic system is challenging because of the large number of uncertainties mentioned in section 2.1, and because of this, one has to sometimes settle for qualitative analysis. It is often beneficial to begin reliability studies with failure modes and effects analysis (FMEA), which helps to identify potential failure modes and effects related to them.

Natural circulation reliability is herein evaluated through reliability analysis of the components designed to assure the best conditions for the function of it. It calls for identification of the mechanisms which maintain the intrinsic phenomena. Thus the reliability assessment can be conducted according to the classical procedure using for example fault trees. System unavailability can be a result of either a defect of some component or a failure of natural circulation.

4.1. Reliability data and failure modes and effects analysis

In PCCS, there are not many major components. The most critical ones are obviously the heat exchangers and in addition to that, piping is of great significance. In reference [12], a similar study was performed for the isolation condenser system. In that study, component reliability data was taken from sources [13] and [14]. Also expert judgements were availed. The same reliability estimates are used here, and the relevant ones with respect to this study are in Table 4. For complete heat exchanger failure, it is assumed that multiple pipe plugging or ruptures are needed.

The failure probability of the natural circulation upon which the system operation is based implies the identification of the corresponding failure modes. Three main failure modes can be identified to be a loss of heat transfer, high molar fraction of noncondensible gases and envelope failure, i.e. loss of primary boundary.

Table 4: PCC component reliability data. [12]

Component	Failure mode	Failure rate
Heat exchanger	Single pipe rupture	$3.0 \cdot 10^{-10}/\text{h}$
Heat exchanger	Multiple pipe rupture	$3.0 \cdot 10^{-11}/\text{h}$
Heat exchanger	Single pipe plugging	$3.0 \cdot 10^{-10}/\text{h}$
Heat exchanger	Multiple pipe plugging	$3.0 \cdot 10^{-11}/\text{h}$
Piping	Rupture	$2.4 \cdot 10^{-8}/\text{h}$

Loss of heat transfer to an external source (PCCS pool) can be due to insufficient water in the pool or due to heat exchanger pipe excessive fouling. The lack of water can occur because of leakages or malfunction of devices responsible for maintaining sufficient water level. Presence of noncondensible gases can result from a fouling in vent line. In that occasion, the system is unable to purge the noncondensibles into the suppression pool in the wetwell. The envelope failure is in principle present also in the component based analysis as a piping rupture. The reliability data for natural circulation failure modes are once again from [12], except for the insufficient water, for which the failure rate evaluation is given by the author, thus containing uncertainty of the highest kind. The values are in Table 5.

Table 5: Natural circulation reliability data. [12]

Component	Failure mode	Failure rate
Vent line	Excessive pipe fouling	$3.0 \cdot 10^{-11}/\text{h}$
PCCS pool	Insufficient water	$1.0 \cdot 10^{-7}/\text{h}$
Heat exchanger	Excessive pipe fouling	$3.0 \cdot 10^{-11}/\text{h}$
Primary boundary	Rupture	$2.4 \cdot 10^{-8}/\text{h}$

Failure modes and effects analysis (FMEA) is a step-by-step approach to identify the possible ways in which a system of interest might fail. The method also studies the effects and consequences resulting from different failure modes. Sometimes failures are prioritized according to the seriousness of consequences and failure frequency. The purpose of the FMEA is to discover which actions are most essential to take in order to eliminate or reduce failures. [15]

In Table 6 is a simple outline of FMEA for PCCS. It does not commit itself on the evaluation of severity of failures or on probabilities of any kind, but FMEA could consider these aspects as well. In many occasions a system component or function is given a risk priority number. In case of PCCS, failures are probably not observed until the consequences emerge, but for water level in PCCS pool there could be indicators. Inspections could be one way to identify failures beforehand. FMEA is a useful tool for further analysis of the system.

Table 6: A simplified failure modes and effects analysis for PCCS.

Component/Function	Failure mode	Failure cause	Consequence	Identification
Heat exchanger	1. Pipe rupture 2. Pipe plugging		System not operational	
Piping	Pipe rupture		System not operational	
Natural circulation	Insufficient heat transfer	1. Insufficient water in PCCS pool 2. Pipe fouling	Decreased heat transfer capability	1. Water level indicators
	Envelope failure	Piping rupture	System not operational	
	High concentration of noncondensible gases	Vent line fouling	No vent line flow	

4.2. Fault tree and failure probability

A fault tree constructed for the PCCS is in Figure 4. It is consistent with FMEA in Table 6 and it consists of two branches, one for failures due to natural circulation and the other for PCC component failures. PCCS failure rate can be quite easily calculated with help of this tree and the component failure rates are given in Table 4 and Table 5. It is worthwhile to consider failure probabilities of each branch separately, because an indication of relative importance can thus be acquired. Because there are only "or"-knots present in the tree, exact probabilities are straightforward to calculate by using complement probabilities. In general, fault trees are analyzed by using Boolean algebra.

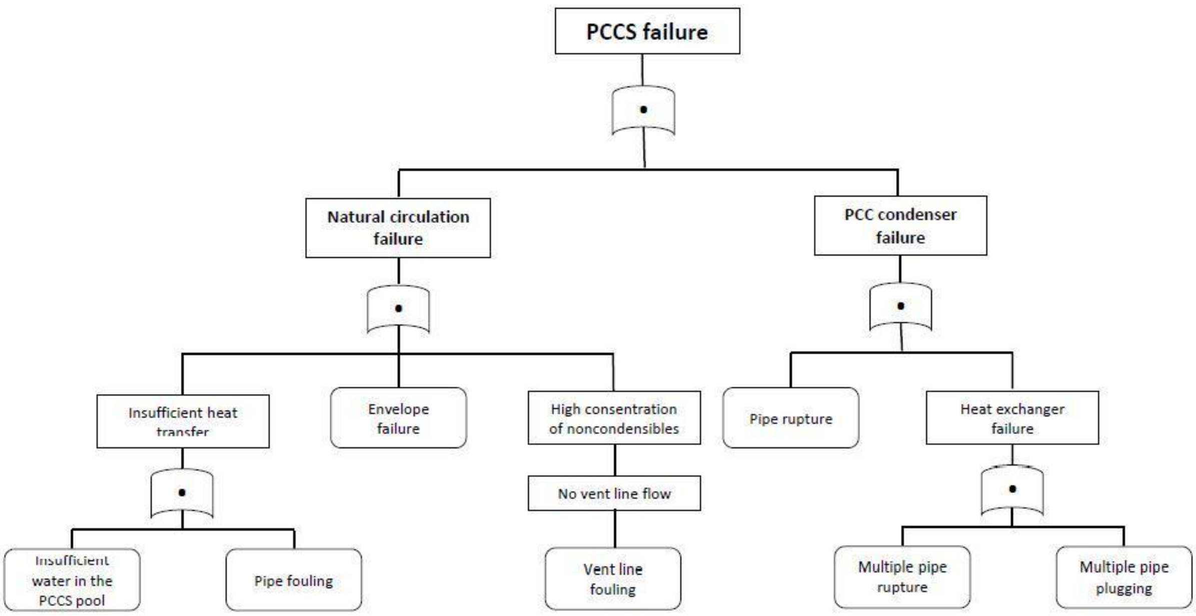

Figure 4: Fault tree for PCCS.

For large fault trees approximations for failure probabilities are calculated as the sum of minimal-cut-set probabilities. In fact, by using minimal-cut-sets, one obtains the upper limit for the failure probability. This can be convenient if the fault tree is of high complexity and the minimal-cut-sets are still possibly to identify. There may not even be need for exact probabilities, because approximations may provide sufficient total failure probability estimates. In this case, due to the structure of the fault tree, the minimal-cut-set approximation gives precisely the same failure probability as the exact value.

The events in the tree are denoted as follows, and for example A means the probability of the event A to happen, i.e. $\mathrm{A} \equiv \mathrm{P(A)}$, and $\overline{\mathrm{A}}$ is the complement event for A.

NCF	Natural circulation failure
A	Insufficient water in the PCCS pool
B	Heat exchanger pipe fouling
C	Envelope failure
D	Vent line fouling
PCF	PCC condenser failure
E	Pipe rupture
F	Multiple heat exchanger pipe rupture
G	Multiple heat exchanger pipe plugging

Natural circulation failure probability:

$$\mathrm{NCF} = 1 - \left(\overline{1 - \overline{\mathrm{A}} \cdot \overline{\mathrm{B}}}\right) \cdot \overline{\mathrm{C}} \cdot \overline{\mathrm{D}} = 1 - \overline{\mathrm{A}} \cdot \overline{\mathrm{B}} \cdot \overline{\mathrm{C}} \cdot \overline{\mathrm{D}} = \mathrm{A} + \mathrm{B} + \mathrm{C} + \mathrm{D}$$

PCC condenser failure probability:

$$\mathrm{PCF} = 1 - \overline{\mathrm{E}} \cdot \left(\overline{1 - \overline{\mathrm{F}} \cdot \overline{\mathrm{G}}}\right) = 1 - \overline{\mathrm{E}} \cdot \overline{\mathrm{F}} \cdot \overline{\mathrm{G}} = \mathrm{E} + \mathrm{F} + \mathrm{G}$$

Total PCCS failure probability:

$$\mathrm{TF} = 1 - \overline{\mathrm{NCF}} \cdot \overline{\mathrm{PCF}} = \mathrm{NCF} + \mathrm{PCF} = \mathrm{A} + \mathrm{B} + \mathrm{C} + \mathrm{D} + \mathrm{E} + \mathrm{F} + \mathrm{G}$$

With help of the fault tree and the failure rates, one obtains only the PCCS failure rate, not probability. In order to get the failure probability, a mission time for the system must be determined. Based on the PCCS specifications, it is reasonable to choose mission time to be 72 hours. In Table 7 are failure probabilities for both fault tree branches and the total failure probability for this mission time.

In this case, failure probability estimates are only rough approximations and should not be given too much weighting. Especially the percentage contributions of fault tree branches to total probability are very sensitive to component reliability values. The matter of substance in this analysis was to point out that, in principal, passive systems can be examined by using classical reliability methods. It must also be taken into account that there are six heat exchanger units in ESBWR, but the analysis above applies only to one unit.

Table 7: Failure probabilities for the PCCS for 72 hours mission time.

Failure type	Failure probability	Contribution
Natural circulation	$8.932 \cdot 10^{-6}$	83.76 %
PCC condenser	$1.732 \cdot 10^{-6}$	16.24 %
Total	$1.066 \cdot 10^{-5}$	100 %

5. MELCOR simulations

MELCOR is a fully integrated code that models the progression of severe accidents in light water reactor nuclear power plants. It is being developed at Sandia National Laboratories for the U.S. Nuclear Regulatory Commission as a plant risk assessment tool. Various accident phenomena, in both boiling and pressurized water reactors, can be modelled in MELCOR, and characteristics of accident progression include thermal-hydraulic response in the reactor coolant system, reactor cavity, containment etc. MELCOR has been designed to facilitate sensitivity and uncertainty analyses through the use of sensitivity coefficients. [11]

MELCOR modelling makes use of a "control volume" approach in describing the plant system. No specific nodalization of a system is forced on the user, which allows a choice of the degree of detail appropriate to the task at hand. Reactor-specific geometry is imposed only in modelling the reactor core. MELCOR is composed of a number of different packages, each of which models a different portion of the accident phenomenology or program control. For example core package evaluates the core behaviour. [11]

In this study, special emphasis is placed on the condenser package, which models the effects of the isolation condenser system and the passive containment cooling system. The basic idea of both systems relies on heat exchangers immersed in large water pools.

The MELCOR simulations are conducted by using an input file initially created for Olkiluoto 1 (OL1) boiling water reactor, located in Eurajoki, Finland. Some modifications are needed, though. OL1 is operated by Teollisuuden Voima Oyj (TVO), which is a non-listed public company founded to produce electricity for its shareholders at cost price. The accident scenario is a station blackout, i.e. the plant completely lacks offsite electric power.

The Olkiluoto reactor design does not contain passive containment cooling system. Because the PCCS is here added to the input file, the simulations are not plant-specific anymore and do not represent any actual reactor. The Olkiluoto containment is shown in Figure 5 and the PCCS is then added to this frame. The PCCS pool with heat exchangers is located above and outside the containment. Also the GDCS pool is added to the input because it is where the condensed steam is drained. However, the GDCS is not modelled and there is not any safety function related to that pool.

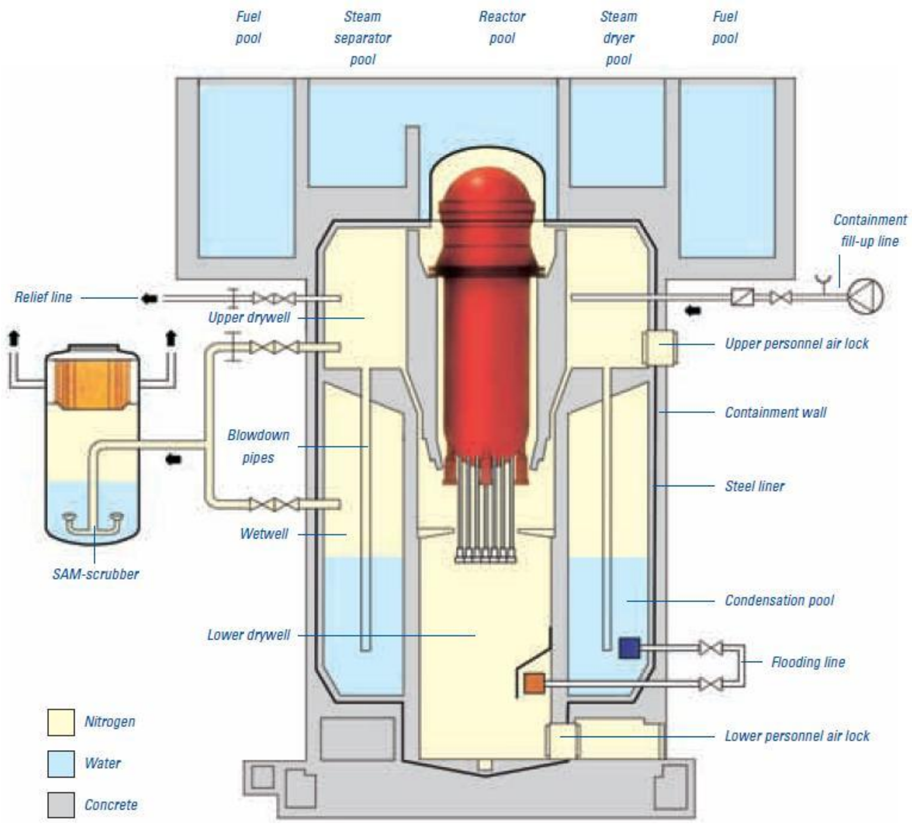

Figure 5: The containment of Olkiluoto 1 unit. In this study, the PCCS is also present. [16]

5.1. The accident scenario

Because the main purpose of the PCCS is to control the pressure difference between the drywell and the wetwell and provide heat removal, the most interesting quantities are related to the drywell atmosphere, pressure and temperature being the most obvious variables of interest. Also the mole fraction of noncondensible gases in the drywell is substantial, because it has such a big influence on the function of the PCCS. The basic nature of the accident scenario, a station blackout (SBO), is here introduced with help of the following couple of pictures, generated by 86400 second's (24 hours) example simulations with no PCCS.

The studied accident scenario is assumed to start with a station blackout. The reactor is scrammed successfully by control insert and the containment is isolated successfully following the scram. The operator initiates successfully the depressurization of reactor coolant system and flooding of cavity according to Severe Accident Management guidance at 1800 s after the beginning of the accident. Due to loss of off-site and on-site power, no safety injection or containment sprays can be started. Containment venting system does not need power and is available to relief containment pressure through filtered venting path when the upper drywell pressure exceeds 600 kPa. The opening point of vacuum breakers was modified to be 10 kPa. Table 8 collects the assumptions of operation of various safety systems during the investigated scenario and the timing of some of the key events is shown in Table 9.

Table 8: The availability of safety systems in the accident scenario at issue.

Safety system	221/354 Scram	311 MSIV	312 FW	313 MCP	314/ SRV	314/ ADS	316
Availability	**yes**	**yes**	**no**	**no**	**yes**	**yes**	**yes**
Safety system	321	323 LPI	327 HPI	322 cont. spray	351	362 filter vent	Ped. flood
Availability	**no**	**no**	**no**	**no**	**no**	**yes**	**yes**

Table 9: Key event summary of the investigated station blackout scenario.

Event	**Approximate timing [s]**
Reactor scram	0
MSIV closure	900
Start of RCS depressurization (314/ADS)	1800
Top of core uncovered	900
Whole core dry	1800
Start of cavity flooding	2000
Start of fission product release (cladding failure)	2700
Core support plate failure	5100
RPV failure	15000
Start of containment filtered venting	49000

In Figure 6 is the drywell pressure displayed in kPa units. The pressure rises quite steadily until the reactor pressure vessel breaches at ca. 15000 s and 220 kPa. Then the pressure jumps up about 100 kPas almost instantly. After that the pressure rises further, until the drywell rupture disk venting begins at ca. 49000 s. Subsequently the pressure drops virtually in an exponential manner.

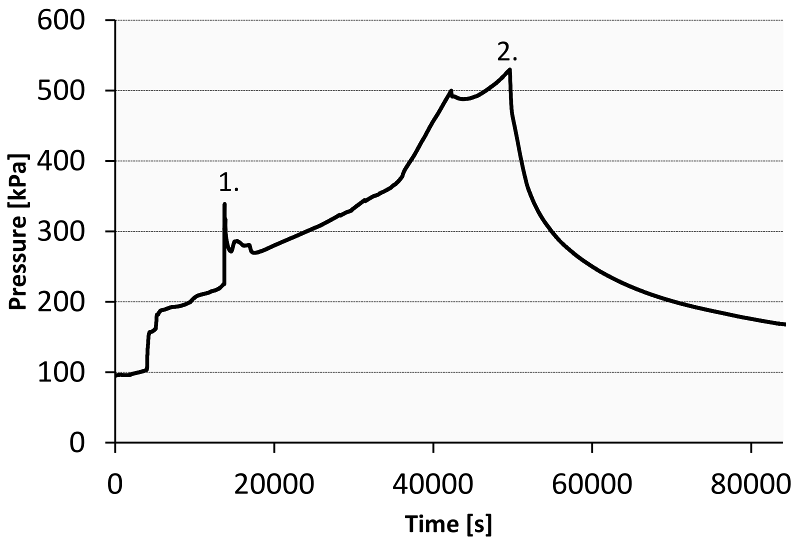

Figure 6: The pressure development in the drywell during example simulations with no PCCS. 1. Reactor pressure vessel breach. 2. Drywell rupture disk venting.

In Figure 7 the pressure differential between drywell and wetwell is shown. Again, the pressure vessel breach is distinct as the drywell pressure becomes over 40 kPa higher than the pressure in wetwell. After that, the pressure difference first fluctuates between 0 and 10 kPa, and then starts to rise at quite a high rate. The differential pressure collapses already before the drywell venting begins. The differential pressure is an important quantity, because the natural circulation and thus the function of the PCCS are highly dependent on it. The PCCS operation would work to equalize the pressure difference.

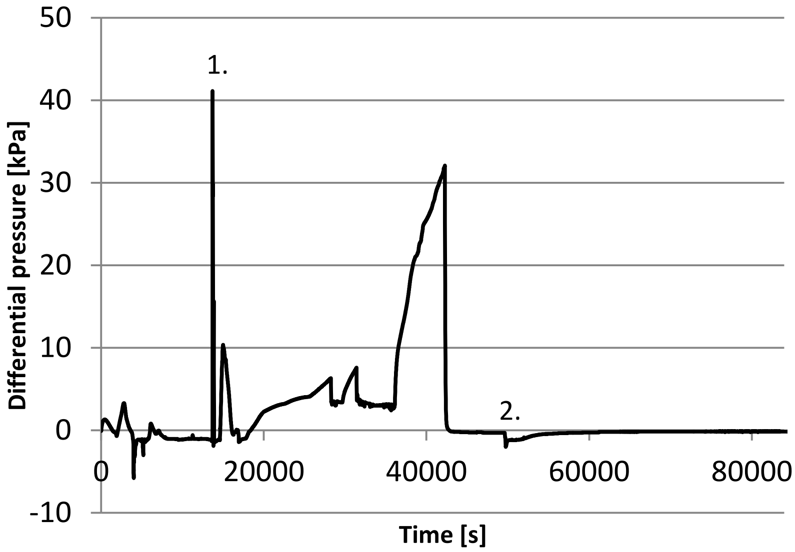

Figure 7: The pressure differential between the drywell and the wetwell during example simulations with no PCCS. 1. Reactor pressure vessel breach. 2. Drywell rupture disk venting.

Some effects can also be seen in Figure 8, which depicts temperature in the drywell. The vessel breach is easy to spot; the temperature rises over 50 degrees virtually instantaneously. No major effects, but a temporary small drop, are distinguishable resulting from the drywell venting. However, a little after that, the temperature begins to drop at a pretty slow rate.

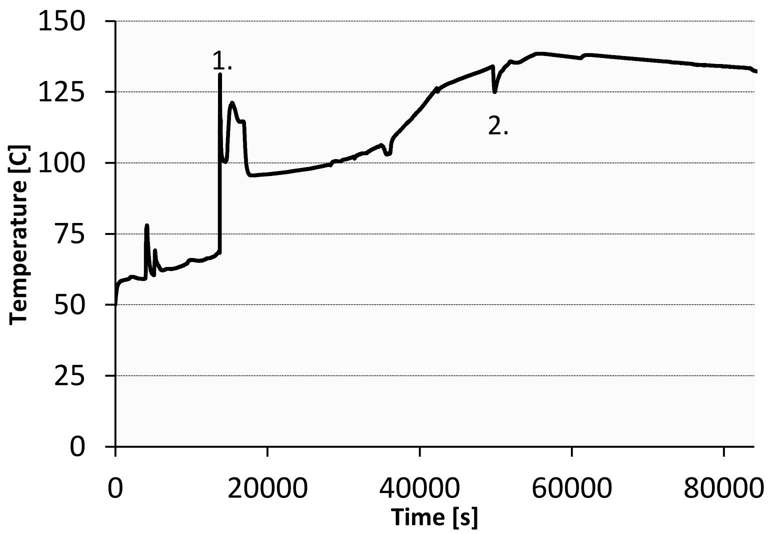

Figure 8: The temperature in the drywell during example simulations with no PCCS. 1. Reactor pressure vessel breach. 2. Drywell rupture disk venting.

Figure 9 and Figure 10 are very illustrative describing the effect of mole fraction of noncondensible gases in the drywell on the capacity of the PCCS units. The PCCS capacity is plotted for one unit with capacity of 11 MW in nominal conditions. The capacity at its most is over 100 % compared to the nominal capacity, because of the favourable conditions at that time.

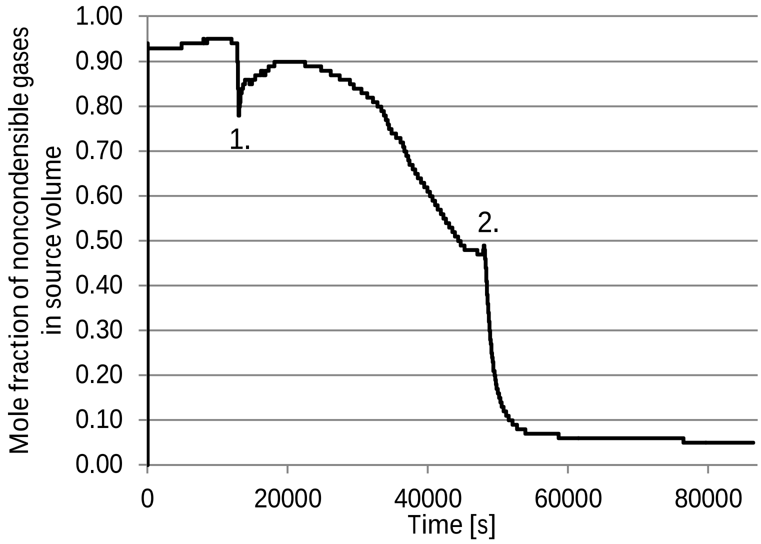

Figure 9: Mole fraction of noncondensible gases in source volume. One PCCS unit in example simulations. 1. Reactor pressure vessel breach. 2. Drywell rupture disk venting.

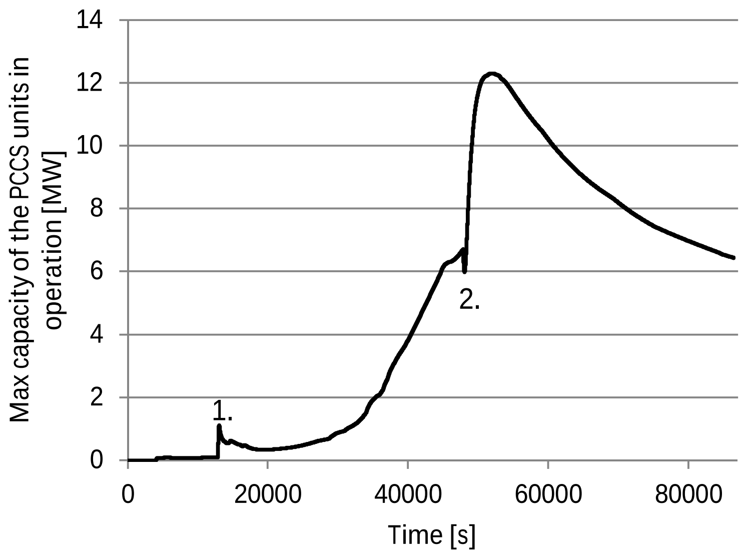

Figure 10: Max capacity of the PCCS unit in operation. One PCCS unit in example simulations. 1. Reactor pressure vessel breach. 2. Drywell rupture disk venting.

High amount of noncondensibles affects the capacity by interfering with the heat transfer process. First the fraction of noncondensibles is pretty high and the heat transfer capacity is very low. When the condensable steam displaces noncondensable gases, capacity increases. Reactor pressure vessel breach is seen as a discontinuity in both curves. Until the drywell venting begins, the curves in Figure 9 and Figure 10 are almost mirror-like. After that, the effect of drywell pressure on the capacity can be observed: The capacity drops similarly to pressure development in Figure 6, albeit the fraction of noncondensibles remains low.

In the context of the SBO simulations, the PCCS performance is mainly evaluated in two occurrences. First, how the system copes with the sudden rise in pressure when the pressure vessel breaches. Second, what can be said about the performance during the whole simulation time. There are a couple of interesting quantities to measure the performance: The total energy transferred to the PCCS pool and the integrated total flow through the PCCS vent line into the pressure suppression pool. These are very usable in describing the efficiency of the system. MELCOR does not offer remarkable spectrum of different parameters to vary. Special emphasis is here given to the number of PCCS units and the water level of the pool receiving the heat.

5.2. Effects of number of PCCS units on performance

One way to evaluate the performance of the passive containment cooling system and also the effects of heat exchanger unavailability is to vary the number of units, i.e. heat exchangers, conducting the heat transfer process. In ESBWR, there are six units in total, à 11 MW; ergo, the total heat transfer capacity is 66 MW in nominal conditions. The condenser package in MELCOR allows only three units, which forces one to alternate the maximum capacity of single unit in order to emulate ESBWR's PCCS with, say, 4 units in function.

Obviously the pressure and temperature in the drywell are essential quantities to determine the performance of the PCCS. After all, the system is designed to keep these variables within tolerable values. However, the accident scenario implementation used in these simulations is such, that the progression of the accident sequence is inevitable: The PCCS does not have any significant effect on neither the pressure nor the temperature in the drywell. This can be seen in Figure 11 and Figure 12, when compared to Figure 6 and Figure 8, respectively.

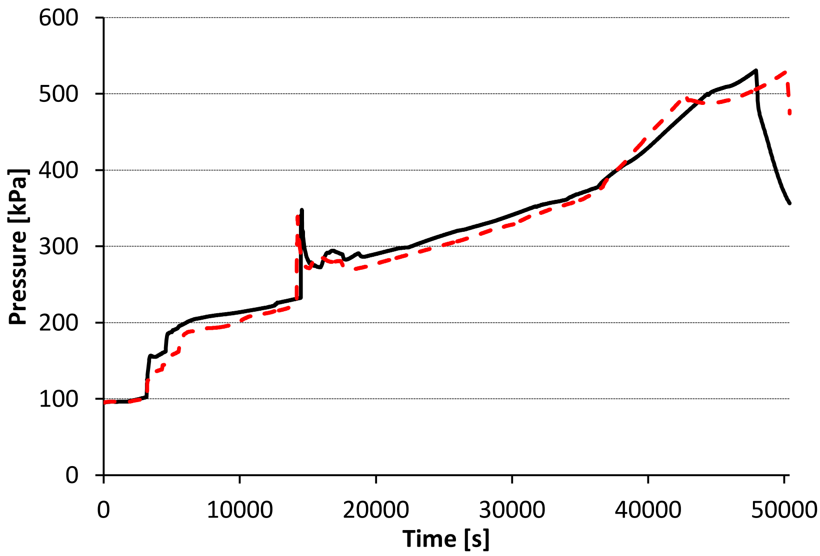

Figure 11: The pressure development in the drywell during simulations with three heat exchangers. The dashed line is from Figure 6 with no PCCS.

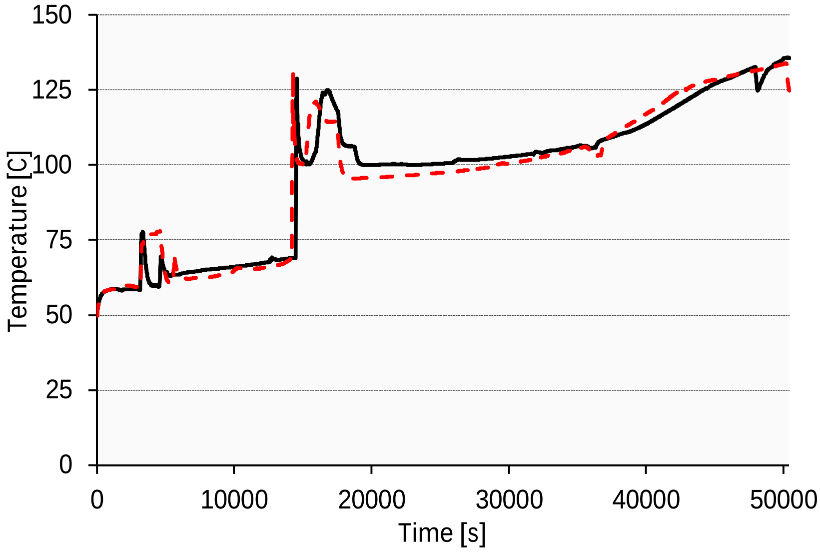

Figure 12: The temperature in the drywell during simulations with three heat exchangers. The dashed line is from Figure 8 with no PCCS.

The lack of decrease in pressure and temperature derives from the fact that during the simulations the pressure differential between drywell and wetwell is only occasionally sufficient enough to maintain the flow through the vent line. Adequate pressure differential to initiate the vent line flow is about 10 kPa, depending on current conditions. Heat transfer occurs only when natural circulation operates flawlessly. Whenever there is reasonable pressure differential, the system equalizes pressures efficiently, no matter whether there are one or six units in action. Figure 13 in comparison to Figure 7 illustrates this phenomenon, around time 40000 s. Figure 13 is generated with three heat exchangers, each of 11 MW capacity.

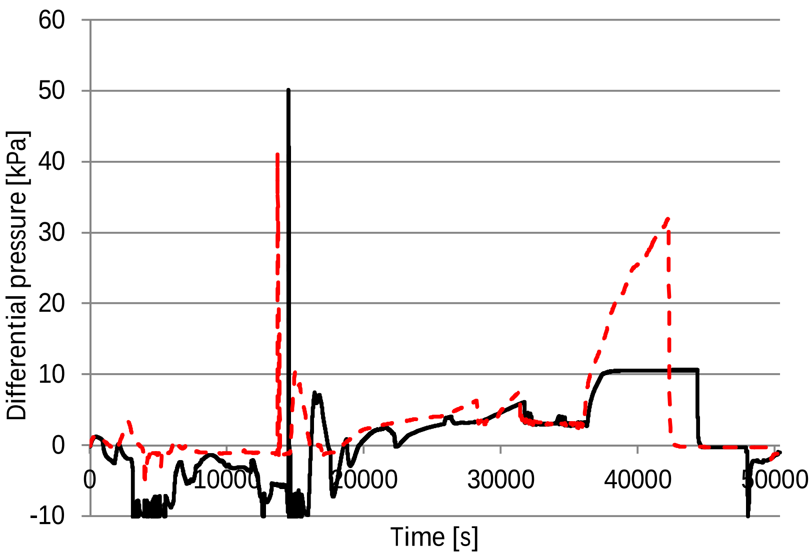

Figure 13: Differential pressure between the source volume (drywell) and the vent volume (wetwell). Three heat exchangers. The dashed line is from Figure 7 with no PCCS.

Figure 14 and Figure 15 describe the cumulative energy amount transferred to the PCCS pool and the mass flow through the vent line. Results are obtained with four different PCCS configurations. It can be seen clearly that the PCCS functions at two occurrences. When the reactor pressure vessel breaches, a rather quick operation is demanded from the system and fairly big energy volumes are transferred nearly instantaneously. Then the system remains inactive until pressure differential initiates the system to function again. This time the rising rates in mass flow and energy amounts are more restrained. The rise continues as long as adequate pressure differential exists, after which natural circulation cancellation follows.

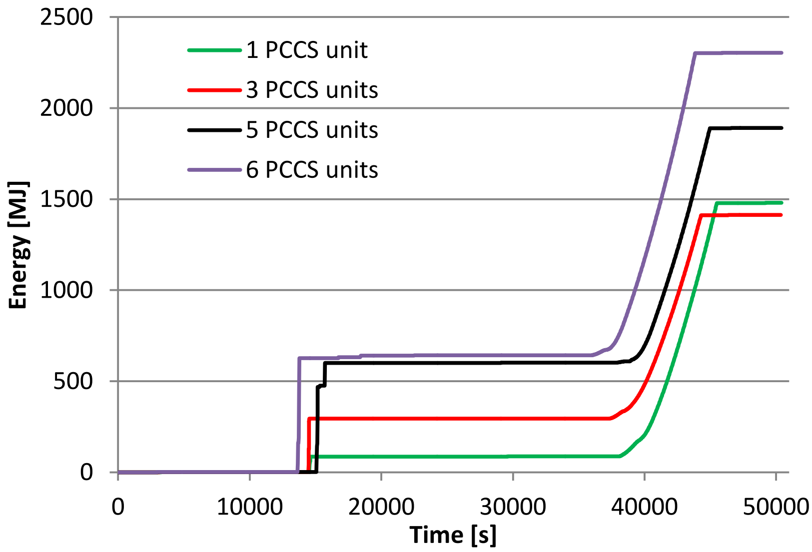

Figure 14: The cumulative total energy transferred to the PCCS pool during simulations with different number of units.

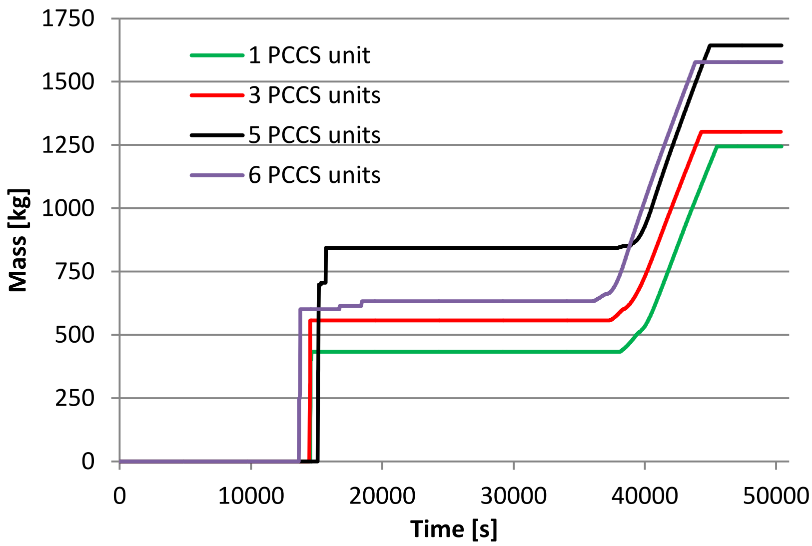

Figure 15: The cumulative flow through vent line during simulations with different number of units.

A notable fact in Figure 14 and Figure 15 is that the pressure vessel breach takes place at somewhat different times, depending on how many PCCS units are in action. This may have effect on how extreme conditions emerge in the drywell. Nothing else in the MELCOR input file has been changed but the number of PCCS units. Recalling that the code is deterministic, i.e. simulations with the same input provide exactly the same results, the phenomenon may indicate something about the robustness of the code. In ideal situation the conditions would be almost precisely the same for all PCCS configurations.

In general, it can be deduced that the more PCCS units, the more energy is transferred and the bigger the flow through the vent line. This was of course an expected result. However, also some inconsistencies can be observed: The total energy transferred during simulations with only one PCCS unit is higher than with 3 units. Moreover, the mass flow through the vent line during RPV breach is over 40 % higher with 5 units than it is with 6 units. Still the transferred total energy amount is higher with 6 than 5 units. Nothing really specific cannot be said about the dependencies, and slight mismatches presumably result from little different conditions emerged in different simulations.

Table 10 shows numerically how the number of heat exchangers affects the performance of the system. Six units case is regarded as the standard state and comparisons are made with respect to it. The amount of energy transferred to the PCCS pool and the vent line flow are used as performance measures. Another interesting measure is how effectively the system suppresses the sudden peak in differential pressure between drywell and wetwell after the RPV breach. It can be said that when the system is in use, there is a significant improvement in suppression time in comparison to situation where the PCCS is disabled. Nevertheless, the number of heat exchangers seems not to have any remarkable effect on suppression time as long as there is at least one functioning.

Table 10: The PCCS performance dependency on the number of units. 6 PCCS units case is regarded as the standard condition and the percentage comparisons are made with respect to it.

	No PCCS	1 PCCS unit	3 PCCS units	5 PCCS units	6 PCCS units (standard)
Energy transferred during RPV breach	-	86.4 MJ (13.8 %)	294.1 MJ (46.9 %)	600.8 MJ (95.9 %)	626.8 MJ
Total energy transferred	-	1479.1 MJ (64.2 %)	1413.2 MJ (61.4 %)	1891.4 MJ (82.1 %)	2302.6 MJ
Vent line flow during RPV breach	-	433.3 kg (72.1 %)	557.6 kg (92.8 %)	844.0 kg (140.5 %)	600.6 kg
Total vent line flow	-	1244.0 kg (78.8 %)	1302.0 kg (82.5 %)	1643.4 kg (104.1 %)	1578.0 kg
Pressure peak suppression time (RPV breach)	167.0 s (484.1 %)	45.5 s (131.9 %)	38.5 s (111.6 %)	40.0 s (115.9 %)	34.5 s

5.3. Effects of PCCS water pool level on performance

The water level in the PCCS pool should in theory have effect on the performance of the PCCS system. Insufficient amount of water hinders the heat transfer process and full capacity of the heat exchangers located in the PCCS pool cannot be exploited. In MELCOR the water level is one of the PCCS related parameters to be easily adjusted. The simulations were run for multiple different pool water levels in the event of a SBO. The standard pool level is 4.8 meters and the tested pool levels were mainly lower than that, the lowest being 1.8 meters. The chosen pool level values may seem arbitrary, but the choices were influenced by the fact that not all simulations succeeded. In addition, some of the simulations yielded inconsistent and unconvincing results and were ignored. In Figure 16 and Figure 17 are the cumulative energy transferred to the PCCS pool and the cumulative flow through the vent line with seven different pool water level values.

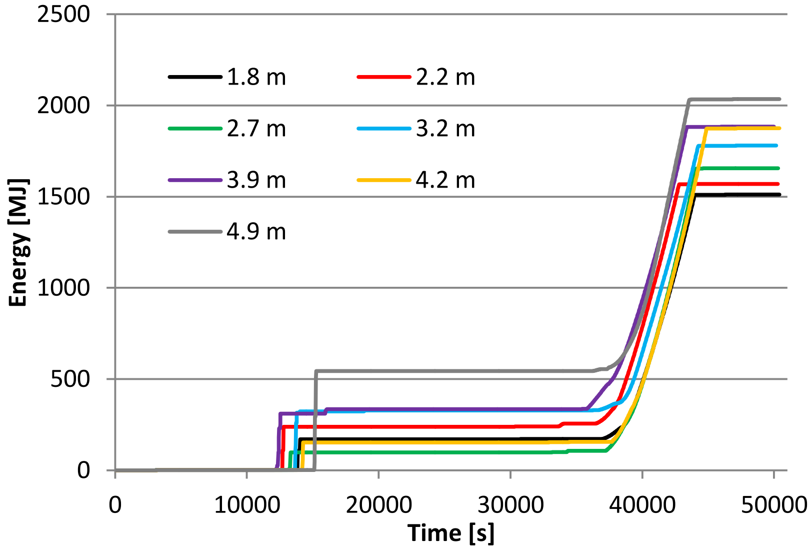

Figure 16: The cumulative total energy transferred to the PCCS pool. The PCCS pool water level is varied.

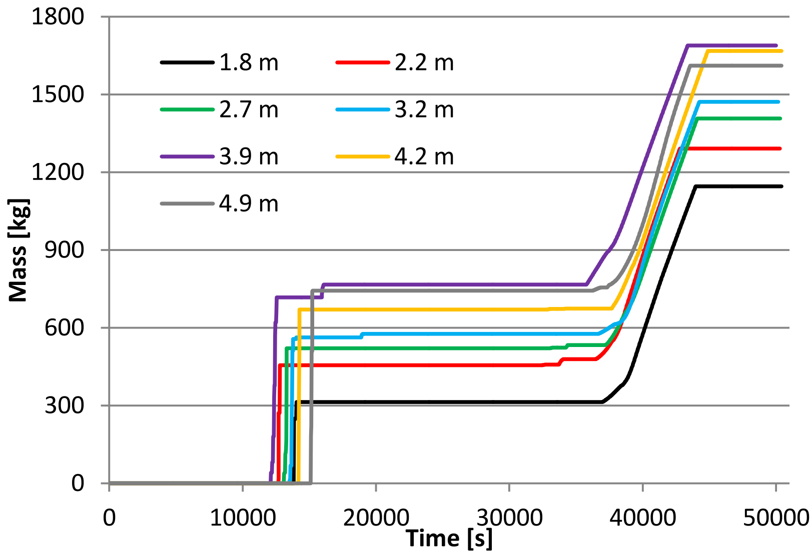

Figure 17: The cumulative flow through vent line. The PCCS pool water level is varied.

As can be seen from these figures, there seems to be a positive correlation between the PCCS pool water level and the efficiency of the system. The dependence seems a little stronger in the case of the flow through the vent line. After the reactor vessel breach, the curves in Figure 17 remain in the same order of magnitude until the end of the simulation. When it comes to energy transferred to the pool, the order at the end is somewhat different than it is just after the vessel breach. The time needed to suppress the pressure peak after the pressure vessel breach is in practise the same for all pool water level configurations. Table 11 shows numerically how the pool level affects the total energy transferred to the pool and the total vent line flow. The highest pool level is used as the point of comparison.

Table 11: The PCCS performance dependency on the PCCS water pool level. Percentage comparisons are made with respect to pool level of 4.9 meters.

Water level	1.8 m	2.2 m	2.7 m	3.2 m	3.9 m	4.2 m	4.9 m (reference)
Total energy transferred	1511.9 MJ (74.3 %)	1570.3 MJ (77.2 %)	1656.5 MJ (81.4 %)	1780.2 MJ (87.5 %)	1883.9 MJ (89.2 %)	1875.5 MJ (92.2 %)	2034.3 MJ
Total vent line flow	1145.9 kg (71.1 %)	1291.3 kg (80.1 %)	1407.4 kg (87.3 %)	1470.9 kg (91.3 %)	1688.9 kg (104.8 %)	1667.2 kg (103.5 %)	1611.3 kg

5.4. Self-built PCCS model in MELCOR

Another approach to emulate PCCS with MELCOR is to implement an own model by creating necessary control volumes and flow junctions. The PCC tubes and other essential heat structures are included in the model in order to describe the thermal-hydraulics of the system in a satisfactory manner. Obviously the MELCOR condenser package is disabled, so some of the interesting plotting opportunities are lost. This rather simple own model is implemented to provide a reference to results obtained by using MELCOR's condenser package. New results can also be used to validate the earlier results, should they be consistent enough with each other.

It is not possible to get data for example of the energy transferred to the PCCS pool via heat exchangers, so the comparison of the self-built model with the condenser package must be based mainly on the temperature and the pressure of the drywell. In Figure 18 and Figure 19 are the pressure and temperature in the drywell when the own PCCS model is functioning with full capacity. Some simulations were run with reduced capacity, but none of them really stood out with any remarkable significance.

Comparison is made with Figure 11 and Figure 12, although in these figures the PCCS capacity is only half of the full capacity. Some improvement can be observed especially with respect to the temperature in the drywell. The temperature remains under 100 degrees for the majority of the simulation time. In the end of the simulation the temperature starts to rise and ends up almost 140 degrees. Also the pressure is somewhat more satisfactory in the earlier parts of the simulations in comparison to simulations with MELCOR's condenser package.

However, the improvements may partly derive from the earlier RPV breach in self-built model simulations. It is possible also in the own model to plot the mass flow rate through the vent line. According to that data, the cumulative mass flow through vent line into the suppression pool during the simulations is about 700 kg. The amount is a little smaller than the numbers in Table 10, but it is close enough to be considered analogous with MELCOR's model.

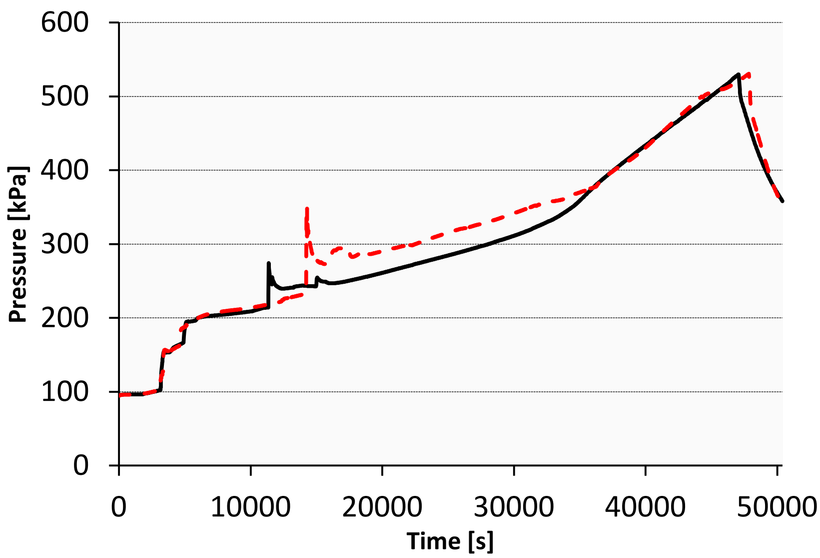

Figure 18: The pressure development in the drywell with own PCCS model with full capacity. The dashed line is from Figure 11 with 3 heat exchangers in MELCOR's condenser package.

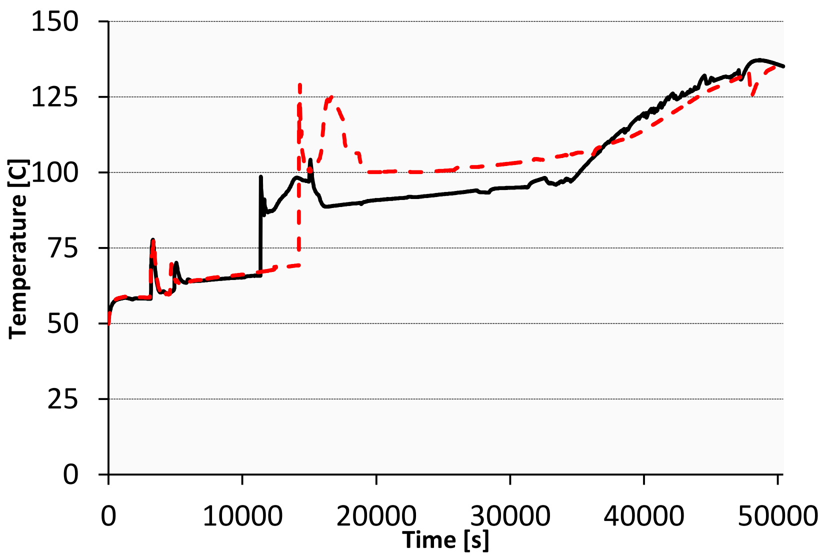

Figure 19: The temperature development in the drywell with own PCCS model with full capacity. The dashed line is from Figure 12 with 3 heat exchangers in MELCOR's condenser package.

Despite minor improvements, the own model was not efficient enough either. The PCCS should provide tolerable conditions for 72 hours, but clearly this was not the case. Nevertheless, these results bring confidence to the validity of simulations run using MELCOR's condenser package, because they are pretty consistent with each other after all. Thus the results also suggest that it could be pretty difficult to get PCCS operate properly in OL1 containment. This is a plausible conclusion, considering that natural circulation based T-H systems can be quite sensitive and need thorough design and accurate calculations. From reliability point of view there is not much value added generated from the own model. With reduced plotting opportunities the own model lacks some diversity.

5.5. Attempts to enhance PCCS workload

As the effects of the PCCS on the drywell atmosphere and on the performance measures of the system remained modest, some attempts to create more favourable conditions for the system were examined using MELCOR's condenser package. Firstly, the drywell rupture disk venting is disabled in order to let the pressure and the temperature in the drywell ascend further. Also the flow between the drywell and the wetwell is reduced. Secondly, it is reasonable to experiment a little different accident scenario. The PCCS is designed especially to provide safety in the event of LOCA, although it should be useful in various accident situations. The accident sequence used so far, a station blackout (SBO), is altered to represent main steam line LOCA.

Some longer, 20 h test simulations with original SBO input were run so that the drywell rupture disk venting and the flow junction between the drywell and the wetwell were disabled. Consequently the differential pressure starts to rise particularly in the latter part of the simulations. The idea is to force conditions in which a bigger contribution is demanded from the PCCS. The PCCS is working with full capacity, i.e. six units, to equal this pressure difference. However, the pressure and temperature in the drywell rise almost linearly during these simulations, so the PCCS did not manage in this occasion either. The pressure and the temperature at the end of the simulation are nearly 900 kPa and 200 degrees Celsius, respectively. The system equalizes the pressure differential efficiently, but the main influence of this is that the two pressures rise now nearly synchronically. The heat transfer to the PCCS pool is bigger than earlier, ca. 43000 MJ, during these simulations but still not good enough.

Another approach examined is a change in the accident scenario. A main steam line LOCA should fit better for the PCCS than SBO. In this case the mass and the energy from the RPV go into the upper drywell instead of being directed into the suppression pool in the beginning of the accident sequence. As a result, the pressure differential between the drywell and the wetwell rises substantially. Also in this case, there is no power available and safety injection and the containment spray is not functioning, so the characteristics of SBO remain.

The changes in the accident sequence are quite significant, as can be seen from Figure 20 and Figure 21, which depict the pressure and the temperature in the drywell, respectively. In these figures the effects of 6 PCCS units is compared to the situation where there is no PCCS functioning. This time the accident development is a little more aggressive than in the case of a SBO, and the drywell rupture disk venting begins already before 30000 s. The pressure curves are very similar with each other, but more remarkable effects can be seen in the temperature curves. The drywell temperature is significantly lower with PCCS, and the temperature difference at highest is as much as 150 degrees, which suggests that PCCS has notable positive effects on the drywell atmospheric conditions. Even so, the pressure and temperature figures are too high to be considered safe, and therefore the PCCS fails to fulfil its safety function in this occasion as well.

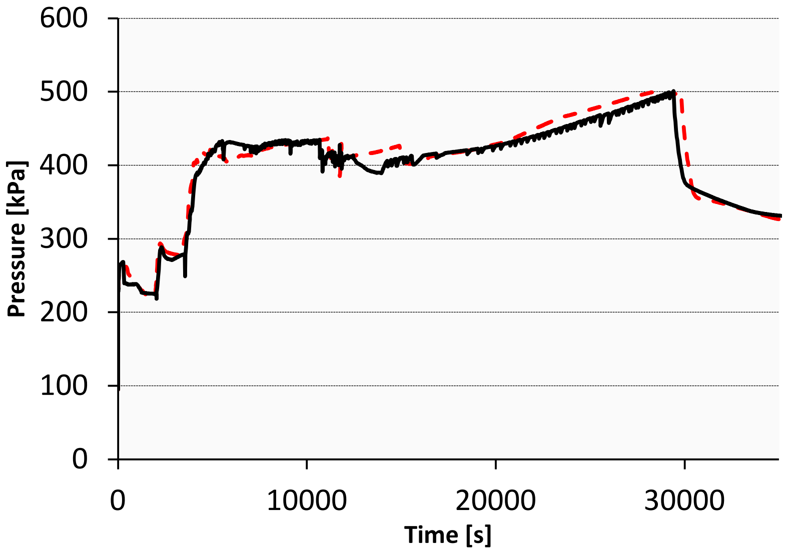

Figure 20: The pressure development in the drywell with 6 PCCS units and with no PCCS (dashed line). The accident scenario is main steam line LOCA.

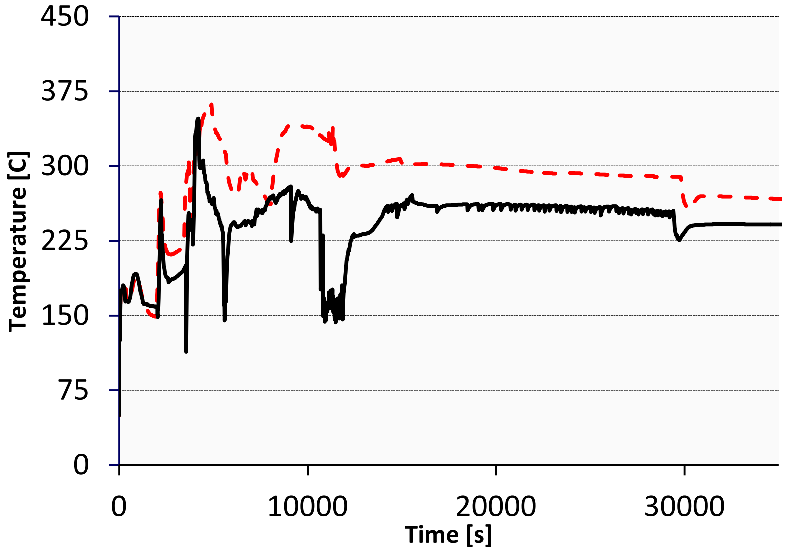

Figure 21: The temperature in the drywell with 6 PCCS units and with no PCCS (dashed line). The accident scenario is main steam line LOCA.

In Figure 22 is the cumulative energy transferred to the PCCS pool with three different PCCS configurations when the accident scenario is a LOCA. Like in the case of a SBO, there seems to be a positive correlation between the number of units and the system performance. However, this time the energy amounts are over 40 times higher and the maximum value exceeds 100000 MJ. Most of the heat transfer takes place in the earlier parts of the simulations and the PCCS functioning is more constant and not that clearly sequential as with the SBO.

After these attempts to create more demanding conditions for the PCCS, it seems that the accident scenario plays a big role in the system performance. The PCCS is able to transfer far bigger energy amounts in the event of a LOCA than in the case of a SBO. This is a digestible result, as the PCCS is designed to provide safety especially in the occurrence of a LOCA. Of course the system should be, and is, useful in other occasions as well. In spite of all, the pressure and temperature rise too high too fast in the case of LOCA as well. This implies the same as the earlier results with SBO: The dimensions and the design of the containment should take the PCCS into account for the PCCS to work as efficiently as possible. An afterwards installed system in containment with wrong type of geometry may not have desirable effects. Also, because the majority of other safety systems are disabled, the demands for PCCS are too big. PCCS alone cannot fulfil the safety requirements.

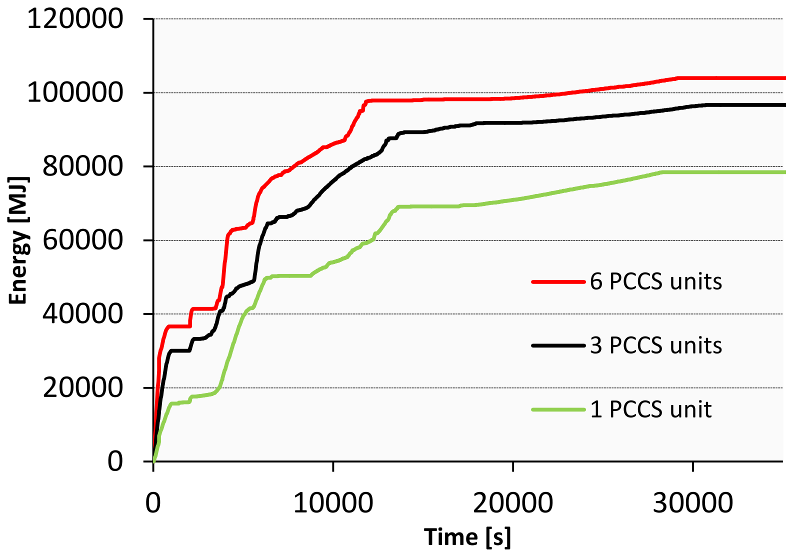

Figure 22: The cumulative total energy transferred to the PCCS pool in main steam line LOCA simulations with different PCCS configurations.

5.6. Interface with reliability analysis

The results above, dealing with the effects of the number of PCCS units and the effects of the water level of the PCCS pool on the PCCS performance, both in the event of a SBO and a LOCA, do not relate directly to the reliability assessment of PCCS. The results are more useful illustrating the PCCS operation. This applies also to the self-built condenser model. However, the information is valuable among other things for the determination of failure criteria for further reliability analysis and also builds up the understanding of the phenomena involved.

One example of a candidate for a failure criterion is the total energy transferred to the PCCS pool. Other quite obvious alternatives are the drywell pressure and temperature. Criterion can be chosen to be some percentage value of a performance measure in nominal conditions. Simulations make it easier to adjust appropriate values for failure criteria. Supposedly the total energy amounts and vent line flows would have been much higher than what they were in the SBO simulations, if the PCCS would have worked as intended, but e.g. maximum flow rates could possibly be useful as performance indicators as well.

The connection of MELCOR simulations to reliability assessment and probabilistic safety assessment (PSA) could also be studied through “point of no return” events, and their reliance on certain phenomenal parameters. RPV breach and containment failure are examples of such events. The phenomenal parameters contain uncertainties and they could be presented as random variables having probability distributions, which could be assumed to be given in this case. The idea in this dynamic approach would be to examine with help of MELCOR simulations how the parameter values affect the timing of the events of interest. The combined effect of the parameters would be an interesting question as well, and design of experiments type of approach would be useful. The eventual purpose would be to model the events with help of probability distributions and dependencies between them. Figure 23 presents a highly simplified Containment Event Tree (CET) made to illustrate different approaches, static and dynamic, to model the reliability of PCCS.

In the CET in Figure 23 it is assumed that the performance of PCCS has impact on the recovery of core cooling in order to avoid the RPV failure (event A) and on the protection of the containment integrity (event B). Both events can have several failure modes and there can be several time points of interest associated with the events, e.g. the vessel breach time T_A and the containment failure time T_B. The event failure modes and the time points of critical events are necessary input for the consequences of the sequences $C1, \dots, C8$, which are source terms associated with the CET end states.

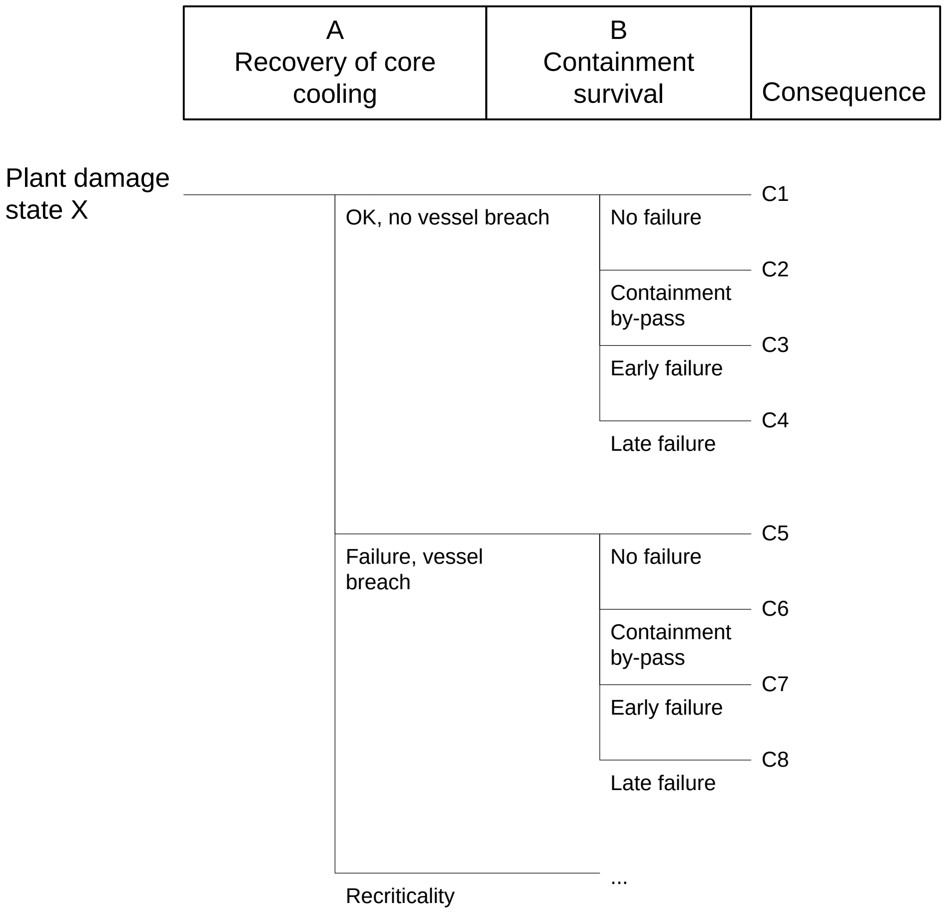

Figure 23: Simplified example of a containment event tree.

In a static approach the branch probabilities, such as $\mathrm{P}(\mathrm{B} = \text{Early failure} \mid \mathrm{A} = \text{Failure})$ or $\mathrm{P}(\mathrm{A} = \mathrm{OK})$, are static values, and are derived e.g. by fault trees linked to the branch. The PCCS failure is then modelled as a fault tree or just as a single basic event which is linked to the event tree branch. There may be different variants of the fault tree depending on the CET sequence and branch. As a result, for each consequence $\mathrm{C1}, \ldots, \mathrm{C8}$, one obtains a minimal-cut-set list which can be used to quantify the probability of the sequence. With regard to the time point of failures and consequences of the sequences, some representative values need to be defined.

In a dynamic reliability modelling approach, the system failure probabilities and the time points of critical events (e.g. $\mathrm{T_A}$ and $\mathrm{T_B}$) can generally be modelled by probability functions depending on each other. Subsequently, the consequences $\mathrm{C1}, \ldots, \mathrm{C8}$ can also be defined as functions of input variables of interest (like $\mathrm{T_A}$ and $\mathrm{T_B}$) instead of being point values. In this approach, the reliability of PCCS does not need to be (but can be) modelled as a Boolean function. It may be more practical to find a reasonable descriptive but simple correlation between the status of PCCS and the containment temperature and pressure, which in turn have impact on the probability and time point of events A and B. The reliability of the PCCS is no longer a single number but a probability function of the dynamic reliability model. The result of the CET is then a (multi-dimensional) probability distribution for the source term.

In general, containment event trees are used to model the accident progression in order to identify the accident sequences that lead to challenges to the containment and releases of radioactive material to the environment. Source terms, for one, determine the quantity of radioactive material released from the plant to the environment. Both terms, CET and source term, relate to level 2 PSA, which evaluates the chronological progression of core damage sequences. Level 2 PSA identifies ways in which associated releases of radioactive material from fuel can result in releases to the environment. It also estimates the frequency, magnitude and other relevant characteristics of the release. [17]

If the objective of the analysis is to obtain a reliability estimate for PCCS, the reliability assessment would probably be more profitable with some other, more specific simulation tool. Parameters such as pipe inclinations have effect on PCCS function and the MELCOR condenser package does not let the user vary these kinds of factors. Also the deterministic nature of the code is a little problematic. Maybe the most practical approach to simulation based reliability analysis would be to give system parameters some distributions from which to sample the values for them. The failure criteria would have been determined beforehand. This kind of Monte Carlo method would require quite many simulation runs and the system reliability estimate would be determined according to the fraction of runs which do not exceed the chosen failure criteria. This cannot be performed with MELCOR, but as pointed out above, the MELCOR simulations can be advantageous for example in determination of reasonable failure criteria and in dynamic approach to CET modelling.

6. Discussion and conclusions

This study has examined passive nuclear safety, concentrating on the reliability aspect. An overview on the methodology utilized in reliability assessment of such entities was given, and also uncertainties related to passive systems were handled. Special emphasis was given on the passive containment cooling system, a thermal-hydraulic passive safety system, and the function of the system was introduced quite thoroughly. Tools such as failure modes and effects analysis (FMEA) and fault tree analysis were used to conduct reliability assessment for PCCS. Component reliability data was taken from literature. Estimate for failure probability was obtained, but it must be regarded only as a suggestive approximation, as the main point was to show how to use classical methods in reliability assessment of passive systems. The PCCS was then investigated with help of MELCOR simulations.

When running simulations using a condenser package provided by MELCOR, the PCCS did not work as efficiently as it should have. Keeping the drywell pressure and temperature in the control limits did not succeed even though the PCCS is designed to secure tolerable atmospheric conditions during a transition phase. Also the energy amounts transferred to the PCCS pool in the station blackout accident scenario should presumably have been considerably bigger. In this study the PCCS was added to the Olkiluoto MELCOR model afterwards

The main reason for the rather poor performance is that the required pressure differential between drywell and wetwell did not exist for the most of the time. Without the needed conditions the natural circulation is dead and no heat transfer takes place. Some modifications to the SBO model were examined, but no major improvements to PCCS functioning emerged.

Some better results regarding system performance were obtained when the accident scenario was altered to represent a main steam line type of loss of coolant accident. The changes improved the PCCS operation and now e.g. the energy amounts transferred to the PCCS pool were manifold compared to the SBO case. Despite the slight improvements in the development of the drywell atmospheric conditions, pressure and temperature rose too high, and the PCCS effects were not satisfactory in the LOCA simulations either.

The problems encountered were not necessarily only modelling related. Systems based on natural circulation can be very sensitive and they must be designed thoroughly and carefully, requiring accurate calculations. Obviously, in Olkiluoto designs, the addition of such a system is not taken into account e.g. in the dimensions of the containment. It is possible, perhaps even probable, that also in reality an afterwards installed PCCS would not function desirably in the given setting. In this respect, it is understandable that the results turned out to be somewhat modest. Also, there are not many safety systems operating in the scenarios examined. Thus the workload for PCCS is too big and the system alone cannot cope with the extreme conditions emerging.

The results are dependent on the choice of simulation tool used in this study. MELCOR is intended to model the progression of severe accidents. It is quite simple, approachable and flexible through its block based nature, but it may not be very effective in conducting analysis of performance or reliability for a single safety system such as PCCS. If intention is to obtain a numeric reliability estimate for PCCS, some more specific thermal-hydraulic codes could potentially be more practical for this purpose of use. With MELCOR it is difficult to introduce probabilistic aspects into the analysis. It would be beneficial to conduct reliability assessment with a tool with which it is possible to sample system parameter values from given distributions. Another issue would then be to determine appropriate distributions.

However, information gained via simulations can be exploited e.g. for determination of failure criteria. The simulation information can also be used in a dynamic approach to CET modelling, thus linking up with level 2 PSA. The result of the CET is then a probability distribution for the source term (consequence) of the CET.

Despite the difficulties in PCCS performance in simulations, some results were obtained regarding the dependence of performance on the number of units and on the water level in the PCCS pool. As the PCCS did not yield highly significant improvement in drywell conditions, the quantities of interest were chosen to be the energy amount transferred to the PCCS pool and the vent line flow of noncondensable gases from drywell to the suppression pool in wetwell. The results were as anticipated. The more heat exchanger units available, the better the system performance is. Also a higher water level seems to result in enhanced heat transfer capability. The simulations help to quantify the effects of these two factors.

The simulations with self-made PCCS model did not offer many new insights from reliability point of view, but they provided a reference point to MELCOR's own PCCS implementation. It seems that self-built model may have performed even a little better than MELCOR's model, but neither of them were capable of sustaining tolerable conditions in the containment. The own model lacked some plotting opportunities available in MELCOR's implementation, which made the comparison of the two models a little harder.

The importance of research on passive systems seems to be increasing and future reactor types will most likely exploit more of these safety features. Thus the need for proper methods for reliability analysis of such systems becomes more urgent. The passive containment cooling system represents passive systems with thermal-hydraulic properties and therefore poses further challenges. This study on PCCS reliability should be regarded as a preliminary analysis, because the simulations did not yield any reliability estimate. However, the basis for further analysis exist now, and with suitable tools the assessment should be possible to conduct.

References

[1] International Atomic Energy Agency, IAEA. 1991. Safety related terms for advanced nuclear plants.

[2] L. Burgazzi. 2007. State of the art in reliability of thermal-hydraulic passive systems. Reliability Engineering and System Safety. Vol. 92. Issue 5. pp. 671-675.

[3] L. Burgazzi. 2007. Addressing the uncertainties related to passive system reliability. Progress in Nuclear Energy. Vol. 49. Issue 1. pp. 93-102.

[4] E. Zio, N.Pedroni. 2009. Building confidence in the reliability assessment of thermal-hydraulic passive systems. Reliability Engineering and System Safety, Vol. 94. No. 2. pp. 268-281.

[5] M. Marquès et al.. 2005. Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment. Nuclear Engineering and Design. Vol. 235. Issue 24. pp. 2612-2631.

[6] European Commission, 5th Euratom framework programme 1998-2002. 2002. RMPS project, Reliability methods for passive systems, Synthesis version of the final report.

[7] United States Patent; No. 5337243. 1994. Passive containment cooling system with drywell pressure regulation for boiling water reactor.

[8] Hinds, David, C. Maslak. January 2006. Next-generation nuclear energy: The ESBWR. Nuclear news. Vol. 49. No. 1. pp. 35-40.

[9] Beard, J. Alan, GE Nuclear Energy. 2006. ESBWR Overview.

[10] GE Nuclear Energy. 2006. ESBWR Design Control Document. Tier 2, Chapter 6: Engineered Safety Features.

[11] Sandia National Laboratories. 2005, MELCOR Computer Code Manuals. Vol. 2: Reference Manuals.

[12] L. Burgazzi. 2001. Passive system reliability analysis: A study on the isolation condenser. Nuclear Technology. Vol. 139. No. 1. pp. 3-9.

[13] N. C. Rasmussen. U.S. Nuclear Regulatory Commission. 1975. Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants.

[14] S.E. Mays, EG&G Idaho. 1982. Interim Reliability Evaluation Program: Analysis of the Brown Ferry Unit 1, Nuclear Power Plant, Appendix C—Sequence Quantification.

[15] ASQ, American Society for Quality. ASQ: The Global Voice of Quality. Failure Modes and Effects Analysis (FMEA). [Online] [Cited: 15 September 2011.] http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html.

[16] Teollisuuden Voima Oyj. 2008. Nuclear power plant units Olkiluoto 1 and Olkiluoto 2.

[17] International Atomic Energy Agency, IAEA. 2010. Development and application of level 2 probabilistic safety assessment for nuclear power plants, Specific safety guide.