PSAM11 & ESREL 2012
Helsinki, 26 June 2012

Thoughts in the aftermath of accident at the Fukushima Daiichi NPP

Jukka Laaksonen

Vice President of Rusatom Overseas

Outline

- PSA results versus operating experience
- Lessons from major NPP accidents
- Experience from provision of three essential safety functions at NPPs
- Protecting safety systems from external and internal hazards
- New questions on safety after accident at Fukushima Daiichi
- Conclusions from ”stress tests” conducted after accident at Fukushima Daiichi
- Examples from safety enhancing measures aiming to prevent another accident like Fukushima Daiichi

The accident at Fukushima Daiichi has shaken the trust on nuclear safety !

Can we still believe on our ability to make safe nuclear power plants and operate them safely?

Can we regain society confidence on our ability?

What should we think about PSA results? - 1

- It has not been unusual to claim high safety level of NPP’s by referring to the results of PSA :

  “the frequency of severe reactor core damage at older NPP’s is in the range 10^{-4} … 10^{-5}/year; in the new NPP’s around 10^{-6} /year”.

- However, the experience now indicates a frequency of more than 3 x 10^{-4} /y

  five NPP reactor cores have been damaged in less than 15 000 operating years!

- Can we believe in any quantitative predictions on nuclear safety ?

What should we think about PSA results? - 2

PSA gives us information on scenarios that we have modelled – PSA is definitely a good tool for identification and comparing risks when we use it right !

but

None of the severe accident scenarios we have seen,

TMI – Chernobyl – 3 x Fukushima

was properly modelled and studied with PSA before the accident occurred !

TMI – 1979

Immediate cause: Operators did not handle right a relatively simple incident.

Root cause: **Lack of knowledge**. Inadequate understanding of reactor systems behaviour in transient conditions.

- Until 1979, the safety research had been focusing mostly on large break loss of coolant accident.
- The behaviour of a PWR primary circuit had not been thoroughly studied and was not understood.
- The operators had no instructions for the event they met.

Chernobyl – 1986

Immediate cause: The reactor was not inherently safe, as was required in the US regulations that were developed already in 1960´s and adopted in most other countries.

Root cause: **Lack of safety culture**. Inadequate attention to inherent reactor safety and safety in general.

- The designers were aware of the possibility of explosive reactivity increase, and this had been seen in precursory events. Operators were not clearly warned of the danger.
- Operators did not take seriously the warnings in instructions written by reactor designers. Instead they took orders from the grid control centre.

Fukushima – 2011

Immediate cause: Large earthquake followed by tsunami.

Root cause: **Lack of adequate regulations.** Not enough attention to site specific hazards.

- Tsunamis are well known in the Japanese history – large tsunamis have been recorded typically three times in each century.
- Tsunamis were not used as a design basis for Fukushima plants – they were brought to the Japanese nuclear safety regulations less than ten years ago but only modest protection was enforced.

Next accident – ???

Immediate cause: surprise again ???

Root cause: not addressed in design, operation, regulation ???

- We must not tolerate any more accidents.
- Safety reassessments (“stress tests”) have been made in all nuclear power plants to identify risks not recognized previously
- New insights have been gained again: we have a real opportunity to take actions to strengthen nuclear safety
- It is time to take strong actions to eliminate severe nuclear accidents in the foreseeable future.

Continuous strive towards perfection is needed

We shall require and provide designs that are able to withstand new surprises.

Questions on safety

- The question we must not make:

  “are our plants safe enough?”

- The right question is:

  “how can we make our plants more safe?”

Learning from experience is necessary

In the development of all new technologies, progress has required learning from past mistakes and taking corrective actions to avoid repeating them.

Nuclear technology is no exception:

- many of the safety principles and approaches can be traced back to specific accidents or near misses;
- accidents and unexpected incidents have given new insights and have led to enhanced level of safety;
- learning needs to continue

What means “nuclear safety” ?

“Nuclear safety” means

1. preventing major damage of the reactor core or the used nuclear fuel bundles

2. if this is not successful, preventing release of radioactive nuclides from the damaged core to the environment

Basic safety functions for ensuring nuclear safety

Nuclear safety can be assured by providing the three basic safety functions:

1. Control of reactivity
   - preventing uncontrolled reactor power increase and shutting the reactor when needed,
2. Removal of decay heat to the ultimate heat sink
   - cooling of shutdown reactor and used nuclear fuel
3. Containment of radioactive materials
   - preventing significant radioactive releases to the environment

This was the message given to operators in emergency operating procedures that were developed after TMI !

Fulfilment of basic safety functions

Fulfilment of the basic safety functions shall be assured in all situations:

1) preferably by means of inherent safety features relying on the laws of nature, and
2) as the second alternative by reliable active safety systems designed to carry out these functions (high quality, redundancy, diversity are essential).

Based on lessons from Fukushima, the priority shall be in alternative number one (1).

In addition, the systems and structures providing the basic safety functions shall be protected from hazards that may threaten their integrity and intended function.

Concept for fulfilment of basic safety functions

The fundamental basis to ensure fulfilment of basic safety functions is the concept of **Defence-in-Depth:**

- Defence-in-Depth concept has been developed since the inception of nuclear power development
- Its importance has been understood better and better after each severe accident
- The concept is thoroughly explained in the International Safety Groups' report *INSAG-10, Defence in Depth in Nuclear Safety* (google: "INSAG-10").

Levels of Defence-in-Depth

1. Deviations from normal operational situations and failures of systems, structures and components are prevented with high reliability and good safety margin.
2. If deviations from normal operation or failures occur, they are promptly detected and corrected, and normal situation is returned by appropriate protective measures.
3. If normal situation cannot be returned by protective measures, the safety functions are ensured by activating specific safety systems that prevent the accident from progressing to a reactor core damage.
4. **If a reactor core damage would occur, the accident progression would be controlled by mitigating the accident consequences and preventing releases of radioactive materials to the environment.**
5. **If a radioactive release to the environment would occur, mitigation of the radiological consequences would be provided through a well planned off-site emergency response.**

Control of reactivity - 1

Reliable control of reactivity has been the paramount issue since designing the first reactors.

Nevertheless, some accidents have resulted from failure to control reactivity.

Control of reactivity - 2

Lessons from loss of reactivity control EBR-I reactor in 1955

- Fast breeder reactor EBR-I (1,7MWe) started operation in 1951 on a test site in the Idaho desert.
  - It was known to have features that in certain circumstances could lead to explosive increase of nuclear power (positive reactivity coefficient with respect to coolant voids, leading to prompt criticality)
  - Safety pre-cautions were planned to avoid uncontrolled reactivity increase
  - In a certain test of the reactivity properties in 1955 the operating staff made an error causing a loss of criticality control and a partial core meltdown.
- The accident was actually a "Chernobyl accident in miniature size".
  - It gave an important lesson to US designers but due to the small size and remote location of the reactor no serious consequences in the environment resulted.

Control of reactivity - 3

Lessons from reactivity accident at EBR-I in 1955 (cont.)

- The EBR-I accident raised a proposal on a mandatory reactor design principle: always providing a negative power coefficient of reactivity when a reactor is producing power.
- This principle was kept in mind in the design of all reactors in the USA
- In 1969 the principle was included in the very first General Design Criteria for Nuclear Power Plants that were issued as formal regulations by the US AEC.
  - these criteria are presented since then in 10 CFR 50, Appendix A,
  - in the latest revision of the Appendix A, the principle is written in a re-formulated form as Criterion 11, *Reactor inherent protection (*google: “Appendix A of 10 CFR 50).

Control of reactivity - 4

Current state-of-the-art in providing reactivity control

- Reactivity control and shutdown systems have achieved a mature state.
  - Inherent characteristics of the reactor core ensure safe feedback on disturbances and prevent an uncontrolled fast power increase.
  - All reactors designed since the very first one have had fast shutdown systems based on potential energy and a system that starts the shutdown function with high reliability.
- The shutdown systems have been found reliable since the early years of nuclear reactors: failure of a fast shutdown system has not led to fuel damages in a properly designed reactor .

Control of reactivity - 5

Current state-of-the-art in providing reactivity control (cont.)

- Adding of boron to the coolant is generally used as diverse means to shutdown the reactor
- In the PWR reactors:
  - adding boron to the coolant is in most reactors necessary to maintain the reactor subcritical when it is cooled below its normal operating temperature
  - **in some of the new PWR reactors** the control/shutdown rods are not able to provide subcritical conditions after xenon has decayed in the shutdown core , and thus **boron addition to the coolant is necessary already a few hours after shutdown, even in hot shutdown state**– this is an example of dangerous reduction of safety margin and should not be allowed
  - an example of different development was found **in the new VVER design, AES-2006** offered to Finland and being constructed as LAES-2: **control rods alone keep the core subcritical in less than 100 deg C**.

Control of reactivity - 6

Current state-of-the-art in providing reactivity control (cont.)

- In the BWR reactors
  - the control/shutdown rods insert enough “negative reactivity” when they are functioning as designed, and can thus maintain the shutdown state in all possible temperatures.
  - however, it is necessary to insert the control rods always fast – **if fast insertion does not succeed when cold feedwater having by-passed the preheaters is supplied**, the diverse system for **slow insertion of rods**, e.g. with electrical motors, would deform strongly the power distribution and **would cause serious fuel failures in the top part of the reactor core**.
  - if fast control rod insertion fails, a reliable boron (or other liquid neutron absorber) injection system is necessary for ensuring safety

Removal of decay heat - 1

Removal of decay heat from the shutdown reactor has turned out to be more demanding than provision of reliable reactivity control:

- Removal of decay heat requires reliable function of the heat transfer systems for a long time;
- **The main risks of a severe accident are thus resulting from a loss of the decay heat removal.**

Removal of decay heat - 2

- Decay heat removal was not emphasized in the early nuclear era and it was not explicitly mentioned in the first set of criteria incorporated in Appendix A of 10 CFR 50 in 1969.
- This shortcoming was corrected in 1971 when the major revision of Appendix A incorporated
  - Criterion 34 concerning reliability of the front line decay heat removal system
  - Criterion 44, concerning the reliability of cooling circuits that transfer the heat further to the ultimate heat sink.
- In spite of the retrospective issuance of general design criteria, the "second generation" reactors worldwide meet, with possibly a few exceptions, the criteria that are currently in force in the USA and are almost unchanged since 1971 (for current requirements, google: "Appendix A to 10 CFR 50").

- **However, we have to question the adequacy of the old criteria from 1970's !**

Removal of decay heat - 3

Insights from the reactor safety study

- Reactor Safety Study was the first Probabilistic Risk Assessment (PRA) of a nuclear power plant as a whole. The report was issued as draft in 1974 and as final in 1975; it is generally known as WASH-1400 or “Rasmussen report”.
- The study combined the best available knowledge and data of that time with a best estimate analysis and gave quite new insights on importance of different factors for ensuring nuclear safety.
- Main conclusion of the WASH-1400 was that the highest contribution to the severe core damage probability is caused by the initiating events that are not so infrequent but could lead to unexpected accident scenarios and finally the loss of decay heat removal.
- Although the WASH-1400 got much attention, it found initially very little practical application in nuclear power plant design or in nuclear regulation.
- The value of WASH-1400 was recognized only after the accident at Three Mile Island (TMI-2) plant in 1979.

Removal of decay heat - 4

Lessons learned from TMI-2 accident in 1979

- The TMI-2 accident was initiated by a relatively frequent event: stopping of normal feed water pumps.
  - Loss of normal feed water caused opening of the pressurizer relief valve, as anticipated at Babcock & Wilcox designed plants (due to unique once through type steam generators).
  - However, the event took an unexpected path when the relief valve failed to close.
  - This started continuous loss of reactor coolant from the pressurizer through the open valve.
- The immediate cause of the accident was that operators were not able to handle right this relatively simple incident scenario (they did not recognize the continuous leak, and stopped the HP emergency core cooling pumps).

Removal of decay heat - 5

Lessons learned from TMI-2 accident in 1979

- The TMI-2 accident was initiated by a relatively frequent event: stopping of normal feed water pumps.
  - Loss of normal feed water caused opening of the pressurizer relief valve, as anticipated at Babcock & Wilcox designed plants (due to unique once through type steam generators).
  - However, the event took an unexpected path when the relief valve failed to close.
  - This started continuous loss of reactor coolant from the pressurizer through the open valve.
- The immediate cause of the accident was that operators were not able to handle right this relatively simple incident scenario (did not recognize the continuous leak, stopped HP emergency core cooling pumps).

Removal of decay heat - 6

Lessons learned from TMI-2 accident in 1979 (cont.)

After TMI-2, many changes took place for enhancing nuclear safety:

- Nuclear safety research was diverted to a large variety of topics.
- Plant specific full-scope control room simulators were installed for operator training.
- Plant specific PRA models were developed and were used for finding and eliminating risks that had not been recognized before.
- Emergency operating instructions were thoroughly revised for all reactor types: instructions were no more based on managing of specific pre-determined event scenarios but instead the focus was in maintaining the three basic safety functions in any scenarios.
- With advanced analytical models it was noted that reactor internals of many PWR plants could actually not withstand dynamic forces caused by large break LOCA– a sudden guillotine break of a main line of the reactor coolant system. This led to development of the “leak before break” approach that was aimed to eliminate very fast break of the main coolant line and the resulting sharp pressure wave moving at high speed inside the primary circuit.

Removal of decay heat - 7

Current state-of-the-art in decay heat removal

The lessons learned from past accidents and from extensive analysis and testing have provided significant amount of knowledge on means to prevent accidents caused by loss of the decay heat removal.

In the design of some “third generation” plants, it has been considered adequate to provide the following means for the decay heat removal:

- Availability of two alternative ultimate heat sinks: open air and large water reservoir (sea, lake or river).
- High decree of redundancy and diversity of systems that can remove heat from the reactor core, both in a state with intact reactor coolant system and in a state with leaking coolant circuit.
- High decree of redundancy and diversity of electrical power sources that are needed to drive the active components.

Based on lessons from Fukushima accident, the adequacy of decay heat removal systems of most NPPs, including generation III designs, is now seriously questioned !

Containment of radioactive materials - 1

Lessons from Windscale accident in 1957

Windscale was graphite moderated and gas cooled plutonium production reactor, **directly cooled with open air, only with simple filters at the outlet**.

In October 1957, a sudden release of potential energy accumulating in crystal lattice under neutron bombardment took place in the graphite moderator of the reactor. It caused many failures in fuel cladding and ignited a fire in graphite.

- Radioactive nuclides were released from the failed fuel directly to the air. Estimated releases of iodine-131 and cesium-137 were about 3000 times less than respective releases from the Chernobyl accident.
- No evacuation of the public was considered necessary but milk produced in an area of about 500 km^2 was destroyed for a time of one month.

The Windscale accident was an important contributor to establishing a general concept of multiple barriers for preventing radioactive releases.

Containment of radioactive materials - 2

Insights from the study known as WASH-740

In order to have some basis for the reactor site criteria, a study was made on radiological consequences of “worst conceivable accident” in a 500 MWth reactor.

- Results were published in1957 in the report known as WASH-740.
- Due to a lack of experimental evidence, the study involved much engineering judgment and used pessimistic assumptions. For instance, it was postulated that air born release would be 50% of all fission products and wind would blow directly to a city of 1 million people at 50 km distance.
- WASH 740 predicted up to 3400 death, up to 47000 injuries and a significant property contamination.
- After issuing of WASH-740 it was evident that a reactor containment for preventing large releases had to be made mandatory.

First plant with a containment, Shippingport, was commissioned in the USA in December 1957. A leak tight containment has been required since then in all nuclear power plants built in the USA and in many other countries.

Containment of radioactive materials - 3

Containing radioactive releases from core meltdown accident

The TMI-2 accident demonstrated that it is possible to maintain containment integrity and to prevent practically any significant releases after a partial core meltdown.

At TMI-2, the decay heat removal was lost only for a quite short time and thus the loads to the containment were not extreme.

The accident gave a strong boost to research of severe accident phenomena. Major research programs were established especially in Germany but research was started also in France, USA, Japan, and Switzerland. The goal was

- to explore and understand the conditions to be expected after a full core melt down accident and
- to develop means for protecting the containment integrity even under the worst conceivable conditions.

Containment of radioactive materials - 4

Containing radioactive releases from core meltdown accident (cont.)

Based on the encouraging results of the severe accident research, some countries such as Sweden and Finland issued rules in early 1980’s requiring that

- all physical phenomena threatening the integrity of the containment after a core meltdown accident had to be considered and dedicated protective measures had to be provided to ensure the containment integrity.

In Finland the requirement was at that time intended to concern the design of new plants.

Containment of radioactive materials - 5

Containing radioactive releases from core meltdown accident (cont.)

The Chernobyl-4 accident was of such a nature that evidently no containment would have helped to avoid large releases.

Nevertheless, the serious consequences and great public concern gave a reason to study possibilities to contain a core meltdown accident even at operating plants.

Containment of radioactive materials - 6

Containing radioactive releases from core meltdown accident (cont.)

Today all nuclear power plants in Sweden and in Finland are back-fitted with dedicated systems that are designed to take into account all conceivable physical phenomena occurring after a core meltdown, and to protect the containment integrity against each of them.

For some systems the implementation took about 15 year of work, including planning, experimental research, safety analysis, design, and installation.

Containment of radioactive materials - 7

Current state-of-the-art in providing containment of radioactive materials

Provision of leak tight reactor containment has been one of the basic requirements for nuclear power plants in most countries since 1957.

- It has been proven in practice that containments with adequate strength and leak tightness can be built.
- The strength requirement for ensuring the reactor containment integrity was initially based on the highest pressure that can be expected inside the containment after a large break LOCA (typically 5 atmospheres).
- Leak tightness requirement for containments was already in 1962 specified on the basis of very high postulated release of radioactive materials inside the reactor containment.

Containment of radioactive materials - 8

Current state-of-the-art in providing containment of radioactive materials (cont.)

Research has demonstrated that meeting the LOCA peak pressure requirement provides adequate strength for a containment to maintain its integrity even in connection with a severe accident.

The original LOCA leak tightness requirement from 1962 gives assurance on small releases also in connection with severe accidents.

Ensuring containment integrity in connection with severe accidents requires that it is equipped with dedicated systems that protect it from physical phenomena expected after core meltdown: 1) extensive hydrogen generation, 2) gradual build-up of high pressure and temperature, and 3) interaction of structures with molten core.

In addition, it is necessary to reduce the primary circuit pressure with a reliable dedicated system before core meltdown.

Protection of safety functions from hazards - 1

In the early years of nuclear power plant development, protection against internal and external hazards received very little attention.

The first version of 10 CFR 50, Appendix A, issued in 1969, included a very general criterion on fire protection but no other hazards were explicitly mentioned.

Protection of safety functions from hazards - 2

The revision of Appendix A issued in 1971 took an important step towards improved protection of safety systems against hazards. It contained three well formulated criteria:

- Criterion 2—Design bases for protection against natural phenomena.
- Criterion 3—Fire protection.
- Criterion 4—Environmental and dynamic effects design bases.

These criteria gave a good starting point for the designers and regulators, but several events after issuing the criteria have shown the need for more stringent application than what was initially thought.

Protection of safety functions from hazards - 3

Lessons learned from protection against extreme natural phenomena

The criterion 2 of Appendix A states following:

"Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect:

(1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed."

Protection of safety functions from hazards - 4

Lessons learned from protection against extreme natural phenomena (cont.)

The natural hazards that have received most attention in the nuclear safety research and in design are the earthquakes.

As concerns protection against seismic hazards we have a good reason to state that experiences from Japan are most encouraging:

- Plants designed by competent engineers to withstand postulated seismic hazards have not suffered damages in the safety related parts although they have been hit by much larger earthquakes than the design bases earthquake.
- Especially one should mention the Niigata Earthquake of July 2007 near Kashiwazaki-Kariwa and the Great East Japan Earthquake of March 11, 2011.

Similar positive experiences have been recorded in other countries, most recently in the USA at North Anna plant.

Also one could be mention the Armenian NPP that in 1988 provided uninterrupted power after an earthquake that killed 25 000 people and left much of the northern Armenia in ruins.

Protection of safety functions from hazards - 5

Lessons learned from protection against extreme natural phenomena (cont.)

Unfortunately the tsunamis have not been considered in the design in a manner that could be said to be in compliance with before mentioned Criterion 2 in 10 CFR 50, Appendix A.

According to the statistics that I have found from the internet, tsunamis have caused large destruction on Japanese coasts on the average three times in a century and tsunamis are well known in the Japanese history and arts.

Protection of safety functions from hazards - 6

Lessons learned from the Browns Ferry fire in 1975

In March 1975, a fire was experienced in the cable spreading room below the main control room of the Browns Ferry-1 plant in the USA. It caused

- a loss of control of many of the engineered safety features
- disturbances also at Browns Ferry-2

An NRC team set up to investigate the event found

- lack of definitive criteria, codes, or standards related to fire prevention or fire protection in NPP’s
- need for revision of the criteria covering separation of redundant control circuits and power cables

The findings started major revision of fire safety criteria and guidance and research on fire safety was intensified.

Protection of safety functions from hazards - 7

Lessons learned from the Browns Ferry fire in 1975 (cont.)

The NRC team also recommended that the regulatory guidance regarding the proper balancing of the three factors identified as defence-in-depth principles for fires be augmented:

1. Preventing fires from getting started.
2. Detecting and extinguishing quickly such fires that do get started and limiting their damage.
3. Designing the plant to minimize the effect of fires on essential functions.

Respective criteria have been adopted and implemented in other countries.

Protection of safety functions from hazards - 8

Consideration of air plane crashes

Initially the design basis air plane crash was selected on the basis of statistical data and its probabilistic analysis:

- Main factors influencing the choice were the air routes and airports close to the plant site.
- Also the frequency of military flights and statistics on military plane crashes was considered.

Depending on the plant, the design basis could be a crash of a small four seat aircraft, a mid size passenger aircraft, or a military air craft used in the respective country.

The protection was often provided by the outer shell of a double containment or an strengthened single containment.

Protection of safety functions from hazards - 9

Consideration of air plane crashes (cont.)

After the malevolent plane crashes in New York on September 11th 2001, there was a new public concern that led to more stringent requirements.

In the case of malevolent act the probabilistic considerations were no more meaningful. Therefore the design basis required for new plants is crash of a large passenger plane.

The new requirement has resulted in

- significant strengthening of the reactor containments and safety systems buildings
- in eliminating the risks from fires and vibrations inside the buildings.

Experiments and analytical calculations have given confidence on adequate protection against largest plane crashes at plants that meet the new requirements.

Protection of safety functions from hazards - 10

Current state-of-the-art in protecting safety functions from internal and external hazards

Physical protection of safety functions from external hazards has received much attention in the design of “third generation” nuclear power plants.

Protection against most hazards, including earthquakes, fires and air plane crashes has achieved a state that gives good confidence on adequate protection.

Many other hazards have been assessed in the recent safety re-evaluations that were started after the accident at TEPCO’s Fukushima Dai-ichi plant.

A hazard that evidently needs more attention and improved protection is tsunami.

New safety questions raised after Fukushima - 1

- Should safety functions be provided without any AC power for an extended time? How long time?
- Should control rod insertion alone provide adequate long term subcriticality of an intact core?
- Should two diverse ultimate heat sinks be required ? What is considered adequate diversity?
- What should be required from systems that protect containment integrity in connection with core meltdown?
- Which systems should be protected from external hazards?

New safety questions raised after Fukushima - 2

Can transportable equipment – AC or DC power sources, water pumps and tanks – provide reliable protection if all permanently installed systems implementing certain safety function are lost? What should be required concerning their

- safety classification?
- installation and operation in harsh conditions?
- storage place?
- protection in storage?
- connection point accessibility and protection?

Would permanently installed diverse, robust, independent and well protected safety systems be more reliable than transportable equipment?

Conclusions from “stress tests” - 1

Protection against complete loss of AC power

- Most of the currently operating NPP’s are not designed to withstand a long term complete loss of AC power
  - without any AC power, the time to core meltdown at different plants and in different accident conditions varies from less than one hour to a couple of days
- Especially in Europe, the emphasis has been in high reliability of AC power supply (as a design basis the AC power is postulated not to be lost)
  - multiple redundancies (up to 4) in on-site AC power sources
  - diverse redundant (2) on-site AC power sources
  - dedicated supplies from nearby hydropower or gas turbine plants
- However, a common view is emerging after the accident at Fukushima Dai-ichi that protection should be provided for
  - loss of all AC power sources
  - loss of the internal AC power distribution system, or
  - common cause damage of electrical motors connected to internal AC power network

Conclusions from "stress tests" - 2

Protection against complete loss of AC power (cont.)

- In some countries a new requirement has been set: a possibility for decay heat removal from reactor and containment has to be provided without any AC power for extended times (e.g., for three days)
  - the system not needing AC power could be based, for instance, on passive heat removal by natural coolant circulation or on driving of pumps by independent permanently installed diesel motors that are air cooled and well protected against external and internal hazards
  - turbine driven pumps can hardly be considered reliable enough, due to their complicated interaction with other systems and excess burden to operators in emergency situations
- In some other countries, transportable AC power supply systems are considered to provide adequate protection and such equipment have already been supplied.
- Decisions on strengthening the off-site power supply have been made, e.g. Japan is going to improve resistance of external grid to seismic hazards.
- Many plants are also improving reliability of on-site power supply, e.g. with diverse cooling of diesel generators or new diverse power sources.

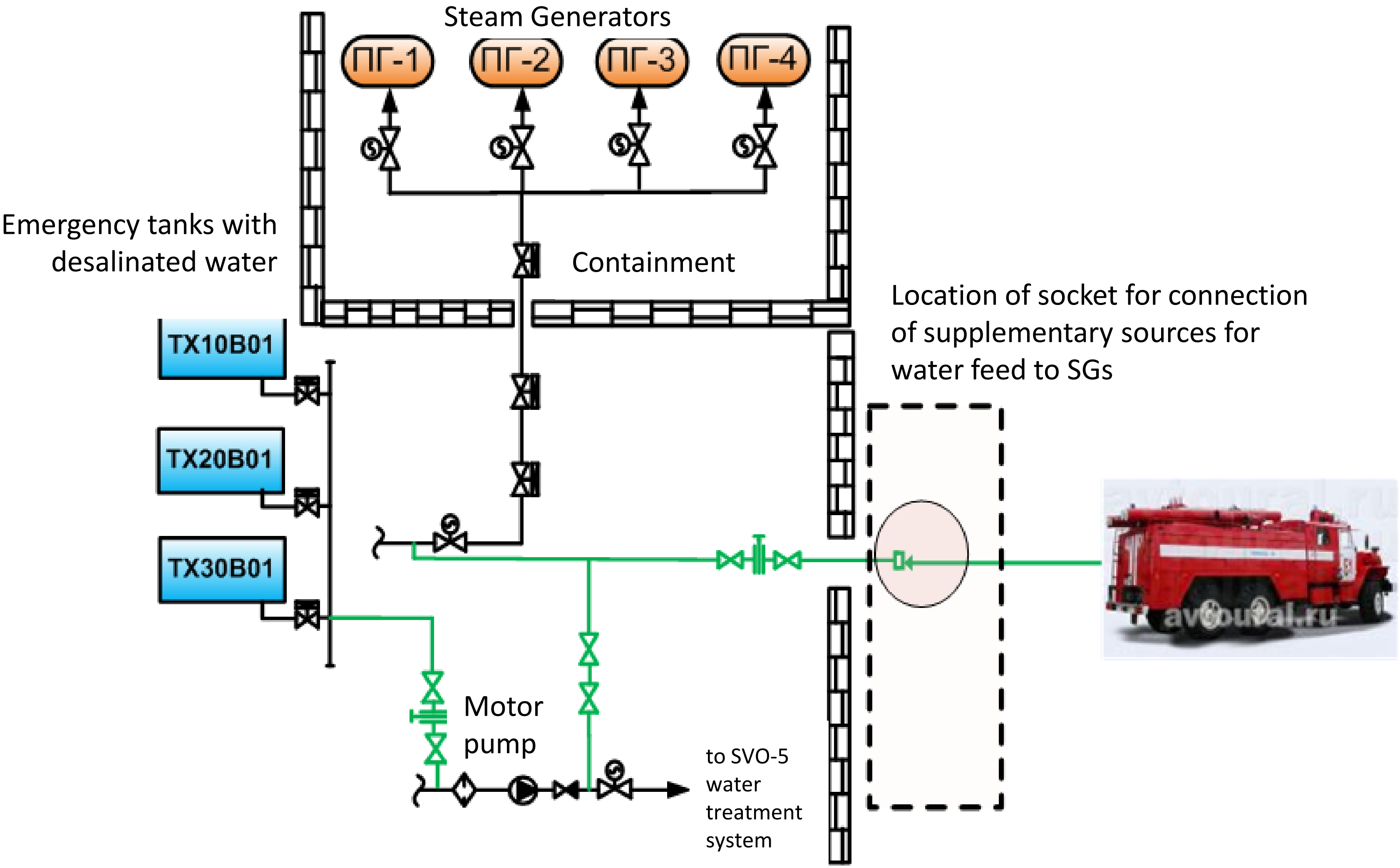
Conclusions from “stress tests” - 3

Diverse ultimate heat sink

- Two diverse ultimate heat sinks are generally required but – the question on what should be considered as adequate diversity has turned out to be difficult and no consensus has been achieved yet among national regulators. Among others, following questions have been discussed:
  - If sea water is used as a primary heat sink and the sea water outlet is well separated from inlet, under which conditions if any can coolant circulation in reverse direction (from the outlet to inlet) be considered to provide a diverse heat sink?
  - If groundwater or a large water pool is available as an alternative heat sink in case of loss of primary water based heat sink, what is required from the cooling circuits to provide adequate diversity?
  - Can feed and bleed operation of PWR’s (feeding water into steam generators and releasing steam to the atmosphere) be considered to provide adequate diversity and under which conditions?
  - Can feed and bleed operation of BWR’s (feeding water into reactor vessel and releasing slightly radioactive steam to the atmosphere) be considered to provide adequate diversity and under which conditions?

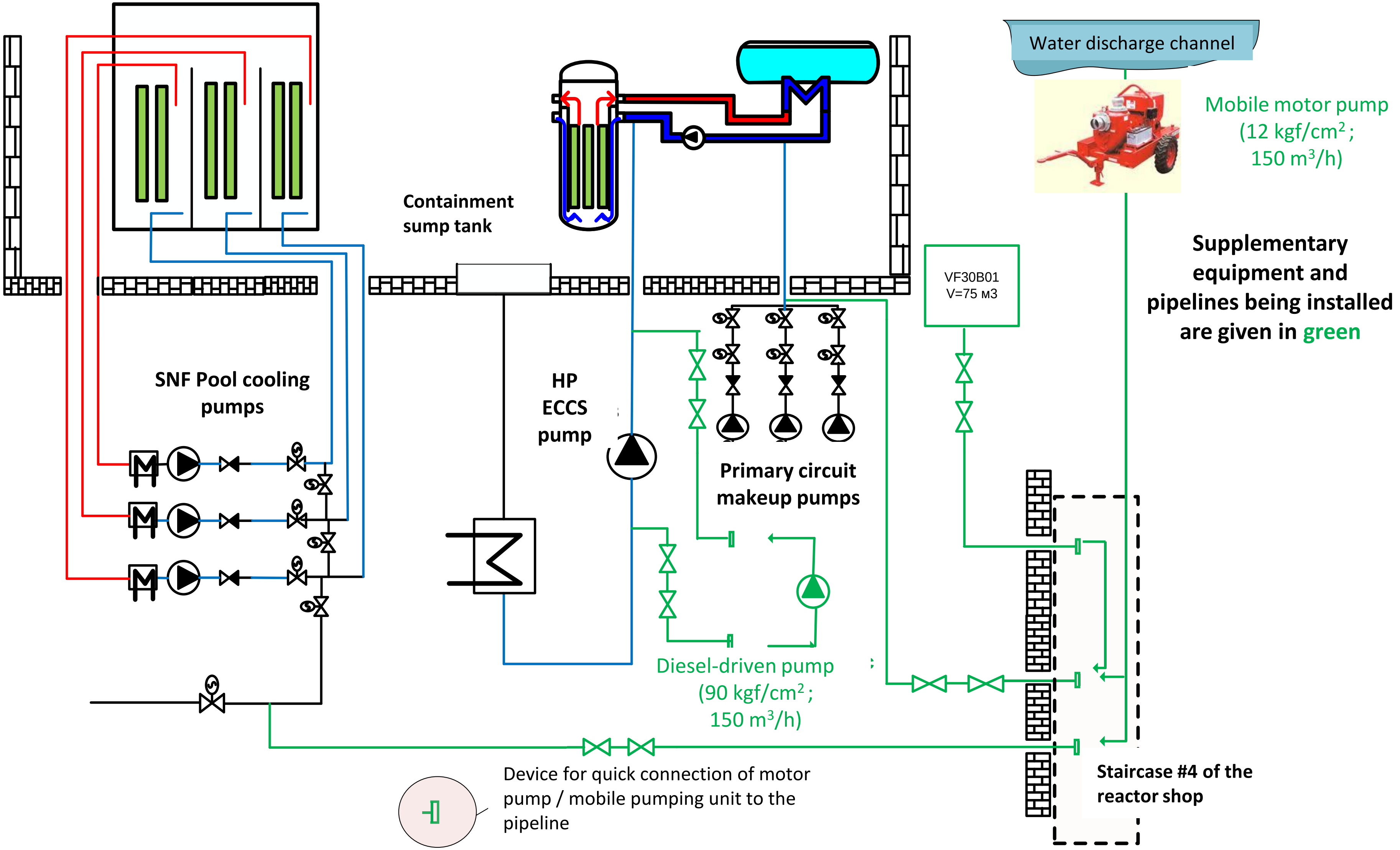
Scheme of water supply to SGs of VVER-1000

Backup system for water supply to SGs from fire fighting vehicles, motor pumps



Steam Generators
ПГ-1
ПГ-2
ПГ-3
ПГ-4
Emergency tanks with desalinated water
Containment
Location of socket for connection of supplementary sources for water feed to SGs
TX10B01
TX20B01
TX30B01
Motor pump
to SVO-5 water treatment system
avtoural.ru

Scheme of primary circuit makeup and heat removal provisions for VVER-1000 using supplementary sources and mobile means



Conclusions from “stress tests” - 4

DC power supply, battery capacities and recharging

- Typical battery discharge times by design have been found to be in the range of 1-3 hours. Some plants have confirmed by testing that actual times are much longer, i.e. 6-9 hours.
- A general conclusion is that a systematic evaluation of requirements for DC power sources is needed at all plants
    - battery capacities for each purpose: design requirements and actual performance
    - strategies and procedures for load shedding and battery staggering in different situations
    - possibilities to provide recharging with new permanently installed or transportable equipment
    - possibilities for easy replacement of batteries
    - on-line condition monitoring of batteries

Conclusions from “stress tests” - 5

Cooling of spent fuel in storage pools

- a common view has emerged that in all circumstances there is enough time to provide adequate cooling of spent fuel with transportable equipment
    - connections, preparedness and procedures are needed to supply water to fuel pools from fire trucks, in order to be prepared for complete loss of the fixed systems providing decay heat removal
        - as concerns timing, most critical are the pools that are designed to receive all reactor core soon after reactor shutdown – fuel could start uncovering in 7-9 hours at some plants
    - robust instrumentation is needed for temperature and water level monitoring in fuel storage pools

Conclusions from “stress tests” - 6)

Primary coolant pump seals in connection with loss of AC power

- primary coolant pump seals seem to have quite different capability to maintain their integrity and leak-tightness in loss of AC power situations – a pump seal LOCA is difficult to handle without AC power
  - some pump seals are told to survive only a few hours, while others report test results indicating very small leaks (200 liters/hour) from all seals together in conditions simulating no seal cooling, full pressure, and normal operating temperature
- it is evident that actions are needed at many plants to address the concern of seal leaks

Conclusions from “stress tests” - 7

Operation of vital valves during loss of AC power

- verification of valve positions at loss of AC power
  - are the positions most safe and are they well known by the operators in all circumstances?
  - how can the position of a critical valve be changed if the normal drive system is not available?

- at least following valves need to be considered:
  - valves in feed water injection lines
  - steam generator relief valves and safety valves (PWR)
  - depressurization, relief and safety valves of primary circuit
  - containment isolation valves
  - valves in passive cooling systems

Conclusions from "stress tests" - 8

Elevated outage risks in some PWR's during mid-loop operation

- risks during mid-loop operation have been identified in PRA studies but loss of AC power during a mid-loop operation needs special attention
  - evaluation of resources and means to provide decay heat removal
  - procedures and training for operators

Conclusions from “stress tests” - 9)

Dedicated systems to protect containment integrity after core meltdown accident

A common view emerged from ”stress tests” that dedicated containment protection systems have to be installed at all operating plants that have not yet done so.

- The ”severe accident management” based on existing hardware is not any more acceptable.
- Until these days, many plants have based the ”severe accident management” on hardware that is not safety classified, not independent from other plants systems and not qualified for conditions where safety systems could be lost.

Conclusions from ”stress test” - 10

Dedicated systems to protect containment integrity after core meltdown accident (cont.)

Comprehensive and systematic protection of containment integrity should consider all identified threats, and at least the following:

- need to avoid core meltdown in high pressure
- gradual pressure increase inside the containment (due to decay heat)
- containment bottom/wall penetration of the molten core
- hydrogen management
- containment by-pass sequences
- re-criticality of molten core

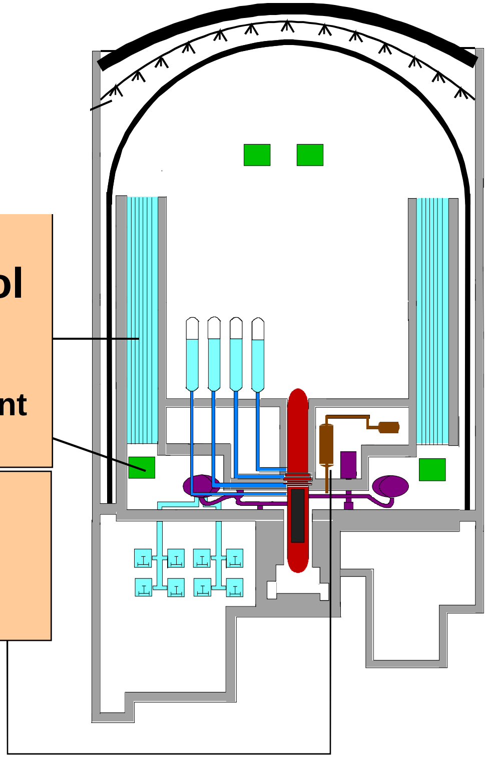
Conclusions from “stress tests” - 11

Dedicated systems to protect containment integrity after core meltdown accident

When designing the dedicated systems for severe accident management, one has to consider the following

- safety classification and the respective quality requirements
- seismic qualification requirements
- level of redundancy
- independence and separation from other plant systems
- protection against external hazards
- dedicated power supply
- dedicated and qualified control instrumentation

Loviisa 1 & 2 plant modifications for severe accidents



3. Hydrogen control

- Ice condenser doors
- Recombinators
- Glow plug improvement

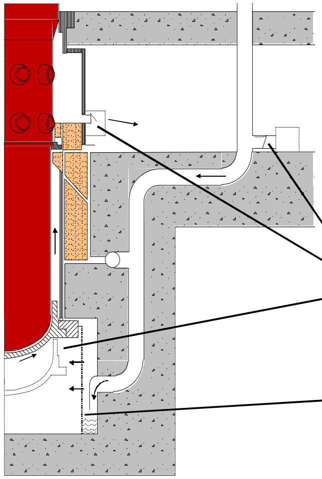
1. Primary system depressurisation

4. Containment pressure control

- External spray

5. Containment isolation

- Manual actuation as back-up
- Monitoring of leak-tightness
- Leakage control



2. Melt retention within pressure vessel

- Inlet valves
- Steam outlet
- Lowering the neutron shield
- Debris removal

6. Severe accidents instrumentation & control

Advanced systems in new plants

Some of the new plants that are under construction have already design features that take properly into account the ”Fukushima issues”:

- long term cooling of reactor core without AC power
- long term decay heat removal that is not relying on primary ultimate heat sink
- protection of reactor containment integrity after potential core meltdown accident

The following slides present examples of such design features.

Passive heat removal systems for Steam Generators and for Containment, Leningrad NPP-2

1 – emergency heat removal tanks (EHRT) outside containment

2 – steam lines

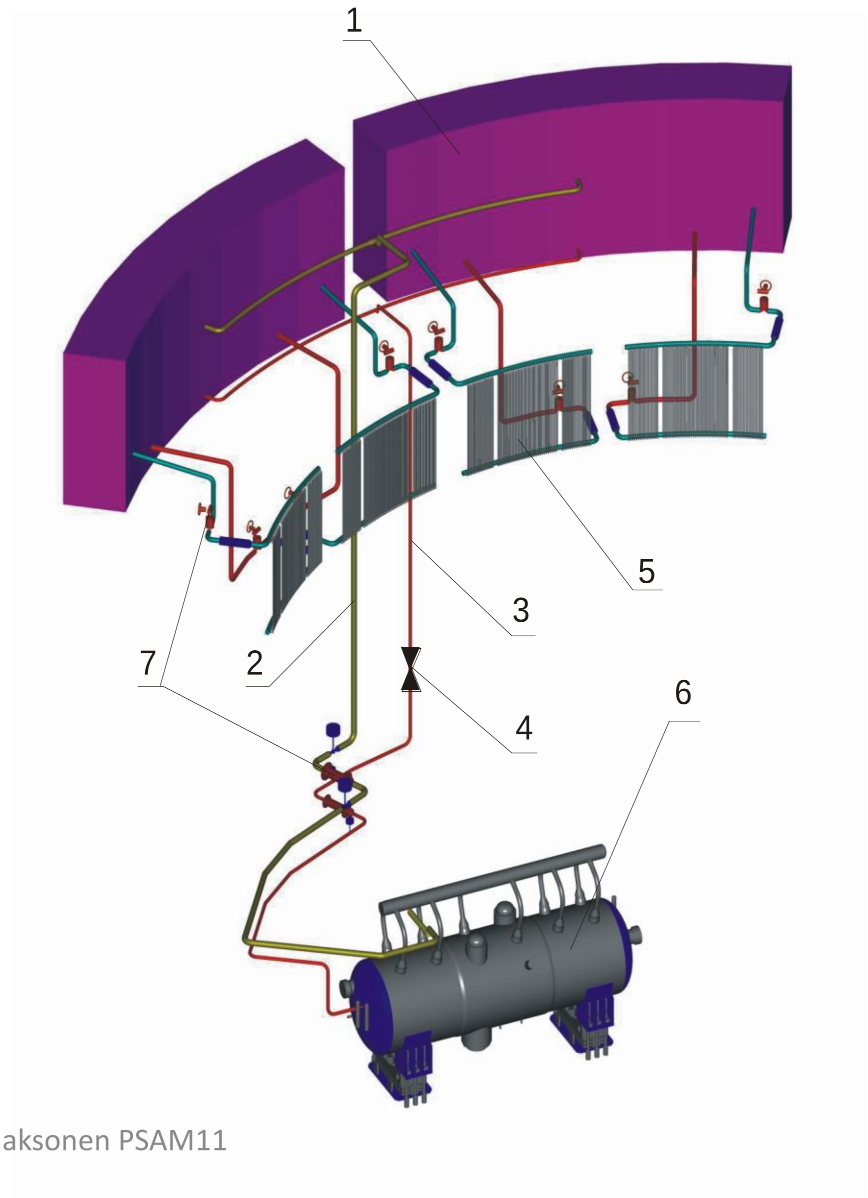
3 – condensate pipelines

4 – PHRS-SG valves

5 – heat exchangers / C-PHRS condensers inside containment

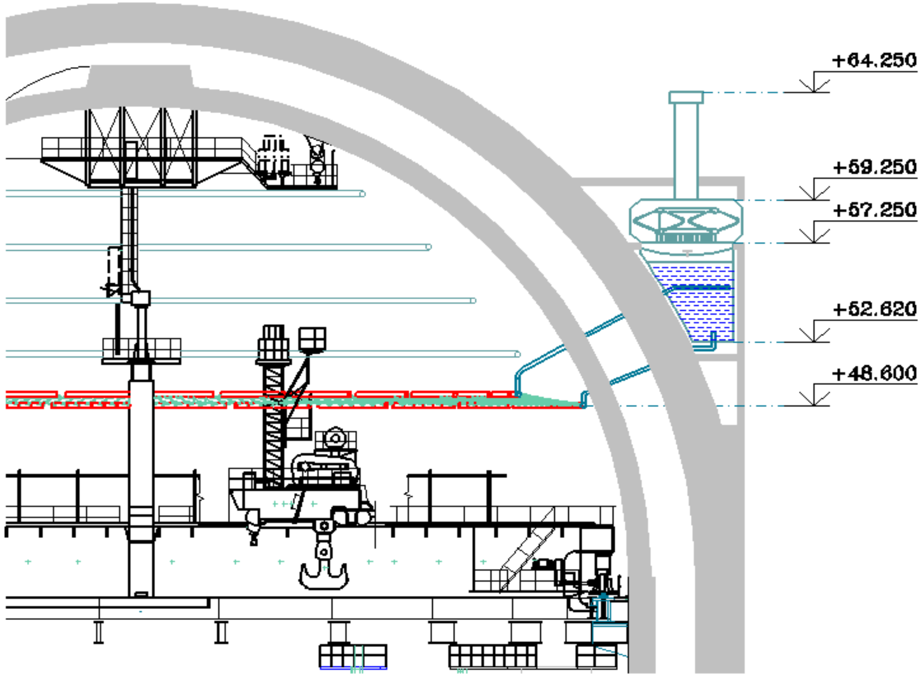
6 – steam generators

7 – cutoff valves



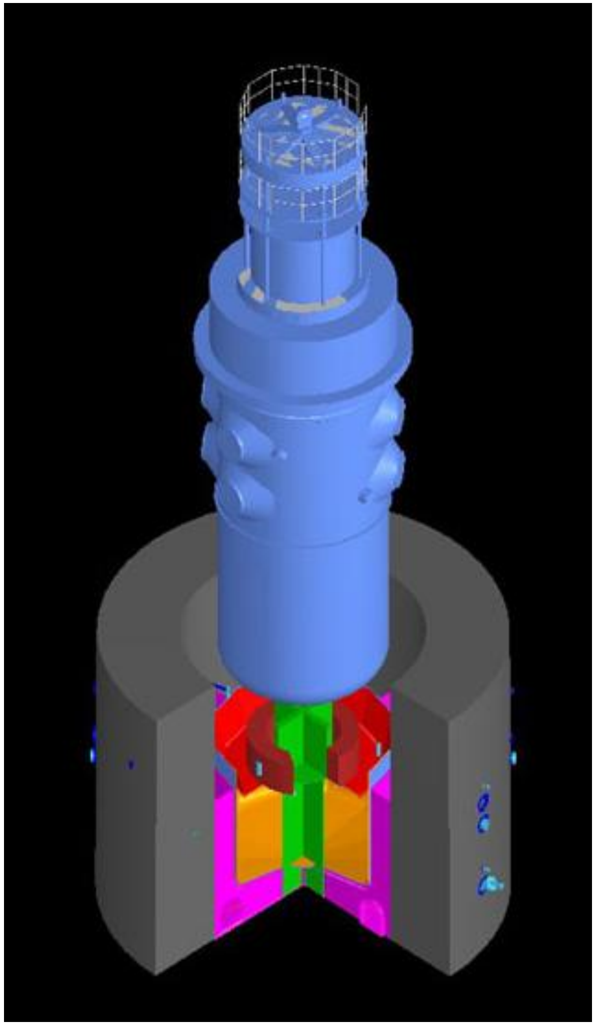
SAM systems to protect containment – 1
Leningrad NPP-2

- Passive Containment Heat Removal System
  - Steam-gas pressure reduction and heat removal from the containment into the environment during BDBA
  - 4x33% redundancy structure
- Containment hydrogen monitoring and removal systems
  - Preventing the formation of explosive mixtures inside the primary containment during DBA and BDBA by passive autocatalytic hydrogen recombiners
  - Hydrogen monitoring system - 2x100% redundancy structure
- Containment iodine binding system:
  - Reduces radioactive releases from the containment during LOCA

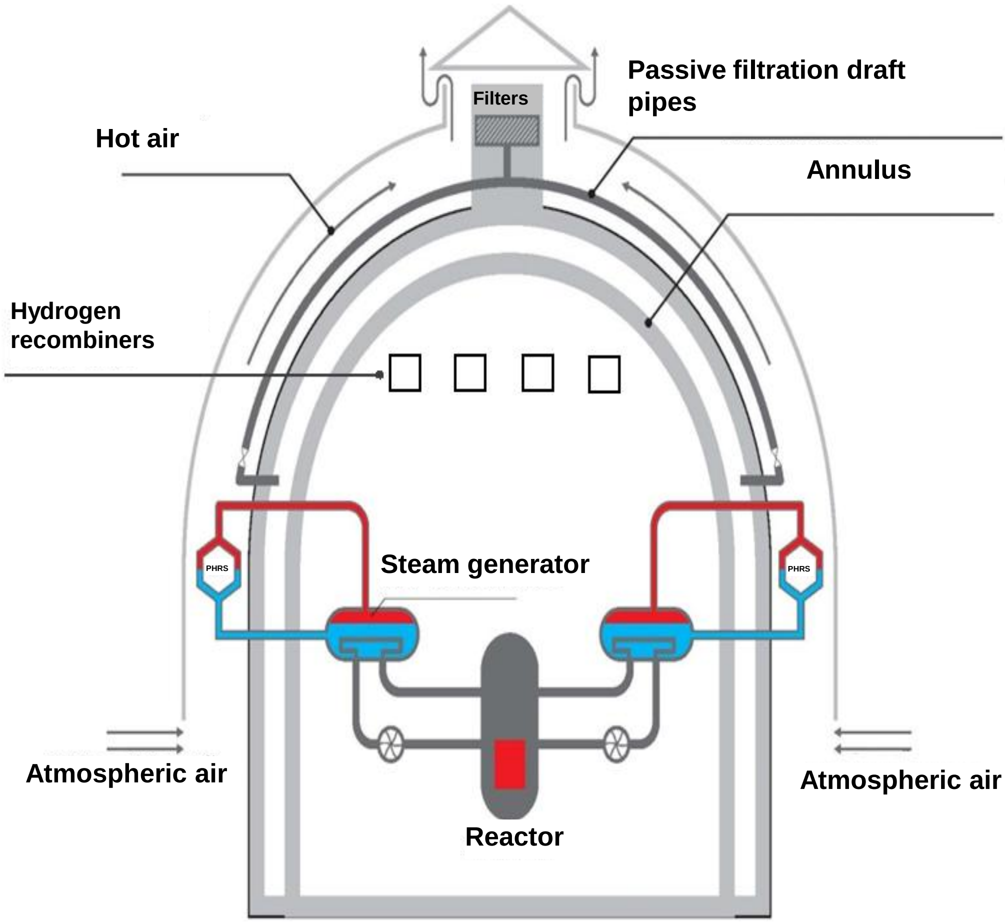


SAM systems to protect containment – 2, Leningrad NPP-2

- Core melt localization device (core catcher)
  - Placed in the reactor vault
  - Reactor vault protected against corium thermomechanical interaction
  - Reception and accommodation of solid and liquid corium components
  - Heat transfer from corium to cooling water surrounding the "core melt pot"
  - Molten core mixes with neutron absorbing material inside the "core melt pot" to ensure subcriticality
  - Decreased hydrogen and radionuclides transfer into the containment



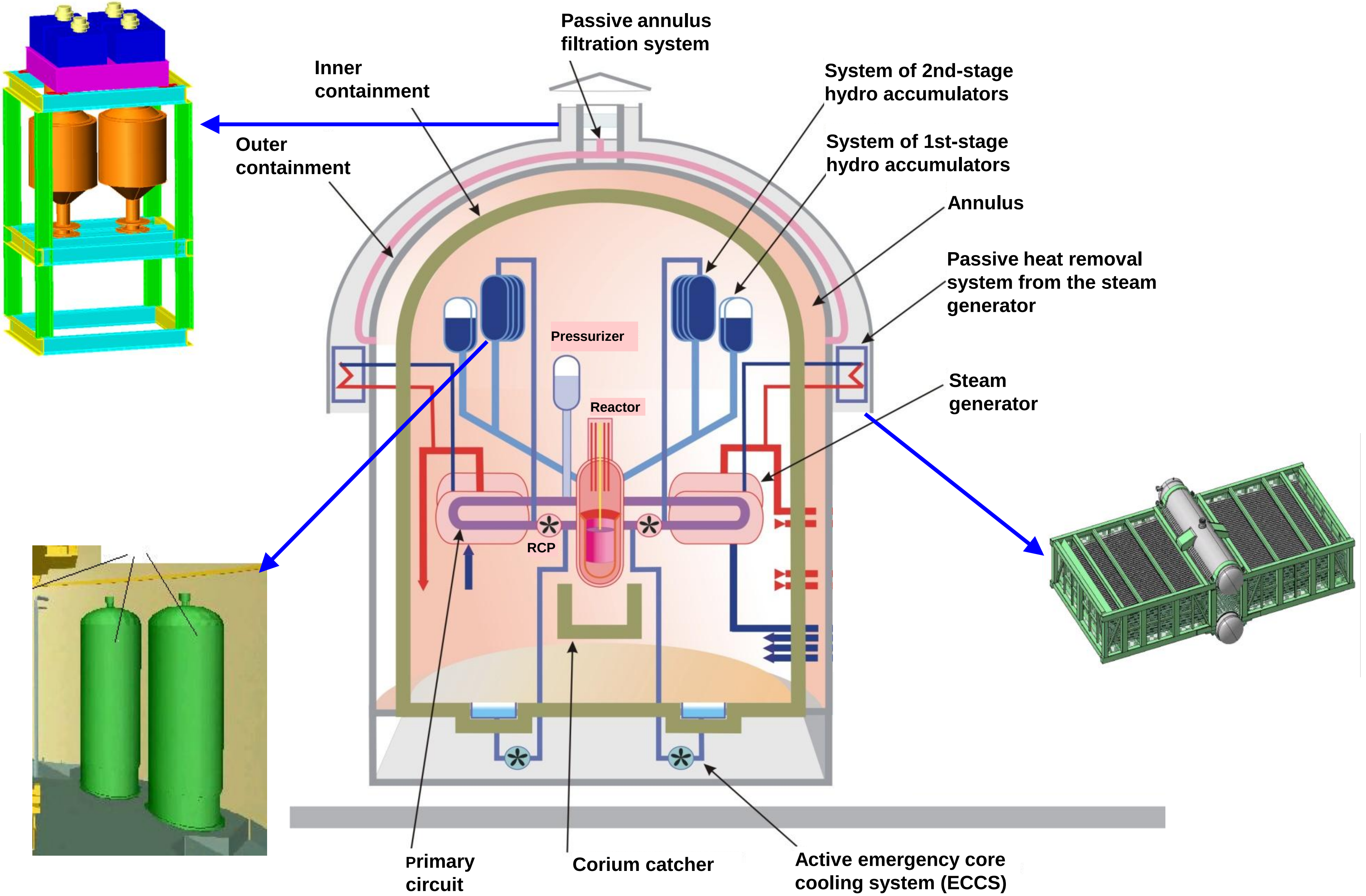
Passive system for decay heat removal from Steam Generators (Novovoronesh-2)



- Separate passive system maintains vacuum in the annulus and filters possible radioactive leaks from inner containment

- The passive heat removal system is intended for long-term removal of the reactor residual heat when there are no sources of power supply; it can operate both with the intact reactor coolant system and when leaks of reactor coolant occur
- The system consists of four independent loops for natural circulation of the secondary coolant: one loop per each circulation loop of the reactor plant
- Each loop has air ducts for passive removing of decay heat to the atmosphere, and direct-action passive devices that control the air flow rate

Passive safety systems of Novovoronesh-2


Passive annulus filtration system
Inner containment
Outer containment
System of 2nd-stage hydro accumulators
System of 1st-stage hydro accumulators
Annulus
Passive heat removal system from the steam generator
Pressurizer
Reactor
Steam generator
RCP
Primary circuit
Corium catcher
Active emergency core cooling system (ECCS)

Conclusions

- Severe accident at Fukushima Daiichi has shown us that we still have a lot to learn from experience
- Insights gained from the accident have already been taken into account in strengthening the safety of old plants with backfits and in extending the scope of issues to be addressed when designing new plants.
- We have good reasons to believe that global nuclear safety has enhanced during the past year but we must not think that we are able to address all risks in advance in our safety analysis.
- Although we are better prepared to face new hazards, future events may take us by surprise again.

Thank you for your attention !