TOPSAFE

Dubrovnik, Croatia, 30.09 - 3.10.2008

TopSafe 2008

Transactions

Dubrovnik, Croatia
30.9. - 3.10.2008

HND

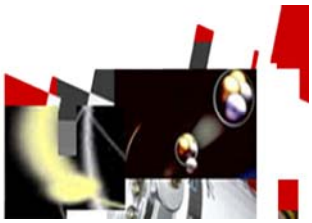
AEN NEA

IAEA International Atomic Energy Agency
Atoms For Peace

European Nuclear Society
Rue Belliard 65
1040 Brussels, Belgium
Phone + 32 2 505 30 54
Fax +32 2 502 39 02
E-mail ens@euronuclear.org
Internet www.euronuclear.org

ISBN 978-92-95064-06-5

These transactions contain all contributions submitted by 30 September 2008.



Design and Safety Issues

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

APPLICATION OF CFD CODES IN NUCLEAR REACTOR SAFETY ANALYSIS

T. Höhne[1], E. Krepper, U. Rohde
Forschungszentrum Dresden- Rossendorf (FZD)
Institute of Safety Research
P.O.B. 51 01 19, D-01314 Dresden, Germany
Email: T.Hoehne@fzd.de

ABSTRACT

Computational Fluid Dynamics (CFD) is increasingly being used in nuclear reactor safety (NRS) analyses as a tool that enables safety relevant phenomena occurring in the reactor coolant system to be described in more detail.

Numerical investigations on single phase coolant mixing in Pressurised Water Reactors (PWR) have been performed at the FZD for almost a decade. The work is aimed at describing the mixing phenomena relevant for both safety analysis, particularly in steam line break and boron dilution scenarios, and mixing phenomena of interest for economical operation and the structural integrity.

On the other hand slug flow as a multiphase flow regime can occur in the cold legs of pressurized water reactors, for instance after a small break Loss of Coolant Accident (SB-LOCA). Slug flow is potentially hazardous to the structure of the system due to the strong oscillating pressure levels formed behind the liquid slugs. For the experimental investigation of horizontal two phase flows, different non pressurized channels and the TOPFLOW Hot Leg model in a pressure chamber was build and simulated with ANSYS CFX.

In a common project between the University of Applied Sciences Zittau/Görlitz and FZD the behaviour of insulation material released by a LOCA released into the containment and might compromise the long term emergency cooling systems is investigated. Whereas in FZD CFD models are developed in Zittau the corresponding experiments are performed.

Moreover, the actual capability of CFD is shown to contribute to fuel rod bundle design with a good CHF performance.

1 INTRODUCTION

The last decade has seen an increasing use of three-dimensional CFD codes to predict steady state and transient flows in nuclear reactors because a number of important phenomena such as pressurized thermal shocks, coolant mixing, and thermal striping cannot be predicted by traditional one-dimensional system codes with the required accuracy and spatial resolution. CFD codes contain models for simulating turbulence, heat transfer, multi-phase flows, and

[1] Corresponding Author

chemical reactions. Such models must be validated before they can be used with sufficient confidence in NRS applications. The necessary validation is performed by comparing model results against measured data. However, in order to obtain a reliable model assessment, CFD simulations for validation purposes must satisfy strict quality criteria given in the Best Practice Guidelines (BPG).

Our partner for CFD code qualification is ANSYS CFX [1], which is one of the leading CFD codes worldwide. Based on this partnership the models developed are implemented into the code and thus contribute to the code qualification. The following topical issues, where CFD calculations have been performed, will be briefly discussed in the paper:

1. Coolant Mixing
2. Horizontal Stratified Flow Phenomena in the Hot Leg of PWR
3. Debris Transport Phenomena in multidimensional water flow
4. Sub-cooled boiling - Application to fuel rod bundle safety assessment

The material presented has been prepared by FZD partly under the sponsorship by the European Commission and the German Government (BMWi).

2 COOLANT MIXING

Numerical investigations on coolant mixing in Pressurized Water Reactors (PWR) have been performed by other institutes and at the FZD for more than a decade [2-9]. The work was aimed at describing the mixing phenomena relevant for both safety analysis, particularly in steam line break and boron dilution scenarios, and mixing phenomena of interest for economical operation and the structural integrity.

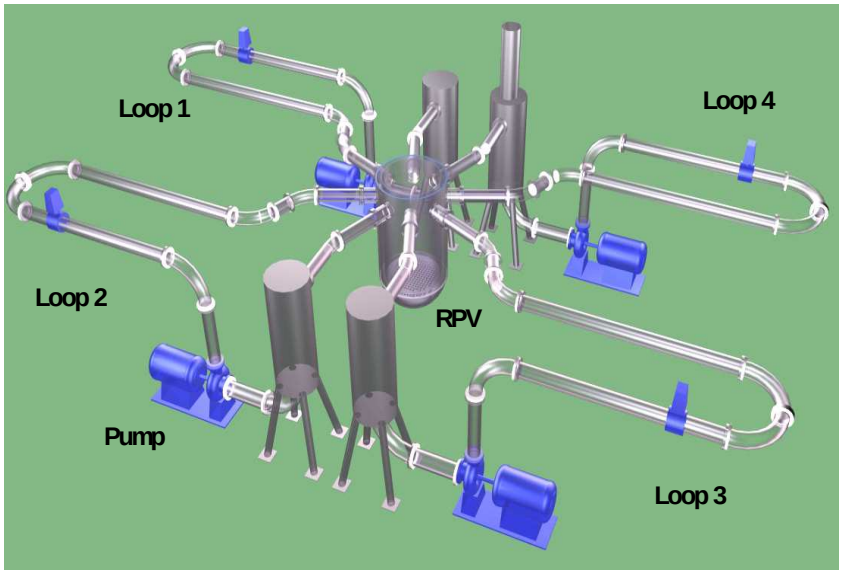


Fig. 1 Scheme of ROCOM

With the set-up of the ROCOM [8,9] test facility (Fig. 1), a unique data base has been created to be used for the validation of Computational Fluid Dynamics (CFD) codes for the application to turbulent mixing in nuclear reactors. Benchmark problems based on selected experiments were used to study the effect of different turbulent mixing models under various flow conditions, to investigate the influence of the geometry, the boundary conditions, the grid and the time step in the CFD analyses. In doing the calculations the Best Practice Guidelines for nuclear reactor safety calculations have been followed [5].

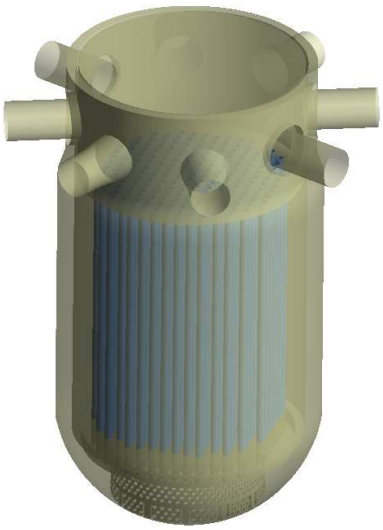


Fig. 2 Grid model of ROCOM

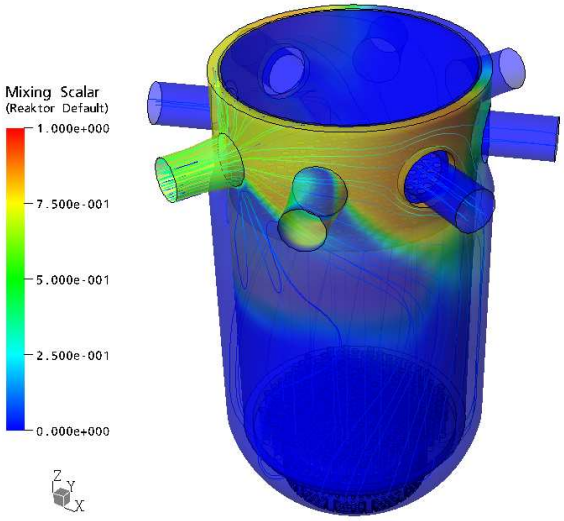
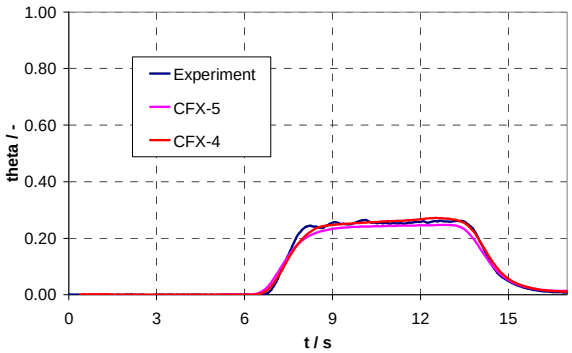
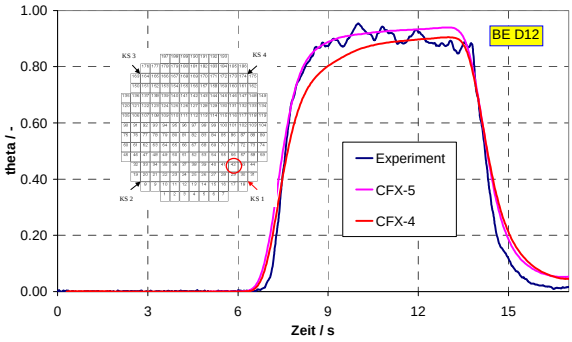


Fig. 3 Pump Start-up



a) Time dependent global averaged mixing scalar at the core inlet



b) Time dependent local mixing scalar at the core inlet, position near the wall

Fig. 4 Comparison of the measured and calculated mixing scalar (steady state flow field, 185 m³/h)

A selection of the performed work is described in [5]:

- stationary and transient flow and mixing studies of the coolant in the PWR Konvoi and the ROCOM test facility with CFX-4 and ANSYS CFX-5-11 during oron dilution transients (start-up of the first coolant pump), Fig. 3
- main steam line break scenarios, Fig. 4
- density driven flows after an inherent dilution with ECC injection (generic experiments at the ROCOM test facility), [7]

The CFD calculations were carried out with the CFD-codes CFX-4 and CFX-5. Calculations were performed on the FZD LINUX cluster (operating system: Linux Scientific 64 bit, 32 AMD Opteron Computer Nodes, node configuration: 2 x AMD Opteron 285 (2.6 GHz, dual-core), 16 GB Memory). Using the block-structured code CFX-4 internals were modeled using the porous media approach and additional body forces. Sensitivity studies showed, that the k-ε turbulence model together with the higher order HYBRID discretization scheme give the best results. Within ANSYS CFX-5-11 it was possible, to model all internals of the RPV of ROCOM in detail. A production mesh with 7 Million elements was generated (Fig. 2). Detailed and extensive grid studies were made. It was shown, that a detailed model of the perforated drum in CFX-5 gives the best agreement with the experiments. Sensitivity studies

showed that the SST turbulence model and the automatic wall functions together with higher order discretization schemes should be used if possible (further details see [5]).

In the case of stationary mixing, the maximum value of the averaged mixing scalar at the core inlet was found in the sector below the inlet nozzle, where the tracer was injected (Fig. 4). The mixing scalar is a dimensionless representation of the tracer concentration in the experiment or boron concentration/fluid temperature in reality. There is a good agreement between the measurement and the CFD calculations, especially in the averaged global mixing scalar at the core inlet. At the local position of the maximum mixing scalar the time course of the measurement and the calculations is also in good agreement (see Fig. 4).

At the start-up case of one pump due to a strong impulse driven flow at the inlet nozzle the horizontal part of the flow dominates in the downcomer (Fig. 3). The injection is distributed into two main jets; the maximum of the tracer concentration at the core inlet appears at the opposite part of the loop where the tracer was injected [6].

3 CFD-SIMULATIONS FOR STRATIFIED FLOWS

Slug flow as a multiphase flow regime can occur in the cold legs of pressurized water reactors, for instance after a small break Loss of Coolant Accident (SB-LOCA). Slug flow is potentially hazardous to the structure of the system due to the strong oscillating pressure levels formed behind the liquid slugs. It is usually characterized by an acceleration of the gaseous phase and by the transition of fast liquid slugs, which carry out a significant amount of liquid with high kinetic energy. For the experimental investigation of air/water flows, a horizontal channel with rectangular cross-section was build at Forschungszentrum Dresden-Rossendorf (FZD) [10,11]. Experimental data were used to check the feasibility to predict the slugging phenomenon with the existing multiphase flow models build in ANSYS CFX. Further it is of interest to prove the understanding of the general fluid dynamic mechanism leading to slug flow and to identify the critical parameters affecting the main slug flow parameters (like e.g. slug length, frequency and propagation velocity; pressure drop). For free surface simulations, the inhomogeneous multiphase model was used, where the gaseous and liquid phases can be partially mixed in certain areas of the flow domain. In this case the local phase de-mixing after a gas entrainment is controlled by buoyancy and inter-phase drag and is not hindered by the phase interface separating the two fluids. The fluid-dependent shear stress transport (SST) turbulence models were selected for each phase. Damping of turbulent diffusion at the interface has been considered.

The picture sequence (see Fig. 5) shows comparatively the channel flow in the experiment and in the corresponding CFD calculation. In both cases, a slug is developing. The tail of the calculated slug and the flow behind it is in good agreement with the experiment. The entrainment of small bubbles in front of the slug could is not be observed in the calculation. However, the front wave rolls over and breaks. This characteristic of the slug front is clearly to be seen in Fig. 5. It is created due to the high air velocity.

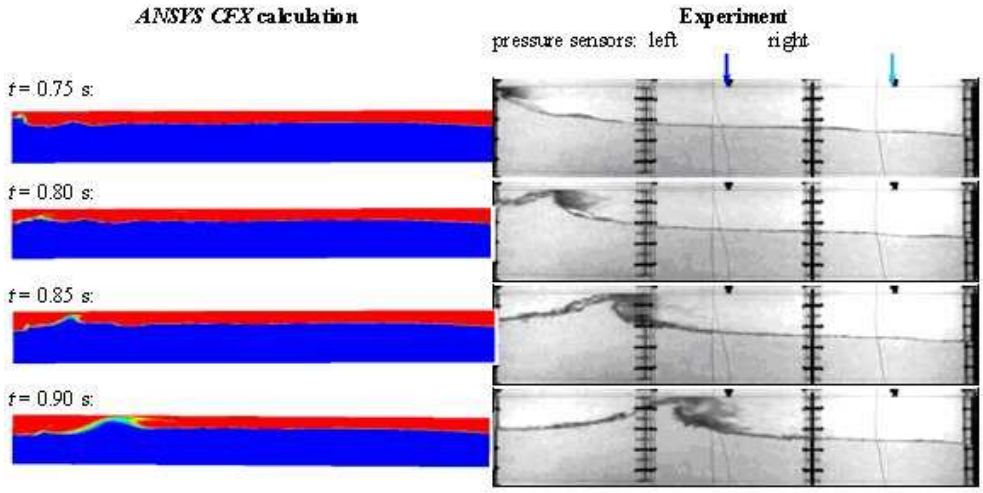


Fig. 5 Comparative picture sequence of the recalculated slug

Furthermore, pre-test calculations CFD were carried out to simulate a slug current in a real geometry and under parameters relevant for the reactor safety. These calculations were performed for a flat model of the hot leg which represents the geometry of a 1:3 scaled Konvoi reactor (Fig. 6). Steam and water were taken as a model fluid with a pressure of 50 bar and the accompanying saturation temperature of 264 C. To be able to perform the experiments at high pressure, the whole hot leg model is put into a pressure chamber.

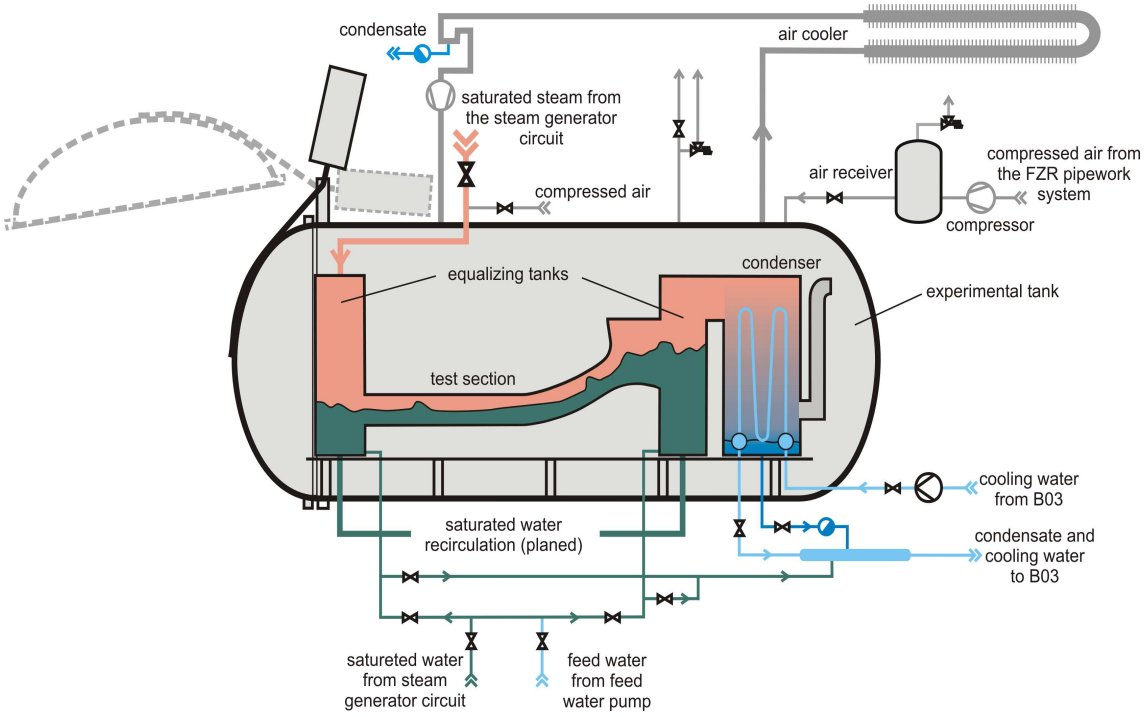


Fig. 6 Scheme of the Hot Leg Model in the pressure chamber

The pretest calculations began with a partial water-full channel and quiescent gas phase. At the beginning of the steam supply the surface of the still standing water phase rises in the direction of the steam generator simulator. This effect is caused by the momentum exchange between flowing out steam and quiescent water. The calculation shows spontaneous waves

which grow in the elbow to slugs originate in the horizontal part of the hot leg model. The Fig. 7 shows this state as a snapshot of the results of the calculations.

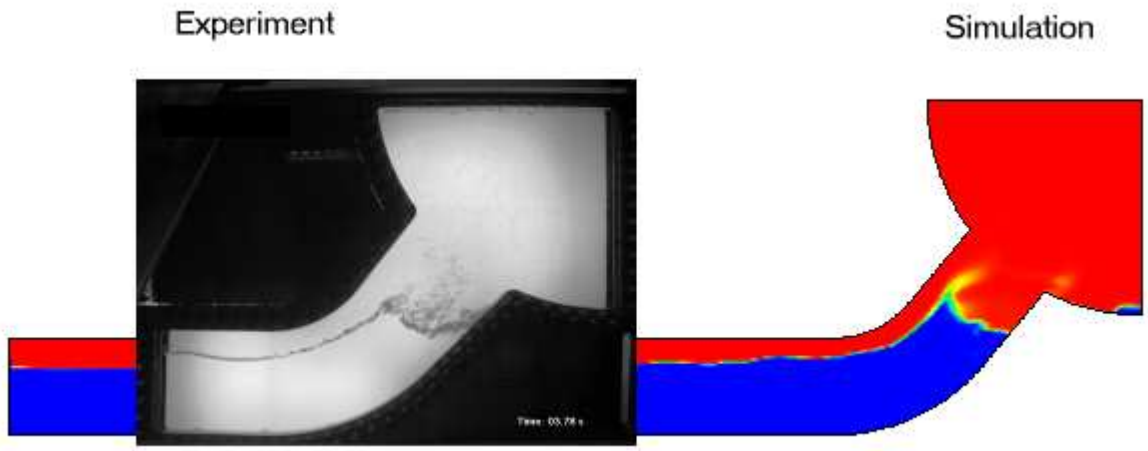


Fig. 7 Snapshot of the results of the calculations

4 INVESTIGATIONS OF INSULATION FIBER TRANSPORT PHENOMENA IN WATER FLOW

The investigation of insulation debris generation, transport and sedimentation becomes more important with regard to reactor safety research for PWR and BWR, when considering the long-term behaviour of emergency core coolant systems during all types of loss of coolant accidents (LOCA). The insulation debris released near the break during a LOCA incident consists of a mixture of disparate particle population that varies with size, shape, consistency and other properties. Some fractions of the released insulation debris can be transported into the reactor sump, where it may perturb/impinge on the emergency core cooling systems [12-15].

Open questions of generic interest are the fibre transport in an aqueous flow, the sedimentation of the insulation debris in a water pool, its possible re-suspension and transport in the sump water flow and the fibre load on strainers and the corresponding pressure drop.

A joint research project on such questions is being performed in cooperation of the University of Applied Sciences in Zittau/Görlitz and the Forschungszentrum Dresden-Rossendorf. The project deals with the experimental investigation and the development of CFD models for the description of particle transport phenomena in coolant flow. While the experiments are performed at the University Zittau/Görlitz, the theoretical work is concentrated at Forschungszentrum Dresden-Rossendorf. Details were published by Krepper et al. 2008 [16].

The main topics of the project are

- Primary particle constitution: Experiments are performed to blast blocks of insulation material by steam under the thermal hydraulic conditions to be expected during a LOCA incident (i.e. at pressures up to 11 MPa). The material obtained by this method is then used as raw material for further experiments.

- Sedimentation of the fibres: The transport behaviour of the steam-blasted material is investigated in a water column by optical high-speed video techniques. The sinking velocities of the fibres are then used to derive the drag coefficients and other physical properties of the modelled fibre phase, which is necessary for the implementation of an adequate CFD simulation. Fig's. 7 and 8 show the measured distribution of sinking velocities and particle size for the insulation material MD2.

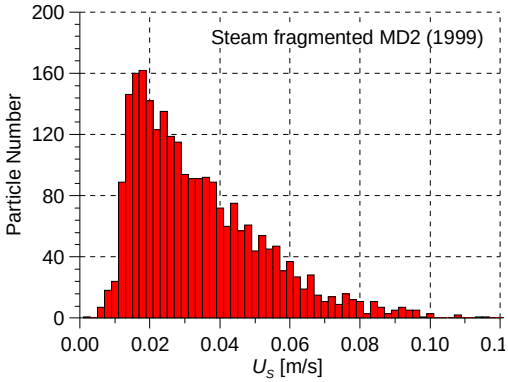


Fig. 8 Distributions of the sinking velocities

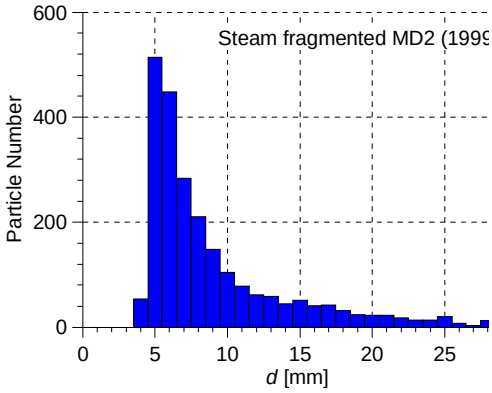
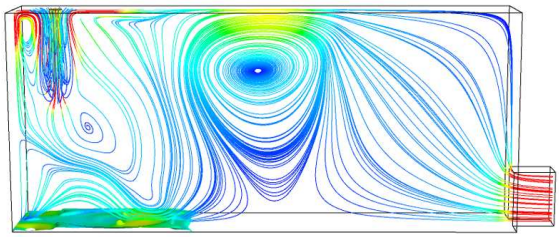


Fig. 9 Distributions of the particle size

- Transport of fibres in a turbulent water flow: For these investigations, a narrow channel with a racetrack type configuration was used with defined boundary conditions. Laser PIV measurements and high-speed video were used for the investigation of the water flow-field and the fibre concentration. Besides the drag acting on the particles, the turbulent dispersion force plays an important role in determining the momentum exchanged between the water and the fibrous phase.
- Deposition and re-suspension of fibres: The deposition and re-suspension behaviour at low velocities was investigated by the same techniques and the narrow racetrack channel. Except that, in this case obstacles were inserted into the channel to change locally the flow regime. The experiments are designed to work with laser PIV measurement and high-speed video to investigate the fibre agglomeration in the obstacle region. CFD approaches consider the influence of the fibre material on the mixture viscosity and the dispersion coefficient on the transport of the solids.
- Effect of strainers: A test rig was used to study the influence of the insulation material loading on the pressure difference observed in the region of the strainers. A CFD model was developed that uses the approach of a porous body. The calculated differential pressure considers compactness of the porous fibre layer. Correlations from the filter theory known in chemical engineering are adapted to the certain fibre material properties by experiments. This concept enables the simulation of a partially blocked strainer and its influence on the flow field.
- Behaviour of a plunging jet in a large pool and impact on fibre transport: By using high-speed video and laser (LDA and PIV) measurements, the progression of the momentum by the jet in the pool is investigated. Of special importance is the role that entrained gaseous bubbles play on disturbing the fluid and potentially influencing the fibre sedimentation and re-suspension. Fig. 10 shows

that under certain flow conditions the entrained air causes a swirl, which transports the injected fibres below the jet. In Fig. 11 the fibre mass accumulated in the tank dependent on the inlet jet velocity is shown. In the case of only 1.5 m/s a left turning swirl was found and the fibre material was transported directly through the tank. For the other case of 5 m/s jet velocity a right turning swirl occurred (s. Fig. 10), which deposited the fibres below the jet and accumulates fibres for longer time in the tank (s. Fig. 11)



deposited fiber material

Fig.10 Water flow field induced by the entrained air

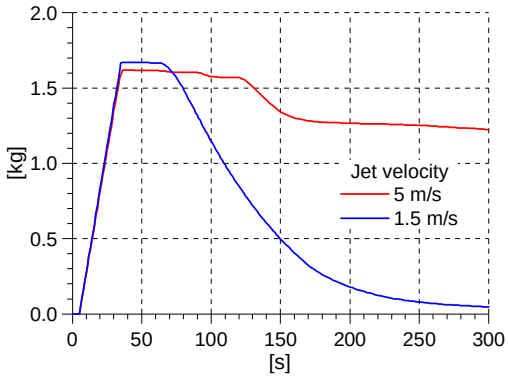


Fig. 11 Accumulated fibre mass dependent on the inlet velocity

5 CFD-CALCULATION OF A HOT CHANNEL OF A FUEL ROD BUNDLE

Boiling is a very effective heat transfer mechanism. Liquid cooling including phase transfer very large heat fluxes can be established. Exceeding the critical heat flux, however, the heat transfer coefficient suddenly decreases, the temperatures increases leading to possible damaging of construction material. The critical heat flux depends not only on fluid properties but also on flow conditions and on geometric circumstances [17].

For the case of a fuel rod, the permissible heat flux can be influenced by the geometrical design. Especially the spacer grids equipped with mixing vanes play an important role to increase the permissible heat flux. The verification of design improvements and their influence on the critical heat flux require very expensive experiments. Therefore, the supplementation ore even the replacements of expensive experiments by numerical analyses are of relevant interest in fuel assembly design.

Although the CFD modelling of critical heat flux is not yet state of the art, the simulations shall demonstrate the capability of CFD supporting the fuel assembly design. In the calculations only sub-cooled boiling is simulated, which is here considered as a preliminary phenomenon towards departure of nucleate boiling (DNB). DNB might occur at the thermal hydraulic conditions of a PWR. A situation was investigated, when at full power and full pressure the inlet temperature rise caused undesired boiling in the channel.

A section of coolant channel between two spacer grids having a length of z=0.5 m was simulated. The grid represents a sub-channel between 4 rods having a diameter of 9 mm and a rod distance of 12.6 mm. The thermal hydraulic and transport water properties were set for a pressure of 15.7 MPa, typical for PWR conditions. The heat flux at the rod surface was

assumed to be $1.0 \cdot 10^6$ W/m^2 and the sub-cooling at the inlet was set to 12 K expecting the generation of vapour in the simulated section. The axial water velocity was set to V_Z = 5 m/s. The faces at the low and high x respective at low and high y were simulated as periodic boundary conditions, assuming that the channel is infinitely extended in these four directions.

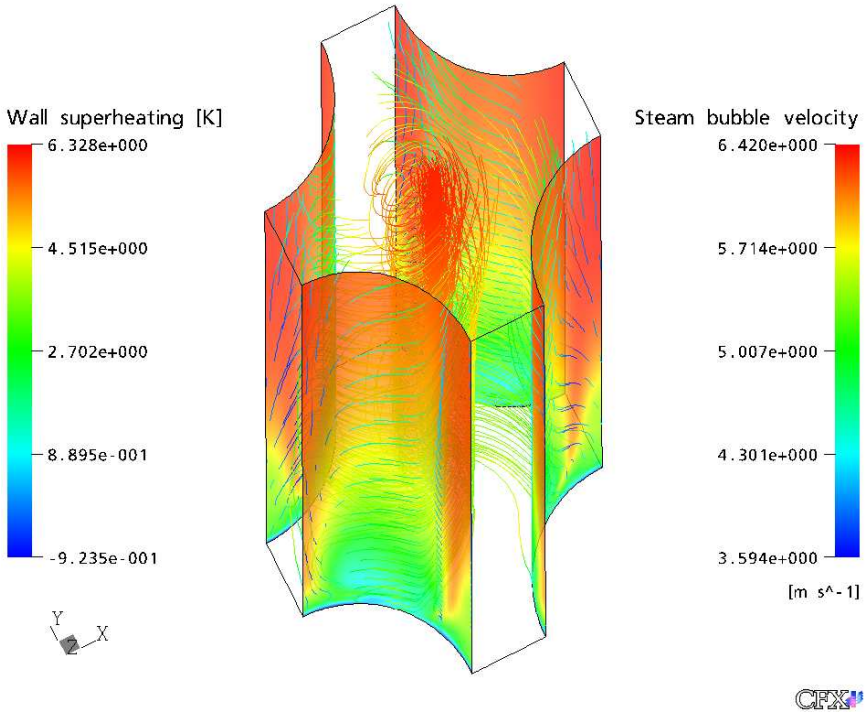


Fig. 12 Hot channel vapour flow streamlines and rod surface temperatures

The figure shows the flow condition in the considered channel section (axially shortened presentation). The mixing vanes generate a strong swirl in the actual calculation given as inlet condition. They are not modelled in this calculation, but a swirl was introduced into the flow as boundary condition at the inlet of the channel section. The overall vapour generation can be decreased by the swirl effect.. Due to the centrifugal force, the heavier fluid component - the water - is pushed outwards, whereas a large amount of the lighter component - the vapour - is accumulated in the centre of the channel. The streamlines show vapour bubbles moving in the centre of the channel caused by the centrifugal forces. The colours represent the temperatures of the metal surface. Their distribution can be used as qualitative criterion of the effect of a mixing vane. Further details were published by Krepper et al. (2007), [18].

CONCLUSION

Computational Fluid Dynamics (CFD) is increasingly being used in nuclear community to model safety relevant phenomena occurring in the reactor coolant system. For this reason the long-term objective of the activities of the FZD R&D program lies in the development of theoretical models for basic phenomena of transient, three-dimensional single and multiphase systems. Local geometry independent models for mass, momentum, heat transfer and scalar transport are developed and validated. Such models are an essential pre-condition for the application of complex fluid dynamic codes to the modelling of flow related phenomena in nuclear facilities. Our partner for CFD code qualification is ANSYS. Their code CFX is one of the leading CFD codes worldwide. Based on this partnership the models developed are implemented into the code and thus contribute to the code qualification.

ACKNOWLEGEMENT

The work reported about in this paper was supported by the EU within the FLOMIX Project and the German Federal Ministry of Economics and Labour, project numbers 150 1265, 1501270 and 150 1307.

REFERENCES

[1] ANSYS CFX User Manual. ANSYS-CFX. 2008.

[2] D. Alvarez et al. 1992. Three dimensional calculations and experimental investigations of the primary coolant flow in a 900 MW PWR vessel. Proc. NURETH-5, vol. II, pp. 586-592.

[3] Alavyoon, B. Hemström, Andersson, R. Karlsson 1995. Experimental and computational approach to investigating rapid boron dilution transients in PWRs. CSNI Specialist Meeting on Boron Dilution Reactivity Transients, State College, Pennsylvania, USA, October 18-20, 1995.

[4] B. Woods 2001. UM 2x4 Loop Experimental Findings on the Effect of Inertial and Buoyancy forces on Annular Flow Mixing for Rapid Boron Dilution Transients. Ph.D. Thesis, University of Maryland, USA, 2001

[5] Rohde, U., Höhne, T., Kliem, S., Hemström, B., Scheuerer, M., Toppila, T., Aszodi, A., Boros, I., Farkas, I., Muehlbauer, P., Vyskocil, V., Klepac, J., Remis, J., Dury, T., Fluid mixing and flow distribution ín a primary circuit of a nuclear pressurized water reactor – Validation of CFD codes, Nuclear Engineering and Design 237(2007)15-17, 1639-1655

[6] Cartland Glover, G. M., Höhne, T., Kliem, S., Rohde, U., Weiss, F.-P., Prasser, H.-M., Hydrodynamic phenomena in the downcomer during flow rate transients in the primary circuit of a PWR, Nuclear Engineering and Design 237(2007)7, 732-748

[7] Höhne, T., Kliem, S., Bieder, U., Modeling of a buoyancy-driven flow experiment at the ROCOM test facility using the CFD-codes CFX-5 and TRIO_U, Nuclear Engineering and Design 236(2006)12, 1309-1325

[8] Rohde, U., Kliem, S., Höhne, T., Karlsson, R., Hemström, B., Lillington, J., Toppila, T., Elter, J., Bezrukov, Y., Fluid mixing and flow distribution in the reactor circuit - Part 1: Measurement data base, Nuclear Engineering and Design, 235(2005), 421-443

[9] Prasser, H.-M., Grunwald, G., Höhne, T., Kliem, S., Rohde, U., Weiss, F.-P., Coolant mixing in a PWR - deboration transients, steam line breaks and emergency core cooling injection - experiments and analyses, Nuclear Technology 143 (2003) 37-56

[10] Vallee, C., Höhne, T., Prasser, H.-M., Sühnel, T., Experimental investigation and CFD simulation of horizontal air/water slug flow, Kerntechnik 71(2006)3, 95-103

[11] Höhne, T.; Vallee C.; Prasser, H.-M., Experimental and numerical prediction of horizontal stratified flows. International Conference on Multiphase Flow ICMF 2007, 09.-13.07.2007, Leipzig, Deutschland, paper S5_Tue_C_23

[12] Knowledge Base for Emergency Core Cooling System Recirculation Reliability, NEA/CSNI/R(95)11

[13] Knowledge Base for the Effect of Debris on Pressurized Water Reactor Emergency Core Cooling Sump Performance, NUREG/CR-6808; LA-UR-03-0880

[14] Knowledge Base for Strainer Clogging -- Modifications Performed in Different Countries Since 1992, NEA/CSNI/R(2002)6

[15] Debris impact on Emergency coolant recirculation, Workshop Albuquerque, NM, USA February 2004, Proceedings OECD 2004 NEA No. 5468

[16] Krepper, E.; Cartland-Glover, G.; Grahn, A.; Weiss, F.-P.; Alt, S.; Hampel, R.; Kästner, W.; Seeliger, A., 2008. Numerical and experimental investigations for insulation particle transport phenomena in water flow, *Annals of Nuclear Energy* 35 (2008), 1564–1579

[17] Anglart, H., Nylund, O., Kurul, N. and Podowski, M.Z., "CFD prediction of flow and phase distribution in fuel assemblies with spacers," Nucl. Eng. Des., vol. 177, pp. 215-228, 1997

[18] Krepper, E., Koncar, B., Egorov, Y., 2007, Modelling of subcooled boiling – concept, validation and application to fuel assembly design, *Nuclear Engineering and Design* 237 716-731

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

SAFETY IMPROVEMENTS IN MOCHOVCE 3&4 DESIGN

Eugenio Bianco, Federico Peinetti
ENEL/Slovenské Elektrárne
Mochovce Nuclear Power Plant Units 3&4 (Slovakia)
eugenio.bianco@enel.it, federico.peinetti@enel.it

Ivo Tripputi
SOGIN
Via Torino, 6 – 00184 Roma (Italy)
tripputi@sogin.it

ABSTRACT

In 2006 ENEL became the majority shareholder of Slovénske Elektrárne (SE) and after the completion of a feasibility study it was decided to complete Mochovce Nuclear Power Units 3 and 4. The Basic Design was revised to include additional safety improvements; the Preliminary Safety Analysis Report was updated accordingly. Before the start of the Basic Design revision process, ENEL/SE decided to establish an independent Safety Board composed of six outstanding nuclear safety experts to supervise the development of the Basic Design revision with specific reference to issues of primary interest from the point of view of nuclear safety.
In the following the major safety improvements and the main conclusions drawn by the Safety Board are presented.

1 INTRODUCTION

The construction of Mochovce Units 1 and 2 started in November 1982. Construction of Mochovce Units 3 and 4 started three years later, in 1985 (a view of the site is provided in Fig. 1).

In 1992 the construction works were suspended due to lack of financial resources. In 1996, construction of Units 1 and 2 was resumed. Unit 1 was connected to the grid in 1998, and Unit 2 in 2000.

Since suspension of works, the civil structures and mechanical components of Mochovce 3&4 were put under a preservation program which was concurred with the Slovak Nuclear Regulatory Authority (NRA).

In 2006, ENEL became the majority shareholder of Slovenské Elektrárne (SE) and after the completion of a feasibility study it was decided to proceed with the completion of Mochovce Units 3&4.

Fig. 1: View of the Units 1&2 (on the right) and of the Units 3&4, with the cooling towers of the Units 3&4 (on the left).

In the mean time a large amount of safety upgrades had been implemented in other Nuclear Power Plants of this type (VVER 440/213) and, considering the evolution of the design criteria for the current-generation reactors, it was agreed with the Nuclear Regulatory Authority to implement additional major safety improvements in the design of Mochovce 3&4. The Basic Design and the Preliminary Safety Analysis Report of Mochovce 3&4 were therefore revised.

The safety-improvement program took into account the current international safety requirements (IAEA, WENRA [1], [2]), the recommendations of all international missions carried out in Mochovce 1&2 and, in general, the experience feedbacks from similar nuclear power plants currently in operation in several countries (Slovakia, Czech Republic, Hungary, Ukraine, Finland and Russia). In addition, further consideration was given to the results of research and experimental activities carried out in the last fifteen years on severe accidents and on the VVER 440/213 pressure-suppression containment.

Many important safety improvements were implemented, including those to cope with severe accidents and related effects on containment integrity. Several other important modifications were introduced, such as the improvement of the reliability of the power supply during accident conditions. Furthermore, a state-of-the-art I&C has been specified.

An expert Board ("*Safety Board*") was established in 2006 by ENEL as an independent body to assess the safety aspects during the execution of the revision of the Basic Design of Mochovce 3&4. The Safety Board was composed of 6 peer members internationally recognized as leading experts in nuclear power plant safety (Prof. Boeck from Austria, Mr Lipar from Slovakia, Ms Carnino from France, Prof. Birkhofer from Germany, Prof. Bolshov from Russia and Prof. Cumo from Italy), with the technical support of SOGIN.

2 MAJOR SAFETY IMPROVEMENTS FOR SEVERE ACCIDENTS

The design work performed on Mochovce 3&4 took advantage of the results of extensive studies and experiences of several reactors of the same design.

In this paper, the features already identified by IAEA to be implemented in this type of plants and already largely included in most or all plants are not described. All these safety features along with all the safety features already implemented in Bohunice V2 Nuclear Power Plant and in Mochovce Units 1&2 have been implemented also in the design of Mochovce 3&4.

This paragraph mainly focuses on the additional improvements which were included in the design.

2.1 Severe Accident Prevention

The improvements implemented for the prevention of core melt sequences proved to be very effective, further reducing the Core Damage Frequency (CDF) to less than 1E-5 per year, as recommended by INSAG [3] for new plants.

The most important preventive measures are:

1. interconnection of all the Units at the 6 kV level (non–safety switchboards) that allows, when needed, to feed the auxiliaries from another Units. This helped reduce significantly the contribution to the CDF.
2. implementation of several measures, such as the possibility of manual interconnection between the safety divisions of different Units at the 6 kV level, to avoid the evolution of station black-out to severe accident.
3. improvements in the design of safety and safety-related systems (e.g., HP and LP ECCS, Service Water System) aimed at increasing the reliability of these systems by incorporating the operating experience feedbacks of Mochovce 1&2 and Bohunice NPPs.

It has to be remarked that, within the revision of the Basic Design, the impact of hardware modifications on the Probabilistic Safety Assessment (PSA) figures has been fully evaluated while the impact of human error on the CDF has not been completely assessed. Ad-hoc operating and emergency procedures are meant to be used to evaluate the impact of human error, which will be prepared during the development of the Detailed Design. For this reason, in the first design phase (Basic Design revision) the results of the human reliability analysis already carried out for Mochovce 1&2 has been preliminarily used for Mochovce 3&4.

A significant reduction of the full-power contribution to the total CDF has been already evaluated for Mochovce 3&4 with respect to Mochovce 1&2, while a meaningful estimation of the impact of the proposed design modifications on the low-power/shut-down contribution to the CDF will be done later. Nonetheless, it is expected that one of the important results of the safety-improvement program of Mochovce 3&4 will be to obtain a PSA being well balanced between full-power and shut-down and with no initiating events having an excessive impact on the CDF.

2.2 Severe Accidents Mitigation

Particular emphasis has been given to severe accidents mitigation. Severe accidents have to be taken into account in the design and in the licensing documents as required by the Slovak Law in compliance with recommendations by IAEA Safety Standards.

The main elements of the severe accident mitigation strategy are:

1. Primary circuit depressurization. To avoid scenarios of high-pressure vessel failure, which may pose a serious threat to containment integrity, an additional 80 mm diameter pipe has been designed to be connected to the pressurizer relief

and safety valves header. This pipe shall be provided with two valves in series which shall be operated according to emergency operating procedures. The steam shall be discharged into the containment; pressure will be suppressed by the bubbler condenser. In this way the pressure inside the Reactor Pressure Vessel will reach values below 2 MPa in a few minutes, thus excluding scenarios of direct containment heating.

2. Retention of corium inside the Reactor Pressure Vessel by flooding the reactor cavity and removing the heat through the reactor vessel wall (eliminating any ex-vessel corium interaction with water, containment atmosphere and reinforced concrete structures).
3. Limitation of hydrogen concentration by self-actuated igniters and recombiners preventing detonation risks.
4. An additional power supply to cope with station-blackout scenarios.
5. Additional independent water storage tanks available for containment spray also during station-blackout scenarios.
6. Heat sinks composed of structures and other masses inside the containment have been taken into account to control the initial pressure peak while containment spray by external circulation of sump water has been accounted for in the long term.
7. Also the adequacy of the containment leak-tightness has been ascertained.

The modifications that have been implemented in the design are grouped in the following categories:

1. Management of containment atmosphere;
2. Corium in vessel retention;
3. Additional water sources;
4. Monitoring systems dedicated to severe accidents;
5. Control room habitability;
6. Instrumentation and Control.

2.2.1 Management of the Containment Atmosphere

The containment for the Mochovce Units is of the pressure-suppression type and relies on a large amount of water for the condensation of steam in case of large loss-of-coolant accidents. This important feature of the Mochovce containment has allowed a significant reduction of the containment design pressure and allows for the early termination of radioactive releases in case of design basis accidents (DBA) by providing for a quick reduction of containment overpressure.

In case of a large Loss of Coolant Accident (LOCA), a considerable amount of air is displaced from the containment zone housing the primary circuits (steam generator boxes) to separate containment areas (air traps). In this way, the effectiveness of the containment spray is greatly enhanced providing a quick reduction of pressure in the steam generator boxes. A set of pipes connecting the air-traps with the steam generator boxes has been designed (complying with redundancy and diversification criteria required for systems designed to cope with DBA scenarios) to avoid excessive containment under-pressurization. Such pipes are normally closed but are opened automatically in case of low pressure in containment zones housing the steam generator boxes to equalize the pressure. Appropriate verifications will be performed during the execution of the Detailed Design also to make sure that no drawbacks exist from the point of view of hydrogen management (due to the ingress of air in potentially hydrogen-rich areas).

The issue of hydrogen management has been investigated for a long time in the field of nuclear safety, as hydrogen uncontrolled burning is recognized to pose a severe threat to containment integrity. In addition, the fact that the containment of VVER 440 reactors is divided in many compartments makes the hydrogen issue even more important for this type of reactors, as high concentrations of hydrogen can be reached locally more easily than in "western-type" containments.

In the early phase of such investigations, strategies like pre- and post-inertization of the containment atmosphere were also evaluated but then have been rejected as being unpractical.

The solution identified as the most appropriate is based on the use of a combination of Igniters and Catalytic Recombiners: Igniters to quickly burn the hydrogen produced at the beginning of the accident at a high production rate (up to 150 g/s during core relocation in the worst cases) and Catalytic Recombiners to maintain a low concentration of hydrogen in the long term. Both will be passive and autocatalytic. Such solution is widely adopted also in many other operating NPPs where retro-fittings to cope with severe accident scenarios have been introduced.

It is expected that the capacity of the recombiners will be sufficient for adequate hydrogen management for the large majority of severe accident scenarios while the igniters are deemed to be necessary to cover only few limiting cases of lower probability of occurrence but potentially responsible for the most severe consequences.

It is foreseen to install 32 passive autocatalytic recombiners and 30 autocatalytic igniters plus sensors qualified for severe accident conditions. It is expected that the igniters will be located in the steam generator boxes (sprayed zones) although the precise position of such devices inside the containment will be determined during the detailed design.

2.2.2 Corium In-Vessel Retention

The concept of keeping the corium inside the reactor vessel by external cooling with water is not new. It has been already designed for Westinghouse AP600/AP1000 reactors and implemented in Loviisa NPP as a plant modification. The solutions have been approved in all cases by the respective safety authorities and have been used successfully to eliminate the need to deal, in the safety analyses, with ex-vessel phenomena such as ex-vessel steam explosion or molten core-concrete interaction.

Taking into account that the feasibility of IVR has been demonstrated for a very similar plant of the same power (i.e., Loviisa NPP), a similar concept has been developed for Mochovce 3&4, although with some differences in the way it has been implemented.

The key point is to take advantage of the large amount of coolant already available in the containment as energy vector for removing residual heat from the degraded core and transferring it to the ultimate heat sink. Depending on the preceding scenario, such water may be completely available at the floor of the steam generator boxes or partially stored in the 12 trays of the bubbler condenser tower. Taking into account also the volume of water of the primary circuit (including the hydro-accumulators) and the water from the ECCS tanks, it can be estimated that more than 2000 m^3 of water are available for ex-vessel core cooling.

By modification of the existing ventilation lines in and around the reactor cavity, a connection for reactor cavity flooding has been designed. Water shall flow from the connection corridors between the steam-generator box and the bubbler-condenser tower, leading to the reactor cavity and then through the gap between the thermal shield and the reactor pressure vessel up to the reactor vessel nozzles, allowing the steam to flow to the steam generator boxes. The steam released in the steam-generator boxes will be condensed by the containment spray water supplied by the additional water storage tanks dedicated for severe accident scenarios.

For the IVR, a considerable amount of thermo-hydraulic analyses had to be performed together with the implementation of a certain amount of design modifications (as depicted in Fig. 1), basically aimed at:

- effectively cooling the bottom part of the vessel (by modifying the thermal shield to allow the ingress of water at the upper part of the reactor cavity);
- preserving the water inventory, by excluding the possibility of water losses to ex-containment rooms of the reactor building (e.g., through the ventilation lines or through the drainage line of the reactor cavity);
- flooding the reactor cavity and removing heat also in station-blackout conditions (by connecting all the relevant equipment to the station-blackout power supply),
- ensuring that, with the additional source of water, the overall thermal capacity of the containment is sufficient to manage the severe accident for the time the ultimate heat sink is postulated to be unavailable (12 hours).

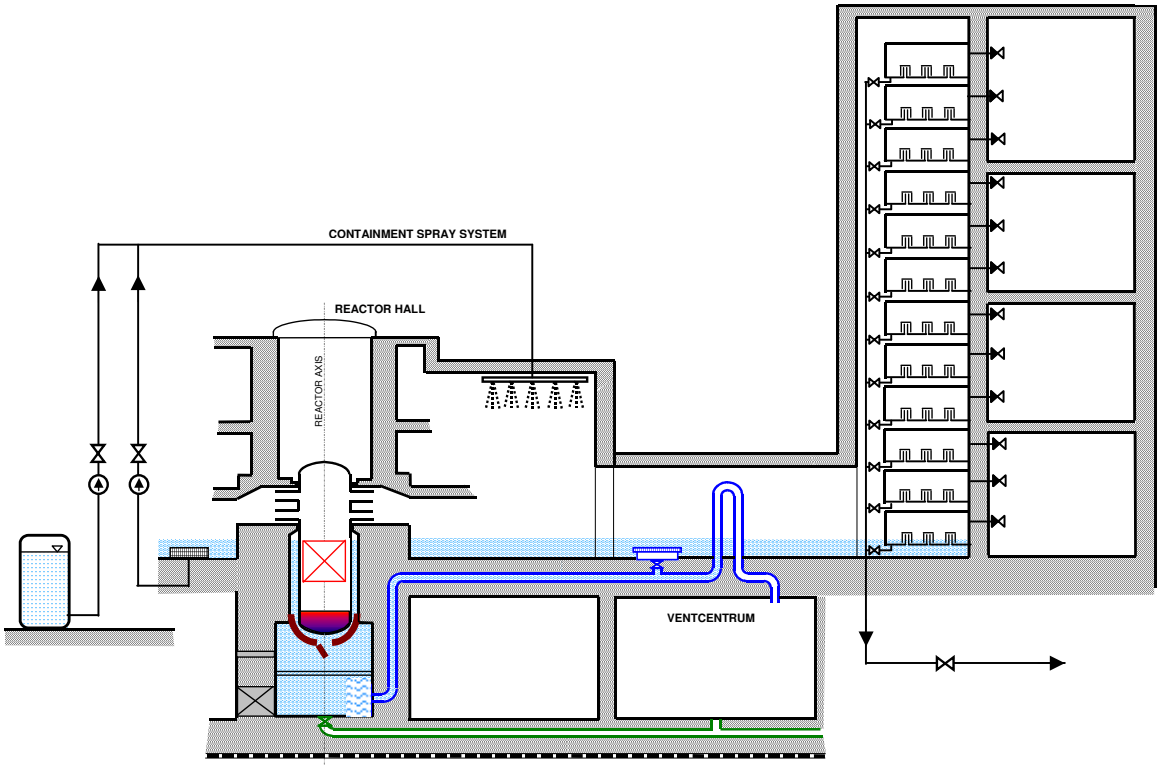


Fig. 2: Sketch of the design modifications adopted for the implementation of the In-Vessel Retention strategy for severe accident management

2.2.3 Additional Water Sources

Three 500 m^3 additional tanks external to the containment have been included in the design to ensure the containment spray during the early phase of a severe accident also in station-blackout conditions and to increase the inventory of water available for core cooling, simultaneously increasing the overall thermal capacity of the containment. By means of a dedicated pump, the system is capable of injecting water: a) into the primary circuit via the low-pressure ECCS lines in case of open vessel scenarios; b) to the containment spray system; c) inside the spent fuel pool. The system features its own diesel generator for station-blackout scenarios.

The requirement to add an additional external source of water derived from the results of analyses of hydrogen management. Additionally, a need arose, which was identified during preparation of both emergency operating procedures and severe accident management guidelines for Mochovce 1&2, to increase the availability of the coolant (borated water) for emergency supply into the primary circuit. Finally, as identified by the Probabilistic Safety Assessment (PSA) for similar units (Bohunice V2), the open reactor sequences needed to be considered. For this reason, by evaluating various alternatives, the direct connection to an external source of coolant was selected to be most beneficiary. The proposal of the system is based on the following requirements:

- to provide early spray of the containment in order to reduce the steam content of the containment atmosphere to allow a quick start of the igniters. Igniters should be able to burn hydrogen from the very beginning of the severe accident (i.e., within minutes from the beginning of core relocation when an intense oxidation of the fuel cladding is expected). This is fundamental to prevent the formation of high hydrogen concentrations inside the containment (i.e., 10-12%) which would lead to unbearable consequences for the containment integrity.
- to provide extra thermal capacity for the adequate management of containment temperature and pressure during the first 12 hours since accident initiation, (postulated time of ultimate heat sink unavailability);
- to decrease the radioactive content of the containment atmosphere, thus reducing the off-site consequences of a severe accident;
- to decrease the safety risk, identified by PSA analyses, deriving from the loss of coolant from the spent fuel pool.
- to decrease the safety risk, identified by PSA analyses, associated with open reactor sequences.

2.2.4 Monitoring Systems Dedicated to Severe Accidents

A significant set of newly-monitored parameters has been included into the Plant and Unit monitoring systems in order to include severe accident control and mitigation. The system is designed as an integral part of the unit monitoring system (it is incorporated into the post accident monitoring system). The list of parameters monitored for severe accident purposes has been derived also taking into account the design inputs resulting from the development of the Severe Accident Management Guidelines (SAMGs) for Mochovce 1&2. The list can be divided in two parts. The first part contains containment and system parameters needed directly for SAMG purposes (decision taking). Systems for monitoring the following parameters are included in this group:

- Core outlet temperature
- Pressure in containment
- Temperature of containment in selected rooms
- Hydrogen concentration in selected rooms
- Coolant level in steam generator boxes
- Coolant level in reactor cavity
- Pressure in air locks
- Temperature in the air locks
- Pressure in reactor pressure vessel
- Pressure difference between primary and secondary circuit
- Radiation level in representative points in the containment
- Selected additional informative parameters, as e.g.:

- Coolant level in steam generators
- Feedwater flow into steam generators
- Pressure in hydro-accumulators

The second group of parameters to be monitored for severe accident mitigation purposes contains the parameters necessary to control and monitor the equipment dedicated to severe accident management such as: indicators of position of relevant valves, interlocks, flows, etc.

All monitoring systems and related components will withstand severe accident conditions and will provide reliable and full-scale information during a severe accident.

2.2.5 Control Room Habitability

The issue of assuring the habitability of the Main Control Room (MCR) in all conceivable situations – including severe accident scenarios - has been analyzed extensively.

This issue has found increasing interest in the recent years with the objective of creating a safe working environment for MCR personnel also in case of a severe accident.

Based on relevant information available for modern reactor designs, the general main basic features of the MCR emergency habitability issue can be summarized as follows:

- normally, severe accidents are managed from the MCR, which is a part of the radiologically non-controlled area, and obviously contains no radioactivity.
- the two potential radiological impacts on the MCR staff are: a) direct radiation; b) inhalation of the radioactive substances from the air supplied by the Heat, Ventilation and Air Conditioning (HVAC) system into the MCR. For all modern designs, direct radiation is negligible as compared with inhalation.
- the MCR ventilation system is equipped with sensors to detect hazardous substances such as smoke, airborne radioactivity or, in special cases, chemical and/or biological agents.
- in case of detection of high radioactivity at the ventilation intake, the MCR emergency habitability system is completely isolated from the outside atmosphere. Afterwards, a slight overpressure and acceptable working conditions are ensured in the MCR by a supply of breathable air from compressed air tanks. The capacity of the tanks is sufficient to maintain MCR habitability for several hours.
- in addition and as a back-up to the MCR emergency ventilation and compressed air tanks, there are protective clothing, respirators, and portable breathing equipment with air bottles stored inside the MCR pressure boundary for individual use by the MCR staff members.

In Mochovce 3&4, a set of pressurized air bottles provide fresh air for at least 12 hours after the beginning of the accident. In the assumed conditions, the internal contamination of the MCR has been eliminated for the first most significant part of the accident and therefore the doses to the MCR staff are limited to irradiation from the source term external to the MCR.

2.2.6 Instrumentation and control

Instrumentation and control is a key element to ensure the achievement of a high safety level in the plant. For Mochovce 3&4, the system has been re-designed and shall be supplied entirely new with state-of-the-art design criteria and equipment.

The new design of the I&C will be strongly oriented to the improvement of the human-machine interface (e.g., through the adoption of a safety parameter display system) in order to allow an optimized management of the plant by the MCR staff in all plant conditions.

3 THE CONCLUSIONS OF THE ADVISORY SAFETY BOARD

The mandate of the Safety Board, which has lasted 18 months, has been to supervise the development of the design revision with specific reference to the issues of primary interest from the point of view of nuclear safety, to assess the design adequacy with respect to the best current international practices and also to provide recommendations to ENEL/SE for the next stages of the Project.

The Safety Board recognized that the safety of VVER 440/213 Nuclear Power Plants had been reviewed by international and western organizations and had been continuously upgraded during the last fifteen years. Eighteen reactors of the same type in six different countries have been and are operating with very good safety and operational performances. However the safety of new nuclear power plants is always reviewed and their design is improved taking into account the development of technical knowledge, evolution of the safety criteria and lessons learned from operating experience. In this respect, the Safety Board highlighted that the Mochovce 3&4 revised design is the most advanced among those so far implemented in VVER 440/213 plants, and that the safety and operational targets of Mochovce 3&4 are comparable to those of other reactors currently under construction in Europe.

In particular, it is worthwhile to mention at least the following points highlighted by the Safety Board:

- the severe accident prevention and mitigation are addressed explicitly during the design process.
- PSA results in terms of core damage frequency are in the range of most modern plants.
- the safety review made by IAEA and operating experience from similar plants have been fully considered to improve the design.
- several systems are being designed and will be built with state-of-the-art components (e.g. Instrumentation and Control System, Electrical Systems).
- all IAEA Safety Requirements for the design have been considered and largely implemented.
- several aspects have been reviewed in depth by IAEA ad-hoc teams in relation with the Mochovce site and with Mochovce 1&2 Units, always with very satisfactory results (including an OSART mission in September 2006).

The Safety Board has been able to identify all safety issues and to propose solutions to be implemented during the design revision phase or in the future Project phases, or even at the operational phase. ENEL/SE assured that all recommendations have been or will be taken into account and that the implementation is being tracked.

In conclusion, the Safety Board believes that no design aspect that has been reviewed and discussed prevents Mochovce 3 and 4 units from achieving a very high safety standard and protecting the workers, the public, and the environment according with current applicable international standards.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[2] WESTERN EUROPEAN NUCLEAR REGULATORS' ASSOCIATION, WENRA Reactor Safety Reference Levels, 2008.

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

Analysis, by RELAP5 code, of Boron Dilution Phenomena in Small Break LOCA and in Mid Loop Operation Transients, Performed in PKL III Test Facility

Fulvio Mascari, Giuseppe Vella
Dipartimento di Ingegneria Nucleare, Università di Palermo
Viale delle Scienze, Edificio 6, 90128 Palermo, Italy
fmascari@din.unipa.it, vella@din.unipa.it

Francesco D'Auria
Dipartimento di Ingegneria Meccanica, Nucleare e della Produzione, Università di Pisa
Via Diotisalvi 2, 56123 Pisa, Italy
dauria@ing.unipi.it

ABSTRACT

The present paper deals with the post test analysis of PKL III E2.2 and E3.1 experiments, by RELAP5/Mod3.3 code. These experiments have been executed in the framework of the OECD/SETH Project in the integral test facility PKL III which is operated by AREVA NP GmbH in Erlangen, Germany. The main purpose of the project is to investigate pressurized water reactor safety issues related to boron dilution phenomena. In particular, the E2.2 experiment investigates the boron dilution issue during a small break LOCA transient and the E3.1 experiment investigates the boron dilution issue during shut down conditions (for refueling) with the reactor coolant system closed and the reactor placed in mid loop operation conditions. This analysis is focused on assessing the capability of the RELAP5 code to correctly predict boron dilution phenomena and the thermal-hydraulic parameters in transients with a) asymmetric loop behavior, b) natural circulation in one and two-phase flow, c) steam generator in reflux condenser mode, and (only for E3.1 experiment) d) the primary system under low pressure conditions in the presence of nitrogen. The E2.2 calculated results show a good agreement with regard to the main thermal-hydraulic experimental parameters but show that is challenging for the code predict the different natural circulation onset in the loops. A sensitivity analysis, carried out by simulating the SG primary side with seven U-tubes of seven different lengths, show that the code predicts the delay of the onset of the natural circulation in the loop 2. The E3.1 experiment demonstrates that it is challenging for the code because it is at low pressure and in the presence of non-condensable (nitrogen). Sensitivity analyses have focused on these transients. The results of these sensitivity analyses show the importance of the mass flow through the upper head by-pass to predict the main thermal-hydraulic parameters during the transients.

1 INTRODUCTION

Assessing the safety of a nuclear installation requires the use of a number of highly specialized tools: computer codes, experimental facilities and their instrumentation, special measurement techniques and so on. Of these tools, thermal-hydraulic system codes are widely

used to perform design, safety and licensing analyses of Nuclear Power Plants (NPP). The performance assessment and validation of large thermal hydraulic codes and the accuracy evaluation, when calculating the safety margins of Light Water Reactor (LWR), are among the objectives of international research programs.
In this framework, the execution of experiments in Integral Test Facility (ITF), simulating the behaviour of a NPP, plays an important role for the system code assessment and for the possibility to identify and characterize the relevant phenomena during off-normal conditions.
Organization for Economic Cooperation and Development (OECD) sets up a test campaign named SETH (SESAR (Senior Group of Experts on Nuclear Safety Research) Thermal-Hydraulics) project to be carried out in the Primärkreisläufe (PKL) facility, addressing the investigation of inadvertent boron dilution events in a Pressurized Water Reactor (PWR) [1].
The present paper is related to the application and the assessment of RELAP5/mod3.3 code against boron transport experiments [2].
The first part of the paper is focused on the E2.2 test which simulates a break in a cold leg (CL) with a contextual high pressure injection in two CLs and a secondary system cooling rate of 100 K/h [3,4]. The transient has been analyzed by comparing experimental and RELAP5 calculated data. This activity has been performed in the framework of a collaboration between the Department of Nuclear Engineering (DIN) of the University of Palermo and APAT (Agenzia per la Protezione dell'Ambiente e per i Servizi Tecnici) started in the 2002.
The second part of the paper is connected with the participation in the OECD SETH/PKL Benchmark on test E3.1 [5,6,7], and in particular aimed at understanding the limits of the current generation of thermal hydraulic system codes. This second activity is performed in the framework of a collaboration between the DIN and the San Piero a Grado Nuclear Research Group of the University of Pisa started in the 2006.

1.1 Boron (Mixing and) Transport (Including Dilution)

Boron is a highly neutron absorbing material and will consequently affect the core power when inserted or removed from the core. Thus boron mixing and transport will not directly influence the thermal hydraulics but will do so indirectly through the core power which is a thermal-hydraulic boundary condition.
In PWRs boron is added to the coolant-moderator and its concentration will control the long term variation of core reactivity. Because of the high liquid velocity in the reactor coolant system (RCS) the added boron will be mixed quite homogeneously with the coolant without steep gradients and its transport through the RCS will closely follow the liquid transport.
However there are low flow conditions, for example at idle reactor coolant pumps, when the pump power has temporarily been lost or when inhomogeneous boron concentration can be attained in the loops with rather steep concentration gradients, in which the diffusion of boron within the liquid can be quite substantial and thus the boron transport will be different from the liquid flow.
Boron mixing and transport within the RCS is of crucial importance for core power control in LWRs. The mixing and transport of boron influences through reactivity feedback the local core power during normal and off normal operation of PWRs. During normal operation of a PWR the initial excess reactivity of a fresh core is compensated by adding boron to the coolant. This added boron is gradually decreased as the fuel burnup increases in order to keep the core reactivity essentially constant throughout the core lifetime.
During a Small Break Loss of Coolant Accident (SBLOCA) in a PWR with U-tube Steam Generators (SG) it has been found that in the reflux condensation phase there exists a

mechanism which can accumulate boron-free condensate in the loop seal (LS). These transients could become a reactivity induced accident (RIA) initiator.
It also a well known fact that a PWR cannot be kept in a sub-critical cold shutdown condition immediately after refueling without the boron concentration in the coolant being above some value, despite all the control rods being inserted. Thus the boron concentration and its mixing and transportation with the coolant are also of major concern at shutdown conditions.
It also has been found that in some specific cases, during shutdown conditions, in PWRs there could be situations where pronounced heterogeneities in the boron concentrations could develop and thus could potentially cause a RIA [8].

1.2 Small Break LOCA Transients

In general, SBLOCA's are characterized by an extended period (this can be tens of minutes to several hours at the lower end of the break spectrum) after the occurrence of the break, during which the primary system remains at a relatively high pressure and the core remains covered.
As soon as the pumps are tripped, either automatically or manually, gravity controlled phase separation occurs and gravitational forces dominate the flow and distribution of coolant inside the primary system. The subsequent sequence of events, whether or not the core uncovers and is recovered or reflooded, depends not only on the location, shape and size of the break, but also on the over-all behaviour of the primary and secondary systems. This behaviour is strongly influenced by both automatic and operator initiated mitigation measures.
In a SBLOCA however due to the continuous loss of primary coolant inventory through the break, degradation of core cooling is expected to occur or not, depending on break size and location, availability of mitigating equipment and nature of operator actions.
The critical flow through breaks is a very important element in analyzing plant behaviour during the course of the complete spectrum of LOCAs.
The break flow determines the depressurization rate of the system and the time to core uncovering which in turn are of, major concern for when and how different mitigation auxiliary systems will be initiated and function [9].

1.3 Shutdown and Mid Loop Operation Transients

The design of many PWRs requires that, during certain phase of the shutdown period, maintenance operations are performed while the water level in the primary system is lowered. The water level may be reduced to the mid-point of the outlet leg (Hot Leg) of the primary coolant system, and thus the term mid loop applies. During this operation condition it is necessary to provide a continuous heat removal system for the reactor decay heat. Inasmuch as the SGs can no longer perform this function (there is no forced or Natural Circulation (NC) through the SGs) the sole heat removal system is the Residual Heat Removal System (RHRS). During the heat removal process it is important to maintain the reduced level within a somewhat narrow range. The level must be low enough to enable opening of the inspection hatches, but not so low as to uncover the pipe leading from the HL to the RHRS (this pipe is sometimes referred to the drop line). If the water level is too low, the water supply to the RHRS is disrupted. At first a vortex may form and air may be ingested. A complete interruption of water supply leads to a pump damage mechanism known as cavitation; this can lead to irreversible pump damage. At such times a small error in accomplishing the desired water level can lead to drainage below the HL and interruption of the heat transport to the RHR heat exchanger system [10].

2 BRIEF DESCRIPTION OF THE PKL III FACILITY AND THE E2.2 AND E3.1 EXPERIMENTS

2.1 PKL III Facility

The PKL facility [11] is a full-height ITF that models the entire primary system and most of the secondary system (except for turbine and condenser) of a PWR of KWU design of the 1300-MW class. All the elevations are scaled 1:1 while the volumes, power and mass flows are modeled by the scaling factor 1:145. Similarly to other test facilities of this size, the scaling concept aims to simulate the thermal hydraulic system behaviour of the full-scale power plant.
This facility is subdivided in RCS, SG secondary side and the interfacing systems on the primary and secondary side.
The RCS comprise the rod bundle vessel containing the heater bundle (simulation of reactor core), the four loops, with the reactor coolant pumps and the SGs, the down-comer (DC) model and the pressurizer (PRZ). The four loops on the primary side are symmetrically arranged around the pressure vessel (RPV). The PRZ is connected to the RCS by the surge line. The vessel models the Upper Head (UH) plenum, the Upper Plenum (UP), the reactor core, the reflector gap and the lower plenum (LP). The reactor core model consists of 314 electrically heated fuel rods and 26 control rod guide thimbles. The maximum electrical power of the test bundle is 2512 kW. The fuel rods, arranged in three concentric zones, can be heated independently of one another. The DC is modelled as an annulus in the upper region and continues as two stand pipes connected to the LP. This configuration permits symmetrical connection of the 4 CLs to the RPV, preserves the frictional pressure losses and does not unacceptably distort the volume/surface ratio. The UH bypass is modelled by four parallel by pass lines associated with the respective loops to enable detection of asymmetric flow phenomena in RCS.
The four steam generators of the facility are vertical U-tubes bundle heat exchangers. In keeping with the scaling factor of 1:145 the number of tubes for each SG was therefore obtained as 28. The tubes have seven different lengths.

The operating pressure of the PKL facility is limited to 45 bar on the primary side and to 56 bar on the secondary side. This allows simulation over a wide temperature range (250 °C to 50 °C) that is particularly applicable to the cooldown procedures investigated.

2.2 E2.2 Experiment

The test E2.2 investigates the inherent boron dilution during SBLOCA. The test was executed January 15, 2002 [3].
The test E2.2, simulates a SBLOCA with these main boundary conditions:

- break (32 cm^2/145) in the CL of loop 1, between RCP and RPV;
- all 4 SGs running down at a cooling rate of 100 K/h;
- active High Pressure Injection Systems (HPIS) in loop 1 and 2;
- active Low Pressure Injection Systems (LPIS) in loop 1 and 2 when the pressure in RCS drops below 10 bar for the first time.

The aim of the test was to answer the following questions:

- what are the mass flow rates as NC start up and how long is the time lag between the commencement of circulation in the individual loops and the condensate slugs from the individual loops reaching RPV;

- what is the lowest boron concentration that can ever be attained at the inlet of the RPV in the event of an accident involving a small cold-side break, cold-side injection of emergency cooling water, inherent boron dilution.

The test initial conditions are established in two phases: a pre-conditioning phase and a conditioning phase. The first one (subcooled NC) is performed to reach a steady state condition before the conditioning phase.
At the end of the pre-conditioning phase:

- the primary system is completely filled with 2300 kg of water with an homogenous boron concentration of 1000 p.p.m.;
- the heater rods supply a constant power of 530 kW;
- the pressure in RCS is about 42 bar and the core outlet temperature is 250 °C (3°C of subcooling);
- heat is removed by NC in all 4 loops;
- main steam pressure is about 28 bar.

The conditioning phase initiates 6450 s before test starts (t=0) (Start of the Transient (SOT)) by insulating the main steam line with the purpose of increasing the pressure in secondary side to reduce the primary to secondary temperature difference. This induces saturated conditions at core outlet and consequently an increasing pressure in RCS. When the RCS pressure reaches 44 bar (5270 s before the SOT), the break in CL 1 is opened and the pressure difference between primary and secondary falls down to 1-2 bar. The level in RPV drops rapidly reaching the lower CL edge, while U-tubes of the SGs and PRZ completely empty. At 4430 s before SOT the main steam line is opened again so the primary pressure reaches about 40 bar. The pressure of secondary system is controlled at about 39.4 bar in order to decrease the NC in RCS. When the coolant inventory is about 1170 kg (3950 s before SOT), the break is closed and the primary system remains in reflux-condenser conditions for 3240 s. At the end of this phase, about 200 kg of condensate are formed per loop and low-borated water is accumulated in LSs. At 710 s before SOT an high pressure injection in CLs 1 and 2 begins at a reduced flow rate in order to avoid rapid condensation which could cause high mass flows in RCS, and, therefore, mixing processes between low-borated and high-borated water. At the end of this phase, the mass inventory is about 1440 kg.
At t=0 the test starts with the opening of the break in CL 1, the injection by HPIS in CLs 1 and 2 of a total flow rate of about 0.8-0.9 kg/s and the cooldown of the SGs at 100 K/h. At the beginning, the mass flow which goes out through the break is greater than the mass flow injected by HPIS. The coolant inventory has a minimum at about 1200 s, than return to increase owing to a decreasing RCS pressure and an increasing flow rate injected. When RCS pressure drops below 10 bar, LPIS is activated in CL 1 and 2, and it is switched off again when the same pressure rise again above 10 bar. At t=5980 s the HPIS is switched off and the test is considered ended at t=8430 s, when the RCS and the secondary side pressures are about equal to external pressure.
This experiment shows that the restart of the NC is a “very sensitive mechanism” which is strongly influenced by the prevailing boundary conditions in the individual loops e.g location of the break, connection of the PRZ and Emergency Core Cooling Systems (ECCS) injection. In this connection some of the relevant experimental results are here reported. NC starts at different times in the different loops. NC first sets in the two unfed loops 4 and 3. In the loop 4 NC starts, with an initial very small mass flow, at 3020 s (final phase of refill), about 160 s earlier than in loop 3. The onset of the NC in the loops supplied with ECCS is experimentally detected after LPIS injection ends. In particular, a forward flow starts in the loop 1 at 3830 s and the NC starts in the loop 2 at about 6450 s, only after the HPIS is switched off.
As regard the boron concentration it is noteworthy that the condensate slugs with the lowest boron concentration are formed only in the loops 4 and 3 which are not feed with ECC water.

In particular the minimum boron concentration measured at the RPV inlet is about 350 ± 100 p.p.m. at 3050 s in the loop 4 and at 3400 s in the loop 3. After the onset of the NC in the loops supplied with ECC water there is no significant drop in the boron concentration at the RPV inlet. As regard the loop 1 it is noteworthy that, though the NC is started at 3830 s, the entire water flowing through SG 1 is escaping via the break with any condensate present. Therefore no drop in the boron concentration is observed at the CL 1 RPV inlet. In the loop 2, only after t=6450 s a distinctly forward moving two phase NC is starting (due to the steam that enters HL 2 via the surge line from the PRZ). However the boron concentration at the CL 2 RPV inlet don't drop but rise.

2.3 E3.1 Experiment

The second experiment that is analyzed in this paper is the test PKL III E3.1 "Loss of Residual Heat Removal System (RHRS) in 3/4 loop operation with the RCS closed" which was conducted at the facility on July 25, 2002 [5].
The scenario starts simulating the failure of the RHRS which, during the stationary condition of the experiment, is removing the decay heat of the core simulator. The boundary conditions of the experimental facility simulate the condition of the prototype NPP in preparation for the refueling. The reactor coolant inventory is reduced at the 3/4 loop operation level, the space above the water inventory is filled with nitrogen that is injected into the RCS, the primary side pressure is 1 bar and the temperature at core outlet is 61 °C. For the purpose of this test, it is postulated that the PRZ has already been largely cooled down when the transient starts, and its temperature varies between 56 °C (bottom) and 49 °C (top).
The test was designed to investigate:

- the capability of the water-filled SG to remove the decay heat following the failure of the RHRS via only one operational SG;
- the heat transfer mechanism when nitrogen is present in the primary side and in the SG;
- what is the primary side pressure when the heat removed by the secondary side allows stable equilibrium conditions;
- the deboration process connected with the reflux condenser mode occurring following the failure of the RHRS.

To better address this issue the test is performed with borated coolant and special instrumentation suitable for boron concentration measurements.
The experiment can be subdivided in the following phases:

0. phase prior to starting the test, before the RHRS failure (until 0 s);
1. test phase until the set point for SG 1 operation (from 0 s to 8225 s);
2. test phase with SG 1 pressure controlled (from 8225 s to 33095 s);
3. test phase with the accumulator injection (from 33095 s to 37650 s).
4. test phase following the restoration of RHRS (from 37650 s to the end of the experiment).

The phase prior to starting the test is performed in order to reach the condition of the test begins. At the end of this phase the primary side is at about 1 bar, in stable conditions with core power at 217 kW. The energy is removed by normal operation of RHRS. The RCS mass inventory including the PRZ has been reduced to 1300 kg which correspond to 3/4 loop level on the primary side. Secondary–side pressure in all SGs is approximately 1 bar. SG 1 and 2 are filled with water on the secondary side (level approximately 12.2 m) and the secondary sides of SG 3 and 4 contain no water and are completely filled with air. Only the SG 1 is ready for operation while the SG 2, 3 and 4 are not operated during the experiment.

The experiment starts simulating the loss of the RHRS (phase 1). Following this event the primary side energy is not removed and coolant temperature in the core increases. Nearly 700 s after the SOT, saturated condition are reached in the core outlet. At 1270 s after the SOT, following the increase of voiding in the core, the PRZ level rises because the two phase mixture in HL 2 is entrained into the PRZ and here it condenses due to the low temperature of the PRZ wall. During this phase the core power is removed mainly from the secondary side of SG 1 and 2, filled with water. Due to the increased flow of steam into SG 1 and 2, the swell level in the inlet chambers of these SGs continues to rise and reaches the U-tubes with resultant heat removal in reflux condenser mode 1955 s after the SOT. The swell level in SG 3 and 4 simultaneously drops back into the HLs. An accurate investigation of the balance of energy of the system shows that notwithstanding the SG 3 and 4 are filled with air their contribution is not negligible. The energy removed from the primary side is accumulated in their structural materials. The energy removed by the SG 1 and 2 causes the temperature increase in the mass inventory of these systems, and after 5500 s the saturated conditions are reached in SG 1. The SG 2 follows the SG 1 behaviour with a delay of 1600 s. When the saturated conditions are reached, the secondary side pressure rises more quickly. Secondary side pressure in SG 1 rises to 2 bar (SG 1 pressure set point) 8225 s after SOT resulting in activation of the SG 1 secondary side pressure control system.
The SG 1 starts to be operated (phase 2) and the pressure is maintained at 2 bar for the remaining of test period. On the contrary the SG 2 pressure follows the trend of the primary side. Following the start of SG 1 operation, as a result of the steam flowing from the core to this SG, a displacement of mass from SG 2 U-tubes into SG 1 U-tubes takes place. At 12180 s, the primary mass inventory of the SG 2 is completely displaced. As a result of the SG 1 U-tubes level increase, at 13300 s a first notable over-spilling happens. That causes a rapid dilution of the boron concentration in the LS 1 under the SG 1 outlet. Between 13500 s and 14780 s after SOT the boron concentration drops from an initial value of approximately 2150 p.p.m. to approximately 830 p.p.m. This overspill creates a positive flow conditions in these U-tubes. That allows coolant to be transported from the inlet to the outlet of the SG and onward through the LS. Primary coolant with a low boron concentration below the reactor coolant pump and in the upper DC region is consequently transported to the core, producing a short term decrease in the boron concentration there. Then the boron concentration in the LS rises because the diluted water accumulated at the inlet of the SG U-tubes is replaced by the higher borated water in the HL, and then it starts to decrease slowly (reflux condenser mode conditions occurring in the primary system). The primary pressure is stabilized at 4.8 bar, with the SG 1, now, capable to remove the energy of the primary side. During this phase, the pressure in the secondary side of SG 2 remains above the pressure of the primary side. This is related to the presence of the non-condensable in the closed system.
Until the first accumulator injection a quasi steady state condition prevails in SG 1 with intermittent flow through individual U-tubes and the reflux condenser conditions in the remaining U-tubes.
The third phase of the experiment is characterized by the hydro-accumulators activation.
Five accumulator injections are performed: four of these into CLs of loops 1-4 and one into HL of loop 4. The purpose of this phase is to investigate the effect of the injection location (Cold and HLs) and the effect of different injection masses on the RCS pressure profile.
The last phase (phase 4) is connected with the restoration of the RHRS system that removing the decay heat causes a continuous decrease in the pressure and temperature. From 39380 s till the end of the test the core remains in subcooled condition. The experiment is stopped at 42725 s with core outlet temperature of 98 °C and the pressure of 4.3 bar.

3 E2.2 CODE APPLICATION

3.1 RELAP5 Model for E2.2 Test

The PKL III RELAP5 model used to study the E2.2 experiment is reported in figure 1 and is the DIN modified version of the model delivered by FRAMATOME-ANP [4].

The RCS nodalization comprises the rod bundle vessel containing the heater bundle, the four loops, with the reactor coolant pumps and the SGs, the PRZ and the DC model. The four loops are modelled separately. The vessel nodalization comprises the UH, the UP, the reactor core, the reflector gap and the LP. The core region is modelled with a pipe and an annulus which simulates the reflector gap of the facility. The 314 core channels are lumped in only one thermal hydraulic region, thermal coupled with three different active heat structures in order to simulate the three concentric zones. The annular part of the vessel DC is modelled with a “fictitious” 3D model taking into account the geometric location of the CLs. The four SGs are modelled separately and the two SG DC pipes are lumped in only one pipe in each SG. The U-tubes are modelled with three different tubes each one of different height that respects the elevation vs volume ratio and the real heat-exchange surface. The nodalization models the main steam piping system present in the facility. In particular the main steam line, the warm up line, the steam header and the silencer are modelled separately for each SG. The PRZ heaters and SG heaters are modelled as well.

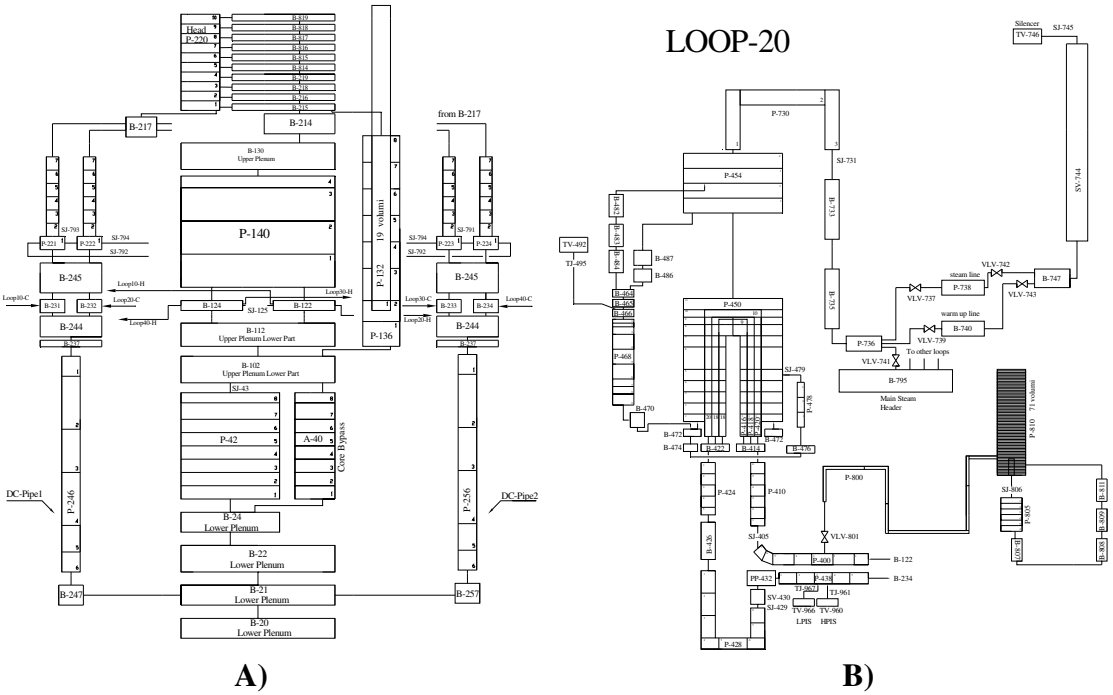


Figure 1: PKL III reference RELAP5 nodalization of A) the vessel and B) the loop 2.

3.2 RELAP5 Model Qualification Process

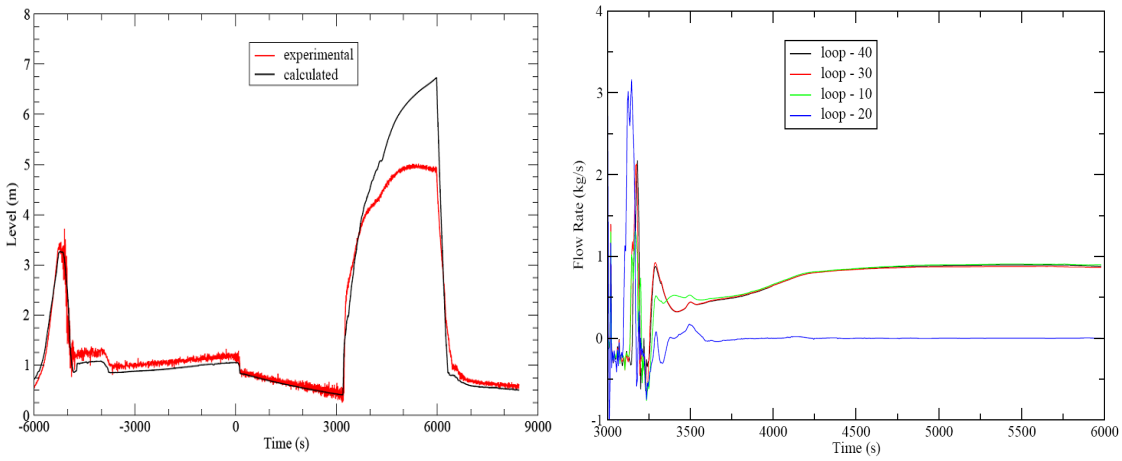
A nodalization representing an actual system (ITF or NPP) can be considered qualified when a) it has a geometrical fidelity with the involved system, b) it reproduces the measured nominal steady-state conditions of the system and c) it shows a satisfactory behaviour in time dependent conditions. Taking into account these statements, the standard procedure reported in [12] has been considered. The steps of the qualification process performed in this phase of the activity are: a) the steady state results analysis, b) the reference calculation results analysis, c) the results from sensitivity studies (still in progress).

3.3 RELAP5 Model Steady State and Conditioning Phase Level Qualification Process

The steady state level qualification process has been performed and the steady state acceptability criteria described in Ref [12] have been verified. The conclusions of this step of the code assessment procedure are: a) the criteria for nodalization qualification are fulfilled, b) the steady state and the conditioning phases are reproduced with a very good accuracy. In particular, during the reflux condenser phase, the mass of condensate predicted by this RELAP5 simulation is in a good agreement with the experimental data (about 850 kg). The initial conditions obtained in the RELAP5 simulation, at the end of the conditioning phase, are in a very good general agreement with E2.2 experimental values as shown in figure 2 A [4].

3.4 E2.2 Reference Calculation and Sensitivity Analysis Results

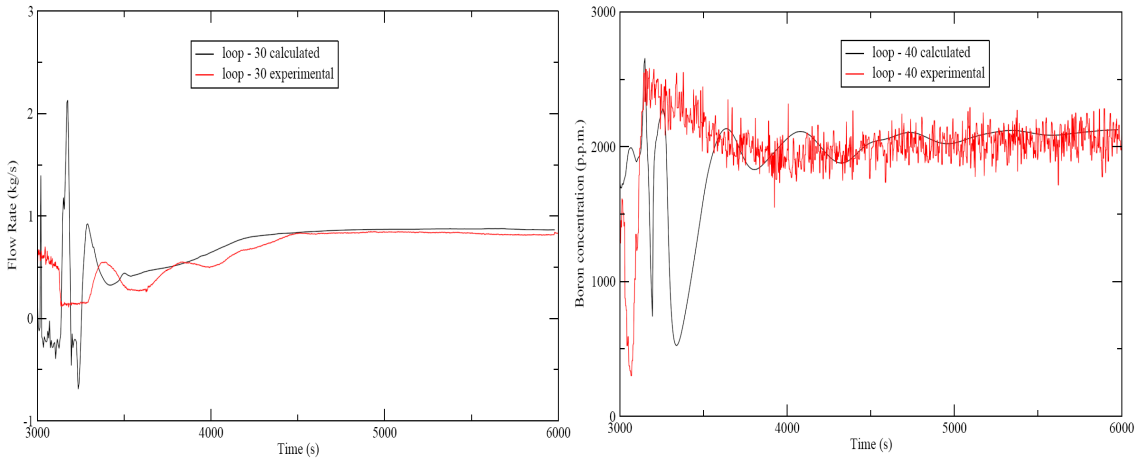
The E2.2 reference calculated results show a good agreement with the experimental data for a number of main important variables as the primary system pressure, the level in RPV, the level in PRZ, reported in figure 2 A, and SGs and the value of mass flow in core. The primary mass inventory has the same behaviour as the experimental case, reaching the minimum value (about 1250 kg) at about 1200 s after the start of the test and the maximum value (about 2880 kg) when the HPIS is switched off. In the reference calculation, only three equivalent U-tubes for each loop are used to model the SG primary side, the results show a simultaneous restart of NC in the four loops and a minimum boron concentration of 700 p.p.m. (experimental data below 500 p.p.m.) at CL 3 and 4 RPV inlet after the start of NC. A preliminary sensitivity analysis (indicated as SEN7) aiming at the improvement of the NC restart in the four loops, is carried out by simulating the SG primary side with seven tubes of seven different lengths. The simulation shows that the NC restart almost simultaneously in the loop 1, 3, and 4 and later in the loop 2, figure 2 B and 3A.



A) **B)**

Figure 2: A) E2.2 experiment and reference analysis results for the PRZ level; B) sensitivity analysis (SEN7) results for the mass flow rate in the different loops.

The boron concentration in the CL 3 and 4 RPV inlet drops at about 500 p.p.m., for a short time, as shown in figure 3 B; boron concentration in the loops 1 and 2 remains constant. The results of other sensitivity analysis show the importance of the mass flow through the reflector gap and the UH by-pass to predict the main thermal-hydraulic parameters during the transient. These quantities shown itself to be key parameters to correctly predict the UP, UH and the annulus DC thermal-hydraulic behaviour.



A) **B)**

Figure 3: E2.2 experiment and sensitivity analysis (SEN7) results for A) loop 3 mass flow rate after restart of the NC; B) boron concentration in the CL 4 RPV inlet.

4 E3.1 CODE APPLICATION

4.1 RELAP5 Model for E3.1 Test

The nodalization of PKL III facility used to simulate the E3.1 experiment and to participate in the "OECD SETH/PKL benchmark on test E3.1" in 2006, is a scaled nodalization of ANGRA-2 NPP, that is a PWR Siemens-Framatome reactor. After the analysis of the previous reference calculation [7], presented at the "OECD SETH/PKL benchmark on test E3.1" [6], and the analysis of some sensitivity calculations [13], a preliminary review of the SGs secondary side model was carried out in order to better reproduce its thermal hydraulic behaviour.

The PKL III nodalization vessel consists of a core channel heated by 3 active heat structures representing the 3 radial concentric heated zones. The two DC pipes have been modelled with 2 pipes connected to the LP region and to a common volume representing the annular region of the DC in the upper part of the vessel where the CLs are connected. In the above mentioned previous sensitivity study, the annular part of the vessel DC was modelled with a "fictitious" 3D model taking into account the geometric location of the CLs, but it is not used in this first results updating. Two pipes model the UH in order to allow recirculation in this zone. The four loops are modelled with pipes, primary pump component in each loop and only one pipe representing the U-tubes preserving the heat exchange surface area. The secondary side of the facility is also modelled. Each loop has a SG composed by a main pipe, the riser; the 2 DC pipes are represented by one single pipe. The time dependent volumes representing the steam lines are connected in the top side of the SGs nodalization. The steam pressure and the level control in the SGs are represented by time dependent volumes and junctions. The length of the volumes in the riser region follows the same length progression increase of the U-tubes to which they are associated. The compensation for heat losses circuit has also been modelled but not activated during the E3.1 simulation.

4.2 RELAP5 Model Steady State Level Qualification Process

The steady state level qualification process has been performed and the steady state acceptability criteria described in reference [12], have been verified. The conclusions of this

step of the code assessment procedure at steady state level are: a) the criteria for nodalization qualification are generically fulfilled, b) the initial conditions obtained in the RELAP5 simulation, at the end of the preliminary phase, are stable and in general agreement with the E3.1 experimental values. Few discrepancies in the initial conditions at the SOT are due to the assumed hypotheses to simulate the preliminary phase.

4.3 E3.1 Reference Calculation and Sensitivity Analysis Results

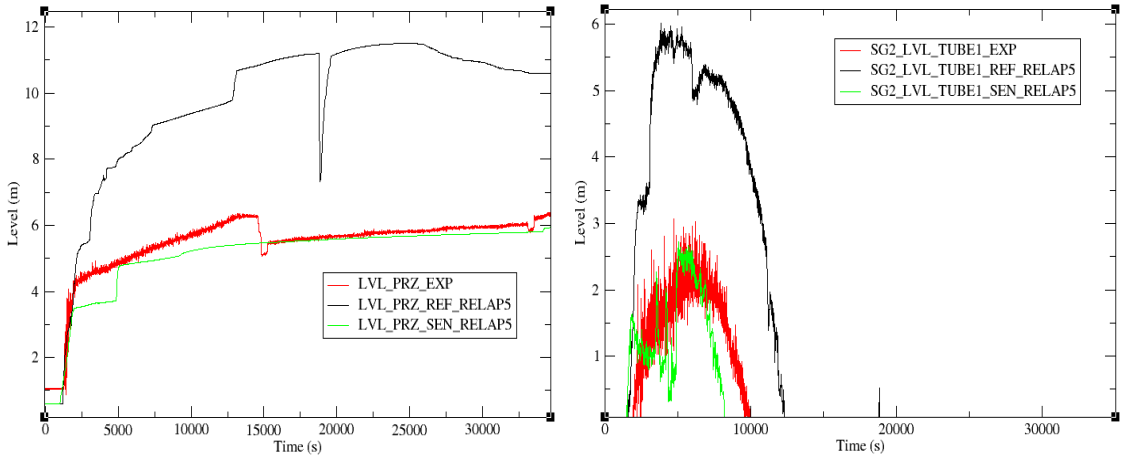
The post test analysis has been limited to the first two phases of the experiment, just before the accumulator's injection, as in the specification of the previous OECD SETH/PKL benchmark on test E3.1. A comprehensive comparison between measured and calculated trends or values has been performed.

In the new reference calculation analysis (indicated as REF) at the beginning of the test when the RHRS has been shutdown, the core is completely covered by subcooled water and there is no mass flow to remove the decay heat. The calculated core outlet temperature reaches the saturated value after about 578 s of delay compared to the experimental data, due to a prompt liquid circulation between the core and the reflector gap. The core inlet temperature increase starts around 200 s after the SOT (about 1300 s before the experimental data) due to the beginning of the liquid circulation inside the core. The core outlet temperature shows the same increase as the experimental value in the first part of its rise; an overestimation is present in the second part and during the "quasi" steady state condition. When saturation temperature is reached at core outlet the simulation shows a decrease of the vessel collapsed level and a two phase mixture enters in the HL of loops 1 and 2. After that, the mixture levels arrive at the inlet of SGs and the reflux condenser mode starts followed by the heat exchange from primary to secondary. The calculated results show an insurge of two phase mixture in the PRZ via the surge line and an increase of the PRZ collapsed level. The collapsed level in the PRZ has the same trend as the experimental data in the first part of its rise, and shows an overestimation in the second part reaching a "quasi" steady state condition, as shown in figure 4 A. The PRZ pressure begins to rise about 100 s before the experimental data and shows an overestimation during its rise and during the "quasi" steady state phase with regard to the experimental data. The pressure overestimation during the "quasi" steady state condition is due to the overspilling absence in the calculated results. In the primary side the steam flows to UH via UP then arrives in CL and DC pipes after passing through the UH by-pass and DC annulus. The effect of this flux is one of the reasons, in the calculated results, of the rise of the DC, CL and LS temperature although the absence of the overspilling phenomenon. The condensation in CL and DC produces boron dilution. Differential pressure between HL and CL across LS produces boron dilution and transport. The simulation doesn't predict the overspilling in the SG 1 but predicts the mass displacement from SG 2 to SG 1 (primary side) figure 4 B, although the SG primary side is modelled with only one tube. The calculated results predict the temperature build-up in the core but don't show the transit of a cold-water slug at the core inlet. The PRZ temperature behaviour is qualitatively predicted and shows an overestimation compared to the experimental data. The boron concentration dip and the dilution rate in the LS of loop 1 is not predicted because of the overspilling absence in the calculated results, as shown in figure 5 A. The short term decrease in boron concentration at the core inlet is not predicted.

The primary side thermal hydraulic parameters, about 21000 s after the SOT, show a temporary perturbation. This perturbation seems due to a temporary increase of the UH by pass flow. This flow increase creates a temporary reverse flow into the core from the HLs. This reverse flow creates a decrease of the water level in the SG 1 U-tubes and a temporary

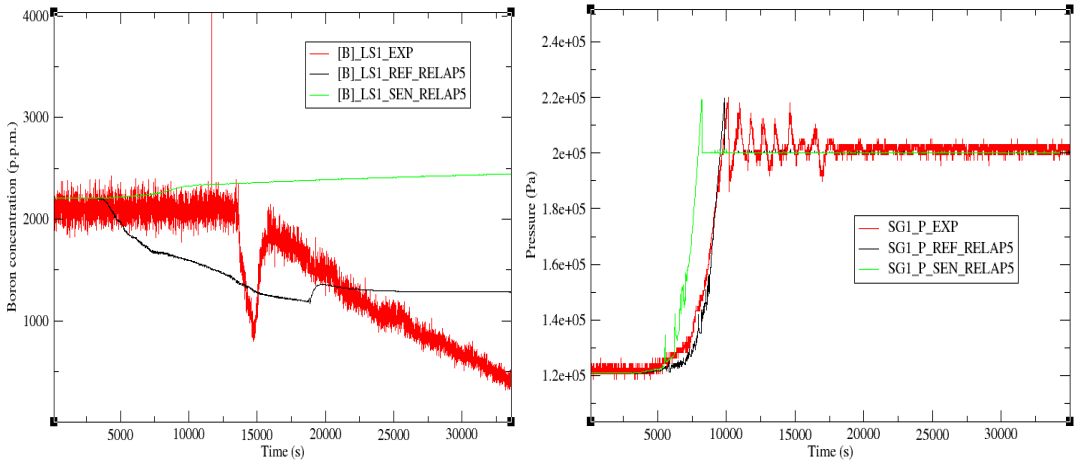
decrease of SG 1 heat exchange. The PRZ level shows a temporary decrease due to a reverse flow through the surge line.

Secondary side pressure increase is due to the heat exchange from primary to secondary side by reflux condenser mode. The SG 1 trend is correctly predicted but is needed a more detailed model of the steam line in order to correctly reproduce the SG 1 experimental pressure oscillation, as shown in figure 5 B. The SG 1 pressure control starts about 350 s before the experimental data. The SG 2 pressure shows an overestimation with regard to the experimental parameters. The temperatures behaviour on the SG 1 secondary side is well predicted by RELAP5 calculations in the "quasi" steady state condition. The feedwater and steam flow in SG 1 show continuous oscillations; the degree of the SG 1 feed water and steam flow oscillations, present in the calculated results, depend on the method adopted for the feedwater and steam discharge regulation.



A) B)

Figure 4: E3.1 experimental and calculated level results for A) PRZ; B) SG 2 tube 1 inlet.



A) B)

Figure 5: E3.1 experimental and calculated results for A) boron concentration in the LS 10; B) SG 1 secondary side pressure.

The sensitivity analysis (indicated as SEN) is carried out in order to investigate the code sensibility to the effect of the UH by-pass [14] in the prediction of the level and pressure of the PRZ and in the prediction of the main thermal hydraulic primary parameters, during the transient. This sensitivity analysis, carried out by closing the UH by pass, shows a better prediction of some primary side thermal hydraulic parameters; in particular the PRZ level

shows a significant decrease, as shown in figure 4 A. The simulation again doesn't predict the overspilling in the SG 1. The DC pipes temperature shows a reduction with regard to the reference calculation results and continues to show a missed behaviour with regard to the experimental data. The SG 1 and 2 pressure start their rise before the reference and experimental data, figure 5 B. The previous temporary perturbation of some primary side thermal hydraulic parameters is now not present.

5 CONCLUSIONS

The analyses here presented are focused on assessing the capability of the RELAP5 code to correctly predict boron dilution phenomena and the thermal-hydraulic parameters in transients with a) asymmetric loop behaviour, b) NC one and two-phase flow, c) SG in reflux condenser mode, and (only for E3.1 experiment) d) the primary system under low pressure conditions in the presence of nitrogen.

The E2.2 reference calculated results show a good agreement with the experimental data for a number of main important parameters. By using only three equivalent U-tubes for each loop to model the SG primary side, the calculated results show a simultaneous restart of NC in the four loops and an overestimation of the boron concentration at CL 3 and 4 RPV inlet after the start of NC. The sensitivity analysis, carried out by simulating the SG primary side with seven U-tubes of seven different lengths, shows that the NC restarts almost simultaneously in the loops 4, 3, and 1 and later, in a good agreement with the experimental data, in the loop 2. The boron concentration at the CL 3 and 4 at the RPV inlet drops at about 500 p.p.m., for a short time after the start of the NC in these loops, in agreement with the experimental data and their related uncertainty.

The results of other sensitivity analysis show the importance of the mass flow rates through the reflector gap and the UH by-pass to better predict the UP, UH and the annulus DC thermal-hydraulic behaviour. More accurate studies of condensation processes in the PRZ and UH region in this transient could improve the simulation results during the phase in which the pressure rises rapidly, after the LPIS intervention.

The E3.1 experiment is challenging for the code because it is at low pressure and in the presence of non-condensable. The difficulty to simulate the experiment is due to the simultaneous presence of low pressure condition and of nitrogen in various parts of the facility, the variation in the performance of individual U-tubes and the large influence of pressure drop and heat losses including their spatial distribution. The correct prediction of the transient is strongly influenced also by the nitrogen and the void fraction distribution at the beginning of the transient.

The model with only one equivalent U-tube resulted not suitable for the prediction of the overspilling phenomenon in this kind of transient. Therefore the evolution of the boron concentration in the LS and core inlet is not reproduced by the code. The results of the previous E3.1 benchmark show that it might be necessary to simulate the steam generator U-tubes in a "tube-by-tube" fashion in order to correctly predict the unplugging/overspilling phenomenon observed in the experiment, but the long computing time for the current modelling also shows that this approach is unfeasible with current monoprocessor machines.

The fill up of the PRZ shows an overestimation compared with the experimental trend.

The E3.1 sensitivity analysis, shows a better prediction of some primary side thermal hydraulic parameters although the overspilling is not predict by the code. In particular the PRZ level shows a significant decrease.

Again, more investigations need the effect of the reflector gap mass flow rate and the UH by pass, in order to investigate the code sensibility to them, in this kind of transient, and

better reproduce the general thermal-hydraulic behaviour. The prediction of the water levels and the non-condensable redistribution during the transient should be more analyzed.

REFERENCES

[1] T. Mull, B. Schoen, K. Umminger, "Final Report of the PKL Experimental Program within the OECD/SETH Project", FRAMATOME ANP, FANP NGTT1/04/en/04, December 2004.

[2] RELAP5/MOD3.3,Code Manuals, Nuclear Safety Analysis Division, NUREG/CR-5535/Rev1-Vol I-VIII, Information System Laboratories (ISL) Inc. Rockville, Maryland, Idaho Falls, Idaho, December 2001,.

[3] T. Mull, K. Umminger, "Test PKL III E2.2:", FRAMATOME ANP, FANP TGT1/02/en/44, December 2002.

[4] Giuseppe Rizzo, Giuseppe Vella, "Analysis, by RELAP5 Code, of Boron Dilution Phenomena in a Small Break LOCA Transient, Performed in PKL III E2.2 Test" Proc. International Conference Nuclear Energy for New Europe 2007, Portoroz, Slovenia, September 10-13 (2007).

[5] B. Schoen, K. Umminger, "Test PKL III E3.1: Loss of Residual Heat removal in 3/4 Loop Operation with the Reactor Coolant System Closed" FRAMATOME ANP, FANP TGT1/03/en/10, December 2003.

[6] "OECD SETH/PKL Benchmark on test E3.1: Boron Dilution During Loss of the Residual Heat Removal System at Mid-Loop Operation"; Co-ordinator A. Bucalossi; authors: A. Bucalossi, P. Junninen, J.F. Villanueva, S.Carlos, J.Segurado, S.Martorell, V. Serradell, F. Kasahara, A.Jasiulevicius, F. Mascari, A. Del Nevo, F. D'Auria, G. Vella, C. Queral, A. Concejal, I. Gonzalez, C. Montenegro (in press).

[7] F.Mascari, G.Vella, A. Del Nevo, F. D'Auria, O. Lllombard Soriano, "Post Test Analysis and Accuracy Quantification of PKL III E3.1 Test" Proc. International Conference Nuclear Energy for New Europe 2006, Portoroz, Slovenia, September 18-21 (2006).

[8] CSNI Integral Test Facility Validation Matrix for the Assessment of Thermal Hydraulics codes for LWR LOCA and Transients", NEA/CSNI/R(96)17 July 1996.

[9] N. Aksan, THICKET 2004, Session V, Paper 13 "International Standard Problems and Small Break Loss-Of-Coolant Accident (SBLOCA)", The OECD/NEA Seminar on Transfer of Competence, Knowledge and Experience Gained Through CSNI Activities in the Field of Thermal-Hydraulics (THICKET), Saclay, France, June 2004.

[10] "Loss of Residual Heat Removal (RHR) While at Mid-Loop Conditions Corrective Actions" NEA/CNRA/R(2006)4 September 15 (2006).

[11] H. Kremin, H. Limprecht, R. Güneysu, K. Umminger, "Description of the PKL III Test Facility", FANP NT31/01/e30, Technical Centre of Framatome ANP, Erlangen, Germany, July 2001.

[12] M. Bonuccelli, F. D'Auria, N. Debrecin, G.M. Galassi, "A methodology for the qualification of thermalhydraulic code nodalizations", Proc. of NURETH-6 Conference, Grenoble (F), October 5-8, 1993.

[13] F. Mascari, A. Del Nevo, G. Vella, F. D'Auria, "Post Test Analisys by Relap5 Code & Accuracy Quantification of PKLIII E3.1 Experiments (Sensitivity calculation)" Proc. International Youth Conference on Energetics 2007 (IYCE '07), Budapest, Hungary, 31 May – 2 June, 2007.

[14] F. Mascari, G. Vella, A. Del Nevo, F. D'Auria, "Analysis, by RELAP5 Code, of Boron Dilution Phenomena in a Mid Loop Operation Transient, Performed in PKL III F2.1 Run 1 Test" Proc. International Conference Nuclear Energy for New Europe 2007, Portoroz, Slovenia, 10-13 September (2007).

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

Industrial Safety and Nuclear Safety Connections

Gianni Petrangeli
University of Pisa
Via Diotisalvi, 2 56123 Pisa, Italy
g.petrangeli@gmail.com

ABSTRACT

Process plant safety and nuclear plant safety have grown up as two substantially separated branches of the safety technology. There are good reasons for that because nuclear plants employ essentially one process only (heating water by nuclear power, producing steam and finally electricity), process plants use many different processes; the size (investment) of the plant also is very variable, as opposed to the situation of a nuclear plant. However, both technologies might benefit of enhanced knowledge exchanges. Fields where such exchanges could be increased are: more intrinsic and passive safety, probabilistic analysis of large plants, fire prevention and mitigation, defence against external natural and man-made events. On the contrary, fields where beneficial interactions seem less promising are: index-based analysis methods, probabilistic analysis of small plants, containment technology. All the previously listed issues are discussed in the paper. Finally, possible ways to enhance knowledge transfer between the two fields are addressed.

1 INTRODUCTION

Process plant safety and nuclear plant safety have initially grown up as two substantially separated branches of the safety technology. There are good reasons for that because nuclear plants employ essentially one process only (heating water by nuclear power, producing steam and finally electricity), process plants, on the other side, use many different processes. The size (investment) of the plant also is very variable, as opposed to the situation of a nuclear plant.

However, both technologies might benefit of enhanced knowledge exchanges. Fields where such exchanges could be increased are:

- more intrinsic and passive safety
- probabilistic analysis of large plants
- fire prevention and mitigation
- defence against external natural and man-made events

On the contrary, fields where beneficial interactions seem less promising are:

- index-based analysis methods
- probabilistic analysis of small plants
- containment technology

2 FIELDS WHERE EXCHANGES SHOULD BE INCREASED

2.1 More Intrinsic and Passive Safety

2.1.1 General Remarks

The nuclear reactors now operating incorporate both passive and active safety features. As an example, reactors have a passive limitation of power excursions through a negative power coefficient of reactivity, which is, for most of them, the outcome of an early recognition that a power excursion might be difficult to limit in presence of self-enhancing dynamic reactor features. On the other side, most reactor emergency cooling systems are active. The variety of solutions does not reflect a precise choice in the early days of nuclear power towards active or passive systems: it reflects the best choice according the sensibility of the designers of that time. Passive and intrinsic safety solutions were adopted when recognized as effective and economically convenient. Moreover, the fundamental safety functions to be accomplished in a nuclear reactor are limited to reactor shutdown, reactor and containment cooling and containment of radiotoxic products: the most natural engineering solutions for these functions were in general adopted, with obvious variations, in all of the reactor designs developed.

With passing time, in depth safety studies and data of operating experience both tended to expand the safety requirements beyond those originally devised. Plants became more complex and part of the passive safety originally present tended to disappear. This is evident, as an example, in containment cooling, which was originally more entrusted to passive, natural mechanisms.

At a certain time in its development, the nuclear industry had, unfortunately, to suffer the two big accidents of Three Mile Island and of Chernobyl, different in many respects from each other, but equally rich of lessons in their applicable technical environment.

Besides these two events, and in a certain sense, anticipating, some of their indications, the integral safety studies of typical plants, starting with the Rasmussen study, called the attention of the technical experts on the need for a complete rethinking on the safety approach until then followed.

Since then, everybody in the technical field was convinced, or, I should say, even more convinced, that accident prevention and mitigation in nuclear plants deserved a very special attention: serious accidents could be avoided, but a continued attention to safety in design and operation was warranted, also including the consideration of important plant design alternatives.

Some facts, in particular, became even more evident than before: in the first place the potential importance of multiple failures in complex safety systems and, secondly, the possible serious consequence of human errors.

Hence, attention was called on passive and, as an extreme, on inherent or intrinsic safety systems which needed less auxiliary systems, were simpler, with a lower number of parts which could fail and did not require as much operator intervention as active systems.

“Passive safety” is the expression currently used to qualify the operating safety features of structures and devices designed to counteract specific events without reliance on mechanical and/or electrical power, forces or “intelligence” signals external to the same structures and devices. These features should rely only on natural laws and properties of materials, as well as on lack of human action. Different degrees of passivity exist; as an example, a safety system may operate without external power but may require some sort of active actuating signal: in this case, too, the system is qualified as passive even if not to the highest degree.

“Inherent safety” means the elimination of hazard by choice of material or design concept; as an example, elimination in a plant of any combustible material (if possible) would implement inherent safety in front of the danger of fires.

In the last few years, much discussion took place on the merits of passive and - intrinsic safety, mostly because, to my opinion, it was too easily postulated by the public that such a thing as an intrinsically safe plant, or, at least, as a passive safety plant, should necessarily exist: the attention was erroneously misplaced more on "intrinsic-passive" than on "safety".

Although it is evident that a substantial research and development effort on simpler and less vulnerable nuclear plants is still warranted, it appears now more generally recognized that the best possible and safest plant at this point in time and one in which serious accidents can be avoided throughout all of its life, probably includes both active and passive features in an optimization perspective. Passive systems, although at first sight attractive for their simplicity, may have drawbacks, as the one of being less powerful and slower in their action; moreover, their reliability is more difficult to evaluate.

The conceptual development in the process (mainly chemical) industry is somewhat similar. Even there, a number of Three Mile Island-Chernobyl type of events exists, which are named Flixborough, Seveso, Bhopal and others.

The first one was an open-air explosion of a flammable gas (Unconfined Vapour Cloud Explosion, UVCE) released into the air by a Nylon plant, which killed the 28 plant employees present and caused extensive property damage in the surrounding territory. Too large inventory of flammable, substances and faulty maintenance operations were mainly blamed as the cause of the event. The second is well known for the dangerous release of dioxin due to poor plant safety features and to human underestimate of the possibility of a runaway reaction. The third one, which killed a still unknown number of people in the order of 4000, was referred again to too large inventory of toxic substances and to very poor staff attention to operability of safety features.

Also in the process industry, plants tended to grow bigger and bigger with passing time and to became, therefore, more complicated and dangerous for the high amount of stored chemicals.

A rethinking period then started also in the chemical industry, pointing to the study of "more inherently safe" plants. The wording chosen is indicative of the need to eliminate the wrong idea of a completely safe plant.

In the following, the main directions followed by these studies in the two fields explored and the main results will be discussed.

2.1.2 **Some passive systems and components for nuclear plants**

Systems and components discussed in the last few years range from complete reactor concepts to single components.

References [1] and [2] list and comment most of the existing proposals.

A rather arbitrary selection of a few among such proposals is presented in the following. They are all well known concepts in the nuclear industry and they are here recalled because they are considered among the most interesting ones.

Passive plant reactors (e.g., AP600, AP1000 W) are proposed future reactors that use the technology of current reactors, but include also significant changes in plant design and layout.

Safety, in the event of an accident, depends on passive safety systems and on safety systems which are passive in operation although started up by a simple action such as valves opening.

In AP 600 and AP 1000, PCCS (**Passive cooling containment system**) is provided to remove heat from the steel reactor containment. The operation of PSIS (Passive safety injection system) following a LOCA results in steam released from

the reactor core being passively condensed inside containment. Steam condensation reduces containment pressure. The PCCS firstly consists of a large tank above the containment structure that allows gravity drain of water on the outside of steel containment vessel. Secondly, opening of air dampers supplies natural circulation air cooling of the external surface of the steel containment. The air and evaporated water exhaust through an opening "in the roof of the shield building. The passive containment cooling system is capable of removing the thermal energy following a design basis event so that the containment pressure remains below the design value with no operator action required for (three) days. The passive containment cooling system is designed to reduce containment pressure to less than one-half its design pressure within 24 hours following a LOCA. After three days, if theresn't supply of water, the heat removal is assured by air alone with an increased pressure (till about design pressure).

In nuclear power plants, the containment is the final barrier to prevent the radioactive release to the environment during accident events. Because of containment importance in mitigating the postulated consequences of an accident, it is necessary not only to assess its integrity during, but also to ensure that it is and stays leak-tight after accident occurrence

Typical allowable primary containment leakage rates lay in the range of 0,1-1% volume/day, but-the operating experience sometimes has indicated “real world” values above allowable limits.

That is usually due to excessive valves or penetrations leakage, valves or penetrations left open after testing, airlocks failure etc.

Studies have been made on the following aspects:

- containment leak tightness enhancement (better choice of valves type, reduction of the number of penetrations, valves stems leakage reduction etc.)
- research of root causes for leak tightness degradation (e.g. debris reduction and deposition on valve seal surfaces and valves behavior under severe accidents)
- conception of a secondary containment to reduce the primary containment releases by hold-up, deposition, filtration, elevated release (for example a secondary containment that envelopes possibly affected buildings equipped with filtration systems)
- monitoring capabilities to detect pre-existing openings in the containment boundary (e.g. monitoring nitrogen leaks in inerted containments)

The ALWR passive plants employ safety grade passive decay heat removal (PDHR) systems in order to enhance the capability (relative to current plants) to maintain the plant in a safe shut-down condition following non-LOCA events.

The approach developed for these systems is founded on meeting the following requirements:

- the PDHR system is employed for both the hot standby and long-term core

cooling modes. This system can operate at full reactor coolant system pressure and places the reactor in the long-term cooling mode immediately after shut-down.

- operation in the long-term cooling mode is automatic.
- operation of the system does non require any ac power, either on site or off site
- operation of the system does not require any pumps or valve operation

once initial alignment is established.

- no make-up water is required for a period of at least three days following reactor shut-down.
- the systems are located entirely within containment.

The passive RHR systems haven't, however, the ability to bring the plant to cold shut-down conditions of 100° C. This is inherent in the passive heat removal process itself because heat removal is accomplished by heat exchangers located within a pool of water, and the temperature on the reactor coolant side of the heat exchanger tubing will, of necessity, exceed the boiling point of water at normal pressure. Cold shut-down can be achieved by the reactor shut-down cooling system, proposed as a non-safety-grade system.

More in particular for non LOCA events the AP600/1000 PRHR system, for example, is designed to perform the following functions:

- automatically actuate to provide reactor coolant system cooling and to prevent water relief through the pressurizer safety valves;
- removing core decay heat assuming the steam generated in the in-containment refuelling water storage tank (IRWST) is condensed on the containment vessel and returned by gravity into the IRWST. The PRHR should provide decay heat removal for at least 72 hours if no condensate is recovered;
- the PRHR heat exchangers are designed to cool the reactor coolant system to 400 F (200 °C) in about 72 hours;
- during a steam generator tube rupture event, the PRHR system remove core decay heat and reduces reactor coolant system temperature and pressure, equalizing primary pressure with steam generator pressure and terminating break flow, without overfilling the steam generator.

During the TMI accident, one of the strategies unsuccessfully tried by the operators to regain control of core cooling was to depressurize the reactor system: the reactor was not designed for that operation and the maneuvre did not succeed. A reactor depressurization system would probably have helped there.

Moreover even the initial PRAs did evidence the possibility of high pressure severe accident sequences for current LWRs. The idea then started to be studied of designing a depressurization system into LWRs. This was a new thing especially for PWRs [3] since BWRs had relief system in order to cope with the possibility of loss of condenser accidents. In principle, a primary depressurization system has many advantages: its operation tends to create an immediate, yet temporary, reactor shutdown effect; it decreases the primary water temperature and favors core cooling; finally, it allows water to be supplied to the core either by high pressure injection systems and by low pressure "jury-rigged" emergency systems (fire truck water and so on). New passive LWRs incorporate a powerful depressurization system which allows emergency water injection to be made by gravity driven (passive) arrangements. Moreover the operation of the primary depressurization system also ensures that the reactor coolant system would be depressurized during a severe accident. Therefore, violent ejection of molten core debris from a pressurized reactor coolant system is highly unlikely for the passive plant with a corresponding reduction in the potential for direct heating of the containment atmosphere. That is also applicable to the evolutionary light water reactors, in fact the NRC staff has concluded (SECY 90.016) that ALWR designs (evolutionary and passive) should include a depressurization system to preclude the ejection of molten core debris under high pressure from the reactor vessel.

Nevertheless the reactor coolant release to containment has the potential for adverse effects on in-containment equipment.

Accordingly, the ALWR plants should be designed to minimize such adverse effects by ensuring that the frequency of inadvertent actuation is extremely low ($2x10^{-3}$/y for passive plants, EPRI, Electric Power Reasearch Institute, U.S.A., requirements) ensuring that recovery from such inadvertent actuation is feasible

without compromising plant availability for a long period (EPRI requirements for passive plants: recovery within 30 days or less). As an example a short description of the AP 600/1000 depressurization system is mentioned in the following.

The AP600/1000 automatic depressurization system consists of sixteen valves divided into four depressurization stages. These valves are installed in the reactor coolant system at three different locations.. The first three stages valves are connected to nozzles on top of pressurizer. The fourth stage valves are connected to the hot leg of reactor coolant loop. The main actuating signals for each depressurization stage come from different level set points in the core make up tanks (CMTs that provide high pressure make-up by gravity).When the CMT is going to deplete, the depressurization takes place to allow low pressure injection from IRWST (in-containment refuelling storage tank) by gravity.

Moreover the depressurization system together with passive injection of borated water from IRWST could ensure safe shutdowns in the long term in case of ATWS if other active systems are not available for this purpose.

The design of hydraulic engineered safety features of LWR's has been traditionally performed according to high reliability and leak tightness standards. These systems are usually called into operation to protect the fuel barrier in the case of a loss of the primary system barrier. In addition, being strictly connected to the primary circuit pressure boundary, they have to be equipped with leak tight isolation devices, normally closed during plant operation. Squib valves, initially used for applications in the space industry, have been considered very attractive for the application in an advanced passive reactor. These valves are characterized by a no-leak capability and, once actuated, they are designed to maintain the open position.

The inlet chamber of the valves in normally closed by a sealing cap. When the valve is actuated, an explosive initiator pushes a plunger that shears the cap off.

This kind of actuation has resulted very reliable from operating experience and qualification tests. These valves require very limited maintenance. If fact no periodic intervention, other that the substitution of the initiator, is necessary.

Additional benefits associated to their use in Automatic Depressurization Systems are related to the possibility of providing a flow area larger than that traditionally obtained with standard Safety Relief Valves (SRV). Such a large area is very important in passive reactors to depressurize the primary system at very low pressures, consistent with the operation of injection systems based on gravity.

The installation in the core cooling injection system, in addition to the benefits associated to the leak tightness characteristics, allows to ensure, during normal operation, a pressure shielding function on the upstream check valves. Therefore, these valves do not remain forced in the closed position for long times,. and that improves their reliability when called to open under a low differential pressure.

The "density locks" (or "hot-cold interfaces") are passive devices which perform the same function of normally closed valves during normal operating conditions. However in case of transient or accident conditions they allow cooling flow without need of power supply or motion of mechanical parts.

The density locks have been applied in the PIUS (Process inherent Ultimate Safety) reactor concept [1] [2]. In it the reactor core is immersed in a large pool of pressurized, cold, borated water. The hot primary water and the cold pool water are in contact by two "hot-cold interfaces" (high and low elevation in the cooling

circuit) where, during normal operation, substantial mixing is prevented by design details and by pump speed (head) adjustment, governed by the lower interface temperature. In case of uncontrolled accidents of any origin, the core will tend to overheat causing water boiling and the decrease of the hydrostatic head in the riser pipe above it, beyond the correction capability of the pump speed control system.

In these conditions, natural circulation between the cold pool, the core and the riser pipe will be established through the two "hot-cold interfaces" along an always open natural circulation path. The pool cold borated water will then enter into the core and will shut the reactor down and remove the decay heat. In a certain sense, PIUS safety is based on the use of an essentially unstable cooling circuit, which needs active pump action to ensure stability during normal operation; in off-normal conditions, the system automatically switches to its stable condition which also is a safe shutdown condition.

The "density locks" carry on a fundamental role in PIUS to ensure core cooling during emergency conditions and thus the potential for their blockages caused by gas collection, material distortion or plugging by detached insulating materials should be analyzed in depth. The density lock concept has been used in other new reactor schemes.

Fluidic diodes and vortex valves are passive devices whose application to future NPP's is currently under evaluation with reference to their potential of use as check valves or actuation valves in safety related systems. Fluidic diodes, used in reprocessing plants and chemical industries, are one-way valves with no moving parts. They are characterized by a very high flow resistance in one direction with respect to the other.

This characteristic allows their application to NPP's as flow limiters to maintain core coolant boundary integrity in the case of a LOCA event. In a potential application to a typical PWR system, a fluidic diode is installed on the reactor pressure vessel nozzle of cold legs to avoid reverse flow conditions following a pipe break. Due to the diodes characteristics, instead of a massive release of coolant, only limited leaks would occur.

Vortex valves are "normally active - passive during emergency" devices designed to maintain separation between environments normally operating at different pressures. This function is performed by the fluid movement provided by a normally operating pump. A potential application to NPP's safety features is as actuation valves in case of transients or accidents.

In fact during normal operation the two environments remain isolated as if they were provided by a standard isolation valve. Following a transient the pump operation is expected to be interrupted or its head capacity to be overcome and water can flow from the environment at high pressure to that at low pressure.

In the field of Process Industry Plants the concept of more inherently safe design is a recurring theme in the three reports of the Advisory Committee on Major Hazards (ACMH), which was set up in U.K. after the Flixborough accident. These reports set the general principles of the "new" process industry safety in U.K. and they represent in their field what, as an example, the IAEA "Safety Fundamentals" documents does in the nuclear industry.

A full account of the developments of this concept is given in References [4], [5],[6]. The magazine "Loss Prevention Bulletin, Institution of Chemical Engineers, England" is also a "must" for interested people; it is available in most technical libraries and a list of the main articles appeared over the years is included in Ref. [4], Vol.3. The basic principles of inherently safer designs in the process industry are:

- intensification, namely carrying the chemical reaction in a smaller volume in order to have a lower inventory of dangerous substances and smaller consequences of an accident,

- substitution (of a dangerous process or substance, e.g. an heat transfer medium, with a less dangerous one),

- attenuation (adoption of a less hazardous process condition, e.g. of a lower pressure in combination with the improvement of a catalyst)

-simplicity (e.g. designing a vessel or pipe for full overpressure instead of adopting a pressure-relief system); as Henry Ford used to say "What you don't fit costs nothing and needs no maintenance",

- operability (adoption of a process which can be easily controlled and adjusted to off-normal conditions)

- fail-safe design (where the failure of the system leads directly to a safe condition)

- second chance design (second line of defense)

Interesting examples of proposals in the process industry follow.

The first typical example concerns the fabrication of nitroglycerine. It has to be classified as an "intensification" of the process, namely as a drastic reduction of the inventory of the dangerous substance. Nitroglyceryne is manufactured by the reaction between glycerin and a mixture of concentrated nitric and sulphuric acid. The reaction is highly exothermic and the mixture has to be continuously cooled and stirred, otherwise a violent explosion may occur due to the uncontrolled decomposition of nitroglycerine. Originally the reaction was performed in batches using large (one ton) pots. The operator had to continuously monitor the temperature and check that stirring was effective: since the reaction lasted a rather long time (hours) there was the danger for the operators to fall asleep and, therefore, they used to work sitting on one-legged stools, as it can be seen in historical pictures, one of which is sketched in Figure 1.

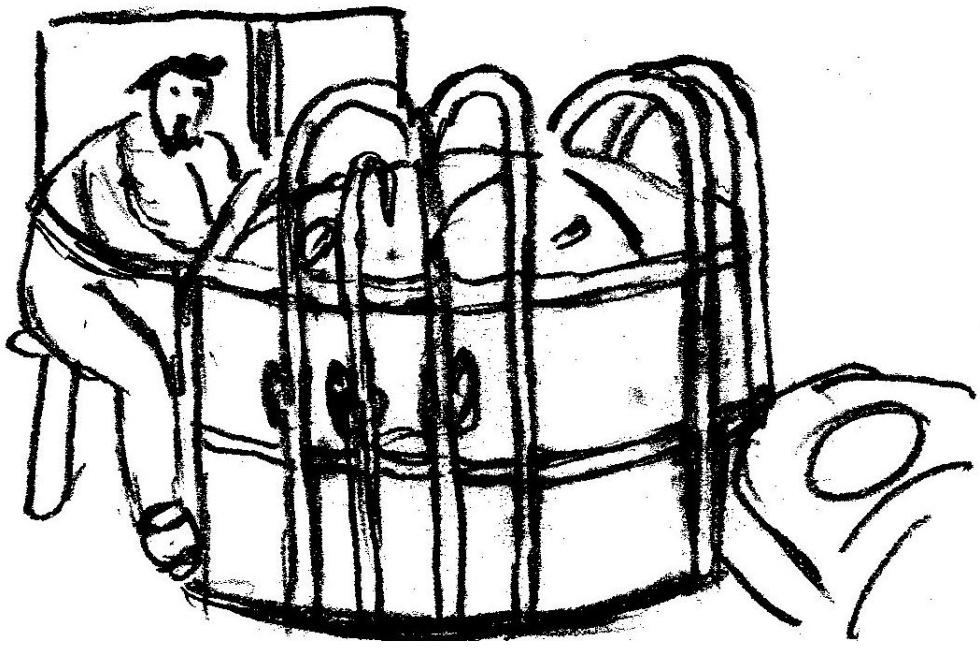


Figure 1: Manufacture of nitroglycerine in old times

This kind of process continued to be used until fifty years ago with a number of casualties and complete plant losses. The same reaction is now obtained in a, small injector where the acid jet entrains the correct amount of glycerin and, due to the turbulent mixing, the reaction time has been reduced down to minutes and the reaction is complete at the exit from the injector. The amount of nitroglycerine in the reactor is reduced to a

few kilograms and the operators can be protected by a blast wall. In another reaction, the adipic acid reaction, the process was previously performed in a huge reactor with external circuits for cooling; now it is performed in a smaller integral vessel with internal cooling and agitation and with a very smaller possibility for leaks. A similar evolution has taken place in nuclear reactors which were transformed from external to internal recirculation units or in integral proposals for future reactors.

It is also worth mentioning the so called Higee ICI process, where the process of gravitational separation is enhanced by centrifugal forces in a rotating unit, with consequent decrease in amount of substance in the separator.

Many examples are available concerning the substitution of one process with a less dangerous one.

In a number of cases in the chemical industry the choice has to be made between the availability of a large storage of substances and the reduction of stored substances concurrent with the continuous production of them on site. In the first-case, continuity of production is better assured but the risk of the storage is present. In the second case, the opposite advantages- drawbacks are present. The concept of inherent safety would incline to make the second choice. It has to be remembered that in the case of Bhopal, a total pessimization of the situation was created because at a certain point in time it was decided to produce methyl isocyanate (MIC, the poison which was released in the accident) on site instead of importing it from another factory, but the already existing huge MIC tanks continued to be used with the consequent risk. Major reductions of inventories have, however taken place in the last years on safety grounds, following the Bhopal event and some new regulations concerning, in particular, hazardous substances as ethylene oxide, propylene oxide and sulphur trioxide.

A large progress in the safety of the chemical industry is being made in a field of strong interest for the nuclear plants too: the reduction of the possibility of leaks from containments through the reduction in the number and the dimension of penetrations.

Simplification of detailed design is also pursued by such measures as design for overpressure and design modification to avoid instrumentation, simple cases of the latter operation is the use of suitable piping arrangements to avoid reverse flow and to provide for automatic sump voiding (high turns of pipe with anti-syphoon openings, selfpriming syphoons and so on).

It seems worth noting, concerning the operability-,concept of the above included list, its similarity with those provisions, in the nuclear plants which tend to provide a longer "grace period" in case of mistakes or accidents (increase of the water inventory in water reactors, and so on).

Speculative proposals for the long range also exist. One of them considers the advantages to have distributed manufacture of chemicals using miniaturized plants at the users site; such plants would be more environmentally friendly and would deliver their products on a "just in time" basis; they should also be completely automated, highly reliable, self cleaning and sealed for life.

As it is apparent from what discussed above, in a number of instances the process industry has gone beyond the study phase in the way of the adoption of more inherently safe provisions.

Safety experts in the process industry, however, complain that not enough has been done [5] in this direction. Some of the constraints towards a higher level of inherent safety are: - time ("the technical options available for the next plant are usually limited by time, so if major advances are to be made there has to be thought about the "Plant after next", namely during the design stage of a plant there is not enough time to discuss and to develop alternative designs); - desire for certainty of production (if a new process or a

new equipment is used, then unforeseen difficulties may cause trouble during start-up, perhaps delay or prevent the achievement of design output or efficiency); - the influence of the process licencers is often on the side of tradition (for the possibility of unforeseen snags and surprises); - technical misconceptions (like the belief that, e.g., reduction in the inventory of dangerous substances may render the control of the process more difficult); - organization scheme (the organization of a company in business areas instead of in functional departments is not favorable to innovations because of the strong influence of the control of expenditures); ill defined responsibility for design innovation (research departments or design departments).

It has been remarked that it is difficult to convince interested people that there is a problem of improvement of safety level: many are accustomed to think that hazard is inherent in industry (which may be true to a certain extent) and it didn't occur to them that in many cases 'it may be possible to avoid hazards.

2.2 Probabilistic Analysis of Large Plants

A full complete probabilistic analysis of a large plant may cost millions of euro. Although this amount is reduced for smaller, simpler plants, it often occurs for process plants that a full probabilistic safety analysis is not justified on economical grounds. This is the reason why this kind of analysis will be confined to nuclear plants or to large process plants or industrial areas, as it was the case with the famous Canvey Island complex analysis in years 1975-78 or with the Rijnmond area in The Netherlands.

2.3 Fire Prevention and Mitigation

Fire prevention provisions and techniques were, till several years ago, much more advanced in the process plant field than in the nuclear plants. Presently, nuclear plants regulations have made important progress in the fire protection area. A fire risk analysis is now common place in presently operating plants. Various accidental events contributed to increase the attention towards this phenomenon in nuclear plants. The most famous event was the Brownsferry Fire in 1975, where a penetration leak-tightness check made by a candle flame (very sensitive instrument, indeed) caused a local fire and the incapacitation of a number of essential electrical circuits [7]. Remedial actions by the plant personnel were put into effect, including “heroic” and creative actions not envisaged by the plant emergency procedures and the function of damaged emergency systems was recovered at last. The event was very dangerous indeed and thorough inquiries followed by general recommendations for the future.

2.4 Defence against External Natural and Man-made Events

Natural events like earthquakes and tornadoes are of interest both to nuclear and process plants. The most significant advancements in the study of these phenomena and in the response of industrial structures and components were made firstly in the nuclear field and then adapted to the more general case of industrial plants. The most vivacious developments started in the nuclear field at the end of the years ‘50s. Before that time, essentially civil building rules were applied also to industrial plants. The problem is that the objectives of the seismic study of civil buildings are different from those of nuclear and process plants. In fact, as it is known, the legislator intends to reach two objectives for the protection of civil buildingss:

1. *Avoiding any form of damage to structures* in case of an earthquake with a return time roughly equal to the normal life of a building (e.g. 100 years),

2. *Avoiding the collapse of the structure,* even accepting damages, in case of the most violent earthquake expected on the site.

On the contrary, for an industrial plant either nuclear or in any case with a risk of a serious accident, the protection objectives could be expressed in the following way:

1. *To ensure the continued operation of the plant* in the occasion of an earthquake with a return time equal to its normal life, possibly after an inspection and simple and occasional repairs of damaged components,
2. *Avoiding a serious accident* in the case of the most violent earthquake expected on the site.

As it is evident, the two points of view are different and, while the current norms considers damages and collapses, the needs of protection of a plant concern its functionality and the absence of accidents; these concepts imply, in particular, the absence of significant leaks of noxious gases and liquids, the absence of reactions and of uncontrolled and destructive phenomena and the functionality of the safety equipment (shutdown, cooling, containment and control). Moreover, the components and the phenomena of interest in industrial plants are not covered by the methods used in the civil structures. In particular, in the plants, phenomena not taken into consideration by the norms can happen and therefore the need arises to indicate acceptable verification methods, which are in any case logically compatible with the spirit of the norms themselves. A typical case concerns the phenomenon of liquid oscillations in industrial tanks caused by earthquakes and of the possible consequent effects (in particular for large atmospheric tanks, Figure 2: impact of the liquid against the roof and consequent damage, A, increase of the overturning moment on the tank and possible damage of anchors ,C, and elastic-plastic instability of the vertical wall, B).

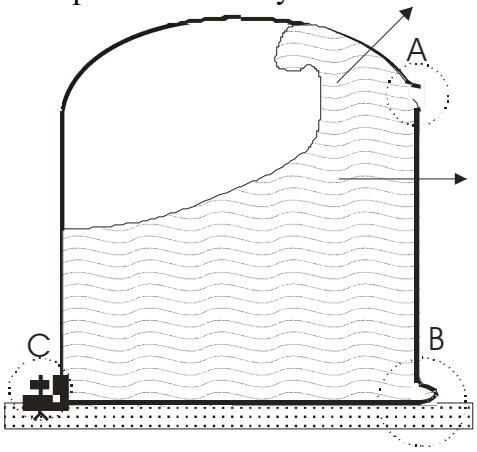


Figure 2: Weak points of a tank in case of earthquake

Concerning man-made events, it is generally thought that this issue is mainly of interest to nuclear plants, for which any accident has a wider resonance in the media and in the public opinion. They should, however, be also considered possible for other types of plants and of installations. The September 11 2001 attack to the World Trade Center in New York City was, indeed, aimed at buildings, although of extremely high significance for the public opinion. In any case, the methods of analysis and the provisions against an aircraft attack have firstly been developed for nuclear plants. This is one of the cases where a bulk of knowledge and of experience can turn to be useful also for process plants. I can quote from my experience of work the study of an aircraft impact on an offshore Liquid Natural Gas (LNG) Terminal, which was performed with satisfactory results using mainly assumptions and methods taken from the nuclear plant experience [8].

3 FIELDS WHERE EXCHANGES SEEM LESS PROMISING

3.1 Index-based Analysis Methods

These methods have originated in the chemical industry for thesimplified yet complete evaluation of the safety level of a plant. Examples are the “Dow Index method” and the “Mond Index method”. In substance, A safety index is calculated as the sum of various contributions which are calculated, by formulas and tables, starting from physical quantities pertaining to the various parts of a plant, as amount of noxious substances present, operating pressure of vessels and piping systems, etc. According to the value assumed by these index, the plant is considered acceptable or not. No general consensus exists on the merits of these methodologies. The principal criticism is based on the doubts about the capability of such methods to give the correct importance to specific features of a plant, which could not be considered in the list of items included in the calculation of the index. However, these methods are rather widely used in a specific context, like sets of similar plants originated by a single design organisation; they are also used as first, quick check of the safety level in view of a subsequent complete safety analysis or for very simple plants. The index-based methods are not considered generally useful for nuclear plants and none of them has been proposed. However it is true that for a class of plants, as for example PWRs of a certain vintage, simplified analysis can be made which are based on experience and knowledge of the most likely weak points of a plant of the category under consideration. These kind of analyses are currently made during the safety reviews performed by working groups assembled upon request by international organisations (e.g. IAEA) in one or two weeks of work. The issues considered in these reviews are chosen on the basis of the past experience of the expert reviewers, who, after many safety reviews, well know where to look for possible weak points in a plant design [7].

3.2 Probabilistic Analysis of Small Plants

The cost of a probabilistic analysis is here the difficulty. The investment involved in a small chemical plant does not warrant the performance of a full probabilistic analysis. It is more convenient to exceed in the implementation of additional and superabundant safety margins in design and operation of the plant. A full probabilistic analysis is likely to stay confined to large nuclear plants or chemical complexes. Some form of limited probabilistic analysis has, however, been studied for smaller plants or parts of plants, like the Hazan method [4].

3.3 Containment Technology

Even for nuclear plants the original concept of a containment system for the confinement of possible noxious releases has for a long time been considered by many as an undue waste of money. After the Three Mile Island accident, however, where the containment played a mayor role in mitigating the external consequences of the accident, a general consensus consolidated on the advisability of a pressure resistant, leak-tight containment around most types of nuclear plants (PWRs, BWRs, FBR and HTRs in particular). No such provision is likely to be applied to other kinds of process plants, with the possible exception of small parts of them. The experience gathered with nuclear plant containments can be useful in such cases. Indeed, the concept of containment is not so simple as it appears at first glance. The containment system is, primarily, a system and not a simple passive container; automatic

isolation devices, leakage reduction and collection-filtration systems, structural protections against thermal damage in accidents and against impact effects of internal origin, protections against external threats etc., are all components of this complex concept [7].

4 Ways to further enhance knowledge exchanges between nuclear safety and process plant safety

The main point is very simple and is that if responsibles within organisations in both fields are convinced that an increased exchange of information can be beneficial to all, all the possible actions will quite naturally follow. Examples are:

- publish in technical magazines of one field some paper coming from specialists in the other field if the subject can be applicable to both,
- give room to papers in both fields in seminars and conventions, as it is done here with this invited paper,
- organize courses, masters, specialisation schools which deal with both fields,
- favor within interested organisations exchanges between the two fields, avoiding a sharp separation between differently oriented organisation units and creating occasions for knowledge exchanges (seminars, mixed working groups, etc).

REFERENCES

[1] C.W.FORSBERG et al., “Proposed and existing passive and inherent safety related structures, systems and components (Building Blocks) for advanced light water reactors”, ORNL-6554, 1989

[2] G.PETRANGELI, Safety Technologies and Safeguards, Proceedings, "50 Years from the Fermi Pile", CIRTEN-Pisa University, 1992

[3] - G.PETRANGELI, R.Tononi, F. D'Auria, M. Mazzini, “The SSN: an emergency system based on intentional coolant depressurization for PWRs”, Nuclear Engineering and Design 143 (1993) 25-54, North Holland

[4] F.P.Lees, Loss Prevention in the Process Industry, 3 Vol., Butterworth-Heinemann, Oxford 1996, Second Edition

[5] T.A.Kletz, Cheaper, Safer Plants or Wealth and Safety at Work, The Institution of Chemical Engineers,Rugby, England, 1984

[6] Proceedings of "Safety in the Chemical Industry - Inherently Safe Plant", University of Manchester, Institute of Science and Technology, Manchester 1982

[7] G. PETRANGELI, “Nuclear Safety”, Elsevier, Oxford, 2006

[8] G.PETRANGELI , “Caduta di un Aereo su un Serbatoio di GNL in Mare” (Fall of an Aircraft on an Offshore LNG Terminal”, Proc. of VGR (Valutazione e Gestione del Rischio negli Insediamenti Civili ed Industriali, Risk Evaluation and Management in Civil and Industrial Installations) 2008, Pisa, 14-16 October 2008

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

Use of PSA in the Design and Construction Phase of NPPs in Finland

Risto Himanen, Jari Pesonen
Teollisuuden Voima Oyj
Olkiluoto, 27160 Eurajoki, Finland
risto.himanen@tvo.fi, jari.pesonen@tvo.fi

ABSTRACT

Teollisuuden Voima Oy (TVO) owns and operates two BWR units (OL1 and OL2) in Southern Finland, and it has one PWR unit (OL3) under construction. This paper presents the main requirements on the use of PSA for new nuclear plants to be built in Finland, and highlights the experiences from the application of PSA in the design and construction of Olkiluoto 3. The Finnish Regulatory Body STUK requires that the design of new nuclear power plants be supported by PSA. The paper gives an overview of the detailed Authority requirements of PSA in numerous applications. The Authority requirements are somewhat tighter for the new plants than for the operating plants, because early use of PSA makes it possible to perform design comparisons and also correct the design weaknesses and errors before commissioning. STUK reviews thoroughly the analysis two times before the commercial operation, namely before granting the construction license and before granting the operation license. Construction license assumes an approved construction phase PSA. The PSA is complemented and updated during the construction phase, and used in several applications in the detailed design. The result is the living PSA for operation phase, approval of which is a condition for the operation license.

1 INTRODUCTION

Teollisuuden Voima Oy (TVO) owns and operates two BWR units (OL1 and OL2) in Southern Finland, and it has one PWR unit (OL3) under construction. In connection with the licensing of the operating plants, probabilistic methods have been used late since the 1970's. The Finnish Regulatory Body STUK published in the year 1985 the first version of the guide YVL 2.8, in which the requirement on PSA including levels 1 and 2 was presented. TVO started the preparation and analysis of level 1 PSA for the identical boiling water plants in the same year, and sent the first report, consisting of the analysis of internal initiating events, to STUK four years later. The PSA for OL1 and OL2 has grown during the last decade as a comprehensive PSA program, and it has been actively used in the safety management of the utility and as a communication tool in discussions with STUK.

The Finnish Regulatory Body STUK requires that the design of the new nuclear power plants is supported by PSA. The requirements are somewhat tighter for the new plants than for the operating ones, because early use of PSA makes it possible to perform design comparisons and also correct design weaknesses before commissioning. The regulatory guide YVL 2.8 also requires a PSA to be performed and applied during the design and construction of the plant. It stipulates that the contents, the documentation and the applications shall be

completed in different phases of the plant life cycle and sets requirements on the quality management. STUK reviews thoroughly the analysis twice before the commercial operation, namely before accepting the construction license application and before accepting the operation license application.

AREVA NP as the vendor is responsible for the conduction of the PSA in the OL3 project, while TVO as the owner reviews and accepts the used methods in advance and the results. However, both parties benefit on having the up-to-date model to reflect most recent design status of the plant. The owner can review in a detailed manner the applications by the vendor, assumed that the models and calculations are transparent. TVO can also make its own analyses and study design alternatives. The common PSA model improves the transparency of safety management of the OL3 project.

2 PSA OBJECTIVES

2.1 TVO practices and objectives

TVO has developed its own living PSA concept. It is widely used in safety management of the plant and fulfils the regulatory requirements. The living PSA is based on four elements:

1. Plant specific and up-to-date PSA model.
2. Plant specific and up-to-date probabilistic data.
3. Fast enough and transparent computer code to run living PSA and to support the operation department and the technical department of TVO.
4. Plant specific and up-to-date procedures for use and updating of the PSA in order to define the responsibilities for the separate organizations.

The speed of the code and the transparency of the model and the results it produces is vital. Flexible tracing of the origin of the min cut sets and studying the results of individual accident sequences are crucial in the serious use of PSA as a support for design and for daily plant operations. Efficient use of PSA requires extensive possibilities for post processing of the minimal cut sets. Similar application of living PSA concept is the objective of TVO also in the construction project of the OL3 unit. TVO has selected fifteen year ago the Finnish code SPSA. The codes for OL3 level 1 PSA are FinPSA, which is a new Windows code based on SPSA, and SPSA for level 2.

2.2 Regulatory safety objectives

The Finnish regulatory guide YVL 2.8 “Probabilistic safety analysis in safety management of nuclear power plants” shows how probabilistic safety analyses are to be performed and used in the design, construction and operation of light water reactor plants.

According to the Government Resolution (395/1991) “*accidents leading to large releases of radioactive materials shall be very unlikely”*. STUK has defined probabilistic target values for the core damage frequency and for the release of radioactive materials. The mean value of the probability of core damage shall be less than $1 \cdot 10^{-5}$/year. The mean value of the probability of a release exceeding the target value defined in section 12 of the Government Resolution (395/1991) must be smaller than $5 \cdot 10^{-7}$/year. The target value for the release is defined so that the release shall not have “*acute harmful health effects to the population in the vicinity of the nuclear power plant nor any long-term restrictions on the use of extensive areas of land and water. For satisfying the requirement applied to long-term effects, the limit for an atmospheric release of cesium-137 is 100 TBq.*” Such a release corresponds less than 0.01% of the Cs 137 inventory in OL3 core.

STUK requires that PSA is used in the design phase to support the balance of the design. The following requirement in YVL 2.8 also sets certain requirements for the tool used: "*The risks associated with various initiators and accident sequences, taking into account their uncertainties, are to be compared with the numerical safety objectives and with each other in order to ensure that no single or few prevailing risk factors will stay at the plant.*"

3 REQUIREMENTS ON THE SCOPE OF PSA

3.1 Authority requirements

There are requirements on the content and documentation of PSA in YVL 2.8. The guide gives a list of topics, which one shall be able to trace from assumptions of the PSA to the final results. In addition to power operation, low power and shut down states and the transfers between them shall be considered in the PSA. Events such as internal failures, disturbances and faults, loss of off-site power, fires, floods, harsh weather conditions, seismic events and other external and human caused initiators shall be included as initiating events. However, YVL 2.8 does not cover intentional damaging of a plant.

The level 1 PSA shall identify the accident sequences leading to core damage and to determine their probabilities. The level 2 PSA shall determine the amount, probability and timing of radioactive substances released out from the containment in consequence of core damage. Besides leaks and ruptures of the containment, also the bypass sequences and controlled release of radioactive materials shall be assessed. YVL 2.8 gives a list of issues that level 2 shall include, e.g. interface with level 1, containment event trees, systems reliability analysis. Source terms from the reactor, transportation, retention and respective probabilities have to be analysed. Appropriateness and efficiency of the strategy of accident management and the balance between systems have to be assessed. YVL 2.8 also gives a list of severe accident issues to be analysed, e.g. reaction forces, hydrogen issues and recriticality. However, the list gives only examples, and all the plant specific issues have to be mapped out and analysed as realistically as possible.

3.2 Scope at the beginning of the life cycle

Voluntary use of PSA in safety management is an integrated part of the developed safety culture, and the fulfilment of the authority requirements is only one part of it. A simplified PSA in the feasibility study of a plant concept can be based on the analysis of an existing plant corrected with the main modifications in the design. Then, it is important to foresee that there are no fundamental problems in the design.

In the bidding phase it is important to show that the plant can meet the regulatory targets. A quite comprehensive level 1 and level 2 PSA is necessary, but it can be based on the analysis of existing plants of similar design or delivered earlier by the same vendor.

STUK reviews the preliminary level 1 and level 2 PSA for the first time in connection with the application for the construction license *i.e. design phase PSA*. STUK may require supplementing the analysis before approving it for the construction license. In any case the PSA needs to be complemented during the construction phase, and during this phase it will be used for several applications.

The result of the work during the construction phase is a complete level 1 and level 2 PSA for the operation phase. An approval of this PSA is a condition for the operating license. STUK reviews the PSA, i.e. construction phase PSA, the second time in connection with the application for an operating license.

4 REQUIREMENTS ON THE APPLICATION OF PSA

4.1 Authority requirements in the PSA specific regulatory guide YVL 2.8

In the guide YVL 2.8 there are several requirements of applications and references to corresponding guides. In YVL 2.8 following applications are required:

In design phase:

- *Safety classification shall be assessed by PSA. The assessment shall be used to demonstrate that the requirements for quality management system concerning the safety classification of each component are adequate compared with the risk importance of the component. The probabilistic review of the safety classification shall be submitted to STUK in conjunction with the safety classification document.*

In construction phase:

- *The purpose of the level 1 and 2 construction phase PSAs is to ensure the conclusions made in the design phase PSA on the plant safety and to set a basis for risk informed safety management during the operation phase of the plant. The level 1 and 2 PSAs shall be based on the plant specifications submitted in conjunction with the application for an operating license.*
- *The application for an operating license shall demonstrate that the plant meets the numerical design objectives set forth in section 2.1 of this Guide. Should substantial risk factors not recognised earlier appear before the commissioning of the plant, the applicant for a licence shall upgrade the safety of the plant. In conjunction with the design of safety upgrades the applicant for a licence shall demonstrate that the safety of the plant assessed after the upgrades is substantially at the same level or better than the objectives presupposed for the design phase.*
- *The technical specifications shall be reviewed by PSA in such a way that the coverage and balance of technical specifications are ensured. The review must cover all operating states of the plant.*
- *The results of PSA shall be applied in the review of safety classification as in the design phase if extensive changes are performed in the plant design in the construction phase.*
- *The results of PSA shall be applied in the working up of programs of safety significant systems testing and preventive maintenance during operation, and in the working up of disturbance and emergency operating procedures*
- *The results of PSA shall be used in the drawing up and development of the inspection programs of piping as per Guide YVL 3.8.While drawing up the risk informed inspection program, the systems of classes 1,2,3,4 and EYT (not safety related) must be regarded as a whole.*
- *The results of PSA shall be taken into account in the planning of personnel training.*

4.2 Authority requirements on PSA applications in other YVL guides

STUK assumes in several other guides application of risk informed methods and PSA. E.g. the top-level guide YVL 1.0 “Safety criteria for design of nuclear power plants” states in connection of human errors that “*According to section 19 of the Council of State Decision (395/91), special attention shall be paid to the avoidance, detection and repair of human*

errors. The possibility of human errors shall be taken into account both in the design of the nuclear power plant and in the planning of its operation so that the plant withstands well errors and deviations from planned operational actions. In that guide, a requirement for PSA application is stated as follows: *"In failure analyses required in Guide YVL 2.7, human error shall be considered and it shall be demonstrated that individual errors do not prevent safety functions. The possibility of multiple human error shall be assessed in the plant probability safety assessment (PSA) and the necessary measures to avoid or reliably detect errors shall be planned".*

The guide YVL 2.0 "Systems design for nuclear power plants" states that: "*Systems design shall employ both deterministic and PSA-based methods.*" It continues: *"With probabilistic safety assessment (PSA) the reliability of various safety functions and the balance of design between them is evaluated. A plant shall be so designed that calculated risks are distributed such that no individual component, system, phenomenon or other factor is risk-dominant and that the share of hard-to-manage risks is as low as possible. A plant designed in such a way has a well balanced design. High reliability of operation is required of all systems and of safety systems in particular. This is why system operation in various failure situations shall be assured. This is accomplished by applying the redundancy, diversity and separation principles (Section 18 of Government Resolution No. 395/1991.*"

The requirement in YVL 2.0 assumes a transparent computer code and a PSA model in order to be able to check the design balance: "*It shall be demonstrated by PSA methods that a plant's design is well-balanced in terms of reliability, as per subsection 2.1. It shall specifically be demonstrated that a well-balanced design has been reached between*

- *various safety functions*
- *different systems carrying out the same function*
- *main systems and support systems*
- *subsystems of the same system*

In addition, it shall be ensured that risks (in terms of both core melt and/or environmental release frequency and severity) are distributed between various initiating events in such a way that no individual event sequence, system, subsystem, structure or component causes a major contribution to overall risk."

Making comparisons between design alternatives requires using a fast and flexible computer code with enhanced post processing capabilities. The FinPSA code used by TVO fulfils this requirement.

PSA support for system evaluation is required during the PSAR phase: *" a description of a system's importance in the accomplishment of a safety function proper if the system supports a system performing a safety function and the reliability target of the safety function in whose implementation the system contributes"* Accordingly, in the FSAR phase (for safety class 1 - 4 systems): *"a probabilistic assessment of a system's significance for plant safety using importance measures (see Guide YVL 2.8)*". YVL 2.0 continues: "*The system's analysis demonstrates the fulfilment of its design bases and requirements. Essential analyses to be included in a safety analysis report or topical reports include among others an analysis of the system's physical operation, a single-failure analysis, a Failure Mode and Effect Analysis (FMEA), and importance measures. The mutual order of importance of the various analysis types varies according to the field of technology".*

The guide YVL 2.6 "Seismic events and nuclear power plants" requires seismic PSA in the design phase in the demonstration of earthquake resistance: "*The results of a design-phase PSA shall also demonstrate that the implementation of seismic design is acceptable from the viewpoint of the nuclear power plant's overall safety.* It continues with more detailed requirements "*The most important initiating events, due to earthquake-induced failures and*

malfunctions, shall be incorporated in the design phase PSA. When choosing the initiating events, the following factors shall be considered: S2[1] *category structures and components plus their supports as well as experiences of the susceptibility to failure of different types of structures and components in actual earthquakes of varying magnitudes. The possibility of failure chains attributable to the simultaneous dynamic loading of large component entities and of common cause failures shall be analysed.*"

The guide YVL 2.7 "Ensuring a nuclear power plant's safety functions in provision for failures" also requires, in connection of general design principles, that: "*Both deterministic and probabilistic design principles shall be employed in the design of safety systems. When setting reliability requirements for the safety functions the likelihood of occurrence of the initiating event and the severity of its consequences shall be considered."*

The guide YVL 3.0 "Pressure equipment of nuclear facilities" states: "*Risk-informed methods may be used in choosing the components to be inspected. The procedure is described in Guide YVL 3.8.*"

The guide YVL 3.8 "Nuclear power plant pressure equipment - In-service inspection with non-destructive testing methods" requires using risk informed methods: "*In the drawing up of inspection programmes for Safety Class 1, 2, 3 and 4 piping and Class EYT (non-nuclear) piping as well as in the development of inspection programmes for operating plants, risk-informed methods shall be utilised to ascertain the inclusion in the inspection scope of those components posing the highest risk.*"

In guides YVL 3.2 "Nuclear facility pressure vessels" and 3.5 "Ensuring the firmness of pressure vessels of a NPP" there is a requirement of estimating the brittle fracture probability.

Fire PSA is required by the guide YVL 4.3 "Fire protection at nuclear facilities": "*Together with the initiating events analysed in the design phase PSA the fires shall be assessed in order to evaluate the fire protection arrangements and to identify the risks caused by fires.*" Especially, the following analyses are addressed: "*Fire hazards analyses shall always be performed for the containment and the control room. By means of the containment fire hazards analysis it shall be demonstrated that the safety functions of the plant can be reliably accomplished during and after any potential fire accident in the containment: the reactor can be shut down and maintained subcritical, the plant can be cooled down to cold shutdown condition and the residual heat can be removed. By means of the fire hazard analysis of the control room it shall be demonstrated that the control of the necessary safety functions can be accomplished in the event of a fire in the control room or in any other fire compartment*". Also, the YVL 4.3 addresses the need of keeping PSA up-to date as follows: "*Maintaining and continuously advancing the fire safety of nuclear power plants is a part of the safety culture conducted in the operation of the nuclear power plants. Maintaining and advancing the fire safety includes updating the PSA, described in Guide YVL 2.8. Also fire hazards analyses and other documents shall be updated if the conditions of the power plant change or modifications of the plant fire protection arrangements are performed. New research results in the fire field, the general progress in the field, accumulated knowledge of the fire events as well as the ageing effects of the components and materials shall be taken into account in the fire hazards analyses and in the operation and inspection activities of the power plant".*

[1] Seismic classification: the structures and components of Nuclear Power Plants are to be classified into the seismic categories S1 and S2 according to their required resistance to earthquakes. Seismic category S1 comprises structures and components whose failure could cause an accident situation directly or indirectly leading to a reactor core melt. Seismic categroy S2 comprises all other structures and components and no earthquake resistance requirements relating to their own operation and integrity are set but their failure must not compromise structures and components in seismic category S1.

The guide YVL 5.2 "Electrical power systems and components at nuclear facilities" requires use of PSA for several purposes, e.g.: "*in the drawing up of testing programmes and preventive maintenance programmes*" and "*to assess alternative solutions*". Also, the guide contains requirements for safety analyses: *"Demonstration of the fulfilment of functional and performance requirements by analyses is part of the qualification of electrical power systems and components. Safety Class 2 and 3 electrical power systems shall be subjected to a failure mode and effects analysis, a common cause failure analysis*

an operating experience analysis, a selectivity analysis to demonstrate the fulfilment of the selectivity requirements for electrical protection, a safety analysis to demonstrate the fulfilment of safety requirements. In addition, Safety Class 2 electrical power systems shall be subjected to a quantitative reliability analysis and Safety Class 3 electrical power systems to a quantitative reliability analysis according to their safety significance". In addition, specific requirements are given for computer-based systems and components in the YVL 5.2.

Similarly, the guide YVL 5.5 "Instrumentation systems and components at nuclear facilities" sets several requirements for use of PSA e.g. *Safety Class 2 systems shall be subjected to a failure mode and effects analysis, a common cause failure analysis, an operating experience analysis, and a quantitative reliability analysis. Safety Class 3 I&C systems shall be subjected to a failure mode and effects analysis, a common cause failure analysis and an operating experience analyses, and, depending on the safety significance, a quantitative reliability analysis. Plant specific PSA shall be updated to correspond to the modified system"*. The YVL 5.5 contains specific requirements in case of using programmable I&C systems.

5 CONCLUSION

The Finnish Regulatory Body STUK has demanding and detailed requirements on PSA and risk informed methods in the design, construction and operation of nuclear power plants. Besides the dedicated regulatory guide YVL 2.8, there are many requirements for risk informed applications in various regulatory guides. Successful fulfilment of the makes it important to begin the PSA programme very early in the design phase. STUK reviews the PSA and first applications in connection with the construction license. An Operating license requires a complete level 1 and level 2 PSA ready for living use. STUK has granted the construction license, and the complementation of the PSA for OL3 is ongoing.

TOPSAFE
Dubrovnik, Croatia, 30.09 - 3.10.2008

Safety Assurance and Goals of Generic NPP Designs

M. El-Shanawany, I. Kouzmina
International Atomic Energy Agency
Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria
M.El-Shanawany@iaea.org, I.Kouzmina@iaea.org

R. Pape
28 Gorse Way, Formby, Liverpool, L37 1PB, UK
dandjpape@talktalk.net

ABSTRACT

This paper outlines those key aspects of the processes of design and assessment of generic designs of Nuclear Power Plant (NPP), which aim to provide assurance of safety. Indications are given of the approach and criteria likely to be required for such process. It is emphasized that design aims for defence in depth, while assessment provides assurance that the defence in depth is adequate for the safety goals of the design. In practice design and assessment would overlap, with the findings of assessment being fed back into design re-iteration. Both deterministic and probabilistic approaches are necessary inputs into assessment. The paper notes the complementary aspects of deterministic and probabilistic assessment approaches. It outlines the key requirements for safe design, and the deterministic evaluation of a design. It then focuses on the requirements for probabilistic risk estimates and criteria. Recommendations are made for the approach to be adopted for generic designs, using deterministic and probabilistic criteria within some form of integrated risk-informed decision making process as aids to judgment.

1 INTRODUCTION

1.1. Background

The International Atomic Energy Agency (IAEA) has recognized a need to provide guidance for NPP vendors, operators and regulators on the information to be supplied for the evaluation of the safety of generic designs. The over-arching design safety goals are to protect people and the environment from the harmful effects of ionizing radiation. This can only be achieved through a systematic process of compliance with a number of fundamental safety principles. This process includes the deterministic safety design aspects and the system features (safety margin, defence in depth, redundancy, diversity, automation, etc.) which aim for safety by design, and the associated specified operational practices. It also includes the deterministic and probabilistic analyses to provide assurance that a high degree of safety will be achieved in practice.

The process of generic design and evaluation is different in context and detail from a specific installation proposal. For example, generic design would be based on an assumption of a ‘typical’ site, or a specification of site characteristics, and then it would need to be reviewed against the characteristics of a particular site. Considerable experience has been

accumulated in some Member States (MSs) where generic designs are certified (e.g. USA). However, much of this is with evolutionary designs of Light Water Reactors (LWRs) based on experience of earlier versions. Consideration is now needed of the possibility of new concepts, passive safety features and other technical developments, together with the developing emphasis on integrated Risk-Informed Decision Making (RIDM) and the use of Probabilistic Safety Assessment (PSA) to complement the deterministic approach.

In past generic design certifications in individual States, there had been considerable interaction between the vendors, operator organizations and the State's regulatory body in the evolution of particular approaches to design and its evaluation. Reference [1] notes that some MSs have detailed deterministic regulatory approaches; while others prefer goal-setting with flexibility on how to achieve the goals.

1.2. Structure of the Paper and IAEA's Safety Standards

This paper adopts a top-down structure, reflecting the IAEA Safety Standards (SSs), which begin with Safety Fundamentals (SFs) [2] providing basic concepts and principles of nuclear and radiation safety. These are supported by a number of Safety Requirements (SRs) publications providing high-level requirements addressing different aspects of safety, e.g. nuclear power plant safety. These in turn are supported by more detailed guidance in the category of Safety Guides (SGs) providing recommendations on the actions needed to comply with SRs.[1] The paper also follows the assurance process presented in SRs for Safety Assessment [3], which begins with the setting of safety and other design objectives. Design proceeds according to good engineering standards and practice, with emphasis on defence in depth. The design is evaluated by deterministic analysis and further reviewed by probabilistic analysis. The results of analyses and comparisons with objectives may lead to re-iteration of aspects of the design; and analyses may be carried out in parallel with the detailed design development.

In this paper, the term 'safety assurance' is used to cover the information required to underpin the safety-related aspects of design plus the safety assessment process. 'Safety analysis' covers the deterministic and probabilistic analyses of a design to indicate the degree to which safety objectives have been achieved. Safety analysis is a major input to 'safety assessment.'[2]

2 SAFETY OBJECTIVES

In 2006, the IAEA published its revised Safety Fundamentals, SF-1 [2]. This states that: "The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation". This is to be achieved by adherence to ten fundamental principles, of which numbers 5, 6 and 8 pay particular attention to safety assessment.

---

[1] The IAEA's Safety Standards are not legally binding on Member States, but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The IAEA's Safety Standards are binding on the IAEA for application in relation to its own operations and on States in relation to operations assisted by the IAEA.

[2] "Safety assessment involves the systematic analysis of normal operation and its effects, of the ways in which failure might occur and of the consequences of those failures. Safety assessments cover the safety measures necessary to control the hazard, and the design and engineered safety features are assessed to demonstrate that they fulfil the safety functions required of them…" [2].

Principle 5 of SF-1 states that “Protection must be optimized to provide the highest level of safety that can reasonably be achieved”. To show adherence to this principle, risks must be assessed. A graded approach to assessment should be used, with the effort put into such assessment being commensurate with the scale of the hazard. For NPP, with the main hazards being the very large radioactive isotope inventory of the core and the spent fuel in store, a very high effort on assessment is expected.

Principle 6 of SF-1 [2] states that “Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm”. Thus “…doses and radiation risks must be controlled within specified limits…” [2]. Quantitative limits for doses are indicated in the Basic Safety Standards [4]. Criteria for risks used in different States are discussed in Ref. [5]. Often, Member State regulations and/or guidance would specify the national implementation of IAEA standards for dose and risk limits. An NPP operator (licensee), or the vendor of a generic NPP design, would be expected to demonstrate that an installation would give doses and risk below such ‘specified limits’.

SF-1 also states that the specified limits “…represent a legal upper bound of acceptability….they therefore have to be supplemented by the optimization of protection…” [2]. This is in line with a trend towards a three-zone approach for risk consideration, with criteria defining the boundaries between zones (for details see INSAG-6 [6]). The following is the framework suggested in INSAG-6:

“… decisions concerning the tolerability of risk should be based on three principles:

- There exist levels of risk from technology to individuals or society that should not be tolerated irrespective of the technology's benefits. Such levels are often referred to as tolerability limits.
- At risks lower than that level, safety cannot be absolute, and the knowledge of how to improve it is never complete. Responsible action includes continued striving for risk reduction, provided that the effort to achieve these improvements is not unreasonably high.
- Well below the tolerability limit, risks are so low that they should be regarded as negligible in order to avoid unnecessary deployment of resources which diverts attention from substantial safety issues which could lead to larger risks of other types. That corresponding low level is sometimes called a ‘de minimis’ limit.”

The three-zone approach is illustrated in Fig. 1. The boundary between the upper zone and middle zone corresponds to a reference level for action (called ‘tolerability limit’ by INSAG-6). If a risk metric lies above this level, every effort must be made to improve safety. Some MSs indicate criteria for this level. In contrast to dose limits, the reference level for action for risk based on PSA results is not usually applied by MSs as a formal legal limit.

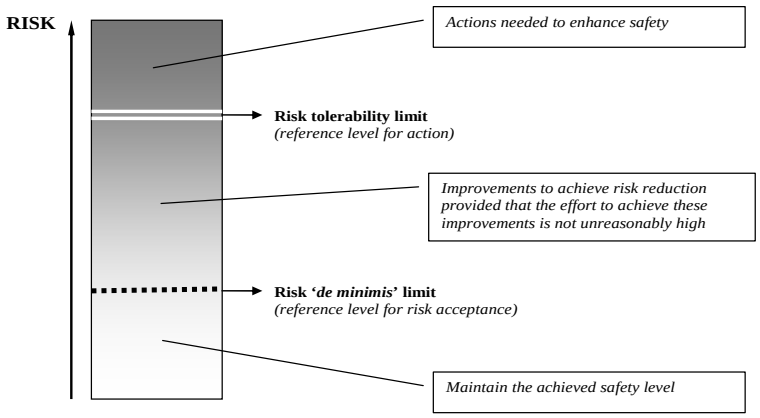


Figure 1: Three-Zone Approach to Safety Consideration

In the lowest zone the risk is broadly acceptable and the emphasis is on ensuring that the risk has been properly assessed and on maintaining the safety situation. In the middle zone the risk should be optimized (i.e. correlate with SF-1 [2] Principle 5) i.e. as low as reasonably achievable (ALARA). There may also be criteria for the boundary between the lowest zone and the middle zone; such lower criteria may be called 'objectives'.

SF-1 Principle 8 [2], dealing specifically with accident risks, states that "All practical efforts must be made to prevent and mitigate nuclear or radiation accidents". The text indicates the basic means to achieve this objective, with particular emphasis on defence in depth, fitness for purpose, and the general principles of good engineering design. It is also usually expected that a designer will begin by attempting to eliminate or minimize risks by using non-hazardous materials and conditions wherever possible. Safety assessment would use deterministic and probabilistic analyses to demonstrate compliance with this Principle. The general interconnection between Deterministic Safety Assessment (DSA), PSA, and Safety Objectives is illustrated in Fig. 2.

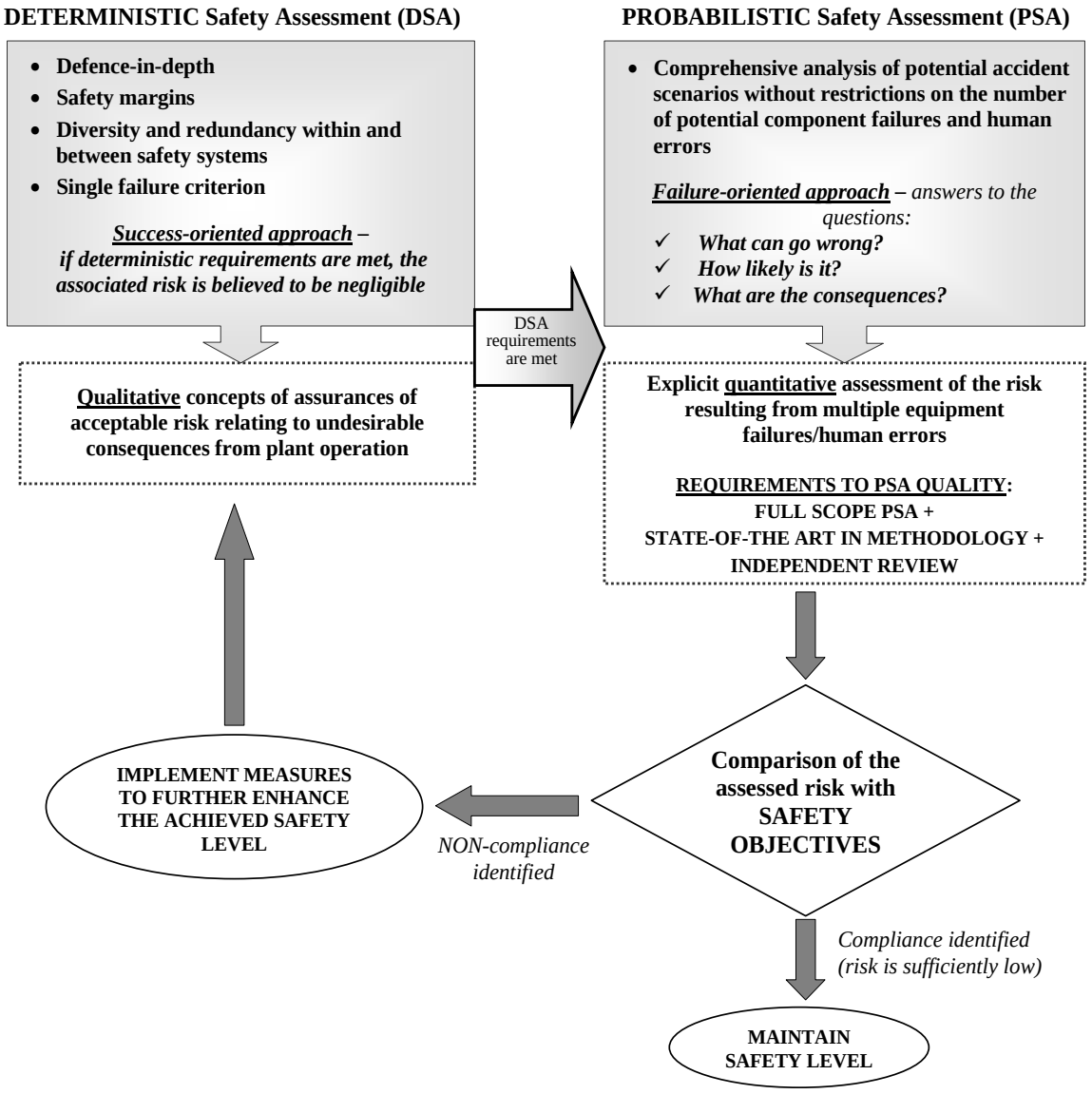


Figure 2: Interconnection between DSA, PSA and Safety Objectives

It is noted in Figure 2 above that DSA is ‘success-oriented’ while PSA is ‘failure-oriented’. The use of both approaches therefore provides a diversity of perspective within the assessment, and enriches the inputs into decisions on the adequacy of safety. This is recognized in the development of integrated risk-informed decision-making that is discussed further.

3 DESIGN AND DETERMINISTIC ASSESSMENT

The basic safety aims of the design and construction are: to limit routine exposures and releases, to prevent accidents, and to limit and mitigate accident consequences. The key aspects to achieve these aims are:

- prevent failures or abnormal conditions (including breaches of security) that could lead to loss of control;
- the primary means to do these is Defence in Depth (D.i.D.), i.e. “the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused…” [2];
- D.i.D. should ensure that no single failure (technical, human or organisational) could lead to harmful effects; and combinations of failures that could do so are very low probability;
- independent effectiveness of D.i.D. levels is necessary;
- D.i.D. combines: management of safety, site selection, design and engineering features providing safety margins, diversity and redundancy of safety systems;
- design and engineering should feature: high quality and reliability (of design, technology and materials); passive and active control, limiting and protection systems, and surveillance; inherent and engineered safety features; operational and accident management;
- structures, systems and components (SSCs), as well as human operators, should have adequate reliability. This is achieved by classifying SSCs according to their safety significance, and implementing them with commensurate quality;
- technology should be already proven in operation or qualified for the proposed application, applying conservative acceptance criteria with margins of safety;
- design should be adequate to withstand initiating events with widespread effects on multiple components.

The proposed IAEA Draft Requirements for the Safety Assessment of Nuclear Facilities and Activities [3] includes the following points which are particularly relevant for generic design evaluation:

- use of proven SSCs where practicable, plus research and development (R&D) to show adequacy of any novel aspects, and equipment qualification;
- clear identification of design principles (as stated above);
- show relevance of international codes and standards, taking account of SSC safety classification;
- cover all relevant internal and external hazards;
- indication of design to take account of the eventual need for safe decommissioning.

General principles of good design should be applied, including:

- elimination or reduction of hazard where possible by choosing inherently safe materials and conditions;
- preference for passive over active systems or their effective combination;
- diversity and redundancy within and between safety systems;

- no single component failure can disable a safety function;
- systems which are fail-safe and whose deterioration is visible;
- explicit consideration of human factors, with automation where beneficial, good ergonomics, and robust procedures.

An NPP design would need to make transparent the design philosophy and its detailed application, to ensure that regulatory bodies and operating organizations understand the reasons for design decisions. This aids the evaluation of the design, and it also reduces the risk of inappropriate later modifications which inadvertently weaken a system. The design would also need to specify various aspects to be addressed in the deterministic and probabilistic assessments such as the schedules, site layout, reliability of off-site services, plant condition monitoring, operator staffing levels and competences, etc.

Starting with an initial design concept and performance (including safety) goals, design proceeds from the definition of the design bases for SSCs, derived by consideration of the possible initiating events which might place demands on them. In principle this requires the analysis of all routine and potential abnormal states or events affecting the plant. Usually some selectivity is applied to exclude plant states or events which are highly improbable, and the remainders are grouped within bounding envelopes to facilitate conservative analysis while not requiring excessive detail. The rationale of selectivity and grouping is an important part of a safety case. Assessment continues with engineering analysis of the SSCs subject to the design basis parameters to demonstrate withstand capability with safety margins as required by appropriate standards.

The deterministic design analysis and assessment aspects form the larger part of a safety case, and there is much detailed guidance in IAEA and international technical standards, and MS' own regulatory standards. Very clear documentation of the standards basis would be required in a vendor's safety case, to provide a route-map for reviewers from different backgrounds. A vendor would itself need to arrange an independent review of the design and the safety case, and to provide evidence of this. In due course, the vendor would also need to ensure that any operating organization has clear information and understanding of the required Technical Specifications, Operating Limits and Conditions, staffing levels and competences, and component specifications as assumed in the generic safety case.

4 PROBABILISTIC SAFETY ASSESSMENT

Historically, the design and operation of NPPs were based on deterministic concepts. The main elements were defence-in-depth provisions, safety margins, diversity and redundancy, and single failure criterion. The implications were that if deterministic criteria are met, the plant would be safe enough, and the risk of unacceptable radiological releases would be sufficiently low. However, the major accidents at NPPs showed that this was not always the case. The PSA technology that started in 1975 with the famous study, WASH-1400 [7], provided the possibility to get additional and new safety-related insights and to unambiguously assess the risk dealing with a particular NPP. To complement the deterministic approach, PSA presented a failure-oriented approach that was aimed at finding answers to the questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

As with deterministic assessment, there is a large body of standards and guidance on the appropriate technical features of PSA. IAEA has recently completed the final draft Safety

Guides on Level 1 and Level 2 PSA (see Refs [8] and [9]). Details of the contents of the safety guides are discussed in Ref. [10]. In addition, TECDOC-1511 [11] details the attributes required in PSAs for particular applications. TECDOC-1511 focuses on Level 1 PSA for NPP at power and internal initiating events only; some MSs would expect more comprehensive coverage. TECDOC-1436 [1] notes that the emerging standard is for at least Level 2 PSA for new NPP. It is not proposed to discuss here how PSA should be done, but rather 'what should be done' at an elevated level of detail.

While PSA is valuable to provide a quantitative indication of risk for overall safety evaluation, it has other uses as well. Such uses derive from the holistic nature of PSA, including the assessment of risk from events beyond the design basis, and the understanding of the interactions within complex systems. For example, PSA may be used to inform accident management planning. PSA is also a valuable tool for assessing the effects of options and the sensitivity of the risk to assumptions on SSC performance. For overall risk assessments using PSA, it is necessary to ensure that all potential initiating events and fault sequences are covered.

It is generally accepted that PSA should be best-estimate, rather than the conservative approach often applied in deterministic assessment. This should be borne in mind when developing or using criteria. Some regulators expect an indication of uncertainties, as well as basing judgements on the 50% confidence results. Others may indicate criteria based on a higher confidence level, such as 95%. INSAG-6 [6] recommended the use of 95 percentiles when testing compliance with broad technical safety objectives such as Level 1 PSA Core Damage Frequency (CDF).

An important need with PSA, as with DSA, is to ensure full and transparent recording of the assumptions and judgments. These would be particularly necessary where a generic NPP design is to be sold to several different operating organizations regulated by different MS licensing bodies that might have different safety objectives stated in their regulations. It would also be necessary to ensure that the regulatory body and operating organization have access to the PSA code and model or arrangements to use them, for reviewing the PSA, for the assessment of modifications during operation, and for periodic safety reviews. It is very important that the PSA used in the licensing process should necessarily undergo a thorough independent review to assure its compliance with the state-of-the-art in methodology and the absence of inadvertent mistakes, omissions, and inconsistencies.

There is international consensus that PSA can provide an in-depth understanding of the level of safety achieved in design, and it should be used as a complement to deterministic safety assessment and as a tool for analysis of compliance with safety objectives. The general iterative process of assurance of the compliance with safety objectives outlined in Fig. 2 could be applicable in the licensing process. It is now recommended that a full-scope Level 1 and Level 2 PSA should be performed. Level-3 PSA is also desirable. Provisions for a 'Living PSA' are desirable as well.

5 RISK INFORMED DECISION MAKING

5.1. RIDM Considerations in IAEA Publications

TECDOC-1436 [1] discusses the achievements in RIDM and risk informed regulation (RIR), mostly in relation to licensing decisions by a regulatory body. RIDM could also be used by a licensee in making a safety case, or an NPP vendor in assessing a proposed design.

The basic aim of RIDM is a 'balanced' decision. This is a decision which takes into account all the available information to an appropriate extent. RIDM combines in a formal process the results from deterministic and probabilistic analyses and other assessment

requirements, plus legal, regulatory, cost-benefit, and any other requirements. The degree to which a requirement is met may be combined with a weighting for that requirement, to give an overall evaluation.

In RIDM, explicit consideration is given to the likelihoods and consequences of events, as well as good engineering practice, deterministic safety margins, and the arrangements for the management of safety. It is recognized that the maturity of PSA allows the explicit use of quantitative risk information, but quantitative PSA results compared with risk criteria are not the sole determinants of design adequacy. For example, PSA alone should not be used to justify a new design which apparently reduces the safety protection compared to generally-accepted deterministic good practice.

RIDM recognizes the strengths of deterministic assessment, for example that it is tried and tested, and very well-developed. However, deterministic analysis alone may have weaknesses, such as focusing on issues which are not the major or only contributors to risk, and being unable to prioritize potential improvements in terms of risk reduction. It may also be difficult to demonstrate deterministic safety margins with a high degree of confidence for radically new designs. Deterministic consideration of possible 'reasonably achievable' safety improvements can only be done qualitatively.

The inclusion of PSA in RIDM recognizes the benefits which PSA should provide in addition to quantitative risk information, such as: comprehensive coverage of initiating events; insights into the importance of events and safety measures; explicit indication of uncertainties and sensitivity analyses of options; degree to which defence in depth, single-failure criterion etc. are met; prioritization of improvements; insights into the safety aspects of novel designs. There are potential difficulties in PSA performance and use, such as: completeness of identification of initiating events; large uncertainties of numerical risk results; data relevance; modelling issues (for example, human errors of commission); limitations (for example, PSA of a restricted scope, e.g. Level 1 PSA, does not address severe accident analysis). It may also be difficult to cross-compare the results of PSAs done with different codes; but the use of the same PSA code to compare options is much less problematic.

TECDOC-1436 [1] states or implies several points about RIDM, for example:

- Avoid compensating for a weakness in one aspect by claiming a strength in another; the aim is to consider all aspects separately and strengthen them as far as reasonably achievable, and then make a balanced judgement about adequacy overall.
- Process requires staff resources with the expertise for the various components, plus the ability to take an overview. (It is recommended in the TECDOC that the final decision is taken by an expert interdisciplinary panel).
- RIDM aids transparency in the decision-making process; and it should aid the retention of corporate knowledge about the reasons for design features.
- Vendors of generic designs may find that the weighting of various aspects (such as deterministic, probabilistic), and key criteria, may differ between MS. Transparency in RIDM data and assumed weightings should facilitate the tailoring of safety cases to fit MS regulatory requirements.

Having recognized the growing incentive for RIDM, in 2007 the IAEA launched a project on developing a guidance document on RIDM [12]. It will provide principles and suggest approaches to integrate the results of deterministic and probabilistic safety analyses, as well as other important aspects to make sound, optimum, and safe decisions. The primary focus of the publication is to provide guidance to Member States on ***how*** to adequately and responsibly perform, document, and report the results of RIDM. An advanced draft document is currently available [12].

5.2. Discussion: Goals for PSA

The three-zone approach outlined above may be taken as a model. Where the PSA risk estimates at 50% confidence level are above a reference level for action, very high priority should be given to reducing the risk by physical and operational measures. Where the risk estimate is below this level, effort should still be made to reduce the risk to as low as reasonably achievable. Where risks are estimated to be below a 'de minimis limit' with a high degree of confidence (such as 95%), the emphasis should be on maintaining that situation. In all cases, there should continue to be periodic and interim reviews to seek reasonably achievable improvements, taking account of operating experience and new knowledge.

With Level 1 PSA, a reference level for action for CDF of 1E-5/ry may be used for new NPP designs, with a lower risk to be aimed for where reasonably achievable (for existing NPPs, the tolerability level of 1E-4/ry recommended in INSAG-12 [13] may be used). If it is desired to have a 'de minimis level', fractions (for instance, 10% or 1%) of the limit figures could be used. Care is needed when defining 'core damage' for designs other than LWR. This would be for MSs, licensees and vendors to propose, by analogy with the significance of a level of core damage in LWRs.

For Level 2 PSA, for Large Early Release Frequency (LERF), a reference level for action set at a factor of 10 lower than the CDF figure is often used, giving 1E-6/ry for new NPP designs. A lower risk should be aimed for where reasonably achievable. If it is desired to have 'de minimis limts', fractions (for instance, 10% or 1%) of the reference level for action figure could be used. For new designs, INSAG-12 [13] now expects the "practical elimination" of accident sequences which could lead to large early release. However, Level 2 PSA would still seem to be necessary, to show completeness in the defences and to show that the overall risk is acceptably low.

A definition is needed for 'Large Early Release'. INSAG-12 [13] says "large off-site releases requiring short-term off-site response". Some MSs use a definition in terms of quantity of a dominant isotope (e.g. Cs 137); others use a fraction of core inventory; others may use a criterion based on breach of containment. It is suggested that further consideration be given to this issue.

Care is needed when comparing PSA information with quantitative criteria. The following points summarise some aspects of this. (These points are derived from a recent IAEA Questionnaire on the use of PSA criteria, see Ref. [5]).

(a) Words used for criteria include 'goals', 'objectives', 'targets', 'limits', 'acceptable', 'standards', etc. It may be unclear whether these terms mean: 'a level of risk which should not be exceeded' (i.e risk tolerability limit discussed above); or 'a level below which the risk is broadly acceptable' (i.e. 'de minimis limit' discussed above); or some other definition. In line with the IAEA Glossary, the words 'reference level for action' should be used for the first meaning, and 'risk objective' for the second, following the principles provided above. This acknowledges that the criteria may not be intended to be used as stand-alone formal or legal criteria, and so should not be called 'limits'.

(b) It should be clear whether an explicit assessment of options to test for reasonably achievable improvements is required where the risk falls between a 'reference level for action' and a 'risk objective'. For new generic designs, it is suggested that such an assessment should be presented as part of a safety case package.

(c) The PSA, and the criteria, should cover all plant states during the operational lifetime. It is suggested that the main metric (CDF or LERF, units ry-1) should be the integral over time of the overall risk from all plant states, assuming the intended operating cycles. PSA should include all initiating events and hazards. The number of units on

the site could be taken into account while defining the 'risk objective' and 'reference level for action'; this issue may become important when several units are to be located at the same site. Subsidiary metrics may be proposed for commissioning and for particular plant states, including the derivation of Technical Specifications. Where PSA is used as an aid to operational decision-making (for example a Risk Monitor), subsidiary criteria may be needed for the action to be taken if the point-in-time risk level rises.

(d) PSA involves many assumptions or specifications relating to the Technical Specifications, quality of construction, operation, maintenance, inspection, testing etc. A generic design would need to make these assumptions explicit so that operating organisations and regulatory bodies can ensure adherence to them. A comprehensive independent peer and/or regulatory review is a standard practice that should be followed. The technical quality of PSA should be in accordance with the state-of-the-art that is reflected in safety standards developed by IAEA and other standards internationally, e.g. ASME PRA Standard [14].

(e) Arrangements are needed for the operating organisation to use, or contract for the use, of the PSA for the assessment of modifications and periodic reviews throughout the NPP lifetime. Also, a 'Living PSA' programme is encouraged.

(f) There may be a requirement for Level 3 PSA in a particular MS; arrangements would then be needed to associate Level 1 and 2 PSA with a Level 3 PSA that is site-specific.

6 CONCLUSIONS

The main design safety goals are to protect people and the environment from the harmful effects of ionizing radiation. A systematic iterative process of compliance with a number of fundamental safety principles at the design stage based on deterministic analysis and complemented by PSA (as outlined in Fig. 2) is likely to result in a design that meets the type of numerical criteria suggested above. Such criteria should not be used as stand-alone decision determinants. They should be used within some form of integrated risk-informed decision making process, as aids to judgment. The PSA used in decision making should be of appropriate technical quality. The new IAEA safety guides on PSA [8, 9] and document on RIDM [12] are specifically designed to provide advanced guidance in these matters.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, "Risk Informed Regulation of Nuclear Facilities: Overview of the Current Status", IAEA-TECDOC-1436, IAEA, Vienna, 2005.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, "Fundamental Safety Principles", Safety Fundamentals No. SF-1, IAEA, Vienna, 2006.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, "Safety Assessment for Facilities and Activities" Safety Requirements (DS 348 Draft), IAEA, Vienna, 2007.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, "International Basic Safety Standards for Protection Against Ionising radiation and for the Safety of Radioactive Sources", Safety Series N 115, IAEA, Vienna, 1996.

[5] Pape R., El-Shanawany M., Kouzmina I., “Safety Assurance and Goals of Generic NPP Designs”, paper presented at INSAG meeting, NSNI/SAS/2007/7, Safety Assessment Section, Division of Nuclear Installations Safety, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, November 2007.

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, “Probabilistic Safety Assessment INSAG-6”, Section 5.3, 75-INSAG-6, IAEA, Vienna, 1992.

[7] Rasmussen, Norman et al., “The Reactor Safety Study”, WASH-1400, Washington DC: U.S. NRC, 1975.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Draft Safety Guide, "Development and Application of Level 1 PSA for Nuclear Reactors”, DS394, IAEA, Vienna, 2008.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Draft Safety Guide, “Development and Application of Level 2 PSA for Nuclear Power Plants”, DS393, IAEA, Vienna, 2008.

[10] Kouzmina I., Yllera J., Reinhard M., “The New IAEA Safety Standards on Probabilistic Safety Assessment and Risk-Informed Decision Making,” Proceedings of the Topical Meeting on Advanced Safety Assessment Methods for Nuclear Reactors, held 30 October – 2 November 2007, Deajon, Korea, 2007.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, “Determining the Quality of Probabilistic Safety Assessments (PSA) for Applications in Nuclear Power Plants”, IAEA-TECDOC-1511, IAEA, Vienna, 2006.

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Draft, “Risk Informed Decision Making,” DS365, IAEA, Vienna, 2008.

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, “Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Revision 1”, INSAG-12, IAEA, Vienna, 1999.

[14] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, ASME, New York, 2002.

European Nuclear Society

Rue Belliard 65
1040 Brussels
Belgium
Telephone +32 2 505 30 54
Fax + 32 2 502 39 02

topsafe2008@euronuclear.org

www.euronuclear.org