Support to the Nuclear Safety Regulator of Brazil (CNEN) through an INSC Project.

N.S.Lapa CNEN, L.C.M.Pereira CNEN, A.A.Madeira CNEN, O.J.M.Wellele CNEN, G.Sabundjian CNEN, S.M.Lee**, I.Aro STUK, T. Steinrötter GRS***, J. G. Varela TECNATOM*
J. Valkonen VTT, E. Piljugin GRS, E. Furieri CNEN, J. Rodríguez GRS

* CNEN National Nuclear Energy Comission, Severiano Street 90, Botafogo, Rio de Janeiro, Brazil
** São Paulo University, IPEN, CEN, Av Prof Lienu Prestes, 2242 Butantã, University City, São Paulo
*** GRS, Schwertnergasse 1, 50667 Cologne, Germany
**** TECHNATOM, Av. de los Montes de Oca, 1, 28703 San Sebastián de los Reyes, Madrid, Spanien
***** VTT, P.O. Box 1000, FI-02044 VTT, Finland

Abstract:

The paper introduces the European Union funded cooperation between the Brazilian nuclear regulatory body (CNEN) and a consortium of several European organizations. The still ongoing cooperation started in 2011 and has provided CNEN with insights and complementary information for licensing and regulatory activities on different reactor nuclear safety issues. The support is described by examples relating to the Severe Accident Management Program (SAMP) of the Angra 2 nuclear power plant NPP and the safety of digital instrumentation and control systems (DI&C) of Angra 3. The goal of the support regarding the SAMP is the review of the SAMP - under the licensing process by CNEN – with the focus on the new procedures and equipment implemented after the Fukushima accident. In parallel, a MELCOR simulation model of Angra 2 has been developed to perform independent calculations in order to support the assessment of the safety analysis presented in the Angra 2 Severe Accident Management Guides (SAMG). The support regarding DI&C is focused on regulatory issues concerning the review and assessment of digital instrumentation and control systems (DI&C) of the Angra 3 NPP under the licensing process by CNEN – providing CNEN with insights and complementary information on licensing experiences of new reactors with a DI&C architecture and technology similar to that of the Angra 3 NPP.

1 INTRODUCTION

Since May 2011, RISKAUDIT has been providing support to CNEN through two EU financed projects in the framework of the EU Instrument for Nuclear Safety Cooperation (INSC). The projects are dedicated to the enhancement and strengthening of the nuclear safety regulatory framework in Brazil in compliance with international criteria and practices.

CNEN has a wide range of competencies, among which are, most importantly, regulatory and licensing activities. The regulatory staff of about 120 professionals covers complex issues at Angra 1 (back-fitting measures related to ageing management and lifetime extension), Angra 2 (periodic safety reviews, power up-rate, probabilistic safety analysis), Angra 3 (construction licensing and commissioning preparedness) and with the Brazilian multipurpose reactor (licensing process).

The first project reinforced CNEN's expertise in regulatory and licensing activities in the areas of severe accident management, emergency preparedness and response, evaluation

of operational experience, digital control and instrumentation systems and safety of new fuels. Against this background, the second Brazilian project constitutes a follow-up support for this reinforcement of expertise in regulatory and licensing activities. The support comprises complementary work on areas which have already started and extends it to new areas, such as probabilistic safety analysis, deterministic analysis of loss-of-coolant accidents and ageing management.

Another important goal of CNEN is to improve its human resources focused on satisfying Brazilian regulatory and licensing requirements. This is consistent with CNEN's commitment to continue cooperation with the EU and their dedication to the two projects. RISKAUDIT's engagement in Brazil has also been recognised as a model project under the INSC projects.

The following describes the support on the examples relating to the Severe Accident Management Program (SAMP) of the Angra 2 NPP and to the safety of digital instrumentation and control systems (DI&C) of Angra 3 NPP.

2 ASSESSMENT OF SEVERE ACCIDENT MANAGEMENT PROGRAM AND AN INDEPENDENT SEVERE ACCIDENT ANALYSIS APPLYING THE INTEGRAL CODE MELCOR FOR ANGRA 2 NPP

Angra 1, 2 and 3 NPPs are located at the Central Nuclear Almirante Álvaro Alberto (CNAAA) site on the Itaorna Beach in Angra dos Reis, 150 km from Rio de Janeiro, Brazil. The location of the nuclear units is close to the main electrical power consumers (São Paulo, Rio de Janeiro and Minas Gerais States) promoting the network stability for the huge national grid.

Figure 1 NPP site, Angra 1 and 2 in operation, Angra 3 buildings erection, Dec-2016

Angra 1 is a two loops PWR Westinghouse design having a gross output of 610 MWe and it was connected to the power grid in 1985.

Angra 2 is a four loops Siemens KWU design with a gross output of 1300 MWe and it was connected to the grid in 2000. The construction of Angra 3, having similar design as Angra 2, started in 1984, but construction was stopped for a long time. Work was started again in 2007 with the conventional buildings and safety evaluations of PSAR in 2008. The Construction License was issued in 2010. In 2015, Angra 3 construction was interrupted again due to severe economic crisis and investigation on bribery and corruption. The plant is now estimated to be connected to the grid by 2024 if the construction resumes under full conditions in 2019.

The Brazilian National Nuclear Energy Commission (Comissão Nacional de Energia Nuclear – CNEN) is responsible for the regulation of nuclear safety and the promotion, orientation and coordination of nuclear research and technological development. After the March 2011 Fukushima nuclear accident, CNEN required the development and implementation of a Severe Accident Management Program (SAMP) for CNAAA – Almirante Álvaro Alberto Nuclear Centre, unit 2 (Angra 2) following guide IAEA SRS 32 [1]. The Eletronuclear (ETN) is a government entity responsible for nuclear power plants operation. To meet this requirement, the ETN prepared the Action Plan 2PA-001.2011 [2].

One of the actions defined in the Action Plan was a targeted safety reassessment of operating nuclear facilities at NPP sites, the so called stress tests. In the framework of the stress tests, the following aspects were analysed in detail:

- Extreme external natural hazards (earthquakes, flooding, external fires, tornadoes, extremely high and low temperatures, extreme precipitations, strong winds, combinations of events);
- Loss of electrical power and/or loss of ultimate heat sink;
- Severe accident management.

The Action Plan complies with the Official Letter No. 012/12-CGRC/CNEN, dated January 30, 2012, which established the evaluation of the performance of Nuclear Power Plants in accordance with the specification "Resistance Assessment of Nuclear Power Plants in Member Countries of the Ibero-American Forum of Regulatory, Radiological and Nuclear Organizations" (FORO), published in September 2011 [3].

According to the specifications of FORO itself, the evaluation takes as reference the technical configuration of the Angra 2 plant on July 30, 2011.

The Action Plan comprises three evaluation areas resulting 30 studies and 28 projects and is reviewed at intervals of no more than six months for the necessary adjustments, considering:

- the development of the initiatives and their results;
- follow-up on international initiatives, including recommendations from international organizations working on the same issues;
- the requirements of the CNEN.

The development of this Action Plan, among the activities to be developed, in line with CNEN requirements, established the elaboration and implementation of a SAMP for Angra 2. A technical cooperation project was established with the European Union, through the Instrument for Nuclear Safety Cooperation (INSC), in order to favor this SAMP assessment process.

Despite CNEN interaction with international organization, the technical support by organizations with recognized experience is important for the suitable SAMP assessment.

The objectives of the INSC Programme imply sustainable transfer of knowledge and capability to the Beneficiary and End User. The Task 5 of the Project INSC BR3.01/12 [4] aims at a supporting of CNEN in the assessment SAMP for Angra 2, including the capacity of CNEN to review an existing and to develop an own MELCOR nodalisation for the Angra 2 NPP.

The requirements are associated with the Stress Test results and were defined after the Fukushima severe accident:

a) Prepared Action Plan 2PA-001.2011, which follows an approach similar to the one adopted for the German NPPs of the Angra 2 similar design:

  - Development of Severe Acident Management Guidelines – SAMG based on the German concept;
  - SAMG incorporates additional equipment, dedicated for control and mitigation of Severe Accidents;
  - Incorporation at a later time of findings from ETN Fukushima Response Plan [2].

b) Planned and installed Plant modifications associated with the Angra 2 SAMP:

- Complementing pressurizer valve station to allow Bleed and Feed (B&F) through the Relief and Safety valves;
- Passive autocatalytic recombiners (PAR);
- Filtered Containment Venting;
- Containment Sampling System for Severe Accident conditions;
- Additional mobile equipment: Small Emergency Diesel Generators, Diesel driven pumps (Fukushima response Plan-Angra 2 Stress Test [6]).

Activities performed in the scope of the SAMP assessment development within the project INSC BR3.01/12

The overall objective of the INSC project is the enhancement and strengthening of a nuclear safety regulatory regime in Brazil (CNEN) in compliance with internationally used criteria and practices.

The objective of the Task 5 is the strengthening of CNEN Severe Accident Management (SAM) capabilities to perform the safety evaluation of Angra 2 SAMP, and to strengthen CNEN capacity in the application of the integral code MELCOR for the subsequent target to perform independent severe accident analyses. This main objective can be split in the follow items:

a) Support in the assessment on prioritized parts (i.e. Individual Plant Examination) of the SAMP submittals, including the link with the Emergency Operation Procedures (EOPs) for Angra 2;

b) Assist CNEN on the development of the Angra 2 simulation model using MELCOR severe accident code;

c) Support CNEN with the development of the following two reports:

- Regulatory evaluation report of Angra 2 Severe Accident Management Program;
- Technical report on the MELCOR simulation model used for the implementation and independent analysis in order to assess the severe accident analysis of Angra 2 performed and submitted by the utility.

Methodology

The European consultants provide guidance to CNEN regarding selected issues based on the state-of-the-art safety requirements for the assessment process for Angra 2 SAMP, according to international practices existent on STUK, GRS and TECNATOM, the European member organizations of the INSC project, expertises.

The know-how of the member organizations is being transferred through programmed workshops where an exchange of information and documentation between the participants occurs, assuring the improvement of CNEN knowledge in the frame of its licensing needs.

The results obtained during the course of the project were documented in reports issued during the three workshops held [7, 8 and 9].

Preliminary results

Hereafter, the preliminary results concerning both the SAMP review and MELCOR results are briefly presented.

The European counterparts presented the practices observed in their respective countries and associated standards and guides concerning SAMP. The main recommendations of the experts concerning SAMP review are presented below.

SAMG

The SAMG of Angra 2 is based on the German concept. It incorporates additional equipment, dedicated for control/mitigation of severe accidents, like PARs, filtered containment venting, containment sampling system etc. Some of these equipments are not yet installed.

The European counterparts concluded that since SAMG actions require system operations, control room operators need SAM procedure(s) to perform the pre-identified immediate actions. They need to know about the containment state, like its integrity and atmosphere conditions, e. g. like containment pressure overpressure protection actions. Measures to assure containment integrity, to perform core cooling and to initiate residual heat removal systems need control room operator actions. More detailed information about these recommendations can be found in [7].

Complementing pressurizer valve station to allow Primary Bleed and Feed (B&F) through Relief and Safety valves

The European experts reviewed the ETN documentation regarding the improvement of primary bleed and feed. They concluded that it covers the objectives to analytically predict the resulting accident sequence and to estimate time periods for accident application of primary side bleed and feed for the AS scenario total loss of heat sink. Experts made some comments and suggestions that should be considered in detailed planning, as documented in [8].

Passive autocatalytic recombiners (PAR)

The European experts also reviewed the ETN documentation regarding the implementation of passive autocatalytic recombiners. PAR phenomena have been tested widely in France and Germany, including international organizations, and results show confidence in the functioning of ETN equipment in various conditions in a reliable manner. Experts made some comments and suggestions that should be considered in detailed planning, as also detailed in [8].

Filtered Containment Venting

This system has not yet been installed in Angra 2. However, according to the experts, the associated ETN preliminary proposal looks suitable for the plant. See [8] for more details.

A project regarding the re-assessment of a filtered venting system of a German PWR reference plant, which has been finished recently at GRS, was presented. The project activities were explained and the main findings regarding the design and operation of the system were discussed.

Containment Sampling System for Severe Accident conditions

This system has not yet been installed in Angra 2 and, till the development of this article, ETN is still selecting a product supplier.

MELCOR results

Significant contribution to core damage states or release categories of PSA Level 2 for Angra 2, among the most probable, are Station Blackout (SBO) and SB LOCA (20 cm^2). Thus, the Task 5 group decided to analyze these two events for the assessment of EOPs and SAMG measures. Some significant results of the simulation of these events are presented below.

It is important to emphasize that some other complementary simulations are still being carried out, according to the European experts' recommendations, as can be seen in [9].

SBO

The following assumptions were defined to simulate SBO, considering that no Reactor Coolant System despressurization was available:

a) Loss of all AC power;
b) All accumulators available;
c) No PBF available;
d) SBF available.

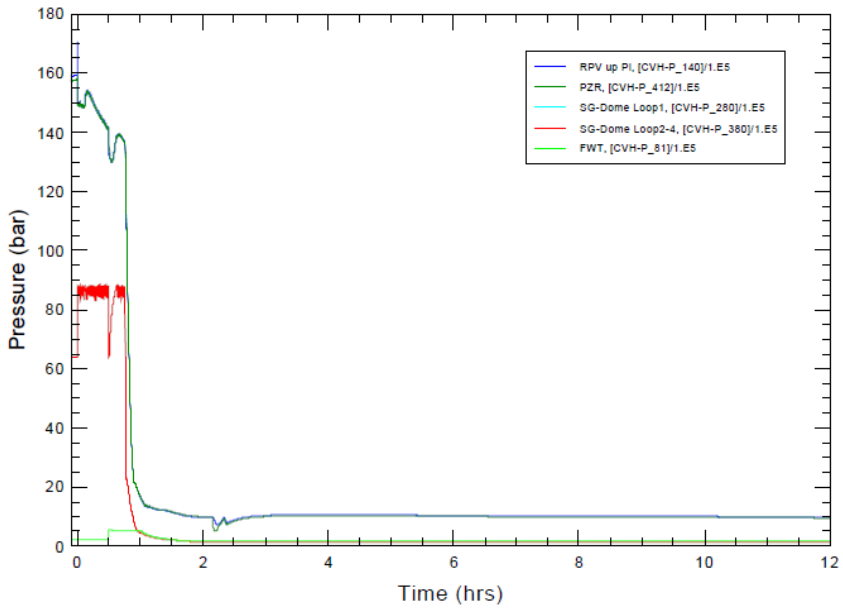

Figure 2 Pressure in RPV, PZR, SG and FW Tank

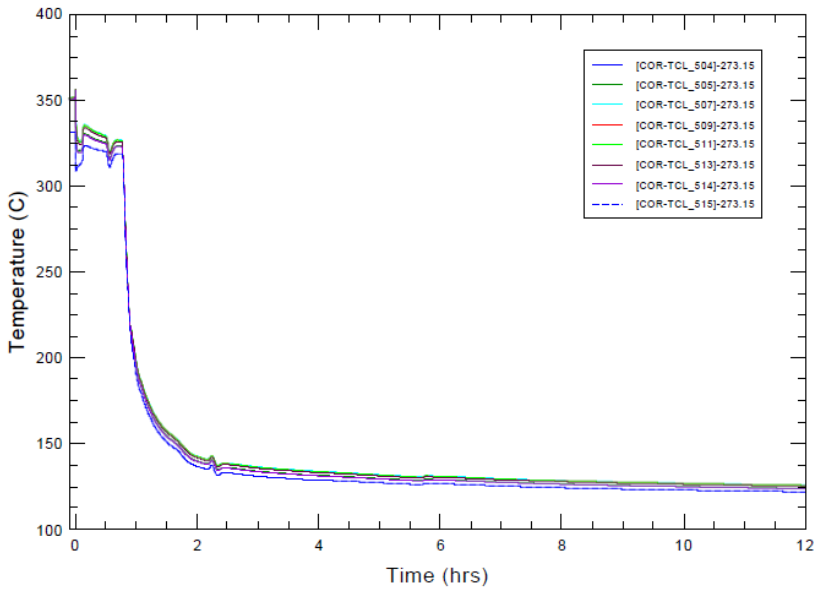

Figure 3 Cladding temperature for outermost ring

Under the BDBA assumption, during secondary side bleed and feed, water injection into the steam generator (SG) can be achieved at the Angra 2 plant by using two different methods [5]. Passive injection from Feedwater Tank Inventory, show in Figures 4 and 5, and from fire fighting pool water inventory, as can see in Figure 6.

The SG feed can be maintained using the fire fighting pool water inventory for more then 50 h (for the residual heat removal and removal of plant stored heat) when it empties, as can see in Figure 5.

Up to a main steam pressure of approximately 7 bar in the steam generator, a sufficient feed rate can be maintained solely because of the elevation head between the fire water pool and the SGs, see Figure 5. At higher main steam pressures a mobile pump is required.

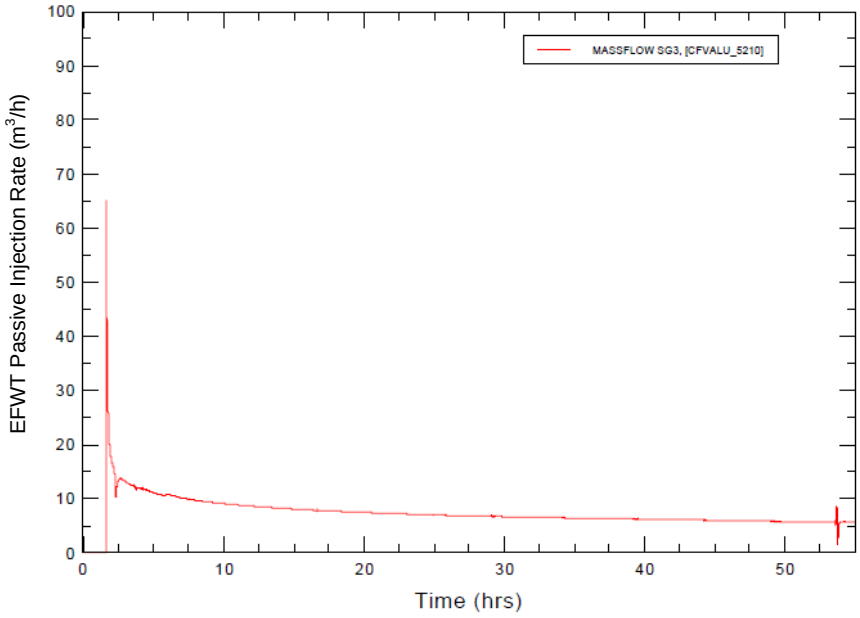

Figure 4 Mass flow SG1 (single loop), passive injection from the EFWT

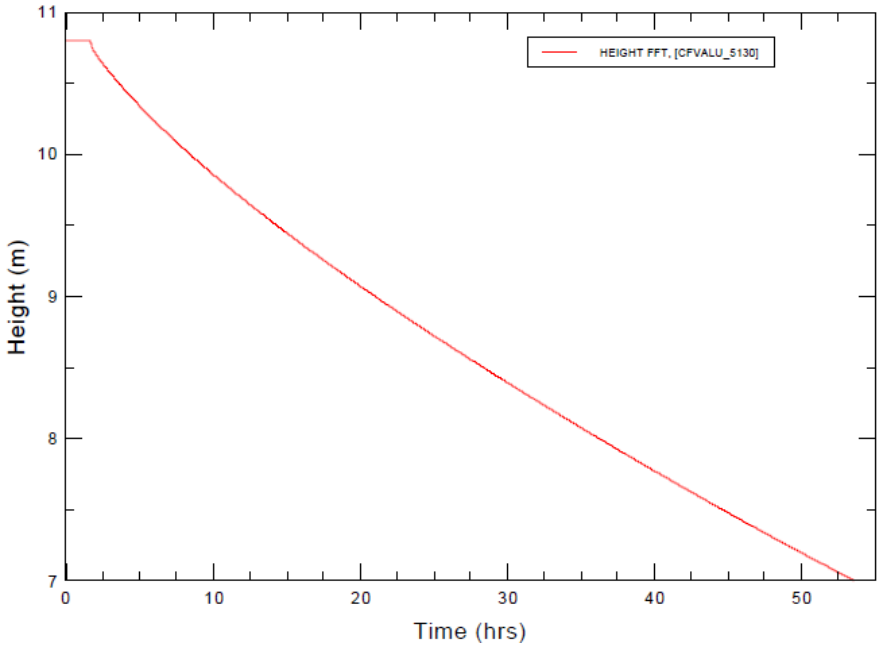

Figure 5 Height in the Fire Fighting Tank

Due to the extensive time during which the reactor core is protected by the secondary bleed and feed (50 h), no core damage can be observed in Figures 2 and 3 because the event is simulated only for 12 h.

SB LOCA

The scenario SB LOCA (20cm2), deals with a leak of 20cm2 in a cold leg of a Reactor Coolant Loop (RCL) together with the following boundary conditions:

- Turbine bypass not available;
- Condenser not available;
- ECCS injection from the refuelling water storage tank (RWST) by Safety Injection Pumps (SIPs) and RHR pumps are available;
- All accumulators are available (cold leg accumulators is automatically locked 500 s after the ECCS signal);
- Loss of suction from the sump and RHR;
- Loss of secondary side 100 K/h cooldown;
- Emergency Feed Water System (EFWS) is available.
- The Secondary Bleed and Feed (SBF) is not activated;
- The Primary Bleed and Feed (PBF) is not activated.

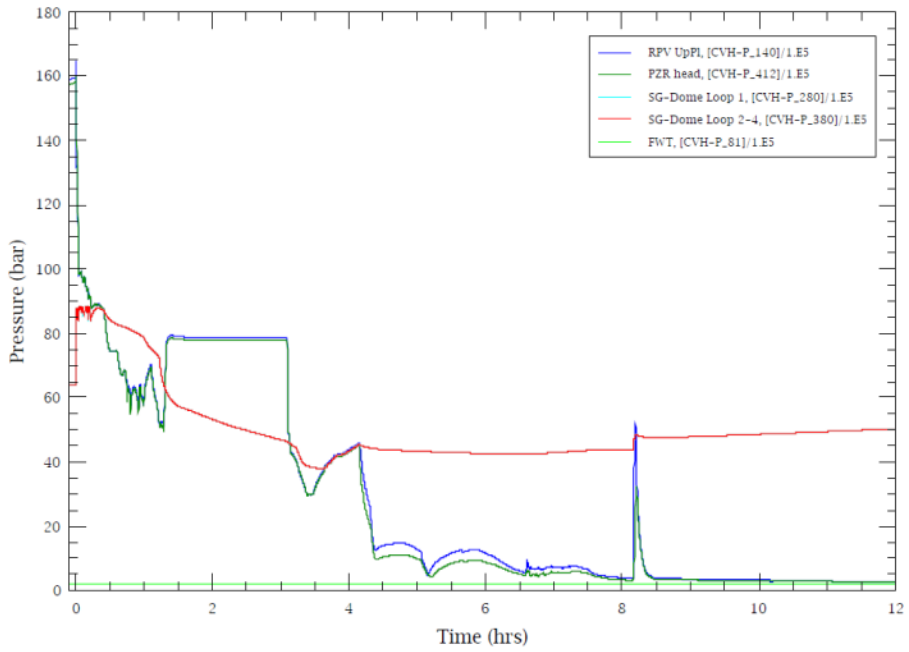

Figure 6 Pressure in RPV, PZR, SG and FW tank

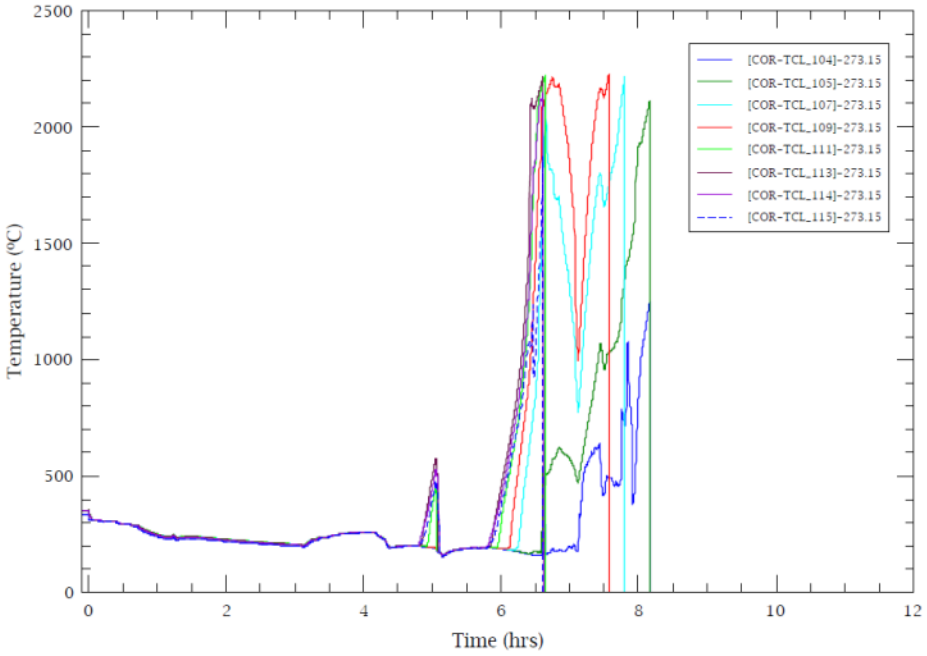

Figure 7 Cladding temperature for innermost ring

Figure 6 presents the pressures in RPV, pressurizer, SG and Feed Water tank. It can be seen that the RCS pressure lifts up sharply at around 1h 18m and remains stagnated up to 3h 7m. This pressure increase and stabilization, about 80 bar, occurs due to the equalization of the leak rate and the injection rate of SIPs, and it continues until the SIP stops due to empty RWSTs (3h 7m). Then, the RCS pressure drops to 50 bar and continues decreasing until 3h 25 m, when the saturation of the water is reached and, therefore, the pressure increases. Due to the fact that the evaporation rate decreases as the water level in the core falls, the RCS pressure drops again and reaches the injection pressure of the four accumulator linked to the hot legsat 26,5 bar. After reaching that pressure, the RCS pressure is determined by the slowly decreasing pressure in the accumulators. The intermittent injection of the four accumulators lasts from 4h 23 m to 10h 10 m, at which RPV failure takes

place. A significant pressure spike due to melt relocation into the residual water appears at about 8h 13 m.

In addition, in Figure 6 it can be observed that the secondary side pressure increases up to 88,3 bar, immediately after the break. It is due to the unavailability of condenser and turbine bypass, and at this point the safety valves open.

Core meltdown begins at 6*h* 30*m*, as can be seen in Figure 7, and it ends at 8*h* 17*m*. According to Figure 8 the maximum cladding temperature is about 2,225°C.

The hydrogen behavior in the plant is depicted by Figure 8. Here, the calculated hydrogen and carbon monoxide mass generated in the core and by Molten Core Concrete Interaction MCCIand the masses recombined are shown.

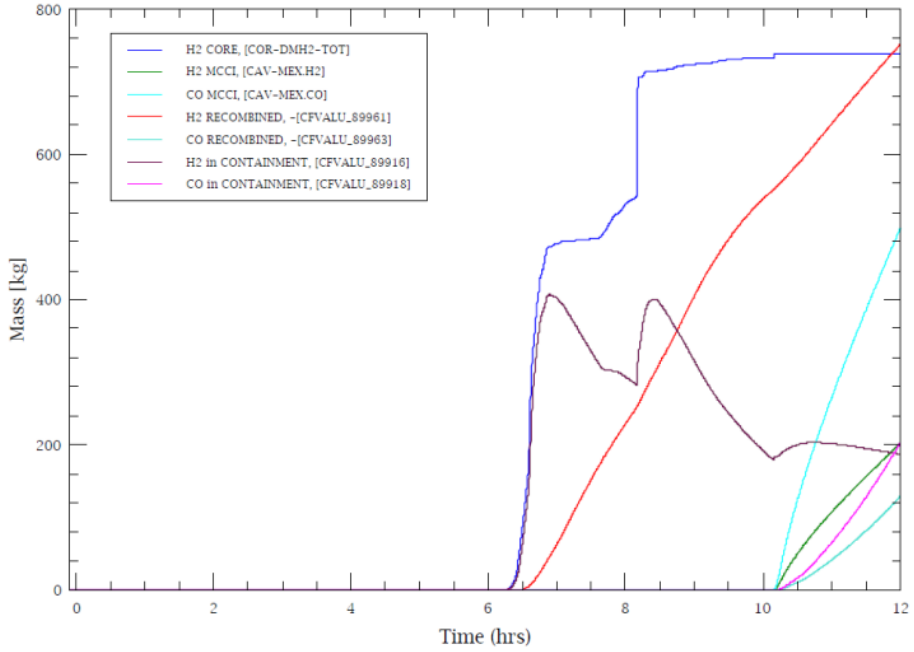

Figure 8 Generated, recombined and residual H2 and CO mass (short-term)

3 EU SUPPORT ON SAFETY OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Beyond modern DI&C and HMI, Angra 3 has incorporated several improvements in relation to the reference plant Angra 2 “as built”, like the combination of seismic events with secondary failures and explosion blast waves for all safety buildings, adoption of F3 tornado, additional features for emergency power supplies and accident management installations regarding Fukushima accident lessons-learned, etc. [10]

AREVA is responsible for the main supplies and services for the overall plant systems and digital I&C systems are implemented with TELEPERM XS (TXS). Siemens is the supplier of the turbine-generator set, human-machine interface (HMI) and systems related to SPPA-T2000.

Digital I&C systems of Angra 3 NPPs

The DI&C important to safety of Angra 3 (AREVA, PWR, 4 loops, 1330 MWe) are set up into 4 x 50 % redundancies following the safety design criteria of the reference plant Angra 2, and it has incorporated concepts of Siemens/KWU PWR-1300 (Konvoi type) plants and also consider TMI-2 accident lessons learned for human-machine interface (HMI) and upgraded accident management supporting installations.

The DI&C architecture of Angra 3 is based on the TELEPERM XS and SPPA-T2000 platforms, designed and arranged according to the diverse and defence in depth concepts (D3) to comply with the three lines of defence as adopted by AREVA designs: preventive, main and risk reduction lines.

Preventive line refers to the actuation/monitoring of process automation systems, process information and control system (PICS) and reactor control and limitation system (RCLS). Main line comprises the actuation of reactor protection system (RPS), autonomous systems (like for emergency diesel generators) and manual actions by the qualified panel safety information and control system (SICS). Risk reduction line deals with design extension functions in response to software common cause failure of RPS, anticipated transient without scram (ATWS) working integrated with dedicated functions of RCLS, as well as to prevent and mitigate beyond design bases consequences.

Figure 9 presents an overview of the main DI&C and HMI blocks of Angra 3, risk reduction blocks assignment and the proposed logic circuit for actuation of diverse system SL4S (SPPA-T2000) in case of RPS (TXS) failure. [12, 13]

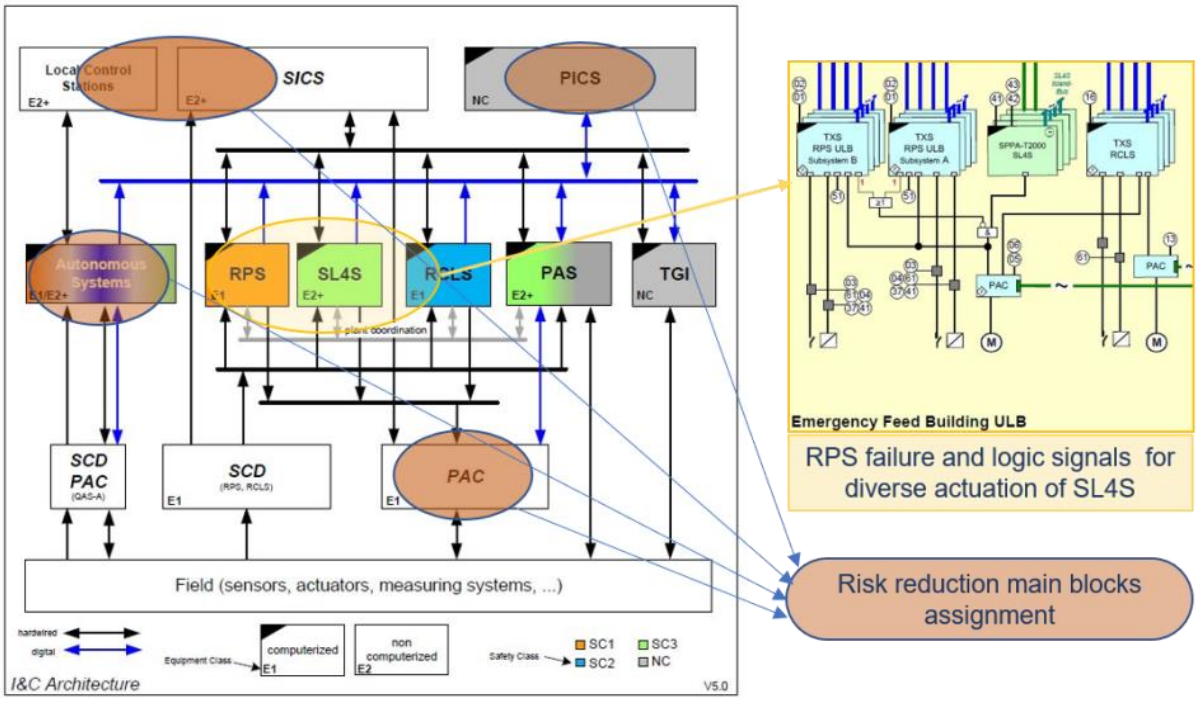

Figure 9 Simplified diagram of Angra 3 DI&C architecture and main reduction blocks assignment (Block diagram, ETN / AREVA copyrights)

Most of the I&C functions important to safety, including the main and emergency control rooms and HMI functions, are located in the switchgear building (UBA) and emergency feed building (ULB), which buildings in Angra 3 are both designed to withstand the SSB events (earthquake SSE plus shock waves due to explosions) and F3 class tornado. Other safety buildings comprise field, radiation monitoring and nuclear instrumentations in the reactor/annulus buildings UJA/UJB and other buildings with autonomous and dedicated safety auxiliary systems.

Table 1 provides an overview of systems platforms, functions, classification, location and defence line assignments, as per PSAR and AREVA life-cycle reports.

Table 1 Overview of Angra 3 DI&C platforms concerning functions, classifications, location and defence line assignments

I&C Systems Comp. Platform	I&C Functions (Levels 1 and 2)	Classification (F. Class)(S. Categ)	Location (Building)	Defence Line Assignment
SPPA-T2000	Process automations	(SC3,NC) (E2+,NC)		
SPPA-T2000	PICS (monitoring, manual HMI)	(NC) (NC)	MCR / ECR	PREVENTIVE
TELEPERM XS	RCLS, PAMS	(SC2,SC3) (E1, E2+)	UBA / ULB	
TELEPERM XS	Autonomous automations	(SC1,2,3) (E1, E2+)		
Hardwired Panel	SICS (conventional HMI)	(-) (E2+)	MCR / ECR / LCS	MAIN
TELEPERM XS	RPS	(SC1) (E1)	UBA/ULB/UJA/UJB	
SPPA-T2000	SL4S (diverse actuation systems for CCF of RPS)	(SC3) (E2+)	ULB	RISK REDUCTION

Reactor Control System (RCS) modernization of Angra 2 to a digital TELEPERM XS “Non-Classified” (NC) category (former analog system, system category E2) was carried out without previous regulatory approval, but with prior technical and organization information from the licensee. The category NC is similar to E2, but not equal, which has been followed as regulatory issue (July 2016) on classification nomenclature for Angra 2 and Angra 3.

The installation and documentation of the new system was inspected and audited, like interfaces of safety systems with existing process computers and aspects related to operating organization, revision of operating procedures, especially aspects dealing with cybersecurity and provisions to conduct on-power calibrations (licensee responsibility) and to support design changes contracted to I&C supplier (core calculations and upgrades).

Licensing process of nuclear installations in Brazil

The licensing process and survey of operation of nuclear installations in Brazil are regulated by the top rules CNEN-NE-1.04, CNEN-NE-1.26 for safety operation of NPP and CNEN-NN-1.16 for licensee‘s quality assurance and organizational programs that shall be applied since the local approval until the operation (including decommissioning). Many other rules are called by those top rules dealing with specific requirements. [14, 15, 16]

The overall review guidance of nuclear reactors has been relied on the Standard Review Plan (SRP) of NUREG-800, starting from Angra 1 NPP licensing and inspection of the pre-operational phase since 1981. The review guidance has been consolidating regulatory experiences and, particularly, several adaptations and updates for Angra 2 licensing, commissioning, operation, modernization and operational experience surveys, which were applied to the licensing and review process of Angra 3 since 2000s. [17]

The scope and licensing objectives of DI&C of Angra 3 described hereinafter are related mainly to the compliance of Section 6 “Construction License” and Item 6.5 “Codes and Technical Standards” of licensing process of CNEN-NE-104, where the proven technology principle plays important role for overall licensing process. Review and assessment include the compliance to the reference plan Angra 2 “as built” and demonstrations to what extent the use of qualified digital technologies and architecture should have been considered a “first-of-kind” or “proven technology” solution.

The final construction license (CL) of Angra 3 was issued in 2010, based on a review and assessment of preliminary safety analysis report (PSAR) and its incorporated references for Revisions 2 and 3. In relation of PSAR Chapter 7, several evaluations have supported the CL Specific Conditions on DI&C and HMI performed by TELEPERM XS (TXS) and SPPA-T2000 computer-based platforms. [18, 19]

First phase of EU-Brazil cooperation

The first phase of the EU-Brazil cooperation in the framework of the European Union INSC programme for BRAZIL (BR3.01/09) started in 2011. The overall objective was to enhance and strengthen the nuclear safety regulatory regime in Brazil (e.g. regulatory framework, procedures, systems, safety culture, etc.) in accordance with international obligations and internationally accepted criteria and practice. The main objective of the task related to the I&C systems of the NPPs was to establish a sustainable capacity within CNEN to carry out or commission independent assessments of the safety of digital I&C systems as part of the licensing process.

During this project, Brasilian beneficiary received assistance in aspects related to the elaboration of internal guidelines for the commissionig and assessment of modern safety I&C based on computer-based techniques as well as hardware programmable solutions. Presentations on regulatory and licensing practices were supported by practical experiences also in the frame of NPP site visits in Europe. Further needs of support from European experts were identified for future activities concerning licensing and assessment of the new constructed as well as digital upgrading of NPP in Brazil.

Parallel with the first phase of the EU Cooperation in 2011, the Licensee started to send responses to CL I&C Conditions which dealt mainly with life-cycle documentation, architecture and diverse and defence in depth concept against the software/hardware common cause failures.

European standards and current practices related to new reactors like EPR of AREVA and the experiences of I&C modernization with TXS platform were discussed with European regulators encompassing review methodologies and specific guidance on assessment of quality and reliability of software and programmable electronics based on IEC standards and consolidation of the internal guideline for review and assessment of DI&C systems. [20, 21]

Objectives of the second phase of EU-Brazil cooperation

The ongoing second phase of the EU-Brazil cooperation started in 2015 and intended to continue the discussions carried out during the first phase. The focus was set on more specific subjects and learning from previous licensing experiences on similar DI&C as Angra 3, such as Olkiluoto 3 new build in Finland.

The objective of the I&C task of the ongoing project is to support CNEN in the area of safety assessment of digital instrumentation and control (I&C) systems of the NPPs Angra 3 and/or Angra 2. The task comprises:

- Support for CNEN regarding the classification and the qualification of I&C systems.
- Peer Review of the CNEN Safety Evaluation Report of Angra 3 digital I&C systems regarding methodology and applied requirements:
  - Review the CNEN assessment of the Digital I&C safety analysis of Angra 3.
  - Support CNEN in the assessment of (a selection of) specific safety functions that are implemented by the digital I&C system of Angra 3.
- Advise and support CNEN in setting up an adequate regulatory process (and underlying methods) for the acceptance of the certification of suppliers of digital I&C systems and components.
- Support CNEN in the development of commissioning procedures involving digital I&C systems and components (including SAT, FAT and corresponding test results).

Methodology

The EU experts working in the project (consultant) provide guidance to CNEN regarding selected issues based on the state-of-the-art safety requirements on digital I&C important to safety, on international practices and on the experience acquired by the participating

consortium member organizations. The know-how transfer is perform based on the long-term experience with international workshops performed also within the CNEN/GRS bilateral co-operation, considering CNEN's knowledge base and regulatory and licensing needs.

The consultant provides also support for specific safety issues in the framework of the licensing of the digital I&C systems. It proposes and agrees with CNEN on adequate working methods to be adopted (e.g. comments/revisions by correspondence, training workshop, review workshop, etc.), monitors the progress made and makes necessary modifications in the working methods in order to ensure their efficiency and that they have been correctly adopted.

The results of work are documented in reports and slide presentations. Early drafts of deliverables are prepared well in advance to allow each topic to incubate and evolve according to latest status of affairs and to ensure all necessary aspects will be considered.

Each activity of the I&C support task was carefully planned prior to project implementation to enable efficient execution of the project.

Preliminary results

The long construction time of Angra 3, together with several interruptions in the design and construction work, has introduced several challenges and regulatory concerns. This has affected the licensing process of the DI&C of Angra 3, which is based on two step review process of PSAR (construction license) and FSAR (authorization for operation).

The combination of deterministic and probabilistic approaches to discuss and justify design criteria for computer-based systems and application of diverse and defence in depth analysis, international concerns on programmable electronics with and without microprocessors have introduced new level of difficulties to face with the so called beyond design basis event caused by common cause failure of software and new challenges related to cybersecurity.

Interpretations on what is a general or specific qualification of digital I&C systems have also raised several concerns to what extent the so called former "proven technology" concept could be applied for safety applications based on digital technology.

In 2016, several regulatory issues related to safety evaluations and licensee responses were discussed during the second workshop in Brazil, with the participation of licensee staff who presented also experiences on modernization of reactor control system of Angra 2 with the TELEPERM XS system. [22]

Safety evaluation report PT-CGRC-056/16 discusses the use of new field instrumentation qualified by IEEE and RCC-E instead of former equivalent systems qualified by KTA-3505 and KTA-3507 that could be no more available to nuclear industry. The use of new FPGA-based components in the European EPRs has led the Brazilian regulator to request additional information from the licensee to get response to open CL I&C condition dealing with D3 analysis.

Recent evaluation report PT-CGRC-069/17 in relation to licensee CL I&C conditions response has addressed relevant issues regarding architecture complexity, licensee response to diversity and defence in depth (D3) report, events and systems classification, cybersecurity and life cycle activities of Angra 3 DI&C, which have been benefited from the technical cooperation workshops and information exchanges.

The evaluation of D3 report has concluded that its information should be partially accepted and considered consistent in respect to PSAR safety criteria and diverse system SL4S functions. However, there is no new clarification on the effectiveness of the diverse system actuation in case of RPS failure. Moreover, since the beginning of evaluations and discussions taken during the workshops and visits of European reactors in operation and in construction with similar DI&C of Angra 3, the evaluations since 2012 by European regulators have also led to increase the level of regulatory concerns on DI&C architecture of Angra 3 and has also increased the importance of cybersecurity issues. [23, 24, 25]

4 CONCLUSION

This article has presented activities conducted jointly in the frame of an INSC Project by experts of the European Union and the Brazilian regulatory body CNEN. The experience gained evidenced that the transfer of important nuclear safety know-how can be achieved in an effective and fruitful way through this kind of project. The examples presented showed that CNEN is improving the assessment of Angra 2 SAMP as well as the use of the severe accident code MELCOR to simulate the main significant severe accident scenarios for this NPP. This project will also favor a more efficient assessment of SAMP for the other Brazilian NPPs constructed or under construction (Angra 1 and Angra 3, respectively). The project has also supported CNEN to consolidate its internal guideline for review and assessment of digital I&C based on modern safety and technical standards and current practices. Furthermore, the EU experts have provided valuable contributions regarding I&C modernization with TXS platform and also encompassing review methodologies and specific guidance on assessment of the quality and reliability of software and programmable electronics.

Acknowledgments

We would like to acknowledge the European Union who provided the project definition and the resources for the implementation of this project BR3.01/12 in the framework of its Instrument for Nuclear Safety Cooperation (INSC).

References

[1] Implementation of Accident Mangement Programmes in Nuclear Power Plants, IAEA SafetyReport Series 32, Vienna, 2004.

[2] P-001/11 – Plano de Resposta à Fukushima - Eletronuclear, 2011.

[3] Evaluación de Resistencia de las Centrales Nucleares em los Países Miembros del FORO Iberoamericano de Organismos Reguladores Radiológicos y Nucleares, September 2011.

[4] BR3.01/12 - Support to the Nuclear Safety Regulator of Brazil, Terms of Reference – INSC Programme 2012, Brazil, Nuclear Safety.

[5] Eletronuclear, Final Safety Analysis Report – Central Nuclear Almirante Álvaro Alberto – Unit 2, ELETRONUCLEAR S. A., Doc. Ident. MA/2-0809.2/060000, Rev. 10, 2006.

[6] DT-006/12 - Relatório De Avaliação De Resistência Das Unidades Da Central Nuclear Almirante Álvaro Alberto Para As Condições Do Acidente De Fukushima (“STRESS TEST”), Eletronuclear, March 29, 2011.

[7] INSC Project BR3.01/12, Task 5: Cooperation with CNEN in Severe Accident Management (SAM), First Workshop report, CNEN, Rio de Janeiro, November, 2015.

[8] INSC Project BR3.01/12, Task 5: Cooperation with CNEN in Severe Accident Management (SAM), Second Workshop report, CNEN, Rio de Janeiro, October, 2016.

[9] INSC Project BR3.01/12, Task 5: Cooperation with CNEN in Severe Accident Management (SAM), Third Workshop report, STUK, Helsinki, October, 2016.

[10] INSC Project BR3.01/12, Task 5: Cooperation with CNEN in Severe Accident Management (SAM), Kick-off Meeting report, CNEN, Rio de Janeiro, July, 2017.

[11] CNEN, 6th and 7th Conventions on Nuclear Safety Report of IAEA, 2013-2016.

[12] Eletronuclear (ETN), PSAR, Revision 2 and 3, 2008-2010.

[13] AREVA, Overall I&C – Plant Configuration (Architecture), TD01-1.31, Dec-2015.

[14] CNEN NE 1.04, Licensing of Nuclear Installations, Dec-2002.

[15] CNEN-NE-1.26, Safety in the Operation of NPP, Oct-1997.

[16] CNEN-NN-1.16, Quality Assurance for Safety of NPP and Other Installations, Apr-2000.

[17] US-NRC, Standard Review Plant, NUREG 800.

[18] CNEN, Angra 3 Construction License, May-2010.

[19] CNEN, Evaluation Report, PT-CGRC-084/08, Oct-2008

[20] ISTec-A-2290, Assessment of Quality and Reliability of Software Based on IEC Standards, Jan-2012.

[21] CNEN, Internal Guideline on R&A of DI&C, Revision 3, Dec-2016.

[22] EU Cooperation BR3.01-12, Task 6, 3rd Workshop Report, Dec-2016.

[23] CNEN, Evaluation Report, PT-CGRC-056/16, Sep-2016

[24] CNEN, Evaluation Report, PT-CGRC-069/17, Sep-2017

[25] AREVA, Diversity and Defense-in-Depth Analysis, BN-31157-0068-100052, Angra BRA011, Jan-2016.