https://doi.org/10.47669/ISER-2-2023

SCIENTIFIC AND ENGINEERING ISSUES AND CHALLENGES OF PHYSICAL SEPARATION OF SAFETY SYSTEMS OF OLD GENERATION NUCLEAR POWER PLANTS

Lusine MELIK- SARGSYAN*

This article discusses the scientific and engineering issues and criticality of physical separation of safety systems of old generation nuclear power plants. Based on the scientific and engineering comprehensive analyses within the framework of this scientific and research work it has been concluded that the physical separation of safety systems at old generation nuclear power plants like Armenian NPP was among deficiencies of VVER 440 reactors identified in with high ranking.

Keywords: *Nuclear energy, nuclear safety, nuclear engineering, physical separation, safety system, Nuclear Power Plant, scientific and engineering analysis*

Armenian NPP has two units with VVER-440/270 type reactors. Unit 2 had been commissioned in 1980. Both units of Armenian NPP were shut down after Spitak earthquake in 1988. In 1993, a decision was made to restart the unit 2 of Armenian NPP. In the course of activities related to the restart of the unit 2, a list of activities for modernization was developed, most of which had been performed before the restart. There were also developed measures, which had to be implemented during the subsequent outages and in the course of the operation of the unit. This list took into consideration the operational experience of other reactors of V-230 type and their programs of modernization, as well as recommendations of IAEA (TECDOC 640). After completion of the repair activities and works related to the safety upgrading, unit 2 has been restarted in 1995.

Elaboration of the design of Armenian NPP had been based on a concept assuming that high quality equipment and components of the reactor facility, as well as proper quality of operation, i.e. control of the equipment and pipelines metal and welds, allowed to avoid their significant degradation, thereby excluding the possibility of serious accident.

* Lusine Melik-Sargsyan, Ph.D. in Nuclear Engineering.

Therefore, as a design basis accident, LOCA-32 was considered.

The accident localization system of the unit includes leak-tight containments, designed for excessive pressure, where the reactor and the primary circuit equipment are installed. The leak-tight containments are equipped with spray system, which is assigned for steam condensation during the accidents.

In the design, there were no strict requirements to the leak tightness of the containment, as no serious damage of the fuel element was assumed.

Moreover, the Armenian NPP has specific safety systems included in the design, which aim at the seismic safety.

After commissioning of the units, a new comprehensive approach started to form to the nuclear power plants as to objects of ultimate hazard. It was based on the principles of safety assurance of the nuclear power plants, accepted by the International Community: defense in-depth, single failure and application of the scientific and engineering method of safety analyses based on the postulated initial events evaluation.

VVER-440 units of the first generation did not meet those standards, of course, thus the necessity of significant modification of the units had risen.

The units of the first generation also have positive design features.

The most specific ones are:

- The V-270 reactor has a small and compact core, which practically is not subject to xenon fluctuations. There is no necessity for local adjustment of the neutron flux, the reactor is stable and has strong negative feedback, which creates favorable conditions for accident management.
- The fuel rating of the core is rather low, which provides significant critical power ratio during various transients, the average temperature of the fuel is not high. The structure of the fuel pellets with a central hole also decreases the peak fuel temperature. This ensures the high level of retention of the radioactive products of fission within the fuel matrix.
- Large volume of the primary circuit coolant and large inventory of water in the Steam Generators from the secondary side enables passive cooling down of the reactor core during long time, which allows to speak about passive safety of the power unit.
- High quality of the primary circuit components and, as a result, lower probability of primary circuit breaking.
- Main Coolant Pumps with flywheels.

These specific features of safety provide significant safety margin and operational flexibility for management of the transients during operation and in case of accidents.

However, the initial design of the power plant has number of significant design deficiencies, including:

- Design basis accident of LOCA type is break with equivalent diameter of only 32mm, and, respectively, the systems have limited possibilities to cope with LOCA accidents (particularly, emergency core cooling system and containment systems);
- Insufficient leak tightness and strength of the containment.
- Inadequacy to the requirements of physical and electric separation of normal operation and safety systems.
- Inadequate redundancy of the safety systems and insufficient physical separation of the redundant channels.
- Incompliance of the safety systems with the single failure criteria.
- Incompliance of the classification and qualification of the safety systems with the requirements of the environmental parameters (including the seismic qualification);
- Limited fire-resistance and flooding protection.
- Deficiencies of automatic actuation of the safety systems.
- Incompliance of the power plant with safety requirements, as the results of the deterministic and probabilistic safety analyses show.

The unit design includes safety systems, which are classified as protective, localizing, control and supporting, according to OPB-88/97. The mentioned systems underwent serious modifications during operation of the unit, which compensated for the most significant deficiencies of safety. The description of safety systems and measures and modifications carried out are detailed in the Safety Analyses Report of ANPP unit 2.

In accordance with the energy strategy of the country, the Government of the Republic of Armenia adopted a decision to continue the operation of the power unit 2 of the Armenian NPP at least by the end of 2016.

The basis for the comprehensive modernization program shall be the clearly defined safety objectives (to be done by ANRA) and problems revealed during development of DSA, PSA and other analyses considering the recommendations of IAEA Missions.

For development and management of the comprehensive analyses of ANPP safety improvement within the framework of the contract ARM 90222–86943V, the main standards have been selected from the list of existing normative documents of RA, RF and guidelines

of IAEA, based on which the safety analyses and elaboration of the complete program of ANPP modernization shall be performed.

Definition of relevant Safety Issues

IAEA Tecdoc 640

Document Ranking of safety issues for WWER-440 model 230 nuclear power plants [2] refers to separation of safety systems in several Issue sheets:

Safety Issue "Electrical 1", entitled "Electrical Redundancy, Separation and Independence", (Rank IV)

There are numerous instances where redundancy, physical and electrical separation and independence of electrical supplies are not adequately provided. It is recommended that either separation and independence of the safety-related electrical power supplies or an additional separate set of power supplies should be provided.

Safety Issue "Systems 8", entitled "ECCS - Redundancy and Physical Separation of Redundant Parts" (Rank IV)

A failure modes and effects analysis (or similar scientific and engineering analysis) should be conducted to identify the major areas where improvements should be made.

A physical separation concept should be developed, segregation of the high-pressure injection and spray systems should be considered. Long term cooling strategies should be analyzed and developed.

Safety Issue "I&C 3" entitled "Control and protection systems interaction" (Rank II)

Full isolation or separation between control and protection functions of instrumentation is not provided.

A fault in the non-safety related instrumentation may induce the failure of safety related equipment.

Safety Issue "I&C 4" entitled "I&C redundancy, separation and independence." (Rank IV)

There are numerous instances where redundancy, physical and electrical separation and independence of safety-related instrumentation channels are not adequately provided. Either separation and independence of the existing safety related instrumentation or an additional separate independent set of instrumentation should be provided

Safety Issue "Electrical 2", entitled "Reliability of Electrical Equipment" (Rank III)

In general, the electric equipment at ANPP needs particular attention due to the age and to the original design that does not meet all necessary safety requirements for separation, segregation and independence.

Safety related functions are performed by electro-mechanical equipment, which should be redundant, to fulfil the single failure criterion and adequately segregated to prevent common cause failures. The corresponding AC power supply systems should then comply with the same design criteria so as not to impair the operability of the safety functions.

In a WWER-440/230, 6 kV and 400 V AC safety-related distribution systems are organized in 2 trains with distribution boards installed in separate rooms. There are, however, interconnections between the distribution boards of the two trains at all levels. Therefore, comprehensive investigation should be performed to determine whether it is possible to implement a strict train segregation concept and to eliminate as many interconnecting cables as possible.

At the same time, the means to improve separation in the layout between the two trains should be investigated and strict procedures should be implemented to keep doors and ducts between rooms of the two trains closed. Potential consequences on the required cooling and ventilation systems' capacity need to be considered.

Cable Segregation: There is no strict separation between the cable routes of redundant trains or between the cable routes of the two twinned units. There are several areas where redundant cable paths cross each other (junction areas). In these junction areas, redundant cables from the same unit or even from different units may be arranged in common trays over a certain distance. Similar junctions exist within the I&C systems or between the I&C and power cables.

Although a strict separation between redundant cables would be impossible within the existing buildings, local improvements are possible: al junction areas should be identified and improvements of local separation and fire protection in these areas should be defined and implemented.

Due to the limitations of such improvements, an independent approach, like an independent cable network, could be considered.

IAEA Mission 2009 issues

Several IAEA missions visited ANPP and inspected the plant and provided recommendations for improvements. So far, the last IAEA mission of 2009 assessed the contemporary status of the plant and how the findings from previous missions were dealt with. As a result, 2009 IAEA mission published 45 issue sheets with assessment of the progress in the outstanding safety issues.

Plant status in November 2003 was assessed. It was stated that the plant implemented several technical and administrative measures:

Safety issue No.11, "ECCS – Redundancy and Physical Separation of Redundant Parts" [3] identified deficiencies in the lack of adequate redundancy of ECCS. Common mode/common cause failure of ECCS function is a general concern because of lack of equipment separation. Several other shortcomings have been identified that influence reliability of existing high pressure injection system and spray system, however not directly associated with the separation of systems.

Conceptual recommendations proposed in the issue sheet include: "A physical separation concept should be developed; segregation of the high-pressure injection and spray systems should be considered. Long term cooling strategy should be analyzed and developed."

Rather extensive works have been performed at ANPP involving modification of ECCS, spray system, heat removal system and other measures. Despite that IAEA 2003 mission specified following conclusions (C) and Recommendations (R):

C1. Physical separation, in existing ECCS 2 trains configuration, does not exist.

C2 Level measurement system in the boron room is not redundant.

C3 Measures to prevent clogging of containment sump, like the measures taken at other V230 NPPs, will be implemented at Armenia NPP in 2004

C4 Intent of IAEA recommendations on this issue is only partly met.

R1 UT/ISI should be performed periodically, at the critical locations of ECCS piping, in order to prevent any ECCS pipe failure, following a LOCA.

R2 System of water level measurement and the drainage pumps in the boron room should comply with the single failure criterion.

R3 Measures to prevent clogging of containment sump should be implemented as soon as possible and no later than the end of 2004, as anticipated.

ANPP implemented another set of measures such as introduction of periodic ultra-sonic tests of critical parts of emergency core cooling system, installation of drain pumps to drain sump of boron unit 3 and measures to prevent from containment sump clogging.

In 2009 IAEA follow-up mission stated that:

The electrical supply of category II (diesel generators), providing the ECCS/SS with power was redesigned into 2 independent channels with 2 DG per channel. Each channel has the potential capacity to feed 2 of 3 ECCS pumps. In view of the new DBA the DG acceleration was improved, thus in the new conditions staggered loading of consumers can

start after 35 s instead 60. The Spray System will be re-designed, and a fourth spray pump is intended to be installed in the boron compartment to ensure complete 2-channel redundancy of the system (except common boron tank).

Contract for "Armenian NPP Unit 2 Improvement of sprinkler system" was signed with Nizhny Novgorod FGUP NIAEP in 2006 and other contract on extending the sprinkler system improvement with Vibroseism Central Engineering Institute, St. Petersburg, in 2008, for selection of optimal pipeline lay-out of the improved sprinkler system with the fourth pump and loads calculation on the system components nozzle.

ANPP has planned replacement of sprinkler pumps and valves within EC programs. The completion was expected during 2011 outage.

Measures to prevent clogging of containment sump are well underway and are intended should be implemented during the 2010-year outage. The screen area is significantly enlarged, the mesh size reduced. The system will undergo factory acceptance test under real conditions before installation.

One recommendation was specified by IAEA 2009 follow-up mission:

R1 To develop and implement a long-term cooling strategy.

Basic engineering for a new design of ECCS that meets requirement for newly defined maximum DBA and capability of long-term cooling is being developed within current project Development of a Comprehensive Modernization Programme of Armenian NPP Unit.

Safety issue No.27, "Control and Protection Systems Interaction" identified that full isolation or separation between control and protection functions of instrumentation is not provided. A fault in the non-safety related instrumentation may induce the failure of safety related equipment.

Despite of multiple measures taken by ANPP, 2003 IAEA mission specified several conclusions (C) and recommendations (R):

C1. The complete separation between protections and interlock or control system is not totally performed on the plant. There are 2 cases where EPS equipment is common with interlocks or control systems: level in pressurizer and pressure in containment. The corresponding improvements to meet.

IAEA recommendations are forecasted in "The list of technical measures."

R1. IAEA recommends to strictly follow requirements of safety standards (see reference): "if signals are used in common by both the protection system and any control system, appropriate separation shall be ensured, and it shall be demonstrated that all safety requirements are fulfilled".

C2. Concerning new cables (inside the same train) to be installed in the future, ANPP intends to install different cable trays for each protection system channel, completely separated from the other cable trays.

C3. Concerning old cables which are installed without separation consideration, ANPP intends also to reorganize the arrangement of these cables to meet the requirements of separation.

ANPP implemented additional measures, including upgrade of the plant protection system to resolve the findings from 2003 mission. Follow-up IAEA mission in 2009 then specified following conclusions and recommendations:

C.1 Comment C.1 and Recommendation R.1 from the previous mission will be resolved once the plant protection system upgrade is completed.

C.2 Comments C.2 and C.3 from the previous mission will be addressed by the protection system upgrade. Final resolution of these comments should be tracked as part of the evaluation of Issue 28. R.1 This issue may be closed once the plant protection system upgrade is completed.

ANPP is implementing new design of reactor protections and interlocks logic, which should completely meet the requirements of "single failure" and "common cause failure":

- Two reactor control, monitoring and protection trains with physical and galvanic separation are being established.
- Measurement detectors are distributed to different rooms to the extent possible.
- Measurement and power cables are separated to the extent possible.
- Emergency protection and safety system actuation logics have been separated.
- Advanced instruments and detectors have been applied for measurement of reactors.

After implementation of modernization two independent reactor protections and interlocks trains with galvanic and physical separation using up-to-date detectors and instruments all weaknesses of the existing logic have been considered and removed from the new design to the extent possible at the Armenian NPP.

Safety issue No.28, "I&C Redundancy and Physical Separation of Redundant Parts" identified are numerous instances where redundancy, physical and electrical separation and independence of safety related instrumentation channels are not adequately provided. ANPP implemented set of measures to improve situation, which included:

- Specifying the common circuits of ANPP protections and interlocks in design diagrams and charts.

- Isolation of the safety system connection signals.

- Installation of additional Δp measuring channels RCPs, steam lines, MSH.

- Isolation of SG level interlocks and signals.

- Reconstruction of cabling connecting the systems, protections, interlocks and other safety and safety important loads to two different power supply systems of categories I and II.

- SUZ-2 (control rod system) powered from physically and galvanically isolated sources of power supply.

- All protections and interlocks of reactor are powered from six bushings of – 220V DC (3 bushings from 2BAB-1 and 3 bushings from BAB-2), the loss of even 4 corresponding bushings won't affect safe operation of the system.

- The process alarm circuits of MCR are powered from two bushings of category I reliability.

In 2003 IAEA Safety Mission stated that:

C1. 15 channels of the emergency system protection (16 in total) are designed with 3 sensors for 2 trains. So, there is no independence between train A and train B. There is the same problem for corresponding electrical supplies. Moreover, there are several common circuits between EPS and control systems: i.e., the same sensor is used for EPS and for other systems. For the other channels (i.e., neutron protections) the principles of physical separation are applied according to international standards.

C2. Even if ANPP intends to completely change EPS in 2005, IAEA recommends careful consideration and vigorous application of IAEA requirements (see ref. 1 and 2) for EPS.

C3. Designs of EPS doesn´t apply diversity principle: only de-energize-to actuate technique is used.

C4. For implementation of new EPS, IAEA recommends analyzing the possible improvement of EPS, by introducing the diversity principle.

After 2003, ANPP has made technical decision No. 42 dated as 01.10.08 regarding establishment of two-way system of reactor protections and interlocks considering requirements of current codes and standards as well as recommendations of IAEA TECDOC-640. Technical specifications and design have been developed. Implementation is scheduled for outage 2011.

In 2009 IAEA Follow-up Mission stated that:

C.1 Installation of the new system should resolve the cable separation issues raised in the previous mission Comments C.2 and C.3 on Issue Sheet 27.

C.2 Installation of the new (reactor protection) *system should also resolve the separation issue indicated in Comment C.1 of this sheet (number 28).*

Comments C.3 and C.4 from the previous mission have not been explicitly addressed. Nevertheless, considerable diversity exists in the proposed design.

- Diverse functions respond to many postulated initiating events.

- Some of these diverse functions involve diverse sensing hardware such as pressure and temperature sensors.

- In the case of reactor trip the new automatic reactor power control system provides for power reduction that uses signal processing and logic that is diverse from the protection system.

- Signal processing and logic hardware is not diverse, but it is planned to implement this design using individual hardware modules in each measurement channel and separate voting logic for each individual actuation function.

- No diversity is planned for the final voting logic, but these are simple relay logic functions for which exhaustive design verification should be possible.

- The two subsystems are in different rooms and should limit the possibilities for simultaneous CCF due to common environmental conditions.

Some points of possible CCF vulnerability remain. For example:

- Each reactor protection system in the new design receives power from a common power source that is auctioneered with a second power source that is unique to each subsystem. Over-voltage on the shared common power source might cause failures in both subsystems. This is of particular interest since the final actuation logic is energized to actuate, and thus is not a "fail-safe" design.

- Both new reactor protection subsystems and the automatic power control system share the same nuclear instrument signals.

Moreover, IAEA 2009 follow-up mission gave the following recommendations:

R.1 The design of the new system should be reviewed against the requirements of NS-R-14 and the recommendations NS-G-1.35 to resolve the recommendation of comment C.2 from the previous mission.

R.2 The degree of diversity in the proposed new design should be described and justified in the safety basis documents.

Current status in the resolving the findings of Safety Issue No 28 is closely associated with resolving of findings in Safety Issue No. 27, since the findings are in general common.

ANPP is implementing new design of reactor protections and interlocks logic, which completely meets the requirements of "single failure" and "common cause failure":

- Two reactor control, monitoring and protection trains with physical and galvanic separation are being established.
- Measurement detectors are distributed to different rooms to the extent possible.
- Measurement and power cables are separated to the extent possible.
- Emergency protection and safety system actuation logics have been separated.
- Advanced instruments and detectors have been applied for measurement of reactors.

After implementation of modernization two independent reactor protections and interlocks trains with galvanic and physical separation using up-to-date detectors and instruments all weaknesses of the existing logic have been considered and removed from the new design to the extent possible at the Armenian NPP.

The original Neutron flux monitoring system was replaced with a new one (Data Systems & Solutions). All neutron flux sensors were replaced with new type sensors and all cable lines were galvanically and physically separated to the extent possible for Armenian NPP. The transmitters (measurement part) were placed in different rooms. Two trains, three measurement channels each, that are galvanically and physically separated were installed.

However, it should be stressed that physical separation of systems have been performed" to the extent possible", i.e. there are still some shortcomings where separation was constrained by spatial limitations. Nonetheless, installation of the new design will mean significant improvement in the reactor protection system.

Safety issue No.33, "Electrical Redundancy, Separation and Independence" [6] identified are numerous instances where redundancy, physical and electrical separation and independence of safety related instrumentation channels are not adequately provided.

ANPP implemented many measures for improving the situation. Major measures included: Diesel generator protection; replacement of the batteries; increased reliability of power supply system; functioning of a two-train reliable power supply system was provided at the plant; cable connections of each train were physically separated and have a fire-resistant covering; supplementary emergency cooling system was installed; a portable diesel generator of low rated capacity was obtained; power supply to I&C was implemented from MCR-2

power supply panels; cooling water for diesel generator station was supplied through two trains from SWS-I-II (Service water system). The trains are physically and galvanically separated. Each train has two operations and one stand-by pump.

In 2003 IAEA Safety Mission specified the following conclusions (C) and recommendations (R):

C.1. ANPP position is that the current EDG configuration provides complete redundancy of the emergency power system for the current analyzed design basis accidents.

C.2. Only one EDG is required for plant safe shutdown during currently analyzed DBA.

C.3. ANPP has plans to perform further enhancement of the EDG such that the redundant diesels of each channel (i.e., each set of diesels) is in the same room. And provide additional capability for a third channel EDG power supply.

R.1. Ensure the planned modifications for EDG systems will satisfy the IAEA safety guide for Emergency Power System concerning Common Cause failure.

After the 2003 mission, ANPP completed separation of DG by trains, including cable communications, installed two trains of uninterruptible power supply. Electronic speed control, monitoring and voltage control were installed on DGs.

Based on the implemented measures and discussion with representatives of ANPP, IAEA 2009 follow up mission specified two recommendations:

R1 Review and improve, where necessary, the physical separation and independence between the two electrical trains at the level of cable routing and equipment inside the building's areas and compartments. Considering the in-progress activity to increase up to 100 mm diameter the DBA, the review of separation and independence requirements shall take into account these new modernization works.

R2 Improve the identification of the cables and cable trays with indication of the belonging electrical safety division (train).

In emergency power supply new DG automatic control systems and generator voltage control excitation were installed. These meet current safety principles:

- "Single failure" and "common cause failure";
- Multichanneling;
- Galvanic and physical separation;
- Electrical and process parameters recording and archiving.
- Requirement of operator non-intervention (for 10 minutes).

CONCLUSION

Separation of safety systems at ANPP was among deficiencies of VVER 440 reactors identified in with high ranking. It was confirmed also for ANPP by IAEA safety missions in 2003 and 2009, when the later identified deficiencies in ECCS redundancy and physical separation of redundant parts, in I&C Redundancy, Separation and Independence and in Electrical Redundancy, Separation and Independence, all classified with ranking IV, which means issues of high concern.

REFERENCES

1. Ranking of Safety Issues for WWER-440 Model 230 Nuclear Power Plants. IAEA-TECDOC-640, Vienna, 1992

2. IAEA Mission at ANPP on 2009: WWER 440/270 IAEA Issue Sheet No. 11, “ECCS –Redundancy and Physical Separation of Redundant Parts”

3. IAEA Mission at ANPP on 2009: WWER 440/270 IAEA Issue Sheet No. 27, “Control and Protection Systems Interaction”.