Transactions of the Korean Nuclear Society Autumn Meeting
Yeosu, Korea, October 25-26, 2018

A Comparative Study of Safety Systems from Selected Advanced Nuclear Reactors

Anselm Niwemuhwezi [a*], Sukho Lee [b]
[a]*Korea Advanced Institute of Science & Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*
[b]*Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon 34142, Republic of Korea*
[*]*Corresponding author: a.niwemuhwezi@kaist.ac.kr*

1. Introduction

Reactor safety systems required for achieving fundamental safety functions in VVER-1200 (V-392M), AP1000 and APR1400 nuclear reactors were compared. These safety functions are; control of reactivity, removal of decay heat and confinement of radioactive material.

The selected reactors are of generation III and III$^+$. Generation III reactors are advanced nuclear reactors that are developed from generation II reactors. They incorporate improvements in areas of fuel technology, thermal efficiency, modular construction, safety systems and standardized design. These reactors are currently under construction. They have a design life of 60 years. Examples include HPR1000, APR1400, ABWR and AP600. Generation III$^+$ are evolutionary reactors developed from Gen III offering significant improvements in safety and economics. Examples include VVER-1200, AP1000 and APR$^+$.

VVER-1200 is a generation III$^+$ pressurized water reactor developed by OKB Gidropress [1]. It is an evolutionary development of VVER-1000 reactor with additional passive safety features. It has distinguishing features from most of the other PWRs, including horizontal steam generators and hexagonal fuel assemblies. There are two designs of VVER-1200 that is V-392M and V-491. The differences are in plant layout, I&C systems, feedwater system, and the main control room. V-392M uses more passive safety systems compared to V-491. However, each of them meets safety requirements and IAEA recommendations for safety of nuclear power plants in design. For this study, V-392M design was considered.

Advanced Passive PWR (AP1000) is a generation III+ pressurized water reactor designed by Westinghouse based on AP600 design [2]. It uses more passive safety features that rely more on natural forces such as gravity and natural convection.

Advanced Power Reactor 1400 MWe (APR1400) is a generation III pressurized water reactor developed by KEPCO/KHNP based on the experience from development, construction, and operation of OPR1000 [3].

2. Objectives and scope of the study

The objective is to study and compare safety systems of VVER-1200, AP1000 and APR1400 reactors necessary for achieving fundamental safety functions. The study will also show how the concept and principles of defense-in-depth (DiD) are applied in the design and operation of these reactors. This comparison will be useful for safety evaluation of the selected designs especially to newcomer countries who plan to utilize nuclear energy.

This study focuses on safety systems of three reactors as representatives of generation III and III+ advanced nuclear reactors. These designs were compared based on the type of safety system present and its ability to execute its safety function. In addition, the application of DiD principle in reactor design was discussed. The purpose is not to provide a ranking but instead to identify and describe safety systems used to achieve fundamental safety functions and how DiD is achieved in design.

Table 1: General reactor specifications

	VVER -1200	AP1000	APR 1400
Thermal output (MWth)	3200	3415	3983
Net electrical output (MWe)	1082	1100	1400
Net plant efficiency (%)	33.9	32	35.1
Design life (years)	60	60	60
Refueling Interval (months)	12 - 18	18	18
Core Damage Frequency (CDF)	<1E−6	<5.09E−7	<1E−5
Large Early Release Frequency (LERF)	<1E−7	<5.94E −8	<1E−6
Safe shutdown earthquake (SSE)	0.25g	0.3g	0.3g

3. Fundamental safety principles

Safety functions must be accomplished to ensure safety of the facility at all conditions that is normal plant condition, anticipated operational occurrences and accident conditions. There are three fundamental safety functions as discussed below.

Control of reactivity: The nuclear reaction is a chain reaction that must be controlled to avoid excessive reactivity that can lead to an explosion. Control rods containing neutron-absorbing materials such as boron, silver, indium and cadmium are used for primary reactivity control. The chain reaction is terminated when control rods are fully inserted but it proceeds by partial or complete removal of control rods. The secondary measure to control reactivity is by use of chemical shim; usually boric acid. Control is achieved by varying concentrations of this neutron-absorbing chemical.

Removal of decay heat: Heat is removed during normal operation by generating steam, which runs the turbine that is connected to a generator that generates electrical energy. When the reactor is shutdown, the core continues to generate decay heat therefore there should be systems to remove the decay heat generated.

Confinement of radioactive materials: Radioactive materials are isolated from the environment by the containment. The containment acts as the last barrier to the release of radioactive material to the environment in case of core meltdown.

4. Application of defense in depth principle (DiD)

DiD is a nuclear safety concept that involves establishment of multiple layers of defense such that failure of one layer is compensated by the other. The first barrier of defense is the fuel matrix, the second barrier is fuel rod cladding, the third barrier is primary circuit boundary, and the fourth barrier is the containment [4]. DiD is applied at all stages of nuclear facilities that is; siting, design, construction, operation and decommissioning. In order to prevent single failure, principles of independence, redundancy and diversity of systems are necessary.

Table 2: Levels of defense in depth and ways of achieving the objectives

Level	Objective	Ways of achieving the objective
Level 1	Prevention of abnormal operation and failures	Conservative design, selection of appropriate design codes, materials, components and systems, proper site selection, quality assurance in design, construction and operation, following operating instructions and operation by qualified and well trained staff.
Level 2	Control of abnormal operation and detection of failures	Provision of specific systems and features in design, use of control systems, limiting systems, protection systems and other surveillance features, establishment of operating procedures to prevent initiating events, minimize their consequences and ensure that the plant returns to a safe state.
Level 3	Control of accidents within the design basis	Use of engineered safety features, safety systems and procedures to prevent damage to the reactor core, prevent release of radioactive material, and return the plant to a safe state.
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management, establishment of mechanisms for continuous cooling of nuclear fuel and confinement of radioactive material.
Level 5	Mitigation of radiological consequences of significant release of radioactive material	Provision of adequate emergency response facilities, emergency plans and emergency procedures for on-site and off-site emergency response.

In addition, safety functions and DiD are ensured through use of physical plant boundaries such as fuel cladding, reactor coolant system pressure boundary and containment pressure boundary. The presence of passive safety systems notably in the AP1000 and other two reactors ensure that core cooling and containment integrity are maintained in case of design basis events. Challenges to integrity of physical barriers, failure of one or more barriers, failure of a barrier due to failure of another barrier and errors during operation and maintenance should be prevented to ensure that DiD is maintained.

5. Safety systems in selected designs

Safety systems perform the fundamental safety functions of reactivity control, decay heat removal and confinement of radioactive materials. They are classified either as active or passive. Active systems rely on external input such as power supply actuation or mechanical movement. They offer a quick response to handle abnormal events, deviations and design basis accidents. A passive system does not depend on external input to function; it needs a change in pressure, temperature or fluid flow. Passive systems can be used for decay heat removal; however, they are not suitable for quick shutdown in case of emergencies.

All the three reactor types meet the fundamental safety principles and fulfill the concept of DiD and safety functions. Even though the passive safety systems are more reliable, there are still existing uncertainties in the performance and reliability of the passive safety system. These include; understanding of physical phenomena, uncertainty in the natural circulation, definition of passive failure, failure probability and dynamic reliability.

5.1 VVER-1200

This reactor relies on both active and passive safety systems.

Table 3: Safety systems of VVER-1200

System	Function
Emergency core cooling system	Cool down the reactor when heat removal through generators becomes ineffective.
Low pressure emergency injection system	Supply boric acid solution to the reactor coolant system in case of LOCA accident
Emergency boron injection system	Inject boric acid into the pressurizer in case of a leak to reduce the primary pressure and create the required concentration of boric acid in the primary coolant under a BDBA without scram.
Passive core flooding system	Maintain coolant level required for the reactor cooling to prevent core damage. It is made up of hydraulic accumulators that can independently ensure core cooling for 24 hours in the case of a leakage of any size.
Passive heat removal system	Remove residual heat and cool down the plant during normal shutdown, in the event of anticipated operational occurrences and DBA.
Steam generator emergency cooldown system	Remove residual heat from the core and cool the reactor down via the secondary side.
Primary overpressure protection system	Protect the primary side equipment and pipelines from excessive pressure under DBA and BDBA conditions.
Secondary overpressure protection system	Prevent overpressure in steam generators and main steam lines.
Main streamline isolation system	Provide quick and reliable steam generator isolation from a leaking section such as leakage of steam or feed water.
Emergency gas removal system	Removes steam-gas mixture out of the primary side and reduces the primary pressure in order to mitigate the consequences of DBA and BDBA.
Core catcher	Protect against containment damage resulting from core meltdown by retaining molten corium in the reactor vessel.
Double-envelope containment	Retain radioactive substances and ionizing radiation within design limit.

5.2 AP1000

AP1000 depends mainly on passive safety systems. It has a simplified design because the passive systems used do not require safety-grade support systems. There is reduction in the number of tests, inspections and maintenance due to few components. Active non-safety related systems ensure reliability in normal operation. Majority of the systems are based on proven design in AP600.

Table 4: Safety systems of AP1000

System	Function
Passive core cooling system	Ensure core residual heat removal, safety injection & depressurization. Provide RCS heat removal, injection, and boration thereby protecting against plant transient and RCS leaks and ruptures. Provide emergency core cooling in the event of LOCA resulting from a break in RCS. Injection of borated water to shut down the reactor or to compensate for reactivity increase caused by cooldown transients.
Passive residual heat removal system	Remove heat from the core and RCS during plant cooldown and refueling operations.
Passive containment cooling system	Cool the containment following an accident to reduce pressure such that the design pressure limit is not exceeded. Provide safety-related ultimate heat sink for the plant.
Containment isolation system	Ensure high reliability of the containment.

In-vessel retention of molten core debris	Retain molten corium in the reactor vessel in case of core meltdown.
Main control room emergency habitability system	Provide fresh air, cooling, and filtration for the main control room following an accident. Isolate the normal ventilation path for the control room and initiate pressurization upon receipt of high radiation signal.

5.3 APR1400

The safety systems are a combination of active and passive systems.

Table 5: Safety systems of APR1400

System	Function
Safety injection system	Injection of core cooling water into the reactor vessel. Injection of borated water for reactor shutdown purposes.
Safety injection tank (with fluid device)	Acts as a source of water for safety injection. The fluid device ensures effective use of the water in safety injection tank.
Shutdown cooling system	Reduce the RCS temperature from the hot shutdown operating temperature to the refueling temperature.
Auxiliary feedwater supply system	Supply feedwater to the steam generators for heat removal from the RCS for events in which the main feedwater systems are unavailable.
Cavity flooding system	Prevent direct containment heating by core debris by convoluting the flow path of the reactor cavity.
External reactor vessel cooling system	Retain molten corium under severe accident conditions.
Safety depressurization and vent system	Depressurize the RCS in the event that pressurizer spray is unavailable during plant cooldown.
Containment spray system	Reduce the containment temperature and pressure in case of accidents in the containment.
Hydrogen mitigation system	Accommodate hydrogen production from 100% fuel clad metal-water reaction and limit the average hydrogen concentration in containment to 10% during accident conditions.
Emergency containment spray backup system	Reduce the containment temperature and pressure during severe accidents by using the spray water supplied from the temporary water source.

5. Conclusion

DiD is an essential concept that should be applied at all stages of the nuclear power plant. Safety functions are met by use of active and passive systems. AP1000 uses more passive systems to achieve fundamental safety functions as compared to APR1400 and VVER-1200, which mainly depend on active systems. Active systems ensure prompt action while passive systems ensure reliable action thus it is better to use both.

In conclusion, all the three reactor types meet the fundamental safety principles with fulfilment of DiD concept and safety functions. Even though the passive safety systems are more reliable, further evaluation of the performance and reliability of the system such as understanding of physical phenomena and dynamic reliability are necessary.

REFERENCES

[1] IAEA, "Status report 107 - VVER-1200 (V-392M) (VVER-1200 (V-392M))," IAEA NPTDS, Vienna, 2011.
[2] IAEA, "Status report 81 - Advanced Passive PWR (AP 1000)," IAEA NPTDS, Vienna, 2011.
[3] IAEA, "Status report 83 - Advanced Power Reactor (APR1400)," IAEA NPTDS, Vienna, 2011.
[4] IAEA, Safety of Nuclear Power Plants: Design, Vienna: International Atomic Energy Agency, 2016.