A Comparative Study of Safety Systems from Selected Advanced Nuclear Reactors

Anselm Niwemuhwezi
Department of Nuclear & Quantum Engineering,
Korea Advanced Institute of Science & Technology (KAIST)

Sukho Lee
International Nuclear Safety School,
Korea Institute of Nuclear Safety (KINS)

PO1C01

Abstract

- 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 levels of defense in depth, ways of achieving the objectives of these levels and application of this principle in NPP design are discussed.
- The selected reactors are all pressurized water reactors (PWRs); AP1000 and VVER-1200 (model: V-392M) are generation III+ PWRs whereas APR1400 is a generation III PWR.
- Most of the safety systems (for example; ECCS, RHRS & CSS) in these three reactors were found to be comparable. However their configurations and individual functions differ.
- AP1000 uses more passive safety features that rely more on natural forces such as gravity and natural convection as compared to other reactors.
- Passive safety systems are considered more reliable compared to active systems. However, further evaluation of their performance and reliability is necessary.

	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

Objective & scope of the study

- To compare safety systems of VVER-1200, AP1000 and APR1400 reactors necessary for achieving fundamental safety functions.
- To show how the concept of defense-in-depth (DiD) is applied in the design and operation of the selected reactors. This comparison will be useful for safety evaluation of the selected designs especially to newcomer countries who plan to utilize nuclear energy for the generation of electricity.
- 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 the system's ability to execute its intended function.

Fundamental safety principles

There are three fundamental safety functions that is; control of reactivity, removal of decay heat and confinement of radioactive materials. These safety functions must be accomplished to ensure safety of the facility or installation at all conditions; that is normal plant operation, anticipated operational occurrences and accident conditions.

Application of defense in depth principle

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 procedures and operation by well qualified and 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.

Safety systems in selected designs

- A safety system is a system important to safety provided to ensure safe shutdown of the reactor, removal of residual heat from the core, or to limit the consequences of AOO and DBA. They consist of protection systems, safety actuation systems and safety system support features. 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.
- Passive systems do not depend on external input to function; they depend on changes 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.

VVER-1200

System	Function
Emergency core cooling system (active & passive) • Emergency injection system (Low & High pressure) • Emergency boron injection system	Cool down the reactor in case of loss of coolant accident (LOCA). Supply boric acid solution to the reactor coolant system in case of LOCA 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 decay heat removal system	Remove residual/decay heat and cool down the plant during normal shutdown, in the event of anticipated operational occurrences and DBA.
Overpressure protection system • Primary & Secondary	Protect the primary side equipment and pipelines from excessive pressure under DBA and BDBA conditions. Prevent over pressurization in steam generators and main steam lines.
Containment Spray system	Reduce pressure and temperature inside the containment in case of LOCA
Containment isolation system	Isolate pipes and structures in order to prevent release of fission products to the environment
Steam generator emergency cooldown system	Remove residual heat from the core and cools down the reactor via the secondary side.
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.

AP1000

System	Function
Passive core cooling system • Passive safety injection & depressurization	Ensure core residual heat removal, safety injection & depressurization.
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.

APR1400

System	Function
Emergency core cooling system • Safety injection system • Safety injection tank (with fluid device)	Injection of core cooling water into the reactor vessel. Injection of borated water for reactor shutdown purposes. SIT 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 hot shutdown operating temperature to the refueling temperature.
Containment spray system	Reduce the containment temperature and pressure in case of accidents in the containment.
Safety depressurization and vent system	Depressurize the RCS in event that the pressurizer spray is unavailable during plant cooldown.
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.

Conclusion

- Most of the safety systems in the selected designs are similar. Examples are ECCS, RHRS(SCS) and Containment spray/isolation system. However, the configuration and functioning of these systems differ.
- All the three reactor types meet the fundamental safety principles with fulfilment of DiD concept and safety functions.
- 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.
- 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," IAEA, Vienna, 2016.