Addressing the fundamental issues in reliability evaluation of passive safety of AP1000 for a comparison with active safety of PWR

HASHIM Muhammad, YOSHIKAWA Hidekazu, and YANG Ming

College of Nuclear Science and Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001, Heilongjiang, P.R. China (hashimsajid@yahoo.com, yosikawa@kib.biglobe.ne.jp, myang.heu@gmail.com)

Abstract: Passive safety systems adopted in advanced Pressurized Water Reactor (PWR), such as AP1000 and EPR, should attain higher reliability than the existing active safety systems of the conventional PWR. The objective of this study is to discuss the fundamental issues relating to the reliability evaluation of AP1000 passive safety systems for a comparison with the active safety systems of conventional PWR, based on several aspects. First, comparisons between conventional PWR and AP1000 are made from the both aspects of safety design and cost reduction. The main differences between these PWR plants exist in the configurations of safety systems: AP1000 employs the passive safety system while reducing the number of active systems. Second, the safety of AP1000 is discussed from the aspect of severe accident prevention in the event of large break loss of coolant accidents (LOCA). Third, detailed fundamental issues on reliability evaluation of AP1000 passive safety systems are discussed qualitatively by using single loop models of safety systems of both PWRs plants. Lastly, methodology to conduct quantitative estimation of dynamic reliability for AP1000 passive safety systems in LOCA condition is discussed, in order to evaluate the reliability of AP1000 in future by a success-path-based reliability analysis method (*i.e.*, GO-FLOW).

Keywords: passive safety systems; active safety systems; AP1000; large break LOCA; GO-FLOW

1 Introduction

Reliability evaluation of passive safety systems of advanced nuclear power plants will be an important subject, as the construction of several advanced Pressurized Water Reactors (PWRs) such as AP1000 and European Pressurized Reactor (EPR) have been progressing around the world. The AP1000 employs the passive safety systems while reducing the number of active safety systems, in order to provide significant improvement in plant safety design, simplification, cost reduction, *etc*. [1 - 3]. According to the definition by International Atomic Energy Agency (IAEA), a passive component does not require any external input or energy to operate, and only relies on natural physical laws (gravity, natural convection, conduction, *etc*.) [4, 5].

The passive system concept employed in AP1000 aims at attaining a higher reliability than that of the active systems of conventional PWR, by decreasing possible opportunities of hardware failures and human errors. However, both functional and economic comparison should be made of active versus passive safety systems in order to accomplish the same mission successfully, although it is said that the advantages of passive safety systems are as follows: (i) no external power supply (no loss of the power accidents), (ii) minor human intervention (minor human error), (iii) better impression for public acceptance due to the presence of “natural forces” and (iv) less complex system, *i.e.* more favorable in economic competitiveness than active systems [6]. In spite of these, there have been no detailed comparisons between both safety system concepts, judging from the aspect of reliability comparison when big accidents happen in the plant. Therefore, it is important to make reliability analysis of AP1000 passive safety systems to compare with that of active safety systems of conventional PWR.

The objective of the present study is to discuss the fundamental issues on reliability evaluation of AP1000 passive safety systems to be compared with active safety systems of conventional PWR, prior to applying success tree-based system reliability analysis tool called GO–FLOW [7] for a relative comparison. Here, the fundamental questions the authors of this

Received date: July 7, 2013
(Revised date: July 25, 2013)

paper have in mind are: Is indeed such a passive system concept more reliable than active system in the event of a big accident? How should the reliability of passive safety systems of AP1000 be properly evaluated? What will be compared with the conventional active safety systems of PWR?

In what follows, a comparison is made in Chapter 2 between conventional PWR and AP1000 to show where the main differences exist in the configuration of safety systems of both PWRs. In Chapter 3, the safety of AP1000 is discussed from the prevention of severe accident in the event of loss of coolant accident (LOCA). In Chapters 4 and 5, detailed fundamental issues of reliability evaluation of AP1000's passive safety systems are discussed qualitatively by using single loop model assumptions of both plant systems. Finally in Chapter 6, the necessary information of how to conduct quantitative estimation of dynamic reliability of AP1000 passive safety systems are introduced to evaluate the reliability of AP1000 by GO-FLOW, which is the authors' further study.

2 Comparison of AP1000 and conventional PWR plants

2.1 Passive safety design of AP1000 from the cost reduction aspect

The major difference between AP1000 and conventional PWRs is that AP1000 utilizes passive means for safety systems to ensure its safety in the event of accident, while conventional PWRs rely on activation of various systems such as pump, fans, diesels, chillers, or other rotating machinery [8, 9]. The AP1000 design includes advanced features for plant simplifications in construction, operation, and maintenance of the plant [10]. The use of passive safety system eliminates many safety-related active components such as pumps, valves, *etc*., and their associated buildings. These result in great simplifications in procurement, start-up and normal power operation, including in-service inspection/ testing, maintenance, digital instrumentation and control systems. Significant design simplifications together with the reduction of piping, cabling, pumps, valves and seismic grade building size will contribute to reduction in investment cost. The passive safety systems have one-third the quantity of remote valves as typical active safety systems, and they contain no safety-grade pumps [11].

There are 60% fewer valves, 75% less piping, 80% less control cables, 35% fewer pumps, and 50% less seismic building volume than in a conventional reactor [12]. These quantitative simplifications of AP1000 are given in Table 1. However, the deviations of the natural forces or physical principles upon which they rely on to work, can impair the system performance expected for accident prevention and mitigation [13, 14]. It is said that passive components have comparatively less failure rate than active components, due to redundancy/diversity of safety components and avoidance of external electrical power.

Table 1 AP1000 quantitative simplifications

Components	1000 MW (PWR)	AP1000	Reduction
Safety valves	2844	1400	51%
Pumps	280	184	34%
Safety piping	33528 m	5791.2 m	83%
Cables	2773680 m	365760 m	87%
Seismic building volume	359624 m^3	158574 m^3	56%

Owing to these effects, AP1000 may lead to cost reduction by decreasing the AC power sources. It is however necessary to confirm the expectation by the reliability evaluation of AP1000 passive safety systems to be compared with conventional PWR active safety systems. Nonetheless before embarking on reliability evaluation, it is important to summarize the main differences existing in the configurations of safety systems of both PWR plants.

2.2 Differences between the safety systems of AP1000 and conventional PWR

AP1000 passive safety systems mainly consist of passive core cooling system (PXS) and passive containment cooling system (PCCS), while emergency core cooling system (ECCS) and containment spray system (CSS) comprise the conventional PWR. The active safety systems (ECCS and CSS) of the conventional PWR shown in Fig. 1 are mutually dependent systems due to the common share of borated water and electricity. Conversely, the passive safety systems (PXS and PCCS) of AP1000 are independent from each other due to different water resources and functional mechanism. Table 2 shows the

Table 2 Comparison of the safety systems between AP1000 and conventional PWR

Conventional PWR		AP1000	
Safety systems	Subsystems	Safety systems	Subsystems
Emergency core cooling system (ECCS)	Accumulator injection system (AIS) (it uses check valves and normally open motor operated valves (MOVs)) High Pressure Injection System (HPIS) (it uses MOVs, High Pressures Injection Pumps (HPIP)) Low pressure injection system (LPIS) (it uses residual heat removal pumps (RHRPs), Residual heat removal heat exchanger (RHR-HX) and MOVs)	Passive core cooling system (PXS)	Passive safety injection system (PSIS) Accumulators injection system Core make up tanks injection system In-containment refueling water storage tank (IRWST) gravity injection system Recirculation sump injection system
			Four stages automatic depressurization system (ADS)
			Passive residual heat removal system (PRHRS)
Containment spray System (CSS)	Subsystems	Passive containment cooling system (PCCS)	Subsystems
	Redundancy of two parallel lines with pump circulation (it uses containment spray pump (CSP), Containment spray heat exchanger (CSHEX) and MOVs)		Redundancy of three parallel lines from Passive containment cooling water storage tank (PCCWST) and function due to natural circulation of air and internal condensation
Water resources for ECCS charging and CSS spray both for injection and recirculation phase in LOCA: accumulator tanks, RWST, and containment recirculation sump (CRS)		Water resources for PXS charging and recirculation phase in LOCA: accumulator tanks, core makeup tanks (CMTs) , IRWST, recirculation sump screens and for PCCS is PCCWST	

comparison of both systems. The PXS and ECCS systems are composed of further subsystems with their respective active and passive components used in these subsystems [15]. The PWR safety injection systems drive the borated water through the pump, and the pump injects the water into the primary system to maintain core coolant in the event of a loss of coolant accident (LOCA). Such pump-driven system is termed as "active" systems, since it requires alternating current (AC) power sources for its actuation.

By contrast, the AP1000's PXS is located inside the containment, and uses staged reservoirs of borated water that are designed to discharge into the reactor vessel at various threshold state points of the primary system.

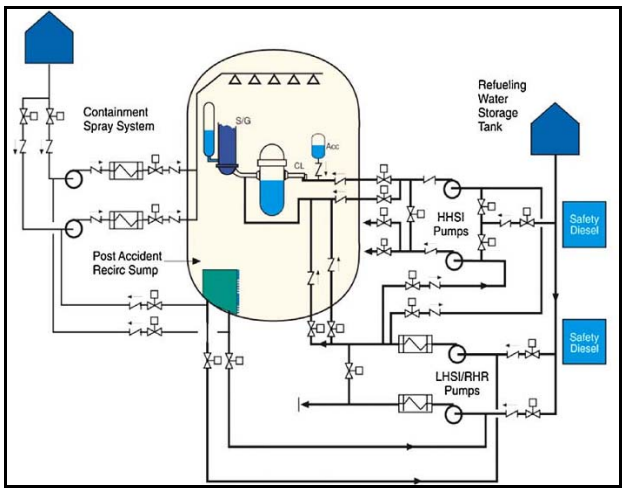

Fig.1 Active safety systems of conventional PWR.

In the configuration of PXS, there are no pumps and AC power sources; all injection systems are composed of air operated valves (AOV), squib valves, check valves, and normally open motor operated valves (MOV), and they only rely on natural forces of gravity, natural circulation, *etc*. AP1000's passive core cooling system has redundancies of additional subsystems than that of ECCS system of conventional PWR, such as two core make-up tanks (CMTs) and four stages of an automatic depressurization system (ADS) with the redundant number of passive valves. The major features of passive safety systems of AP1000 are summarized in Table 3, wherein relevant passive components which replace the active components of conventional PWR are also explained. The successful conditions of individual subsystems of PXS in accident condition are explained in subsections 2.2.1-2.2.4.

2.2.1 Passive safety injection system (PSIS)

The functions of a passive safety injection system are to provide safety injection and decay heat removal from the RCS in accident situations. The PSIS consists of the following subsystems:

(1) Two CMTs provide relatively high-flow borated water for a long duration at any pressure.

(2) Two pressurized accumulators (ACCs) provide high-flow borated water in a short time after system pressure drops below 4. 83MPa (700psia)

Table 3 Major features of passive systems used in AP1000

1. Accumulator injection system is similar to that of a conventional PWR, and uses check valves and normally opens MOV.
2. CMT injection system- Full RCS pressure, natural circulation replaces the HPIP, and uses air operated valves (AOV) and checks valves.
3. IRWST gravity injection system- Low pressure replaces LPIP, and uses squib valves, check valves and normally open motor operated valves (MOV).
4. Containment recirculation sump- gravity recirculation replaces pumped recirculation. It uses squib valves and checks valves normally open MOV.
5. Automatic RCS depressurization system- Staged controlled depressurization.
6. Stages 1-3 inject into IRWST, and stage 4 injects into containment. It uses MOV for 1 to 3 and squib valve for 4.
7. Natural circulation. Heat removal replaces auxiliary feedwater pumps, and uses AOV.
8. PCCS cool the outer surface of steel containment shell using natural circulation of air and water evaporation.
9. Ultimate heat sink is the atmosphere, and uses AOV and normally open motor operated valves

(3) IRWST provides low-flow borated water for a longer time after system pressure drops to near the containment pressure.

(4) Two containment sump screens provide the way to inject recirculation water to the primary system after the primary system is fully depressurized and the gravity head becomes great enough.

2.2.2 Automatic depressurization system (ADS)

The ADS system releases the pressure from reactor coolant system and enables safety injection (in the pressure ranges from moderately high to low) into the reactor coolant system for long-term cooling. This is accomplished by using the automatically actuated depressurization valves, which are composed of four-stage valves in series (stages 1 to 4). Each set of valves comprises two parallel paths of two valves. As shown in Fig.2, the first three stages of ADS are connected from the pressurizer steam space via the sparger to the IRWST, where the pressurizer steam is quenched to release the reactor pressure [15]. Additionally, the fourth-stage ADS releases the pressure directly into the containment atmosphere until equilibrium is reached.

2.2.3 Passive residual heat removal system (PRHRS)

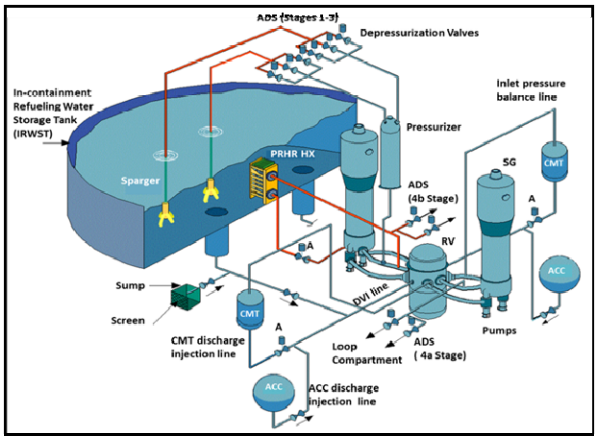

Fig. 2 AP1000 RCS and passive core cooling system.

The passive residual heat removal heat exchanger (PRHR-HX) is designed to operate without any use of active equipments. The PRHRS system depends on reliable passive components that utilize the processes of gravity effect and natural circulation [16]. The main component of PRHRS is immersed in IRWST, which acts as the heat sink. For a conventional PWR, however, the residual heat removal system is the low-pressure injection system (LPIS) which actuates only in recirculation phase of low RCS pressure. LPIS is composed of motor operated valves, residual heat removal pumps (RHRPs), and residual heat removal heat exchanger (RHR-HX).

2.2.4 AP1000 passive containment cooling system (PCCS)

The role of passive containment cooling system (PCCS) of AP1000 is different from that of the conventional PWR's CSS. (See Fig.1 for PCCS, while for CSS see Fig. 3). In the PCCS, the containment isolation function has been improved by eliminating 50% of penetrations and all of the ECCS lines that circulate highly radioactive water outside containment after LOCA accident [2]. In CSS systems, the water resources of CSS are shared mutually by ECCS due to common usage of borated water in RWST and sump. In the PCCS of AP1000, however, water resource of the PCCS is independent of PXS.

There are two modes of operation in the CSS system: injection mode from refueling water storage tank (RWST), and as a recirculation mode from sump for residual heat removal. The time point of phase change from injection to recirculation modes (in LOCA) is 1800 seconds into transient: injection phase of 0-1800 seconds and recirculation phase of 1800-3600 seconds,

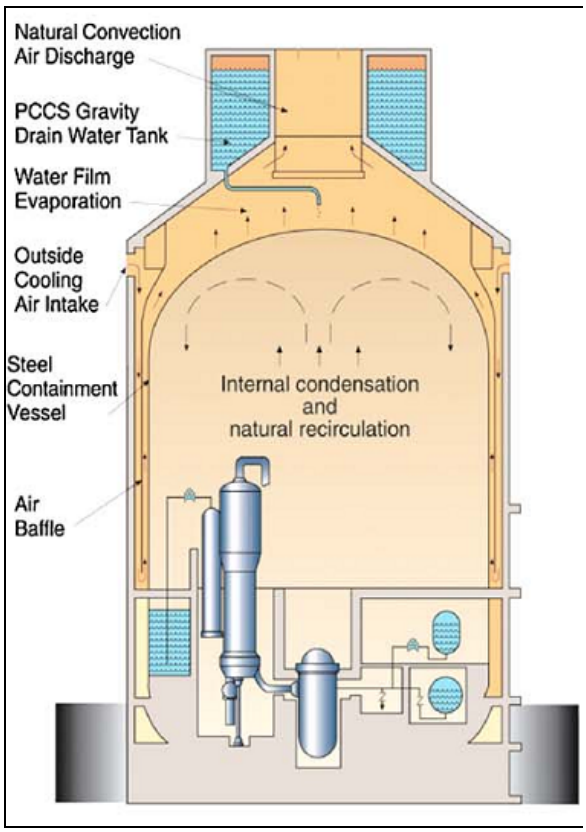

Fig. 3 Passive containment cooling system (PCCS) of AP1000.

respectively. The CSS system decreases the containment pressure and wash-out radioactive inorganic iodine into the containment sump. It consists of active components such as containment spray pumps (CSP), and many motor-operated valves (see Table 2), all of which need power sources for their actuation. On the other hand, the major components of PCCS are passive components such as AOVs, their functions of which are achieved by using (i) battery-powered valve actuation, (ii) compressed gasses (nitrogen, air), (iii) condensation, and (iv) natural circulation/evaporation.

The primary objective of a PCCS is to reduce the containment temperature and pressure following the LOCA, so that the design pressure does not exceed 59 psig (~0.40MPa). It can also provide the ultimate heat sink in an accident condition. The steel containment vessel provides heat transfer surface that removes heat from inside containment and transfers it to the atmosphere for 72 hours. Heat is removed from the containment vessel by continuous natural circulation of air. During an accident, air cooling is supplemented by water evaporation and water drains by gravity from PCCWST, which is located on top of the containment shield building.

3 Safety of AP1000 from the aspects of preventing severe accidents

AP1000 is anticipated to achieve a higher safety performance against severe accidents than the conventional PWR, owing to the fact that both prevention and mitigation measures for severe accidents have been addressed during the design stage [17, 18]. The passive systems are dedicated to mitigation of severe accident phenomena, and this approach is applicable to core cooling, containment cooling, spent fuel cooling, control room habitability, and the electric power supply for instrument and control systems (I & C). The simplification of plant systems greatly reduces the operator actions required for the management of a severe accident. The passive plant is expected to maintain safe shutdown for 72 hours without operator action and both non safety-related onsite and offsite power, which is sufficient enough than that of a conventional PWR plant (30 minutes).

The mitigation of severe accident phenomena in the event of loss of coolant accident (LOCA) is addressed in AP1000 by the following ways:

(1) In-vessel retention (IVR) provides reliable means of cooling damaged core, and external reactor vessel cooling also prevents vessel failure. The tests and analysis of IVR were reviewed by the United States nuclear regulatory commission (U.S. NRC) [19].
(2) High pressure core melt sequences are eliminated by highly redundant and diverse ADS passive systems.
(3) Hydrogen detonation will be prevented by hydrogen igniters and passive autocatalytic recombiners.
(4) Steam explosions will be also prevented by the introduction of IVR.
(5) Core concrete interaction will be eliminated by IVR.

In-vessel retention of a molten core is the key feature of AP1000, which provides a robust and reliable means of preventing a molten core from breaching the reactor vessel. The reactor vessel has no penetrations in the bottom head, and cooling water from the large IRWST can be used to flood the reactor cavity and cool the outside of the reactor vessel. The reactor vessel insulation forms an annulus that allows cooling water

to directly contact the vessel. Vents are provided for steam to escape the annulus, and therefore vented steam will condense on the containment walls and be directed back to the cavity.

Passive system reduces significantly risk contribution from the loss of offsite power (LOOP) and station blackout (SBO) events. In addition, the AP1000 design eliminates several important contributions to risk for operating Nuclear power plant (NPP) as well as the risks associated with failure of support systems (*e.g.* AC power and component cooling) and failure of active components (*e.g.* pumps and diesel generators) to start and run [20]. However, those aspects of severe accident preparedness of AP1000 for various situations other than LOCA are not treated in this paper.

4 Fundamental issues to be considered for reliability evaluation of AP1000

In this chapter, several fundamental issues will be introduced for the reliability evaluation of AP1000 passive safety systems in order to address the fundamental question: Is such a passive system concept certainly more reliable than the active system in the event of LOCA accident?

4.1 How to properly evaluate the reliability of passive safety systems of AP1000

A fundamental issue concerns the assessment of the reliability of passive safety systems of AP1000, where the probability of failure of various passive mechanisms such as gravity, natural circulation, *etc.* upon which the successful functioning of these systems is dependent. Generally, the reliability of passive systems could be gauged from two main aspects: (i) Reliability of systems/components (*e.g.* piping, valves, and pump), and (ii) Reliability of realizing and maintaining the requested physical phenomena (natural circulation stability, condensation, heat removal from boundary conditions, *etc*).

The first aspect is akin to that of the active safety system. The second aspect, however, depends on the surrounding conditions and thermal hydraulic parameters (gravity, density, temperature/pressure, flow rate and heat transfer, *etc*). Therefore, reliability assessment of passive safety components depends on the two types of failure modes, which may arise not only (i) by structural failure and physical degradation (Type A failure), but also (ii) by curbing of intended natural phenomena that can challenge and impair the passive safety principles of either natural laws or inherent characteristics (Type B failure).

The identifications of these two types A and B of failure modes concern both mechanical components (valve, piping, heat exchanger) and natural phenomena (mainly sustainability of natural circulation in the flow passage), as “virtual” component (phenomenological). The factors leading to disturbance of passive safety systems of AP1000 are thought to be caused by (i) unexpected mechanical and thermal loads which challenge the primary boundary integrity, (ii) HX plugging, (iii) mechanical component malfunction (*i.e.* drain valve), (iv) non-condensable gas build-up, (v) heat exchange process, reduction of heat by surface oxidation, thermal stratification, piping layout, thermal insulation degradation, *etc*.

In addition, failure mechanisms or critical parameters which can impair or hinder the natural circulation are thought to be as follows: (i) existence of non-condensable gas (non-condensable gas fraction), (ii) undetected leakage (crack size or leak rate), (iii) partially opened valve (POV) in the discharge line, (iv) heat loss, (v) piping inclination, and (vi) plugged pipes in HX. Each of these failure modes driving parameters is examined to determine the expected failure probability of passive safety systems by defining the range and the probability distribution function pertaining to the parameter.

4.2 Comparisons with the conventional active safety systems of PWR?

A second issue is related to the comparison of reliability results of both PWR plant systems. For this, it is necessary to make reliability analysis of the respective target safety systems of both plants under the same accident conditions, and by using the same methodology of analysis. To discuss these fundamental issues pertaining to the reliability evaluation of the passive safety system of AP1000, the single loop modeling of safety systems for both PWR plants (AP1000 and conventional PWR) are introduced in the following chapter.

5 Single loop modeling of safety system of AP1000 plant

5.1 Summary of reliability evaluation for conventional PWR's safety system

A summary of the reliability evaluation of the active safety system of a conventional PWR will be given prior to embarking on the main subject of this chapter. The dynamic reliability evaluation of the active safety systems (ECCS and CSS) of conventional PWR has been conducted by using GO-FLOW. The attained results were presented in the author's previous papers [21 - 24]. Here, the reliability evaluation of active safety systems of conventional PWR is summarized, by employing a single loop model of PWR's active safety systems comprising both ECCS and CSS as shown in Fig.4. Large break (LB) LOCA was assumed as an initiating event in the cold leg of the target PWR plant, and reliability analysis was conducted based on the assumption that all the electric power sources (alternating current (AC) and direct current (DC)) are maintained during the accident.

The water resources for ECCS charging, CSS spray and their recirculation mode operation are shared by both the ECCS and CSS. In addition, some of the components for both ECCS and CSS line-up are also commonly used. Therefore, ECCS and CSS systems are considered to be mutually dependent systems.

The transient behavior of the damaged plant by LBLOCA is assumed to follow the successful sequence of (i) reactor shutdown, (ii) ECCS charging with containment spraying prior to the complete loss of water resources, and (iii) water recirculation mode of both ECCS and CSS until the time of reactor should be at hot stand-by condition or until a stable cool-down state. There are two different modes (or "phased missions") of this active safety system: water injection mode and water recirculation mode. The first phased mission period for injection phase is 0-1800 seconds while that for recirculation phase 1800-3600 seconds, to maintain the water continuously into the reactor vessel in order to remove the decay heat after LBLOCA accident in the cold leg.

5.2 Configuration of single loop model of passive safety systems of AP1000

In the case of AP1000, the same GO-FLOW analysis should be conducted for a single loop model of passive safety systems, in order to evaluate the dynamic reliability of AP1000 plant under the same accident conditions and assumptions. The single loop model of passive safety system of AP1000 comprising passive core cooling system (PXS) and passive containment cooling system (PCCS) is illustrated in Figs. 5 and 6. Figures 5 and 6 can be compared with

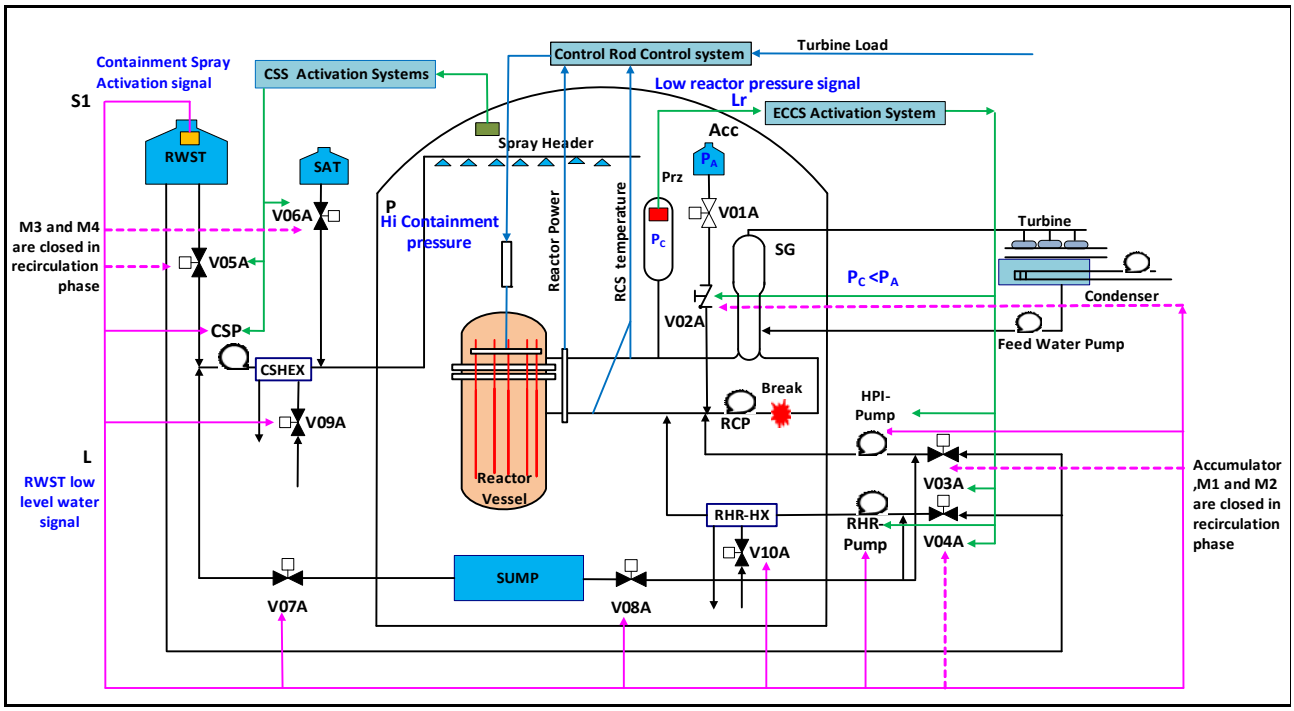

Fig. 4 Single loop model of active safety system of conventional PWR.

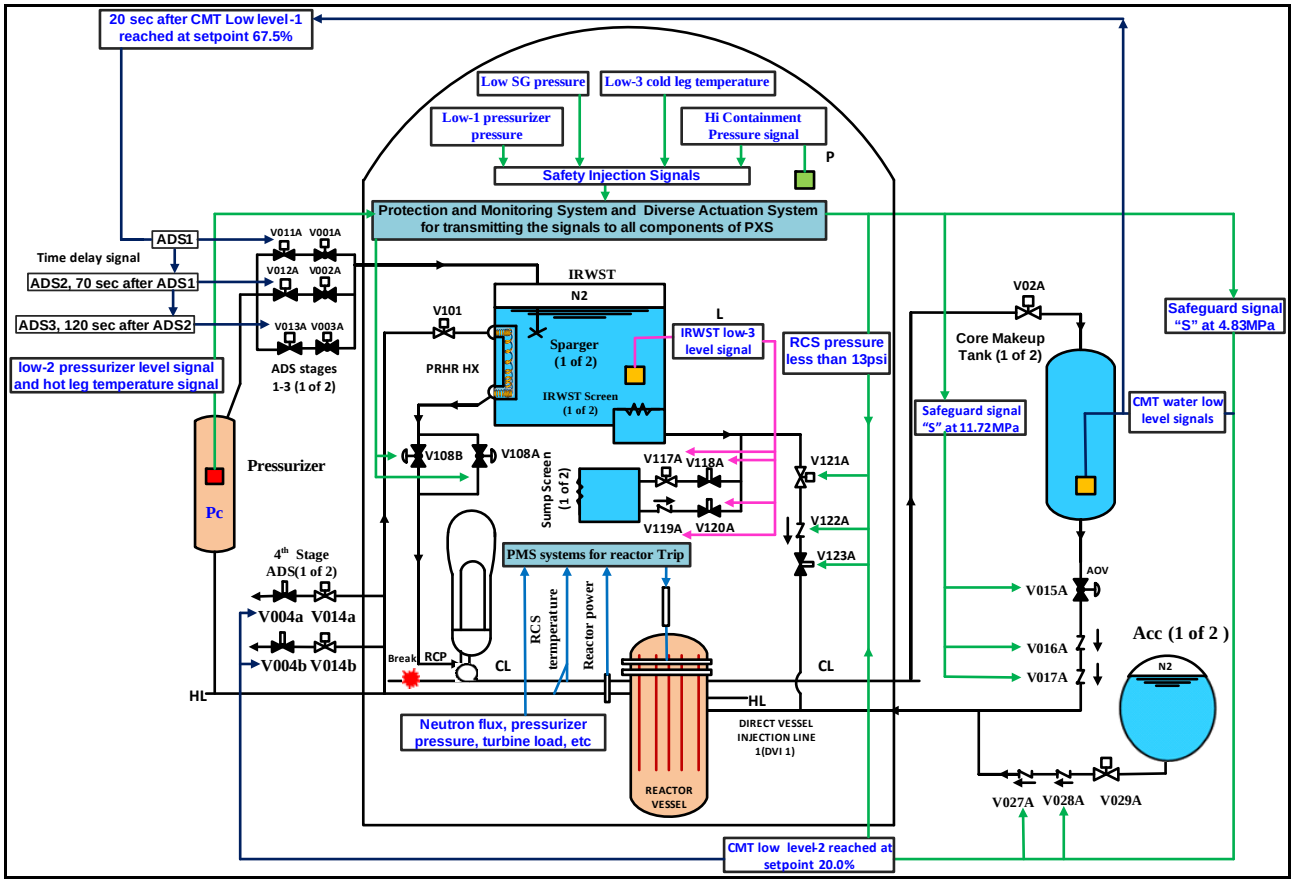

Fig. 5 Single loop model of AP1000 Passive Safety System.

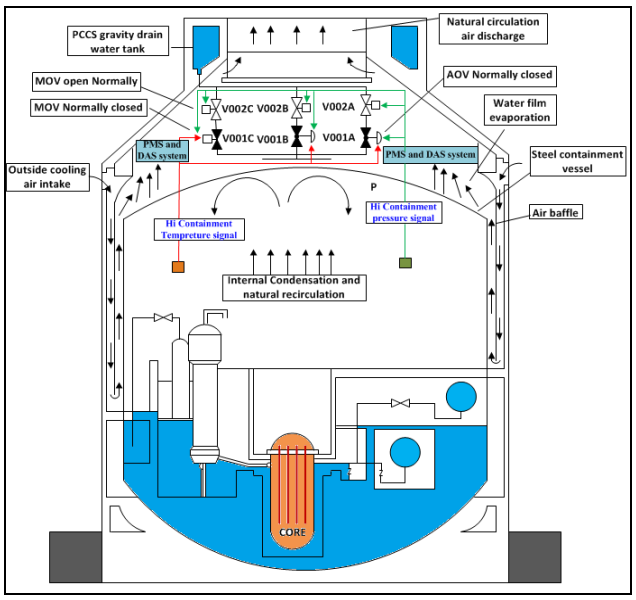

Fig.6 AP1000 passive containment cooling system.

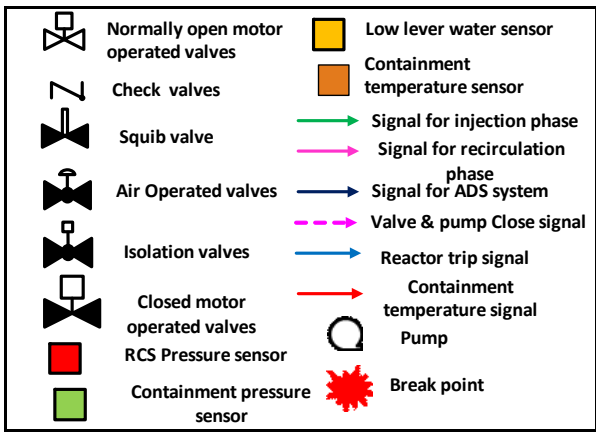

Fig.7 Components symbols used in both safety system.

the single loop model of emergency core cooling system (ECCS) and containment spray system (CSS) of PWR, as shown in Fig.4. The different component's symbols used in these single loop models of both safety systems are shown in Fig. 7.

The passive safety systems (PXS and PCS) can be treated separately for reliability analysis by GO-FLOW. The configuration of PXS includes four functions of (i) reactor shutdown system (reactor protection system (RPS)), (ii) single train of all passive safety injection system (PSIS), (iii) passive residual heat removal system (PRHRS), and (iv) automatic depressurization systems (ADS). PCS consists of three parallel lines from the passive containment cooling water storage tank (PCCWST) with air operated valves (AOV), normally motor

operated valves (MOV) and steel containment surface. For instruments and control systems in AP1000, all actuation signals for passive safety systems (PXS and PCS) are transmitted automatically by protection and safety monitoring system (PMS) or diverse actuation system (DAS) to the relevant actuating components of RPS, PXS and PCS, as shown in Figs. 5 and 6. These actuation signals can also be transmitted through manually actuation system by operator action in the case of failure of PMS and DAS systems.

There are five independent water resources: IRWST, recirculation sump, accumulator tank, and CMT for PXS, while PCCWST for PCS system. The volume of the water resources should be sufficient to cool the reactor and reduce the containment temperature until the time when reactor attains cold standby or hot standby condition.

The function and behavior of passive safety systems are also considered under the same accident condition of LBLOCA caused by internal factors such as rapid crack propagation. Although important, no assumption of LBLOCA occurrence is considered for the external event such as big earthquake, explosion, and so on. The transient behavior of a damaged plant by LBLOCA is assumed to be a successful sequence of (i) reactor shutdown systems, (ii) passive core cooling system and (iii) passive containment cooling system as shown in Figs.8 and 9.

The AP1000 PXS has different phases during the LBLOCA, and phased mission time for the phases of PXS is longer than that of ECCS systems of PWR. Similarly, passive containment cooling system provides cooling to the containment shell for 72 hours for long-term cooling, which is larger than that taken for a containment spray system of PWR (*i.e.* 3600 seconds). PCS system actuates from blow-down phase to long-term cooling phase (*viz.*, 30 seconds to 72 hours).

5.3 Chronology of LBLOCA of AP1000

In the case of AP1000 plant, LBLOCA transient can be characterized by six distinct phases according to the functions and behaviors of PXS and PCS systems in the respective phases, with respect to change in reactor pressure condition and temperature with the passage of time after the LOCA occurred. These phases are: (i) blow-down phase, (ii) refill phase, (iii) reflooding phase, (iv) ADS blow-down phase, (v) IRWST gravity injection phase, and (vi) recirculation sump injection phase for long-term cooling.

Details of LOCA chronology are elaborated in Table 4, where a sequence of all phases of PXS during the LBLOCA are illustrated with actuation signals and time of relevant used components of PXS during LOCA phases. The time and components used for PCS system are given in the last two rows of Table 4.

The transient behaviors of PXS and PCS during LOCA are illustrated in Figs.8 and 9, respectively, by using charts time versus pressure, where the actuation time of various components of PXS and PCS are indicated (note that reactor coolant system (RCS) pressure in Fig. 8, while containment pressure in Fig. 9). In Fig.8, state of components such as “start", “stop” and “empty” are illustrated by different dots and the time intervals. From Fig.8, it is seen that the water injection into the reactor continues until *ca*. 3600 seconds after LBLOCA occurrence and after then recirculation of water follows. It is also seen that the initial water injection stage is divided into four phases of (i) blow-down phase (0-85 seconds), (ii) refill/reflood phase (85-750 seconds), (iii) ADS blow-down phase (750-1800 seconds), (iv) IRWST gravity injection phase, before changing the mode of (v) Recirculation-sump log term cooling phase.

5.4 Prerequisite information for quantitative reliability evaluation by GO-FLOW

Quantitative dynamic reliability evaluation of the single loop passive safety system of AP1000 should start with the conductance of failure mode and effect analysis (FMEA) for LBLOCA of AP1000, and then the dynamic reliability evaluation by using GO-FLOW. This GO-FLOW reliability analysis can be conducted separately for both passive core cooling system and passive containment cooling system of AP1000 plant. The FMEA [25] provides important information such as, failure modes of all passive components, impacts on whole plant system, degree of fatality, and their pertinent parameters, which can eventually contribute to functional failure of a system. Failure data for conducting GO-FLOW reliability analysis can be

selected on the basis of failure mode of passive components of PXS and PCS systems. The failure data consist of: (i) operational failure rate per hour and (ii) failure probability per demand, similar to the case of an active safety system (Type A failure), while special consideration will be made on how to take into account for Type B failure in the passive system. The GO-FLOW quantitative reliability evaluation of passive systems will be the subject of the authors' future study.

5.5 Contribution of common cause failure (CCF) and uncertainties in the system reliability

CCF is the simultaneous failure of multiple components by the same causal factor, and has important contribution to the system reliability results.

Table 4 Sequence of events during LBLOCA in AP1000 with actuation signals of passive safety systems

Accident: Large break LOCA in the cold leg of RCS system at 0.0 sec (Reactor normal pressure 15.5 MPa (2250 psia)						
Activation Systems	Phases of LOCA (Injection and Recirculation phases)		Detecting device (sensors, Timer)	Actuation Signals of RPS, PXS and PCS	Time (sec) from LOCA	Components to be used for actuation in different phases
Reactor Protection system	Blow-down phase	Reactor scram (Rector Trip)	Pressure sensors and Temperature sensors	Hi-neutron flux, low coolant flow, over temperature. RCS 12.41 MPa, *etc*.	2.0 sec	Reactor trip switchgear breakers.
		Safeguard signal "S"		RCS 11.72 MPa	2.2 sec	Safety actuation system
		Steam generator (SG) feedwater		After trip signals	3.2 sec	Feedwater control valve close
Passive Core cooling system		CMT injection system	RCS Pressure sensor in pressurizer	Low-2 pressurizer pressure, safety injection signals, safeguard S signal at 11.72 MPa	4.2 to 85 sec	CMTs tanks, V015A, V016A, and V017A.
		PRHR system			4.2 to 3600 sec	PRHR HX, V108A/B, V101,
		Main steam isolation		After "S" signal	11.2sec	Isolation valves start to close
		RCS pumps trip		After "S" signal	12.4sec	Pump trip
	Re-fill/ Reflood Phase	Accumulator start which stop CMT injection	RCS pressure sensor	S signal at 4.83 MPa RCS pressure	85 to 450 sec	ACC Tank, V027A, V028A, and V029A.
		CMT start again after ACC empty	Certain RCS pressure value	Accumulator empty signal	450 to 2000	CMTs tanks, V015A, V016A, and V017A
	ADS blow-down Phase	ADS stage 1	CMT water level sensor	20s after 67.5% liquid volume fraction in CMT	750 to 3600 sec	ADS 1, V001A, V011A
		ADS stage 2	Time delay timers	70 s after ADS-1 actuation	820 to 3600 sec	ADS 2, V002A, V012A
		ADS stage 3	Time delay timers	120 s after ADS-2 actuation	940 to 3600 sec	ADS 3, V003A, V013A
		ADS stage 4a	Time delay timers	20.0% liquid volume fraction in CMT and 120s after ADS-3 actuation	1491 to 3600 sec	ADS 4a, V004a, V014a
		ADS stage 4b	Time delay timers	60s after ADS-4a actuation	1551 to 3600 sec	ADS 4b, V004b, V014b
	IRWST gravity injection phase	IRWST Gravity injection lines flow	RCS pressure sensor, CMT water level sensor	RCS pressure less than 89.6 KPa/13psi plus the containment pressure	1800 to 3600 sec	IRWST tank, IRWST screen1, V121A, V122A, V123A
	Recir sump long term cooling phase	Recirculation injection lines flow	IRWST low level water sensor	IRWST low-3 level signal	3600 to 7000sec	Sump, Recir Screen 1, V117A, V118A, V119A, V120A
Passive Contain-ment Cooling system	Contain-ment cooling	Natural circulation of Air with water spray	Containment's temperature and Pressure sensors	Hi-2 containment pressure signal59psig, Hi containment temperature	30 sec to 72 hours after LOCA	PCCWST, V001A/B/C, V002A/B/C

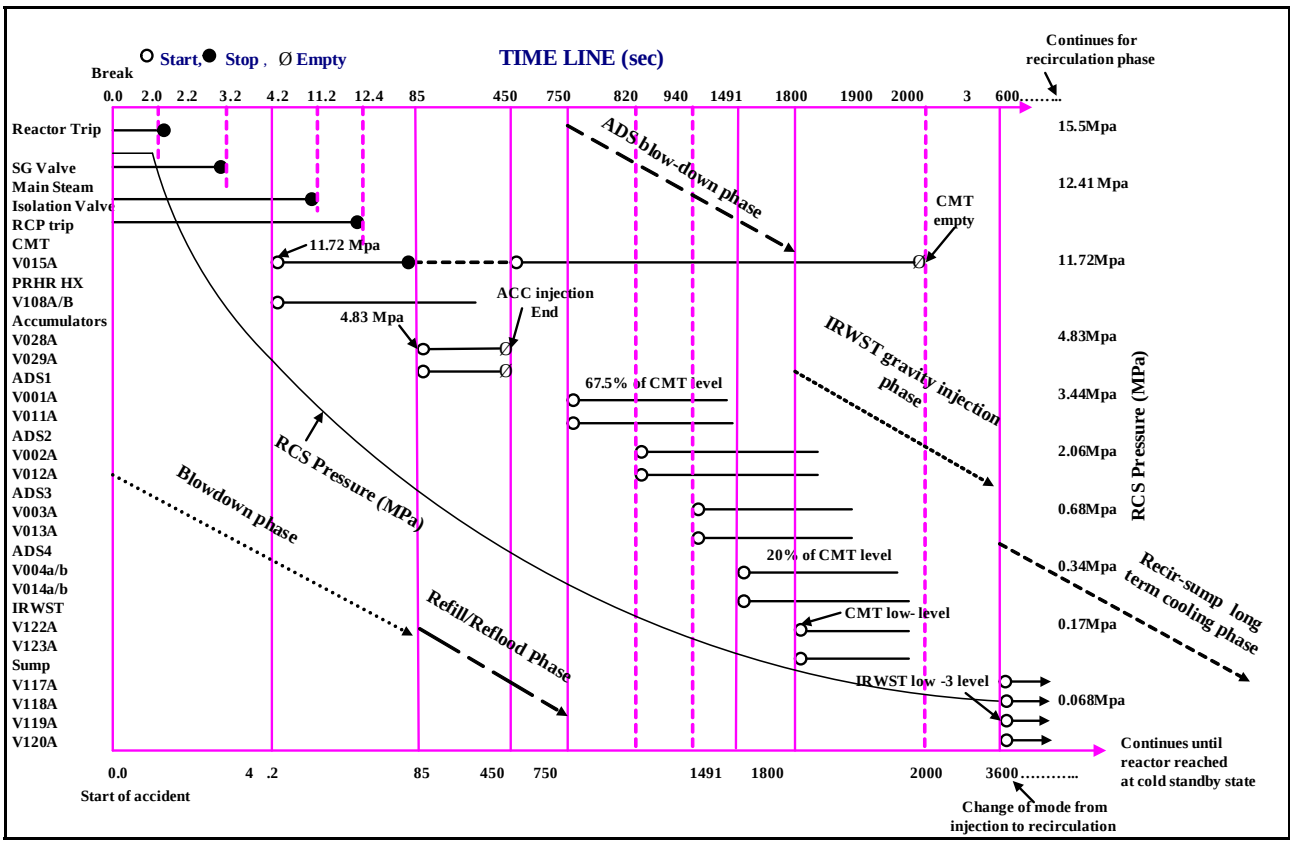

Fig. 8 Time Chart of AP1000 PXS components with reactor pressure after the LOCA.

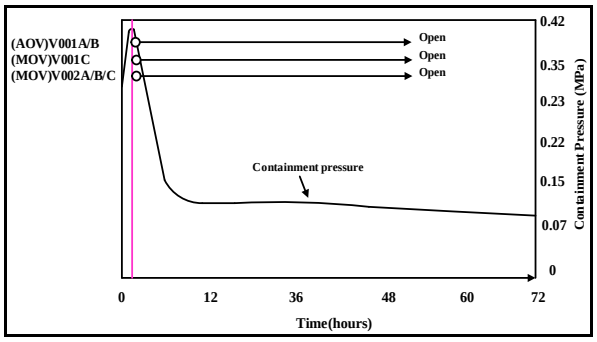

Fig. 9 Time chart of AP1000 PCS components.

Loss of electricity, or loss of water resources is a good example of CCF that causes LOCA accident. Similarly, uncertainties of the failure of passive components to compose the whole safety system affect the results of reliability of the whole system [26].

In case of passive safety system, uncertainties may arise from: (i) the deviations of the natural forces or physical principle upon which they rely on (gravity and density difference), (ii) the expected conditions due to the inception of thermal-hydraulic factors impairing the system performance, or (iii) changes of the initial and boundary conditions. Therefore, in order to obtain a more realistic and practical evaluation of the reliability of passive safety system, the CCF analysis and uncertainties analysis should be considered. These analyses conducted by GO-FLOW will be also the subject of the authors' future study.

6 Conclusion and future work

In this paper, the authors discussed on the fundamental issues on reliability evaluation of AP1000 passive safety systems. In order to discuss the issues pertaining to the reliability of passive safety systems, a comparison of passive safety systems of AP1000 and active safety systems in the conventional PWR plant has to be made to clarify what factors should be especially focused for the reliability comparison.

Towards the above-mentioned goal, firstly the physical mechanisms and functions of safety systems equipped with the AP1000 plant system and the conventional PWR were compared with each other from the aspect of prevention of severe accident phenomena in the event of loss of coolant accident. As the result, it was pointed out that (i) the main difference in the configurations of safety systems of

AP1000 to be compared with that of conventional PWR reactors is the conspicuous reduction of active components with adoption of passive elements based on physically natural mechanism, and that (ii) for the reliability assessment of passive safety components it is necessary to consider not only (i) Type A failure caused by structural failure and physical degradation but also (ii) Type B failure caused by curbing of intended natural phenomena that can challenge and impair the passive safety principles of either natural laws or inherent characteristics.

Then, the behavior of safety systems of AP1000 in the event of LBLOCA was summarized from the published safety analysis report of AP1000. For the quantitative evaluation of the reliability of passive safety system of AP1000 by GO FLOW, a single loop model of safety systems was reduced and the on-off behaviors of various components comprising the AP1000's safety systems were plotted on the pressure versus time diagrams in order to estimate the phased mission scheme of the AP1000 safety systems.

To sum up of this study, the necessary information is obtained for conducting on the quantitative dynamic reliability analysis of AP1000 passive safety system by utilizing FMEA and GO-FLOW methods. To conduct on GO FLOW analysis it is needed to assemble the proper failure data for various components of both active and passive mechanism. Finally by comparing the obtained reliability results of AP1000 with that of conventional PWR under the same LBLOCA conditions, it will be possible to discuss the reliability of AP1000. For the practical evaluation of reliability results, common cause failure analysis and uncertainties analysis will also be conducted by GO-FLOW methodology.

Acknowledgement

The authors would like to acknowledge the financial support from National Natural Science Foundation (NFSC) of China (Grand 364 No.60604036) and the 111 Project (Grand No. b08047).

References

[1] BURGAZZI, L.: Reliability of passive systems in nuclear power plants, http://dx.doi.org/10.5772/47862. (accessed August 6, 2013)

[2] SCHULZ, T. L.: Westinghouse AP1000 advanced passive plant. Nuclear Engineering and Design, 2006(236): 1547-1557.

[3] JIYONG, O.: Methods for comparative assessment of active and passive safety systems with respect to reliability, uncertainty, economy and flexibility. PhD thesis, Massachusetts Institute of Technology, 2008.

[4] IAEA: Safety related terms for advanced nuclear power plants, IAEA TEC-DOC-626, 1991.

[5] BURGAZZI, L.: IAEA-CN-164-3S08, Open issues associated with passive safety systems reliability assessment. (accessed June 3, 2013)

[6] BURGAZZI, L.: State of the art in reliability of thermal-hydraulic passive systems, Reliability Engineering and System Safety, 2007(92): 671–675.

[7] MATSUOKA, T., and KOBAYASHI, M.: GO-FLOW A new reliability analysis methodology, Nuclear Science and Engineering, 1998, 175(3): 64-78.

[8] KAMYAB, S., NEMATOLLAHI, M., KAMYAB, M., and JAFARI, A.: Evaluating the reliability of AP1000 passive core cooling systems with risk assessment tool. International MultiConference of Engineers and Computer Scientists (IMECS), 2010, Hong Kong.

[9] MATZIE, R. A.: AP1000 will meet the challenges of near-term deployment, Nuclear Engineering and Design 2008 (238): 1856–1862.

[10] PAOLO, G.: Westinghouse electric company, AP1000 the PWR revisited, IAEA-CN-164-3S05, 2013.

[11] WINTERS, J. W.: AP1000 construction schedule. Proceeding of 9th International Conference on Nuclear Engineering, (ICONE-9), 2001.

[12] BURGAZZI, L., FIORINI, G. L., MAGISTRIS, F. De., and LENSA, W. V.: Reliability assessment of passive safety systems, Proceedings of the 6th international conference on nuclear engineering, (ICONE-6), San Diego (USA), 1998.

[13] FIORINI, G. L.: Reliability methods for passive safety functions, Proceedings of the post smirt 14.

[14] WESTINGHOUSE electric company. Westinghouse AP1000 design control document revision, 2004 (14).

[15] WRIGHT, R. F.: Simulated AP1000 response to design basis small break LOCA events in APEX-1000 test facility, Nuclear Engineering and Technology, 2007, 4(39): 287–298.

[16] USNRC: Probabilistic risk assessment and severe accident evaluation for new reactors, NUREG-0800, chapter 19, 2012.

[17] SCOBEL, J. H.: Westinghouse AP1000 probabilistic risk assessment maturity. International congress on advances in nuclear power plants (ICAPP), 2005, Seoul, Korea.

[18] WESTINGHOUSE electric company. Probabilistic risk assessment chapter 19, AP1000 design control document appendix 19B, 2009.

[19] GIDDENS, J., SCHULZ, T., and LUCA, O.: AP1000 safety concepts and robustness to external hazards, Westinghouse electric company, 2012.

[20] HASHIM, M., YOSHIKAWA, H., MATSUOKA, T., and YANG, M.: Reliability monitor for PWR safety system using FMEA and GO-FLOW methodology-application of Risk Monitor for Nuclear Power Plants. 21th International conference on nuclear engineering (ICONE-21), 2013, Chengdu, China.

[21] HASHIM, M., MATSUOKA, T., YOSHIKAWA, H., and MING, Y.: Dynamical reliability analysis for ECCS of pressurized water reactor considering the large break LOCA by GO-FLOW methodology. Nuclear Safety and Simulation, 2012, 3(1): 81-90.

[22] HASHIM, M., MATSUOKA, T., and YANG, M.: Development of a reliability monitor for safety related subsystem of a PWR considering the redundancy and maintenance of components by fault tree and GO-FLOW methodologies. Nuclear Safety and Simulation, 2012, 3(2): 164-175.

[23] HASHIM, M., YOSHIKAWA, H., MATSUOKA, T., and YANG, M.: Common cause failure analysis of PWR containment spray system by GO-FLOW methodology. Nuclear Engineering and Design, 2013(262): 350-357.

[24] YOSHIKAWA, H., LIND, M., YANG, M., HASHIM, M., and ZHANG, Z.: Configuration of risk monitor system by plant defense-in-depth risk monitor and reliability monitor. Nuclear Safety and Simulation, 2012, 3(2): 140-152.

[25] DAVID, M. L.: Failure Modes and Effects Analysis, Tyco Electronics Corp,
URL: dmlittle@tycoelectronics.com.

[26] HASHIM, M., YOSHIKAWA, H., MATSUOKA, T., and YANG, M.: Considerations of uncertainties in evaluating dynamic reliability by GO-FLOW methodology–example study of reliability monitor for PWR safety system in the risk-monitor system, Journal of Nuclear Science and Technology, 2013, 50(7): 695-708.