Journal of Nuclear Science and Technology
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tnst20

Quantitative dynamic reliability evaluation of AP1000 passive safety systems by using FMEA and GO-FLOW methodology

Muhammad Hashim[a], Hidekazu Yoshikawa[a], Takeshi Matsuoka[ab] & Ming Yang[a]
[a] College of Nuclear Science and Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001 Heilongjiang, P.R. China
[b] Mechanical System Engineering, Department of Engineering Utsunomiya University, 7-1-2 Yoto, Utsunomiya City, 321-8585 Japan
Published online: 05 Feb 2014.

To cite this article: Muhammad Hashim, Hidekazu Yoshikawa, Takeshi Matsuoka & Ming Yang , Journal of Nuclear Science and Technology (2014): Quantitative dynamic reliability evaluation of AP1000 passive safety systems by using FMEA and GO-FLOW methodology, Journal of Nuclear Science and Technology, DOI: 10.1080/00223131.2014.881727

To link to this article: http://dx.doi.org/10.1080/00223131.2014.881727

Journal of Nuclear Science and Technology, 2014
http://dx.doi.org/10.1080/00223131.2014.881727

Taylor & Francis
Taylor & Francis Group

ARTICLE

Quantitative dynamic reliability evaluation of AP1000 passive safety systems by using FMEA and GO-FLOW methodology

Muhammad Hashim[a*], Hidekazu Yoshikawa[a], Takeshi Matsuoka[a,b] and Ming Yang[a,†]

[a]*College of Nuclear Science and Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001 Heilongjiang, P.R. China;* [b]*Mechanical System Engineering, Department of Engineering Utsunomiya University, 7-1-2 Yoto, Utsunomiya City, 321-8585 Japan*

(*Received 17 October 2013; accepted final version for publication 23 December 2013*)

The passive safety systems utilized in advanced pressurized water reactor (PWR) design such as AP1000 should be more reliable than that of active safety systems of conventional PWR by less possible opportunities of hardware failures and human errors (less human intervention). The objectives of present study are to evaluate the dynamic reliability of AP1000 plant in order to check the effectiveness of passive safety systems by comparing the reliability-related issues with that of active safety systems in the event of the big accidents. How should the dynamic reliability of passive safety systems properly evaluated? And then what will be the comparison of reliability results of AP1000 passive safety systems with the active safety systems of conventional PWR.

For this purpose, a single loop model of AP1000 passive core cooling system (PXS) and passive containment cooling system (PCCS) are assumed separately for quantitative reliability evaluation. The transient behaviors of these passive safety systems are taken under the large break loss-of-coolant accident in the cold leg. The analysis is made by utilizing the qualitative method failure mode and effect analysis in order to identify the potential failure mode and success-oriented reliability analysis tool called GO-FLOW for quantitative reliability evaluation. The GO-FLOW analysis has been conducted separately for PXS and PCCS systems under the same accident. The analysis results show that reliability of AP1000 passive safety systems (PXS and PCCS) is increased due to redundancies and diversity of passive safety subsystems and components, and four stages automatic depressurization system is the key subsystem for successful actuation of PXS and PCCS system. The reliability results of PCCS system of AP1000 are more reliable than that of the containment spray system of conventional PWR. And also GO-FLOW method can be utilized for reliability evaluation of passive safety systems.

Keywords: dynamic reliability analysis; passive core cooling system; passive containment cooling system; AP1000; large break LOCA; active safety system; passive safety system; failure mode and effect analysis (FMEA); GO-FLOW methodology

1. Introduction

The increased concern against severe accidents expanded the safety requirements in the current nuclear reactor design which has led to a growing adoption of passive safety systems in the advance pressurized water reactors (PWRs) such as AP1000 and European pressurized water reactor. The inclusion of passive safety-related systems in the advanced pressurized reactor (AP1000) claimed high system reliability than that of active safety systems of conventional PWR because of the less factors of hardware failures and less human errors due to decreased human–machine interaction by avoidance of external power [1,2]. According to International Atomic Energy Agency, the passive component does not need any external input or energy to operate and fully relies upon natural laws (e.g. gravity, natural circulation), inherent characteristics (internally stored energy) and dispense with active components (e.g. electromotor-driven valves and pumps) [3,4]. The AP1000 employs the passive safety systems while reducing the number of

[*]Corresponding authors. Email: hashim@hrbeu.edu.cn; yangming@hrbeu.edu.cn
[†]Present address: Mechanical System Engineering, Department of Engineering Utsunomiya University, 7-1-2 Yoto, Utsunomiya City, 321-8585 Japan.

active safety systems in order to provide significant simplification of plant safety design to reduce production cost.

The functional comparison of passive safety systems with the active safety system can be made on the basis of reliability of both plants systems to accomplish the same mission successfully. Here, the definition of "reliability" is the ability of the system to carry out its safety function under the prevailing accidental conditions when required [4]. The qualitative comparison between the safety systems of both plants, AP1000 and conventional PWR, are described in the published paper [5], where authors have discussed the fundamental issues regarding the reliability evaluation of passive safety systems to be compared with active safety systems of conventional PWR. The comparison was made from the both aspects of cost reduction and safety design, and it was noticed that main differences between both PWRs exist in the configuration of safety systems. From the author's study [5], it was mentioned that the failure of passive safety components depends on the two types of failure modes, type A failure (hardware failure) caused by structural failure and physical degradation, and type B failure (functional failure) caused by blocking of intended natural phenomena that can challenge and impair the passive safety principles of either natural laws or inherent characteristics [6]. The first step of reliability assessment of passive safety systems is the identification of all relevant failure modes [7]. Therefore, fundamental questions arise: is it sure that such passive systems concept be more reliable than the active systems in the event of the big accidents of both PWR plants? How should the reliability of AP1000 passive safety systems be evaluated by assuming both types of failure modes (types A and B)? And then what will be the comparison of reliability results of both PWRs?

Regarding these questions, the subject of this paper is to conduct the quantitative dynamic reliability evaluation of AP1000 passive safety systems by utilizing the qualitative method "failure mode and effect analysis (FMEA) in order to identify the potential failure mode" [8] and the success-oriented quantitative reliability analysis tool called GO-FLOW [9] for dynamic reliability evaluation. For this, a brief description of passive safety systems of AP1000 and two types of failure modes (types A and B) is summarized first in Sections 2 and 3, respectively, and a single loop model of AP1000 passive core cooling system (PXS) and passive containment cooling system (PCCS) depicted in Section 4 for dynamic reliability analysis. The transient behaviors of these passive safety systems are taken under the large break loss-of-coolant accident (LBLOCA) [10]. And then the discussions of FMEA and GO-FLOW analyses for PXS and PCCS system are illustrated in the subsequent Sections 4.2 and 4.3, which are conducted independently. While calculated reliability results of both safety systems are described in Section 4.4, comparison of reliability results of the PCCS of AP1000 with that of the containment spray system (CSS) of conventional PWR are presented in Section 4.5.

2. Description of AP1000 system

AP1000 is a two-loop, 3400 MWt Westinghouse-designed PWR which received final design approval by US Nuclear Regulatory Commission (NRC) in 2004 and was certified in 2006 as a Generation III + reactor [11]. AP1000 utilizes passive means for safety systems to ensure its safety in the event of the accident, while conventional PWRs rely on the external power source for the activation of various systems such as pump, fans, diesels, chillers or other rotating machinery. The use of the passive safety system eliminates many safety-related active components such as pumps, motor operated valves (MOVs), fans and their associated buildings. The brief description of AP1000 passive safety system is given in the following Sections 2.1 and 2.2.

2.1. Passive core cooling system

The schematical diagram of AP1000 passive core cooling system is shown in **Figure 1**, which consists of the following aspects [2,11].

(1) Two core makeup tanks (CMTs) provide relatively high flow borated water in a long time at any pressure. The CMT subsystem is a passive, safety-related subsystem that injects water into the reactor coolant system (RCS) if inventory is being lost. Steam is supplied to the CMT to displace the cold injection water.
(2) Two pressurized accumulators (ACCs) provide high flow borated water to the reactor vessel in a short time interval after system pressure drops below 4.83 MPa (700 psia).
(3) An in-containment refueling water storage tank (IRWST) provides low flow borated water in a longer time after system pressure drops to near the containment pressure. The function of the IRWST/gravity injection is to provide flooding of the refueling cavity for normal refueling, post-LOCA flooding of the containment to establish long-term RCS cooling, and to support the passive residual heat removal system-heat exchangers (PRHR-HXs) operation.
(4) A PRHRS with C-shape tube HX is located inside the IRWST to provide the passive energy removal through a natural circulation path connecting the pressurizer-side hot leg and the steam generator exit plenum. It consists of one PRHR-HX and associated valves, piping and instrumentation. The IRWST provides a heat sink to perform the high pressure natural coolant circulation to fulfill the core cooling function.
(5) The automatic depressurization system (ADS) consists of two trains of depressurization valves with the first three stages (1, 2, and 3) coming

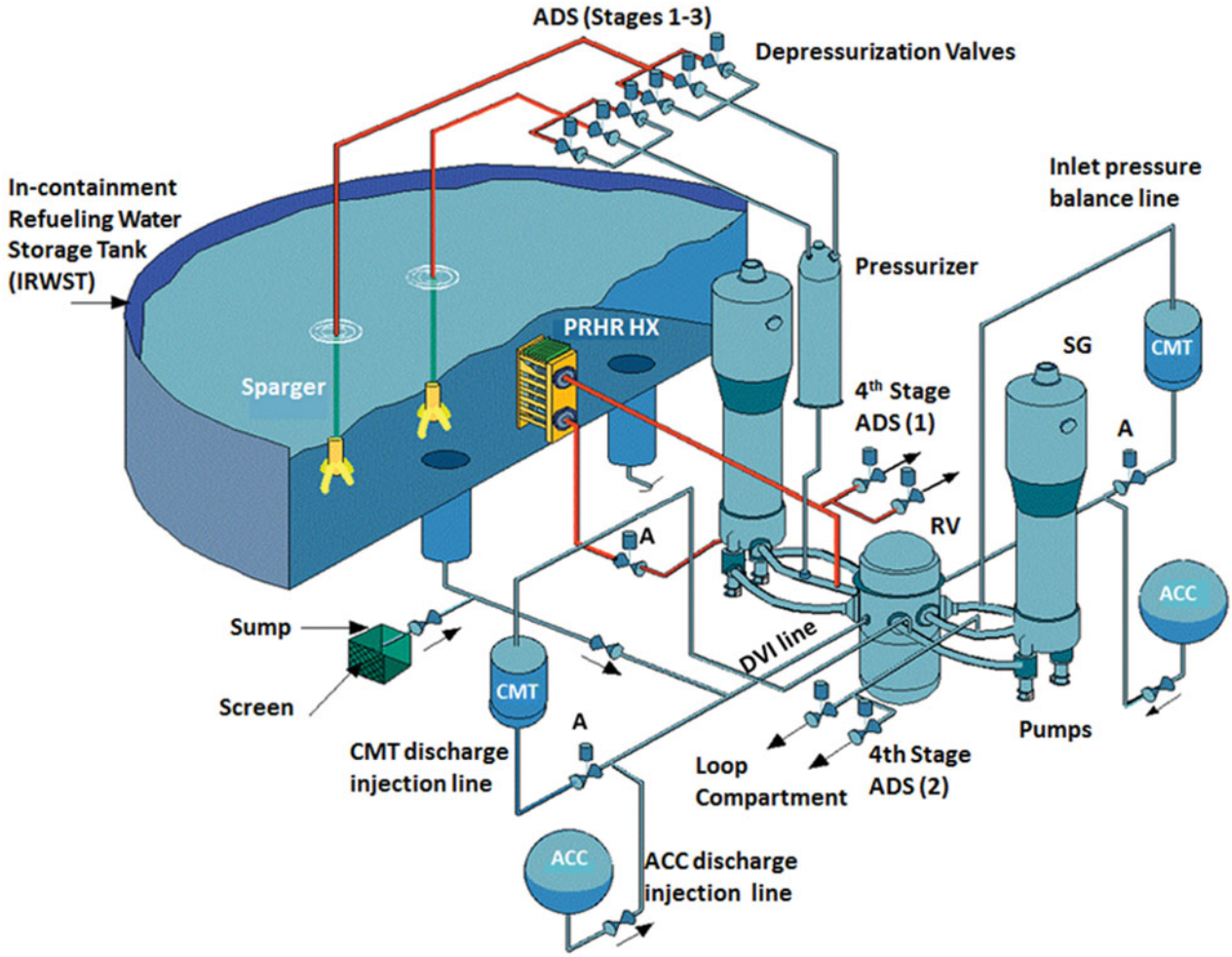

Figure 1. AP1000 RCS and passive core cooling system.

from the pressurizer and fourth-stage valves coming from hot legs [12]. Steam from the first three stages is quenched in the IRWST which acts as a heat sink. Fluid (single phase water or steam or two-phase mixture) from the fourth-stage valve is vented directly to the containment. During the LOCA, these valves open subsequently to provide a controlled depressurization rate of the primary system.

(6) A recirculation sump collects the water discharged from the primary system and steam that condenses within the containment. And it provides 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. *Passive containment cooling system*

In PCCS, the containment isolation function has been improved by eliminating the 50% of penetrations and all of the emergency core cooling system (ECCS) lines that circulate highly radioactive water outside containment after LOCA accident as shown in **Figure 2** [11]. The primary objective of PCCS is to reduce the containment temperature and pressure following the LOCA so that the design pressure does not exceed 59 psig (~0.40 MPa). It can also provide the ultimate heat sink in 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 the PCCS gravity drain water tank located on top of the containment shield building.

3. Hardware failures and functional failures for AP1000 passive safety system (type A and B)

The reliability assessment of passive systems requires a basic step to identify the all relevant potential failure modes of passive safety components that affect the system, and their consequences associated with passive system operation. The reliability assessment of AP1000 passive safety components depend on two types of failure modes, that is, type A failure caused by structural failure (hardware failure), physical degradation, and

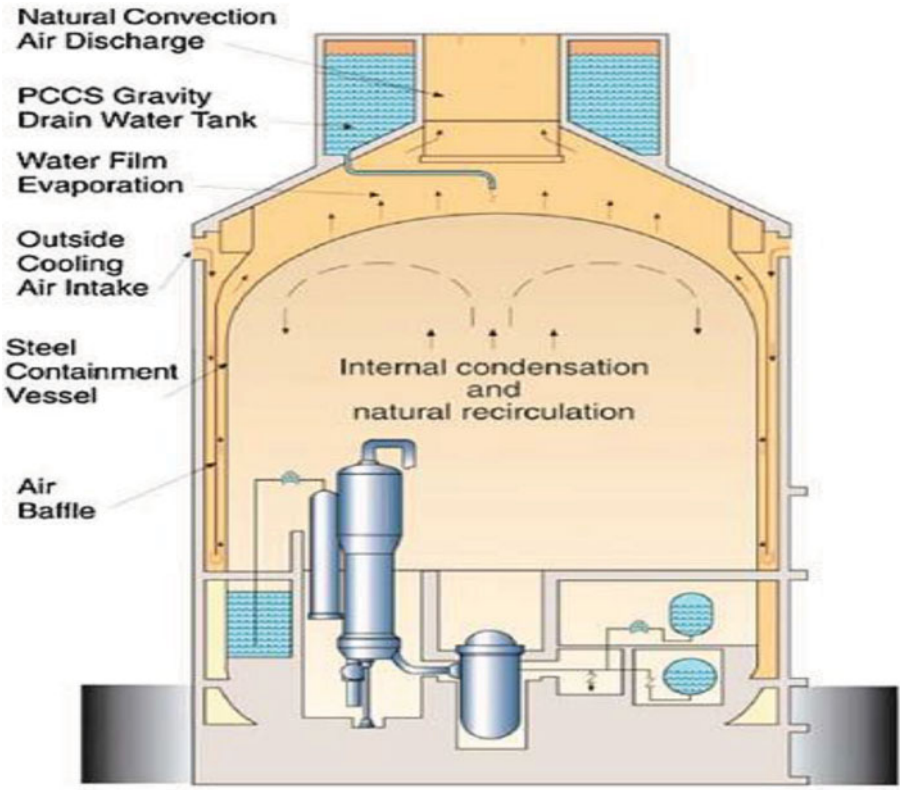

Figure 2. AP1000 passive containment cooling system.

type B failure caused by functional failure due to blocking of intended natural phenomena that can challenge and impair the passive safety principles of either natural laws or inherent characteristics [4]. The qualitative analysis is often necessary so as to identify potential failure modes such as FMEA which can be used to identify the parameters judged critical for the performance of passive system and to help associate failure modes and corresponding indicators of failure cause. The identifications of these two types (A and B) of failure modes concern with both mechanical component (drain valve, piping, HX) and natural phenomena (mainly sustainability of natural circulation in the flow passage), as "virtual" component (phenomenological) [5].

In passive safety systems, because of their design, the mechanical failures (pipe failure, hardware) are very unlikely to happen. Thus, the failure probability of the overall system is very low due to hardware failure. However, the uncertainties involved in AP1000 passive systems might be larger than that in active components of conventional PWR, which may come from the deviations of natural forces or physical principle upon which they rely on (gravity and density difference). Even if there is no hardware failure occurred and the system may not be able to accomplish the mission successfully then functional failure is said to have occurred due to uncertainties in the temperature and pressure of the fluid [13]. The factors leading to disturbance in passive safety systems are thought to be caused by the following: (1) unexpected mechanical and thermal loads, challenging the primary boundary integrity, (2) HX plugging, (3) mechanical component malfunction, (4) non-condensable gas build-up, and (5) heat exchanges process, reduction of heat by surface oxidation, thermal stratification, piping layout, thermal insulation degradation, etc. Finally a set of critical parameter direct indicators of failure within the system is identified; these include the following: (1) existence of non-condensable gas (non-condensable gas fraction), (2) undetected leakage (crack size or leak rate), (3) partially opened valve in the discharge line, (4) heat loss, (5) piping inclination, and (6) plugged pipes in HX. Each of these failure mode 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 [5].

4. Dynamic reliability evaluation of AP1000 by GO-FLOW method

4.1. Single loop model of AP1000 passive safety systems for GO-FLOW analysis and its function during LBLOCA

To evaluate the dynamic reliability of AP1000 plant, a single loop model of AP1000 passive core cooling system (PXS) and PCCS have been considered independently. The schematic diagrams of PXS and PCCS systems are illustrated in **Figures 3** and **4** for GO-FLOW reliability analysis. These passive safety systems (PXS

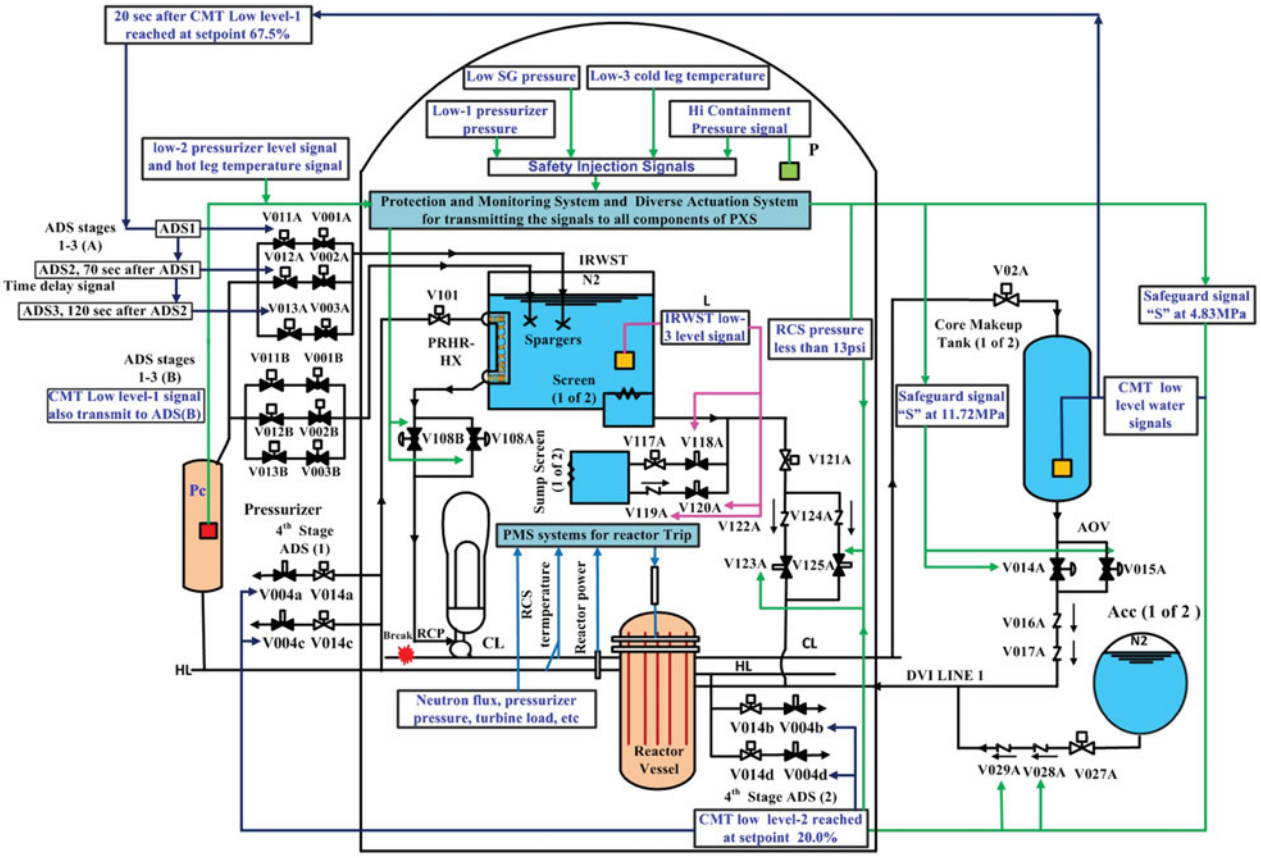

Figure 3. Single loop model of AP1000 PXS system.

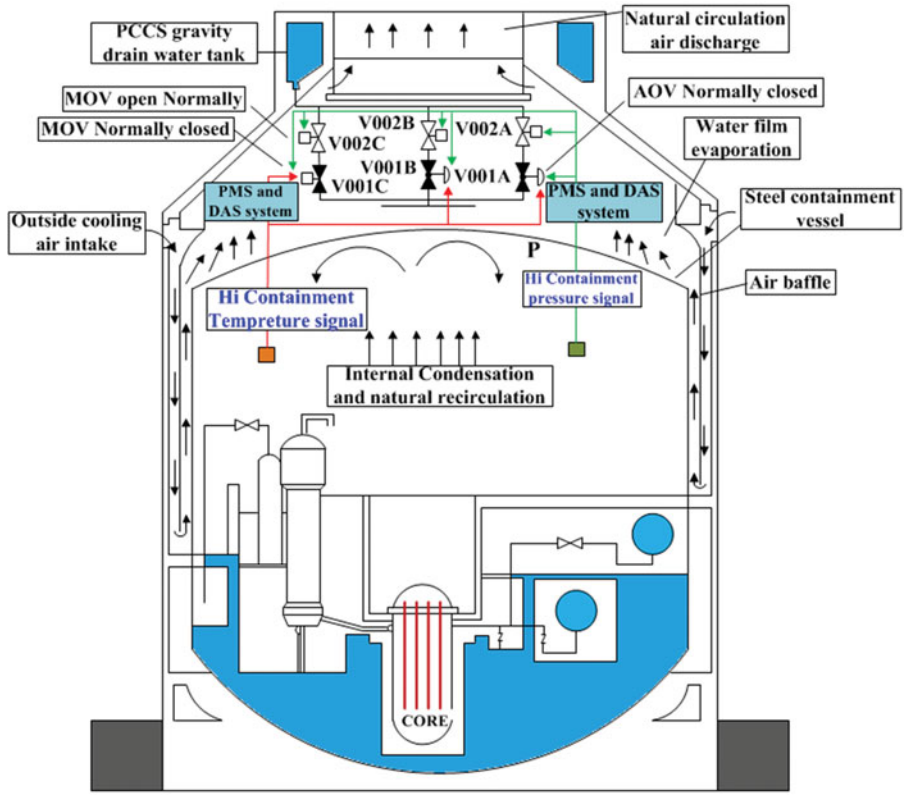

Figure 4. Model of AP1000 PCCS system.

and PCCS) can be treated separately for analysis because these systems are mutually independent of each other. The configuration of PXS includes four functions of (1) reactor shutdown system (reactor protection system RPS), (2) single train of all passive safety injection system (PSIS), (3) PRHRS and (4) ADSs. PCCS system consists of three parallel lines from the PCCS gravity drain water tank with air operated valves (AOVs), normally open MOVs and steel containment surface.

For instruments and control systems in AP1000 plant, all actuation signals for passive safety systems (PXS and PCCS) are transmitted automatically by protection and safety monitoring system and diverse actuation system (DAS) to the relevant actuating components of RPS, PXS and PCCS (see Figure 3 for PXS and Figure 4 for PCCS). When automatic actuation fails, the individual component can be initiated by operator action from main control room using the DAS. There are five independent water resources such as IRWST, recirculation sump, accumulator tank, and CMT for PXS system, while PCCS gravity drain water tank for PCCS systems. The volume of these water resources should be large enough to cool the reactor and to reduce the containment temperature/pressure and washout radioactive material following the LOCA until the time when the reactor attains cold standby condition or hot standby condition.

The PSIS system of AP1000 consists of accumulator injection system, CMT injection system, IRWST gravity injection and containment recirculation sump injection systems. All subsystems of PXS and PCCS are composed of passive valves such as check valves, squib valves (isolation valves), AOVs and normally open MOVs which do not need any power source for their actuation. The injection systems of CMT, IRWST and recirculation sump are designed to have redundancies of safety components complying with the single failure criteria. The different component's symbols used in these single loop models of PXS and PCCS systems are given in **Figure 5**, where components can be distinguished by different color symbols.

In the model, all stages (1–4) of ADS are assumed because of the success criteria and successful actuation of ADS during the accident. The ADS is a unique safety

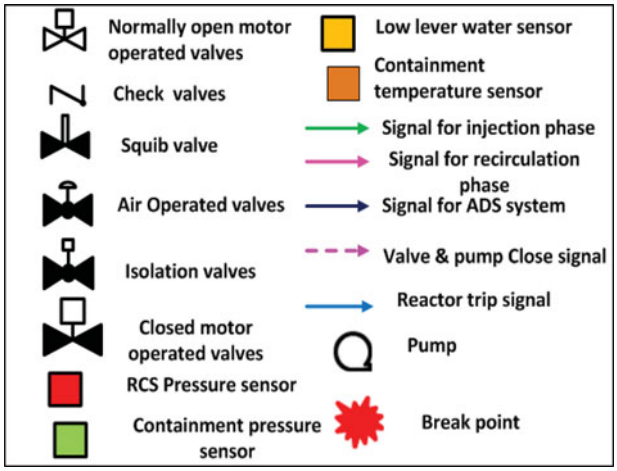

Figure 5. Component symbols used in models of PXS and PCCS.

feature of AP1000 comparatively to conventional PWR, which is added in order to releases, the pressure(in the pressure ranges from rather high to low) from the reactor coolant system in controlled fashion and enables the safety injection from CMTs, IRWST and containment recirculation sump into the reactor coolant system for long-term cooling. It is required primarily to mitigate loss of coolant accidents. The successful actuation of ADS-1 depends on CMT level-1 (67.5%), while the ADS-2 and ADS-3 valves are actuated sequentially after certain time delay defined by timers following opening of the previous stage of depressurization valves. And CMT liquid level decreased with time to reach the Low-2 setpoint (20%) which actuates the ADS-4 and IRWST injection. The success criteria of ADS in order to release the RCS pressure in controlled fashion and enable the safety injection into the reactor vessel during LBLOCA is given in **Table 1** [14].

The functional behaviors of passive safety systems are observed under the accident of LBLOCA and assumption of LBLOCA occurrence is the internal cause of failure such as, loss of water source, loss of command signal, design fabrication and physical environment (high temp and pressure) and no external event (such as big earthquake, explosion, etc., are considered

Table 1. Success criteria of AP1000 ADS for RCS depressurization.

ADS stages	ADS components	Success criteria of ADS (stages 1–4)	Number of paths	Valves opening time (seconds)
ADS-1 stage (A/B)	V011A, V001A, V011B, V001B	V011A × V001A and V011B × V001B	2 out of 2	20
ADS-2 stage (A/B)	V012A, V002A, V012B, V002B	V012A × V002A and V012B × V002B	2 out of 2	30
ADS-3 stage (A/B)	V013A, V003A, V013B, V003B	V013A × V003A and V013B × V003B	2 out of 2	30
ADS-4 stage (a/b/c/d)	V014a/b/c/d, V004a/b/c/d	(1) V014a × V004a and V014b × V004b and V014c × V00c, or (2) V014a × V004a and V014b × V004b and V014d × V004d or (3) V014b × V004b and V014c × V004c and V014d × V004d	3 out of 4	2

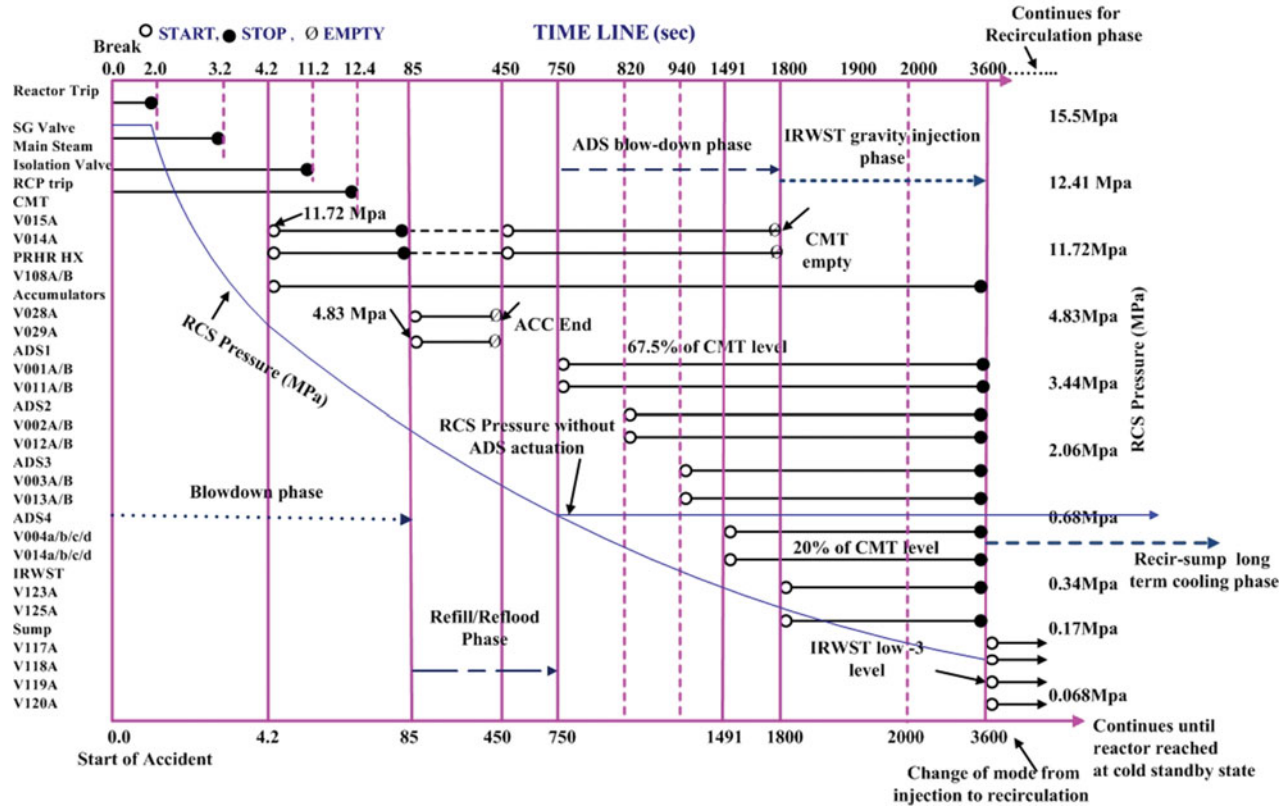

Figure 6. Transient behavior of AP1000 PXS system during LBLOCA.

here). Before the break occurs, the RCS is assumed to be operating at full power in an equilibrium condition (pressure 15.5 MPa), and steam generators are assumed to be isolated immediately at inception of the break to maximize their stored energy.

The transient behavior of damage plant by LBLOCA is assumed to be a successful sequence of (1) reactor shutdown systems, (2) passive core cooling system and (3) PCCS as shown in **Figures 6** and **7** [15]. The transient analysis of PXS and PCCS did not conduct by author himself but has been reduced by the Westinghouse, AP1000 accident analysis reports and some other research papers [16–18], where the authors have characterized the LBLOCA into six distinct phases with respect to change in RCS pressure and temperature (p–t curve) with the passage of time after the LOCA occurred and activation timing of various safety components of PXS and PCCS systems in the respective phases. Therefore, the phased mission profile of AP1000 passive safety systems can be mentioned by following phases

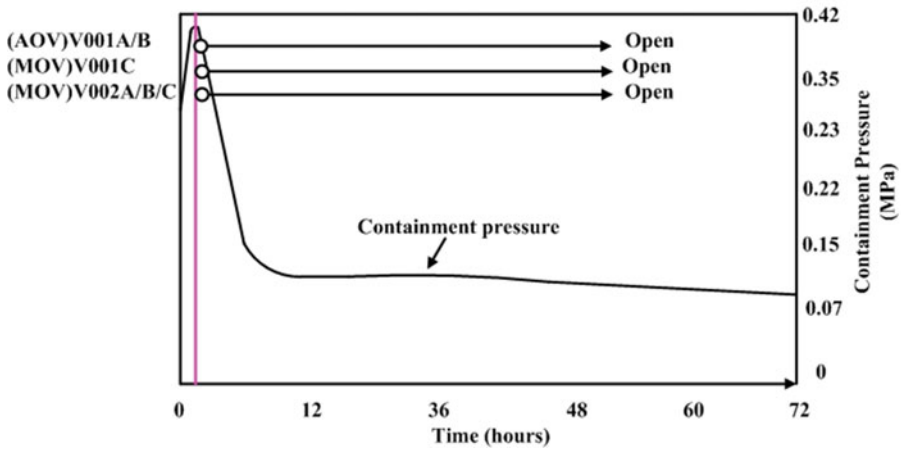

Figure 7. Transient behavior of AP1000 PCCS system.

Table 2. Sequence of events during LBLOCA in AP1000 with actuation signals of passive safety systems.

Activation systems	Phases of LOCA (injection and recirculation phases)		Detecting device (sensors timer)	Actuation signals of RPS, PXS and PCCS	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	Reactor trip switchgear breakers
		Safeguard signal "S"		RCS 11.72 MPa	2.2	Safety actuation system
		Steam generator feedwater		After trip signals	3.2	Feedwater control valve close
Passive core cooling system		CMT injection system	RCS	Low-2 pressurizer pressure, safety injection signals, safeguard S signal at 11.72 Mpa	4.2–85	CMTs tanks, valves V014A–V017A
		PRHR system	Pressure sensor in pressurizer		4.2–3600	PRHR HX, valves V108A/B, V101
		Main steam isolation		After "S" signal	11.2	Isolation valves start to close
		RCS pumps trip		After "S" signal	12.4	Pump trip
	Re-fill/reflood phase	Accumulator start which stop CMT injection	RCS pressure sensor	S signal at 4.83 MPa RCS pressure	85–450	ACC tank, valves V027A–V029A
		CMT start again after Acc empty	Certain RCS pressure value	Accumulator empty signal	450–1800	CMTs tanks, V014A–V017A
	ADS blow-down phase	ADS stage 1 (A/B)	CMT water level sensor	20 sec after 67.5% liquid volume fraction in CMT	750–3600	ADS-1, V001A/B, V011A/B
		ADS stage 2 (A/B)	Time delay timers	70 sec after ADS-1 actuation	820–3600	ADS-2, V002A/B, V012A/B
		ADS stage 3 (A/B)	Time delay timers	120 sec after ADS-2 actuation	940–3600	ADS-3, V003A/B, V013A/B
		ADS stage 4 (a/b/c/d)	Time delay timers	20.0% liquid volume fraction in CMT and 551 sec after ADS-3 actuate	1491–3600	ADS-4, V004a/b/c/d, V014a/b/c/d
	IRWST injection phase	IRWST gravity injection lines flow	RCS pressure and CMT water level sensor	RCS pressure less than 89.6 KPa/13 psi plus containment pressure	1800–3600	IRWST tank, IRWST screen 1, V121A–V125A
	Recirculation sump long term cooling phase	Recirculation injection lines flow	IRWST low level water sensor	IRWST low-3 level signal	3600–6000	Sump, recirculation screen 1, V117A, to V120A
Passive containment cooling system	Containment cooling	Natural circulation of Air with water spray	Containment's temperature and pressure sensors	Hi-2 containment pressure signal 59 psig, high containment temperature	30 sec–72 hours after LOCA	PCCS gravity drain water tank. V001A/B/C, V002A/B/C

Table 3. Severity rank of each failure.

Ranking	Effect	Severity of effect
5	Hazardous	Very high severity ranking when a potential failure mode effects safe system operation
4	Very high	System inoperable with destructive failure without compromising safety
3	High	System inoperable with equipment damage
2	Moderate	System inoperable with minor damage
1	Low	System inoperable without damage

such as (1) blow-down phase, (2) refill phase, (3) reflood phase, (4) ADS blow-down phase, (5) IRWST gravity injection phase, and (6) recirculation sump injection phase for long-term cooling. The actuation timing of various safety components of PXS and PCCS during LBLOCA chronology is given in **Table 2**, where a sequence of all LOCA phases are illustrated with actuation signals for relevant used components. The actuation time and components used for PCCS system are shown in the last row of Table 2. The detail descriptions of LOCA phases are given in [10,16,17].

The phased mission time for different phases of PXS in LBLOCA is larger than that of PWR's ECCS systems. Similarly, PCCS provides cooling to the containment shell for 72 hours for long-term cooling, which is larger than that of 3600 seconds for conventional PWR's CSS.

4.2. *FMEA for AP1000 passive safety systems (PXS and PCCS systems)*

FMEA is a qualitative hazard analysis, which is utilized in the present context for the reliability evaluation of passive safety system and for the identification of potential failure modes affecting the natural circulation on the qualitative basis. It is a bottom-up procedure conducted at the component by which each (1) failure mode in a system is investigated in terms of failure causes, (2) preventive actions on causes, (3) consequences on the system, (4) corrective/preventive actions to mitigate the effects on the system, and (5) eventually classification according to its severity. The main purpose of utilizing FMEA is to provide a framework to structure the experts' thought processes and to focus their attention toward basic system processes and dependencies in the hopes of identifying hard-to-spot failures. The FMEA approaches are applied for both mechanical components within the system (piping, drain valve, heat exchanger), and "virtual" component (phenomenological) in order to identify the two types (types A and B) of failure modes. The critical parameters affecting the natural convection reliability pointed out by FMEA are described earlier in Section 3.

Authors built the FMEA for AP1000 passive safety system on the basis of behavior of PXS and PCCS signal activation systems and sequence of operational events during LBLOCA as shown in Figures 6 and 7 and Table 2. The FMEA worksheet for PXS and PCCS are given in **Table 4**, where most of the components comprising the passive safety systems with a reactor trip system are listed up. Failure modes are ranked according to a severity index related to the estimated range of frequency of occurrence of fault. The failure mode, effect to the plant system operation, detection method and rank of severity for each component are described in Table 4. The rank of severity of individual failure of a certain component is noticed as hazardous, very high, high, moderate and low from the aspect of whether or not the failure of corresponding component may develop into the harmful state of severe accident, and consequence of the corresponding state is a worrisome one or not. The rank of severity of each failure and severity of effect are given in **Table 3**. The two types (type A – hardware failure and type B – functional failure) of failure modes are indicated in the last column of Table 4.

From this FMEA, it can notice the influence of component failure on other components and systems as a whole. This information can be useful for quantitative reliability analysis for PXS and PCCS systems. After the completion of the FMEA qualitative reliability analysis, one can reveal the significant failure modes and important effects to system performance for quantitative reliability analysis of passive safety systems by GO-FLOW method.

4.3. *GO-FLOW analysis of AP1000 passive safety systems (PXS and PCCS)*

The GO-FLOW quantitative analysis has been conducted for a single loop assumption of PXS and PCCS systems of AP1000 in order to obtain the dynamical reliability for advance PWR AP1000. The GO-FLOW charts of PXS and PCCS systems have been made separately because of their independent function during LBLOCA as shown in **Figures 8** and **9**. As the PXS system has redundancies of all injection subsystems and components which can make the system large and complex to consider all subsystems in the same GO-FLOW chart, therefore, authors considered the single loop assumption of the passive safety system in order to conduct dynamic behavior of AP1000 by GO-FLOW.

In the GO-FLOW charts, the passive safety components are represented by relevant operators and the meanings are written by the side of corresponding

Table 4. FMEA Worksheet for AP1000 passive safety systems (PXS and PCCS).

Components	Failure mode	Effect on system operation	Detection method	Severity rank	Types A and B
Reactor trip breaker	Failure to get reactor trip signal	No safe shutdown, damage to fuel and cladding	No operation	Hazardous	A
RCS pressure sensor	Failure to detect low pressure signal	PXS subsystems not actuate	Abnormal operation	Hazardous	B
High containment pressure/ temperature sensors	Fails to detect high containment pressure/ temperature signals	Instantaneous loss of internal condensation and natural circulation	No operation	Very high	B
Accumulator check valves-V028A, V029A	Failure to open	No urgent core cooling	No valve position indication	Moderate	B
Acc, MOV-V027A	Failure to remain open	Acc unable to supply water	Observe at faucet	Moderate	A and B
CMT outlet isolation AOV-V014A, V015A	Failure to open on demand or failure to close on demand	CMT not provide high-pressure water injection	Valve position indication alarm in MCR and RSW	High	B
CMT discharge line check valves – V016A, V017A	Failure to open on demand	No prevention of reverse flow during LBLOCA	Valve position indication alarm in MCR and RSW	High	B
CMT, MOV-V02A	Failure to remain open	No steam/cold water natural circulation mode	Observe at Faucet	Low	A and B
CMT low level water sensor	Fail to transmit low level water signal	IRWST and ADS may delay to actuate	No operation	Hazardous	B
PRHR-HX outlet line isolation AOV-V108A/B	Failure to open	PRHRS may not supply enough water to reactor core	PRHR-HX flow indication in MCR and RSW	High	B
PRHR-HX MOV-V101	Failure to remain open	Cannot remove the residual heat		Low	A and B
IRWST gravity injection line check valves – V122A, V124A	Failure to open	IRWST gravity injection parallel lines are affected and lead to low flow rate	Valve position indication alarm in MCR and at RSW	Hazardous	B
IRWST gravity injection line squib valves – V123A, V125A	Failure to open	IRWST gravity injection lines cannot charge the borated water into the reactor vessel		Hazardous	B
IRWST MOV-V121A	Failure to remain open	Leakage problem	Abnormal operation	High	A and B
IRWST low water sensor	Fail to transmit low level water signal	No circulation mode for long term cooling	No operation	Very High	B
Containment recirculation line Check valve – V119A	Failure to open	Not provide recirculation through a parallel branch line	Valve position indication alarm in MCR and at RSW	Low	B
Squib valve – V120A	Failure to open	No recirculation through a parallel branch line		High	B
Squib valve – V118A	Failure to open	No flow through a MOV and squib valve		High	B
MOV – V117A	Failure to remain open	No flow through a MOV and squib valve	Abnormal operation	High	A and B

Table 4. (*Continued*).

Components	Failure mode	Effect on system operation	Detection method	Severity rank	Types A and B
ADS Stage 1–3 MOV V001A, V011A, V002A, V012A, V003A, V013A	Failure to open on demand	Sufficient RCS pressure will not reduce sequentially for long-term core cooling	Valve position indication alarm in MCR and at RSW	Very high	A and B
ADS stage 4 squib valves – V004a/b/c/d	Failure to open on demand	The primary coolant will not vent directly into the containment		High	B
ADS stage 4, MOV V014a/b/c/d	Failure to remain open		Abnormal operation	Very high	A and B
PCS AOV-V001A/B	Failure to open on demand	Failure blocks flow of containment cooling water from PCCWST	Close to open valve position indication in MCR and at RWS	Hazardous	B
PCS MOV-V001C	Failure to open on demand				A and B
PCS MOV-V002A/B/C	Spurious valve closure	Spurious closure blocks flow of containment cooling water from PCCWST	Open to close valve position indication in MCR and at RWS	Very high	A and B

operators. The connecting lines between every operator identify the signal intensity which controls the system operation and main input signals' sub-input signals and output signals, which are shown by different color intensity lines. The GO-FLOW chart of PXS composed of different parts according to the function of passive safety components in different phases of LBLOCA (blow-down, refill/reflood, ADS blow-down, IRWST gravity injection, and recirculation sump injection) is given in Table 2.

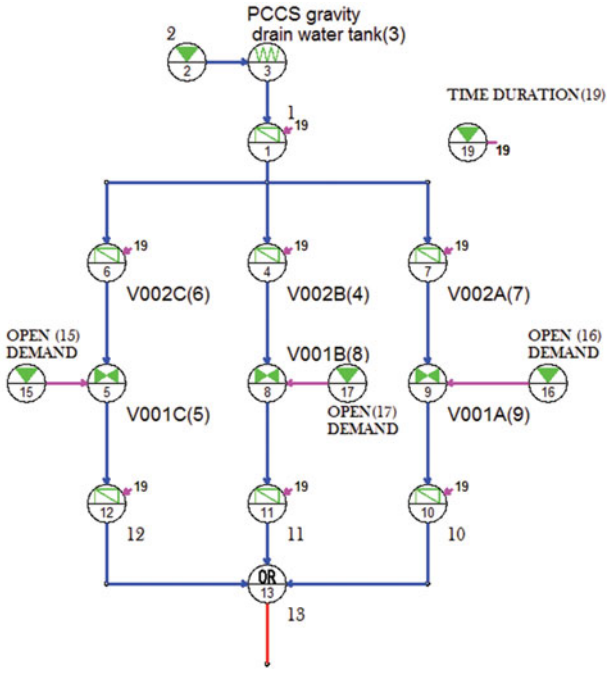

Figure 8. GO-FLOW chart of AP1000 PCCS system.

These GO-FLOW charts are for subsystems of accumulator and CMT, IRWST with recirculation sump, PRHRS and ADS stages (1–4). And these charts are combined together by their output connecting intensities' lines on their correct places for whole PXS. The output failure probabilities of these passive subsystems are presented by operators 75, 21, 182 and 175, respectively, while the failure probability of whole PXS and dynamic reliability of AP1000 are indicated by operators 22 and 177. Similarly, the final failure probability of AP1000 passive containment cooling system is indicated by operator 13 as shown in Figure 8.

In Figures 8 and 9, almost all normally closed valves and normally open valves are assigned sub-input signals for close and open state upon the demand basis and actuation time. Time duration for function of PXS and PCCS system in all phases is indicated by operators 12 and 19 (see Figures 8 and 9). Time points for PXS are 22, while for PCCS are 10,, and analysis has been made at all-time points in order to obtain failure probability results. The time intervals for all passive components of PXS and PCCS used for different phases of LBLOCA are given in Table 2, which are taken on assumption base for GO-FLOW reliability analysis and collected from the Westinghouse accident analysis reports for AP1000 and from some other published research papers [10, 17, and 18]. These time intervals may change with the size and location of LOCA accident. The reliability data assigned to every component of PXS and PCCS are furnished in **Table 5**, which consists of successful probability/demand and operational failure rate/sec and has

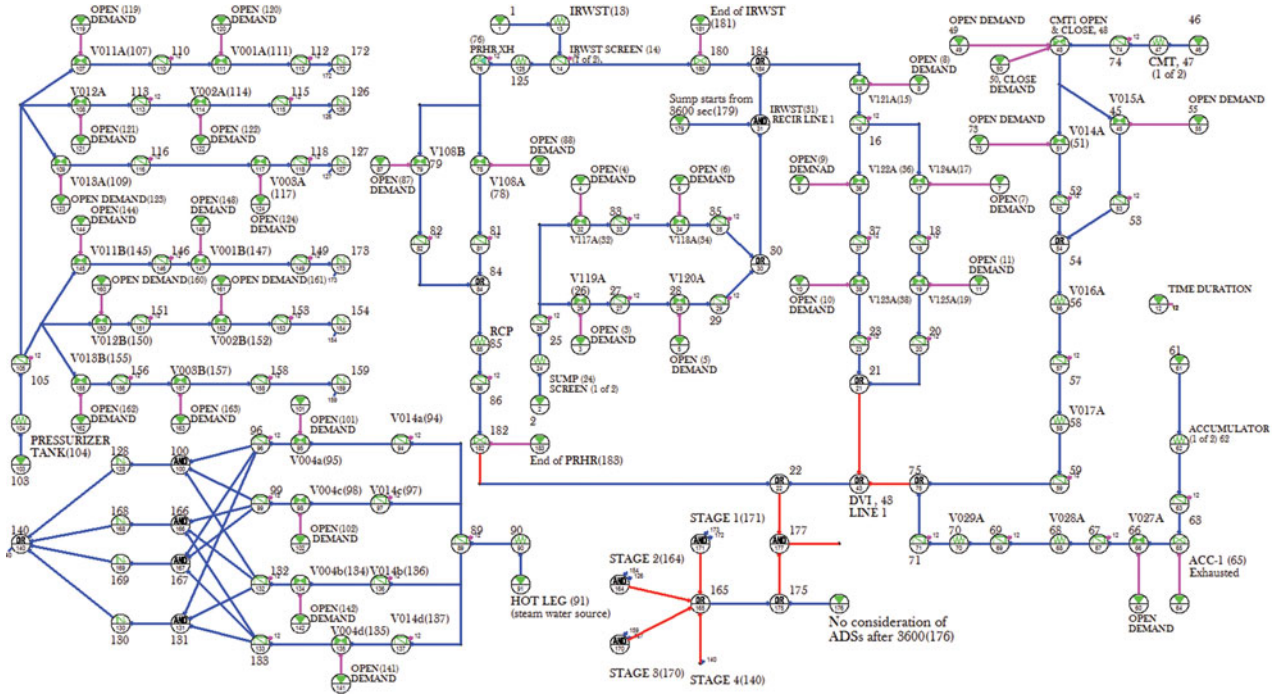

Figure 9. GO-FLOW chart of AP1000 passive core cooling system.

Table 5. Success probability and failure rate of AP1000 PXS and PCCS component.

Components of PXS and PCCS	Success probability (per demand)	Failure rate (sec) λ_o, λ_c	Components	Success probability/ per demand	Failure rate (sec) λ_o, λ_c
V014A, V015A	$P_g = 0.999$	1.00×10^{-6}	IRWST	$P_g = 0.999999$	1.00×10^{-5}
V016A, V017A	$P_g = 0.99999$	1.00×10^{-8}	Sump	$P_g = 0.999999$	1.00×10^{-5}
V028A	$P_g = 0.9982480$	2.00×10^{-7}	V121A	$P_g = 0.99$, $P_p = 0.00$	1.00×10^{-6}
V029A	$P_g = 0.9982480$	2.00×10^{-7}	V123A, V125A	$P_g = 0.99$, $P_p = 0.00$	1.00×10^{-5}
V027A	$P_g = 0.999992$	1.00×10^{-8}	V122A, V124A	$P_g = 0.98$, $P_p = 0.00$	2.00×10^{-7}
Accumulator-1	$P_g = 0.9999$	1.00×10^{-5}	V117A	$P_g = 0.99$, $P_p = 0.00$	1.00×10^{-6}
Core makeup Tank-1	$P_g = 0.99$, $P_o = 1.00$	1.00×10^{-5}	V118A, V120A	$P_g = 0.99$, $P_p = 0.00$	1.00×10^{-5}
CMT open and close action	$P_c = 1.00$, $P_p = 1.00$				
ACC-1 exhausted	$P_g = 1.00$		V119A	$P_g = 0.98$, $P_p = 0.00$	2.00×10^{-7}
PRHR-HX	$P_g = 0.999$	1.00×10^{-8}	RCP	$P_g = 0.99$	1.00×10^{-5}
V108A/B	$P_g = 0.98$, $P_p = 0.00$	1.00×10^{-6}	ADS-4 V014a/b/c/d	$P_g = 0.98$	1.00×10^{-5}
ADS-1 V001A/B, V011A/B	$P_g = 0.9781$	1.00×10^{-5}	ADS-4 V004a/b/c/d	$P_g = 0.99$	1.00×10^{-4}
ADS-2 V002A/B,V012A/B	$P_g = 0.9781$	1.00×10^{-5}	Pressurizer tank	$P_g = 0.99999$	1.00×10^{-5}
ADS-3 V003A/B,V013A/B	$P_g = 0.9781$	1.00×10^{-5}	Hot leg steam	$P_g = 0.9999$	1.00×10^{-6}
PCS-V002A/B/C	$P_g = 0.99$	1.00×10^{-5}	PCS-V001A/B	$P_g = 0.999$	1.00×10^{-6}
PCS-V001C	$P_g = 0.99$	1.00×10^{-5}	PCCWST	$P_g = 0.99999$	1.00×10^{-5}

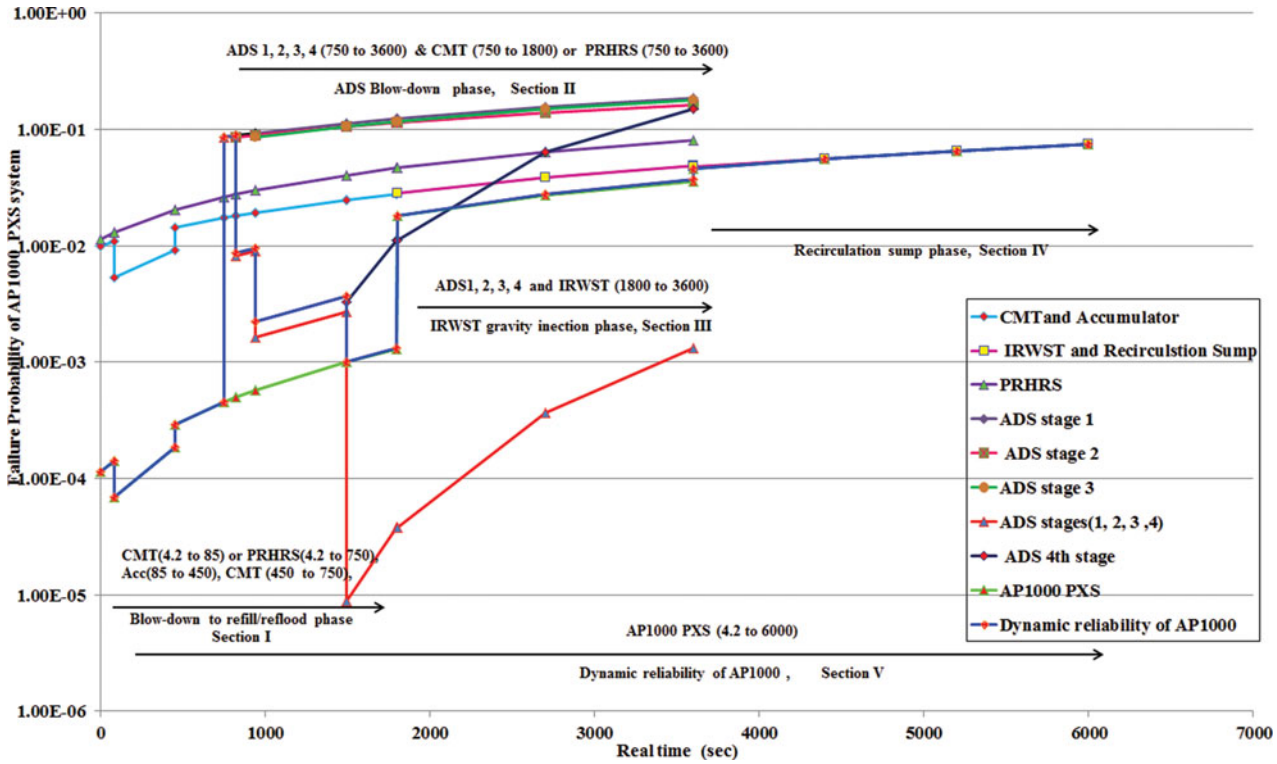

Figure 10. Failure probability of AP1000 PXS system.

been collected from the literature of probabilistic safety assessment of AP1000 for LOCA [19,20]. In Table 5, P_g is the probability for successful operation, P_p is the probability for premature operation, P_o is the probability for valve successfully open, P_c is the probability for valve successfully close, λ_o is the failure rate for open state, and λ_c is the failure rate for close state.

4.4. *Discussion on reliability results*

The failure probability results of passive core cooling systems and PCCS conducted by GO-FLOW method are presented in six different sections from I to VI as shown in **Figures 10** and **11**, respectively. In these sections, the failure probability results for PXS system are explained separately for accumulator and CMT, IRWST with recirculation sump, PRHRS, all stages (1–4) of ADS and for whole PXS system because these systems have different time intervals for their function during LBLOCA accident. The failure probability curves are drawn versus real time taken for these subsystems in case of LBLOCA.

4.4.1. *Section I*

The failure probability results of CMT injection system (4.2–85 and then 450–750), PRHR and accumulator (85–450) lie in this section from blow-down phase to refill/reflood phase. Failure probability results are subtle in start of a system owing to each component functioning correctly after LOCA. The accumulator starts from time 85 to 450 seconds after accident when check valves are open and borated water is forced through the reactor coolant system by gas pressure. Failure probability is very small during this time because one accumulator can provide sufficient inventory for short-term core cooling without injection from the core makeup tanks. ADS 1 and 2 stages may be needed for successful operation of refill and reflood phase. But after 450 seconds, the failure probability increases with passage of time due to higher failure probability of AOVs and check valves. And CMT established the emergency reactor coolant inventory control, emergency boration and emergency core decay heat removal.

4.4.2. *Section II*

The failure probability results of ADS stages (1–3) and their sum are a little bit different from each other because of differences in their mission time due to different flow capacities and the size of ADS valves. The valves of ADS-2/3 and ADS-1 depressurization lines are 8-inch and 4-inch motor operated valves, respectively. The failure probability of these three stages change with time after an accident with blunt rate. Similarly, the ADS-4 stage is equipped with 14-inch squib valves and 14-inch normally open isolation valves. The failure probability results increase continuously due to the larger failure probability of squib valves but total failure probability of first three stages decreases from stages 1 to 3 and is smaller than that of individual one because of redundancies of lines of three stages. CMT system is important to provide low level-1 and

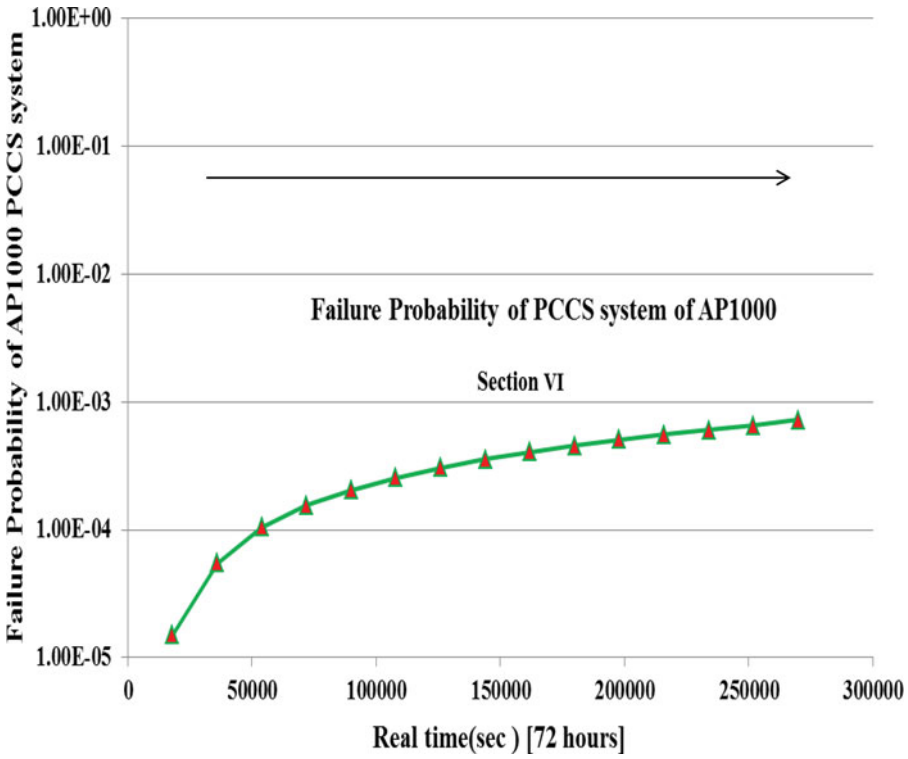

Figure 11. Failure probability of passive containment cooling system of AP1000.

level-2 signals in order to actuate all stages (1–4) of ADS. The failure probability results of PRHRS increase exponentially with time after accident due to reduction of natural circulation flow rate in PRHRS. The PRHR system provides emergency core decay heat removal during transient's accidents, or whenever the normal heat removal system path via the steam generator are lost and depends on reliable passive components by the process of gravity effect and natural circulation. After the ADS actuation, the heat removal rate nearly tended to be zero. In this case, the PRHRS was no longer important in mitigating the accident consequence. The ADS is a key safety system of AP1000, which releases the pressure from the reactor coolant system in the controlled manner to enable the safety injection into the reactor coolant system for long-term cooling.

4.4.3. Sections III and IV

In these sections, failure probability results are presented in two different phases: gravity injection mode from IRWST and then recirculation mode from recirculation sump. The first phased mission period for injection phase is 1800–3600 seconds while that for recirculation phase is 3600–6000 seconds to charge the borated water continuously into the reactor vessel for long-term cooling. The ADS stages remove the decay heat after LBLOCA and enable the safety injection from IRWST and recirculation sump. The failure probability results are small in injection phase and then increase continuously from the beginning of IRWST injection phase to recirculation phase due to increased failure probability of system components with passage of time. The failure probability results increase drastically in Sections III and IV from Section II due to higher failure probability/may be higher failure rate of various squib valves/check valves and MOVs in IRWST gravity injection and recirculation lines and also in Section III, there is only one cooling system IRWST, that is, there is no redundancy.

4.4.4. Section V

The failure probability results for whole PXS are very small from blow-down phase to IRWST gravity injection phase and increase discontinuously in the recirculation phase because the water injection sources reduced only into the recirculation sump. The other discontinuities from Sections II to V are due to different actuation time of ADS stages (1–4) because ADS stages actuate sequentially after time delay to reduce RCS pressure sufficiently so that long-term core cooling can be provided. The dynamic reliability results of AP1000 indicate that the successful actuation of ADS system increases the dynamic reliability of PXS system and is essential to enable the safety injection from IRWST and recirculation sump into the reactor vessel by reducing the RCS pressure. In the failure case of ADS depressurization system, the safety injection into the core may not be guaranteed due to large pressure difference between reactor vessel and water resources. As a consequence, a steam bubble might form in the reactor

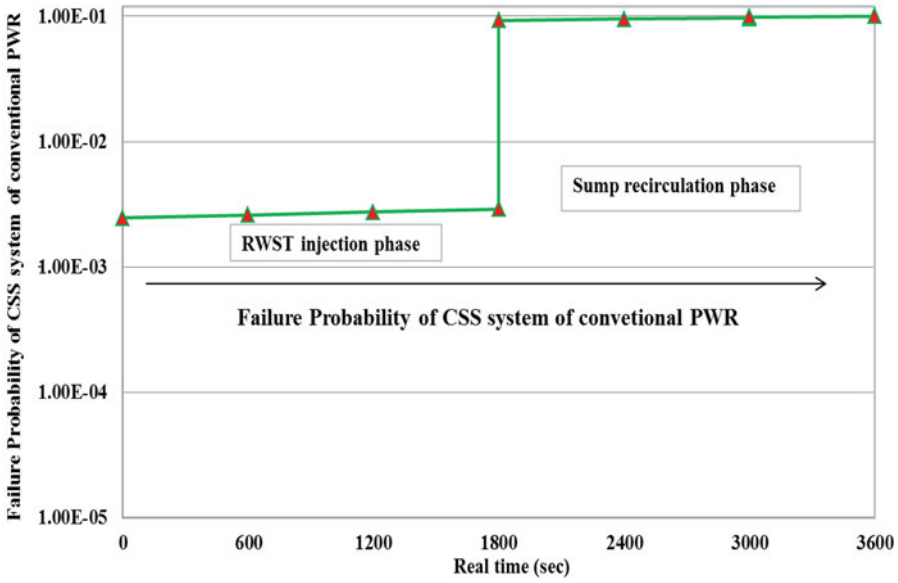

Figure 12. Failure probability of containment spray system of conventional PWR.

pressure vessel, and fuel elements might not be covered with water anymore.

In the present ADS conditions, the failure probability of PXS system sometimes increase stepwisely in very small interval of time at starting point of ADS 1–3. PXS system is temporally in the failed state and then goes back to success state very quickly. And this temporally failure does not affect the safety of power plant system because the successful opening of ADS (1–3) valves reduce the RCS pressure in a controlled manner until the safety limit and enable the quick injection from IRWST and recirculation sump for long-term cooling. The reasons of increase of failure probability of PXS in the start of ADS (1–3) are that ADS works as an active system itself and failure probability of its MOVs and control valves are rather high. And also all valves of ADS (1–3) take different opening time for their actuation (see Table 1) during the event to perform the RCS depressurization. There may be some time consumed in opening of ADS valves and in reaching the required pressure signal setpoint for gravity injection from IRWST and sump.

The reliability of whole PXS system is high due to urgent flow from CMTs, accumulators, successful performance of ADS after the accidents and also due to redundancies of various passive valves in IRWST gravity injection and recirculation sump lines, which are most contributors' factors for the high reliability of PXS system.

4.5. *Intercomparison of reliability results of PCCS of AP1000 and containment spray system of conventional PWR*

4.5.1. *Section VI*

Similarly, the failure probability results of PCCS system are small at the binging and then increase bluntly with passage of time after the accident due to increase of failure probability of PCCS components such as AOVs and MOVs as shown in Figure 11. PCCS has redundancies of three parallel lines from PCCS gravity drain water tank in order to reduce containment temperature and pressure after LOCA and provide an ultimate heat sink in accident conditions. Heat is removed from the containment vessel by continuous natural circulation of air to atmosphere for 72 hours.

For an intercomparison of reliability results of respective passive safety systems of AP1000 and equivalent active safety systems of conventional PWR, authors of this study have compared the reliability results of PCCS of AP1000 with the reliability results of CSS of conventional PWR as shown in **Figure 12** as an example. The main differences in the configuration of both safety systems (CSS and PCCS) are earlier presented in [5], and while reliability results of CSS of conventional PWR are published in papers [21,22]. For relative comparison, it can be seen from Figures 11 and 12 that the failure probability results of PWR's CSS are presented into two phases, "phase 1, RWST injection phase" and "phase 2, sump recirculation phase" and failure probability is small in RWST injection phase and then it discontinuously increases in recirculation sump phase because injection sources from RWST and spray additive tank has reduced only into containment recirculation sump [see 21,22 for detail]. And also the availability or reliability of the NPPs has been affected adversely by the failures of the components and systems with the passage of time which are responsible for a reliable power production. While failure probability results of PCCS system increase slightly with time and are smaller than that of failure probability results of CSS system of conventional PWR because of less opportunities hardware failure and human error. The PCCS of AP1000 can provide cooling to the containment shell until 72 hours for long-term

cooling after accident which is larger than that of cooling time (1 hour) of CSS system of conventional PWR for LBLOCA. Hence, the PCCS of AP1000 is more reliable than the CSS of conventional PWR in order to reduce the containment pressure and washout radioactive material in the event of a big accident.

The reason the PCCS system is more reliable is that PCCS system is composed of only passive components, and its function is achieved by using (1) battery-powered valve actuation, (2) compressed gasses (nitrogen, air), (3) condensation and (4) natural circulation/evaporation. While CSS system of conventional PWR composed of active components such as containment spray pump, and various MOVs, which need external power for their function. And also water resources in conventional PWR are shared mutually by ECCS and CSS system but on the other hand, water resources of PCCS and PXS are independent of each other in AP1000. Therefore, due to the passive design of safety systems of AP1000, there is less chance of hardware failure and human error due to decrease of human–machine interaction by avoidance of external power.

In fact, the increased rate of all results of failure probability of both passive safety systems (PXS and PCCS) of AP1000 is less than that of active component used in conventional PWR because they only rely on natural forces such as gravity, natural circulation, and compressed gas simple physical principles, etc., to perform their accident prevention and mitigation functions once actuated and started. The present analysis has been conducted by considering both types (A and B) of failure modes on the basis of qualitative FMEA analysis. Hence, the GO-FLOW methodology can be used to evaluate the dynamic reliability of passive safety systems. These calculated results can be utilized in the safety evaluation since the analysis results by GO-FLOW is qualitatively reasonable, correct and easy to recalculate. However, complete comparison for the reliability results for both PWR's plant safety systems (AP1000 and conventional PWR) will be conducted in the future study by considering the redundancies of safety components of plant's systems, sensitivity analysis, uncertainties, common mode failure consideration and also reliability of reactor shutdown systems of both reactors.

5. Conclusion

In this paper, quantitative dynamic reliability analysis of AP1000 passive safety systems have been conducted in order to confirm, how to evaluate dynamic reliability of passive safety systems by GO-FLOW methodology; the passive safety systems concept is more reliable than the PWR's active safety systems. And then what is the comparison of reliability results of AP1000 passive safety systems with active safety systems of conventional PWR. For this purpose, authors first described the failure modes of passive safety system, which was the first step of reliability assessment of passive safety system, and it was discussed that AP1000 passive safety components depend on the two types of failure modes, that is (type A) structural failure (hardware failure) and physical degradation and (type B) functional failure due to blocking of intended natural phenomena that can challenge and impair the passive safety principles of either natural laws or inherent characteristics.

Then, a single loop model of AP1000 passive core cooling system and PCCS were considered for quantitative dynamic reliability analysis. The transient behavior of these passive safety systems was summarized in the event of LBLOCA taken from published safety reports of AP1000, where the LBLOCA was divided into six phases. The qualitative reliability analysis tool "FMEA" was applied in order to identify the potential failure modes (for both types A and B), and parameters judged critical for the performance of the passive system. Quantitative reliability analysis was conducted by using success-oriented system reliability analysis, GO-FLOW method and failure data of passive components were collected from the Westinghouse AP1000 literature documents.

Finally, dynamic reliability results are presented quantitatively for PXS and PCCS according to LBLOCA phases and then reliability results of PCCS system of AP1000 and CSS of conventional PWR are compared for relative comparison of equivalent safety systems of both plants. From these results of passive safety systems of AP1000, it was concluded that in LBLOCA, the reliability of AP1000 is higher from the blow-down phase to IRWST gravity injection phase and then decrease discontinuously in the recirculation phase because the redundancies of injection subsystems of PXS only reduced into the recirculation sump and also due to increase in the failure probability of components with time. The urgent flow from CMT, accumulator into the reactor core, successful performance of ADS after the accidents and redundancies of various passive valves in IRWST gravity injection and sump lines are main contributors for high reliability of PXS system. The analysis results also indicate that ADS is a key safety system of AP1000 for the successful actuation of subsystems of PXS and PCCS, comparatively to PWR plant. From the comparison of reliability results of PCCS and CSS systems, it was noticed that passive safety systems of AP1000 are more reliable than active safety systems of conventional PWR because passive safety systems only depend on natural phenomena and do not need any external power sources for their actuation.

However, complete comparison between both PWR plants (AP1000 and conventional PWR) from the aspect of reliability analysis will be conducted in the future study by considering the redundancies of components of safety systems of both plants (active and passive), sensitivity analysis, uncertainties analysis, common mode failure consideration and also including the reliability of reactor shutdown systems of both PWR plants.

Acknowledgements

The authors would like to express great thanks for the valuable suggestions of Prof. Zhang Zhijian (Dean of CNST).

Funding

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

References

[1] Ahmed W, Burgazzi L. Nuclear Power-Practical aspects: Reliability of passive systems in nuclear power plants. 2012. Chapter 2; pp. 23–58 (ISBN 978-953-51-0778-1).
[2] Schulz TL. Westinghouse AP1000 advanced passive plant. Nucl Eng Des. 2006;236:1547–1557.
[3] International Atomic Energy Agency. Safety related terms for advanced nuclear power plants. TEC-DOC-626. Vienna: International Atomic Energy Agency; 1991.
[4] Burgazzi L. Evaluation of uncertainties related to passive systems performance. Nucl Eng Des. 2004;230:93–106.
[5] Hashim M, Yoshikawa H, Ming Y. Addressing the fundamental issues in reliability evaluation of passive safety AP1000 to be compared with active safety PWR. Int J Nucl Saf Simulation. 2013;4:147–159.
[6] Burgazzi L. Passive system reliability analysis: a study on the isolation condenser. Nucl Tech. 2002;139:3–9.
[7] Jiyong O. Methods for comparative assessment of active and passive safety systems with respect to reliability, uncertainty, economy and flexibility [dissertation]. Cambridge (MA): Massachusetts Institute of Technology; 2008.
[8] David ML. Failure modes and effects analysis. Tyco Electronics Corp. Available from: dmlittle@tycoelectronics.com
[9] Matsuoka T, Kobayashi M. GO-FLOW – a new reliability analysis methodology. Nucl Sci Eng. 1998;175(3):64–78.
[10] Westinghouse Electric Company. Application of ASTRUM methodology for best-estimate large-break loss-of-coolant accident analysis for AP1000. DCP/NRC2182; 2008. Avaialble from: https://www.ukap1000application.com/doc_pdf_library.aspex
[11] Paolo, G. AP1000 the PWR revisited, Westinghouse Electric Company report, IAEA-CN-164-3S05; 2013.
[12] Kemper RM, Hochreiter LE, Takeuchi K. The LOCA performance of the AP600 passive safety systems. Trans Am Nucl Soc. 1992;66:601–603.
[13] Pagani LP, Apostolakis GE, Hejzlar P. The impact of uncertainties on the performance of passive systems. Nucl Tech. 2005;149:129–140.
[14] Westinghouse Electric Company. AP1000 pre-construction safety report, UKP-GW-GL-732, Revision 2; 2009. Avaialble from: https://www.ukap1000application.com/doc_pdf_library.aspex
[15] Westinghouse Electric Company. AP1000 design and control document. Engineered safety features, Revision 1. Westinghouse electric company; 2009. Avaialble from: https://www.ukap1000application.com/doc˙pdf˙library.aspex
[16] Yang J, Wang WW, Qiu SZ, Tian WX. Simulation and analysis on 10-inch cold leg small break LOCA for AP1000. Ann Nucl Energy. 2012;46:81–89.
[17] Wright RF. Simulated AP1000 response to design basis small-break LOCA events in APEX-1000 test facility. Nucl Eng and Tech. 2007;39:287–298.
[18] Westinghouse Electric Company. AP1000 design control document. Accident analysis. Westinghouse Electric Company; 2009. Avaialble from: https://www.ukap1000application.com/doc_pdf_library.aspex
[19] Westinghouse Electric Company. AP1000 design control document. Probabilistic safety assessment. Westinghouse Electric Company; 2009. Avaialble from: https://www.ukap1000application.com/doc_pdf_library.aspex
[20] Westinghouse Electric Company. AP1000 design control document. Probabilistic risk assessment. Westinghouse Electric Company; 2009. Avaialble from: https://www.ukap1000application.com/doc_pdf_library.aspex
[21] Hashim M, Matsuoka T, Yang M. Development of a reliability monitor for the safety related subsystem of a PWR considering the redundancy and maintenance of components by fault tree and GO-FLOW methodologies. Int J Nucl Saf Simulation. 2012;3:164–175.
[22] Hashim M, Yoshikawa H, Yang M. Development of reliability monitor by GO-FLOW methodology for the safety related sub-systems in PWR. Int J Nucl Energy Sci Tech. 2013;8:21–36.