Nuclear Engineering and Design 278 (2014) 209–221

Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes

Application case study of AP1000 automatic depressurization system (ADS) for reliability evaluation by GO-FLOW methodology

Muhammad Hashim*, Yoshikawa Hidekazu, Matsuoka Takeshi, Yang Ming

College of Nuclear Science and Technology, Harbin Engineering University, No. 145, Nantong Street, Nangang District, Harbin, Heilongjiang Province 150001, PR China

HIGHLIGHTS

- Discussion on reasons why AP1000 equipped with ADS system comparatively to PWR.
- Clarification of full and partial depressurization of reactor coolant system by ADS system.
- Application case study of four stages ADS system for reliability evaluation in LBLOCA.
- GO-FLOW tool is capable to evaluate dynamic reliability of passive safety systems.
- Calculated ADS reliability result significantly increased dynamic reliability of PXS.

ARTICLE INFO

Article history:
Received 3 January 2014
Received in revised form 10 June 2014
Accepted 27 June 2014

ABSTRACT

AP1000 nuclear power plant (NPP) utilized passive means for the safety systems to ensure its safety in events of transient or severe accidents. One of the unique safety systems of AP1000 to be compared with conventional PWR is the "four stages Automatic Depressurization System (ADS)", and ADS system originally works as an active safety system. In the present study, authors first discussed the reasons of why four stages ADS system is added in AP1000 plant to be compared with conventional PWR in the aspect of reliability. And then explained the full and partial depressurization of RCS system by four stages ADS in events of transient and loss of coolant accidents (LOCAs). Lastly, the application case study of four stages ADS system of AP1000 has been conducted in the aspect of reliability evaluation of ADS system under postulated conditions of full RCS depressurization during large break loss of a coolant accident (LBLOCA) in one of the RCS cold legs.

In this case study, the reliability evaluation is made by GO-FLOW methodology to determinate the influence of ADS system in dynamic reliability of passive core cooling system (PXS) of AP1000, i.e. what will happen if ADS system fails or successfully actuate. The GO-FLOW is success-oriented reliability analysis tool and is capable to evaluating the systems reliability/unavailability alternatively to Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) tools. Under these specific conditions of LBLOCA, the GO-FLOW calculated reliability results indicated that ADS is a key safety system of AP1000 NPP to reduce RCS pressure in controlled fashion and enables the all safety injections for automatic core cooling successfully after the accident. And dynamic reliability of the passive core cooling system of AP1000 plant is increased by the successful actuation of ADS system. Thus, by this application case study, it is pointed out, that high reliability of the passive safety system of AP1000 would depend on the full reliability of ADS system that it would work surely when needed.

1. Introduction

AP1000 is one of the advanced light-water reactors, which incorporate the passive engineering safety features to perform its safety-related functions in the event of transients or severe accidents. AP1000 employed the various passive safety systems while reducing the number of active safety systems in order to provide the significant improvement in plant safety design, simplification,

* Corresponding author. Tel.: +923334477607/8057793.
E-mail addresses: hashimsajid@yahoo.com, hashim@hrbeu.edu.cn (M. Hashim), yosikawa@kib.biglobe.ne.jp (Y. Hidekazu), mats@cc.utsunomiya-u.ac.jp (M. Takeshi), myang.heu@gmail.com (Y. Ming).

http://dx.doi.org/10.1016/j.nucengdes.2014.06.040
0029-5493/

Nomenclature

ACC	accumulators
ADS	automatic depressurization system
CMT	core makeup tank
DAS	diverse actuation system
ECCS	emergency core cooling system
ETA	even tree analysis
FMEA	failure mode and effect analysis
FTA	fault tree analysis
I & C	instrument and control system
IRWST	In-containment refueling water storage tank
LBLOCA	large break loss of coolant accident
MOVs	motor operated valves
MCR	main control room
NRHRS	normal residual heat removal system
NPP	nuclear power plant
PXS	passive core cooling system
PSA	probabilistic safety assessment
PRA	probabilistic risk assessment
PCCS	passive containment cooling system
PRHRS	passive residual heat removal system
PRHR-HX	passive residual heat removal heat exchanger
PMS	protection and safety monitoring system
RCS	reactor coolant system
RCP	reactor coolant pump

cost reduction, etc. These passive safety systems of AP1000 do not need any external input or energy (AC power) for their successful actuation and only rely upon the natural physical laws such as gravity, natural convection, conduction, and/or on inherent characteristics (properties of materials, internally stored energy, etc.) and/or 'intelligent' use of the energy (decay heat, chemical reactions, etc.). The AP1000 passive safety systems mainly consist of passive core cooling system (PXS) and passive containment cooling system (PCCS). The PXS is further divided into several subsystems such as: (i) core makeup tanks (CMTs), (ii) accumulators (ACC), (iii) in-containment refueling water storage tank (IRWST) for water injection, (iv) recirculation sump for long-term cooling, (v) passive residual heat removal system (PRHRS), and (vi) automatic depressurization system (ADS) (Shahabeddin and Mohammadreza, 2012). One of the unique safety features of AP1000 is the "four stages ADS system" to be compared with the conventional PWR which has no such depressurization system. The AP1000 ADS system works as an active safety system (Hashim et al., 2013a). In this paper, the authors first discussed the reasons in detail why AP1000 is equipped with four stages ADS system to be compared with conventional PWR in the aspect of reliability. And then explained the full and partial depressurization of RCS system by ADS in events of transient and LOCA accident. Lastly, the application case study of AP1000 ADS system has been conducted in the aspect of reliability evaluation of four stages ADS system under postulated conditions of full RCS depressurization during LBLOCA in one of the RCS cold leg.

The reliability evaluation is made by GO-FLOW method in order to determinate the influence of ADS system in dynamic reliability of AP1000 PXS system, i.e. what will happen if ADS system fails or successfully actuate. Here, the definition of "reliability" is a ability of the system to carry out its safety function under prevailing accidental conditions when required (Burgazzi, 2004). The GO-FLOW technique utilized for present analysis because it is a success oriented reliability analysis (Matsuoka and Kobayashi, 1988) and is capable of evaluating the system dynamic reliability and availability of target systems instead of FTA/ETA (USNRC, 1981) used in conventional living probabilistic safety assessment (PSA). By the use of GO-FLOW, it becomes easier than by FTA/ETA to treat the phased mission problem.

In what follows, the discussions of this paper started from the brief description of passive safety systems of AP1000 summarized in Section 2. While the GO-FLOW methodology discussed in Section 3. And then configuration and reasons of adding AP1000 ADS system are presented in Sections 4 and 5 respectively. Lastly, in a Section 6, application case study of ADS system is conducted in the aspect of reliability evaluation by GO-FLOW method and calculated reliability results are explained in subsequent Section 6.4.

2. Brief description of AP1000 passive safety systems

The passive safety systems of AP1000 as shown in Fig. 1 combine to protect the AP1000 plant against the leakage and rupture of various size and locations. The detail descriptions of these passive subsystems with their safety function during the LBLOCA and actuation timing was explained in the authors published papers (Hashim et al., 2013a, 2014), Wherein fundamental issues in reliability evaluation of passive safety systems of AP1000 to be compared with the active safety systems of conventional PWR are also discussed. And they are related with several aspects such as: difference of safety systems configuration in both PWR plants, differences in potential failure modes of passive safety components and how to evaluate the reliability of passive safety system.

And then safety of AP1000 is addressed by passive safety systems in aspect of prevention and mitigation of severe accident phenomena in LOCA. The AP1000 passive design represents a significant improvement over conventional PWRs, and is developed around the fundamental design principles of safety, simplification and standardization. The brief description of all subsystems of AP1000 PXS is given as follows (Schulz, 2006):

1. 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 RCS if inventory is being lost.
2. Two pressurized accumulators (ACC) provide high flow borated water to the reactor vessel at RCS pressures of 4.83 MPa.
3. An IRWST provides low flow borated water in a longer time after system pressure drops to near the containment pressure. The function of IRWST/gravity injection is to provide flooding of refueling cavity for normal refueling, post LOCA flooding of containment to establish the long-term RCS cooling, and to support the passive residual heat removal heat exchanger (PRHR-HX) operation.
4. The PRHRS provides passive energy removal through a natural circulation path connecting the pressurizer-side hot leg and the steam generator exit plenum. The IRWST provides a heat sink to perform the high pressure natural coolant circulation to fulfill the core cooling function.
5. Two recirculation sumps provide the way to inject recirculation water to the primary system after the primary system is fully depressurized, and gravity head becomes great enough. A recirculation sump that collects the water discharged from the primary system and steam that condenses within the containment.
6. The four stages ADS, which comprise a set of valves, connected to the pressurizer steam space and the two hot legs. The detail description of ADS system configuration and application case study of ADS conducted in aspect of reliability assessment are explained from sections 4 to 6.

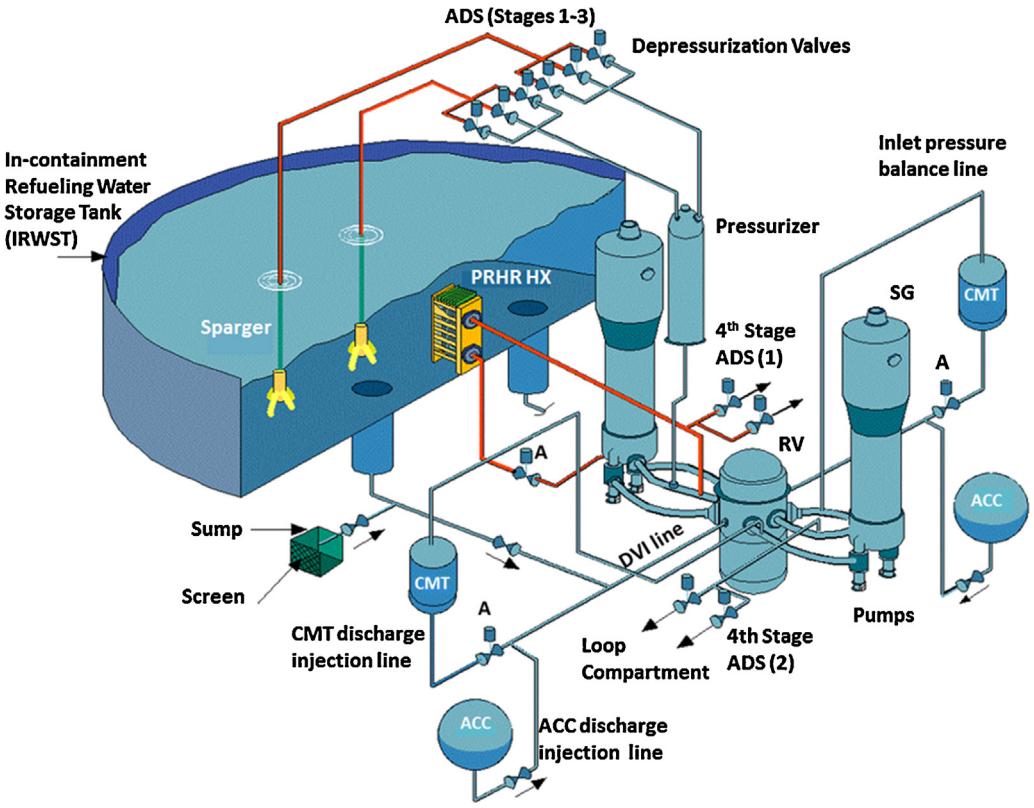

Fig. 1. Passive core cooling system of AP1000.

3. GO-FLOW methodology

The GO-FLOW methodology is a reliability analysis methodology, which was developed by two Japanese Professors Matsuoka Takeshi and Kobayashi. It is success-oriented system analysis technique and is capable of evaluating system reliability and availability. The modeling technique produces a chart which consists of signal lines and operators, and represents engineering function of the components/subsystems/system. The operators model function or failure of the physical equipment, and also represent logical gates, signal generators. Fourteen different types of GO-FLOW operators are currently defined as shown in Fig. 2. Specific probabilities (point estimates) of component operations or failure are given as input data (Matsuoka and Kobayashi, 1988).

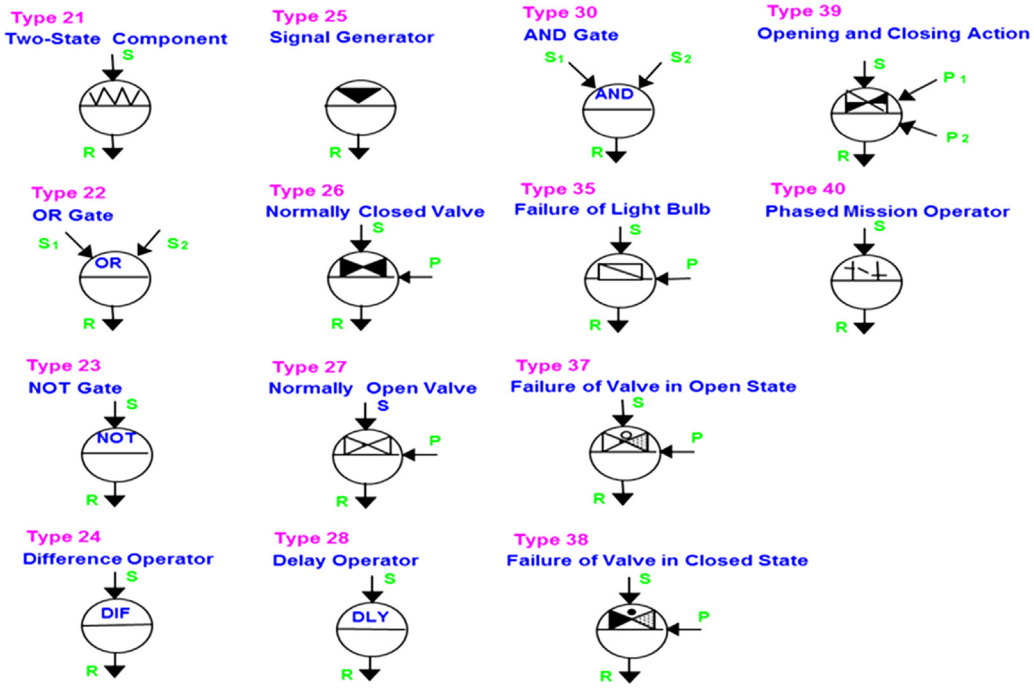

Fig. 2. Symbols of operators used in GO-FLOW methodology.

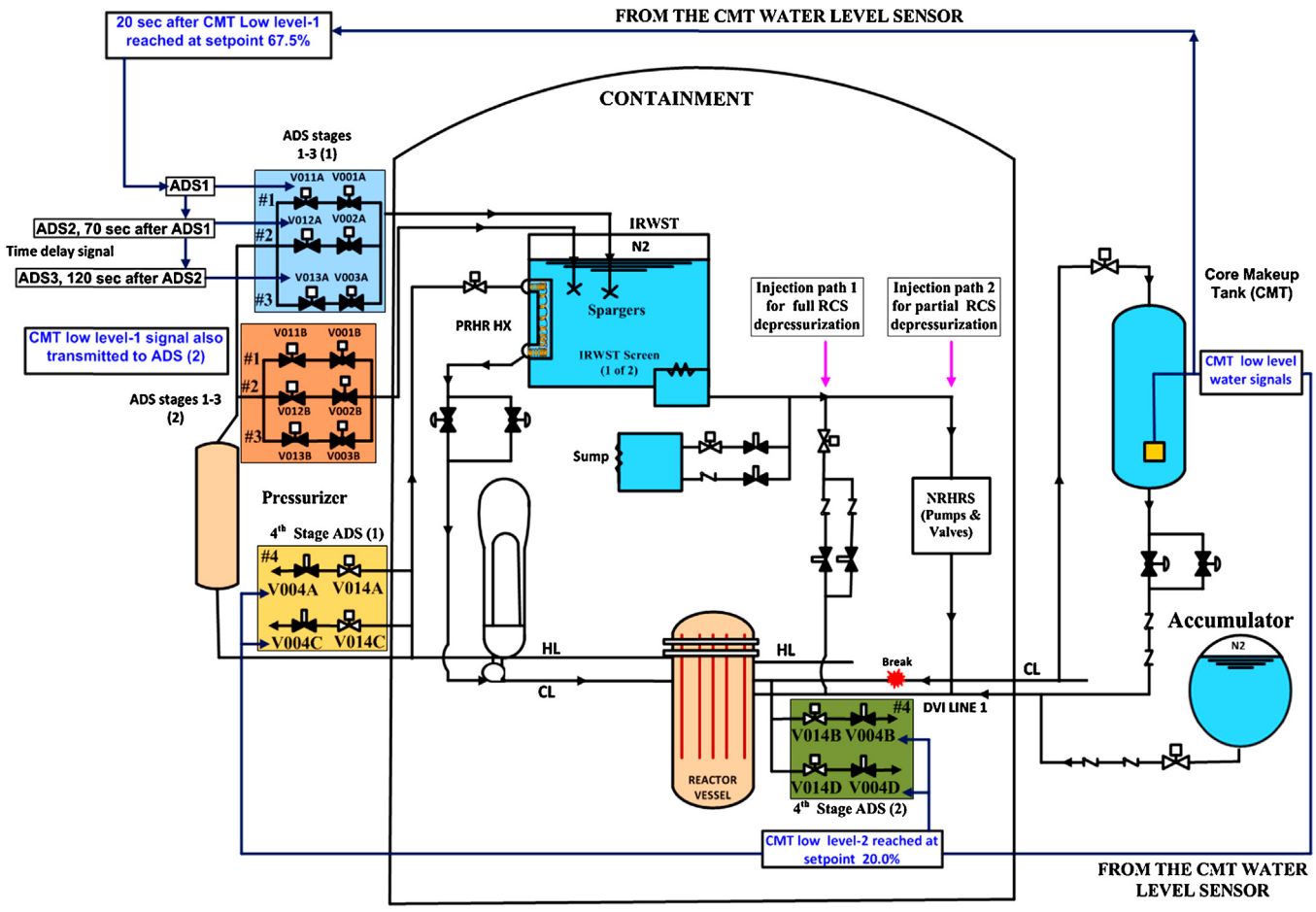

Fig. 3. Schematical model of four stage ADS system (Westinghouse Electric Company, 2009b).

Signals represent some physical quantity or information. The existence of a signal means the existence of a physical quantity or information.

In the GO-FLOW methodology, the existence of a signal is interpreted as both the actual and the potential existence of a signal. "Potential existence" means that a signal exists when all the resistances of downstream are removed. A quantity called "intensity" is associated with a signal. Usually the intensity represents the probability of signal existence. When a signal is used as a sub-input signal to type 35, 37 or 38 operators, the intensity represents a time interval between the successive time points. A finite number of discrete time values (points) are required to express the system's operational sequence. The value does not necessarily represent the real time, but correspond to it and represent an ordering. First step of the analysis is to construct a GO-FLOW chart, which is a modeling of an engineering system. An analyst interactively constructs a chart on a PC display with the support of the GO-FLOW chart editor. During the construction of a chart, component failure data and analysis conditions are assigned in a chart.

An analysis is performed from the upstream to the downstream signal lines. In most cases, only one, or at most few of all the defined signals are of interest; these signal lines are termed as final signals. An analysis is complete when the intensities of these final signals at all the time points are obtained. The GO-FLOW methodology possesses the following significant features: (a) The GO-FLOW chart corresponds to the physical layout of the system and is easy to construct and validate, (b) alternations and updates to a GO-FLOW chart are readily accomplished, and (c) GO-FLOW contains all the possible system operational states. And GO-FLOW methodology can perform following functions such as: (a) analysis of phased mission problem, (b) aging and maintenance effects, (c) identification of minimal cut sets, and parametric studies of (d), common cause failure analysis by parametric model, (e) Uncertainty analysis, and (f) sensitivity analysis.

In the reliability evaluation of a phased mission system, the condition of components may be critical for one particular phase and transition from one phase to another is the critical event leading to mission failure and failure of the components can occur at any point during the mission (Hashim et al., 2012; Xing and Dugan, 1999). For the solution of a phased mission problem, the fault tree has some difficulties such as: (i) fault trees may reveal human error (They hardly can determine the underlying causes vide infra), (ii) analysis can lead to the generation of a plethora of failure trees if the analysis has very wide scope, (iii) fault trees need detailed knowledge of the operation, construction and design of the system, (iv) fault trees may become very robust and intricate, (v) significant training and experience is necessary to use this technique properly; and hence explains why it is time-consuming, (vi) the tree does not represent the transition routes between states of any events, (vii) different fault trees must be developed for different top events, and (viii) same event may appear in different parts of the tree, leading to some initial confusion (Mo et al., 2007). Mindful of these difficulties the authors have utilized the GO-FLOW methodology for analyzing the dynamical reliability of passive safety systems of AP1000 that undergo phased missions.

For GO-FLOW quantitative reliability assessment for safety systems of conventional PWR and AP1000, the qualitative reliability analysis FMEA gives the important informations such as all

Table 1
Actuation signals and valves opening time of ADS system (Westinghouse Electric Company, 2009a).

ADS stages	Actuation signals	Size of ADS valves (in.)	Valves opening time (s)	Valves flow area (in.^{2})	Design pressure (Psig)	
					Open	Close
ADS stages	Manual initiation OR					
ADS-1 stage (A/B)	Low-1 CMT level in either CMT AND CMT actuation signal	4-in. MOVs	20 s	4.6	2485	2485
ADS-2 stage (A/B)	First stage ADS signal AND time delay set by timer	8-in. MOVs	30 s	21	2485	1200
ADS-3 stage (A/B)	Second stage ADS signal AND time delay set by timer	8-in. MOVs	30 s	21	2485	1200
ADS-4 stage (1/2)	Low-2 CMT level in CMT AND third stage ADS signal AND time delay OR Low hot leg level AND time delay	14-in. MOVs & squib valves	2 s	67	200	200

associated possible potential failure modes, impacts on whole safety system and degree of fatalness, etc. (Hashim et al., 2013b, 2014). This information is useful to make the quantitative reliability analysis for safety systems. The failure data for GO-FLOW analysis can be prepared on the base of action and failure modes of components from the literature documents and accident analysis reports for the LOCA accidents. By considering the suitable failure data of components, the GO-FLOW analysis can be proceed for safety system in order to obtain the dynamic reliability results.

4. Configuration of ADS system used in AP1000

The design of AP1000 ADS system consists of four stages depressurization valves that open sequentially as shown in Fig. 3. The ADS stages are interlocked (operate as the unit), so that stage 1 is initiated first, and subsequent stages are not actuated until previous stages have been actuated. The stages (1–3) of ADS are arranged into two identical groups, and each group has a common inlet header connected at the top of reactor pressurizer and a common discharge line to one of the spargers in IRWST. Due to two redundant parallel paths, there is no single failure prevents operation of ADS stages when it is called upon to actuate (Westinghouse Electric Company, 2009a).

Each of two lines of ADS 1–3 are arranged with two motors operated valves (gate valves and globe valves) in series, which are normally closed and are supported by the electric power system (battery) for control and motive (motor-operated valves) power; and by the protection and safety monitoring system (PMS) and the diverse actuation system (DAS) for actuation. According to IAEA classification of passive safety component, ADS valves address the intermediary zone between active and passive where execution of the safety function is made through passive methods except that internal intelligence is not available to initiate the process. So ADS valves included in the lowest category of passivity, i.e. "Category D: external signals and stored energy (passive execution/active initiation)". Because this system's component relying on no external power supply but using a dedicated internal power source (e.g. a battery) to supply an active component (Burgazzi, 2012).

When ADS-1 is actuated, two motor operated valves open and release heat via spargers into the IRWST. The ADS 1–3 gate valves provide low leakage and globe valve control the flow with specified opening time. The second and third stages of ADS system open with a programmed time delay and also release decay heat via sparger into the IRWST.

Fourth stage of ADS is the ultimate safety feature to depressurize the RCS and also arranged into two identical groups. Each group has a common inlet header connected to one of RCS hot legs and discharges separately into the associated RCS loop compartment directly to reactor containment. Each line of ADS-4 composed of an explosively opening valve (squib valve), and normally open motor operated valve in series. Once opened the squib valves cannot be closed again and stay open.

Table 2
Specific conditions of ADS system in LBLOCA for reliability analysis (Westinghouse Electric Company, 2009d).

ADS stages	Components	Conditions of four stages ADS system
ADS-1 stage (A/B)	V011A, V001A, V011B, V001B	V011A × V001A and V011B × V001B
ADS-2 stage (A/B)	V012A, V002A, V012B, V002B	V012A × V002A and V012B × V002B
ADS-3 stage (A/B)	V013A, V003A, V013B, V003B	V013A × V003A and V013B × V003B
ADS-4 stage (1/2)	V014A/B/C/D, V004A/B/C/D	V014A × V004A and V014B × V004B and V014C × V004 C OR V014A × V004A and V014B × V004B and V014D × V004D OR V014B × V004B and V014C × V004 C and V014D × V004D

Motor operated valves (MOVs) of ADS (1–4) are designed with different opening time and different size due to expected maximum differential pressure during opening and closing of valves in the reactor coolant pressure boundary. In Table 1, the size and opening time of ADS (1–4) valves are given with flow area and design pressure for opening and closing of each valves. The large size of the ADS-4 valves eliminates the possibility of leakage and provides highly reliable actuation. The ADS system automatically actuated with coincident core makeup actuation and low level-1 and low level-2 of CMT signals by PMS. In the event of CMT failure, or when automatic actuation fails, then ADS is initiated by operator action from the main control room (MCR) by DAS. Manual actuation of stage 4 via the DAS bypasses the RCS pressure interlock. The actuation signals for ADS system are also given in Table 1 (Westinghouse Electric Company, 2009a).

5. Reasons of why four stages ADS system are added in AP1000

The ADS system is a unique safety feature of AP1000 to be compared with the active safety systems of conventional PWR and is added in AP1000 to release the pressure from RCS system in controlled fashion and enables all safety injections into the reactor

Table 3
Functional time of ADS system during LBLOCA (Westinghouse Electric Company, 2009d).

ADS blow-down phase during LBLOCA			
Stages of ADS system	Detecting device (sensors, Timer)	Actuation time of ADS stages (s)	Time (s) from LOCA
ADS stage 1	CMT water level sensor	20 s after 67.5% liquid volume fraction in CMT	750–3600 s
ADS stage 2	Time delay defined by timers	70 s after ADS-1 actuation	820–3600 s
ADS stage 3	Time delay defined by timers	120 s after ADS-2 actuation	940–3600 s
ADS stage 4A/B/C/D	Time delay defined timers	20.0% liquid volume fraction in CMT and 551s after ADS3 actuate	1491–3600 s

Table 4
Component data of ADS system assigned in GO-FLOW analysis.

ADS system stages and water sources	Components of ADS system	Components failure mode of ADS system	Success probability (/demand)	Failure rate (s)
ADS stage-1	MOVs (V001A/B, V011A/B)	Failure to open on demand	Pg = 0.9781	1.00×10^{-5}
ADS stage-2	MOVs (V002A/B, V012A/B)	Failure to open on demand	Pg = 0.9781	1.00×10^{-5}
ADS stage-3	MOVs (V003A/B, V013A/B)	Failure to open on demand	Pg = 0.9781	1.00×10^{-5}
ADS stage-4	MOVs (V014A/B/C/D)	Failure to remain open on demand	Pg = 0.98	1.00×10^{-5}
ADS stage-4	Squib valves (V004A/B/C/D)	Failure to open on demand	Pg = 0.99	1.00×10^{-4}
Pressurizer	Pressurizer tank	Failure due to leakage	Pg = 0.99999	1.00×10^{-5}
HOT leg	HOT leg (steam water source)	Failure to ruptured	Pg = 0.999	1.00×10^{-6}

vessel for long-term core cooling in events of transient or severe accidents. Especially for LOCA accident's depressurization of the primary circuit is imperative by ADS system due to reason that, at the time of the accident the mass and energy are lost, and decay heat removed through the break point, and degree of RCS depressurization is somewhat smaller provided by break flow. Therefore, ADS operation allows the continued cooling and RCS depressurization to the pressures at which the gravity injection systems or normal residual heat removal system (NRHRS) can operate to maintain the core cooling. The ADS is crucial to manage the LOCA safety in AP1000.

As the PXS and PCCS are passive safety systems and their successful actuation ensured on the reduced setpoint values of RCS pressures, which are controlled by ADS system. The gravity injection starts from IRWST until RCS pressures should reduce enough to 89.6 kPa.

Without depressurization safety injections into the core could not be guaranteed because of the large pressure difference between reactor vessel and water resources. And three general levels of overpressure control systems such as, secondary side heats removal, passive residual heat removal, and pressurizer safety valves are not enough to remove the decay heat and reduce the RCS design pressure for all safety injections should be started at the required time. When ADS depressurization fails, the coolant temperature may reach to saturation temperature and boiling start and steam bubble might form in the reactor pressure vessel. The fuel elements might not be covered with water anymore. This situation leads to dangerous state of reactor safety because of reason that if the core remains uncovered for a considerable period of time, then fuel rod temperature will increase, which may eventually lead to significant and irreversible core degradation.

The ADS valves act in conjunction with PXS to mitigate accident and allow the required safety injection from accumulators, CMTs and IRWST and recirculation sump. ADS is important in aspect of reliability evaluation of PXS of AP1000 plant to be compared with reliability results of the emergency core cooling system (ECCS) of conventional PWR, because ECCS system has no such ADS system and composed of active safety components such as pumps and MOVs.

5.1. Full and partial depressurization of RCS system by ADS system

Full depressurization of RCS system is the reduction of system pressure to sufficient values (89.6 kPa) such that gravity injection can be initiated from IRWST and recirculation sump by injection path-1 for long-term core cooling as shown in Fig. 3 (Kamyab et al., 2010). When reactor pressure decreases to less than that of IRWST water pressure then water will flow from IRWST to reactor vessel due to gravity potential difference. In case of LBLOCA accident, only full depressurization is vital for urgent core cooling because the CMT injection is not sufficiently rapid to prevent core damage and injection from accumulators is also necessary. The success criteria for large LOCA require for successful actuation of CMT, automatic ADS and IRWST injection to accommodate the most limiting failure. Switchover from injection to recirculation is automatic when RCS pressures reduced to 44. 75 kPa at the low-level water signal of IRWST and is transmitted to require actuating components in recirculation mode.

In other hands, partial depressurization mode is the reduction of RCS pressure to such sufficient required value to allow the NRHRS operation by path-2 but not gravity injection from IRWST (see Fig. 3). If the automatic and manually actuation of CMT fails to actuate and IRWST injection line squib valves fail to open, then operator can manually initiate RCS depressurization with the ADS and initiate NRHRS injection. When IRWST low-3 level setpoint is reached and coincident with an ADS system actuation signal then normal closed MOVs/squib valve flow path and check valve/squib valve flow path are open to provide recirculation flow from sump for long term cooling.

These two injection flow paths are designed to have redundancy complying with the single failure criteria for core cooling of AP1000 during the accidents. Where one method is taken as passive (automatically open → path-1) while other method works as an active system (manually actuate → path-2) as shown in Fig. 3.

AP1000 PRA model required different success criteria of ADS system (ADS lines' configuration) to manage the full and partial RCS depressurization in event of transient and different size of LOCA accidents. The AP1000 PRA model does not credit operation of NRHRS to mitigate LBLOCA, since the system may be isolated because of high containment radiation. These lines' configurations of ADS system are used for partial and full depressurization of RCS by seeing the ON and OFF status of CMT and PRHRS (Westinghouse Electric Company, 2009c).

6. Application case of AP1000 ADS system for reliability evaluation

In this section, the application case study of four-stage ADS system has been conducted in the aspect of reliability analysis of ADS

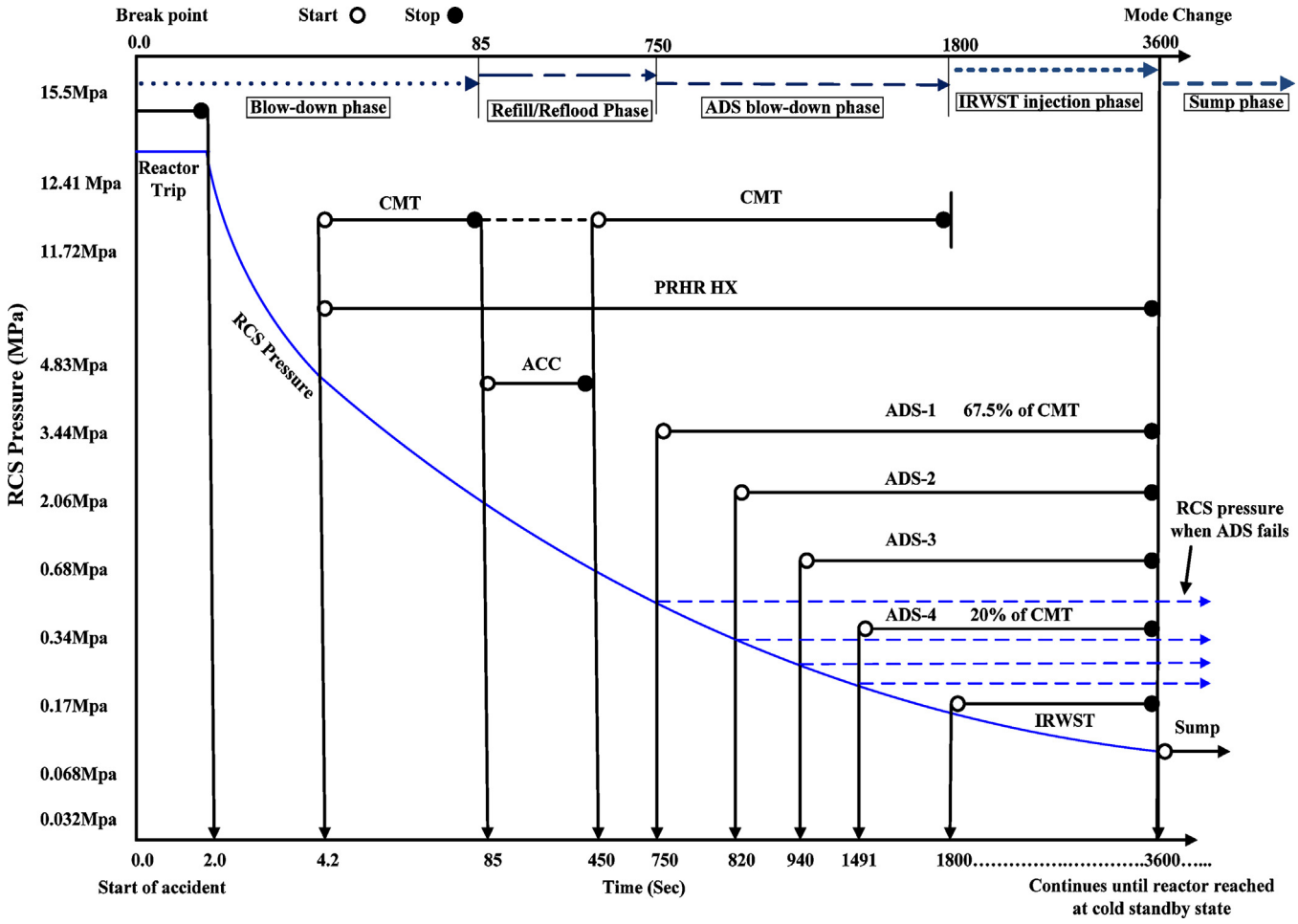

Fig. 4. Transient behavior of AP1000 PXS system during LBLOCA.

system under the specific conditions for full RCS depressurization during LBLOCA accident. And analysis is made in order to determinate the influence of ADS system in the reliability evaluation of AP1000 PXS system. "That is what will happen in the AP1000 plant system when ADS system fails or successfully actuate". The postulated specific conditions of ADS for full RCS depressurization are given in Table 2 and are taken on assumptions base of LBLOCA at one of four cold leg of RCS system as an initiating internal event of failure. If the break point location and size changed, then the conditions (values) of temperature and pressure of RCS system will be different for the actuation of ADS system including other subsystems of PXS and in this situation core cooling evolution might also be changed.

6.1. Failure modes of ADS components for reliability analysis

The basic step of reliability evaluation of passive safety systems of AP1000 is the identification of all relevant potential failure modes of safety components that affecting the system operation. From the research study of AP1000 (Hashim et al., 2013b), it has been observed that passive safety components particularly depend on two types of failure modes to be considered for the reliability evaluation of passive safety systems of AP1000 power plant.

"Type A failure" caused by structural failure (hardware failure), and physical degradation and "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 (gravity-fed water injection, heat transfer by natural convection, etc.) or inherent characteristics (Lorenzo et al., 2005). The identifications of these two types (A & B) of failure modes concern both mechanical components (valves, piping, heat exchanger) and natural phenomena (mainly sustainability of natural circulation in the flow passage), as "virtual" component (phenomenological). The qualitative analysis (Failure Mode and Effect Analysis: FMEA) detects the potential failure modes affecting the system, and their consequences associated with passive system operation. The purpose of such analysis is to identify the critical parameters for natural circulation performance/stability, allowing associating to each of failure modes a proper parameter direct indicator of the failure causes (David, 2013).

The potential failure modes for all AP1000 ADS system components (as shown in Table 4) and critical parameters, which can impair or hinder the natural circulation are identified in the qualitative reliability analysis by qualitative technique FMEA (Hashim et al., 2014) in aspect of both types of failure modes. These types of failure modes of ADS system are taken for quantitative reliability evaluation of ADS systems by GO-FLOW.

6.2. Function of ADS system during LBLOCA

To understand the function of ADS (1–4) system during the LBLOCA, schematical model of four stages (1 to 4) ADS system's components is indicated in Fig. 3. In this model, the instrument and control system (I & C) of ADS system indicated for the actuation signals which are transmitted to ADS-1 to 3 at first low level-1 of CMT water fraction 67.5% and then to ADS-4 at second low

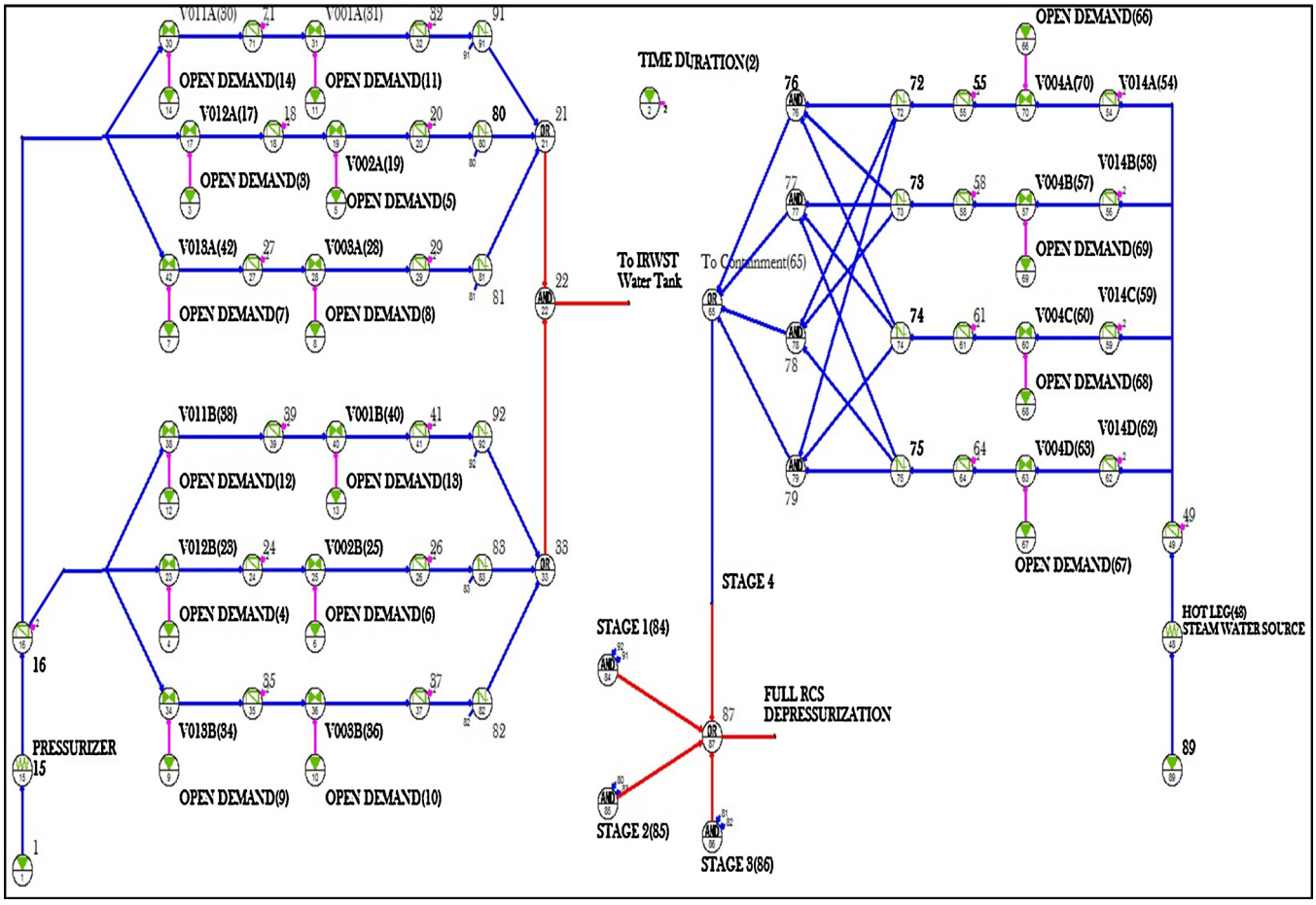

Fig. 5. GO-FLOW chart of ADS system of AP1000.

level-2 of CMT water fraction 20%. These signals are sent through PMS system and DAS system in case of manual actuation.

After a LBLOCA occurred in the cold leg, the mass and energy loss from the break point and primary system undergoes depressurization. Reactor scram signal generated at low pressurizer pressure setpoint (12.41 MPa) and core thermal power falls rapidly to the decay heat level with the effect of shutdown rods. The safety system actuation signal "S" activated at low-low pressure setpoint (11.72 MPa) of pressurizer which causes the opening of CMT and PRHR-HX isolation valves. Following the actuation of CMTs and PRHR-HX, two natural circulation flow paths are established immediately after the accident through which the core decay heat is removed effectively. The steam (i.e., hot liquid from cold leg) which circulates through the cold leg balance (inlet of CMT) collects at the top of the CMT, and CMT injects cold borated water into RCS through the DVI line as a result of gravity-driven natural circulation. The PRHR-HX is located above RCS system provide inlet and outlet pressure difference by free convection in IRWST, which drives the RCS coolant flow from one hot leg, through the PRHR HX, and back into its associated steam generator outlet plenum and cold leg.

The water level in CMT drops continuously and thus controls the action of four stages of ADS valves. When the water level of CMT dropped to 67.5%, then MOVs V001A/B and V011A/B open gradually at 750.0 s in the ADS-1 depressurization lines. Later on, the ADS-2 and ADS-3 valves V002A/B, V012A/B and V003A/B, V013A/B are actuated sequentially after certain time delay defined by timers following the opening of previous stage of depressurization valves. After the liquid level falls below 20%, the ADS-4 squib valves V004A/B/C/D open and primary liquid vents directly to containment with a time delay of 551 second after opening of ADS-3. During the ADS-4 depressurization process, large amount of coolant may be entrained through the branch line, which can affect the branch quality and the depressurization process dramatically and this situation has been not considered in present study as time being. And ADS-4 stage actuation permits the gravity drain of IRWST automatically into the reactor vessel to provide core cooling until equilibrium is reached.

Normally, after LBLOCA, the decay heat is removed through four flow paths such as: break point, steam generator, PRHR HX and CMT recirculation flows. When RCP trips after a short delay, then primary system is cooled by natural circulation flow paths. If any natural circulation flow paths (CMT and PRHR-HX) reduce (fails due to any reasons) to remove the decay heat, then actuation timing of ADS valves will change and, which may also change the core evaluation.

After the accident, the steam discharges into the containment due to continues operation of depressurization system and also results in automatic actuation of passive containment cooling system (PCCS) for several hours. In the present case study, the functions of I & C system are considered successfully to operate during the accident, and it is included the pressure detecting sensors to detect the RCS pressure value and water level sensor in CMT to judge the low water level and timers (triggers) in ADS 1–3 to transmit the time-delay signals to next ADS stage as shown in Fig. 3. ADS system works from 750 to 3600 s after the accident in ADS blowdown phase of LBLOCA phases (Hashim et al., 2013b) until the time of IRWST becomes an empty and recirculation sump injection start for long term cooling. This is functional time of ADS (1–4) system for LBLOCA in one of RCS cold leg.

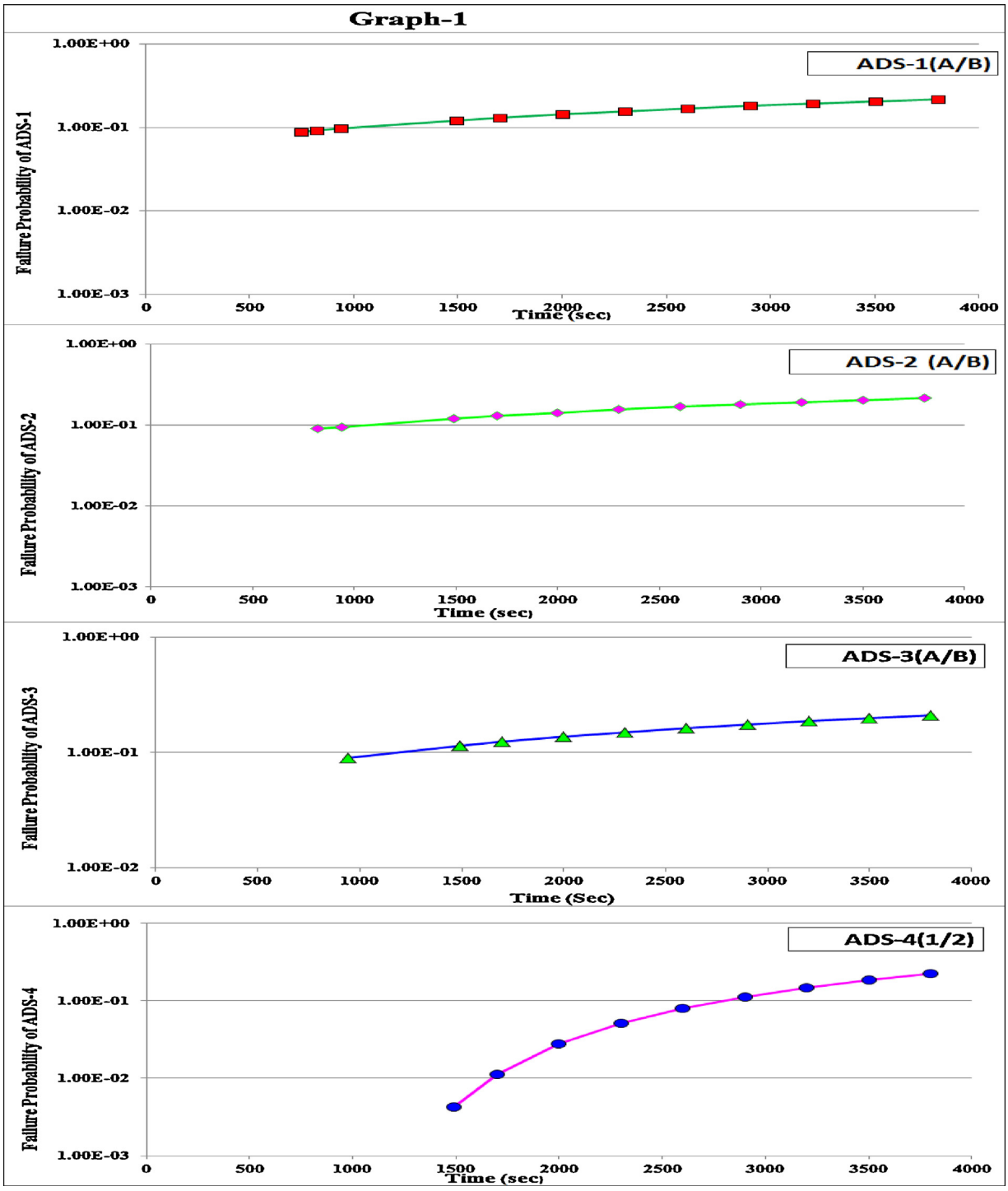

Fig. 6. Failure probability results of individual ADS stages (1–4).

The functional and actuation time of ADS system is given in Table 3 with detecting devices (sensor & timer, etc.). The transient behavior of damage plant by LBLOCA is assumed to be successful sequence of (i) reactor shutdown systems, (ii) and all safety injection systems (subsystems of PXS such as: CMT, ACC, PRHRS, IRWST, Sump) as shown in Fig. 4 (Westinghouse Electric Company, 2009e).

The transient analysis is reduced on the base of AP1000 accident analysis reports and research papers, which is conducted by RELAP5 and Westinghouse-developed LOCA analysis code NOTRUMP (Wright, 2007; Frepoli et al., 2004; Banerjee et al., 1998). On the base of this transient behavior of PXS of AP1000, authors of this study have characterized the LBLOCA accident into six distinct phases such as: (i) blow-down phase, (ii) refill phase, (iii) reflood phase, (iv) ADS blow-down phase, (v) IRWST gravity injection phase, and (vi) recirculation sump phase for long term cooling (Yang et al., 2012). These phases are taken with respect to change in RCS pressure and temperature by the passage of time after LOCA occurred and activation timing of safety injection systems, including ADS system.

The state of components such as “start” and “stop” are indicated by different dots and time intervals as shown in Fig. 4. The detail description of all these LOCA phases has been explained in the

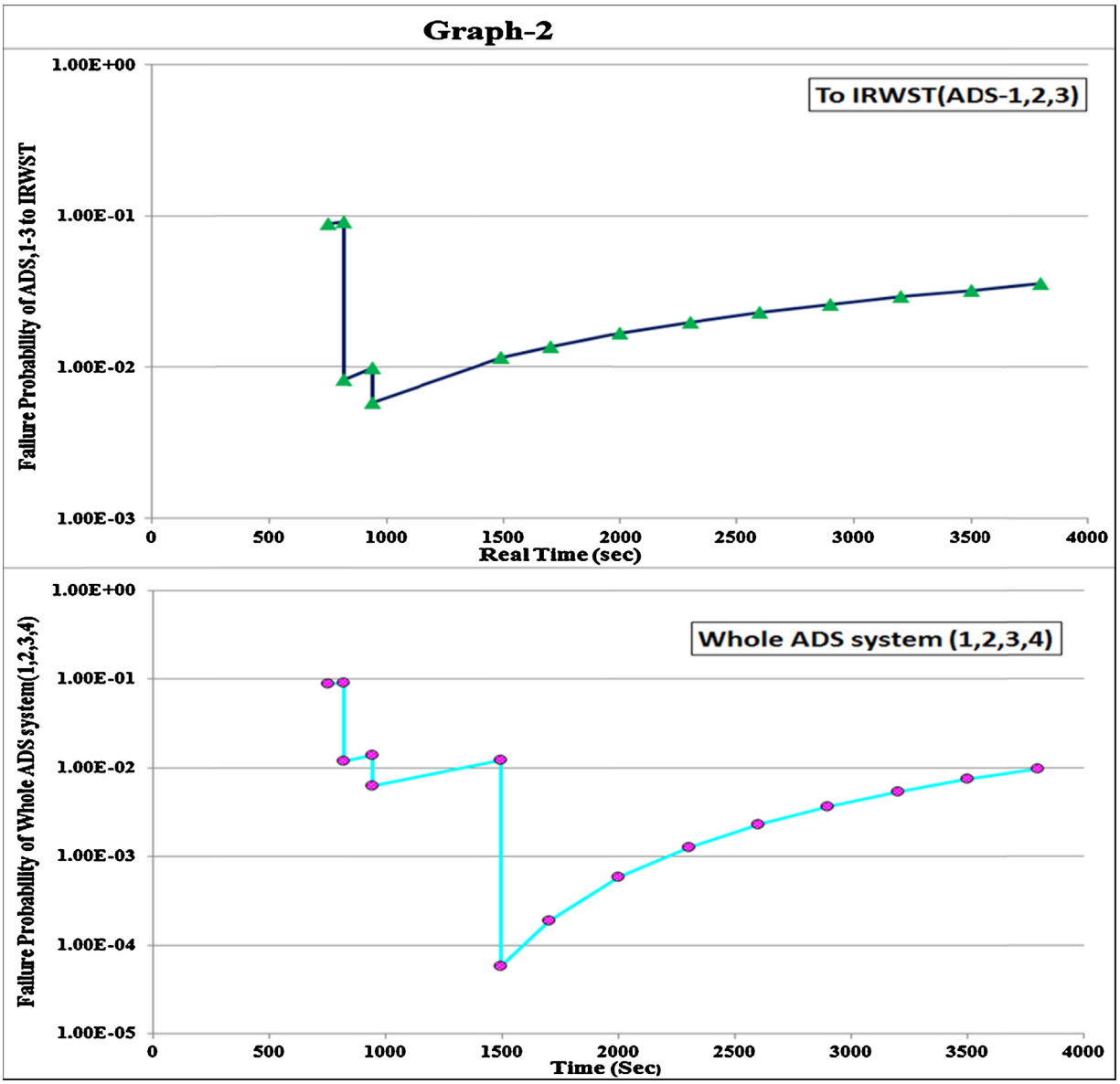

Fig. 7. Failure probability results of ADS (1–3) to IRWST and whole ADS system (1–4).

presented papers (Hashim et al., 2013a,b). The behavior of RCS pressure is shown by four dotted blue colored lines when ADS 1–4 fails one by one. If ADS-1 fails, then ADS-2 to 4 fails, which causes the failure of IRWST and recirculation sump injections into the reactor vessel for long term cooling. Similarly, failure of ADS-2 or 3 cause the same effect.

6.3. GO-FLOW analysis of ADS system

From the viewpoint of implementation of GO-FLOW methodology in presented study, the GO-FLOW method has been implemented for various purposes as described in Section 2 for active safety systems in different fields. But in the recent days, first time researcher have implemented the GO-FLOW method in their research work in order to conduct the quantitative dynamic reliability evaluation for passive safety system that undergoes different phases during their functioning (phased mission system).

And also there are many factors leading to disturbance in the function of passive safety systems of AP1000 which leads to point out two types of failure modes in reliability analysis (as discussed in Sections 6.1 and 3). So it will be innovative to make the reliability evaluation of passive safety system by new method GO-FLOW. The GO-FLOW analysis in the present study has been deduced from the previous research work, where dynamic reliability has been conducted for whole model of PXS and PCCS of AP1000, including their reliability result's inter-comparison with that of active safety systems (Hashim et al., 2012–2014).

The GO-FLOW chart of four stages ADS system is shown in Fig. 5. Where the components of ADS system are presented by suitable operators, and the names of each component is indicated on the side of corresponding operators. Output failure probability results of ADS-1, 2, 3 and 4 stages are represented by operators 84, 85, 86 and 65 respectively. The total failure probability results of first three stages to IRWST and all four stages of ADS are shown by operators 22 and 87. All closed motor operated valves of ADS stages (1 to 4) are given subinput signals in order to open the ADS valves according to actuation time of each stage.

Time duration for the function of ADS system is indicated by operator 2. There are seventeen time points were declared for complete function of ADS system from time 750 to 3600 s. Time point 1

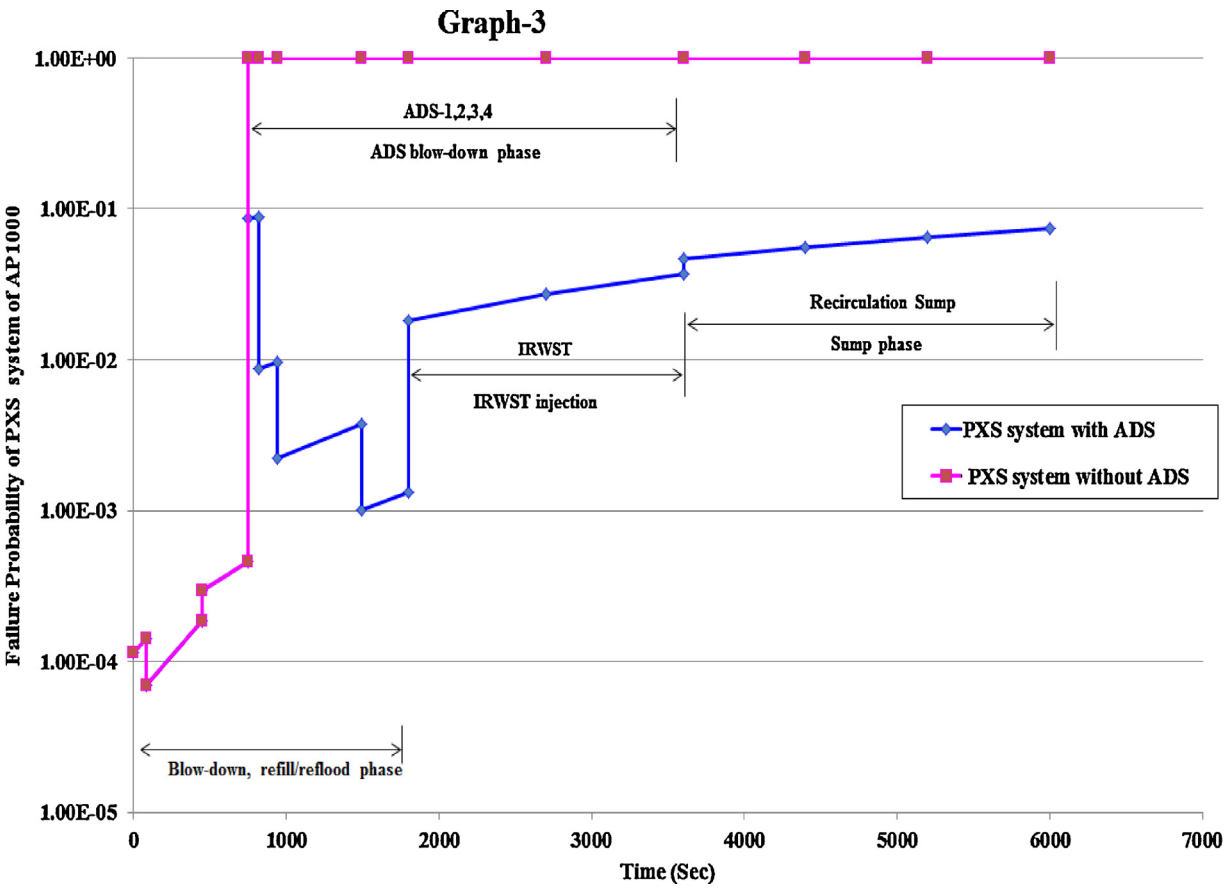

Fig. 8. Failure probability of PXS of AP1000 when ADS system fails and successfully actuate.

is an initial time and at time point 2, the system operation of ADS-1 is demanded and continued to 17 time points until the end of analysis. The operators 1 and 89 are signal generators, and their output signals represent the water flow; time period between successive time points, and demand signal to start the system operation. There are also AND & OR logic gate operators who represent the successful operation of ADS system.

The values of component failure data assigned in this GO-FLOW analysis are furnished in Table 4. The failure data consists of successful probability/demand and failure rate/second of ADS components. This date has been collected from the literature documents of probabilistic safety assessment (PSA) of AP1000 for LOCAs accident (Westinghouse Electric Company, 2009f,g).

6.4. Discussion on reliability results of ADS system of AP1000

Failure probability results of AP1000 ADS system conducted by GO-FLOW method explained in Figs. 6–8. Where the calculated results are presented comprehensively in three different graphs for the individual ADS stages (1–4), total of first three ADS stages (1–3) to IRWST and for whole ADS system (all stages). These failure probability curves are drawn against the real time taken over the function of ADS system of AP1000 during LBLOCA. The failure probability results of ADS 1–4 increases slightly with the passage of time due to higher failure probability of ADS motor operated valves and squib valves. And the difference in failure probability results of four stages is only in their starting point because ADS 1–4 actuate from 750 s, 820 s, 940 and 1491 s respectively.

But failure probability results of first three stages of ADS are different from 4th ADS stage because of different flow capacity and opening time of valves (as given in Table 1). The total failure probability results of first three stages (Graph-2) to IRWST decreased due to redundancies of lines of three stages as shown in Fig. 7.

And similarly, the failure probability result of whole ADS system decrease rapidly and are very smaller than that of all individual ADS stages. These failure probability results indicate the behavior of only ADS system for full RCS depressurization during the large breaks LOCA accident.

Now, let's discuss the influence of ADS system in the reliability evaluation of the passive core cooling system of AP1000 in LBLOCA accident, i.e. when ADS fail or successfully actuate. The reliability results for the PXS of AP1000 are shown in Fig. 8 (Graph-3). Where the failure probability results are displayed according to LOCA phases, including ADS blow-down phase. These GO-FLOW results of PXS system have been conducted in detail in the author's presented paper (Hashim et al., 2013b). From Fig. 8, it can be seen that the successful actuation of ADS system increases the dynamic reliability of PXS of AP1000 plant and is essential to enable the injection from subsystems of PXS such as: ACC, IRWST, and recirculation sump, etc., into the reactor vessel by reducing the RCS pressure until their actuation setpoint values achieved.

The failure probability results of 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 the blow down phase to ADS blow-down phase are due to different actuation time of ADS stages (1–4) because ADS 2–4 stages actuate sequentially after the programmed time delay.

In this ADS system's conditions, the failure probability of PXS system sometime increased stepwisely in the very small interval

of time at the starting point of ADS 1–3. It may be due to the failure of I & C components and due to dependability of the failures of triggering ADS 1 to ADS 4. PXS system is temporally in failed state and then goes back to success state very quickly. And this temporally failure does not affect to the safety of the power plant system due to successfully opening of ADS (1–4) valves reduced the RCS pressure in the controlled manner until the safety limit and enable the quick injection from IRWST and recirculation sump for long term cooling. In the failure case of four-stage ADS system, failure probability of the passive core cooling system of AP1000 reached at its high values because the injection from IRWST and recirculation sump stop without ADS system.

Thus, the calculated reliability results of whole ADS system conducted by GO-FLOW indicates that the ADS is an important safety system of AP1000 to reduce the reactor coolant pressure and accomplish the core cooling successfully in the LOCAs accidents. The ADS originally work as an active safety system for full and partial depressurization of RCS to help safety principles of water injection into the reactor vessel.

This application case study of ADS system is conducted under the specific conditions of LBLOCA for RCS depressurization to determinate the influence of ADS system in the dynamic reliability of AP1000 plant. Aside from reliability evaluation of ADS, it is necessary for safety evaluation to consider what will be the situation when four-stage ADS fail in different LOCAs situations. Although it is not treated in this paper, it is necessary to evaluate the problem of “IF FAILURE, THEN WHAT HAPPEN” and then “WHETHER OR NOT ANY COUNTERMEASURE”. This kind of safety evaluation for AP1000 together with common mode failure analysis and uncertainties in the reliability assessment of ADS system will be conducted in the future study by GO FLOW methodology.

7. Conclusion and future work

In this study, authors discussed the application case study of four-stage automatic depressurization system (ADS) of AP1000 in the aspect of reliability evaluation of passive safety systems of AP1000 NPP. The four-stage ADS system is the unique safety system of AP1000 to be compared with active safety systems of conventional PWR. The discussion of this paper started first from the brief description of safety systems of AP1000, explanation of GO-FLOW methodology, and configuration and reasons of adding four-stage ADS system in AP1000 were also explained. And then full and partial depressurization of RCS system was discussed by four stages ADS in events of transient and LOCA accidents.

Finally, application case of four stages ADS system of AP1000 was studied for reliability evaluation by GO-FLOW methodology utilized alternatively to Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) tools in order to determinate the influence of ADS system in dynamic reliability of AP1000 PXS system. For this, the specific conditions were postulated for full RCS depressurization by ADS system under the LBLOCA accident in the cold leg.

In this application case study of ADS system, the GO-FLOW calculated reliability results indicated that ADS is a key safety system of AP1000 NPP to reduce RCS pressure in controlled fashion and enables the all safety injections for automatic core cooling successfully after the accident. And dynamic reliability of the passive core cooling system of AP1000 plant is increased by the successful actuation of ADS system. Because the failure probability of PXS reached its high value if ADS system fails, and automatic injection from IRWST and recirculation sump is not possible without ADS system. Thus, by this application case study, it is pointed out, that high reliability of the passive safety system of AP1000 would depend on the full reliability of ADS system that it would work surely when needed. And the GO-FLOW methodology can be used with its advance function to evaluate the dynamic reliability of passive safety systems of AP1000 which change changes their operation with time (phased mission system).

Aside from reliability evaluation of ADS, it is necessary for the safety evaluation to consider what will be the situation when four-stage ADS fail in different LOCAs situation (with full and partial depressurization). Although it is not treated in this paper, it is necessary to evaluate the problem of “if failure, then what happen” and then “whether or not any countermeasure”. This kind of safety evaluation for AP1000 together with common mode failure analysis and uncertainties in the reliability assessment of ADS system will be conducted in the future the study by GO FLOW methodology.

Acknowledgment

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

Banerjee, S., Ortiz, M.G., Larson, T.K., Reeder, D.L., 1998. Scaling in the safety of next generation reactors. Nucl. Eng. Des. 186, 111–133.
Burgazzi, L., 2004. Evaluation of uncertainties related to passive systems performance. Nucl. Eng. Des. 230, 93–106.
Burgazzi, L., 2012. Reliability of passive systems in nuclear power plants. http://dx.doi.org/10.5772/47862 (accessed 06.08.13).
David, M.L., 2013. Failure Modes and Effects Analysis. Tyco Electronics Corp dmlittle@tycoelectronics.com (accessed 20.11.13).
Frepoli, C., Ohkawa, K., Kemper, R.M., 2004. Realistic large break LOCA analysis of AP1000 with astrum. In: The 6th International Conference on Nuclear Thermal Hydraulics, Operations and Safety.
Hashima, M., Yoshikawa, H., Yang, M., 2013a. Addressing the fundamental issues in reliability evaluation of passive safety of AP1000 for a comparison with active safety of PWR. Int. J. Nucl. Safety Simulat. 4 (2), 147–159.
Hashimb, M., Yoshikawa, H., Matsuoka, T., Yang, M., 2014. Quantitative dynamic reliability evaluation of AP1000 passive safety systems by using FMEA and GO-FLOW methodology. J. Nucl. Sci. Technol. 51 (4), 526–542.
Hashim, M., Yoshikawa, H., Matsuoka, T., Yang, M., 2012. Dynamical reliability analysis for ECCS of pressurized water reactor considering the large break LOCA by GO-FLOW methodology. Int. J. Nucl. Safety Simulat. 3 (1), 81–90.
Hashim, M., Yoshikawa, H., Matsuoka, T., Yang, M., 2013b. Reliability monitor for PWR safety system using FMEA and GO-FLOW methodology-Application of risk monitor for nuclear power plants. In: Proceeding of the 21st International Conference on Nuclear Engineering (ICONE21), Chengdu, CHINA.
Kamyab, S., Nematollahi, M., Jafari, A., 2010. Evaluating the reliability of AP1000 passive core cooling systems with risk assessment tool. In: International Multi Conference of Engineers and Computer Scientists (IMECS), Hong Kong.
Lorenzo, P., Pagani, George, E., Apostolakis, Pavel, H., 2005. The impact of uncertainties on the performance of passive systems. Nucl. Technol. 149, 129–140.
Matsuoka, T., Kobayashi, M., 1988. GO-FLOW: a new reliability analysis methodology. Nucl. Sci. Eng. 98, 64–78.
Mo, Y., Liu, H., Yang, X., 2007. Efficient fault tree analysis of complex fault tolerant multiple-phased systems. Tsinghua Sci. Technol. 12 (1), 122–127.
Schulz, T.L., 2006. Westinghouse AP1000 advanced passive plant. Nucl. Eng. Des. 236, 1547–1557.
Shahabeddin, K., Mohammadreza, N., 2012. Performance evaluating of the AP1000 passive safety systems for mitigation of small break loss of coolant accident using risk assessment tool-II software. Nucl. Eng. Des. 35, 32–40.
US Nuclear Regularity Authority: USNRC, 1981. Fault Tree Handbook, NUREG-0492, Washington, D.C. 20555.
Westinghouse Electric Company, 2009a. AP1000 Pre-Construction Safety Report. UKP-GW-GL-732 Revision 2.
Westinghouse Electric Company, 2009b. Reactor coolant system and connected systems, chapter 5. AP1000 design control document.
Westinghouse Electric Company, 2009c. Probabilistic risk assessment, chapter 19. AP1000 design control document appendix 19B.
Westinghouse Electric Company, 2009d. Probabilistic risk assessment chapter 11. AP1000 design control document.

Westinghouse Electric Company, 2009e. Engineered safety features, Chapter 6. AP1000 design and control document, Revision 1.
Westinghouse Electric Company, 2009f. Probabilistic safety assessment chapter 32. AP1000 design control document.
Westinghouse Electric Company, 2009g. Accident analysis chapter 15. AP1000 design controls document, Revision 14.
Wright, R.F., 2007. Simulated AP1000 response to design basis small-break LOCA events in APEX-1000 test facility. Nucl. Eng. Technol. 39 (4), 287–298.
Xing, L., Dugan, J.B., 1999. Reliability Analysis of Static Phased Mission Systems with Imperfect Coverage. Department of Electrical Engineering University of Virginia.
Yang, J., Wang, W.W., Qiu, S.Z., Tian, W.X., 2012. Simulation and analysis on 10-in. cold leg small break LOCA for AP1000. Ann. Nucl. Energy 46, 81–89.