Time dependent reliability analysis for a critical reactor safety system based on fault tree approach

Ahmad Hassan¹,a), Zahira Mokhtar¹, Mazleha Maskin²

¹Faculty of Applied Sciences and Technology, Universiti Tun Hussein Onn Malaysia, 86400 Muar, Johor, Malaysia.
²Malaysian Nuclear Agency (Nuclear Malaysia), Bangi, 43000 Kajang, Selangor, Malaysia

a)hassan@uthm.edu.my

Abstract. Loss of coolant in the operation of any nuclear power plant will eventually become the primary source of hazard in the sequence of events leading to reactor core uncover. Subsequent failure in removing the nuclear decay heat and preventing the core uncover will further lead to loss of coolant accident (LOCA). In conjunction to this safety concern, it is crucial that the reliability of the plant emergency core cooling system is systematically and critically assessed. This article presents a case study on the time dependent reliability analysis for a safety injection system (SIS) of an advanced pressurized water reactor, based on the failure mode and effect analysis (FMEA) and fault tree (FT) analysis approach. The identified generic data for component reliability are carefully reviewed and used in this study. Based on the base case model, sensitivity and importance measure analysis for basic events are performed and the outcomes gained are presented and discussed. From the analysis, it is shown that the safety injection pumps of the SIS contribute significantly to the reliability of the system. In the short (at 0.5 hour) and long (7.0 hours and 72.0 hours) run, safety injection pumps are critical and influence the reliability of the SIS the most. The SIS’s FT logic model that has been developed and calculated shows the usability of the FMEA and FT approach that are implemented in analysing SIS time dependent reliability.

1. Introduction
The history of nuclear power has expanded almost nearly a century and within this timeline, the world has witnessed the raise and decline of its demand. Among many other factors to this declination is the safety issues, that were usually seen argued and discussed intensively after the occurrence of major accident at a nuclear power plant. On March 2011, Fukushima Daiichi Nuclear Power Plant marked another history of nuclear disastrous event.

The safety of a nuclear power plant is analyzed as early as in the stage of reactor design, and after that are the design licensing, site selection, construction, commissioning and up to the decommissioning which involve and follow strict and stringent procedures. However, Fukushima event was so far an exception since the actual sequence of event that has propagated was complex, mainly due to the occurrences of multiple simultaneous initiating events. Since then, the nuclear safety community has initiated the efforts on considering such complex occurrence and it is to be carefully analyzed, especially by means of the probabilistic approach[1].

For the year of 2020, it is reported that the share of nuclear energy to the global primary energy generation is around 4.3%[2]. For any particular nuclear power plant, it is worth to realize that the
energy is originated from the fission in the nuclear fuel core. However, during any plant incidents that involve the loss of integrity at the primary coolant boundary, the core will eventually become the source of hazard in the anticipated sequence of events that lead to core uncovery. Failure in the recovery of primary coolant and preventing the core uncovery will lead to the sudden increase in the fuel cladding temperature, and thus damaging the fuel rods and fuel assemblies[3]. Thus, in every plant, a robust and reliable emergency cooling function must be critically designed and analyzed.

This article is about a case study on a time dependent reliability analysis of a safety injection system (SIS) of an advanced pressurized power reactor during post-large break loss of coolant accident (LOCA), performed based on fault tree (FT) analysis approach. Technically, this involves the familiarization of the system and definition of the accident scenario, failure mode and effect analysis (FMEA), FT modeling and FT quantification.

The next section of this article briefly the design feature of the Advanced Power Reactor 1400 (APR1400), and later the structure of SIS is explained in detail. The summary of large break LOCA accident phenomena that were analyze by others and the scope of analysis in the current study are addressed. In Section 3, the failure mode and effect analysis (FMEA) is explained. Mathematical fundamentals for the fault tree analysis are explained and the use of a computer software is addressed. For component reliability data, generic data available from literature are used. The result of this study is presented in Section 4. Based on the base case model, sensitivity and importance measure analysis are performed and the insights gained are further discussed. Finally, Section 5 summarizes the outputs and insights of the current study and recommendation for future studies are addressed as well.

2. Overview of APR1400 reactor and the safety injection system

The reactor that is considered in this study is the APR1400 reactor, which design evolved from the historic Korean Optimized Power Reactor 1000 (OPR1000) reactor[4,5]. The plant is an advanced plant, which was eventually granted the standard design certification by United States Nuclear Regulatory Commission (USNRC) in 2018[6], whereas long before that in 2001, by the Korean regulation authority[7]. As of in the middle of 2020, there are 2 APR1400 plants that have been connected to grid in Korea while 8 other plants are under construction in Korea and United Arab Emirates (UAE)[8].

The electrical power output of the reactor is 1450MWe while the thermal power output is 4000 MW. This thermal power which is generated inside the reactor pressure vessel (RPV) is transferred out via two coolant loops system. Each loop consists of one hot leg and two cold legs, one steam generator and two recirculation pumps. A pressurizer is connected to one of the hot legs. Major engineered safety features of the plant to cope with the severe accident are the auxiliary feedwater system (AFWS), containment spray system(CSS) and SIS[7]. As depicted in Figure 1, a single SIS train basically consist of an In-containment Refueling Water Storage Tank (IRWST), motor operated valves (MOV), check-valves (CV) and a Safety Injection Tank (SIT) [9]. For the APR1400, there are 4 SIS trains in total; 2 trains are connected to direct vessel injection (DVI) nozzles whereas the other 2 trains are designed with connection to both the DVI nozzles and the hot legs(HL), as shown in Figure 1[8]. The location of these DVI nozzles is above their respective cold leg connections on the RPV. It was reported that the small and medium break LOCA events contribute about 20.1% to the core damage frequency[10]. After the initiation of large break LOCA events, borated water from the IRWST is injected into the RPV with the safety injection pump (each with 50% capacity), and at the same time rapidly from the safety injection tank[11]. Meanwhile, for the long term cooling after a large break LOCA, borated water must be continuously injected into the RPV via the latter type trains i.e. Train 1A and Train 2B. To achieve the 100% pump capacity during this long term cooling, both of the trains must be available[10]. The reliability of this cooling function by the SIS is modelled and analysed in the next sections.
3. Methodology
FMEA involves the identification and screening of the relevant failure mode of the SIS’s subsystems and components and their effects on the defined functionality of the SIS during the post-large break LOCA long term cooling. These outcomes of FMEA are then arranged deductively as basic events or intermediate events, leading to top event of the intended FT model.

![Figure 1. Schematic diagram of the SIS (Train 1A) [8]](image)

Unavailability and unreliability share the same technical definition, except that the former usually used to refer to repairable type component[12]. Assuming that the time to failure, $t$ for most of the physical component follows the exponential distribution (constant failure rate), the time dependent unreliability, $Q(t)$ of a component is given by[13]:

$$Q(t) = 1 - e^{-\lambda t}$$  \hspace{1cm} (1)

$\lambda$ is the component failure rate which taken from available literature. To calculate the FT top event probability, the probability of components in a cut set are multiplied together, i.e.:

$$C_i(t) = \prod_{k=1}^{n_i} Q_k(t)$$  \hspace{1cm} (2)

$C_i(t)$ is the probability of the $i$th cut set, $n_i$ is the number of component in the $i$th cut set and $Q_k(t)$ is the probability (unreliability) of the $k$th components in the $i$th cut set at specific time $t$. The FT top event probability $Q_{top}$ is gained by adding together probability of the all $n$ cut sets[14]:

$$Q_{top}(t) = \sum_{i=1}^{n} C_i(t)$$  \hspace{1cm} (3)

Thus, $Q_{top}(t)$ represent the unreliability of the SIS for post large break LOCA long term cooling

In this study, the graphical construction and calculation of the FT is performed by using RISK SPECTRUM computer software[15]. The software generates cut sets for the constructed FT based on the gates used, simplifies the cut sets according to the Boolean rules for the generation of minimal cut sets (MCSs). The probability of each MCSs and the FT top event is calculated according to equation (2) and (3). Based on the base case model output, the Fussell-Vesely (FV) importance is performed to evaluate the fractional contribution of the basic events to the SIS failure[16] and the sensitivity of a generic operator recovery action the top event probability is analyzed.

4. Results and discussion
4.1. FMEA
The outcomes of FMEA for the active components in Train 1A are summarized in Table 1 below. Although not included in the table, the outcome of FMEA for Train 2B is similar to that of for Train 1A, due to the trains’ similarity. The success criteria for each train is: cooling water is injected into the PRV via DVI nozzle and the hot leg. These components’ reliability parameter (mean value) that was selected from NUREG/CR-6928[17], based on the description and failure mode are also included in the table. The unreliability of component with probability upon demand parameter is treated as $Q(t)=probability$ (constant).
4.2. SIS long term cooling fault tree
As notified in Section 2, the long term cooling after the large break LOCA requires continuous water injection by both Train 1A and Train 2B. Thus, with the outcome of FMEA in Table 1, failure of this function can be represented by the main FT shown in Figure 2. To keep the size of the main FT at a manageable size, the events under Train 2B are transferred to a separate FT. Although not presented here, the separated FT of the Train 2B is identical to Train 1A, identifiable in Figure 2 under the gate @SIS A1 & 2B-2.

Table 2 lists all the minimal cuts sets (MCSs) of events that can lead to the failure of post-large break LOCA long term cooling by the SIS at time \( t = 0.5 \) hour, with the top event unreliability \( Q(t=0.5) = 9.78E-3 \). The list is ranked by the cut set’s probability. None of the MCSs consist of multiple events. Thus, any single component failure event will directly prevent the SIS in reaching the prescribed success criteria. The top in the list (1\(^{st}\) and 2\(^{nd}\)) are the failure of safety injection pumps to start. After a sufficiently longer time i.e. 5.0 hours, the top in the list (1\(^{st}\) and 2\(^{nd}\)) are the failure of safety injection pumps to run (the MCS for list for \( Q(t=5.0) \) is not presented here).
Figure 2. FT for SIS long term cooling
Certainly, 72.0 hours) demonstrated a considerable degradation of the SIS during its mission and generic data. This study has performed in depth analysis, the reliability improvement. It is shown that the reliability of the SIS as function of time. At 72nd hours, the unreliability reaches approximately 6 times of the initial unreliability (complement to this, the reliability decreases). This is observed due to the reliability of the individual SIP1A and SIP2B, which decrease by time, whereas other components which remain with constant failure probability. Thus, it can be strongly suggested that other mitigating measure to recover the long term cooling such as operator recovery actions is worth to be considered.

4.3. Time dependent reliability

Figure 3 shows the unreliability increment of the SIS as function of time. At 72nd hours, the unreliability reaches approximately 6 times of the initial unreliability (complement to this, the reliability decreases). This is observed due to the reliability of the individual SIP1A and SIP2B, which decrease by time, whereas other components which remain with constant failure probability. Thus, it can be strongly suggested that other mitigating measure to recover the long term cooling such as operator recovery actions is worth to be considered.

4.4. IM and sensitivity analysis

In this current analysis, the definition of FV importance of a basic event is the ratio of reduced unreliability of the SIS when the basic event is completely reliable (i.e. no failure at all) to the base case unreliability. The output shows that the FV importance for both SIPs fail to run is 1 and this indicates that the reduction of the SIS unreliability is 100%, if both pumps are running without any failure. For other basic events, their values are less than 1.0E-3. Thus, the pumps are the dominant contributor to the failure of SIS. If human action with nominal performance (human error probability = 0.011[18]) is considered for the recovery of the system, for the total duration of 72 hours, the mean unreliability (obtained by integration and time averaging of $Q_{op}(t)$[15]) of the system decrease from 3.63E-2 to 3.99E-4. This considerably improve the reliability of the system and therefore it is crucial that the plant operators are well trained and prepared for wide range of reactor abnormal conditions.

5. Conclusion

This study has performed a time dependent FT analysis on the APR1400’s SIS for post-large break LOCA long term cooling. To this end, FMEA was inevitable for the systematic construction of the FT, and generic data originated from the similar industry have been adopted. It is shown that the reliability of the SIS degrades during its mission and mitigating measures such as human recovery actions demonstrated a considerable reliability improvement. In the short (at 0.5 hour) and long (7.0 hours and 72.0 hours) run, safety injection pumps are critical and influence the reliability of the SIS the most. Certainly, the total failure of the SIS must be followed by the next phase accident management that has
been carefully understood and planned. Even though the significance of safety injection pumps was considerably highlighted, the present study has omitted other important basic events such as human errors, electrical power failures, passive components (IRWST and SIT), instrumentation and control (I&C) failures as well as the common cause failure events from the consideration. In addition, the uncertainty values of the component reliability parameter were neglected. Therefore, these topics would be the concern of our future works toward the wider scope of system analysis under the standard framework of PSA.

6. References

[1] Kwag S, Ha J G, Kim M K and Kim J H 2019 Development of efficient external multi-hazard risk quantification methodology for nuclear facilities Energies 12 1–25.
[2] BP 2020 Statistical Review of World Energy 2020 | 69th edition
[3] Zinkle S J, Terrani K A, Gehin J C, Ott L J and Snead L L 2014 Accident tolerant fuels for LWRs: A perspective J. Nucl. Mater. 448 374–9.
[4] Lee S S, Kim S H, Suh K Y 2009 The design features of the advanced power reactor 1400 Nucl. Eng. Technol. 41 995–1004.
[5] Zubair M, Al Suwaidi R R and Al Souqi A A 2021 Behavior of Emergency Core Cooling System (ECCS) during the early stage of Loss of Coolant Accident (LOCA) for APR 1400 with Flownex software Prog. Nucl. Energy 141 103949.
[6] Shamsi A 2018 The Peaceful Nuclear Energy Program in the United Arab Emirates : Background and history Nucl. Law Bull. 2018 73–83.
[7] Kim H-G 2011 The Design Characteristics of Advanced Power Reactor 1400 ICONE-13, Beijing, China.
[8] KEPCO Engineering & Construction Company 2020 Status Report – APR1400 ( KEPCO E & C / KHNP ).
[9] Rezk O, Jung J and Lee Y 2016 Application of Reliability Centered Maintenance Strategy to Safety Injection System for APR1400 J. Korea Soc. Syst. Eng. 12 41–58.
[10] Yun J, Kim T and Kim J 2015 Verification of SAMG entry condition for APR1400 Ann. Nucl. Energy 75 404–12.
[11] Multinational Design Evaluation Programme 2018 MDEP Technical Report TR-APR1400-01
[12] Dutuit Y and Rauzy a. 2005 Approximate estimation of system reliability via fault trees Reliab. Eng. Syst. Saf. 87 163–72.
[13] Caldarola L 1977 Unavailability and failure intensity of components Nucl. Eng. Des. 44 147–62
[14] Rasmussen D M 1992 A comparison of the small and large event tree approaches used in PRAs Reliab. Eng. Syst. Saf. 37 79–90.
[15] Scanpower AB 2012 RiskSpectrum Analysis Tools Theory Manual.
[16] Van der Borst M and Schoonakker H 2001 An overview of PSA importance measures Reliab. Eng. Syst. Saf. 72 241–5.
[17] Eide S A, Wierman T E, Gentillon C D, Rasmussen D M and Atwood C L 2007 Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants
[18] Whaley A M, Kelly D L, Boring R L and Galyean W J 2011 SPAR-H Step-by-Step Guidance INL/EXT-10-18533.

Acknowledgement

This research was supported by the Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS/1/2019/TK05/UTHM/03/1).