FAILURE MODE AND EFFECT ANALYSIS OF PUSPATI TRIGA SYSTEMS: A PRELIMINARY STEP TOWARDS PSA LEVEL 1

Mazleha Maskin[1], Fedrick Charlie Matthew Brayon[2], Phongsakorn Prak Tom[3], Mohd Zulfadli Ramli[4], Ahmad Hassan Sallehudin Mohd Sarif[5]

[1,3] *Malaysian Nuclear Agency: Bangi, 43000 Kajang, City, Selangor, Malaysia, and mazleha@nm.gov.my*
[2,4] *Atom Malaysia: Bangi, 43000 Kajang, City, Selangor, Malaysia, and fedrick@atom.gov.my*
[5] *Universiti Tun Hussein Onn Malaysia: Pagoh Education Hub, 84600 Muar, Johor, and hassan@uthm.edu.my*

ABSTRACT

The PUSPATI TRIGA reactor (RTP), a vital component of Malaysia's nuclear research infrastructure, requires a robust safety assessment to ensure its reliable and secure operation. As a preliminary step towards conducting a comprehensive Level 1 Probabilistic Safety Assessment (PSA), this study focuses on the identification and analysis of failure modes and their effects across critical systems and components of the reactor. Failure Mode and Effect Analysis (FMEA) was utilized to systematically identify potential failure modes, assess their impact on reactor safety, and prioritize them based on severity, occurrence, and detectability. The findings highlight key vulnerabilities in reactor systems and provide insights into the relative risk contributions of each failure mode. This work lays the foundation for quantitative PSA Level 1 modeling, enabling the estimation of core damage frequency and guiding the development of targeted risk mitigation strategies. The results will support the enhancement of the reactor's safety framework and compliance with international nuclear safety standards.

Keywords: PUSPATI TRIGA, Failure Mode and Effect Analysis (FMEA), Probabilistic Safety Assessment (PSA), reactor safety, core damage frequency.

I. INTRODUCTION

In the Asia-Pacific region, growing nuclear research capacity brings a shared responsibility to ensure reactor safety is robust and well managed [1]. The devastating Fukushima disaster of 2011 reminded the world that even research reactors demand rigorous scrutiny – indeed, analysts observed that in its wake "the safety aspects of the one and only research reactor (31 years old) in Malaysia need be reviewed" [2]. This spirit of vigilance is especially important for Malaysia's sole nuclear facility: the PUSPATI TRIGA research reactor

Commissioned in 1982 as a 1-MW TRIGA Mark II reactor [3], the PUSPATI TRIGA (RTP) at Bangi has been a workhorse for Malaysian nuclear science and engineering. Over the decades it has supported neutron- beam experiments, neutron radiography, and the production of medical and industrial radioisotopes [3]. It also serves as a training and education platform for students and operators. As Malaysia's only research reactor, RTP occupies a strategic niche in the national nuclear landscape; its safe operation is therefore a matter of both technical and national importance.

Modern nuclear safety analysis employs both deterministic design rules and probabilistic methods. Probabilistic Safety Assessment (PSA) – sometimes called PRA – is now a standard tool used to quantify nuclear plant risk [4]. In a PSA model, a plant is systematically represented by its design and operating procedures, and a spectrum of possible "disturbances" (known as initiating events) is considered [4]. Each initiating event (for example, a pump failure or operator error) is then traced through the logic of the plant's safety systems and operator responses. The result is a comprehensive picture of accident sequences and their probabilities. In short, PSA asks "what can go wrong, how likely is it, and what is the end effect?" – yielding core-damage frequencies or radiological risk measures. Because PSA relies on having a complete set of initiating events, the accuracy of the risk picture depends critically on identifying all plausible beginnings of accident chains [4].

As according to the International Atomic Energy Agency (IAEA) [5], a powerful way to ensure completeness in initiating-event analysis is Failure Mode and Effects Analysis (FMEA). FMEA is a well-known bottom-up technique that examines each system component to ask "what can fail and what happens then" [6], [7]. In practice, engineers list each component or subsystem, enumerate its potential failure modes (e.g. "valve stuck closed"), and then trace the consequences of that failure on

larger subsystems and plant functions. By doing so, FMEA uncovers how individual hardware failures or human errors could serve as initiating events. As one authoritative source puts it, "FMEA can be used to determine the initiating events…which could lead to the hazard," by tracing individual failures forward to the final effect . In other words, FMEA complements PSA's top-down approach (often fault trees or event trees) by exhaustively finding bottom-up accident starters. For the RTP project, a systematic FMEA of its major systems reveal all potential component malfunctions and the hazards they could cause including human error [4], [8].

This paper's scope is a detailed FMEA of RTP's systems, covering relevant operational modes and core safety functions. Both full-power (steady-state) operation and shutdown/maintenance conditions are analyzed, as system dependencies and risks vary with reactor state. In each mode, we examine how failures would affect the reactor's fundamental safety functions, namely:

1. Reactivity Control: shutting down or controlling the chain reaction through control/safety rods and reactivity feedback.
2. Heat Removal: removing decay heat from the core via the primary cooling system and auxiliary cooling.
3. Radioactive Confinement: containing radioactive material through shielding and containment structures.

Each of these safety functions is supported by redundant components and protective systems (for example, multiple control rods and diverse cooling loops). Our FMEA traces how failures in pumps, valves, sensors, or operator actions in each system could disable these functions. By doing so, we enumerate the credible initiating events for RTP – the very inputs needed for a Level-1 PSA (core damage frequency calculation).

II. METHODOLOGY

The study utilizes existing documentation and system diagrams of the RTP to identify all critical components and functions. The systems and subsystems were carefully reviewed, with expert input from operators and engineers involved in the reactor's maintenance and operation. RTP has seven (7) safety systems, consisting of: (1) Reactor core and control system; (2) Primary cooling system; (3) Secondary cooling system; (4) Purification system; (5) Instrumental and control system; (6) Electric power supply; and (7) Auxiliary system.

II.A. Identification of Failure Modes

All RTP's safety related systems and components that can fail the system are identified. For each component, all possible ways of failure could happen then were identified next which is known as potential failure modes show a loss of that function. Failure mode is different for each component. TABLE 1 indicates an example of designator failure mode for each component.

TABLE 1. Failure Mode Designator

Component Type	Failure Mode
Pump and diesel generator (DG)	Fails to start [FS]; Fails to run [FR]
Valves	Fails to open [FO]; Fails to close [FC]
Equipment	Mechanical failure [MF]
Automatic signal	No signal [NS]
Operator action	Human error [HE]
Offsite power	No power supply [NP]

II.B. Identification of Consequences

For each failure mode, if the component fails, all the consequences on the system are identified. Eventually whether it is an IE or vice versa is then identified.

II.C. Human Reliability Analysis

In PSA, evaluation of the human factor contribution to the risk this is fulfilled under the framework of human reliability analysis (HRA) [9]. A Type A human errors (HE) happen before something goes wrong, during normal operations. These actions can cause important safety systems to be unavailable later when they are needed in an emergency. Type A HEs usually happen during tasks like repair, maintenance, testing, or calibration. If mistakes from these actions are not found and fixed,

they can cause system failure when needed. Type B HEs are mistakes that directly cause unwanted events, either on their own or along with equipment failure while Type C HEs are critical responses operators must take after an event has occurred. To support the current FMEA study, the focus is on the Type A and Type B HEs.

Routine (scheduled) human actions, done during normal conditions, can lead to Type A or B HEs. These actions are based on normal operating, testing, and maintenance procedures. Since the main purpose of a research reactor is to support research, procedures for research activities are also part of normal operations.

The written procedures at RTP for the following tasks are reviewed: i) Reactor startup, operation, and shutdown, ii) Loading, unloading, and moving fuel or irradiated materials, iii) Inspecting and testing safety-related items, iv) Setting up and running experiments. In addition, various technical documents - such as logbooks, maintenance/test reports, the Safety Analysis Report (SAR), system and component drawings, and vendor manuals for maintaining safety-related reactor systems are also reviewed. The procedures and documents are then checked by discussing and walking through them with the reactor operators. This helps confirm the information and gather more details, such as who does the task, the steps involved, how long it takes, any special tools needed, and the working environment. These details help in understanding the nature of the actions [10].

Following the identification of the routine human actions, qualitative screening is performed on these human actions. The purpose of qualitative screening is to select human actions with significant potential errors that could contribute to the system failure and initiating event (IEs).

III. RESULTS

TABLE 2 presents the lists of systems or components (SCs) with its failure mode and the consequences or effects to RTP if it fails to function properly. Each of the SCs was also noted as either to be a probable IE or not in the current scope of study. Of the seven systems with 98 related components involved, both failure mode and consequences were listed in this table.

Meanwhile, for HRA study, 88 tasks were identified, following the qualitative screening phase, two Type A HEs for the significant reactor systems during accident condition have been derived: i) area radiation monitor (ARM) system miscalibration during the maintenance (effect: ARM unavailable) and ii) erroneous dropping of foreign objects into the reactor pool (effect: degradation of SCRAM). Meanwhile, a HE which contributes to an accident initiation is identified: unintended insertion of sample with large positive reactivity influence is considered as the Type B HE (IE: reactivity insertion accident (RIA)).

TABLE 2. List of IEs and related systems and components in FMEA

No	System / Component	Failure Mode	Consequences / Effects	IE
A	Reactor Core and Control System			
1.	Motor Driven Safety Rod	Fail to Insert	Degradation of the System	Yes
		Spurious Withdraw	Reactivity Increase	Yes
2.	Motor Driven Shim Rod	Fail to Insert	Degradation of the System	Yes
		Spurious Withdraw	Reactivity Increase	Yes
3.	Motor Driven Regulator Rod	Fail to Insert	Degradation of the System	Yes
		Spurious Withdraw	Reactivity Increase	Yes
4.	Pneumatic Drive Transient Rod	Spurious Withdraw	Reactivity Increase	Yes
5.	Core Aluminum Tanks	Fail to Retain Integrity	Loss of Coolant	Yes
6.	Bottom Grid Plates	Fail to Provide Support	Reactivity Increase and Loss of Flow	Yes
7.	Neutron Chamber	Fail High	Spurious Automatic SCRAM	Yes
		Fail Low	Degradation of Reactor SCRAM System Reliability	No
8.	Fission Counter Detector	Fail High	Spurious Automatic SCRAM	Yes
		Fail Low	Degradation of Reactor SCRAM System Reliability	No
9.	Thermo-Couple 1	Fail High	Spurious Automatic SCRAM	Yes
		Fail Low	Degradation of Reactor SCRAM System Reliability	No

10.	Thermo-couple 2	Fail High	Spurious Automatic SCRAM	Yes
		Fail Low	Degradation of Reactor SCRAM System Reliability	No
B	Primary Cooling System			
1.	Main circulation pump1	Fail to Start	Loss of Flow	Yes
		Fail to Run	Loss of Flow	Yes
2.	Manual Butterfly Valve	Fail to Open	Loss of Flow	Yes
3.	Motor Operated Valve	Fail to Open	Loss of Flow	Yes
4.	Manual Butterfly Valve	Fail to Open	Loss of Flow	Yes
5.	Heat Exchanger	Fail to Function	Loss of Heat Removal	Yes
6.	Temperature Probe	Fail to Function	Unavailability of Safety Parameter	Yes
C	Secondary Cooling System			
1.	Secondary Circulation Pump	Fail to Start	Loss of Flow	Yes
		Fail to Run	Loss of Flow	Yes
		Fail to Run	Loss of Flow	Yes
2.	Manual Butterfly Valve	Fail to Open	Loss of Flow	Yes
3.	Motor Operated Valve	Fail to Open	Loss of Flow	Yes
D	Purification System			
1.	Demineralizer	Fail to Function	Loss of Flow	Yes
2.	Demineralizer Pump	Fail to Start	Loss of Flow	Yes
		Fail to Run	Loss of Flow	Yes
3.	Manual Butterfly Valve	Fail to Open	Loss of Flow	Yes
E	Instrumental and Control System			
1.	Magnet Power key	Fail to Function	Unavailability of Control System	Yes
2.	Power On Switch	Fail to Function	Unavailability of Control System	Yes
3.	Reactor Power Display	Fail to Function	Unavailability of Safety Indicator	Yes
4.	Safety Channel	Fail to Function	Unavailability of Safety Indicator	Yes
5.	Power Measuring Channel	Fail to Function	Unavailability of Safety Indicator	Yes
6.	Operation Mode Switch	Fail to Function	Unavailability of Control System	Yes
7.	Bistable Circuit	Fail to Function	Unavailability of Control System	Yes
8.	Shim Rod Initiation Circuit	Fail to Function	Unavailability of Control System	Yes
9.	Safety Rod Initiation Circuit	Fail to Function	Unavailability of Control System	Yes
10.	Regulating Rod Initiation Circuit	Fail to Function	Unavailability of Control System	Yes
11.	Transient Rod Initiation Circuit	Fail to Function	Unavailability of Control System	Yes
12.	Shim Rod Actuation Circuit	Fail to Function	Unavailability of Control System	Yes
13.	Safety Rod Actuation Circuit	Fail to Function	Unavailability of Control System	Yes
14.	Regulating Rod Actuation Circuit	Fail to Function	Unavailability of Control System	Yes
15.	Transient Rod Actuation Circuit	Fail to Function	Unavailability of Control System	Yes
16.	Control Rod Switch Up / Down	Fail to Function	Unavailability of Control System	Yes
17.	Control Rod Position Indicator	Fail to Function	Unavailability of Safety Indicator	Yes
18.	Period / Second Indicator Log	Fail to Function	Unavailability of Safety Indicator	Yes
19.	Safety Channel Indicator	Fail to Function	Unavailability of Safety Indicator	Yes
20.	Water temperature indicator	Fail to Function	Unavailability of Safety Indicator	Yes

21.	Fuel Temperature Indicator	Fail to Function	Unavailability of Safety Indicator	Yes
F	Electric Power Supply			
1.	11kV Bus1	Fail to Function	Reactor Blackout	Yes
2.	Substation Transformer 1	Fail to Function	Reactor Blackout	Yes
3.	Substation Transformer 2	Fail to Function	Reactor Blackout	Yes
4.	Substation Transformer 3	Fail to Function	Reactor Blackout	Yes
5.	Substation Transformer 4	Fail to Function	Reactor Blackout	Yes
6.	500kV Genset1	Fail to Start	Reactor Blackout	Yes
		Fail to Run	Reactor Blackout	Yes
		Failure on Demand	Reactor Blackout	Yes
7.	Uninterruptable Power Supply (UPS)	Fail to Function	Station Blackout	Yes
G	Auxiliary System			
1.	Compressed Air Supply System	Fail to Function	Unavailability of Transient Rod	Yes
2.	Ventilation And Air-Conditioner System	Fail to Function	Negative Pressure Loss in Reactor Hall	Yes

IV. DISCUSSION

The preliminary findings from the FMEA highlight several key vulnerabilities in the PUSPATI TRIGA reactor's systems. While the reactor has multiple safeguards in place, the analysis underscores the importance of regular maintenance, system updates, and training to mitigate the identified risks. The next step will involve using these findings as a foundation for a Level 1 PSA, which will estimate the probability of core damage and guide the development of safety enhancements.

V. CONCLUSIONS

In summary, this narrative-driven introduction has highlighted the centrality of the RTP to Malaysia's nuclear mission, the global imperative of stringent safety, and the complementary roles of PSA and FMEA in risk assessment. Conducting this FMEA is a preliminary step: it ensures that the upcoming Level-1 PSA for the RTP rests on a solid foundation of well-identified failure modes. In turn, this work will strengthen Malaysia's reactor safety framework and support informed safety improvements for the TRIGA reactor.

ACKNOWLEDGMENTS

The authors wish to thank the team at the Malaysian Nuclear Agency, Atom Malaysia, Universiti Kebangsaan Malaysia and Universiti Tun Hussein Onn Malaysia for their support in conducting this study. Special thanks are also extended to the reactor operators for their invaluable input.

REFERENCES

[1] G. J. Storr and K. Kwong, "Initiatives supporting research reactor safety in the Asia-Pacific region," in *Research Reactors: Safe Management and Effective Utilization*, 2011

[2] M. Maskin *et al.*, "Development and methodology of level 1 probability safety assessment at PUSPATI TRIGA reactor," in *Proceedings of the International Nuclear Science, Technology & Engineering Conference 2013 (iNuSTEC2013)*, Feb. 2014 pp. 240–244 doi: 10.1063/1.4866138.

[3] M. S. Minhat *et al.*, "Instrumentation and control system at reaktor TRIGA PUSPATI (RTP)," in *Reaktor TRIGA PUSPATI Colloquium RTP 39 years*, 2021
[4] IAEA, *Defining initiating events for purposes of probabilistic safety assessment (TECDOC Series) No. 719*. International Atomic Energy Agency, Vienna, Austria (1993).
[5] IAEA, *Development and application of level 1 probabilistic safety assessment for nuclear power plants specific safety guide (Safety Series) No. SSG-3*. International Atomic Energy Agency, Vienna, Austria (2010).
[6] S. Authén, J. E. Holmberg, T. Tyrväinen, and L. Zaman1, "Guidelines for reliability analysis of digital systems in PSA context - Final report," Nordic Nuclear Safety Research, NKS-330, 2015.
[7] R. R. Fullwood, *Probabilistic safety assessment in the chemical and nuclear industries*. Butterworth-Heinemann Publications, Boston, MA (1998). doi: 10.1016/B978-075067208-5/50010-X.
[8] C. A. Ericson, "Failure mode and effect analysis," *Hazard analysis techniques for system safety*, pp. 235–455, John Wiley & Sons, Inc., Hoboken, NJ (2005).
[9] IAEA, *Human reliability analysis in probabilistic safety assessment for nuclear power plants (Safety Series No. 50-P-10)*. International Atomic Energy Agency, Vienna, Austria (1996).
[10] A. Kolaczkowski, "Good practices for implementing human reliability analysis (HRA)," US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Division of Risk Analysis and Applications, Washington, DC, 2005.