
This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

A petri net methodology for modeling the resilience of nuclear power plants

PLEASE CITE THE PUBLISHED VERSION

https://doi.org/10.3850/978-981-18-2016-8_109-cd

PUBLISHER

Research Publishing Services

VERSION

VoR (Version of Record)

PUBLISHER STATEMENT

Reproduced with permission of the author

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Yan, Rundong (Derek), Sarah Dunnett, Silvia Tolo, and John Andrews. 2021. "A Petri Net Methodology for Modeling the Resilience of Nuclear Power Plants". Loughborough University.
<https://hdl.handle.net/2134/16740331.v1>.

A Petri Net Methodology for Modeling the Resilience of Nuclear Power Plants

Rundong Yan; Sarah Dunnett

Department of Aeronautical and Automotive Engineering, Loughborough University, UK.

E-mail: r.yan@lboro.ac.uk

E-mail: s.j.dunnett@lboro.ac.uk

Silvia Tolo; John Andrews

Resilience Engineering Research Group, Faculty of Engineering, University of Nottingham, UK.

E-mail: silvia.tolo@nottingham.ac.uk

E-mail: john.andrews@nottingham.ac.uk

In the paper, a novel Petri Net (PN) method for assessing the resilience of nuclear reactors is presented. The PN model constructed aims to simulate the failure of the subsystems in a reactor caused by either natural degradation or external disruptive events such as tsunamis and earthquakes, the resultant accidents due to the failure of different reactor subsystems, the responses of the reactor to different accidents, and the recovery and maintenance of the reactor after the accident. The simulation results are analyzed to identify the key characteristics of the resilience of the nuclear reactor. To demonstrate the feasibility and the capability of the proposed approach, the failure of four heat transport pumps in the primary cooling system of an experimental reactor is chosen as a case study. The research shows that PN modeling is an effective tool for evaluating the resilience of nuclear power plants.

Keywords: Resilience, Nuclear power plant, Petri nets, Maintenance, Mathematical modeling, Simulation.

1. Introduction

Nuclear power generation is widely recognized to be a well-established and mature technology. Nuclear power plants (NPPs) have been in operation for over 60 years. At the end of 2018, there were about 449 operable nuclear reactors and 55 more under construction in the world (Rising, 2019). However, due to the potentially catastrophic consequences of nuclear accidents such as those that occurred at Three Mile Island, Chernobyl, and Fukushima, the safety of such facilities is of interest to the public, as well as the scientific community. These accidents have highlighted the vulnerability of nuclear installations to a wide range of hazards, from human errors to natural disasters and design defects, and have demonstrated the potential safety issues associated with NPPs (Aoki and Rothwell, 2013). This has resulted in much past research on the reliability and safety of nuclear systems. In particular, many studies have adopted classical risk assessment approaches such as event tree analysis and fault tree analysis (USNRC, 1975). However, it is found that these conventional methods have difficulty accounting for the influences of unpredictable events, such as earthquakes and tsunamis (Park et al., 2013; Francis and Bekera, 2014). In addition, as the complexity of NPPs increases the traditional methods are no longer adequate in modeling it. Hence there is a need for a different approach.

Resilience engineering offers a promising alternative (Costella et al., 2009). Different from conventional risk assessment methods that aim to predict the failure rate or reliability of the system and eliminate the root causes of the

failure, resilience analysis considers the ability of the system to recover in the presence of failure. Since many extreme events, such as severe weather and earthquakes, are inevitable, resilience analysis aims at enhancing the systems' ability to anticipate and absorb the unexpected events, restore the performance, and adapt from the event.

Considering the context, this study aims to develop a method for assessing the health and safety of NPPs with the focus on resilience engineering. An experimental reactor based on CANadian Deuterium Uranium (CANDU) reactor design is chosen for analysis. Petri nets (PNs) are used for modeling the health state of the nuclear subsystems, the mitigation of the consequences of disruptions, the corresponding responses to different risks, and the recovery from abnormal conditions. In addition, a physical model coupled together with the PNs is developed to simulate the variations of the critical physical parameters of nuclear systems.

2. Resilience Engineering

Resilience engineering, a relatively new topic in engineering research, is still in its early stages of development (Kim et al. 2018). The approach searches for proactive solutions aimed at anticipating and planning for the unexpected. However, resilience engineering is still far from being well established or widely applied and even lacks a universally agreed definition. Most of the available definitions incorporate four critical aspects: avoiding threats, withstanding threats, recovery from threats and

adapting to threats (Hosseini et al., 2016). It is common practice to visualize these features as a system resilience curve (SRC) by plotting the performance metrics of interest against the time. As shown in Fig. 1, the generic SRC (adapted from (Greene, 2018)) can be divided into five phases. In Phase 1, the system operates normally at a steady-state performance until the occurrence of the disruptive event at time t_0 . In Phase 2, the performance of the system decreases until the lowest performance is reached at time t_1 . The descending slope and the worst state of the system depend on many factors including the type and magnitude of the disruptive event, the availability of the safety systems, the detection of the event, the corresponding response time, etc. Assuming that the worst state of the system is still within the recoverable region, recovery actions are conducted to restore any critical functionality of the system in Phase 3. Following this, the system can be fully restored to its original status and restart its normal operation in Phase 4. Finally, the system is expected to learn from the event occurred to improve its resilience against future similar events as shown in Phase 5.

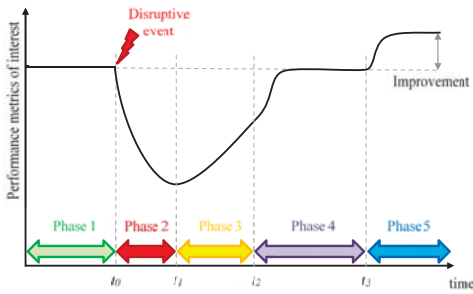


Fig. 1. System resilience curve, representing normal operation (Phase 1), shock and response (Phase 2), recovery and maintenance (Phase 3), performance restoration (Phase 4), adaptation from threat (Phase 5)

In this paper, a method for evaluating the resilience of nuclear reactors is proposed. For demonstration purposes, an experimental reactor based on the CANDU reactor design and its responses to a typical major accident, which is the loss/decrease of primary coolant flow due to the failure of the heat transport (HT) pumps has been analyzed.

3. Case Study

The demonstration CANDU reactor system used in this work is a Canadian pressurized heavy-water reactor design (CANDU 6 Program Team, 2005). Fig. 2 is a schematic diagram showing a loop of the primary heat transport system of the reactor, where the uranium fuel is loaded into horizontal pressure tubes. The system has two identical loops connected to a common pressurizer. The heavy water coolant is pumped through the reactor core's tubes in a closed-loop ensuring the removal of heat produced by the fission chain reaction in the reactor. For each loop, there are two core passes with coolant flowing in opposite directions. The available thermal power is then transferred to a secondary cooling loop in the form of high-pressure steam

obtained with the use of steam generators. The steam powers the turbines resulting in the production of power by the electric generators.

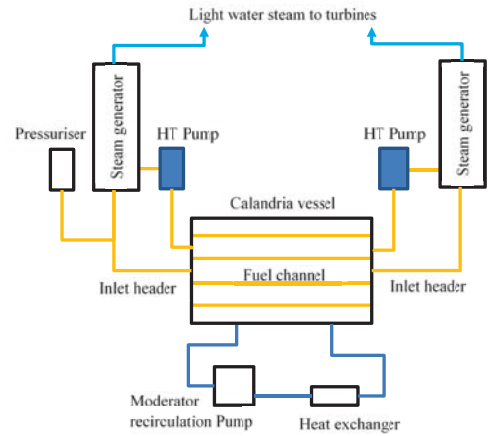


Fig. 2. A schematic of a loop of a CANDU primary heat transport system

The CANDU design includes a series of safety features aimed at enhancing the reactor's tolerance to accidents. However, it should be noted that only three main safety systems including two shutdown systems and one power control system, are investigated in this research in order to demonstrate the methodology developed. Two independent and diverse, fast-acting safety shutdown systems are in place: the primary system (SDS1) relies on the use of neutron-absorbing shutoff rods suspended above the reactor by electromagnets; the secondary system (SDS2) is designed to inject high-pressure gadolinium nitrate into the moderator. The control rods are a part of the reactor regulating system. Their purpose is to cause rapid power reduction when required. It is assumed that the failure of these subsystems follows Weibull distributions. The distribution parameters including the shape parameter (β) and characteristic life (η), are listed in Table 1. The table also contains information about the average time for repairing each subsystem (T_r). This information is derived based on historical failure data (International Atomic Energy Agency, 1988).

It should be noted that other power control systems, fault detection systems, and the safety systems for maintaining long-term cooling after shutdown are not considered in the study but will be studied in future work.

Table 1. Failure and repair data of the subsystems in the reactor

Subsystems	β	η (year)	T_r (hour)
HT pump	1.4335	11.42	154
Control rods	1.2840	73.92	120
SDS1	1.3000	656.89	120
SDS2	1.5320	5.70	200

To simulate the possible consequences of the failure of the HT pumps due to external events and natural degradation, the PN method was chosen. As the available

safety systems could also be damaged by external events, or fail without been revealed due to natural degradation, the reactor response will vary.

4. Model Construction

A PN is a direct bipartite graph that consists of three types of symbols, namely circles, rectangles, and arrows as illustrated in Fig. 3. Circles represent the places, which are conditions or states of a system. The condition place, marked light gray in the figure, means the model will perform predefined actions if the conditions are met in the place. In addition, the place filled dark gray means the simulation will end if a token is placed in one of these places. Rectangles represent the transitions, which are actions or events causing the change of condition or state. If the time of the transition is zero, the rectangle will be filled black, otherwise it is empty. Arrows, known as arcs in PNs, link places and transitions together. Arcs with a slash on and a number, n , next to the slash represent a combination of n single arcs and the arc is said to have a weight n . A transition can be enabled if the number of tokens in every input place is greater than or equal to the corresponding weights of the arcs to the transition. Once a transition is enabled it will fire after the time associated with it and tokens will be taken out of the input places and put into the output places. In addition, the dashed arrows mean the link between the connected places and transitions are conditional. After a transition is enabled, the probability of the expected tokens being produced in the output places connected by a conditional arc is predefined. In addition, an arc with a small circle on one end is known as an inhibit arc. This is able to prevent a transition from firing when enabled. Finally, small black filled circles represent tokens that carry the information in the PNs. The movement of the tokens between the places in the net gives the dynamic properties of PNs. The positions of the tokens in a PN at a given time shows the state of the system being modeled at that time.

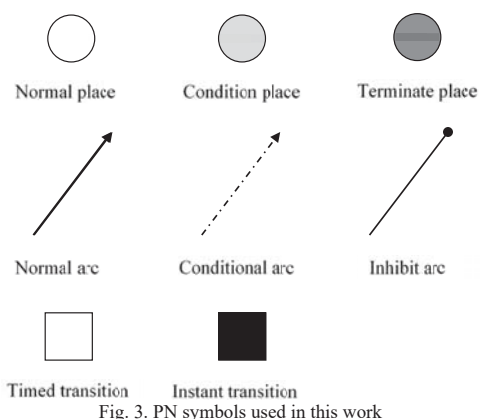


Fig. 3. PN symbols used in this work

To facilitate the research, three PNs are constructed to model the states of the reactor system, the accidents or hazards and the corresponding consequence, and more

importantly the responses to the accidents and recovery from the accidents. These are:

- Reactor System Petri Net (RSPN) – describes the working and failure states of the subsystems and safety systems in the reactor.
- Detection and Response Petri Net (DRPN) – governing the responses of the reactor to different accidents.
- Recovery and Maintenance Petri Net (RMPN) - describes the recovery and maintenance processes.

These three PNs are linked together and share information with each other as well as with a physical model as illustrated in Fig. 4. Firstly, the external events such as earthquakes will be generated as the inputs of the PNs. Their impacts on the subsystems and safety systems in the reactor will be simulated in the RSPN. The information about the failure of any subsystems leading to changes in the physical parameters of the reactor will be fed to the DRPN and the physical model. In this way, the behavior of the CANDU reactor subject to different accidents can be simulated. The times of some key transitions such as those representing the time for fault detection and activating the safety system, are dependent on outputs from the physical model, which represents the reactor thermodynamics. Finally, the recovery and maintenance of the reactor after the failure can be modeled via the RMPN.

The details of the nets and physical model are discussed in the following sections.

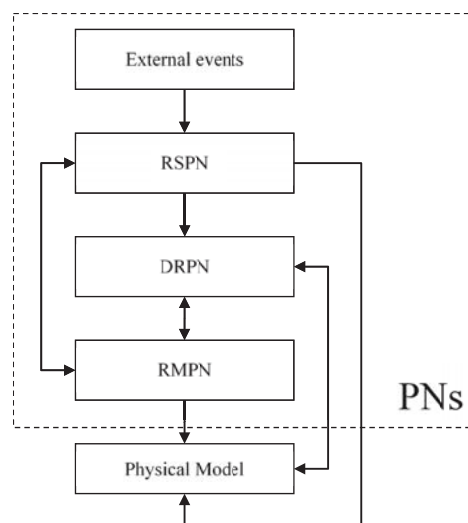


Fig. 4. The overall structure of the model

4.1 Physical model

The physical model is constructed to simulate the transfer of heat energy produced by the reactor core. The key parameters computed in it include the coolant pressure, the coolant temperature and the power output. The normal operating conditions of the reactor used for the analysis in

the paper are based on the data in (SNC-Lavalin, 2015) and listed in Table 2.

Table 2. Normal operating conditions of the reactor

Parameter	Normal operation value
Reactor thermal output	2084MW
Primary coolant (or HT) flow rate	9200Kg/s
Primary coolant temperature	310.0°C
Primary coolant pressure	10.09MPa

Once a fault, which interrupts the normal operating conditions, has occurred, the physical model will simulate the changes of these key parameters accordingly. Once any of the key parameters reaches a certain critical value, a signal will be sent to the control system so that the reactor will response to mitigate the impact of the fault. Commonly used signals include high neutron flux, high HT system pressure, high containment pressure, high moderator level, etc. In the research, the HT system pressure (primary coolant pressure) is chosen as the activation signal of the safety systems. The thresholds for the activation of the safety systems considered in the study are listed in Table 3. It is worth noting that the damage to the reactor system is assumed to start if the coolant temperature reaches 374.0°C. Once the system is damaged, the recovery time of the reactor will be long (several months to years) and unpredictable.

Table 3. Thresholds for the activations of safety systems

Safety systems	Threshold
Control rods	10.24MPa
Shutoff rods	10.45MPa
Poison injection system	11.72MPa

4.2 Reactor System Petri Net (RSPN)

The RSPN simulating the health states of the reactor subsystems, which include four HT pumps, two shutdown systems, and one control system, is illustrated in Fig. 5. From the figure, it can be seen that the RSPN is divided into several parts, namely, disruptive event, safety systems, system states, functional systems and repair needed as shown by the dotted boxes in the figure. In this research, only two health states for the systems are considered, namely normal (UP) and failed (DOWN). More complex and detailed system health states can be included in the model and this will be considered in the future. The net shown represents the system when all the subsystems are working and there are tokens in all 'UP' places. The timed transitions (F5, F6, F7, F8, S4, S5 and S6) between 'UP' places and 'DOWN' places represent the natural degradation processes of these subsystems. The time for these failure transitions can be computed by using random sampling and the failure rate data given in Table 1.

The disruptive events box models the occurrence of an external event such as an earthquake or tsunami. The time delay D1 is the time to the next event, which can be generated from local historical data. After an external event

has occurred, it could damage the reactor systems. The transitions (F1, F2, F3, F4, S1, S2, and S3) represent the impact of the external event on the reactor subsystems. The conditional arcs, represented by the dashed arcs out from these transitions, connect to both the 'UP' and 'DOWN' places for the subsystems. The probability of the tokens transferring to either of these two places is dependent on the probability of these systems been damaged by the external event. This depends on many factors such as the type and magnitude of the external events, the vulnerability of each subsystem, and the location of these systems, etc.

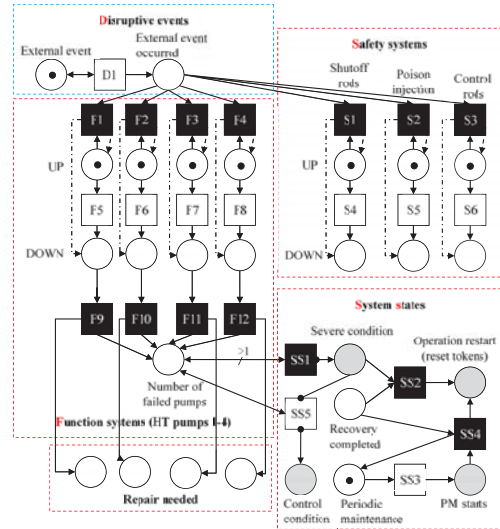


Fig. 5. RSPN

Once there are tokens produced in the 'DOWN' places representing the failure of the HT pumps, the tokens will then be produced in the corresponding 'Repair needed' places which means these pumps can no longer perform their functions normally until they get repaired. In addition, tokens, whose amount is equal to the number of failed pumps, will be produced in the place named 'Number of failed pumps'. If only one pump has failed, a token will be produced in the 'Control condition' place, which means the reactor must lower its power output immediately. This process is known as stepback. However, if more than one HT pump is failed, this will be recognized as a severe condition, which means the reactor has to be shut down immediately and the operation of the reactor cannot be restored until all the pumps are working. The places representing 'control condition' and 'severe condition' are colored light gray meaning that they are condition places. The condition is that the corresponding DRPN will be embedded in the model once they contain tokens.

Periodic maintenance is also considered in this research. This means that all the subsystems in the reactor will be regularly inspected and repaired. It is assumed that the systems will be restored to their 'UP' states after each periodic maintenance. The token produced in the 'PM

starts' place will embed the RMPN representing the maintenance of all systems in the model.

Finally, once there is a token produced in 'Operation restart' place, all the transition times will be recomputed except the time till the next external event.

4.3 Detection and Response Petri Net (DRPN)

The information about the failure of the HT pumps will be fed to the physical model. The reduction in the flow rate of the heavy water coolant due to the failure of the HT pumps will decrease the ability of heat removal of the reactor core so that its temperature will increase rapidly. Once a critical physical parameter reaches a threshold, the reactor will respond accordingly. This is achieved by linking the PN with the physical model. The DRPN can be divided into two parts, namely the controlled operation, and the shutdown of the reactor as shown in Fig. 6. These two parts will be used for different accidents. Fig. 6 includes the detail of the 'controlled operation' part of the net. Once it is embedded in the network, it will gather information from the RSPN and physical model first. The health states of the safety systems will be imported from the RSPN to the DRPN by placing the tokens in the corresponding places. The switching time of the transitions including the fault detection time, FD1, the time for realizing failed control, C2, and the time to lower the reactor power to the desired value, C3, are obtained from the physical model.

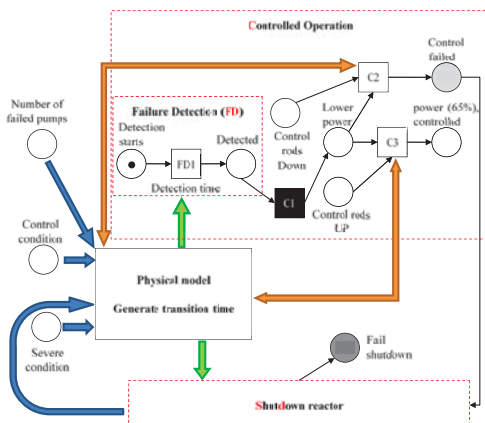


Fig. 6. DRPN (Controlled operation in detail)

If the DRPN is embedded in the model due to the activation by 'Control condition' place in the RSPN, only the controlled operation part of the DRPN will be imported as shown in Fig. 6. Once this abnormal symptom is detected, the control system will respond automatically to bring the system back to a safe status. It is assumed that the CANDU reactor system can operate with just one HT pump failed. However, the operation must be adjusted by reducing the current power output to 65% and the coolant flow rate should be kept at about 70% of normal flow [CNSC, 1993]. If there is a token in place, 'Control rods UP', the power output can be reduced to 65% of the current power after a certain time. This can be achieved by adjusting the depth of

the control rods in the core to control the neutron flux. However, if the control rods are not available, a token will be produced in 'Control failed' place. Then, the DRPN part modeling the shutdown process will be activated. This net is constructed in a similar manner to the controlled operation part. It will also be activated if there is a token in the condition place, 'Severe condition' in the RSPN, which means more than one HT pump has failed.

The shutdown process modeled is that once the HT system pressure reaches 10.24MPa, the shutoff rods (SDS1) will be activated. If SDS1 fails, the pressure will keep increasing rapidly to the threshold for the activation of the poison injection system (SDS2). As the coolant temperature is reduced to the safe value of 177°C, the temperature will keep reducing at a lower rate to minimize the stresses due to the temperature change, which can take up to 8 hours. Finally, the coolant temperature will be kept at 55°C to remove the decay heat continuously after the shutdown until the performance of the reactor can be restored. It should be noted that once any of the conditions, i.e. controlled operation, and safe shutdown, is met, the embedded DRPN will be removed from the model. However, if both shutdown systems are not available, a token will be produced in the terminate place, 'Fail shutdown'. It means that the reactor will not be able to shut down, which then might lead to a very rapid core melting. This is the worst-case considered in the research.

4.4 Recovery and Maintenance Petri Net (RMPN)

After the accident is controlled or the reactor is shut down successfully, the recovery and maintenance processes can be conducted to bring the reactor system back to its normal condition as soon as possible to minimize the loss of power production. Hence, the RMPN will be embedded in the model after the DRPN. Due to space limitation the net is not included in this paper but the process is described below.

Before the RMPN is embedded in the network, it will be initiated by gathering the information from the RSPN. The recovery and maintenance processes are said to be completed only if all the subsystems in the net are back to their 'UP' states. Then the cleanup can be conducted before the reactor performance is able to be restored.

If the reactor is still operating but with a lower power output rather than being shut down after the accident, the maintenance will be conducted only to the failed operating subsystems (i.e. the HT pumps in the research), which reveal themselves. Once these failed subsystems are repaired, the reactor can resume its normal operation. On the other hand, if the reactor is shut down, a complete inspection and maintenance to the whole system including both the operational systems and inactive safety systems will be conducted. After all the maintenance activities are completed, the necessary cleanup processes such as removing the shutoff rods from the core or removing the liquid poison from the moderator, have to be conducted. Then, the reactor can be restarted.

Finally, after all the actions for recovery and maintenance are completed, a token will be placed in 'Recovery completed' place in the RSPN.

This will then activate 'SS2' transition in the RSPN to produce a token in 'Operation restart' place. As a result of this, all the embedded PN's except the RSPN will be removed. The time of all the transitions will be recomputed except the time till the next external event.

5. Simulation

In order to evaluate the resilience of the reactor system, the model proposed in the previous section can be used for simulation. The failure rates and average repair times of all the reactor subsystems listed in Table 1 and the physical parameters and thresholds given in Tables 2 and 3 respectively are used as inputs to the simulation.

The following are the simulation assumptions:

- An external event happens after 2.5 years of the reactor running.
- The probability that the subsystems will be damaged by the external event is assumed to be 0.4 and is the same for all the subsystems.
- Periodic maintenance is conducted every 2 years.

5.1 Simulation results

It is found that the simulation can capture the features of the reactor successfully. The availability of the operating HT pumps in the primary cooling system of the reactor within 30 years in a typical iteration of the simulation is shown in Fig. 7.

The figure shows that there are 6 events of the HT pump failure in total within 30 years. The most severe accident involving the failure of three HT pumps simultaneously happens at 2.5 years after the reactor started its first operation. The graph will be different in every simulation iteration due to the random sampling, the failure distribution method, and the probability of the damage done by the external event.

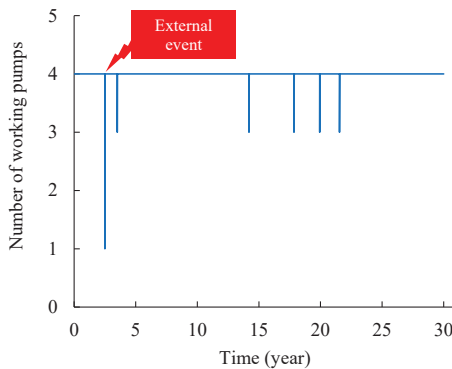


Fig. 7. Availability of the HT pumps

Next, the variations of the critical physical parameters in the reactor due to the external event are investigated in detail. The coolant temperature is chosen to demonstrate the impact of external events. Four typical temperature variations are chosen from the simulation results of four iterations, which are able to show the impact of the external

events and the effectiveness of each safety system as shown in Fig. 8. It is worth noting that the time scale of the figure is in seconds (s), the external event is assumed to happen at 50s in this figure.

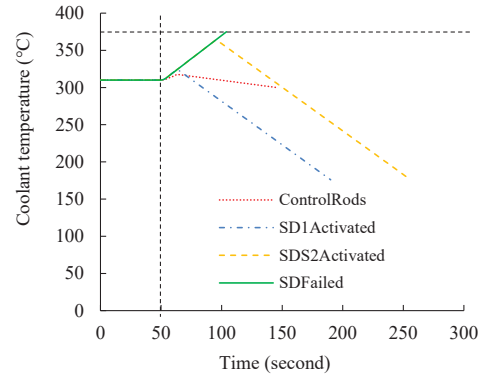


Fig. 8. Coolant temperature variation after the external event

In the figure, the round-dotted line represents the failure of one HT pump and the other three lines represent the failure of two HT pumps simultaneously. If only one pump has failed, the increase rate in the coolant temperature will be relatively lower than if more than one pump has failed. This is shown by the less steep slope of the round-dotted line from 50s to about 70s. After the control rods are activated successfully, the temperature will start to reduce until reaching a new stable point (assumed to be 300°C) for the 65% of the normal power output. The dash-dotted line shows the variation of the coolant temperature with the successful activation of the SDS1. The temperature is reduced effectively after the activation of the SDS1 after 20s of the accidents occurred. A safe temperature, 177°C, is reached after about 124 seconds of the activation. The activation of the SDS2 is about 30 seconds later if the SDS1 is not activated successfully. The highest coolant temperature reached is about 363°C after the accident has happened for about 45 seconds. The solid line represents the failure of both shutdown systems. It reached 374.0°C meaning that the reactor system is damaged and difficult to recover.

The ability of the system to absorb the impact of the external event and recover from the accident is also analyzed. The probabilities of the activation of each safety system and failed shutdown are calculated. The results are plotted against the number of simulation iterations to ensure convergence as shown in Fig. 9. It is found that the simulation results converge after performing at least 4000 simulations. It took about 30 minutes for running 4000 simulations in Visual Studio 2012 on a personal computer equipped with Windows 10, 3.20 GHz CPU and 16GB memory. From the figure, it is found that the probability of the reactor system not being affected by the external event is 0.113. The probabilities of the activation of the control rods, shutoff rods, and poison injection systems are 0.224, 0.396, and 0.073 respectively. In addition, it was found from the model that the average recovery time after the activation

of the different safety systems is 6.4 days, 6.8 days, and 7.8 days respectively. Finally, the probability of the failed shutdown is 0.194.

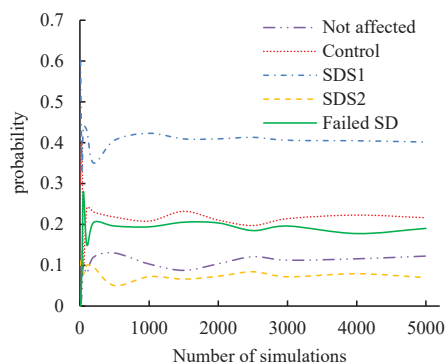


Fig. 9. Probability of different responses taken after the external event

6. Conclusion

In order to develop an effective and reliable approach to assessing the resilience of nuclear reactors, the PN method is adopted in this paper. A physical model is coupled together with the PN to simulate the variations of the critical physical parameters in the experimental reactor. The abilities of the experimental reactor to absorb the impact of the external event and recover from the accident are successfully assessed.

The PN model constructed for the HT pumps can easily be adapted to include other subsystems. The impact of the availability and reliability of the sensors, detectors, and maintenance resources on the system resilience will be investigated in the future. In addition, the effectiveness of different maintenance strategies, safety systems, and response actions will be investigated. This can readily emphasize the adaptability of the system for improving system resilience. It is deemed that the resilience evaluation methodology established in this paper can be used effectively in the design of future resilient NPP's.

Acknowledgement

The authors would like to acknowledge the financial support of EPSRC through grant EP/R021759/1, part of the UK-India Civil Nuclear Collaboration program.

References

Rising, A. (2019, August). *World Nuclear Performance Report*. World Nuclear Association.
Aoki, M. and G. Rothwell (2013) A comparative institutional analysis of the Fukushima nuclear disaster: Lessons and policy implications. *Energy Policy* 53, 240-247.

CANDU 6 Program Team (2005, May). *CANDU® 6 Technical Summary*. Reactor Development Business Unit.
CNSC (1993). Heat Transport System, *CANDU training document for CANDU 6 reactors, Fundamentals of Power Reactors*, Canadian Nuclear Safety Commission.
Costella, M.F., T. A. Saurin and L. B. de Macedo Guimarães (2009). A method for assessing health and safety management systems from the resilience engineering perspective. *Safety Science* 47(8), 1056-1067.
Francis R. and B. Bekera (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety* 121, 90-103.
Greene, S. R. (2018) Are Current U.S. Nuclear Power Plant Grid Resilience Assets?, *Nuclear Technology* 202, 1-14.
Hosseini, S., K. Barker and J.E. Ramirez-Marquez (2016). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety* 145, 47-61.
International Atomic Energy Agency (1988). *Component reliability data for use in probabilistic safety assessment*. IAEA, Vienna, Austria.
Park, J., T. P. Seager, P. S. C. Rao, M. Convertino and I. Linkov (2013). Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. *Risk Analysis* 33(3), 356-367.
SNC-Lavalin (2015). *Enhanced CANDU 6 Technical Summary*. Atomic Energy of Canada Ltd. (AECL), Mississauga, Canada.
USNRC (1975). *Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, WASH-1400, US Nuclear Regulatory Commission, Washington, DC.