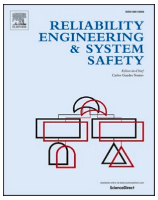
Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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



A Petri net model-based resilience analysis of nuclear power plants under the threat of natural hazards

Rundong Yan [a,*], Sarah Dunnett [a], John Andrews [b]

[a] Department of Aeronautical and Automotive Engineering, Loughborough University, Epinal Way, Loughborough LE11 3TU, UK
[b] Faculty of Engineering, University of Nottingham, University Park, Nottingham NG7 2RD, UK

ARTICLE INFO

Keywords:
Petri net
Resilience
Nuclear power
Station blackout
Loss of coolant accident

ABSTRACT

Due to global climate change, nuclear power plants are increasingly exposed to the threats of extreme natural disasters. In this paper, a resilience engineering approach is applied to tackle all aspects of nuclear safety, spanning from design, operation, and maintenance to accident response and recovery, in the case of high-impact low-probability events. Petri net models are developed to simulate the losses caused by extreme events, the health states of relevant systems, mitigation processes, and the recovery and maintenance processes. The method developed is applied to assess the resilience of a single-unit pressurised heavy water reactor under the threat of three possible external events. Possible loss of coolant accidents and station blackout accidents caused by the events are considered. With the aid of the models developed, both the influence of stochastic deterioration and the impact of external events on the resilience of the reactor can be assessed quantitatively. The simulation results show that the method can comprehensively describe the resilience of nuclear power plants against various disruptive events. It is also found that the stochastic deterioration that does not directly affect the operation of nuclear reactors is critical to the resilience of reactors.

1. Introduction

Nuclear energy now provides around 10% of the world's electricity from about 440 power reactors [1]. The UK government has set out an ambition to construct eight new nuclear reactors to provide 25% of the country's electricity by 2050 [2]. However, the safety of nuclear facilities has consistently been a major concern to the public and scientific community due to the potentially catastrophic consequences of an accident such as the Fukushima Daiichi nuclear disaster which occurred in 2011 [3]. Accidents such as this have motivated active research on the risk assessment and safety design of nuclear systems [4,5]. This disaster, in particular, demonstrated that extreme events beyond the design basis can occur, with potentially catastrophic consequences. Hence, when considering the safety of Nuclear Power Plants (NPPs), various extreme events should be considered. Even if these events are highly improbable, they can induce unexpected impacts and vibrations and consecutively environmental, health and biological hazards and a heavy economic loss. These events are known as high-impact low-probability (HILP) events [6,7]. Due to the impact of climate change, the occurrence rates of extreme events are expected to keep increasing. In addition, the recently developed advanced reactor designs involve increased use of automation and digitisation of control systems. While they offer undoubted advantages in terms of efficiency, they do introduce new and often unknown vulnerabilities into the system, especially against HILP events. Hence, due to the potential of NPPs to produce a considerable proportion of the world's low-carbon electricity and the catastrophic consequences of accidents, the effects of potential HILP events on NPPs must be studied in detail.

Traditional Probabilistic Safety Assessment (PSA) methods based on fault tree and event tree analysis have been adopted for decades to

Abbreviations: BDBA, Beyond design basis accident; CDPP, Combined deterministic and probabilistic procedure; ECIS, Emergency coolant injection system; EDG, Emergency diesel generator; GDCS, Gravity-driven cooling system; HILP, High-impact low-probability; IRPN, Immediate response Petri net; MPPN, Mitigation process Petri net; NPP, Nuclear power plant; HT, Heat transport; LOCA, Loss of coolant accident; LBLOCA, Large-break loss of coolant accident; PHTS, Primary heat transport system; PHWR, Pressurised heavy-water reactor; PN, Petri net; RMPN, Recovery and maintenance Petri net; RSPN, Reactor system Petri net; SHTS, Secondary heat transport system; SBO, Station blackout; SBLOCA, Small-break loss of coolant accident; SCS, Shutdown cooling system; SDG, Standby diesel generator; SDS1, Shutoff rods; SDS2, Poison injection system.

* Corresponding author.
E-mail address: r.yan@lboro.ac.uk (R. Yan).

https://doi.org/10.1016/j.ress.2022.108979
Received 8 September 2022; Received in revised form 5 November 2022; Accepted 11 November 2022
Available online 13 November 2022

ensure the safety of reactor designs [8,9]. These methods are known to work well when considering predictable situations for which there is historical data. However, due to their nature, such information is not available for the HILP events. In contrast to traditional PSA methods, resilience engineering approaches mainly focus on HILP events, multiple simultaneous faults, and common cause failures due to catastrophic damages [10,11]. In recent years, a large number of resilience modelling and analysis studies have been carried out in various applications [12–15]. However, its application in the nuclear engineering sector is still limited [16,17]. For example, Nelson et al. used a resilience philosophy to assess the impact of human error on the safety of an NPP [18]. Ferrario and Zio adopted Goal Tree Success Tree – Dynamic Master Logic Diagram and Monte Carlo simulation combined to assess the physical resilience of an NPP to an earthquake [16]. They assessed the NPP's resilience by analysing the time required to restore the desired level of functionality of a system after the external event. Labaka et al. proposed a qualitative resilience framework to improve the resilience level of NPPs [17]. Zeng et al. developed a resilience framework based on the Markov reward process to model and analyse an NPP under the threat of earthquakes [19]. However, the stochastic deterioration of different safety systems in the NPP and their response and activation time were not considered in the research. In 2022, Yan and Dunnett proposed a novel mathematical resilience modelling framework based on Petri nets (PN) to assess the impact of station blackout (SBO) accidents on the resilience of an NPP consisting of a typical pressurised heavy water reactor (PHWR) [20]. In the study, the stochastic deterioration, damages caused by external extreme events, operating regimes, and recovery strategies were considered. However, only the safety systems needed during SBO accidents were considered and the overall resilience of NPPs was not assessed. Hence, this paper aims to adopt and further develop the mathematical resilience modelling framework proposed by the authors in [20] to achieve reactor system designs, operating regimes and recovery strategies which result in a safe and rapid response to accidents caused by any extreme HILP event beyond the design basis occurring at any point in its lifetime.

In the paper, two typical nuclear accidents which are the most significant contributors to the nuclear core melt frequency, i.e. loss of coolant accident (LOCA) and SBO accidents, are considered. Although the probability of two events happening at the same time is considered to be 'highly unlikely', they could occur under the impact of extreme events [21,22]. These accidents have rarely been studied previously but is attracting interest from both academic and industrial communities in recent years [23]. For example, Yang et al. used a genetic algorithm to optimise the total plant costs subject to the overall plant safety goal constraints, which takes into account both LOCA and off-site power losses [24]. Sun and Yang assessed a LOCA under a loss of power condition for a typical 3-loop NPP [23]. Maio et al. proposed a sensitivity analysis method to quantify the uncertainties affecting the safety parameter evolution along a nuclear accident scenario, which is an SBO followed by a LOCA for a pressurised water reactor [25].

In this paper, PNs are adopted to develop the resilience modelling framework for NPPs. PNs have been widely used for describing complex systems and processes [26,27]. For example, Yan et al. adopted PNs to evaluate reliability and maintenance issues in automated guided vehicle systems [28,29]. Zhou and Reniers proposed a probabilistic PN-based approach to assess the effectiveness of emergency response in preventing fire-induced domino effects [30]. Liu et al. proposed a PN-based approach to model the data-flow error detection and correction strategy for business processes [31]. In this study, the PN model-based framework for resilience analysis is applied to analyse the resilience of a typical pressurised heavy-water reactor (PHWR) under the threat of three external disruptive events.

The detailed methodology developed in this study is described below. Section 2 presents a state-of-art review of related works. In Section 3 the experimental PHWR and its responses to mitigate the impact of LOCAs and SBO accidents on the reactor are described. The PN modelling method is then briefly reviewed in Section 4 and the PN models developed for simulating the NPP are described in Section 5. The simulation calculations and discussion of results are conducted in Section 6. Finally, the paper concludes with a few key conclusions and future work in Section 7.

2. Resilience in the context of nuclear safety engineering

The term resilience originally described the characteristic of a substance or object to return to its original shape after being bent [15]. Over time, as the term and its philosophy were applied to various scientific fields, its definition evolved to become more specific for different applications. In terms of engineering applications, although resilience engineering is still far from being well established and lacks a universally agreed definition [10,15], its concept has been applied as avoiding, withstanding, recovering from and adapting to threats [32,33]. In the field of engineering and industrial systems, it usually means the ability of a system to respond to disruptive events and focuses on how rapidly and efficiently the system can be restored to its pre-event operation state [15,34]. For example, Haimes defined resilience as the "ability of a system to withstand a major disruption within acceptable degradation parameters and to recover with a suitable time and reasonable costs and risks"[35]. Pan et al. conducted a resilience analysis to assess the damage and recovery of the transportation system[36]. Han et al. used the concept of resilience to assess the damage and recovery of urban lifeline networks against intentional attacks [37]. Iannacone et al. used the resilience philosophy to quantify infrastructure's ability to recover after disruptive events [38]. In the paper, we define resilience as the ability of assets, networks and systems to anticipate, absorb, adapt to or rapidly recover from a disruptive event.

It is a common practice to visualise these features as a system resilience curve (SRC) [39–41]. A typical example of SRC adapted from [42] is given in Fig. 1. In the figure, the system operation is assumed to be characterised by a steady-state performance (Phase 1) until the occurrence of the disruptive event at time t_0. This compromises the normal operation of the system, triggering the action of available safety systems aimed at mitigating and absorbing the impact of the event during Phase 2. The worst performance of the system, reached at time t_1, is expected to be restricted within the recoverable region before any recovery actions can be conducted. It is worth noting that the gradient of the curve and the value of the performance minimum reached within Phase 2 depend on many factors such as the magnitude of the event, the available safety systems, the response time of control systems, etc. In Phase 3, recovery actions are conducted to restore any critical functionality of the system. The duration of this phase depends on the difficulty of identifying and diagnosing all failures and conducting the corresponding

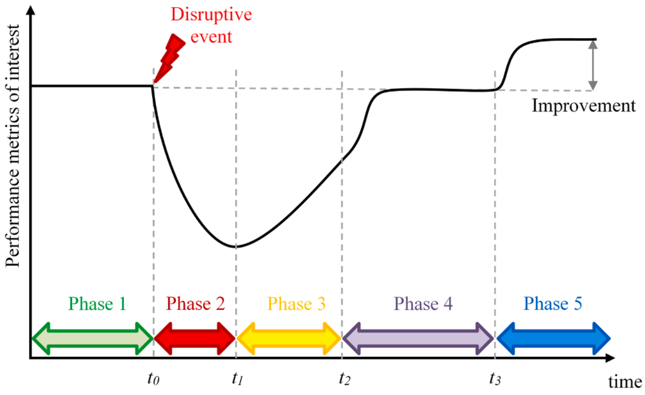


Fig. 1. An example of a system resilience curve after a disruptive event, representing normal operation (Phase 1), shock and response (Phase 2), recovery and maintenance (Phase 3), performance restoration (Phase 4), adaptation from threat (Phase 5) [43].

recovery actions. Following this, the system can be fully restored to its original status in Phase 4. In addition, as shown in Phase 5, the system is expected to learn from the event that occurred in order to improve its resilience against future similar events.

However, the SRC in its current form cannot be applied to the resilience assessment for NPPs. This is because the top priority in an NPP is always to ensure safety rather than maintaining the normal performance of the system [44]. In addition, the SRC cannot reflect the uncertainties of disruptive events and their impact (e.g. the damage probabilities of components). Therefore, a new method is required to address these issues for meeting the unique needs of the resilience assessment of NPPs.

The mathematical resilience modelling framework developed in [20] aims to achieve reactor system designs, operating regimes and recovery strategies which result in a safe and rapid response for any type of threat occurring at any point of its lifetime. The framework consists of three stages:

(1) define the vulnerability of the system's subsystems to external disruptive events; The vulnerability of the system's subsystems will be defined as the probability that the subsystems are damaged by different external events.
(2) simulate the responses of the reactor system to mitigate the impact of the events on the system and evaluate the physical status of the reactor;
(3) model the maintenance process and the system's restoration.

In the first phase, the subsystems' failure caused by stochastic deterioration will also be considered. The second phase aims to model different responses and operations of related safety systems against disruptive events and evaluate the resultant physical status of the reactor. The final phase considers different kinds of inspections, maintenance processes, and restart processes that are essential to restore the normal operation of the reactor. In this paper, the three metrics defined in [20] and a newly defined overall resilience metric are employed to characterise resilience metrics. They are assessed respectively by

(1) resistant capability – the probability that the reactor can maintain its performance after an external disruptive event;
(2) absorption capability – the probability of different operation and health states of the reactor core;
(3) recoverability – the probability of different times that are needed to fully recover the reactor performance.
(4) overall resilience - the probability that a single-unit NPP will be able to absorb the impact of a disruptive event without degrading performance, or fully restore its performance within an acceptable time period in the event of a shutdown or performance degradation, provided the reactor is not significantly damaged or melted. This allows economic losses as well as social and environmental impacts to be kept within acceptable limits. It integrates the resistant, absorption and recovery capabilities together to quantitatively describe the resilience of an NPP against a disruptive event.

3. Description of system and accidents considered

3.1. The PHWR

An experimental PHWR [45] in a single-unit NPP is described below. Its heat transport (HT) system is shown in Fig. 2. The uranium fuel is loaded into horizontal pressure tubes placed within a large vessel. With the aid of the pumps, the heavy water coolant in the primary heat transport system (PHTS) is circulated in a closed-loop through the reactor core's tubes, taking away the heat generated by the fission chain reaction in the reactor core. The yellow and blue lines in Fig. 2 represent the hot and cooled coolants, respectively. The thermal energy is then transferred to the secondary heat transport system (SHTS) to convert water into high-pressure steam in the steam generators. The steam generated can then drive the turbines connected to the electrical generator to generate electricity. The calandria is filled with low-pressure heavy water moderator, which slows fast neutrons down to make them more effective in the fission chain reaction.

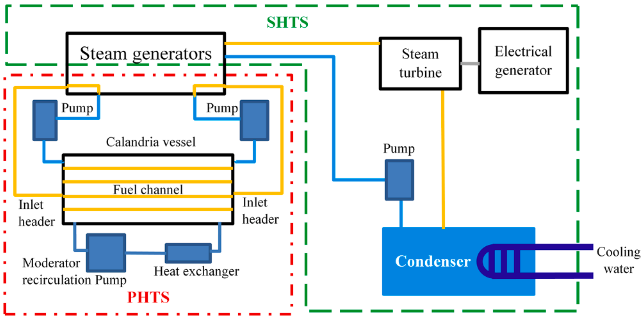


Fig. 2. A schematic of a PHWR heat transport system [20].

3.2. Loss of coolant accident (LOCA)

Coolant escapes from the heat transport system if pipes break, or pump seals fail. Once a LOCA is detected, the reactor must be shut down immediately. Two independent fast-acting shutdown systems, namely shutoff rods (SDS1) and poison injection system (SDS2), will be activated automatically to safely shut down the reactor [46]. However, after the reactor is shut down, heat is still generated by the fuel inside the reactor due to the decay of radioactive fission products. This heat is known as decay heat, which represents a small fraction of the heat produced during normal operation. Hence, after the shutdown, the emergency coolant injection system (ECIS) will be activated to protect the fuel and heat transport system. Its purpose is to set up an alternative heat flow path for removing decay heat. The ECIS considered in the paper consists of three different subsystems, i.e., high-pressure safety injection system (HPSIS), low-pressure safety injection system (LPSIS), and recovery system. The HPSIS is activated to limit fuel overheating, pressure-tube deformation, and forces early cooling once the pressure in the PHTS is reduced to around 5.3 MPa. The time taken to reach this pressure varies due to the break size. In this study, LOCA-type accidents are divided into three categories, i.e. large-break LOCA (LBLOCA), small-break LOCA (SBLOCA), and leak, according to the size of the break in the PHTS.

An LBLOCA involves a break in the heat transport system pressure boundary of sufficient magnitude that the reactor regulating system is incapable of maintaining reactivity balance. If an LBLOCA occurs, the HPSIS can be activated within seconds. The low-pressure safety injection system (LPSIS) takes over when the high-pressure water tanks are nearly empty. It uses low-pressure (~1 MPa) pumps and draws cold water from the dousing tank. This low-pressure injection phase ensures that enough water leaked out can be collected in the basement (i.e., sump) of the containment building before the next recovery phase starts. In recovery injection, the recovery pumps are activated to take water from the containment sump. They pump this water through the heat exchangers to cool it before returning it to the heat transport system. The pressure in the PHTS can be kept low continuously. A new cooling loop is hence formed and it is assumed that this loop can operate for an indefinite time in the study. This phase is the long-term heat sink.

An SBLOCA refers to a break where the reactor regulating system is capable of preventing a significant power excursion. It may occur due to a break in a header or other heat transport parts such as feeders [47]. During an SBLOCA, the coolant begins to boil, and the fuel channels gradually fill with steam. For SBLOCAs, the heat transport system pressure falls slowly because the leak rate is slow. For the injection of the

HPSIS to start quickly, heat must be removed from the system. The steam valves open automatically to release steam. This quickly reduces the heat transport system temperature and pressure so that the injection begins.

For an even smaller PHTS break with a much lower leaking rate, the reactor regulating system is able to keep the heat transport system pressure normal. This is called a leak. For leaks, since crack growth can become unstable and continue, it is essential that the operators detect the presence of the leak and take action before the crack reaches its critical crack length and then grows in an unstable manner [48]. The operators can shut down the reactor manually with the aid of the normal control system. Based on the past literature, it is assumed that the time available for operator response before the leak propagates to a LOCA is 100 h [49]. The operators can manage a controlled shutdown, reduce the pressure, and bring in reserve heavy water. Hence, in this case, none of the special injection safety systems is required.

3.3. Station blackout (SBO) accident

The loss of offsite power is usually caused by stochastic deterioration of its components or direct damage from external events. It can also be caused by a sudden loss of a large amount of electric power generation due to the reactor unit tripping [21]. If the reactor does not trip, the reactor system is designed to switch to onsite power to maintain normal operation after an offsite power failure. The onsite power is generated by the reactor itself. However, if onsite power is also unavailable, this is known as an SBO accident. Due to the loss of power supply, the PHTS will take away the decay heat via natural circulation if there is no leak in the PHTS. To maintain natural circulation over time, the steam generators in the SHTS need to be filled with cooling water constantly. The water must be delivered to the steam generators by the pump of the Shutdown Cooling System (SCS), which requires power to run.

However, if a LOCA also occurs simultaneously, the LPSIS and recovery system for establishing an alternative cooling loop of the PHTS cannot function as both of them need electric power to operate. In addition, the cooling water circulated by the recovery system also needs to be cooled by the SHTS. Any one of the three onsite standby diesel generators (SDGs) is sufficient to meet this power demand. However, if all three SDGs fail, one of three emergency diesel generators (EDGs) stored in a safer location must be activated as an alternative to providing the required power. The EDGs are designed to be seismically qualified, which means that they are unlikely to fail during earthquakes. In extreme circumstances, when all the power supplies used for emergency cooling are no longer working, the decay heat cannot be removed. This is known as a total SBO accident. This type of accident occurred in 2011 when a 15-meter-high tsunami flooded the Fukushima Daiichi NPP in Japan [50]. In this case, water can be injected into the SHTS temporarily by a gravity-driven cooling system (GDCS). The GDCS consists of several pools, which are located above the reactor in the containment. Once the GDCS is activated, the light water in the pools will flow into the steam generator under the action of gravity. Such a self-activating system can temporarily maintain the circulation of cooling water inside the system, thereby providing time for the deployment of emergency mitigation equipment. The emergency mitigation equipment considered in this NPP consists of three fire trucks that can pump water into the SHTS directly. Two of them are required to provide the sufficient cooling capability. However, if more than two of them are unavailable, the water in the steam generators will evaporate. The heavy water coolant in the PHTS will heat up until boiling. Once the primary coolant is exhausted, the fuel will begin to be damaged. As a consequence of this, the moderator in the calandria will start to boil. Once this happens, fire trucks need to inject the water directly into the calandria to prevent further fuel damage [51]. Otherwise, the fuel will continue to overheat and eventually cause the core to melt.

4. Brief review of petri net modelling technique

Since PNs are not only able to capture the features in Fault Tree or Event Tree analysis but also the impact of response, maintenance and recovery processes for different failures [28,52], they have been increasingly adopted in reliability studies. For example, Cho et al. applied PNs to evaluate the cyber-physical security and dependability of digital control systems in NPPs [53] and Gonçalves et al. adopted the PN technique to assess the safety of unmanned aerial vehicles [54]. Wootton et al. adopted PNs to assess the risks of stochastic deterioration of nuclear reactor systems and the effectiveness of scheduled maintenance strategy in reducing the probability of early shutdown [55]. Yan and Dunnett proposed a PN-based method to assess the resilience of NPPs against SBO accidents [20].

The PNs model the system of interest graphically using four types of symbols that are illustrated in Fig. 3. In the figure, circles represent the places, which indicate the conditions or states of the system. In this paper, coloured patterns are used to differentiate different types of places. The condition place, filled with yellow horizontal lines, means that the model will perform predefined actions when the conditions in the place are satisfied. The place filled with red vertical lines means that the simulation will be ended when a token is placed in it. Rectangles represent the transitions, which are actions or events causing the change in condition or state. If the time of the transition is zero, the rectangle is filled in black, otherwise, it is empty. Arrows in PNs are known as arcs, which link places and transitions together. Arcs with a slash and a number, *n*, next to the slash represent a combination of *n* single arcs, i.e. the arc has a weight *n*. When the weight is one, the slash will be absent from the arc for simplicity. A transition is enabled only if the number of tokens in every input place is not less than the corresponding weights of the arcs to the transition. The dashed arcs mean that the links between the connected places and transitions are conditional. The arc with a small circle on one end is known as the inhibitor arc, which is able to stop a transition from firing even if enabled. Finally, small black-filled circles in places represent tokens, which carry the information in PNs. Tokens move between the places in a net and the movement of tokens enables dynamic properties to be effectively modelled. To ease understanding, an example of PN is shown in Fig. 4.

In Fig. 4, the places on the left-hand side of the net contain more tokens than the weights of the arcs linking the places to the transition 'D1'. Therefore, the transition is enabled. Hence, the transition will fire after the time interval *t* associated with the transition. When a transition fires, it takes tokens out of the input places. The number of tokens to be taken out is defined by the arc weight linking the place to the transition. Simultaneously, tokens will be produced in the output place. The number of tokens to be produced is equal to the weight of the arc linking

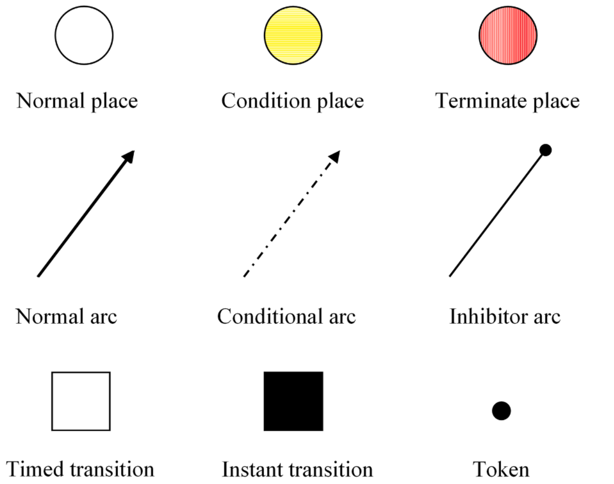


Fig. 3. Graphic representations of different PN symbols [20].

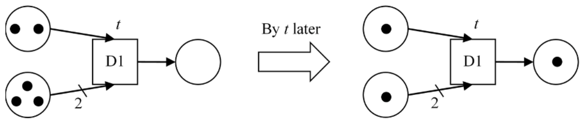


Fig. 4. Example of an enabled transition.

the transition and the output place. Following this rule, after the transition 'D1' is fired, one token is taken out of the top input place and two from the lower and one token is placed in the output place, as shown in the net on the right side of the figure.

As described in [20], four types of PNs are developed:

- Reactor System Petri Net (RSPN) – simulates the health states of all the reactor subsystems and safety systems.
- Immediate Response Petri Net (IRPN) – simulates the immediate response to different accidents.
- Mitigation Process Petri Net (MPPN) - simulates the short-term and long-term mitigation processes for maintaining the safety of the reactor system.
- Recovery and Maintenance Petri Net (RMPN) - simulates the recovery and maintenance processes of the reactor system.

These four different types of PNs are connected, as illustrated in Fig. 5. The health states of the reactor systems and safety systems are simulated in the RSPN. The output of the RSPN, i.e. the conditions that activate safety systems and the health states of different systems, will be fed into the IRPN and MPPN, both of which simulate the responses to the accidents. The maintenance and recovery of the systems are modelled by the RMPN. The final damage level of the reactor and its resilience can be assessed based on key information obtained from the PN, such as the pattern of token markings in the PNs and the time spent in each net.

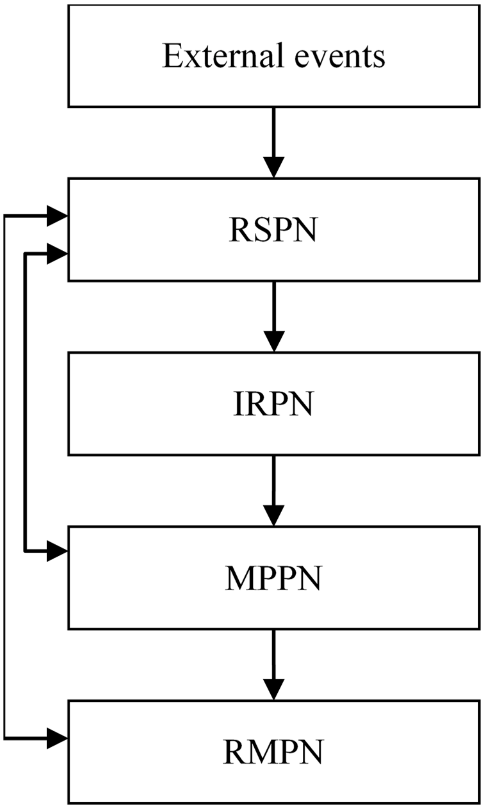


Fig. 5. Overview of the PNs [20].

5. Petri net development for resilience assessment

5.1. Reactor System Petri Net (RSPN)

The RSPN is developed for simulating the health states of the reactor subsystems and safety systems as shown in Fig. 6.

In contrast to the PN model developed in [20], which only simulates SBO accidents, two different nuclear accidents, namely SBO accidents and LOCAs, and the health states of the related subsystems are modelled. The LOCA considered is caused by a break in the primary coolant pressure boundary in the PHTS while the failure of offsite power is the precursor of the SBO accident. The safety systems and the road access condition that are essential to mitigate the impact of these accidents have been included in the net. In detail, 12 different kinds of safety systems, i.e., SDS1, SDS2, normal control system, onsite power, GDCS, SCS, three SDGs, three EDGs, three fire trucks, HPSIS, LPSIS, and recovery system are considered in the model. The failure of safety systems will only be revealed during testing or when demand occurs. In the modelling process, only two health states of the systems, namely normal ('UP') and failed ('DOWN'), are considered for simplicity. Three states for the condition of the access road are considered in the model i.e. normal, moderate damage, and major damage. It is assumed that the road access conditions are only affected by external events. However, its condition has a significant impact on the time required for fire trucks to approach the nuclear reactor system.

All 'UP' places in the figure for the subsystems contain a token, which represents all the systems in a working state. The timed transitions ('IS1' to 'IS9', 'SG4' to 'SG6', 'EG4' to 'EG6', 'FT4' to 'FT6', and 'D3') between 'the UP' and 'DOWN' places represent the stochastic deterioration processes of these systems. In addition, the LOCA scenarios considered in the study are classified into three levels, namely leak, SBLOCA, and LBLOCA. Depending on the break size, the break flow from the primary coolant system is determined, resulting in different depressurisation and, hence different core cooling behaviours. The transitions 'D7', 'D11', and 'D14' represents the natural occurrence of a leak, SBLOCA, and LBLOCA respectively. In the study, it is assumed that they follow an exponential distribution, the failure rates are 0.0282, 0.0020, and 0.0004 failures per year, respectively [56]. The times for these transitions are computed using a random sampling method [57], of which the failure data follows a certain probability distribution with the parameters taken from the literature and listed in Table 1.

In Fig. 6, external events (e.g. earthquakes, tsunamis, etc.) that can lead to LOCA or SBO accidents are considered. The time delay 'D1' represents the time interval to the next external event, which can be obtained from local historical data. The transitions 'IS10' to 'IS18', 'SG1' to 'SG3', 'EG1' to 'EG3', 'FT1' to 'FT3', 'RA1', 'D4', and 'D12' represent the impact of the external event on the systems. The conditional arcs, represented by dashed arrows, connect these transitions to the places representing the health states of the subsystems. Whether a token is transferred to the 'DOWN' state for any subsystem depends on the probability that the corresponding system may be damaged by the external event. This probability is dependent upon many factors, such as the type and magnitude of the external events, the locations of the systems, etc. Hence, the probability data adopted in the paper are deduced based on experts' knowledge, assumptions, and reports of past accidents.

If an SBLOCA or an LBLOCA occurs and is detected, the reactor will be shut down. A token produced in the place 'Shut down the reactor', whose predefined condition for this place will embed the PN modelling the shutdown process, i.e. IRPN, into the simulation. In the study, it is assumed that the leak can only be detected manually. If a leak occurs and it is not detected within 100 h, the leak will develop into an SBLOCA accident modelled via the transition 'D9' [49]. The transition 'D8' is the time for the operators to detect the leak, which is assumed to follow a Weibull distribution with the shape parameter (β) of 1.2 and the scale parameter (η) of 86400 s.

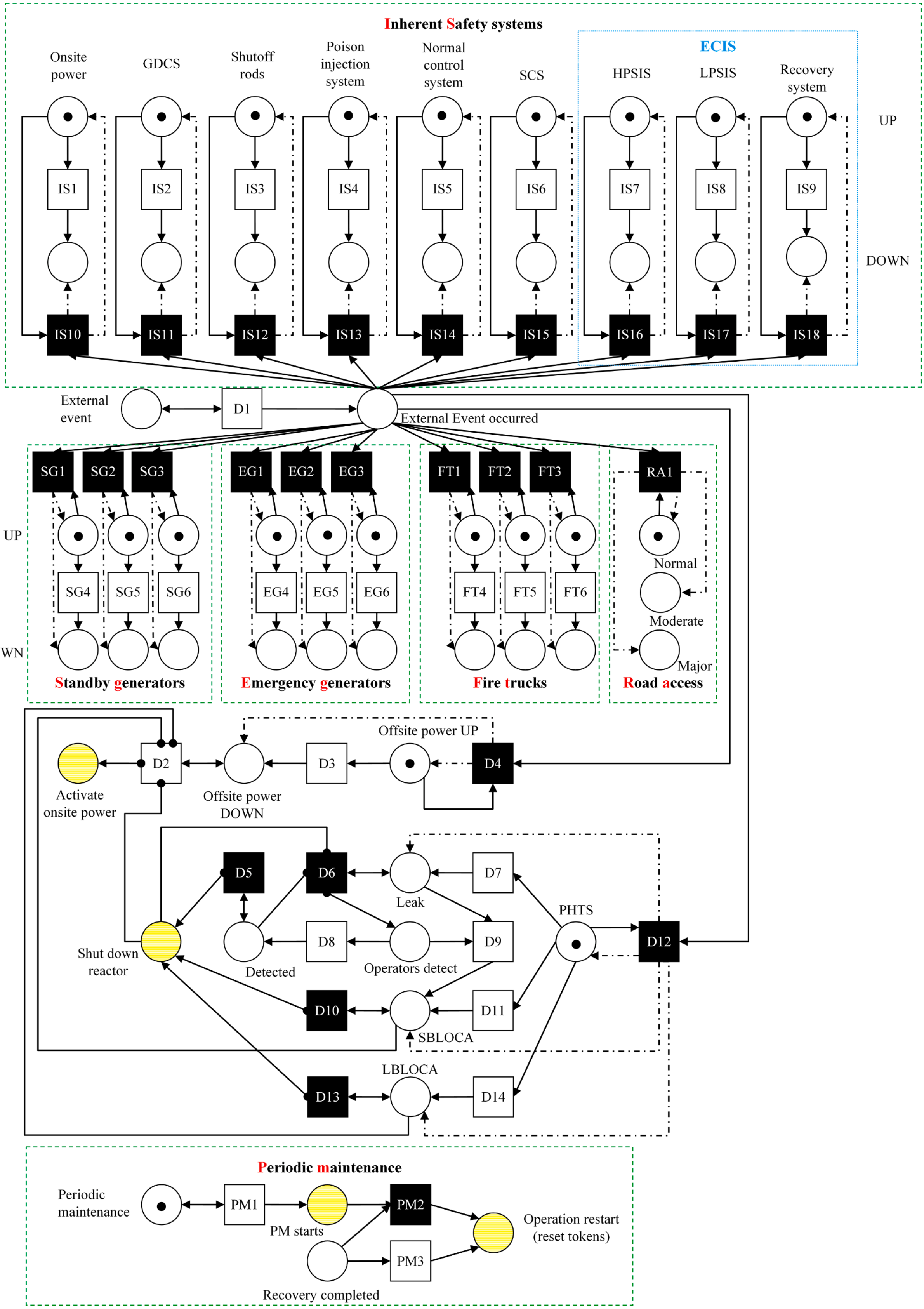


Fig. 6. The RSPN developed.

Table 1
Failure and repair data of the reactor subsystems and safety systems [56,58–61].

System(s)	Distribution	Parameter(s)	Average repair time (hour)
Offsite power	Exponential	failure rate (λ) = 0.0621 (failures per year)	2
Onsite power	Exponential	$\lambda = 0.00227916$ (failures per year)	6
GDCS	Exponential	$\lambda = 0.000227916$ (failures per year)	48 (assumed)
SDS1	Weibull	$\beta = 1.3000$ $\eta = 656.89$ (years)	120
SDS2	Weibull	$\beta = 1.5320$ $\eta = 5.7$ (years)	200
SCS	Exponential	$\lambda = 0.140256$ (failures per year)	184
Diesel generators	Exponential	$\lambda = 0.059$ (failures per year)	11.5
Normal control system	Weibull	$\beta = 1.284$ $\eta = 73.91$ (years)	120 (assumed)
HPSIS	Exponential	$\lambda = 0.0002279116$ (failures per year)	200 (assumed)
LPSIS	Exponential	$\lambda = 0.0024$ (failures per year)	10.8
Recovery system	Exponential	$\lambda = 0.0024$ (failures per year)	10.8
Fire trucks	Exponential	$\lambda = 0.14438$(failures per year)	7
Road access			120 (assumed for moderate damage) 1200 (assumed for major damage)

If there is a token in the 'Offsite power: DOWN' place and no leak or LOCA has occurred a token will be placed in the condition place 'Activate onsite power', which means the system will use onsite power to maintain the normal operation of the reactor. It should be noted that the transition 'D2' is associated with a very short time δ (say 0.0001 s in the research) to ensure that the shutdown process can have a higher priority than the activation of the onsite power to ensure the safety in emergencies where the reactor must be shut down for safety.

5.2. *Response modelling*

The responses of the reactor to an accident can be divided into two categories. The first category refers to immediate responses, such as shutting down the reactor, lowering the power output, activating backup systems, etc. The second category refers to those mitigation responses taken to restore the health state of the reactor to a safe margin and maintain the long-term safety of the reactor system after the reactor shutdown. Both categories of responses are modelled as described below.

5.2.1. *Immediate Response Petri Net (IRPN)*

To demonstrate the methodology, the IRPN for simulating the reactor shutdown process is presented in the paper. Once a LOCA or a leak is detected manually or automatically, the reactor will be shut down. The IRPN shown in Fig. 7 will then be embedded into the model to simulate the shutdown process of the reactor.

For a leak, if the operators detected it successfully within 100 h, a token will be placed in the place 'Detected by operators'. Then, the manual safe shutdown process will be initiated after 60 s modelled via the transition 'SD7'. If the normal control system (NCS) is available, the reactor will be shut down safely. The time required for the manual shutdown process is assumed to be 300 s as modelled via the transition 'SD8'. However, if it is not available, the emergency shutdown system must be activated immediately to trip the reactor. This process is modelled via the transition 'SD9' with an assumed time of 30 s.

LOCA accidents causing the pressure change in the PHTS will be detected automatically by the reactor system itself so that the emergency shutdown systems will be activated. The shutoff rods (SDS1) will be activated first, if this fails, the poison injection system (SDS2) will then be activated. The time required for the pressure to reach the activation threshold of each shutdown system is simulated via the transitions 'FD1' and 'FD2' in Fig. 7. The times for these two transitions are assumed to be 2 and 5 s for LBOCA, and 60 and 70 s for SBLOCA respectively. A reactor trip results in the loss of a large amount of electric-power generation, which can cause voltage instability directly in the offsite transmission-system grid. This instability can degrade voltage protection (relays) which then disconnects the Class 1E buses from the offsite grid [21,62]. This will lead to an SBO accident. As a result, the emergency power supplies (e.g. SDGs) must be activated to provide power for the electrical safety systems such as the LPSIS.

In the worst scenario, if both shutdown systems fail, then the reactor cannot be shut down successfully, which will cause rapid melt of the core. In this case, the operators need to activate the emergency plan to manage the crisis before the core melt. The time of the transition 'SD6' represents the time that the reactor core melts after the moderator is exhausted. Since it is assumed that the melted reactor core is not recoverable, the simulation will be ended immediately once a token is produced in the red terminate place 'core melt'. This event is not pursued further since it is assumed that there are no additional mitigating systems available to limit its consequences in the study.

If the reactor is shut down successfully, i.e. a token is produced in the 'Successful shutdown' place, the MPPN will be embedded into the model to simulate the responses for maintaining the long-term cooling to remove the decay heat.

5.2.2. *Mitigation Process Petri Net (MPPN) for LOCA only*

If the offsite power is available and the SHTS is able to maintain its cooling loop, the only thing to consider is the ECIS that provides the cooling capacity needed to restore the PHTS. As described in Section 3, the reactor will be cooled under manual control if the reactor was shut down due to a leak. The PN for modelling this process is given in Fig. 8. With the aid of offsite power, the break can be isolated by the use of valves. The time assumed for initiating the action is set to be 300 s, which is modelled via the transition 'CR1'. Then the isolation process modelled via the transition 'CR3' will take 30 s. However, if the offsite power has failed, the operators will start to isolate the break using valves manually after 1800 s, which is modelled via the transition 'CR2'. This process, modelled via the transition 'CR4', is assumed to take 300 s. The time taken for identifying and replacing the leaking tube is assumed to be 1 h and this process is modelled via the transition 'CR5'. The heavy water in the PHTS will be restored to its original level by bringing in reserve heavy water. The process is modelled via the transition 'CR6' and the time required for it is assumed to be 300 s.

If the reactor is shut down due to a LOCA event, the ECIS will be activated automatically to mitigate the damage to the reactor core and maintain long-term cooling of the PHTS by establishing an alternative cooling loop for the long-term heat sink. This cooling process is modelled via the PN illustrated in Fig. 9. The activation time of each emergency injection system for different sizes of LOCA is derived based on the past literature and given in Table 2 [63].

The firings of the transitions 'PC2', 'PC3', and 'PC4', indicate the corresponding injection systems are not available. The time delays of the transitions 'PC2', 'PC3', and 'PC4'are set to be 120, 600, and 600 s longer than the transitions 'PC5', 'PC6', and 'PC7' respectively. In the study, it is assumed that the failure of either HPSIS or LPSIS, or both, will result in limited core damage even if the recovery system can be activated to maintain long-term cooling afterwards. The transition 'PC7' represents the time for activating the recovery system, which is assumed to be 30 s. Once the recovery system is activated successfully, long-term cooling is then achieved. However, if the recovery system is not available, then operators must use fire trucks to inject the water directly into the PHTS. The PN modelling of this process is given in the bottom part of

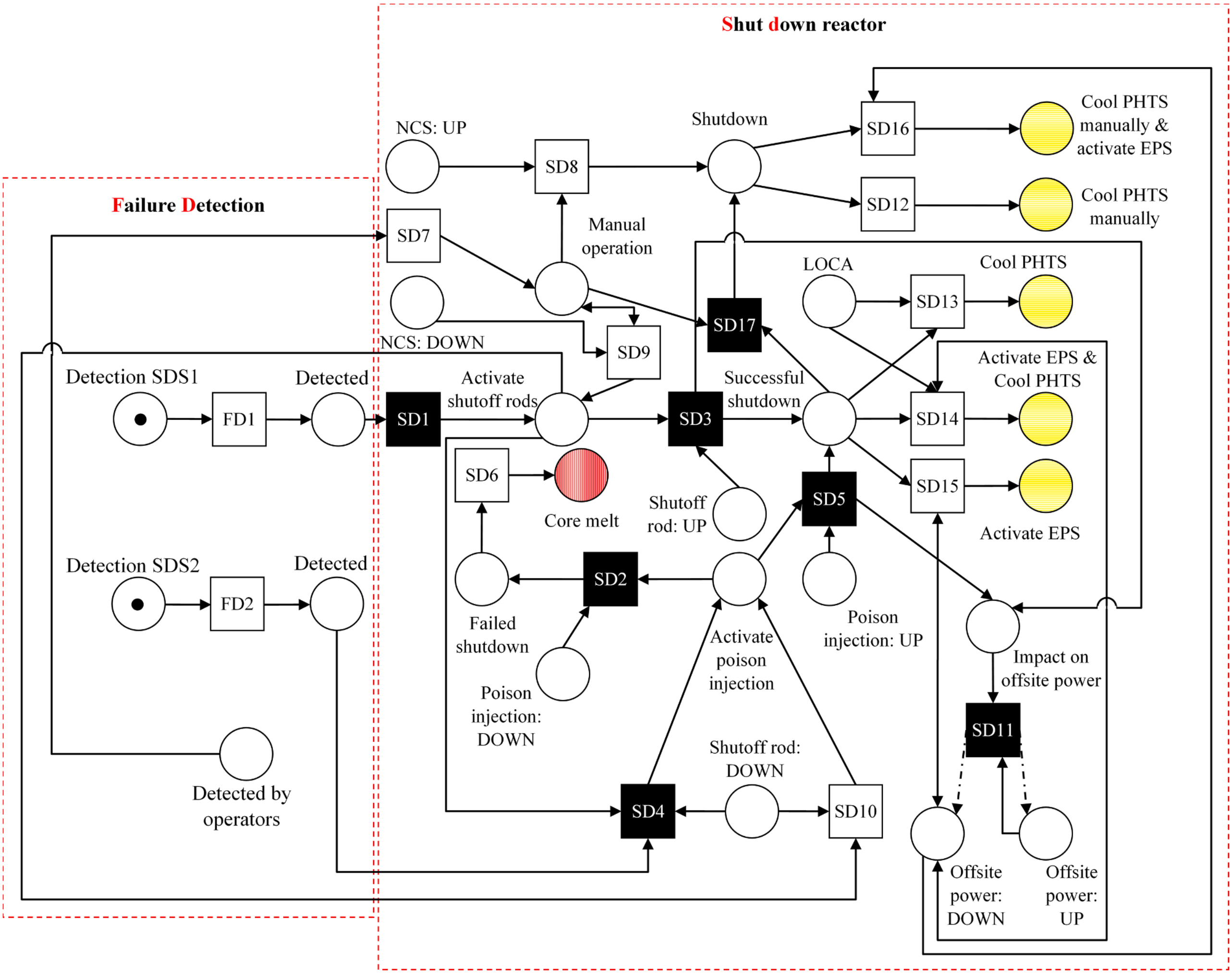


Fig. 7. IRPN – Shutdown process.

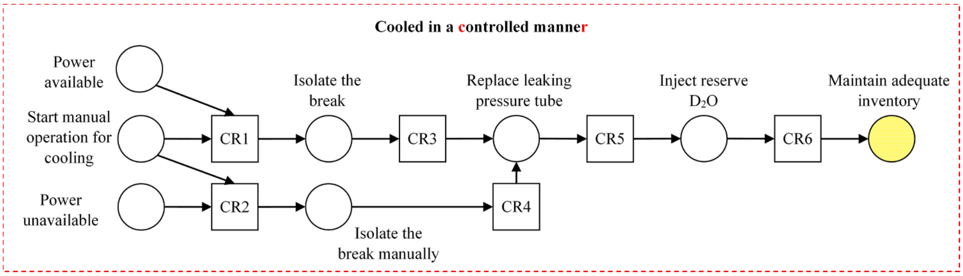

Cooled in a controlled manner
Power available
Start manual operation for cooling
Power unavailable
CR1
CR2
Isolate the break
CR3
Isolate the break manually
Replace leaking pressure tube
CR4
CR5
Inject reserve D₂O
CR6
Maintain adequate inventory

Fig. 8. MPPN for a leak scenario.

Fig. 9.

In the figure, the health state of each fire truck is imported from the RSPN into the model. The transition 'BC1' is the time taken for the emergency response operators to get the fire trucks ready, which is assumed to be 600 s. It is assumed that two fire trucks can provide sufficient cooling for the reactor. Hence, the weight of the arc connecting the 'Number of FTs available' place and the 'BC1' transition is 2. The transition time of 'BC3' is the time taken for the operators to drive the fire trucks to the water injection site, which is assumed to be 5 min, 30 min, and 14 h, respectively under the road access condition of no damage, moderate damage, and major damage, respectively. Road accessibility is modelled in the RSPN. Once the fire trucks arrive at the site, the injection can be initiated after 60 s. This process is modelled via the transition 'BC4'. In the study, it is assumed that the pressure in the system is low enough for the fire truck injection when the fire truck arrives.

The time of the transition 'BC7' taken for reducing the core temperature to 55°C is assumed to be 8 h because the actual injected volume to the reactor core region is difficult to predict [64]. The time can be easily modified or modelled as an appropriate distribution once more relevant data are available. If the transition 'BC9' is enabled, a token will be produced in the 'Long-term core cooling' place immediately because it is assumed that the long-term core cooling can be maintained by the fire trucks. The token in the 'Long-term core cooling' place will embed the RMPN into the model. However, if less than two fire trucks are available the transition 'BC2' will fire and, a token will be produced in

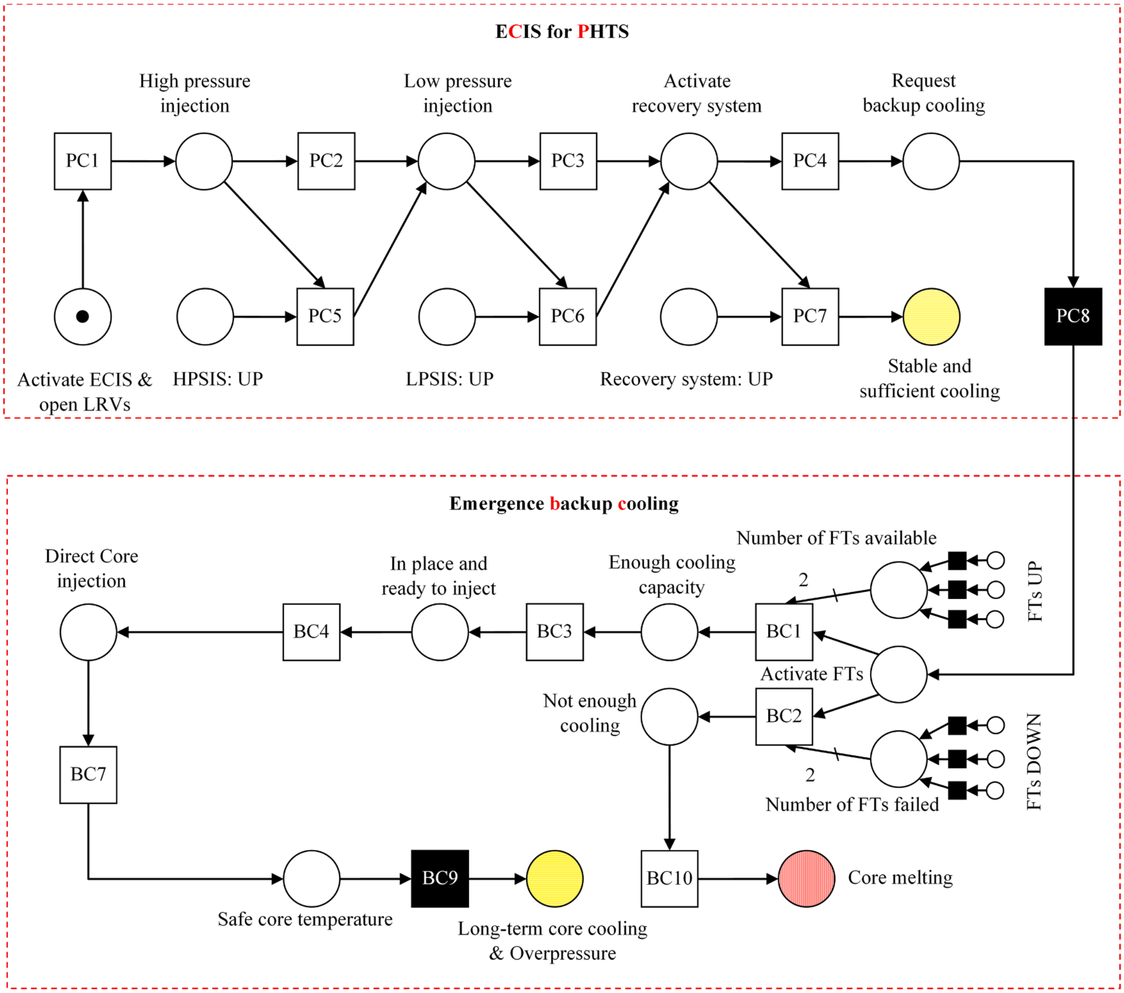


Fig. 9. MPPN for a LOCA accident.

Table 2
The time required for different LOCAs.

Injection activation	Transition	LBLOCA	SBLOCA
Reaching the HPSIS activation pressure	PC1	30 s	300 s
Reaching the LPSIS activation pressure	PC5	180 s	600 s
Recovery system activation time	PC6	180 s	600 s

the 'Not enough cooling' place, which means that there is not enough cooling capability to remove decay heat. Based on the past literature [65], the time (t_D) of the transition 'BC10' is assumed be 31,570 s for a SBLOCA and 28,850 s for a LBLOCA, respectively. The reactor damage can be deduced based on the time (t_S) before a token is produced in a condition place or a terminate place. The details are given in Table 3. It should be noted that these values are currently only based on assumptions for method demonstration purposes and can be easily updated once more accurate data become available.

Table 3
Reactor damage estimation.

Health state of the reactor	Time before core melt (seconds)
No core damage	$21,500 < t_D - t_S$
Limited core damage	$7,800 \leq t_D - t_S < 21,550$
Significant core damage	$0 \leq t_D - t_S < 7,800$
Reactor core melt (i.e. nuclear fuel begins to melt)	$t_D - t_S < 0$

5.2.3. Mitigation Process Petri Net (MPPN) for LOCA with loss of offsite power

If the offsite power is not available after the shutdown, the emergency power supply must be activated to provide essential power for some of the safety systems. In addition, the SHTS must be cooled to remove the heat from the PHTS. The activation sequence of different safety systems for cooling both loops is illustrated in Fig. 10. The left side of the figure illustrates the cooling of the SHTS and the right side is for establishing a new cooling loop for the PHTS. It also shows both the LPSIS and recovery system require power from diesel generators to work. The failure of some critical safety systems, e.g. HPSIS and LPSIS, will have a direct impact on the reactor's state.

The PN for modelling these processes is given in Fig. 11. The activations of the emergency power supply and the ECIS will be initiated simultaneously. The HPSIS, which does not require electrical power, can start its operation automatically once the pressure in the PHTS falls to a certain threshold if it has not failed. Both the LPSIS and the recovery system require electric power to pump water to the PHTS. It is assumed that if either one of the SDGs or EDGs can be activated, the reactor core will not be damaged. Hence, the times of the transitions 'PC3' and 'PC4' are assumed to be 600 s longer than 'PC6' and 'PC7' respectively. The activation times of the SDGs and EDGs, i.e. Transitions 'EP1' and 'EP2', are assumed to be 120 s and 240 s, respectively. If both the recovery system and the emergency power supply are available, The PHTS will have a new cooling loop which will be represented by a token produced in the place 'New cooling loop for the PHTS established'. More details about the PNs for activating the diesel generators can be found in [20].

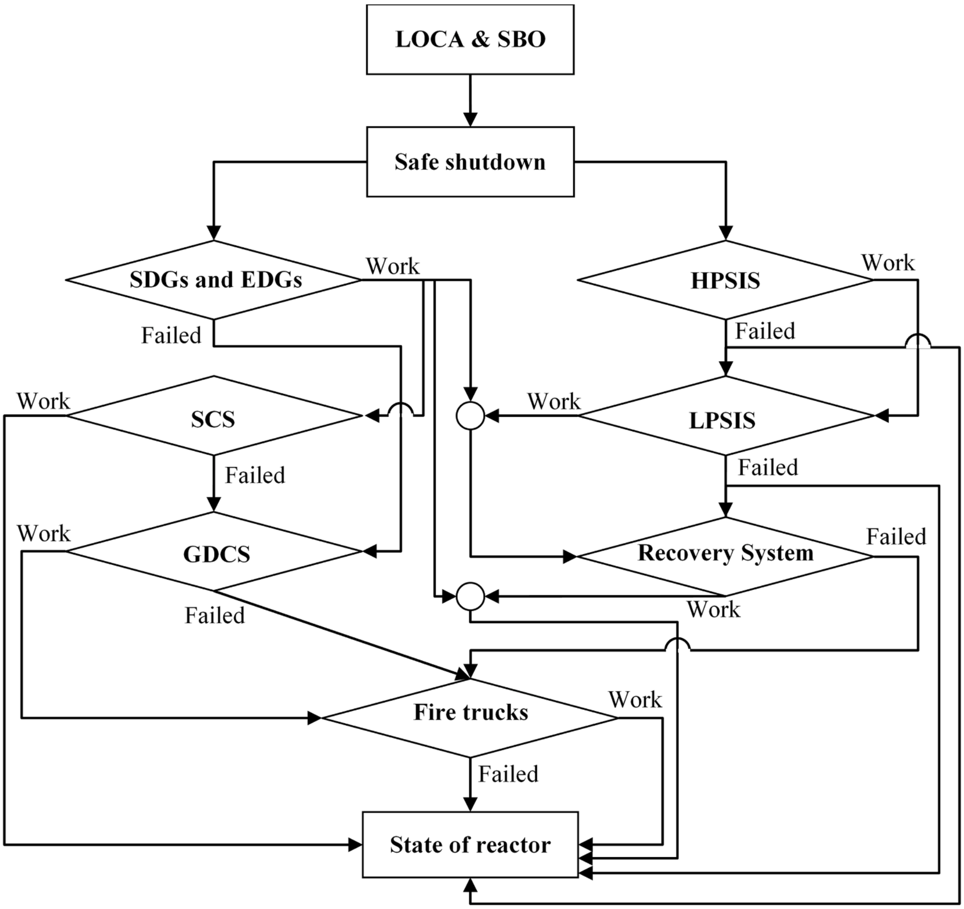


Fig. 10. Flowchart of emergency cooling processes for LOCA and SBO.

The SHTS can maintain its long-term cooling by the SCS with the emergency power supply. The activation time of SCS is assumed to be 30 s which is modelled by the transition 'SC1'. If both the recovery system and the SCS can be activated successfully, the system can maintain its long-term cooling and a token will be produced in the place 'Long-term core cooling'. The health state of the reactor core will then be assessed based on the path and time of the flow of tokens in the PN as stated in Table 3. If the reactor core does not melt, the RMPN will be embedded into the model to model the restoration of the reactor's power generation.

If either of these two safety systems cannot be activated, the operators must use fire trucks to inject the water into the system. If no coolant water leaked out from the PHTS due to a break or the opening of the valves, the fire trucks will inject water into the SHTS. Otherwise, it will inject water into the PHTS to cool the reactor core directly. If only the SHTS cannot be cooled, the GDCS can be activated to provide the cooling for up to 2 h which is the total time of the transitions 'EF1', 'EF3', and 'EF4'. This aims to provide sufficient time for the deployment of the fire trucks. A detailed description of the PNs for the fire trucks is given in Section 5.2.2. However, it should be noted that if the recovery system can be activated successfully, the time (t_D) of the transition 'BC10' is assumed to be 56,770 s based on the past literature [65]. If the GDCS that can provide up to 2 h of cooling is available, the transition time is set to be 63,970 s. More details about the PNs for activating the GDCS and fire trucks can be found in [20]. Based on Table 3, the reactor damage can be deduced following the same logic as described in Section 5.2.2. Once a token is produced in the place 'Long-term core cooling', the RMPN will be embedded into the simulation if the reactor core has not melted. The top part of the PN simulating the activation of ECIS can be replaced by the MPPN developed for a leak scenario if a SBO accident and a leak have occurred simultaneously.

5.3. Recovery and Maintenance Petri Net (RMPN)

Once the accident is under control or the reactor has been successfully shut down and maintained long-term cooling, the recovery and maintenance activities will be initiated to restore its normal operation as soon as possible to minimise the loss of power generation. Hence, the RMPN shown in Fig. 12 will be embedded into the model following the IRPN or MPPN. Before the RMPN is embedded into the model, it will be initiated by gathering information about the failed systems from the RSPN and the health status of the reactor core. In contrast to the RMPN developed in [20], the RMPN in this paper also takes into account the accident assessment and the approval phase of the maintenance plan.

In the study, it is assumed that there are enough maintenance resources to maintain all systems simultaneously. In the figure, the time of the transition 'IN1' is assigned for inspecting all the systems, investigating any areas of concern identified, and a root cause analysis, which is assumed to be 3 days. The transition 'IN2' represents the time for preparing a repair plan following standards and requesting and obtaining approval, which is assumed to be 3 days in the research. The time of the transition 'CM1' is the mean time required to repair the offsite power supply. The PNs for simulating the maintenance of other systems are similar to the PN used for offsite power and these are represented by the dotted boxes in the figure. The overhaul can only be regarded as completed after all systems are maintained, i.e. there is no token left in any 'DOWN' places in the figure. After all the maintenance activities are completed, the necessary clean-up such as removing the shutoff rods from the core, purifying the moderator, or even removing the radioactive materials from the containment, must be undertaken.

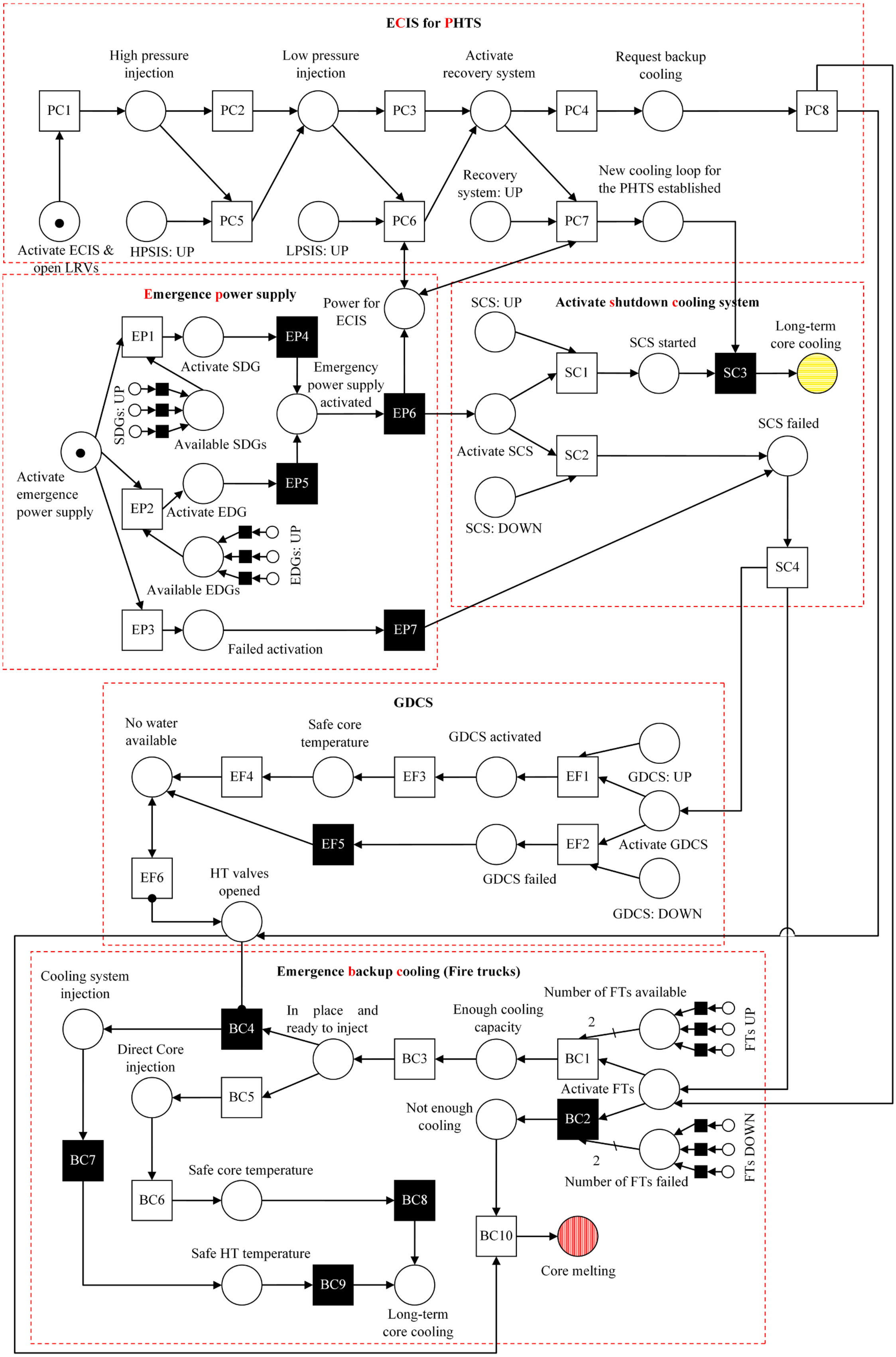


Fig. 11. MPPN for LOCA and SBO.

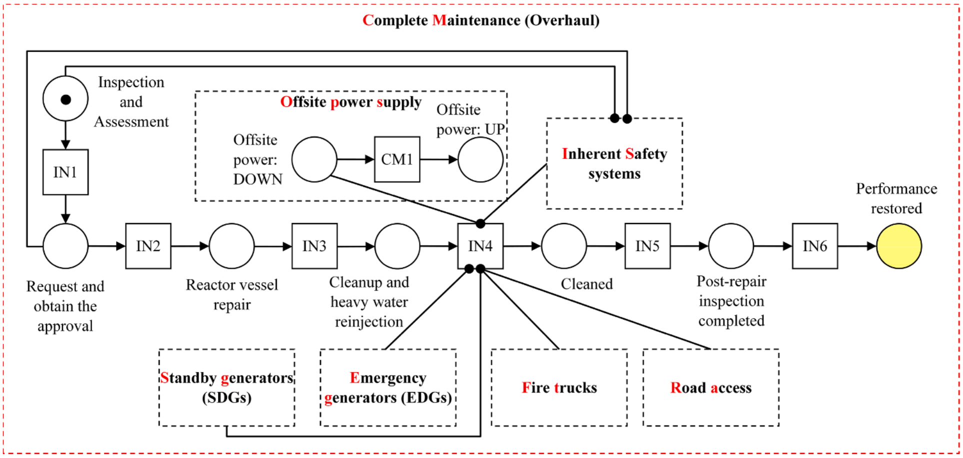

Complete Maintenance (Overhaul)
Inspection and Assessment
IN1
Offsite power supply
Offsite power: DOWN
CM1
Offsite power: UP
Inherent Safety systems
Performance restored
IN2
IN3
IN4
IN5
IN6
Request and obtain the approval
Reactor vessel repair
Cleanup and heavy water reinjection
Cleaned
Post-repair inspection completed
Standby generators (SDGs)
Emergency generators (EDGs)
Fire trucks
Road access

Fig. 12. The PN for simulating the overhaul.

The clean-up and reactor repair times in different scenarios are listed in Table 4. They will be imported into the transitions 'IN3' and 'IN4' respectively. The time of the transition 'IN5' is assigned for the final inspection before restarting the reactor, which is assumed to be 3 days. The transition 'IN6' represents the time needed for the restart process of the reactor. Its associated time is 5464 s, which is deduced based on the fact that the maximum allowable rate of temperature change of the primary coolant is 2.8°C/min in a CANDU 6 reactor, a Canadian pressurized heavy-water reactor design [66]. Finally, a token will be produced in the 'Performance restored' place, which means the reactor has been restarted and resumed its normal operation successfully. Then, the health states of all the systems will be fed back to the RSPN.

6. Resilience assessment

In the following, the PN models developed in Section 5 will be employed to assess the resilience of the single-unit NPP. The PN models developed are analysed using Monte Carlo simulation. During the simulations, critical information, such as the duration of any token's residence in a place, the number of transitions fired, etc. is logged. The failure rates and average repair times of all reactor subsystems and safety systems listed in Tables 1 to 4 are used as inputs of the model. The simulation is based on the following assumptions.

- The systems are as good as new after maintenance.
- The safety systems do not fail when in operation.

The simulation is implemented by the following steps:
Step 1: Initialise the simulation.

(1) Identify and characterise the external event.
(2) Define the time of its first occurrence and the frequency of its occurrence.
(3) For each system considered, define the probability of the external event causing damage.
(4) Initialise the simulation time, i.e. set t = 0.

Step 2: Define the PN model.

(1) Define the places, transitions, the arcs connecting them, and the conditions for every condition place and terminate place.
(2) Define the time for the transitions with a fixed duration. Generate time for the transitions such as time to failure by using random sampling methods from the appropriate distributions as described in [57].
(3) Define the conditional probability of each conditional arc based on the probability of causing damage.

Step 3: Identify and fire the enabled transition with the minimum switching time in the whole model.

Step 4: Check all immediate transitions. If enabled, fire them.

Step 5: Repeat Step 4 until no more immediate transitions are enabled.

Step 6: Repeat Steps 3 to 5 until a token is produced in one of the condition places or terminate places.

Step 7: Define the current health state of the nuclear reactor. Activate the conditions predefined for the condition place or terminate place that contains a token.

Step 8: Check the following two conditions

(1) Has the time reached the lifetime of the nuclear reactor?
(2) Has the nuclear reactor core melted?

If either condition is 'Yes', start the next iteration. Otherwise, repeat Steps 2 to 8.

Step 9: Iterate the above simulation until the defined iteration time is reached.

6.1. Simulation results analysis

The impact of external events on the resilience of the reactor system is investigated using the simulation steps outlined above. The associated mitigation and recovery strategies for the external events are analysed. In the paper, three external events that cause different levels of damage to the reactor systems are considered. These events are defined in Table 5 where the probabilities of the events causing damage to each system are listed. The data in the table is based on past accident reports

Table 4
The cleanup and core repair time required for different scenarios.

Health state of the reactor	Repair time ('IN3' transition)	Cleanup ('IN4' transition)
No core damage, no LOCA, SDS1 activated	0	30 min [63]
No core damage, no LOCA, SDS2 activated	0	1 day (24 h) [63]
No core damage, Leak	1 day (assumed)	5 days (assumed)
No core damage, SBLOCA	3 days (assumed)	60 days (assumed)
No core damage, LBLOCA	14 days (assumed)	60 days (assumed)
Limited core damage	30 days [67]	60 days [67]
Significant core damage	365 days [68]	548 days [68]
Core melting	Not repairable [69]	15 years [69]

Table 5
Probabilities that the systems are damaged by the three external events.

System(s)	The probability of damage		
	External Event 1	External Event 2	External Event 3
Offsite power	40%	90%	100% (earthquake, tsunami, and flood)
Onsite power	20%	70%	100% (reactor has to be shut down due to safety issues after a great earthquake)
GDCS	5%	5%	40%
SDS1	0.1%	1%	5%
SDS2	1%	2%	20%
SCS	20%	40%	70%
SDGs	30%	80%	100%
EDGs	5%	40%	92.3%
Normal control system	0.1%	1%	5%
Leak	1%	2%	20%
SBLOCA	0.5%	1%	10%
LBLOCA	0.05%	0.1%	1%
HPSIS	1%	2%	20%
LPSIS	20%	40%	70%
Recovery system	20%	40%	70%
Fire trucks	10%	20%	20%

Road access	40% no damage;
	50% moderate damage;
	10% major damage
		20% no damage;
		40% moderate damage;
		40% major damage
			10% no damage;
			10% moderate damage;
			80% major damage

and expert knowledge. Due to the uncertainty of the occurrence of these extreme external events and the probabilistic nature of the problem considered, the research aims to anticipate the worst possible realisation of the uncertainty of component failures in the reactor system under external disruptive events. In other words, the settings of all the input parameters (i.e. the damage probability values) in the PN models are assumed to be the highest possible values that may occur. The data for External Event 3 is based on the data recorded from Reactor Unit 1 in the Fukushima Daiichi nuclear power plant when it was hit by the tsunami in 2011 [5,70]. However, some modifications have also been made to adapt to the PHWR considered. It is worth noting that although it has previously been considered that LOCAs, especially LBLOCAs, are highly unlikely to be caused by external events. It is still possible for them to occur as a result of failure of supports of the large components in reactor systems (e.g. reactor pressure vessel) due to a severe event, such as an earthquake. The data of the other 2 events are based on the lower magnitude and severity accidents than that modelled as Event 3 in order to examine their impact on the resilience of the NPP.

The resilience to these external events consists of two parts, mitigation and recovery. The mitigation part is focused on absorbing the different levels of the impact caused by the external events on the reactor system. These impacts are classified into 6 levels, as listed in Table 6. The recovery part is focused on completely restoring the damaged reactor system from varying health states. The recovery state of the damaged reactor system is also divided into 6 levels, as shown in Table 7.

Table 6
Definition of operation and health state level.

Operation & health state level	Definition
5	Normal operation – Offsite power
4	Normal operation – Onsite power
3	Safe shutdown & no damage to the reactor core
2	Limited damage to the reactor core
1	Significant damage to the reactor core
0	Reactor core melt

Table 7
Definition of recovery level.

Recovery level	Definition
5	Normal operation
4	All systems are repaired and the reactor system is cleaned
3	Safe shutdown & no damage to the reactor core
2	Limited damage to the reactor core
1	Significant damage to the reactor core
0	Reactor core melt

The recovery level 4 in Table 7 is different from the operation & health state level 4 in Table 6 as the reactor must be restarted with offsite power for the recovery part. Once an important event (e.g. the shutdown of the reactor, the activation of the HPSIS, etc.) takes place, the relevant time and information can be recorded during the simulation. Then, the corresponding operation & health level or recovery level of the reactor is categorised. The categorised results can then be plotted in a figure against their occurrence time. A typical resilience level line of the reactor following an accident is given in Fig. 13 as an example. The left and right y-axes of the figure represent the operation & health level and the recovery level, respectively. In this figure, it is assumed that the accident happens at $t = 1$s. Then, the line changes from Level 5 to Level 3 within 2 s, indicating that the reactor has been successfully shut down by the SDS1. Subsequently, the line remains at Level 3 until around 520,000 s after which it rises, which means that the long-term cooling has been successfully implemented attributed to the successful activation of the ECISs. As long as the long-term cooling can be maintained, recovery and maintenance activities can be carried out. From the figure, it is found that it then takes around 74 days to fully recovery and clean the reactor system. In the figure, this is represented by the line eventually rising to Level 4. Finally, it took about 3 days for the line to rise to Level 5, which means the final inspection is completed, the reactor was restarted, and the normal operation of the reactor was resumed. It should be noted that the level line may be different for each simulation iteration. This is because the failure time of each system is computed using a random sampling method in the simulation.

To ensure the reliability of the simulation results, a convergence study of the simulation is conducted. The results are shown in Fig. 14, in which the calculated probability of core melt due to External Event 1 without stochastic deterioration of the subsystems considered converges to a stable value after running the simulation iterations 300,000 times. Therefore, in the subsequent calculations, the number of iterations is set to 500,000 to ensure reliable results.

The health state levels and the recovery levels of the reactor and their occurrence probabilities, the probabilities of the final states of the reactor in different scenarios, and the overall resilience of the reactor system are calculated and are given in Table 8. The overall resilience (Re_o) is calculated as the sum of the probability that normal operation will continue (P_N) and the probability that the reactor system will be able to recover its performance within 12 days (P_{short}). It should be noted

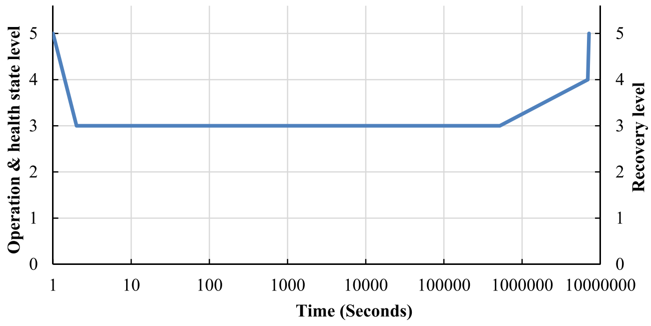


Fig. 13. An example of the resilience line due to an LBLOCA.

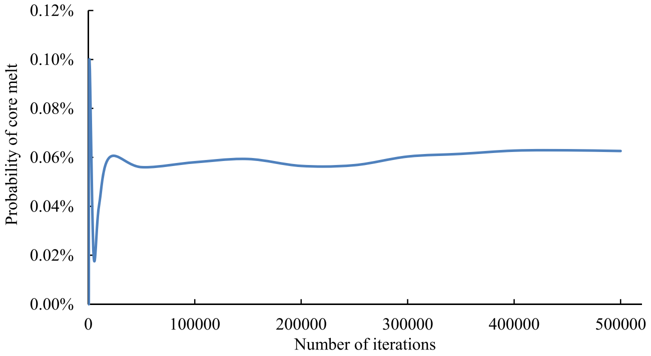


Fig. 14. Simulation convergence.

Table 8
Probabilities of the final status of the reactor in different scenarios.

Resilience metrics	Final health status of the reactor	Probability External Event 1	External Event 2	External Event 3
Resistant capability	Normal operation continued (P_N)	90.59%	35.88%	0.00%
Recoverability	Recovery within 12 days (P_{short})	5.47%	19.51%	1.77%
	Recovery longer than 12 days but shorter than 116 days (P_{mid})	3.87%	41.16%	57.51%
	Recovery longer than 116 days but shorter than 3.5 years (P_{long})	0.01%	0.48%	24.62%
Absorption capability	Limited core damage (P_{LD})	0.26%	9.48%	38.56%
	Significant core damage (P_{SD})	0.01%	0.48%	24.62%
	Core melt (P_{CM})	0.06%	2.97%	16.11%
Overall resilience (Re_o)		96.06%	55.39%	1.77%

that in these results, stochastic deterioration is neglected.

The resilience capability of an NPP to external disruptive events is characterised by how much the reactor is affected by the external events and how soon the reactor can resume normal operation. However, quantifying that resilience is a complex task in practice. It cannot be simply defined using one criterion. From the results in Table 8, it is shown that the NPP displays different resilience capabilities dependent upon external events. The resistant capability, i.e. the probability that it can continue normal operation, is 90.59%, 35.88%, and 0 for the three external events considered. It is 0 for External Event 3 as the reactor has to be shut down for safety reasons and hence cannot maintain its normal operation after an event of such magnitude. For External Event 2, the reactor is most likely to be recovered between 12 days and 116 days if the reactor is shut down. From the results shown in the table, it is also found that there is a possibility of core melt for all scenarios.

In Events 1 and 2, the fire trucks are more likely to arrive in time to provide cooling if fire trucks are required. This will increase the safety of the reactor core to a large extent. Hence, the probability of significant core damage due to the late arrival of fire trucks is much lower than that of limited core damage. On the other hand, it is found that the probability of core melt is higher than the probability of significant core damage. This is because, in the current research, it is assumed that at least two fire trucks are required to provide sufficient cooling capacity. However, we only considered three fire trucks in the modelling. This means that sufficient cooling capacity cannot be always guaranteed because two of the three fire trucks may not arrive due to any reason after external events happened. This is why in Events 1 and 2, the probability values shown for core melt are even greater than the probability values for significant core damage. In practice, this can be avoided by increasing the number of fire trucks and using offsite fire trucks to ensure the required cooling capacity to prevent core melt. This will make core melt rarer than significant core damage. The overall resilience of the reactor system is calculated to be 96.06%, 55.39%, and 1.77% respectively. This means that there are probabilities of 0.9606, 0.5539, and 0.0177 to keep the total economic losses and social and environmental impacts of these three external disruptive events within acceptable limits, respectively.

The impact of stochastic deterioration on the resilience capacity of the reactor system has been investigated by assuming External Event 3 happens after 0, 0.5, 1, 1.5 and 2 years of operation of the reactor. It is assumed that no periodic inspection or maintenance has been conducted during these times. The absorption capability and the recoverability of the reactor system as a function of the external event occurrence time are plotted in Figs. 15 and 16 respectively. From Fig. 15, it is found that the probability of core melt increases linearly with the time of the external event occurrence. The probability of core melt increases from 16.11% to 38.77%, which is more than doubled. It suggests that the unavailability of the safety system especially the fire trucks increased drastically. From this, it can be inferred that setting the interval of periodic maintenance of fire trucks to 2 years is too long to ensure the availability of the fire trucks when required. In addition, the probabilities of no damage, limited core damage, and significant core damage decrease linearly with time as the probability of core melt increases. From Fig. 16, it is also found that the recoverability of the reactor system decreases linearly. In addition, the recovery time (*tr*) is more likely to be within 116 days. However, it is noticed that is unlikely to recover its performance within 12 days after the disruptive event.

The resistant resilience and overall resilience of the reactor system over time by assuming the external event happens after 0, 0.5, 1, 1.5 and 2 years of operation of the reactor, are plotted in Figs. 17 and 18, respectively. All three events are investigated and their impact on the resilience of the reactor system is compared. Fig. 17 shows that the resistant resilience of the reactor remains roughly constant over time for all three events. The reason is that if only an SBO accident occurs, the probability of the onsite power supply failure due to stochastic deterioration is very low within 2 years, and if a LOCA occurs, the reactor must be shut down. From Fig. 18, it is found that the overall resilience keeps relatively constant until the time of the external event occurring is set to be 2 years or higher for Event 1. It dropped by around 1.5% when the time increased from 1.5 years to 2 years. This is because the failure probability of the safety systems due to stochastic deterioration does not increase significantly within 1.5 years and starts to become relatively significant after 2 years. For Events 2 and 3, a linear downward trend can be observed. The reason is that the reactor is more likely to be shut down in these two events. After the shutdown, all the safety systems will be inspected and repaired, which usually takes longer than 12 days as some of the failed safety systems have long repair times (such as the SCS). These systems can fail due to stochastic deterioration. As the

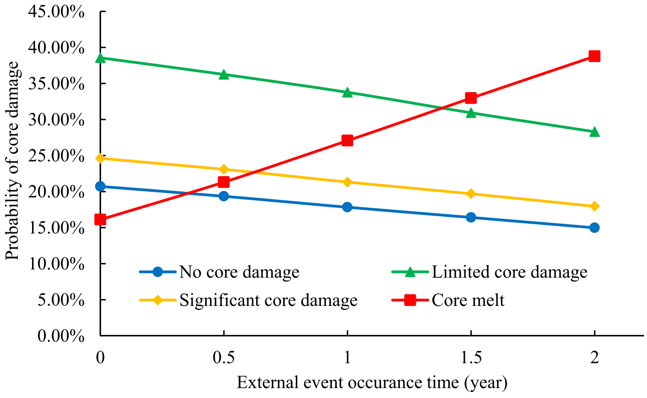


Fig. 15. Probability of different core damage levels against time.

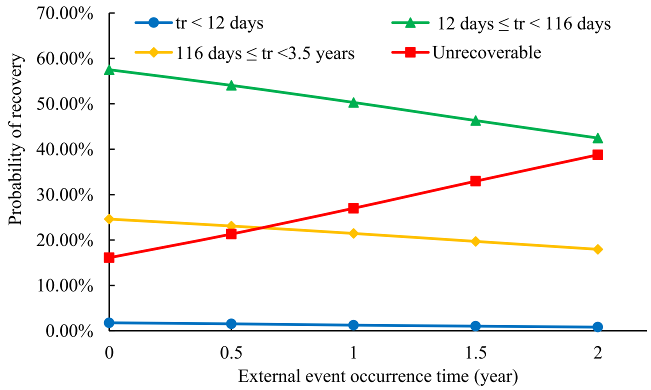


Fig. 16. Probability of different recovery time against time.

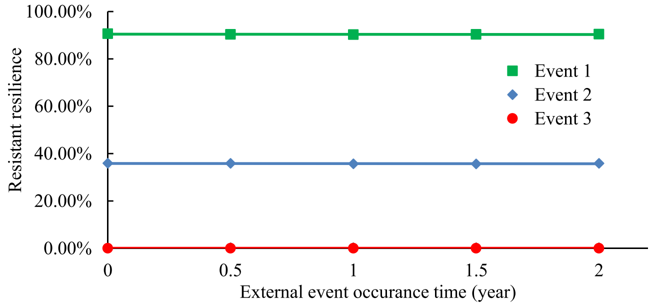


Fig. 17. Resistant resilience against time.

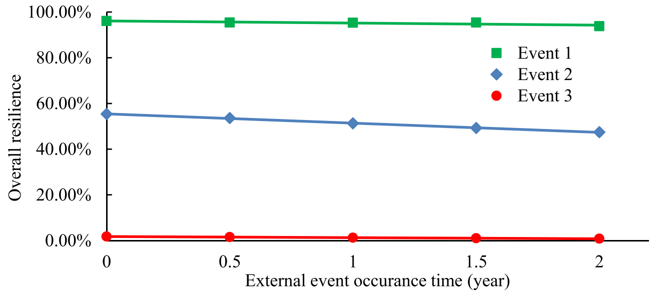


Fig. 18. Overall resilience against time.

failure of most safety systems follows an exponential distribution in the study, these lines tend to be linear.

7. Conclusion

In the study, the PN models are developed for assessing the resilience of NPPs against HILP events. Four metrics, i.e. resistant capacity, absorption capacity, recoverability, and overall resilience, are assessed quantitatively. From the work reported above, the following conclusions can be reached:

- The resilience of the NPP to HILP events can be successfully assessed by using the PN models. The impact of possible simultaneous LOCAs and SBO accidents on the resilience of the NPP is evaluated successfully.
- In comparison with traditional probabilistic safety assessment, the methodology developed in this paper can not only predict the probabilities of core damage in different scenarios, but also the probabilities of different core damage levels. In addition, it can be used to predict how soon the reactor system can be recovered from different kinds of accidents.
- The stochastic deterioration that does not directly affect the operation of nuclear reactors is critical to the resilience of NPPs. Both absorption capability and recoverability decrease linearly with time if no periodic inspection or maintenance is conducted, while the probability of core melt increases linearly. In addition, the overall resilience also decreases linearly over time, especially when the reactor is more likely to be shut down due to external events. On the other hand, the resistant resilience remains roughly constant whenever an external disruptive event occurs.

Despite these important findings from the study, the work can be further improved in the future. For example, the times of some transitions are either based on past literature or assumptions. It is expected to combine the PN models developed with mature thermo-hydraulic codes, such as RELAP or CATHENA [65,71], to further improve the reliability and accuracy of the simulation results. In addition, the control systems can also be modelled using PNs so that human-related events, such as cyber-attacks and human error, can be investigated.

CRediT authorship contribution statement

Rundong Yan: Methodology, Data curation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Sarah Dunnett:** Conceptualization, Supervision, Resources, Writing – review & editing, Project administration, Funding acquisition. **John Andrews:** Conceptualization, Resources, Writing – review & editing, Project administration, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

Data will be made available on request.

Acknowledgement

The work was supported by the Engineering and Physical Sciences Research Council EPSRC (grant number EP/R021759/1), which is part of the UK-India Civil Nuclear Collaboration program.

References

[1] World Nuclear Association. World nuclear performance report. https://www.world-nuclear.org/our-association/publications/global-trends-reports/world-nuclear-performance-report.aspx. [Accessed 25 July 2022].

[2] World Nuclear Association. World nuclear performance report 2022. World Nuclear Association; 2022.

[3] IAEA. The Fukushima Daiichi accident report. Vienna: IAEA; 2015.

[4] Aldemir T. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Ann Nucl Energy 2013;52:113–24. https://doi.org/10.1016/j.anucene.2012.08.001.

[5] Cai Y, Golay MW. Formulation of a risk assessment framework capable of analyzing nuclear power multiunit accident scenarios. Reliab Eng Syst Saf 2020;202:107040. https://doi.org/10.1016/j.ress.2020.107040.

[6] Panteli M, Mancarella P. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. IEEE Syst J 2017;11:1733–42. https://doi.org/10.1109/JSYST.2015.2389272.

[7] Khaloie H, Abdollahi A, Rashidinejad M, Siano P. Risk-based probabilistic-possibilistic self-scheduling considering high-impact low-probability events uncertainty. Int J Electr Power Energy Syst 2019;110:598–612. https://doi.org/10.1016/j.ijepes.2019.03.021.

[8] Touchton RA, Dale Gunter A, Subramanyan N. Automated reasoning with dynamic event trees: a real-time, knowledge-based decision aide. Reliab Eng Syst Saf 1988;22:333–53. https://doi.org/10.1016/0951-8320(88)90082-8.

[9] Kang DG, Ahn SH, Chang SH. A combined deterministic and probabilistic procedure for safety assessment of beyond design basis accidents in nuclear power plant: application to ECCS performance assessment for design basis LOCA

redefinition. Nucl Eng Des 2013;260:165–74. https://doi.org/10.1016/j.nucengdes.2013.03.033.

[10] Park J, Seager TP, Rao PSC, Convertino M, Linkov I. Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Anal 2013;33:356–67. https://doi.org/10.1111/j.1539-6924.2012.01885.x.

[11] Wang J, Zuo W, Rhode-Barbarigos L, Lu X, Wang J, Lin Y. Literature review on modeling and simulation of energy infrastructures from a resilience perspective. Reliab Eng Syst Saf 2019;183:360–73. https://doi.org/10.1016/j.ress.2018.11.029.

[12] Rehak D, Senovsky P, Slivkova S. Resilience of critical infrastructure elements and its main factors. Systems 2018;6:21. https://doi.org/10.3390/systems6020021.

[13] Fang YP, Pedroni N, Zio E. Resilience-based component importance measures for critical infrastructure network systems. IEEE Trans Reliab 2016;65:502–12. https://doi.org/10.1109/TR.2016.2521761.

[14] Folke C. Resilience: the emergence of a perspective for social–ecological systems analyses. Glob Environ Change 2006;16:253–67. https://doi.org/10.1016/j.gloenvcha.2006.04.002.

[15] Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliab Eng Syst Saf 2016;145:47–61. https://doi.org/10.1016/j.ress.2015.08.006.

[16] Ferrario E, Zio E. Goal tree success tree-dynamic master logic diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems. Eng Struct 2014;59:411–33. https://doi.org/10.1016/j.engstruct.2013.11.001.

[17] Labaka L, Hernantes J, Sarriegi JM. Resilience framework for critical infrastructures: an empirical study in a nuclear plant. Reliab Eng Syst Saf 2015;141:92–105. https://doi.org/10.1016/j.ress.2015.03.009.

[18] Nelson PF, Martin-Del-Campo C, Hallbert B, Mosleh A. Development of a leading performance indicator from operational experience and resilience in a nuclear power plant. Nucl Eng Technol 2016;48:114–28. https://doi.org/10.1016/j.net.2015.10.010.

[19] Zeng Z, Fang YP, Zhai Q, Du S. A Markov reward process-based framework for resilience analysis of multistate energy systems under the threat of extreme events. Reliab Eng Syst Saf 2021;209:107443. https://doi.org/10.1016/j.ress.2021.107443.

[20] Yan R, Dunnett S. Resilience assessment for nuclear power plants using Petri nets. Ann Nucl Energy 2022;176:109282. https://doi.org/10.1016/j.anucene.2022.109282.

[21] Martinez-Guridi G, Samanta P, Chu TL, Yang JW. LOCA with consequential or delayed LOOP: modeling of accident sequences and associated core damage frequency. Nucl Technol 2000;131:297–318. https://doi.org/10.13182/NT00-A3118.

[22] Chen Chun-Yu, Shih Chunkuan, Wang Jong-Rong. The alternate mitigation strategies on the extreme event of the LOCA and the SBO with the TRACE Chinshan BWR4 model. Nuclear Engineering and Design 2013;256:332–40. https://doi.org/10.1016/j.nucengdes.2012.08.029.

[23] Sun J, Yang C. Low-power and shut-down condition medium-break loss-of-coolant accident success criterion analysis for a typical three-loop nuclear power plant. J Nucl Eng Radiat Sci 2016;2:041009. https://doi.org/10.1115/1.4033669.

[24] Yang JE, Hwang MJ, Sung TY, Jin Y. Application of genetic algorithm for reliability allocation in nuclear power plants. Reliab Eng Syst Saf 1999;65:229–38. https://doi.org/10.1016/S0951-8320(98)00103-3.

[25] Di Maio F, Picoco C, Zio E, Rychkov V. Safety margin sensitivity analysis for model selection in nuclear power plant probabilistic safety assessment. Reliab Eng Syst Saf 2017;162:122–38. https://doi.org/10.1016/j.ress.2017.01.020.

[26] Latsou C, Dunnett SJ, Jackson LM. A new methodology for automated petri net generation: method application. Reliab Eng Syst Saf 2019;185:113–23. https://doi.org/10.1016/j.ress.2018.12.017.

[27] Yu H, Wu X, Wu X. An extended object-oriented petri net model for mission reliability evaluation of phased-mission system with time redundancy. Reliab Eng Syst Saf 2020;197:106786. https://doi.org/10.1016/j.ress.2019.106786.

[28] Yan R, Jackson LM, Dunnett SJ. Automated guided vehicle mission reliability modelling using a combined fault tree and Petri net approach. Int J Adv Manuf Technol 2017;92:1825–37. https://doi.org/10.1007/s00170-017-0175-7.

[29] Yan R, Jackson L, Dunnett S. A study for further exploring the advantages of using multi-load automated guided vehicles. J Manuf Syst 2020;57:19–30. https://doi.org/10.1016/j.jmsy.2020.08.005.

[30] Zhou J, Reniers G. Probabilistic Petri-net addition enabling decision making depending on situational change: the case of emergency response to fuel tank farm fire. Reliab Eng Syst Saf 2020;200:106880. https://doi.org/10.1016/j.ress.2020.106880.

[31] Liu C, Zeng Q, Duan H, Wang L, Tan J, Ren C, et al. petri net based data-flow error detection and correction strategy for business processes. IEEE Access 2020;8:43265–76. https://doi.org/10.1109/ACCESS.2020.2976124.

[32] Jufri FH, Widiputra V, Jung J. State-of-the-art review on power grid resilience to extreme weather events: definitions, frameworks, quantitative assessment methodologies, and enhancement strategies. Appl Energy 2019;239:1049–65. https://doi.org/10.1016/j.apenergy.2019.02.017.

[33] Norris FH, Stevens SP, Pfefferbaum B, Wyche KF, Pfefferbaum RL. Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. Am J Community Psychol 2008;41:127–50. https://doi.org/10.1007/s10464-007-9156-6.

[34] Bhamra R, Dani S, Burnard K. Resilience: the concept, a literature review and future directions. Int J Prod Res 2011;49:5375–93. https://doi.org/10.1080/00207543.2011.563826.

[35] Haimes YY. On the definition of resilience in systems. Risk Anal 2009;29:498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x.

[36] Pan X, Dang Y, Wang H, Hong D, Li Y, Deng H. Resilience model and recovery strategy of transportation network based on travel OD-grid analysis. Reliab Eng Syst Saf 2022;223:108483. https://doi.org/10.1016/j.ress.2022.108483.

[37] Han L, Zhao X, Chen Z, Gong H, Hou B. Assessing resilience of urban lifeline networks to intentional attacks. Reliab Eng Syst Saf 2021;207:107346. https://doi.org/10.1016/j.ress.2020.107346.

[38] Iannacone L, Sharma N, Tabandeh A, Gardoni P. Modeling time-varying reliability and resilience of deteriorating infrastructure. Reliab Eng Syst Saf 2022;217:108074. https://doi.org/10.1016/j.ress.2021.108074.

[39] Amirioun MH, Aminifar F, Lesani H, Shahidehpour M. Metrics and quantitative framework for assessing microgrid resilience against windstorms. Int J Electr Power Energy Syst 2019;104:716–23. https://doi.org/10.1016/j.ijepes.2018.07.025.

[40] Yodo N, Wang P. Engineering resilience quantification and system design implications: a literature survey. J Mech Des 2016;138. https://doi.org/10.1115/1.4034223.

[41] Zhao S, Liu X, Zhuo Y. Hybrid hidden markov models for resilience metrics in a dynamic infrastructure system. Reliab Eng Syst Saf 2017;164:84–97. https://doi.org/10.1016/j.ress.2017.02.009.

[42] Greene SR. Are current U.S. Nuclear power plants grid resilience assets? Nucl Technol 2018;202:1–14. https://doi.org/10.1080/00295450.2018.1432966.

[43] Yan R, Dunnett S, Tolo S, Andrews J. A petri net methodology for modeling the resilience of nuclear power plants. In: Proceedings of the 31th European safety and reliability conference (ESREL 2021). Research Publishing Services; 2021. p. 2426–32. https://doi.org/10.3850/978-981-18-2016-8_109-cd.

[44] Lundberg J, Johansson BJE. Resilience is not a silver bullet – Harnessing resilience as core values and resource contexts in a double adaptive process. Reliab Eng Syst Saf 2019;188:110–7. https://doi.org/10.1016/j.ress.2019.03.003.

[45] CANDU 6 Program Team, CANDU 6 technical summary. 2005. Atomic Energy of Canada Ltd. https://canteach.candu.org/content%20library/candu6_technicalsummary-s.pdf. [Accessed 10 March 2022].

[46] Cho S, Jiang J. Analysis of surveillance test interval by Markov process for SDS1 in CANDU nuclear power plants. Reliab Eng Syst Saf 2008;93:1–13. https://doi.org/10.1016/j.ress.2006.10.007.

[47] NEA. Nuclear Fuel Behaviour in Loss-of-coolant Accident (LOCA) Conditions. NEA; 2009.

[48] Schmid S, Silber FE, Heckmann K, Kulenovic R, Laurien E, Sievers J, et al. Leak rate testing in the range of leak detection systems. Nucl Eng Des 2021;372:111000. https://doi.org/10.1016/j.nucengdes.2020.111000.

[49] Price EG, Moan GD, Coleman CE. Leak before break experience in CANDU reactors (AECL–9609). Canada; 1988. https://inis.iaea.org/collection/NCLCollectionStore/_Public/22/069/22069578.pdf. [Accessed 10 March 2022].

[50] Hollnagel E, Fujita Y. The fukushima disaster – systemic failures as the lack of resilience. Nucl Eng Technol 2013;45:13–20. https://doi.org/10.5516/NET.03.2011.078.

[51] Park SY, Ahn KI. Evaluation of an accident management strategy of emergency water injection using fire engines in a typical pressurized water reactor. Nucl Eng Technol 2015;47:719–28. https://doi.org/10.1016/j.net.2015.06.010.

[52] Sadou N, Demmou H. Reliability analysis of discrete event dynamic systems with Petri nets. Reliab Eng Syst Saf 2009;94:1848–61. https://doi.org/10.1016/j.ress.2009.06.006.

[53] Cho CS, Chung WH, Kuo SY. Cyberphysical security and dependability analysis of digital control systems in nuclear power plants. IEEE Trans Syst Man, Cybern Syst 2016;46:356–69. https://doi.org/10.1109/TSMC.2015.2452897.

[54] Gonçalves P, Sobral J, Ferreira LA. Unmanned aerial vehicle safety assessment modelling through petri Nets. Reliab Eng Syst Saf 2017;167:383–93. https://doi.org/10.1016/j.ress.2017.06.021.

[55] Wootton MJ, Andrews JD, Lloyd AL, Smith R, Arul AJ, Vinod G, et al. Risk modelling of ageing nuclear reactor systems. Ann Nucl Energy 2022;166:108701. https://doi.org/10.1016/j.anucene.2021.108701.

[56] Birkhofer A. The German risk study for nuclear power plants. IAEA Bulletin 1980;22:23–33. https://www.iaea.org/sites/default/files/225_604792333.pdf. [Accessed 10 March 2022].

[57] Andrews JD, Moss B. Reliability and risk assessment. 2nd Ed. London: Professional Engineering Publishing Ltd; 2002.

[58] IAEA. Electric grid reliability and interface with nuclear power plants, iaea nuclear energy series No. NG-T-3.8. Vienna: IAEA; 2012.

[59] IAEA. Component reliability data for use in probabilistic safety assessment, IAEA-TECDOC-478. VIENNA: IAEA; 1988.

[60] Dulik JD. Use of performance-monitoring to improve reliability of emergency diesel generators. Massachusetts Institute of Technology; 1998. February.

[61] McCurry J. Japan disaster: reconstruction effort puts town on road to recovery | Japan | The Guardian. Guardian; 2011. https://www.theguardian.com/world/2011/mar/24/japan-disaster-reconstruction-road-recovery. [Accessed 14 March 2022].

[62] Martinez-Guridi G, Lehner J. Generic probability of a loop after a large Loca : an evaluation. https://www.nrc.gov/docs/ML0714/ML071430462.pdf. [Accessed 14 March 2022].

[63] Garland WJ. The essential CANDU, a textbook on the CANDU nuclear power plant technology. University Network of Excellence in Nuclear Engineering; 2014. ISBN 0-9730040. Retrieved from, https://www.unene.ca/education/candu-textbook. on 01/2022.

[64] Gauntt RO, Kalinich DA, Cardoni JN, Phillips J, Goldmann AS, Pickering SY, et al. Fukushima Daiichi accident study: status as of April 2012. Sandia National Laboratories 2012. https://doi.org/10.2172/1055601.

[65] Zhou F, Novog DR. Mechanistic modelling of station blackout accidents for a generic 900 MW CANDU plant using the modified RELAP/SCDAPSIM/MOD3.6 code. Nucl Eng Des 2018;335:71–93. https://doi.org/10.1016/j.nucengdes.2018.05.009.

[66] Canadian Nuclear Safety Commission. Fundamentals of Power Reactors Training Course. 1996. https://canteach.candu.org/content%20library/19930204.pdf [Accessed August 30, 2020].

[67] Atomic Energy of Canada Ltd. Protocol for the Restart of the NRU Reactor. 2010. https://nuclearsafety.gc.ca/eng/pdfs/NRU_Restart_Protocol_jan_2010_EN.pdf. [Accessed 30 March 2021].

[68] Carter LJ. Nuclear imperatives and public trust: dealing with radioactive waste. Issues Sci Technol 1987;3:46–61.

[69] United States Nuclear Regulatory Commission. Backgrounder on the three mile island accident. U S Nucl Regul Comm Libr 2018.

[70] Lipscy PY, Kushida KE, Incerti T. The fukushima disaster and japan's nuclear plant vulnerability in comparative perspective. Environ Sci Technol 2013;47:6082–8. https://doi.org/10.1021/es4004813.

[71] Kim JH, Jin DS, Chang SH. Development of safety analysis methodology for moderator system failure of CANDU-6 reactor by thermal-hydraulics/physics coupling. Nucl Eng Des 2013;263:241–54. https://doi.org/10.1016/j.nucengdes.2013.04.012.