13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13)
2~7 October, 2016 • Sheraton Grande Walkerhill • Seoul, Korea • www.psam13.org

A FRAMEWORK FOR POWER RECOVERY PROBABILITY QUANTIFICATION IN NUCLEAR POWER PLANT STATION BLACKOUT SEQUENCES

Hindolo George-Williams[1,2], Min Lee[2], Edoardo Patelli[1]

[1] Institute for Risk and Uncertainty: Chadwick Building, University of Liverpool, Peach Street, Liverpool L69 7ZF, United Kingdom, H.George-Williams@liverpool.ac.uk (Hindolo), edoardo.patelli@liverpool.ac.uk (Edoardo)
[2] Institute of Nuclear Engineering and Science, National Tsing Hua University: No. 101, Section 2, Guangfu Rd, East District, Hsinchu City, 300, Taiwan, mlee@ess.nthu.edu.tw

The safety of Generations II and III nuclear power plants relies on the availability of AC power, which is required for decay heat removal. This AC power (designated offsite power) is provided by sources outside the power plant via a grid that is susceptible to both random and induced failures. When offsite power is lost, alternative emergency sources on-site are started to drive the plant's safety systems. If, however, a situation arises where these sources are also unavailable or unable to provide the required power for the entire period the offsite sources are unavailable, a complete loss of power to the safety buses ensues. This phenomenon is known as Station Blackout (SBO), and its severity depends on its duration as well as, the plant's initial status. Consequently, the time-dependent non-recovery probability of AC power is a key parameter in the risk assessment and management of nuclear power plants. In this work, an easy-to-use and generally applicable reliability framework is proposed to model power recovery in station blackout sequences. It employs a load flow technique integrated into an efficient event-driven Monte-Carlo simulation algorithm. The resulting framework quantifies the probability of power recovery as a function of both time and power level, including other relevant indices. It, therefore, serves the purpose of a rational decision support tool in the mitigation of station blackout accidents. The proposed framework is used to analyze station blackouts emanating from grid and switchyard failures at the Maanshan nuclear power plant in Taiwan.

I. INTRODUCTION

Nuclear power is the product of a highly efficient and controlled fission chain reactions in the core of a reactor vessel. These reactions are often accompanied by a large release of heat, which is harnessed to generate steam and subsequently, electricity. The reactor vessel, with its multiple protective barriers, is placed in a concrete containment to shield the environment from the potential release of radioactive materials produced by the reactions. When the reactor core temperature exceeds a certain threshold or the water level in the core drops below some level, due to a severe accident, the core is said to be damaged. In this state, the likelihood of the containment being breached and the risk of radioactive material release into the environment increase. The goal, therefore, of a nuclear power plant's risk management scheme is its core damage and subsequent containment breach mitigation. Severe accident mitigation is achieved in part by ensuring a reliable cooling water circulation and subsequent excess heat removal from the reactor vessel.[1] Core cooling, during normal/critical plant operation, is carried out through heat exchange between the primary and secondary loops of the plant's main cooling system. However, when the plant is shut down or forced to shut down, normal core cooling ceases and the backup cooling systems are called into action to sustain decay heat removal. Forced shutdown, of nuclear power plants, is induced by initiating events, such as general transients, loss of coolant accidents, earthquakes, loss of ultimate heat sink, and loss of offsite power (LOOP). Like the main cooling system, the backup cooling systems rely on AC power from the safety buses, albeit some are equipped with alternative turbine or diesel-driven pumps to be used during SBO sequences. In spite of their AC power independence, these systems rely for monitoring and control, on DC power from DC power banks. Their sustainability, therefore, regardless of their inherent reliability is limited by the DC battery depletion time. The DC battery depletion time with the boil-off rate of reactor coolant after the failure of the steam-driven backup cooling systems, defines the maximum AC power recovery duration required to prevent core damage.[2]

These considerations exemplify the significance of AC power to the attainment and maintenance of safe shutdown conditions in a nuclear power plant. It's therefore not surprising that SBO accidents contribute largely to the overall risk posed by nuclear power plants, accounting for over 70% of the core damage frequency at some plants.[2,3] Owing to this, the US Nuclear Regulatory Commission (USNRC), in 1988 defined the regulatory guide, RG 1.155 (Ref. 4) for commercial nuclear power plants in the US. The guide stipulates, amongst others that nuclear power plants should be capable of coping with SBO accidents, sustaining adequate core cooling for a specified duration. This duration varies from 2 to 16 hours, depending on the offsite power design, the emergency AC power characteristic group, and the unit average reliability of the Emergency Diesel Generators (EDG).

The contribution of SBO accidents to the overall risk of a plant is determined by the LOOP frequency, offsite power recovery probability, the reliability and availability of on-site Emergency Power Sources (EPS), the reliability and availability of AC independent core cooling systems and the DC power depletion time. LOOP events are classified into four major categories; grid-centered, switchyard-centered, plant-centered and weather related, on the basis of where the power failure originates. Grid-centered LOOP events are due to failure of the transmission network outside the plant, switchyard-centered LOOP arises from failures in the switchyard on the plant premises, plant-centered LOOP is triggered by the operational dynamics of the plant itself while weather-related LOOP events are attributed to failures induced by severe and extreme weather, excluding lightning.[2,3] The effective SBO risk is quantified as the sum of the individual SBO frequencies from each LOOP category.

I.A. Problem Definition

Given their potential consequences on the safe operation of nuclear power plants, LOOP and SBO analyses occupy a central position in nuclear power plant Probabilistic Risk Assessment (PRA). Quantifying how much they affect the core damage frequency, current PRA techniques employ the traditional event and fault tree analyses. The quantification process starts with LOOP event tree analysis, where the EPS availability is queried in the first top event. This event failure, which frequency defines the SBO frequency transfers the analysis to the SBO event tree. In the SBO event tree, the successes of the various mitigating actions and coping mechanisms, including offsite power and EDG recovery at specific times are queried in event tree headings. The time queried for AC power recovery is 7 hours after LOOP,[2] in the Standardized Plant Analysis Risk (SPAR) model, for Westinghouse PWRs but may vary from plant to plant. Every top event in the SBO event tree requires a separate fault tree to model and quantify its unavailability. Fault tree analysis, however, suffers the setback of becoming explosive with large systems or moderate systems with complex interactions. Even with the emergence of dynamic fault trees, they are still limited in the nature and degree of complex interactions they can accurately model. Given the time-dependent non-recovery probability curve, the need for AC power recovery fault trees would have been eliminated. This curve defines the unavailability of AC power and can therefore serve as a benchmark for assessing the reliabilities of the SBO coping systems.

I.B. Proposed Approach and Scope

Monte Carlo Simulation (MCS) possesses the required flexibility to model any system attribute and provides an easy means of obtaining the relevant system performance indices. The current authors,[5] recently published an intuitive event-driven MCS and a multi-state component model for reliability analysis of complex systems. The technique defines the system structure by a graph model and uses a linear programming algorithm to determine system performance for a given combination of component states. This simplifies the MCS considerably, as the need to define system path sets, cut sets, structure function or other complicated system state identification logics is eliminated. In this work, the graph and multi-state models proposed in (Ref. 5) are adopted for system performance evaluation and component attribute definition respectively. The multi-state model is particularly useful to the multiple failure mode representation of the EPS and their other dynamic attributes. This model, for example, could be exploited to investigate the effects of limited maintenance teams and unavailability of spares on EPS repair.[6] The original component model is modified to account for interdependencies, which are commonplace in nuclear power systems. A simple MCS algorithm is developed to manually induce LOOP in the system, reconstruct the sequence of events post LOOP (EPS actuation, failure, and repair) and monitor the availability of power at the various safety buses. Only grid and switchyard centered LOOPs are considered in this paper, given their dominance of the total LOOP frequency studied in Volume 1 of the NUREG/CR-6890 report.[3] The modelling techniques proposed are applicable to both critical and shutdown plant operations; in fact, they are completely independent of the operational state of the plant.

The next section presents the general SBO modelling techniques and the MCS algorithm. A case study, detailing the application of the modelling principles developed to a realistic system is described in Section III. The corresponding outcome is also presented and its risk insights discussed. Section IV concludes the work and discusses the potential for its future development.

II. STATION BLACKOUT MODELLING

A nuclear power plant's power distribution system consists of the grid, the switchyard (s), the EPS, alternative EPS (AEPS) and the safety buses. The AEPS are additional emergency sources (such as Gas Turbine Generators) available at some plants to boost their LOOP/SBO recovery capability. Though on-site, they are connected to the switchyard, considered part of offsite power recovery and are normally not modelled in the EPS fault tree of some PRA models.[2] The system structure is defined by a graph in which each node depicts an element/component and all nodes are connected by perfectly reliable directed links portraying the direction of power flow. Flows from all the safety buses are terminated on a virtual node, introduced to represent the total available power. The graph is mathematically represented by an adjacency matrix, $\boldsymbol{A}$, such that $\boldsymbol{A} = \{a_{ij}\}^{m\times m}$ and $(i,j) \in (1,2,\dots,m)$, where *m* is the total number of nodes. The adjacency matrix is such that, $a_{ij} = 1$ if there's flow from node *i* to node *j* and 0, otherwise. A relationship exists between the system flow equations and $\boldsymbol{A}$, which relationship is used to derive the former.

The multi-state node model used for system elements takes into account their various properties. However, for the purpose of this work, their initial state, capacity vector, and transition matrix are the only required parameters. A node's capacity vector specifies its capacity in each state and its transition matrix defines its possible state transitions with their corresponding probability distributions. Each node capacity is a non-dimensional number defining the proportion of total system output the node can supply, transmit or sink. The total system output is expressed as the fraction of available independent power trains/safety buses. Therefore, if n is the total number of power trains, n_1, the number of power trains the node can simultaneously supply, k, the proportion of power train demand it can satisfy, then, its capacity is given by, kn_1/n. Given this, the grid and switchyard nodes have unity capacity when available and the virtual node representing the global system output; a fixed capacity of unity. Readers are referred to (Ref. 5) for details on system flow calculation and the procedure for determining the next transition time and state of multi-state node models during MCS.

II.A. The LOOP Initiator and Emergency Power Systems Models

For the purpose of this work, the grid and switchyard are the only LOOP initiators, the EPS consist of Emergency Diesel Generators (EDG) and the AEPS are constituted by Gas Turbine Generators (GTG). The following assumptions are invoked in their modelling;

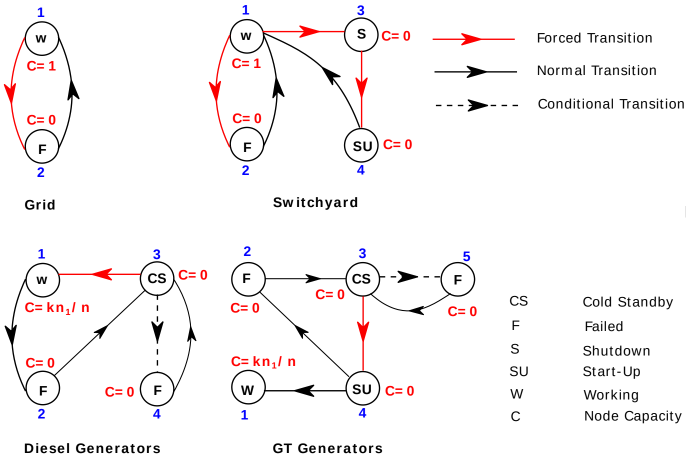
1. The EPS and AEPS are not susceptible to common-cause failures and their unavailability due to test and maintenance is negligible.
2. The AEPS are considered part of offsite power recovery, their failure is included in the grid-centered LOOP frequency.
3. There are sufficient repair teams; node restoration, following failure, therefore, commences immediately.
4. The safety buses are perfectly reliable and have a fixed capacity of $1/n$.

The grid is modelled as a 2-state node; '*Working*', when available and '*Failed*', otherwise. Though grid failures are mostly random, they are modelled as forced transitions[5] since they already are incorporated in the LOOP frequency. Moreover, the objective here is to force a LOOP and evaluate the response of the EPS and AEPS (where applicable). Most often, plants tap their AC power from multiple offsite sources; grid failure is defined as the failure of all these sources. Repair of at least one of the failed sources, on the other hand, is sufficient to achieve grid recovery. For this reason, the transition from 'Failed' to 'Working', of the grid node in the model is defined by the upper bound of the envelope around the cumulative density functions (*cdf*) of the individual source repair distributions. Sampling the next grid recovery time requires generating a uniform random number and reading off its corresponding time from the envelope *cdf*; interpolating where necessary. An important point worthwhile noting is, this approach slightly underestimates the grid recovery probability, as it assumes the individual source repair actions are initiated concurrently. In reality, the sources do not necessarily fail simultaneously and their recovery actions may commence at different times. This implies, by the time the last source node fails (LOOP initiation), the restoration of already failed sources would have been well underway. The actual grid recovery time, therefore, will be less than or equal to that given by the envelope *cdf*. This, however, is acceptable since the goal in risk management is to ensure risk levels are kept within an acceptable range, even in worst case scenarios.

Like the grid, normal switchyard operation could be represented by a 2-state node. However, during grid failures, the switchyard is forced into a temporary shutdown state of zero capacity. On grid recovery, the plant personnel manually initiate the switching process to restore the switchyard, which may be prone to human errors and may require some time. Accounting for these, two additional states; '*Shutdown*' and '*Start-Up*' are introduced in the 2-state node model. The transitions from 'Working' to 'Shutdown' and from 'Shutdown' to 'Start-Up' are respectively determined by grid failure and recovery and are therefore modelled as forced transitions. 'Start-Up' represents the difference between the potential and actual bus recovery times. If this difference is negligible or the potential instead of the actual bus recovery time is required in the analysis, then, the 'Start-Up' state is discarded and a forced transition from 'Shutdown' to 'Working' inserted. Also, in cases where the plant is enhanced with multiple switchyards, switchyard recovery is treated like in the case of multiple grid sources.

Prior to LOOP, the EPS and AEPS are in cold standby. The EPS are normally automatically restarted and aligned on the incidence of LOOP whilst the AEPS require human intervention for start-up and manual alignment. Two EDG failure modes are considered; *failure-to-start* and *failure-to-run*, defining the EDG failure to start and run for the LOOP duration respectively. The SPAR model considers a third EDG failure mode; *failure-to-load,* defining the case when the EDG starts but cannot power the load. This type of failure is categorized as *failure-to-start* in the current model. For EDGs, the transition from cold standby to working is assumed instantaneous since their start-up is automatic whilst the transition from cold standby to 'Failed' is determined by their failure-to-start probability. The latter transition is a special type of forced transition, designated conditional transition by virtue of its lower preference and dependence on an internal event of the node as well as the failure of another node. Like forced transitions, conditional transitions are indicated by ∞ in the relevant position in the node's transition matrix.[9]

The GTGs are modelled in almost the same way as the EDGs, save for two notable variations. Successful start-up of the former is regarded offsite power recovery and the MCS is terminated; their 'Working' state, therefore, is an absorbing state. The second variation stems from their start-up and manual alignment time, which is not negligible for most plants.



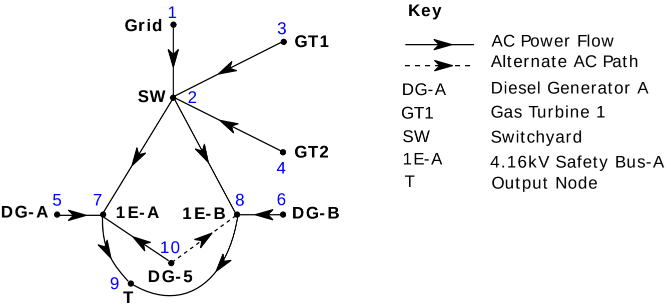


Fig.2. Maanshan nuclear power plant EPS and AEPS layout

Fig.1. Multi-state node models of system elements

Fig. 1 shows the multi-state node models of the key elements of a nuclear power plant's AC power system relevant to SBO.

II.B. Node Interdependencies

Interdependencies exist among the various system elements. The EPS, for instance, are triggered into life by grid and switchyard failures and the AEPS, by EPS failure. These relationships, for some power configurations, may be complex; an intuitive approach is therefore required to keep the MCS algorithm simple. To achieve this, an additional parameter; the *dependency matrix*, **D**, is introduced to define the effects of a node's state transition on the states of other nodes. Let *i* be the ID of the node, its dependency matrix is given by $\mathbf{D}_i = \{d_{j1}, d_{j2}, d_{j3}, d_{j4}\} |\, j = 1,2, \dots, u-1, u$. Where, d_{j1} is the state of i triggering the event, d_{j2}; the affected node, d_{j3}; the state the node has to be in to be affected, d_{j4}; its target state on occurrence of the event and u, the number of relationships. Sometimes, the dependency exhibited by a node also depends on the state of another node and it's referred to as, a joint dependency. These joint dependencies are defined by the joint dependency matrix, $\mathbf{D}'_\alpha$, where, α is the node in joint dependency with node i and β, the state it has to be in to satisfy the joint dependency. The relationship between nodes i and α is included as a dependency in $\mathbf{D}_i$, where, $d_{j2} = \alpha$ and $d_{j3} = d_{j4} = \beta$ since node α doesn't have to undergo a state change as a consequence of the relationship. Matrices $\mathbf{D}_i$ and $\mathbf{D}'_\alpha$ have the same format; the actual state transition triggered by the joint dependency is indicated by a row of the latter. If j is the row index, then, $d_{j1} = \beta$ whilst d_{j2}, d_{j3} and d_{j4} have the same meaning, as defined earlier. A recursive algorithm is proposed to implement these dependencies. If x_i is the new state of node i following a transition, then, the recursive algorithm (designated *Algorithm 1*) is summarized thus;

1. Define a register to hold affected nodes and their target states.
2. Find all nodes affected by the state change (using $\mathbf{D}_i$ and x_i) and update the register defined in step 1.
3. Select the last entry; node α of the register, check the equality of its current and target states.
4. If the equality checked in step 3 is confirmed, delete the records of α from the register and repeat steps 2 and 3, using $\mathbf{D}'_\alpha$ and x_α. Proceed, otherwise.
5. Force the designated transition, as determined in step 3 and delete all the records of α from the register. If the affected node is in cold standby, and its target state; *Working* or *Start-Up*, use the restart procedure for cold standby nodes.
6. Using $\mathbf{D}_\alpha$ and x_α obtained in step 3, repeat steps 2 and 3.
7. Repeat steps 2 through 6 until the register is empty.

In Algorithm 1**, μ,** the vector of current node capacities is updated on every node transition. The following steps, designated Algorithm 2, define the procedure for restarting a node from cold standby.

1. Generate a uniform random number between 0 and 1 and check whether it exceeds the node's failure-to-start probability. Set the latter's current state to *Working* or *Start-Up*, if it does and go to step 3. Otherwise, proceed.
2. Set the node's current state to the appropriate failure mode and apply Algorithm 1, where necessary.
3. Update **μ** and sample the node's next transition parameters using the procedure proposed in (Ref. 5).

II.C. The Monte Carlo Simulation (MCS) Algorithm

The MCS algorithm induces a LOOP event and reconstructs the response of the EPS and AEPS. System response is imitated by generating random failure events of components and their corresponding repair times. For every component transition, the flow through the output node is computed and stored as a function of time. These stored values provide a means of estimating the conditional SBO probability given a LOOP, the conditional recovery probability given an SBO and the proportion of SBOs occurring immediately after a LOOP.

Initially (at time $t = 0$), the grid and switchyard nodes are working while the EPS and AEPS are in cold standby. LOOP is initiated by setting the appropriate LOOP initiator to its failure state and applying Algorithm 1. Node transition times are sampled and the simulation moves to the earliest transition time, t. Nodes with transition time equal to t are identified, the required transitions effected, their next transition times sampled, the new system performance computed and the next simulation time determined. This continues until offsite power is recovered, indicated by the successful return of the switchyard to working state. If multiple LOOPs are investigated, each LOOP is analyzed separately, with the other LOOP initiators frozen in working state (with the exception of shut down and start-up of the switchyard during grid centered LOOP).

Let μ_{old} contain the node capacities at the previous system transition, τ, the vector of next node transition times, N, the number of LOOPs initiated and S, the total number of SBO events. The MCS algorithm is summarized thus;

1. Initialize the register to store flow through the output node, set $N = S = 0$ and define the MCS stopping condition. The stopping condition could be the number of LOOPs, number of SBOs or convergence of SBO probability.
2. Define μ using the current states of system nodes. Set $t = 0, \mu_{old} = \mu, \tau = \{\infty\}^m$ and $X_{out} = 1$, where X_{out} is the total system output and m, the number of nodes. Save X_{out} as a function of time and proceed.
3. Force LOOP, apply Algorithm 1, determine the flow, X_{out}, through the output node and shut down the switchyard.
4. Save X_{out} if $X_{out} < 1$, set $S = S + 1$ if $X_{out} = 0$ and set $t = \min(\tau)$.
5. Find nodes with next transition time equal to t. For each node, force the required transition, sample its next transition parameters (except for nodes returning to cold standby), update μ, τ and apply Algorithm 1, where necessary.
6. Restart nodes returning from cold standby (i.e., apply Algorithm 2) if X_{out}, as previously determined is less than 1.
7. If $\mu_{old} \neq \mu$, determine X_{out} and save as a function of time. Temporarily set the capacity of the switchyard node to 1 if it is in shutdown and calculate the new system flow.[5] If the flow through the switchyard is non-zero, set its current state to *start-up,* sample its next transition parameters and update τ.
8. Set $\mu_{old} = \mu$, $t = \min(\tau)$, $S = S + 1$ if $X_{out} = 0$ and check whether the switchyard is working.
9. Repeat steps 5 to 8 until the switchyard is working. Discard output history N if there is no SBO and set $N = N + 1$.
10. Repeat steps 2 to 9 until the MCS stopping criteria is met and terminate the algorithm.

The conditional probability of SBO, given LOOP and the SBO frequency, f_s, are obtained from S/N and $f_l S/N$ respectively; where f_l is the LOOP frequency. The non-recovery probability, $r(t)$, with respect to a given performance is computed, as the average contribution of the recovery durations to a collection of time-steps, spaced equally over 24 hours. Given an instance of performance history, the time between the occurrence of a 0 and the next occurrence of the desired output or better is obtained and the number of time-steps, t_s, it represents determined. The values stored in the first t_s time-steps are incremented by 1 and the entire procedure replicated for the other performance history instances. $r(t)$ is computed by dividing the final value in each time-step by the total number of recovery times used. It defines the likelihood of recovery duration from an SBO accident exceeding a given time. The corresponding frequency of exceedance, as a function of time, is given by, $f_s r(t)$.

III. CASE STUDY: THE MAANSHAN NUCLEAR POWER PLANT

Maanshan is a twin-unit, 1902 MW, Westinghouse PWR nuclear power plant operated by the Taiwan Power Company. Its offsite power is supplied by six independent sources, four of which are connected to the 345 kV switchyard and the remainder, through the 161 kV switchyard. There are two safety buses, each with a dedicated EDG. A shared EDG, DG-5, is available as a backup in case any of the dedicated EDGs is unavailable. Though this third EDG is connected to both buses, it can only serve one at a time. The dedicated EDGs are automatically started and aligned on LOOP whilst the shared EDG requires human intervention. Its start-up and alignment time, however, is in the range of 2-5 minutes and therefore assumed negligible. Each

EDG is enough to meet the demand on one power train and all three EDGs exhibit the same failure and repair characteristics. The plant is equipped with two gas turbine generators (as part of the AEPS) that also require manual start-up when at least 2 out of the 3 EDGs are unavailable. The GTGs have a mean start-up time of 30 minutes (assumed exponentially distributed) and each is sufficient to meet the demand on both power trains. Applying the procedure outlined in Section II, the buses are assigned a fixed capacity of 0.5, the EDGs and GTGs; a capacity of 0.5 and 1 respectively.

Shown in Fig. 2 is a layout of the plant's AC power system, showing all the elements relevant to an SBO. DG-5, though serving only one bus at a time, is assumed connected to both buses in the system's adjacency matrix. This implies, its flow is divided between the buses, contrary to what obtains in reality. However, since the flows from the two buses are emptied into the output node, T, the total flow from the shared generator is accounted for. The probability of failure to start from cold standby is 0.1 for EDGs and 0.15 for GTGs. Each grid source repair time is lognormally distributed, the mean and corresponding standard deviation sets for the six sources are defined as $\{8.99,11.84,8.24,10.25,9.61,9.15\}$ and $\{6.71,4.83,4.05,6.61,1.92,5\}$ respectively. Similarly, switchyard repair times are lognormally distributed, with $\{8,10.41\}$ and $\{5.83,2.5\}$ respectively being the sets of means and corresponding standard deviations for the two switchyards. The relevant elements of the system are modelled according to Fig. 1 and their transition characteristics are summarized in TABLE I, where all failure, repair and other transition times are in hours. It should, however, be noted that the distribution types and parameters used are only for illustrative purposes and do not represent the actual data for Maanshan or any other nuclear power plant. They were carefully assumed with the view to closely reflecting the reliability data used in Volumes 1 and 2 of the NUREG/CR-6890 report.[2,3] Fig. 3 shows the repair time *cdfs* of the grid sources and their envelope, represented by the dashed lines. A similar figure is obtained for the switchyard and in both cases, the upper bound of the envelope is used as the effective repair *cdf*, as described in Section II.

TABLE I. Element state transition characteristics

Element	Transition	Distribution Type	Parameters
EDG	1-2	Weibull	(100,1.24)
	2-3	Lognormal	(6.42,2)
	4-3	Lognormal	(5,1.2)
GTG	4-1	Exponential	0.5
	4-2	Weibull	(200,1.5)
	2-3	Lognormal	(5,2)
	5-3	Lognormal	(7,1.8)

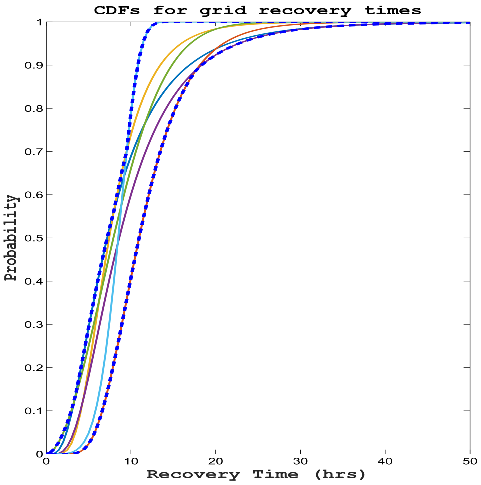


Fig.3. Bounds on grid repair cdf

Grid and switchyard failures trigger start-up of the dedicated EDGs (DG-A and DG-B), which must be in cold standby. When a dedicated EDG fails to start or run, DG-5 is started, which also must be in cold standby. If it fails to start, the start-up of the GTGs is initiated, thereby indicating their dependence on the former. Running failures of DG-5 require restart, from cold standby of the previously failed DG-A or DG-B, given its repair is completed. Otherwise, the GTG start-up procedure is initiated. This case of GTG start-up, only if the previously failed dedicated EDG is still not recovered, is an example of a joint dependency. Other instances of joint dependencies involving GTG start-up from cold standby are;

- DG-A or DG-B fails to start or run and DG-5 is already in operation.
- DG-A or DG-B fails to start or run and DG-5 is in state 2 (fail to run).

A graphical summary of the dependencies described is presented in Fig. 4, where the dependency of GT1 on DG-B and GT2 on DG-A have been omitted for clarity. Their corresponding dependency and joint dependency matrices are also given below.

III.A. Results and Discussions

The proposed approach has been implemented into the open source toolbox, OpenCOSSAN.[7] For a grid LOOP (G-C) frequency of 1.86E-2 per/year and a switchyard centered LOOP (SWYD-C) frequency of 1.04E-2 per/year, the case study was analyzed on a 2.5GHz, E5-2670 v2 Intel ® Xeon ® CPU, using 12 of its 20 cores.

$$\mathbf{D}_1 = \mathbf{D}_2 = \begin{bmatrix} 2 & 5 & 3 & 1 \\ 2 & 6 & 3 & 1 \end{bmatrix}$$

$$\mathbf{D}_5 = \mathbf{D}_6 = \begin{bmatrix} 2 & 10 & 3 & 1 \\ 2 & 10 & 1 & 1 \\ 2 & 10 & 2 & 2 \\ 4 & 10 & 3 & 3 \\ 4 & 10 & 1 & 1 \\ 4 & 10 & 2 & 2 \end{bmatrix} \qquad \mathbf{D}'_{10} = \begin{bmatrix} 1 & 4 & 3 & 4 \\ 1 & 3 & 3 & 4 \\ 2 & 4 & 3 & 4 \\ 2 & 3 & 3 & 4 \end{bmatrix}$$

$$\mathbf{D}_{10} = \begin{bmatrix} 2 & 5 & 3 & 1 \\ 2 & 6 & 3 & 1 \\ 4 & 3 & 3 & 4 \\ 4 & 4 & 3 & 4 \\ 2 & 5 & 2 & 2 \\ 2 & 5 & 4 & 4 \\ 2 & 6 & 2 & 2 \\ 2 & 6 & 4 & 4 \end{bmatrix} \qquad \mathbf{D}'_5 = \mathbf{D}'_6 = \begin{bmatrix} 2 & 4 & 3 & 4 \\ 4 & 3 & 3 & 4 \\ 4 & 4 & 3 & 4 \\ 2 & 3 & 3 & 4 \end{bmatrix}$$

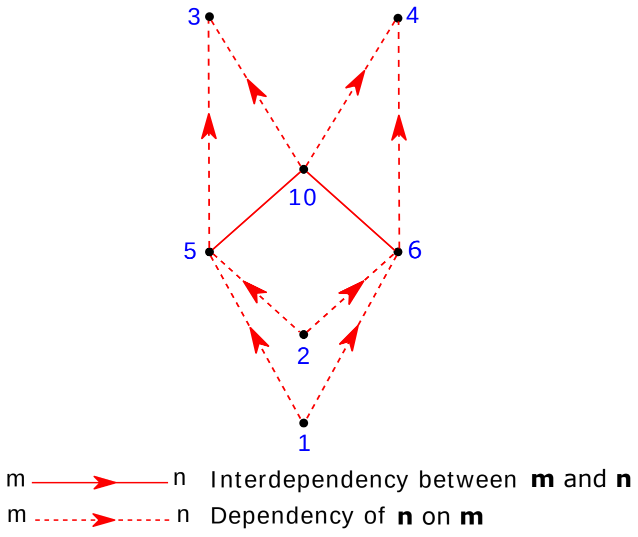


Fig.4. Element Interdependencies

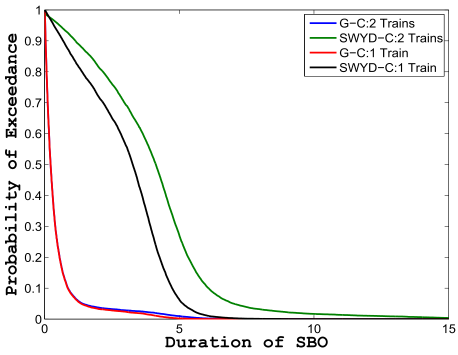


Fig.5. Probability of exceedance vs SBO duration

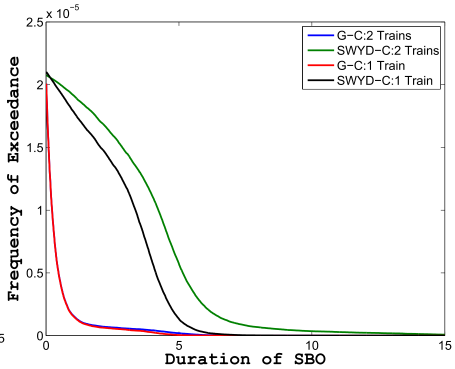


Fig.6. Frequency of exceedance vs SBO duration

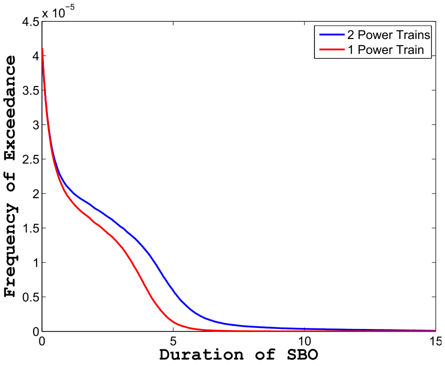


Fig.7. Composite frequency of exceedance vs SBO duration

TABLE II. Summary of static SBO indices obtained from MCS

LOOP Type	SBO Probability	SBO Frequency (per/year)	SBO Probability at Start-Up	MCS Samples Required
Grid	0.0011	2.01E-05	0.9245	2.72E+06
Switchyard	0.0020	2.10E-05	0.5033	8.54E+05

Imposing a 5% coefficient of variation on the SBO probability as the MCS stopping criteria, the entire analysis took 51.58 minutes; the outcome is as described by Figs. 5-7 and TABLE II. SWYD-C LOOP analysis required fewer simulation samples due to its higher probability of occurrence, as portrayed in TABLE II. As a way of checking the convergence of the MCS, the probability of all three EDGs failing at start-up is $(0.1)^3 = 10^{-3}$ and should equal the product of the SBO and SBO at start-up probabilities. From TABLE II, GC-LOOP yields 1.02E-3 whilst SWYD-C yields 1.01E-3, thereby confirming the MCS convergence. The non-recovery probability from an SBO, as shown in Fig. 5, has been expressed as the likelihood of at least a given number of safety buses being recovered within a specified period. Fig. 6 is a translation of this likelihood to the actual number of times the event is expected to happen whilst Fig. 7 expresses the overall SBO risk at the plant. The following risk insights are inferred by the MCS outcome;

1. SBO accidents are 82% more likely, given a switchyard centered LOOP (see TABLE II) and more difficult to recover from, as shown in Figs. 5 and 6. The reason for this is easily deduced from the layout of the plant's AC power system (see Fig. 2). Switchyard failures prevent the use of the GTGs as a standby power source completely as opposed to grid failures. Hence, switchyard centered LOOP contributes more to the overall risk of the plant.
2. The difference between the likelihoods of recovering at least one and two safety buses during grid-induced SBOs is negligible. The difference, however, for their switchyard counterpart is vast and could be explained by the same theory proffered in (1) above. This reiterates the significance of the GTGs in SBO recovery at the plant.
3. TABLE II also reveals SBO accidents are dominated by EDG start-up failures, especially during grid centered LOOP. This, however, is not surprising, given their relatively high start-up failure probability. Implying, EDG start-up failure reduction as one of the most promising SBO mitigation strategies at the plant.

IV. CONCLUSIONS

Station Black Out accidents, though a rare occurrence, can have devastating consequences on a nuclear power plant's ability to achieve and maintain safe shutdown. As a result, a plant's capability to cope and recover from them makes an indispensable input to its Probabilistic Risk Assessment (PRA) model. In this paper, a Monte Carlo Simulation (MSC) approach to modelling grid and switchyard induced SBOs has been proposed and successfully applied to a pressurized water reactor in Taiwan. The simulation yielded key SBO indices, which provided informed insights on the SBO risk at the plant and its mitigation. One of the SBO indices; the non-recovery probability curve, can be absorbed into existing PRA models, getting rid of laborious fault trees. It can also be directly compared with the reliability of the plant's SBO coping mechanism since it depicts the unavailability of AC power. This provides an easier means of determining the need for reliability improvement of the coping mechanism or ascertaining the adequacy of the plant's station blackout recovery capability, without reverting to the PRA model.

The multi-state node model used and the matrices introduced to define element interdependencies, create the foundation for the incorporation of additional dynamic considerations in SBO analysis. Such considerations as the number of maintenance teams on-site, EDG failure during cold standby, optimal inspection interval, delays in initiation of recovery actions, availability of spares and common-cause failures, are a possibility. Efforts are, however, underway to extend the proposed approach to include these considerations, other LOOP categories, epistemic uncertainties and relax some of the assumptions invoked in its development. In the MCS algorithm, direct Monte Carlo has been used to model start-up failures of the emergency power systems, which for realistic start-up failure probabilities, would require large MCS samples. The possibility of using advanced Monte Carlo techniques will be explored, in order to keep the computational effort moderate.

ACKNOWLEDGMENTS

The authors would like to acknowledge the gracious support of this work through the EPSRC and ESRC Centre for Doctoral Training on Quantification and Management of Risk & Uncertainty in Complex Systems & Environments. They also express gratitude to Dr. Shih-Kuei Chen of the National Tsing Hua University and his PRA team for their contribution to this work.

REFERENCES

1. Reactor Concepts Manual, *Nuclear Power for Electrical Generation*, USNRC Technical Training Center, (undated). Available at http://www.nrc.gov/reading-rm/basic-ref/students/for-educators/01.pdf, last accessed, 23rd July 2016.
2. S.A. EIDE, C.D. GENTILLON, T.E. WIERMAN and D.M. RASMUSON, *Reevaluation of Station Blackout Risk at Nuclear Power Plants (Analysis of Loss of Offsite Power Events: 1986-2004)*, U.S. Nuclear Regulatory Commission, NUREG/CR-6890, Vol. 2 (2005).
3. S.A. EIDE, C.D. GENTILLON, T.E. WIERMAN and D.M. RASMUSON, *Reevaluation of Station Blackout Risk at Nuclear Power Plants (Analysis of Loss of Offsite Power Events: 1986-2004)*, U.S. Nuclear Regulatory Commission, NUREG/CR-6890, Vol. 1 (2005).
4. Regulatory Guide (RG) 1.155, *Station Blackout,* U.S. Nuclear Regulatory Commission (1988).
5. H. GEORGE-WILLIAMS and E. PATELLI, "A hybrid load flow and event-driven simulation approach to multi-state system reliability evaluation," *Reliability Engineering & System Safety*, **152**, 351-367 (2016).
6. H. GEORGE-WILLIAMS and E. PATELLI, "Monte-Carlo based reliability/availability analysis algorithm for efficient maintenance planning," *Conference on Structural Mechanics in Reactor Technology*, Manchester, 10-14 Aug., Vol. 23 (2015).
7. E. PATELLI, *COSSAN: A Multidisciplinary Software Suite for Uncertainty Quantification and Risk Management.* In Handbook of Uncertainty Quantification, pp. 1-69, R. GHANEM, D. HIGDON and H. OWHADI, Ed., Springer International Publishing (2016).