Probabilistic Risk Assessment of Station Blackouts in Nuclear Power Plants

Hindolo George-Williams, Min Lee, and Edoardo Patelli

***Abstract*—Adequate AC power is required for decay heat removal in nuclear power plants. Station blackout accidents, therefore, are a very critical phenomenon to their safety. Though designed to cope with them, nuclear power plants can only do so for a limited time, without risking core damage and possible catastrophe. The impact of station blackouts on nuclear power plant safety is determined by their frequency, as well as duration. These quantities, currently, are computed via a static fault tree analysis which applicability deteriorates with increasing system size and complexity. This paper proposes a novel alternative framework based on a hybrid of Monte Carlo methods, multi-state modelling, and network theory. The intuitive framework, which is applicable to a variety of station blackout problems, can provide a complete insight into their risks. Most importantly, its underlying modelling principles are generic, and, therefore, applicable to non-nuclear system reliability problems, as well. When applied to the Maanshan nuclear power plant in Taiwan, the results validate the framework as a rational decision-support tool in the mitigation and prevention of station blackouts.**

***Index Terms*—Nuclear Power Plant, Station Blackout, Risk Assessment, Accident Recovery, Monte Carlo Simulation**

Notations

$min\left(\mathbf{B}\right)$	Least element of set/vector **B**.
$min\{\mathbf{B},\mathbf{Q}\}$	Least element of $\mathbf{B} \cup \mathbf{Q}$.
$\left(\mathbf{B}, i\right)$	i^{th} element of set/vector **B**.

Abbreviations

AC	Alternating Current.
DC	Direct Current.
C	Node capacity.
CCF	Common-Cause Failure.
CCG	Common-Cause Group.
CS	Cold standby state.
F	Failed state.
LOOP	Loss of offsite power.
MCS	Monte-Carlo simulation.
S	Shutdown state.
SBO	Station blackout.
SU	Start-up state.
TM	Test/preventive maintenance state.
W	Working state.

The authors are members of the Institute for Risk and Uncertainty Engineering, University of Liverpool, UK as well as the Institute of Nuclear Engineering and Science, National Tsing Hua University, Taiwan. Email: H.George-Williams@liverpool.ac.uk (Hindolo), mlee@ess.nthu.edu.tw (Min), Edoardo.Patelli@liverpool.ac.uk (Edoardo)

Nomenclature

$\mathbf{A}$	System adjacency matrix.
$\mathbf{C}$	Component capacity vector
$c_x^{\{i\}}$	Capacity of component i in state x.
$\{c_x^{\{i\}}\}_{M\times 1}$	Set of current capacities of all components.
$\mathbf{E}_i$	Set of attributes of component i.
$\mathbf{e}$	System edge matrix.
f_l	LOOP frequency.
f_s	SBO frequency.
$f_{xy}\left(t\right)$	Probability density function for transition from state x to y.
$\mathbf{G}$	System graph object.
k	Number of edges/links in system graph.
$\mathbf{lb}$	Set of minimum flow through edges/links.
M	Number of system nodes.
m	Number of safety buses/trains.
N	Number of Monte-Carlo samples.
n_1	Number of trains a generator can supply.
p_n	SBO probability given the $\left(n-1\right)^{th}$ SBO.
$\mathbf{ub}$	Set of maximum flow through edges/links.
r	Number of components affected by a CCF.
$\mathbf{r}_n\left(t\right)$	Non-recovery probability from the n^{th} SBO.
$\mathbf{S}$	Register indicating SBO occurrence.
$\mathbf{s}$	Set of source nodes.
s_j	SBO indicator for the j^{th} simulation sample.
$\mathbf{T}$	Component transition matrix.
$\mathbf{t}$	ID of virtual output node.
U_{tm}	Unavailability due to test or maintenance.
u	Proportion of train demand generator satisfies.
$\mathbf{V}$	Set of nodes in the system graph.
x_0	Initial component state.
X_{ij}	Flow from node i to j.
X_{out}	Flow into the virtual output node.
$\mathbf{Y}$	Set containing flows through all the nodes.
$\boldsymbol{\Theta}$	System inequality constraint matrix.
$\boldsymbol{\Gamma}$	System incidence matrix.
$\boldsymbol{\Phi}$	System equality constraint matrix.
Ω_{ij}	Maximum flow from node i to j.
$\eth$	Number of intermediate nodes.
$\boldsymbol{\Psi}$	System flow objective function.
$\boldsymbol{\rho}$	Set of components making up CCG.
δ	Number of components in CCG.
$\boldsymbol{\theta}$	Set of CCF probabilities.
β_1	Common failure mode for CCG.
β_2	State rendering CCG vulnerable to CCF.
$\boldsymbol{\tau}$	Vector of next node transition times.
$\boldsymbol{\mu}_{old}$	Vector of node capacities at last system jump.

I. Introduction

Nuclear power is produced by harnessing in a reactor vessel, the heat generated from a fission reaction chain. The reactor vessel is placed in a concrete containment to shield the environment from the potential release of radioactive materials. Core damage ensues when the core temperature exceeds a certain threshold or the nuclear fuel elements in the vessel are uncovered. This event may trigger containment breach, inflicting huge environmental and economic catastrophe.

Severe accident mitigation is achieved in part by ensuring a reliable cooling water circulation in the reactor vessel. This objective, during normal plant operation, is achieved through heat exchange between the primary and secondary loops of the plant's main cooling system. The process, however, ceases on plant shut down and backup cooling systems are required to sustain decay heat removal. Like the main cooling system, the backup cooling systems rely on AC power provided by sources outside the plant (offsite power). When these sources fail (Loss Of Offsite Power-LOOP), emergency sources on-site are started, to drive the plant's safety systems. If the emergency sources are also unavailable or unable to function as required, the plant is said to be in a Station Blackout (SBO). The backup cooling systems, however, are equipped with alternative turbine or diesel-driven pumps to help the plant cope with this incident. These systems, on the downside, require for monitoring and control, DC power from DC power banks. Their sustainability, therefore, regardless of their inherent reliability, is limited by the DC battery depletion time. This time, and the boil-off rate of reactor coolant, define the maximum acceptable AC power recovery duration [1].

SBO accidents are the largest contributor to nuclear power plant risk, accounting for over 70% of the core damage frequency at some plants [1], [2]. LOOP events, which initiate these accidents, are classified on the basis of their origin. A grid-centred LOOP is due to the failure of the transmission network outside the plant, switchyard-centred LOOP arises from failures in the switchyard on the plant premises, plant-centred LOOP is triggered by the operational dynamics of the plant itself, while weather-related LOOP is attributed to failures induced by severe and extreme weather, excluding lightning [1], [2]. The effective SBO risk is the sum of the core damage frequencies induced by the various LOOP types.

A. Review of Existing Models

SBO risk quantification starts with LOOP event tree analysis [3], where the Emeregency Power System availability is checked in the first heading. This event failure, which frequency defines the SBO frequency, transfers the analysis to the SBO event tree [1]. In the latter, the successes of the various mitigating actions, including offsite power and the recovery of the Emergency Diesel Generators at specific times are also checked. These times, however, vary across plants and depend on the status of a plant's mitigating systems. At the Maanshan nuclear power plant, for instance, power recovery is checked at 1, 2, 4, and 10 hours into SBO. Each top event probability in the SBO event tree requires one or more static fault trees [4]–[6] for its quantification.

Static fault tree analysis employs an analytical approach, as such, it carries the important advantage of being computationally efficient. For this reason, its sensitivity, importance, and uncertainty analysis capabilities are outstanding. These attributes explain its wide use for risk analysis in the nuclear, aviation [7], and chemical process industries [8]. Unfortunatley, fault trees become intractable with large systems or moderate systems with complex interactions [8]. They often require a detailed knowledge of the system being modelled, making them both difficult to apply and error-prone. Their static nature also limits their applicability in many ways. For instance;

i. Implementing certain types of interdependencies is either tedious or completely impossible.
ii. The analyst has to assume SBO is coincident with LOOP and that all power recovery efforts start simultaneously **after** SBO sets in. As a consequence,
   a) The SBO frequency and non-recovery probability are overestimated in most cases, since the repair of a failed element is normally initiated immediately.
   b) For plants with multiple emergency power systems, it is impossible to determine which sequence of response minimises the SBO frequency and maximises the recovery probability simultaneously.
   c) It is also difficult to investigate the effects of external factors like logistic problems, extreme environmental events, and human resource constraints on the recovery process.
iii. The analyst is forced to assume the non-occurrence of a second SBO after power recovery. This assumption, however, loses its validity if the emergency sources are recovered first. In this case, a second failure could initiate another SBO sequence before offsite power recovery.
iv. Finally, there is the problem of inconvenience due to repetitive modelling. Since the non-recovery probability is normally required for multiple instances, each would require a dedicated fault tree.

There are numerous instances of remarkable attempts at extending the applicability of fault trees to systems with interdependencies and various forms of dynamic interactions [6], [9]. Kaiser et al. [10], for instance, introduced a state/event fault tree approach that translates fault-trees to Deterministic & Stochastic Petri Nets. Similarly, Zhou et al. [11], quite recently proposed an approach that converts static fault trees to Dynamic Uncertain Causality Graphs in order to tackle the dynamic and uncertainty attributes of practical engineering systems. However, like Kaiser's approach [10], Zhou's [11] is restricted to binary-state components and systems. Even though the performance of most components could be partitioned into two levels, the existence of multiple failure modes makes binary-state models inadequate. Also, from a modelling perspective, there are occasions when the analyst would need to model a binary-state element as a multi-state one in order to fully define its behaviour. Such flexibility requires a framework supporting multi-state modelling. Bobbio's fault tree to Bayesian Network mapping procedure [12] effectively solves this problem. However, like Kaiser's and Zhou's approaches, Bobbio's mapping procedure is also susceptible to deficiencies (3) and (4) outlined above.

Dynamic Fault Trees [13]–[16] are perhaps the closest researchers have come to solving the limitations of static fault trees. Various approaches have been proposed for their solution but Markov analysis [14], [15], [17] remains the most popular. Markov modelling, however, like static fault tree analyis, becomes intractable with large systems and is only applicable to exponentially distributed transitions. Nevertheless, state explosion is no longer an issue, with the introduction of intuitive Dynamic Fault Tree software [18], [19]. Even with these developments, most of the Dynamic Fault Tree solution approaches are susceptible to deficiencies (3) and (4) outlined above. These deficiencies can only be addressed by approaches offering the flexibility to replicate the exact behaviour of the system. Such an approach, however, was put forward by Rao et al. [16], which they used to model the power supply system of a nuclear power plant. The approach simulates a system's Dynamic Fault Tree and addresses most of the limitations of static fault trees. However, like the majority of system reliability models, Rao's work is only applicable to binary-state components. The development of a more universal simulation framework, therefore, is desirable.

B. The Proposed Approach and Scope

As evidenced in Rao's, Rocha's, and Lei's works [16], [20], [21], Monte Carlo Simulation (MCS) is flexible enough to model any system attribute. Its problem, however, is that most of the existing MCS algorithms are system-specific and require either the structure function, cut sets, or path sets of the system. An intuitive event-driven MCS procedure, offering multi-state component modelling opportunities has recently been proposed [22]. This procedure is general and does not require the definition of the system's path & cut sets or structure function, thanks to its embedded graph model.

In this work, the graph and multi-state models proposed in [22] are adopted. The graph model is used to model the topology of the system and allow the performance of the system to be directly computed from the performance of the components. This attribute eliminates the need for an explicit association of component failure combinations to the state of the system. The multi-state model, on the other hand, is used to model the behaviour of the components, overcoming the assumption of a perfectly binary behaviour of components. It is particularly useful to the multiple failure mode and dynamic attribute representation of the Emergency Power Systems. This model, for instance, could be exploited to investigate the effects of limited maintenance teams or the unavailability of spares on the Emergency Power Systems recovery [23]. We extend the original model to incorporate interdependencies by means of a dependency matrix and an efficient recursive algorithm to propagate the effects of failures across the system. Completing the framework, we propose a simple MCS algorithm that induces LOOP in the system, replicate the ensuing sequence of events, and monitor the availability of power at the various safety buses. The number of available safety buses, as a function of time, is computed after each system event. From the simulation history, any SBO index can be computed, thereby providing an opportunity for more insights into SBO risks. The multi-state component model, together with the dependency matrix, adequately captures and represents the redundancies in the emergency power system of the plant. Consequently, the explicit modelling of these redundancies, which poses a significant challenge, is eliminated.

1) Merits & Novelty of Proposed Approach: The framework, for now, is limited to grid and switchyard induced LOOP, given their dominance [2]. Its preliminary results were first presented at the 13^{th} Probabilistic Safety Assessment and Management (PSAM) conference [24]. However, this paper proposes several improvements. Firstly, an extensive review of the suitability of fault trees and their derivatives, to SBO analysis has been included. We have also considered the effects of Common-Cause Failures (CCF), unavailability due to test or maintenance, and human error on the SBO frequency and recovery probability. We also show how the results obtained from the framework can be absorbed in the existing model. Finally, we extend the number of computable SBO indices and consider the effects of system configuration and the sequence of operator response on system recovery.

This paper is the first documented application of load-flow simulation to a complete SBO risk assessment. With respect to the existing models discussed in Section I-A, the proposed framework exhibits the following advantages;

- **Adequacy & Flexibility** - it models realistic attributes of the plant's power recovery and provides more insights into SBO risks. For instance, it enhances the investigation of the possibility of a second SBO after the first.
- **Convenience & Generality** - it is convenient in the sense that the modeller does not need to deduce the combination of component failure leading to system failure. They also do not need to explicitly model component redundancies, as these are implicitly captured by the modelling framework. The modelling framework, in addition, is applicable to many system reliability problems.

2) Solution Sequence: The proposed approach is applied as summarised by the following chronological steps;

i. Identify the key elements of the system, define its topology, and derive its flow equation parameters.
ii. Develop the multi-state model for each system element.
iii. Model the interdependencies between the elements.
iv. Force a LOOP event and simulate the behaviour of the standby power systems.
v. Compute the SBO indices from the simulation history.

II. Station Blackout Modelling

A nuclear power plant's power system consists of the grid, the switchyard, the Emergency Power Systems, alternative Emergency Power System, and the safety buses. The Alternative Emergency Power Systems are additional emergency sources (such as Gas Turbine Generators) available at some plants to boost their LOOP/SBO recovery capability. In this section, we show how the plant's power system is accurately modelled and analysed, in line with the solution sequence outlined in Section I-B2.

A. The System Topology

We represent the topology of the plant's power system by a graph which nodes depict the components of the system. Connecting the nodes are perfectly reliable 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. This virtual node would later be used to compute the non-recovery probability of AC power.

Let the nodes of the system be numbered from 1 to M and represented by the set $\mathbf{V} = \{1, 2, ..., M\}$. Since the links are perfectly reliable, the adjacency matrix, $\mathbf{A}$, of the system is defined as;

$$\mathbf{A} = \{a_{ij}\}_{M \times M} \mid a_{ij} = \begin{cases} 1 & \text{If flow is } i \rightarrow j \\ 0 & \text{Otherwise} \end{cases} \quad (1)$$

The topology of the system, therefore, can be defined by $G \mid G = (\mathbf{V}, \mathbf{A})$. Using the parameters of G only, the flow equations of the system can be derived [22]. These equations can then be used in synergy with the current state properties of the system nodes to deduce the performance of the system. For this, a linear programming algorithm is employed, given the possibility of flow redirection and the need to satisfy the capacity constraints of the nodes and their links. The objective is to find the flow across each link of the system that maximizes the flow into the virtual node. If X_{ij} is the flow across the link between nodes i and j and given there are k such links for all $(i, j) \in \mathbf{e}$, where $\mathbf{e}$ is the edge matrix of the system as defined in [22], the linear programming problem is formulated by (2), (5), (7), and (8).

$$\mathbf{\Theta}\{X_{ij}\}_{k \times 1} \leq \{c_x^{\{i\}}\}_{M \times 1} \mid (i, j) \in \mathbf{e}, \quad \forall i \in \mathbf{V} \quad (2)$$

Equation (2) expresses the inequality constraints to be satisfied, where $c_x^{\{i\}}$ denotes the capacity of node i when residing in state x. $\{c_x^{\{i\}}\}_{M \times 1}$, therefore, is the vector of current capacities of all the nodes of the system. The inequality matrix, $\mathbf{\Theta}$, is related to the incidence matrix, $\mathbf{\Gamma}$, as follows,

$$\mathbf{\Theta} = \{\theta_{iq}\}_{M \times k} \mid \theta_{iq} = \begin{cases} 1, & \gamma_{iq} \neq 0 \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

$$\mathbf{\Gamma} = \{\gamma_{pq}\}_{M \times k} \mid \gamma_{pq} = \begin{cases} 1, & p = i \\ -1, & p = j \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

$\mathbf{\Gamma}$ is related to $\mathbf{A}$ by (4), where $q = 1, 2, ..., k$ (the edge number) is the index of the edge between nodes i and j in $\mathbf{e}$ and $p = 1, 2, ..., M$.

$$\mathbf{\Phi}\{X_{ij}\}_{k \times 1} = \{0\}_{\eth \times 1} \quad \forall (i, j) \in \mathbf{e} \quad (5)$$

Equation (5) expresses the equality constraint to be satisfied, where $\mathbf{\Phi}$ and $\mathbf{\Gamma}$ are related thus;

$$\begin{aligned} &\mathbf{\Phi} = \{\phi_{\lambda q}\}_{\eth \times k} \mid \phi_{\lambda q} = \gamma_{pq} \\ &\lambda = 1, 2, ..., \eth \mid \eth < M \quad f : \lambda \rightarrow p \quad \forall p \in (\mathbf{s} \cup \mathbf{t})' \end{aligned} \quad (6)$$

$\eth$ is the number of intermediate nodes, $\mathbf{s}$ is the set of source nodes, which comprises the grid and standby power systems while $\mathbf{t}$ is the virtual node representing the total output of the system. If the intermediate nodes of the system (i.e., nodes not in $\mathbf{s}$ and $\mathbf{t}$) are arranged in ascending order of their ID, (6) suggests the λ^{th} row of $\mathbf{\Phi}$ is identical to the p^{th} row of $\mathbf{\Gamma}$, where p is the λ^{th} element of the ordered set of intermediate nodes. In other words, $\mathbf{\Phi}$ is a sub matrix of $\mathbf{\Gamma}$, containing all the rows of the latter corresponding to intermediate nodes.

$$\begin{aligned} \mathbf{lb} = \{0\}_{k \times 1}, \quad \mathbf{ub} = \{\Omega_{ij}\}_{k \times 1} \\ \Omega_{ij} = \min\{c_{max}^{\{i\}}, c_{max}^{\{j\}}\} \quad \forall (i, j) \in \mathbf{e} \end{aligned} \quad (7)$$

Equation (7) defines the lower and upper bound vectors, **lb** and **ub**, of the flow through the links, where $c_{max}^{\{i\}}$ is the maximum capacity of node i. Finally, the objective function of the linear programming problem is expressed in (8).

$$\mathbf{\Psi} = -\{\psi_q\}_{1 \times k}\{X_{ij}\}_{k \times 1} \mid \psi_q = \sum_{i \in s} \gamma_{iq} \quad (8)$$

Following the termination of the linear programming algorithm, the vector of flow, $\mathbf{Y}$, through the nodes of the system is given by $\mathbf{\Theta}_{M \times k}\{X_{ij}\}_{k \times 1}$. The total output, therefore, is given by the $\mathbf{t}^{th}$ element, $(\mathbf{Y}, \mathbf{t})$, of $\mathbf{Y}$. Interestingly, all the parameters, but $\{c_x^{\{i\}}\}_{M \times 1}$, required to compute $\mathbf{Y}$ remain static during system simulation. The main task, therefore, is to update $\{c_x^{\{i\}}\}_{M \times 1}$ after each system event. The derivation of (2) to (8) is outside the scope of this paper, interested readers are referred to [22]. However, an illustrative example of the linear programming problem formulation is provided in the Appendix to this paper.

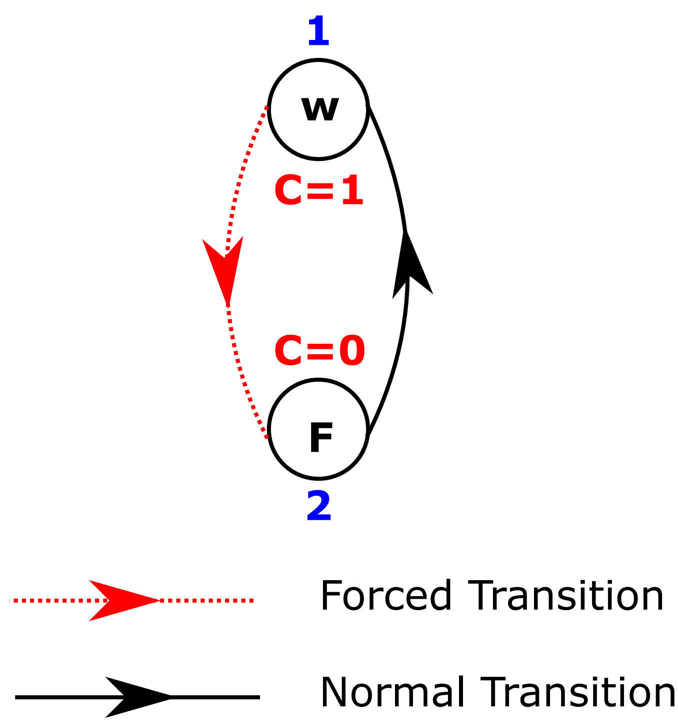


Fig. 1. Multi-state model for Grid and Switchyard nodes

B. The System Components

Each component is defined by a multi-state model that takes into account the various parameters that characterise its

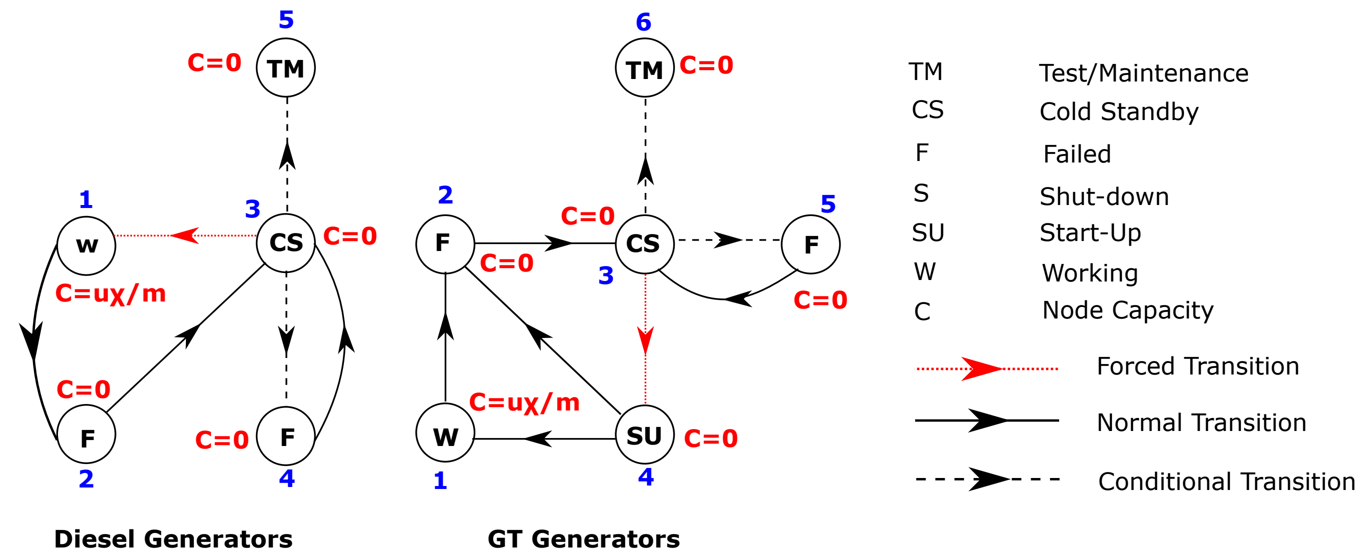


Fig. 2. Multi-state models for Emergency Diesel and Gas Turbine Generators without human error consideration

operation. Let E_i denote component i, then,

$$E_i = (\mathbf{T}, \mathbf{C}, x_0) \tag{9}$$

$$\mathbf{T} = \{T_{xy}\}_{n\times n} \mid x \neq y \quad (x, y) \in \{1, 2, ..., n\}$$

$$T_{xy} = \begin{cases} \infty, & \text{If } x \to y \text{ is a forced transition} \\ 0, & \text{If no transition between states x \& y} \\ f_{xy}(t), & \text{Otherwise} \end{cases} \tag{10}$$

Where $\mathbf{T}$ is the transition matrix of the component; $\mathbf{C} \mid \mathbf{C} = \{c_x\}_{1\times n}$, its capacity vector; x_0, its initial state; c_x, its capacity in state x; n, its number of states; and $f_{xy}(t)$, the probability density function characterizing the transition from state x to y. $\mathbf{T}$ contains the density function objects for all the transitions depicted in the multi-state model of the component and $\mathbf{C}$ defines the capacity of the component in each state.

Each state capacity is expressed as a non-dimensional number defining the proportion of total system output the node can supply or transmit whilst residing in that state. If m is the total number of power trains at the plant, n_1, the number of power trains the node simultaneously supplies, u, the proportion of power train demand it can satisfy, then, its capacity when working perfectly is, $n_1 u m^{-1}$. It expresses the total system output as a fraction of the number of power trains/safety buses present at the plant. On this note, the grid and switchyard nodes are each assigned unity capacity when available and 0, otherwise. The virtual output node has a fixed capacity of 1 and each safety bus, a fixed capacity of m^{-1}.

1) Modelling the Grid and Switchyard: The grid is modelled as a 2-state node; 'Working', when available and 'Failed', otherwise. Though grid failures are mostly random, we model them as forced transitions [23], since they already are incorporated in the LOOP frequency. Most often, plants tap their AC power from multiple offsite sources, and grid failure is defined as the failure of all of these sources. The repair of at least one of the failed sources, however, is sufficient to achieve grid recovery. For this reason, the transition from 'Failed' to 'Working' is defined by the upper bound of the envelope around the cumulative density functions (cdf) of the individual source repair distributions. Given this, sampling the grid recovery time entails generating a uniform random number and reading off its corresponding time from the envelope cdf, interpolating where necessary. An important point to note is, this approach slightly underestimates the grid recovery probability, as it assumes the individual source repair actions are initiated concurrently. In practice, the sources do not necessarily fail simultaneously and their recovery actions may commence at different times. This implies, by the time the last source fails, the restoration of already failed sources would have begun. The actual grid recovery time, therefore,

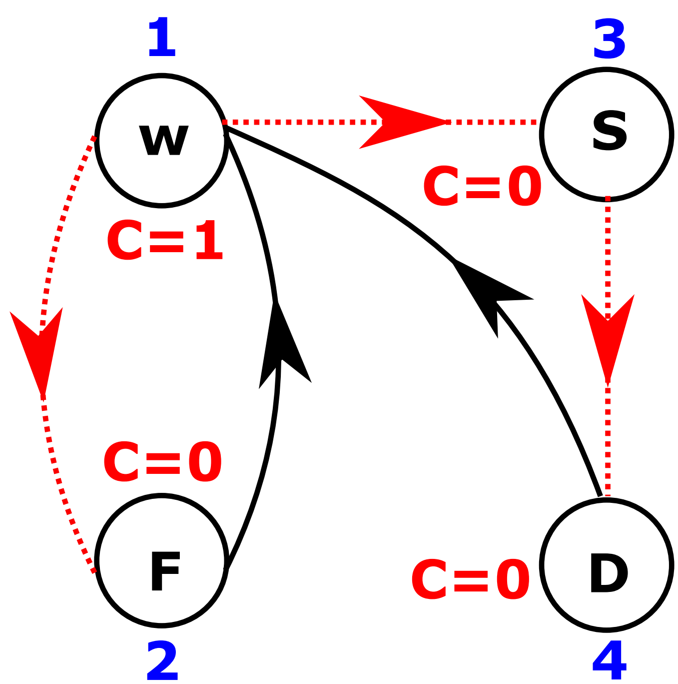


Fig. 3. Multi-state model for switchyard with human error consideration

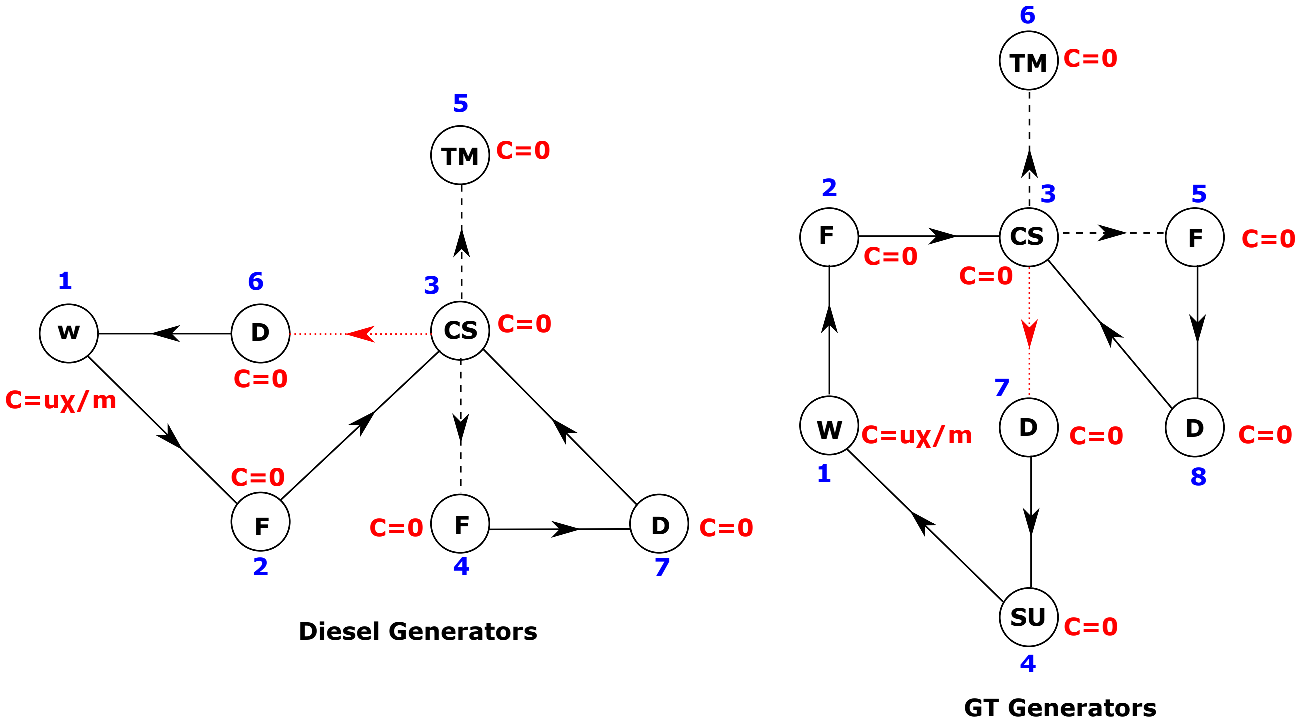


Fig. 4. Multi-state models for Emergency Diesel and Gas Turbine Generators with human error consideration

is less than that given by the envelope cdf. This, however, is acceptable, as the goal in risk management is to ensure risk levels are acceptable, even in worst case scenarios.

Similarly, normal switchyard operation is defined by a 2-state node. In cases where the plant is enhanced with multiple switchyards, switchyard recovery is treated as in the case of multiple grid sources. Fig. 1 shows the multi-state model for the Grid and Switchyard.

2) Modelling the Standby Power Systems: The Emergency Power System is constituted by the Emergency Diesel Generators (EDG), and in this work, Gas Turbine Generators (GTG) constitute the Alternative Emergency Power System. In this section, we model only the multi-state behaviour of the standby power systems, and the effects of redundancies on their operation is considered in a latter section. We make the following assumptions in developing these models;

i. The initiation of test/maintenance is coincident with LOOP, and at any instance, there is not more than one source in test or maintenance.
ii. Sources in test or maintenance remain unavailable through the sequence.
iii. Repairs are commenced immediately.
iv. A generator just from maintenance cannot fail to start. This implies a perfect maintenance scenario.

The Alternative Emergency Power System recovery is assumed offsite power recovery in [24]. This assumption is on the premise that their failure is included in the LOOP frequency. However, the assumption is impractical, given they are mostly a standby source. We, therefore, modify their multi-state model to include running failures, rendering them an on-site source.

We consider failure-to-start and failure-to-run as the only failure modes an Emergency Diesel Generator is susceptible to. Failure-to-start refers to the Emergency Diesel Generator failure to start from cold-standby and failure-to-run denotes its failure to function for the duration of the LOOP. While the former is defined by a crisp probability, the latter is characterised by a time-to-failure probability density function. However, the Standardised Plant Analysis Risk (SPAR) model [1] considers a third Emergency Diesel Generator failure mode, failure-to-load, defining the case when the Emergency Diesel Generator starts but cannot power the load. This failure mode is considered failure-to-start, in the proposed framework. We introduce two additional states, 'Working' and 'TM', as shown in Fig. 2, to account for the perfect operation of the Emergency Diesel Generator and its unavailability due to test or maintenance, respectively. Except otherwise, the transition from cold standby to working is instantaneous, whilst the transition from cold standby to failure or TM is also instantaneous but conditional. Conditional transitions are a special type of forced transition depending on a probabilistic event that is external to the component and with a known likelihood [23]. Conditional and forced transitions have the same representation in the transition matrix of the component (see (10)).

The Gas Turbine Generators behave in almost the same way as the Emergency Diesel Generators, save for the difference in their start-up and manual alignment times. For this, a start-up state is inserted between their cold-standby and working states, as shown in Fig. 2. Whilst in start-up, they could fail, explaining the transition from start-up to failure.

3) Accounting for Human Error: Human error is very important in the risk assessment of engineering systems. In SBO recovery, human errors mostly manifest themselves as delayed response to a certain SBO mitigation action. For instance, the switchyard is forced into a temporary shut down state during grid failures. On grid recovery, the plant personnel manually initiate its restoration, which process is susceptible to human-induced delays. Accounting for these delays, two additional states are introduced in the 2-state model discussed in Section II-B1, as shown in Fig. 3. The transitions from 'Working' to 'Shutdown' and from 'Shutdown' to 'Delay' (D), are influenced by grid failure and recovery respectively. 'Shutdown' denotes grid recovery-in-progress, while 'Delay' represents switching-in-progress. The latter determines 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, the model in Fig. 1 is retained.

Similarly, the Gas Turbine Generator and some Emergency Diesel Generators require manual start-up and alignment, this is the case for shared diesel generators. A generator is said to be shared if it can substitute several units but, however, can only replace one unit at a given instance. Therefore, in the case of sequential multiple unit failures, only the first unit is replaced. For simultaneous failures, any of the units can be replaced, since they normally are identical. Since these replacements are manually executed, they are susceptible to delays, contrary to what most models suggest. Fig. 2, for instance, assumes the transition from cold standby to the fully functional or failure state to be instantaneous. This, by extension, implies, any maintenance action (if the generator fails to start) is initiated at once. However, with human error, the start-up procedure may be initiated latter than scheduled. We, therefore, introduce two states, one each, between cold standby & working and failure & cold standby, as shown in Fig. 4, to account for these delays. We have assumed the plant personnel to be well trained, experienced, and fit to perform their assigned tasks as expected. Consequently, the possibility of inappropriately executed actions is ignored.

Transitions $6 \rightarrow 1$ with $4 \rightarrow 7$ and transition $7 \rightarrow 4$ with $5 \rightarrow 8$, of Fig. 4, account for human error in the recovery of manually operated Emergency Diesel and Gas Turbine Generators respectively. In practical applications, human error is expressed in terms of the probability of not completing a given action within a specified time. If this probability is known for multiple times, a *cdf* could be fitted through the points. For this, we recommend the Weibull distribution, since it can yield a wide range of distributions. Recall the *cdf* of a Weibull distribution is $1 - e^{-(t/a)^b}$, where a and b are its scale and shape parameters respectively. Given the human error probabilities are the likelihoods of inaction, they define the complement of the human reaction time *cdf*. Therefore, the Weibull parameters, a and b, are obtained by fitting the set of probability values to the function $e^{-(t/a)^b}$.

C. Modelling Component Interdependencies

To ensure resilience, system designers often employ multiple layers of defence, either in the form of redundancies or shared components. This proactive strategy inadvertently introduces interdependencies in the system, resulting in modelling accuracy issues. We define interdependency in a more general sense as the potential for a state change in one element to trigger a state change in another. We propose two models, the Common-Cause Failure (CCF) and the cascading failure models, to implement these interdependencies.

1) The CCF Model: This model is used when the random failure of any member of a group of similar components, performing the same task could cause the failure of one or more of the remaining components [25]. Such a group of components is called a Common-Cause Group (CCG), and its key attributes are;

- There is a set of probabilities associated with the number of components involved in any random failure event. Let this set of probabilities be defined by $\boldsymbol{\theta} \mid \boldsymbol{\theta} = \{\theta_r\}^{\delta}$, where r is the number of components affected by the failure event, δ, the total number of components in the group, and $\sum_{r=1}^{\delta} \theta_r = 1$.
- All the components in the CCG fail in the same mode. Implying, the CCG for start-up failures cannot influence the CCG for running failures, for instance.

Each CCG, therefore, is defined by the quadruple, $(\boldsymbol{\rho}, \beta_1, \beta_2, \boldsymbol{\theta})$. Where, $\boldsymbol{\rho}$ is the set of components in the CCG, β_1, the common failure mode, and β_2, the state the components have to be in to be susceptible to this failure mode. The algorithm for propagating CCF is summarised thus;

i. When a component fails, check if its new state matches β_1 for its CCG.
ii. Go to step (v) if there is no match. Else, determine the number of components, r, that will fail.
iii. Go to step (v) if $r = 1$. Else, remove from $\boldsymbol{\rho}$, the component initiating the failure event. From the remainder, randomly select $r - 1$ components.
iv. For each component selected in step (iii), check if its current state matches β_2 and set this to β_1.
v. End procedure.

The procedure above requires $\boldsymbol{\theta}$ to be in conformity with the α-Factor model [25]. CCF probabilities expressed in the Multiple Greek Letter model would need to be converted as in [25].

2) The Cascading Failure Model: This model is used for interdependencies not satisfying the CCF criteria. For instance, the redundancies among the standby power systems and the dependence of the latter on the grid and switchyard. An important assumption invoked in this model, however, is that on occurrence of the trigger event, the dependent event occurs immediately.

Initially proposed in [26], the model defines interdependencies by a dependency matrix. The dependency matrix, $\mathbf{D}_i$, for node i, defines the effects of the node's state transition on other nodes. It takes the form, $\mathbf{D}_i = \{d_{j1}, d_{j2}, d_{j3}, d_{j4}\}_{v \times 4} \mid j = 1, 2, ..., v-1, v$, 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 vulnerable, and d_{j4}, its target state after the event. Each row of $\mathbf{D}_i$ defines the behaviour of an affected node, and v, the number of relationships. For example, consider a 2-component system, with each component existing in 3 possible distinct states. When component 1 makes a transition to state 3, component 2 is forced to make a transition to state 2 as well, if and only if the latter is currently residing in state 1.

Since component 1 is the trigger component in this case, the interdependency is defined by $\mathbf{D}_1$ as,

$$\mathbf{D}_1 = \begin{pmatrix} 3 & 2 & 1 & 2 \end{pmatrix} \quad (11)$$

Let a third 3-state component be added to the system. In addition to its effect on component 2, let the transition of component 1 also affect component 3, such that the latter is forced to state 1 if it is in state 3 at the time of the trigger event. To represent the overall behaviour of component 1, $\mathbf{D}_1$ is updated as shown in (12), to reflect the new information.

$$\mathbf{D}_1 = \begin{pmatrix} 3 & 2 & 1 & 2 \\ 3 & 3 & 3 & 1 \end{pmatrix} \quad (12)$$

(12) shows that each row of the dependency matrix represents a possible outcome.

Occasionally, a state change in a node can only affect another node if a third node is in a certain state. This type of dependency is known as a joint dependency, and it is outside the scope of the initial model in [26]. We introduce the joint dependency matrix, $\mathbf{D}' = \{d'_{j1}, d'_{j2}, d'_{j3}, d'_{j4}\}_{v\times 4}$, to resolve this problem. Element d'_{j1} defines the state the third node must be in to satisfy the joint dependency while d'_{j2}, d'_{j3}, and d'_{j4} have the same meaning as d_{j2}, d_{j3}, and d_{j4} respectively. Assuming a certain state change in node i only affects, say node x, if node ω is in state σ, $\mathbf{D}_i$ defines the relationship between nodes i and ω, while $\mathbf{D}'_\omega$ defines the relationship between ω and x. Nodes i, ω, and x are the trigger, intermediate, and target nodes respectively. The intermediate node does not undergo a state change, meaning its target state is the same as its vulnerable state. Therefore, in $\mathbf{D}_i$, the 3^{rd} and 4^{th} elements of the row corresponding to the intermediate node are equal. Given $j = 1$, for $\mathbf{D}_i$, $d_{12} = \omega$, $d_{13} = d_{14} = \sigma$ and for $\mathbf{D}'_\omega$, $d'_{11} = \sigma$, $d'_{12} = x$. The remaining elements retain their meaning, as defined earlier. Let, for illustrative purposes, the dependency between components 1 and 3 (second row of $\mathbf{D}_1$ in (12)) only hold if component 2 is in state 2.

$$\mathbf{D}_1 = \begin{pmatrix} 3 & 2 & 1 & 2 \\ 3 & 2 & 2 & 2 \end{pmatrix} \quad \mathbf{D}'_2 = \begin{pmatrix} 2 & 3 & 3 & 1 \end{pmatrix} \quad (13)$$

To represent this attribute, the second row of $\mathbf{D}_1$ is modified to reflect the relationship between components 1 and 2, and the relationship between components 2 and 3, defined by $\mathbf{D}'_2$ as shown in (13). Notice $\mathbf{D}'_2$, instead of $\mathbf{D}_2$, has been used, since the relationship between components 2 and 3 is due to a joint dependency with another component.

The dependency and joint dependency matrices, indeed, can be used to represent a wide range of dependencies. However, there are a few instances that may result in large matrices. Such cases require an intuitive manipulation, to keep the matrix size moderate and prevent modelling error. We introduce a negative sign in front of the trigger or vulnerable state to signify that the dependency is satisfied only if the component is **not** in that state. This notation is analogous to the **NOT-gate** in fault trees. For instance, if component 1, in the scenario above, can affect component 3 only if component 2 is in states 2 or 1, it is efficient to exploit the **NOT** notation, instead of inserting an additional row in each of $\mathbf{D}_1$ and $\mathbf{D}'_2$. Recalling that component 2 has 3 states, state 2 **OR** state 1 is logically equivalent to **NOT** state 3. Hence, the dependency matrices, $\mathbf{D}_1$ and $\mathbf{D}'_2$, become,

$$\mathbf{D}_1 = \begin{pmatrix} 3 & 2 & 1 & 2 \\ 3 & 2 & -3 & -3 \end{pmatrix} \quad \mathbf{D}'_2 = \begin{pmatrix} -3 & 3 & 3 & 1 \end{pmatrix}$$

We propose a recursive algorithm to implement the dependency matrices. If x_i denotes the new/current state of node i, the algorithm is summarised thus;

i. Define a register, $\mathbf{R}$, to hold the affected components, their vulnerable, and target states.
ii. Using $\mathbf{D}_i$ and x_i , find all components affected by the state change and update $\mathbf{R}$ with elements 2 to 4 of the rows representing the components.
iii. Select the last row of $\mathbf{R}$ and check if its last two elements are equal. This row defines the dependency induced in component ω by component i.
iv. If the response to the query in step (iii) is in the affirmative, designate the equal elements, ϵ, delete the last row of $\mathbf{R}$, and;
   a) Using ω, $\mathbf{D}'_\omega$, and x_ω as inputs, call steps (i) to (vii), noting that a row in $\mathbf{D}'_\omega$ is affected by the state change only if its first element is ϵ.
   b) Continue from step (iii).

   Else, proceed to step (v).
v. Force the designated transition as determined in step (iii) and delete the last row of $\mathbf{R}$. If the affected node is in standby, and its target state, Working, Delay, or Start-Up, initiate its start-up procedure.
vi. If $\mathbf{D}_\omega$ exists, repeat steps (ii) to (vi), replacing $\mathbf{D}_i$ and x_i with $\mathbf{D}_\omega$ and x_ω respectively.
vii. Repeat steps (iii) to (vi) until $\mathbf{R}$ is empty, and terminate the procedure.

III. System Simulation & Analysis

The system's operation is imitated by generating random failure events of components and their corresponding repairs. For every component transition, the capacity vector, $\{c_x^{\{i\}}\}_{M\times 1}$, of the system is updated and used to deduce the flow, $(\mathbf{Y}, \mathbf{t})$, through the output node. At time $t = 0$, the grid and switchyard nodes are in operation, while the Emergency Power Systems and Alternative Emergency Power Systems are in cold standby. LOOP is initiated by setting the grid (for grid centred LOOP) or the switchyard (for switchyard centred LOOP) to its failure state. The next transition parameters of the standby systems are sampled, and the simulation is moved to the earliest transition time, t. Components with next 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 cycle of events continues until offsite power is recovered.

Let $\boldsymbol{\mu}_{old}$ hold the node capacities at the previous system transition, $\boldsymbol{\tau}$, the vector of next node transition times, N, the number of simulation samples, and $\mathbf{S} = \{s_j\}^N$, the register indicating the occurrence of an SBO. The indicator register, $\mathbf{S}$, is such that, $s_j = 1$ if an SBO occurs in the j^{th} sample, and 0, otherwise. The simulation algorithm is summarised thus;

LOOP	ONSITE POWER FAILURE	REACTOR PROTECTION SYSTEM	RCS	AFW	EMERGENCY PRESURIZATI	RCP SEAL STAGE 1 INTEGRITY	RCP SEAL STAGE 1 INTEGRITY	RCP SEAL STAGE 2 INTEGRITY	RCP SEAL STAGE 2 INTEGRITY	OFFSITE POWER RECOVERY	ONSITE POWER RECOVERY
T(PG)	EM	K	Q	L(T)	X(E)	BP1	O1	BP2	O2	ER1	ER2

Fig. 5. An excerpt from the SBO event tree showing headings (credit: [1])

i. Initialize the register storing the flow through the output node, set $N = 1$, $\mathbf{S} = \{\}$, and define the simulation stopping criterion. The stopping criterion could be the number of LOOP, number of SBO, or convergence of the SBO probability.

ii. Determine which component will be unavailable due to test or maintenance.

iii. Set $s_N = 0$ and $\boldsymbol{\tau} = \{\infty\}^M$, where M is the number of nodes in the system.

iv. Force LOOP as described earlier, accounting for interdependencies according to the procedures described in Sections II-C1 and II-C2. Remember to sample the next transition parameters after every node transition and update $\boldsymbol{\tau}$. See [22] for the procedure for sampling the transition parameters of a multi-state node.

v. Define $\boldsymbol{\mu}$ using the current states of the nodes, that is, $\boldsymbol{\mu} = \{c_{x_0}^{\{i\}}\}_{M\times 1}$ and set $t = 0$, $\boldsymbol{\mu}_{old} = \boldsymbol{\mu}$.

vi. Determine $X_{out} \mid X_{out} = (\mathbf{Y}, \mathbf{t})$ and save as a function of time.

vii. Set $s_N = s_N + 1$ if $X_{out} = 0$ and determine the next simulation time, $t = min\,(\boldsymbol{\tau})$.

viii. 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), and update $\boldsymbol{\mu}$ & $\boldsymbol{\tau}$.

ix. Restart nodes returning from repairs if X_{out}, as previously determined, is less than 1.

x. If $\boldsymbol{\mu}_{old} \neq \boldsymbol{\mu}$;
   a) Compute X_{out} and set $s_N = s_N + 1$ if $X_{out} = 0$.
   b) Save X_{out} if different from the previous.
   c) Temporarily set the capacity of the switchyard node to 1 if it is in 'Shutdown' and calculate the new system flow. If this flow is non-zero, set the switchyard to start-up, sample its next transition parameters, and update $\boldsymbol{\tau}$.

xi. Set $\boldsymbol{\mu}_{old} = \boldsymbol{\mu}$, $t = min\,(\boldsymbol{\tau})$, and check if offsite power is recovered.

xii. Repeat steps (viii) to (xi) until offsite power is recovered. Discard history N if $s_N = 0$ and set $N = N + 1$.

xiii. Repeat steps (ii) to (xii) until the simulation stopping criterion is met, and terminate algorithm.

xiv. Compute the relevant SBO indices

A. SBO Indices: Computation & Relevance

The SBO frequency, f_s, makes the list of the most informative and desired SBO indices. It defines the expected number of times, per year, an SBO occurs at a plant. If p_1 defines the conditional probability of an SBO given a LOOP occurring at frequency, f_l, per year, then,

$$f_s = p_1 f_l \qquad p_1 = \frac{\sum(\mathbf{S} > 0)}{N - 1} \tag{14}$$

The fraction of f_s occurring at start-up is deduced from the number of SBO at time 0. This index could be used to assess the efficiency of the start-up procedure, as well as the vulnerability of the generators in cold standby.

The non-recovery probability, $\mathbf{r}_1\,(t)$, defines the likelihood of recovery duration from an SBO accident exceeding a given time. It is computed as detailed in [26], and like p_1, belongs to the set of inputs to the SBO event tree. Given it defines the unavailability of power at the plant, $\mathbf{r}_1\,(t)$ can be directly compared with the reliability of the SBO mitigating mechanism. The outcome of such a comparison would help ascertain the adequacy of the mitigating mechanism. In addition, $f_s \times \mathbf{r}_1\,(t)$ yields the frequency of exceedance, a measure of the overall SBO risk at the plant. The quantity also presents a means of assessing the relative effectiveness of multiple recovery responses or operational constraints.

Finally, the conditional probability of a second SBO, p_2, given an SBO has already occurred is given by,

$$p_2 = \frac{\sum(\mathbf{S} > 1)}{\sum(\mathbf{S} > 0)} \tag{15}$$

Knowledge of p_2 may shape the recovery response on the occurrence of a second SBO. For instance, a plant with a large p_2 would require the logistics used in the recovery of the first SBO left in the field and the operations staff kept on high alert. This reduces human error, ensuring a lower non-recovery probability, $\mathbf{r}_2(t)$, of the second SBO.

Generally, the conditional probability, p_n, of the n^{th} SBO given the $(n-1)^{th}$ SBO is expressed as,

$$p_n = \frac{\sum(\mathbf{S} > n - 1)}{\sum(\mathbf{S} > n - 2)} \tag{16}$$

If absolute probabilities are required instead, the denominator in (16) is replaced with $N - 1$.

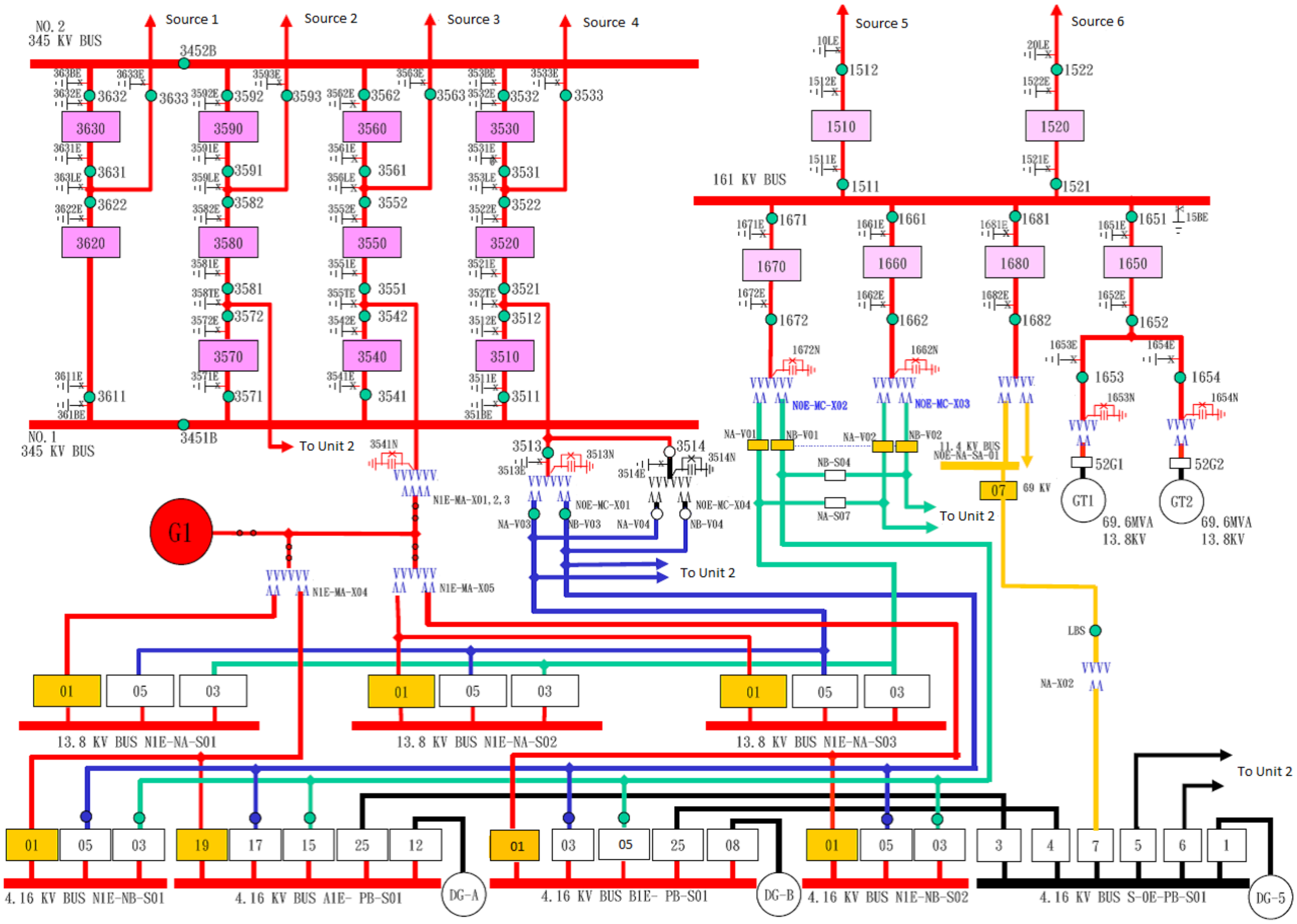


Fig. 6. Layout of the Maanshan nuclear power plant AC distribution system (credit: Dr Shih-Kuei Chen, NTHU, Taiwan)

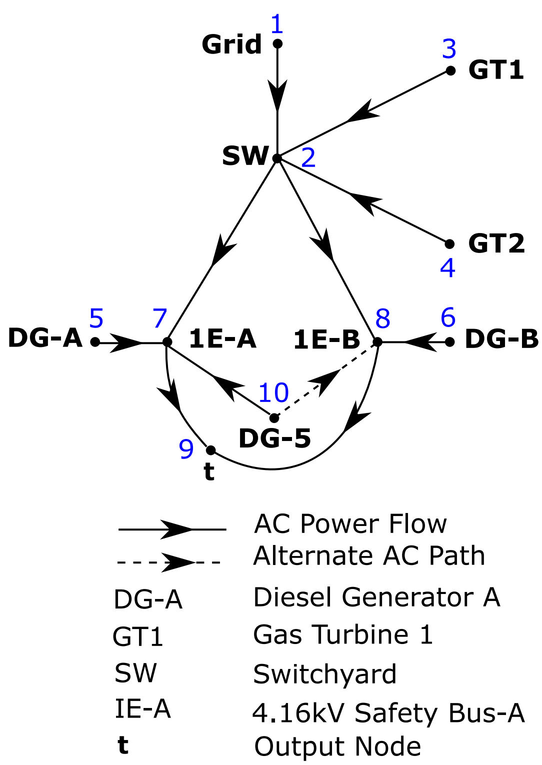


Fig. 7. Simplified schematic of plant's AC distribution system

B. *Incorporation into the Existing Framework*

Shown in Fig. 5 is an excerpt from the SBO event tree presented in [1]. Of its 12 headings, only four; T(PG), EM, ER1, and ER2 are of relevance to SBO recovery. The first depicts LOOP, and requires the LOOP frequency. The second represents SBO occurrence, and requires the unavailability of the standby power systems. Here, the chain of complicated fault trees in the existing model can be replaced with the conditional SBO probability, p_1. The last two headings represent offsite and standby power recovery respectively. These can be merged into one heading, say AC power recovery, and the complicated fault trees replaced with a crisp value read from $\mathbf{r}_1(t)$. With these, the core damage frequency induced by the first SBO is computed by solving the event tree, using standard procedure. For the second SBO, the first is regarded the initiating event. The LOOP frequency, therefore, is replaced with f_s, p_1 with p_2, and $\mathbf{r}_1(t)$ with $\mathbf{r}_2(t)$.

IV. Case Study: An Application to the Maanshan Nuclear Power Plant in Taiwan

The Maanshan plant is a two-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

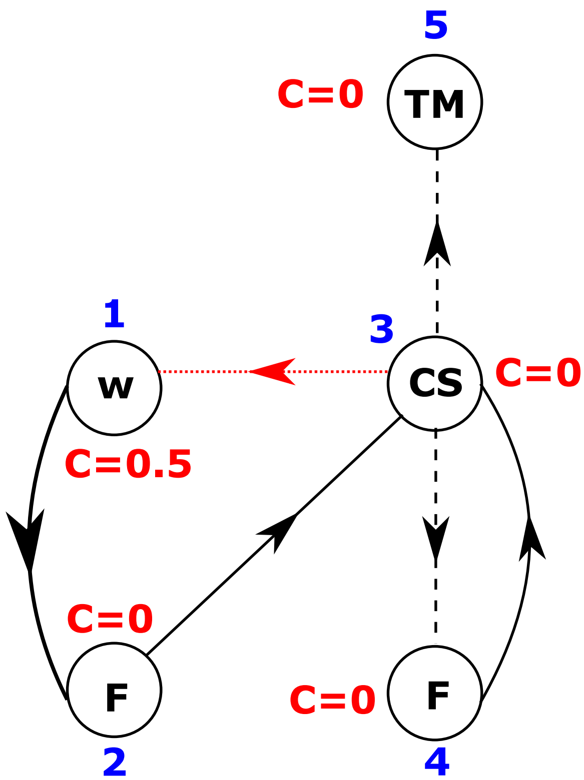


Fig. 8. Multi-state model for the main diesel generators (DG-A & DG-B)

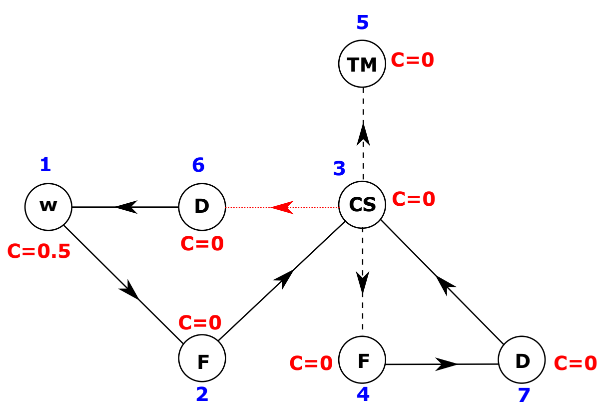


Fig. 9. Multi-state model for the shared diesel generator (DG-5)

and the remainder, through the 161 kV switchyard. It is powered through two safety buses, AIE-PB-S01 and BIE-PB-S01, each with a dedicated Emergency Diesel Generator; DG-A and DG-B, respectively. A shared Emergency Diesel Generator, DG-5, connected as shown in Fig. 6 is available as backup in case any of the dedicated generators is unavailable. In addition to the shared Emergency Diesel Generators, are two Gas Turbine Generators, GT1 and GT2, connected via the 161kV switchyard. These generators form the Alternative Emergency Power System of the plant, each satisfying the demand on both power trains.

During normal plant operation, the safety buses are fed by the main plant generator, G1, via the red lines and the normally closed breakers 19 & 01. On plant shut down, G1 becomes unavailable, and the safety buses are forced to tap

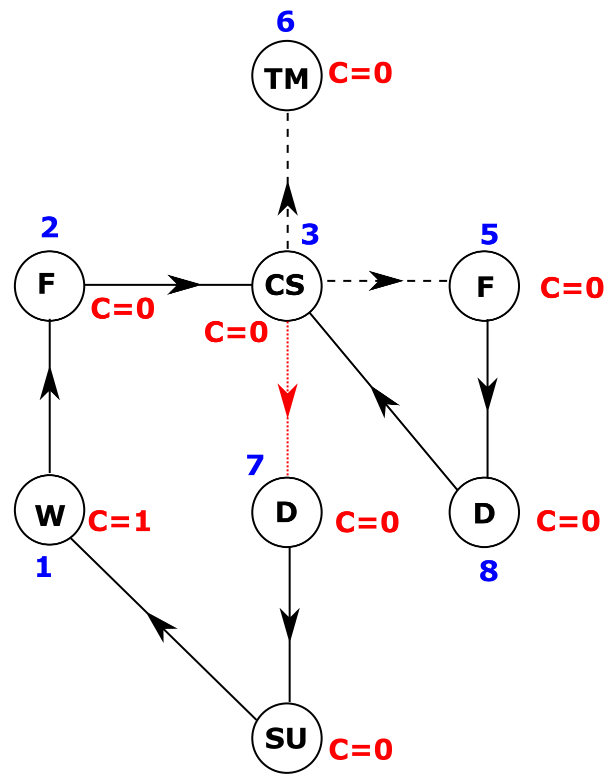


Fig. 10. Multi-state model for the Gas Turbine Generators (GT1 & GT2)

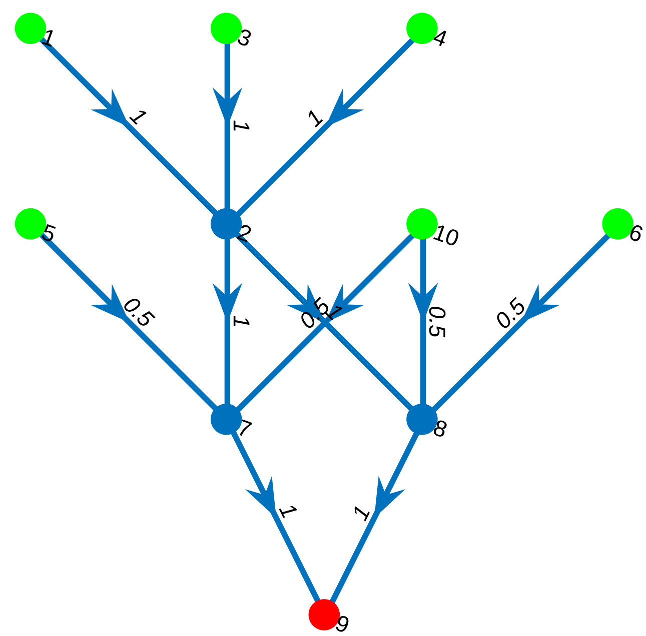


Fig. 11. Full system graph model showing maximum flow along links

power from the 345kV switchyard (via the black lines and the normally open breakers 17 & 03) or the 161kV switchyard (via the green lines and the normally open breakers 15 & 05). When these sources also become unavailable, DG-A and DG-B are automatically started and aligned. DG-5 is manually started and aligned by the plant operators on the failure of any of these. The manual start-up and alignment procedure of GT1 and GT2 is initiated when at least 2 out of the 3

TABLE I
HUMAN ERROR PROBABILITIES FOR GT1 & GT2

Time (h)	1	2	3	4	6	7	8	10
Probability	2.07×10^{-1}	2.07×10^{-2}	3×10^{-3}	3×10^{-4}	2×10^{-4}	1×10^{-4}	1×10^{-5}	1×10^{-5}

TABLE II
COMPONENT RELIABILITY DATA

Component	**Transition**	**Distribution**		U_{tm}	**CCF Parameters**	
		Type	**Parameters**		**Start-up Failure**	**Running Failure**
DG-A & DG-B	1-2	Weibull	(100,1.24)	0.009	$\{0.979, 0.021\}$	$\{0.972, 0.028\}$
	2-3	Lognormal	(6.42,2)			
	4-3	Lognormal	(5,1.2)			
GT1 &GT2	4-1	deterministic	0.5	0.0099	$\{0.959, 0.041\}$	$\{0.962, 0.038\}$
	4-2	Weibull	(200,1.5)			
	2-3	Lognormal	(5,2)			
	8-3	Lognormal	(7,1.8)			
	1-2	Weibull	(100,1.05)			
	7-4	Weibull	(0.2872,0.8194)			
	5-8	Weibull	(0.2872,0.8194)			
DG-5	1-2	Weibull	(100,1.24)			
	2-3	Lognormal	(6.42,2)			
	7-3	Lognormal	(5,1.2)			
	6-1	Weibull	(0.197,0.7467)			
	4-7	Weibull	(0.197,0.7467)			
Switchyard	4-1	Weibull	(0.197,0.7467)			
	2-1	See Fig. 13				
Grid	2-1	See Fig. 12				

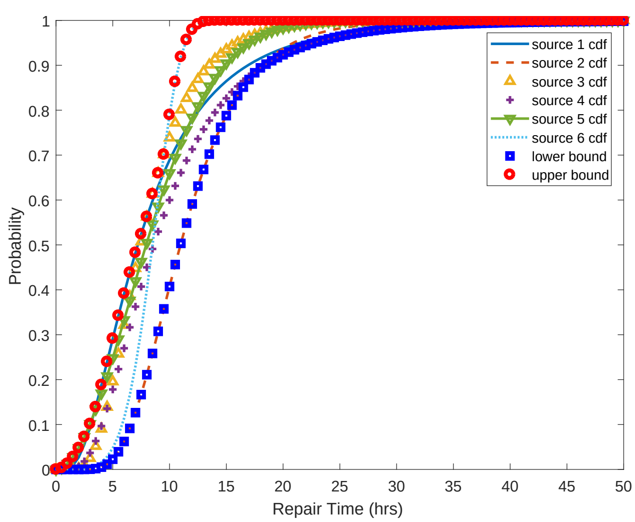


Fig. 12. Effective repair cdf for multiple grid sources

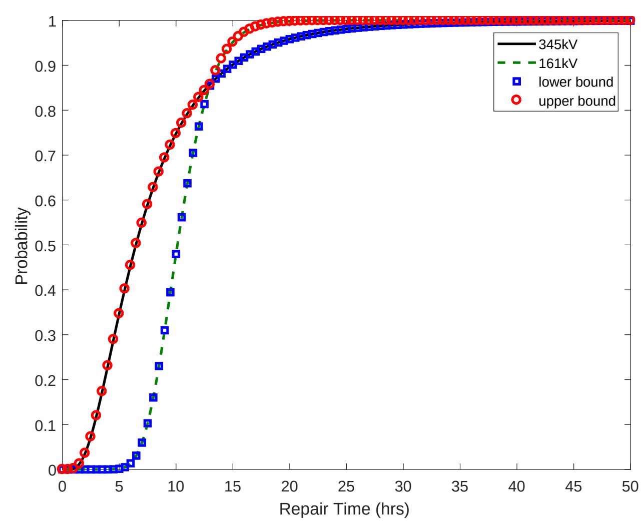


Fig. 13. Effective repair cdf for multiple switchyard nodes

Emergency Diesel Generators become unavailable. Following their successful start-up, the gas turbine generators take about 30 minutes to become fully functional.

A probabilistic assessment of the SBO risk of the plant due to grid and switchyard initiated LOOP is required.

A. *Developing the System and Component Models*

Fig. 7 is the simplified schematic 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 virtual output node, **t**, the total flow from the shared generator is accounted for. As shown, the six grid sources and the two switchyard sources have each been represented by single nodes, as proposed in Section II-B1.

Nodes 1, 7, 8, and 9 are modelled as proposed in Sections II-B and II-B1. The switchyard, on the other hand, is modelled according to Fig. 3, to account for human error during its start-up from shut down. Since DG-A (node 5) and DG-B (node 6) are automatically started following a LOOP, they are not susceptible to human error, and, therefore are modelled as shown in Fig. 8. DG-5, GT1, and GT2, however, require human intervention for their start-up and alignment. Node 10, therefore, is modelled according to Fig. 9 and nodes 3 and 4, according to Fig. 10.

TABLE III
COMMON-CAUSE GROUP DEFINITION

CCG	Description	Attributes	
		Designation	**Value**
1	Emergency Diesel Generator failure to start	$\boldsymbol{\rho}$	$\{5, 6\}$
		$\boldsymbol{\theta}$	$\{0.979, 0.021\}$
		β_1	4
		β_2	3
2	Emergency Diesel Generator failure to run	$\boldsymbol{\rho}$	$\{5, 6\}$
		$\boldsymbol{\theta}$	$\{0.972, 0.028\}$
		β_1	2
		β_2	1
3	Gas Turbine Generator failure to start	$\boldsymbol{\rho}$	$\{3, 4\}$
		$\boldsymbol{\theta}$	$\{0.959, 0.041\}$
		β_1	4
		β_2	3
4	Gas Turbine Generator failure to run	$\boldsymbol{\rho}$	$\{3, 4\}$
		$\boldsymbol{\theta}$	$\{0.962, 0.038\}$
		β_1	2
		β_2	$\{1, 4\}$

Justifying the values assigned to the state capacities of the generators, recall the system consists of 2 safety buses ($m = 2$) with each of DG-A and DG-B serving only one bus at a time ($n_1 = 1$). Since these generators can, however, fully meet the demand on the bus they serve ($u = 1$), they are assigned a capacity of 0.5 when working, as proposed in Section II-B. The Gas Turbine Generators, on the other hand, can fully serve both buses simultaneously ($n_1 = 2$), and therefore, have a capacity of 1 when working. From the multi-state models, the capacity vector for the main diesel generators, the shared diesel generator, and the gas turbine generators are $\{0.5, 0, 0, 0, 0\}$, $\{0.5, 0, 0, 0, 0, 0, 0\}$, and $\{1, 0, 0, 0, 0, 0, 0, 0\}$, respectively. Using these parameters in conjunction with Fig. 7, the adjacency matrix of the system is derived as;

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Given the adjacency matrix, the other parameters of the system flow equations are obtained as described in Section II-A, where $\mathbf{s} = \{1, 3, 4, 5, 6, 10\}$ and $\mathbf{t} = 9$. Fig. 11 is the system's graph model showing the maximum flow along each link, derived from the adjacency matrix and the maximum node capacities.

Component Reliability Data: Though realistic, the data used do not represent the actual data for the Maanshan plant. They were, however, assumed with the view to reflecting the reliability data used in Volumes 1 and 2 of the NUREG/CR-6890 report (see [1], [2]).

The repair times for the six grid sources are lognormally distributed with means and corresponding standard deviations defined by $\{8.99, 11.84, 8.24, 10.25, 9.61, 9.15\}$ 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 effective repair distributions for the grid and switchyard nodes are modelled according to the proposal in Section II-B1, as shown in Figs. 12 and 13, respectively.

All five standby generators are assumed to have a start-up failure probability of 1.756×10^{-2}. Also, the human errors associated with the failure to complete the start-up procedures for GT-5 and the switchyard are assumed equal but one-sixth of those for GT1 and GT2. Table I defines the probability of the operators not completing the start-up of the Gas Turbine Generators within selected times. Using the procedure proposed in Section II-B3, the parameters defining transitions $7 \rightarrow 4$ and $5 \rightarrow 8$ of the Gas Turbine Generators were obtained. The same procedure was used to obtain the parameters for transitions $6 \rightarrow 1$ and $4 \rightarrow 7$ of DG-5 and transition $4 \rightarrow 1$ of the switchyard. These and the parameters for the remaining transitions are presented in Table II. The column, U_{tm}, defines the unavailability due to test/maintenance of the generators. The CCF parameters are defined by a set in which each element represents the probability of a certain number of components being involved in any failure event initiated by the component. The number of components is determined by the index of the element in the set. For instance, from the Table, the probability that the start-up failure of any of the main diesel generators leads to the failure of the other generator is 0.021. This implies a total of two component failures, explaining why the probability value is the second element of the set (see Section II-C1 for details). Transition $4 \rightarrow 1$ of the Gas Turbine Generators depicts their start-up duration, which as we are told in Section IV, takes 30 minutes, explaining why it is assigned a deterministic 0.5 hours.

B. Representing Component Interdependencies

The first and easily recognizable form of interdependency in the system is CCF, where the failure of a generator could trigger the almost instantaneous failure of another generator. This type of interdependency is modelled according to the

CCF model presented in Section II-C1. DG-A and DG-B, as we know, are of the same design and model, different from the make of DG-5. Therefore, while the former are susceptible to CCF, DG-5 is immune. Similarly, GT1 and GT2 are susceptible to CCF, giving rise to four common-cause groups, as defined in Table III. The Table is developed from the CCF parameters in Table II in conjunction with the CCF model proposed in Section II-C1. CCG 1, for instance, represents the CCF due to the start-up failure of any of the main diesel generators. Since these generators are denoted as nodes 5 and 6 in the system, $\boldsymbol{\rho}$, the set of of components in the CCG is defined as $\{5, 6\}$. Now, as shown in Fig. 8, the start-up failure of DG-A or DG-B is denoted by state 4. Also, the other generator could only be affected by this event if it is in cold standby (state 3) at the time of occurrence. This explains why β_1 and β_2 are assigned the values, 4 and 3, respectively. The parameters for CCG 2 to 4 are derived in a similar fashion.

The other form of interdependency, like the grid failure necessitating the start-up of the standby generators or the failure of GT-5 forcing the start-up of the gas turbine generators, is a little more subtle and difficult to deduce. It requires a good knowledge of the operating principle of the system and cannot be modelled by the CCF model. For this, the cascading failure model proposed in Section II-C2 is invoked. To ensure the reproducibility of the case study, the step-by-step procedure for developing the dependency matrices, have been shown by recreating the sequence of events following a LOOP.

i. Let's assume the occurrence of the initiating event (LOOP), due to the failure of the grid (node 1). As already stated at the beginning of Section IV, the main diesel generators, A (node 5) and B (node 6), are restarted from cold standby. This is accounted for by the first 2 rows of the dependency matrix, $\mathbf{D}_1$. However, if the main generators are not in cold standby, maybe

$$\begin{gathered}\mathbf{D}_1 = \mathbf{D}_2 = \begin{pmatrix} 2 & 5 & 3 & 1 \\ 2 & 6 & 3 & 1 \\ 2 & 5 & -3 & -3 \\ 2 & 6 & -3 & -3 \end{pmatrix} \\ \mathbf{D}'_5 = \mathbf{D}'_6 = \begin{pmatrix} -3 & 10 & 3 & 6 \\ -3 & 10 & -3 & -3 \end{pmatrix} \\ \mathbf{D}'_{10} = \begin{pmatrix} -3 & 3 & 3 & 7 \\ -3 & 4 & 3 & 7 \end{pmatrix}\end{gathered} \tag{17}$$

due to test/maintenance or failure, the shared standby generator, DG-5 (node 10), is restarted. Recalling the concept of joint dependency discussed in Section II-C2, the joint dependency between the grid and DG-5 can be deduced. Here, the main generators are the intermediate nodes, since they dictate whether or not to start the shared generator. This behaviour is jointly represented by the last two rows of $\mathbf{D}_1$ and the first row of $\mathbf{D}'_5$ in (17). Again, if the shared generator too is unavailable (i.e., it is not in cold standby), the gas turbine generators, GT1 (node 3) and GT2 (node 4), are restarted (see Fig. 10). This attribute is jointly represented by $\mathbf{D}'_{10}$ and the last row of $\mathbf{D}'_5$. If, however, the gas turbine generators are not in cold standby on arrival of their start-up signal, no action is taken. This is due to the fact that the signal signifies the unavailability of all the standby sources at the plant. $\mathbf{D}'_5$ and $\mathbf{D}'_6$ are equal because nodes 5 and 6 produce the same effect on the shared generator when unavailable for start-up. Similarly, $\mathbf{D}_1$ and $\mathbf{D}_2$ are equal, as the response of the standby systems is the same for grid and switchyard failures.

$$\mathbf{D}_5 = \begin{pmatrix} 2 & 6 & 3 & 1 \\ 4 & 6 & 3 & 1 \\ 2 & 6 & -3 & -3 \\ 4 & 6 & -3 & -3 \end{pmatrix} \tag{18}$$

ii. DG-A (node 5) fails to start or starts but fails to run (see Fig. 2). The system will first check if DG-B (node 6) is available for start-up and initiate its start up, if available. This behaviour is defined by the first two rows of $\mathbf{D}_5$, as shown in (18). The effect of the unavailability of DG-B on arrival of its start-up signal has already been defined in scenario (i) (see the last row of $\mathbf{D}_1$). This representation is adapted to account for the case when DG-A fails to start or run and DG-B is unavailable for start-up, in the last two rows of $\mathbf{D}_5$ (see (18)).

$$\mathbf{D}_6 = \begin{pmatrix} 2 & 5 & 3 & 1 \\ 4 & 5 & 3 & 1 \\ 2 & 5 & -3 & -3 \\ 4 & 5 & -3 & -3 \end{pmatrix} \tag{19}$$

iii. Similarly, DG-B (node 6) fails to start or starts but fails to run (see Fig. 8). The system will first check if DG-A (node 5) is available, and initiate its start-up. The ensuing sequence of events is similar to that in scenario (ii). Hence, the dependency matrix is as obtained in (19).

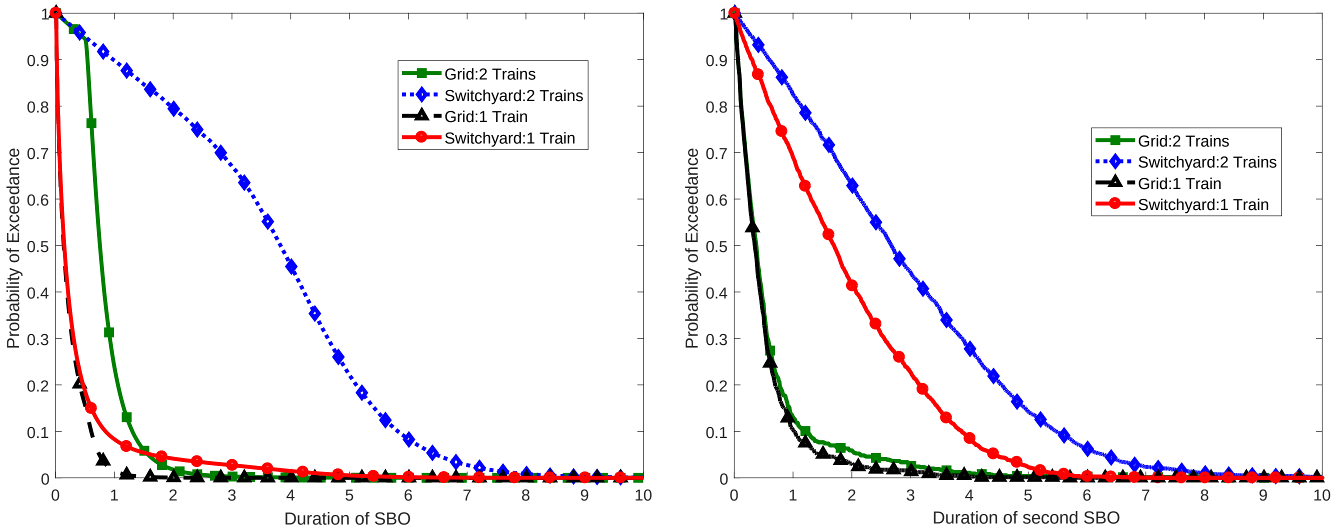
iv. DG-5 in cold standby fails to start or starts but fails to run (see Fig. 9). In this case, any repaired Emergency Diesel Generator is restarted first, otherwise, the Gas Turbine Generator are restarted. The ensuing possible sequence of events are already covered by scenarios (i)-(iii), and it is, therefore, recommended to not explicitly redefine these in $\mathbf{D}_{10}$, for simplicity. It is deducible that the failure of DG-5 induces the same response sequence as grid or switchyard failure. Therefore, recreating a LOOP event accounts for the failure of DG-5. Hence,

$$\mathbf{D}_{10} = \begin{pmatrix} 2 & 1 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 4 & 1 & 2 & 2 \\ 4 & 2 & 2 & 2 \end{pmatrix} \quad \mathbf{D}'_1 = \mathbf{D}_1 \quad \mathbf{D}'_2 = \mathbf{D}_2$$

v. GT1 (node 3) starts up successfully and enters the start-up state (see Fig. 10). Recall, states 7 and 8 account for the time taken by the operator to initiate the start-up of the generator. However, since both GT1 and GT2 (node 4) are in the same location, they are exposed to equal delays. Hence, the transitions, $7 \rightarrow 4$ and $5 \rightarrow 8$, of GT1 and GT2 are equal. To ensure the satisfaction of this constraint, when GT1 enters state 4, GT2 too is forced to state 4 if it is in state 7 or state 8, if it is in state 5. Similarly, when GT1 enters state 8, GT2 is forced to state 8 if it is in state 5 or state 4 if it is in state 7. This

TABLE IV
SUMMARY OF THE STATIC SBO INDICES OBTAINED

LOOP Type	p_1	f_s (per yr)	p_2	% of SBO at Start-Up	Simulation Samples
Grid	0.0033	6.18×10^{-3}	0.0022	29.23	1×10^8
Switchyard	0.0035	3.65×10^{-3}	0.0153	27.97	4.5×10^7



(a) First SBO (b) Second SBO

Fig. 14. Probability of SBO duration exceedance

behaviour is expressed by the first four rows of $\mathbf{D}_3$, as shown in (20).

vi. GT2 (node 4) starts up successfully and enters the start-up state (see Figure 10). This scenario has the same effect on GT1 (node 3) as scenario (v) has on GT2. Therefore, the ensuing sequence of events is accounted for by the first 4 rows of $\mathbf{D}_4$, as shown in (20).

$$\mathbf{D}_3 = \begin{pmatrix} 8 & 4 & 5 & 8 \\ 8 & 4 & 7 & 4 \\ 4 & 4 & 5 & 8 \\ 4 & 4 & 7 & 4 \\ 2 & 4 & 3 & 7 \\ 2 & 4 & 2 & 2 \\ 2 & 4 & 8 & 8 \\ 2 & 4 & 5 & 5 \\ 2 & 4 & 6 & 6 \end{pmatrix} \quad \mathbf{D}_4 = \begin{pmatrix} 8 & 3 & 5 & 8 \\ 8 & 3 & 7 & 4 \\ 4 & 3 & 5 & 8 \\ 4 & 3 & 7 & 4 \\ 2 & 3 & 3 & 7 \\ 2 & 3 & 2 & 2 \\ 2 & 3 & 8 & 8 \\ 2 & 3 & 5 & 5 \\ 2 & 3 & 6 & 6 \end{pmatrix}$$
$$\mathbf{D}'_3 = \mathbf{D}'_4 = \begin{pmatrix} 2 & 1 & 2 & 2 \\ 5 & 1 & 2 & 2 \\ 6 & 1 & 2 & 2 \\ 8 & 1 & 2 & 2 \end{pmatrix} \tag{20}$$

vii. GT1 fails to run. GT2 is restarted, if it is available for start-up, otherwise the system checks whether or not the failed diesel generators have been repaired. The first case is represented by the fifth row of $\mathbf{D}_3$, as shown in (20). The sequence of events involved in the second case is similar to the events following a LOOP. Therefore, a LOOP scenario is recreated, as shown in the last 4 rows of $\mathbf{D}_3$ and $\mathbf{D}'_4$. States 1, 4, and 7 have been left out of the possible GT2 states to necessitate the second case because, they mean either GT2 is already in operation (state 1), or on the verge of operation (states 4 and 7).

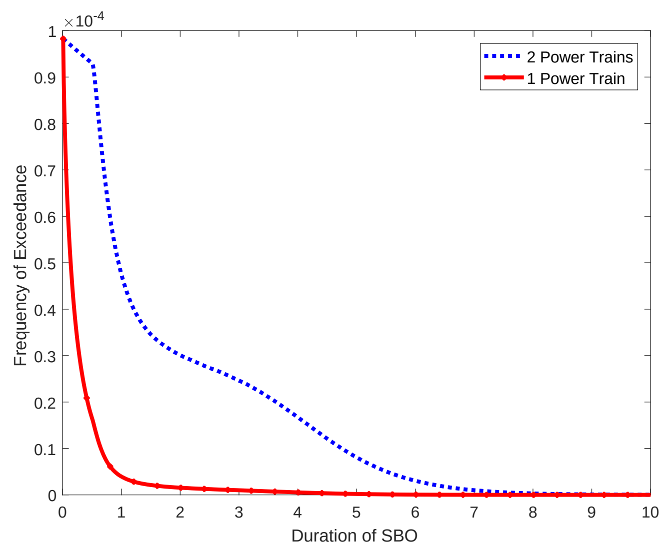


Fig. 15. Composite frequency of first SBO exceedance

viii. Similarly, GT2 failure to run produces the same effect on GT1 and the diesel generators, as in scenario (vii). The ensuing sequence of events is defined by $\mathbf{D}_4$ and $\mathbf{D}'_3$.

We have not considered the sequence of events following the failure of the Gas Turbine Generators to start because, being the last standby sources to be called into operation, their start-up failure means the unavailability of the other standby sources.

C. Results and Discussions

The proposed framework is implemented in the open source uncertainty quantification toolbox, OpenCOSSAN [27], [28] and used to quantify the SBO risk at the Maanshan nuclear power plant. For a grid and switchyard LOOP frequency of 1.86×10^{-2} and 1.04×10^{-2} per/year respectively, the case study was analysed on a 2.5GHz, E5-2670 v2 Intel ® Xeon ® CPU. A 5% coefficient of variation was imposed on the conditional probability of SBO as the simulation convergence criterion. The analysis took about 3 hours, and the results yielded are summarised in Table IV, Fig. 14, and Fig. 15. The probability of exceedance gives a measure of the likelihood of non-recovery from the SBO within a given time. The composite frequency of exceedance is the sum of the frequencies of exceedance yielded by the two LOOP categories.

As shown in Table IV, the probability of an SBO given a LOOP is almost the same for both LOOP categories. The slight difference is due to the fact that the Gas Turbine Generator are unusable during switchyard centred LOOP. Their effect, however, is prominent in mitigating the second SBO. The non-recovery probability from an SBO, as shown in Fig 14, is expressed as the non-recovery likelihood as a function of time and number of safety buses. The overall SBO risk at the plant is defined by the composite frequency of exceedance, as shown in Fig. 15.

As a way of verifying the convergence of the simulation, the product of p_1 and the fraction of SBO at start-up, should match the probability, p_0, of the emergency power system being unavailable at time 0. Bear in mind GT-5 and the Gas Turbine Generator have no influence on p_0, as a result of the delays characterising their start-up. Therefore, the emergency power system is unavailable at start-up only if DG-A (or DG-B) is unavailable due to test/maintenance and DG-B (or DG-A) fails to start or both are not in test/maintenance but fail to start. If U_{tm} is the unavailability due to test/maintenance of DG-A and DG-B and p_s, their start-up failure probability, p_0 is obtained as,

$$\begin{aligned} p_0 &= U_{tm}\left(p_s + p_s\right) + \left(1 - U_{tm}\right)p_s^2 \\ p_0 &= 2U_{tm}p_s + \left(1 - U_{tm}\right)p_s^2 \end{aligned} \tag{21}$$

Substituting the required values in (21), an error of 3.17% is realised for grid LOOP and 4.7%, for switchyard LOOP. Since the error in each case is not in excess of 5%, the convergence of the simulation is verified.

Ensuring an enhanced risk insight, the system was re-analysed for three additional scenarios as follows;

- Case 2: No delays in the start-up of DG-5. This implies, the effects of human error are removed.
- Case 3: Gas Turbine Generator start-up is simultaneous with DG-A and DG-B. The generators, however, are kept in warm standby after start-up.
- Case 4: A combination of Case 2 and Case 3.

Case 1 represents the scenario already analysed, and the results for the four cases are summarised in Figs. 16 to 18 (please note the composite frequencies in Figs. 16 (a) and (b) are expressed on a log-scale). We have used absolute, instead of conditional probabilities in Fig. 18, to ensure uniformity.

The following risk insights are inferred by the outcome of the case study;

i. As shown in Fig. 14 that, station blackouts induced by switchyard failures are more difficult to recover from and, therefore, contribute more to the overall SBO risk at the plant. In this light, feasible reliability improvement programs should be designed to ensure the high reliability of the switchyard. Such a reliability program should be complemented by an efficient repair policy to keep the non-recovery probability low.

ii. The gas turbine generators are the only difference between the recovery durations of grid and switchyard LOOP. These generators, therefore, are very instrumental to mitigating SBO risks at the plant, and their availability should be kept high.

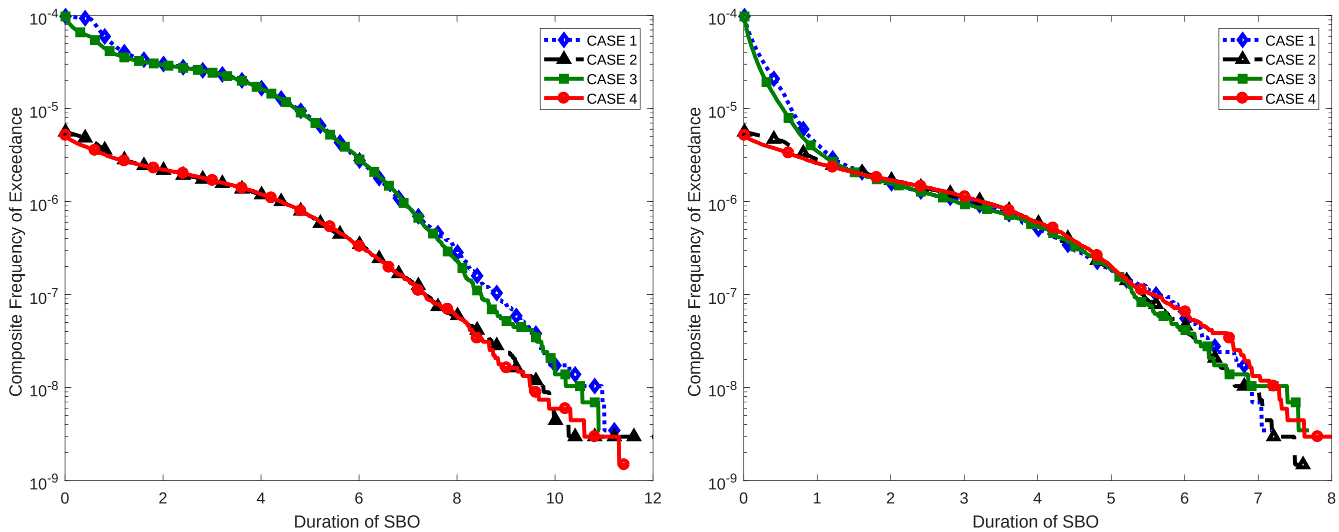
iii. Automating the start-up of DG-5 and initiating the start-up of the Gas Turbine Generator just after LOOP guarantees an improved resilience to SBO, as endorsed by Figs. 16 to 18. However, starting the Gas Turbine Generator simultaneously with the Emergency Diesel Generator brings with it additional costs, borne from fuel consumption and maintenance. This decision, therefore, should be preceded by a robust cost-benefit analysis. In fact, under economic constraints, it is prudent to automate the start-up of DG-5 only, as the difference between the outcomes yielded by Case 2 and Case 4 is only just slight.

In this case study, we have ignored the explicit sensitivity and importance analyses of the individual components, since these quantities can be achieved even with the existing techniques.

V. Conclusions

Station blackout accidents, though a rare occurrence, can have devastating consequences on a nuclear power plant's ability to achieve and maintain safe shut down. Consequently, the plant's capability to cope and recover from such occurrences makes a key input to its probabilistic risk assessment model.

In this paper, we have proposed an intuitive simulation framework to model a nuclear power plant's recovery from station blackout accidents. The framework provides a simple means of defining the complex interdependencies that often characterise the operation of practical engineering systems, and therefore, applicable without unrealistic assumptions. This attribute, coupled with its ability to intuitively tolerate the multi-state behaviour of the system's building block, distinguishes it from the existing approaches. Its applicability has been demonstrated by modelling the SBO recovery of a pressurised water reactor, providing an informed insight into its SBO risks. The proposed approach was able to fully model the dynamic behaviour of the power system and provide valuable insights on the SBO risk at the plant. The non-recovery probability curve obtained, for instance, can be absorbed into the existing probabilistic risk assessment models, getting rid of laborious fault trees. Since this curve also depicts the unavailability of AC power, it can be directly compared with the reliability of the plant's SBO coping mechanism,



(a) Composite frequencies of exceedance when a minimum of two power trains are required for power recovery

(b) Composite frequencies of exceedance when one power train is sufficient for power recovery

Fig. 16. Comparison of composite frequencies of exceedance

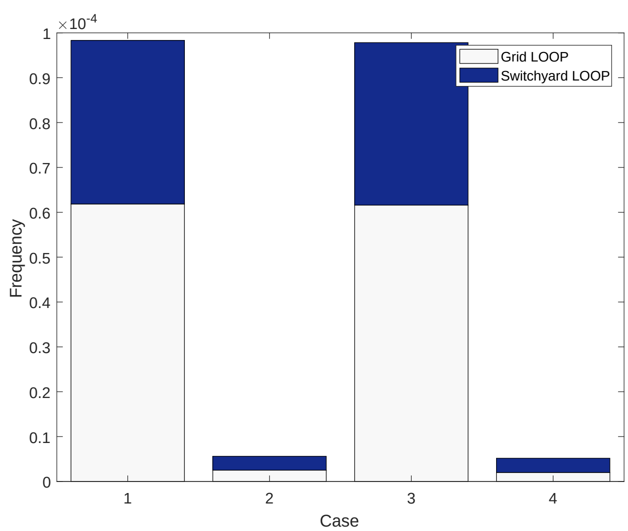


Fig. 17. Comparison of SBO frequencies

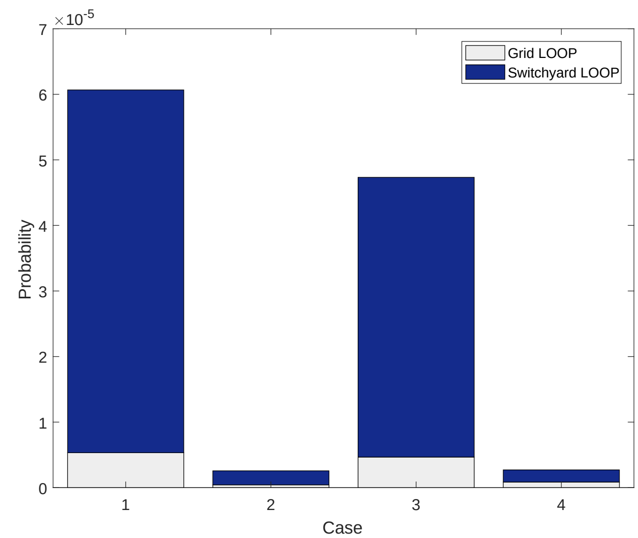


Fig. 18. Comparison of second SBO probabilities

providing an easier means of determining the need for their reliability improvement. It also helps ascertain the adequacy of the plant's station blackout recovery capability, without revisiting the entire model. A key desirable feature of the proposed framework is its wide applicability, even to non-nuclear applications.

In spite of their well documented limitations relative to the proposed framework, the existing static fault tree-based models still possess desirable attributes that give them an edge in importance, sensitivity, and uncertainty analyses. With this in mind, the proposed framework has been developed with the view to complementing their applicability, instead of serving as an explicit replacement. We have, therefore, included a clear description of how its output can be incorporated into these models. The framework, in addition, has been implemented in the open-source uncertainty quantification toolbox developed at the Institute for Risk and Uncertainty (see [27], [28]), thereby rendering it readily available.

The multi-state model and dependency matrices proposed, create the foundation for the incorporation of additional dynamic considerations. Such considerations as the optimal number of maintenance teams on-site, Emergency Diesel Generator failure during cold standby, optimal inspection interval, and the availability of spares, are a possibility. Efforts are underway to extend the framework to these considerations, other LOOP categories, and incorporate epistemic uncertainties.

ACKNOWLEDGEMENT

The authors would like to acknowledge the gracious support of this work through the EPSRC and ESRC Centre for Doc-

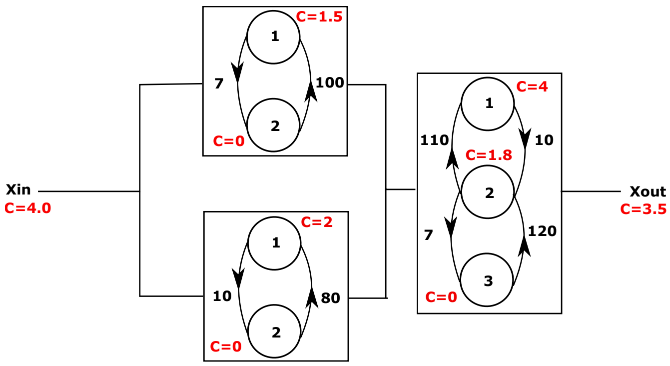


Fig. 19. Structure of a 3-component pipe network

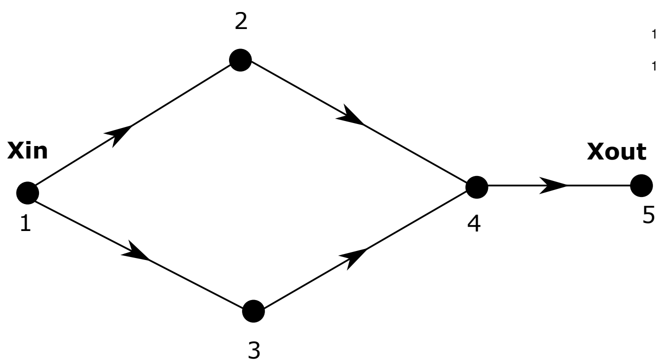


Fig. 20. Network model of pipe network

toral Training on Quantification and Management of Risk & Uncertainty in Complex Systems & Environments. We also are grateful to Dr Shih-Kuei Chen and team, of the National Tsing Hua University in Taiwan, for their invaluable contribution.

APPENDIX

This Section is introduced with the view to providing a detailed example of how the linear programming problem is formulated, stating the exact values of the relevant parameters. The goal is to enable readers to grasp, fully, the concept proposed in this paper, as well as provide a benchmark for validating their implementation of this concept.

Consider the 3-component pipeline shown in Fig. 19, adapted from [22]. A maximum of 4 tons of oil could be pumped from the source, X_{in}, to the output, X_{out}, where the demand is fixed at 3.5 tons. The state-space of each of the other components is shown, with the number beside each state denoting the capacity of the component in that state. The equivalent graph model of the system is shown in Fig. 20. Notice the two extra nodes, 1 and 5, representing the source and output, respectively. The available information is sufficient to formulate the linear programming problem and derive its parameters. The first step is to define the adjacency matrix, since all the other parameters depend on it. From Fig. 20, the adjacency matrix, **A**, is obtained as;

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The next task is to deduce the edge and incidence matrices, **e** and **Γ**, respectively. They are obtained thus,

$$\mathbf{e} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \\ 2 & 4 \\ 3 & 4 \\ 4 & 5 \end{pmatrix} \qquad \mathbf{\Gamma} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

With **A**, **e**, and **Γ** known, the linear programming problem is formulated as follows,

1) At time 0, all the components are in their best performance state. The inequality constraint, therefore, is expressed as,

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X_{12} \\ X_{13} \\ X_{24} \\ X_{34} \\ X_{45} \end{pmatrix} \leq \begin{pmatrix} 4.0 \\ 1.5 \\ 2 \\ 4 \\ 3.5 \end{pmatrix}$$

2) The equality constraint is expressed as,

$$\begin{pmatrix} -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} X_{12} \\ X_{13} \\ X_{24} \\ X_{34} \\ X_{45} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

3) The bounds on the flow through the edges are,

$$\mathbf{lb} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \mathbf{ub} = \begin{pmatrix} 1.5 \\ 2 \\ 1.5 \\ 2 \\ 3.5 \end{pmatrix}$$

4) The objective function is expressed as,

$$\mathbf{\Psi} = \begin{pmatrix} -1 & -1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} X_{12} \\ X_{13} \\ X_{24} \\ X_{34} \\ X_{45} \end{pmatrix}$$

REFERENCES

[1] S. A. Eide, C. D. Gentillon, T. E. Wierman, and D. M. Rasmuson, "Reevaluation of station blackout risk at nuclear power plants," U.S. Nuclear Regulatory Commission, Tech. Rep. NUREG/CR-6890 Vol. 2, 2005. [Online]. Available: https://www.nrc.gov/docs/ML0602/ML060200479.pdf

[2] ——, "Reevaluation of station blackout risk at nuclear power plants," U.S. Nuclear Regulatory Commission, Tech. Rep. NUREG/CR-6890 Vol. 1, 2005. [Online]. Available: https://www.nrc.gov/docs/ML0602/ML060200477.pdf

[3] M. Čepin, *Assessment of Power System Reliability: Methods and Applications*. London: Springer London, 2011, ch. Event Tree Analysis, pp. 89–99.

[4] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, "Fault tree handbook," U.S. Nuclear Regulatory Commission, Tech. Rep. NUREG/CR-0492, 1981. [Online]. Available: https://www.nrc.gov/docs/ML1007/ML100780465.pdf

[5] M. Čepin, *Assessment of Power System Reliability: Methods and Applications*. London: Springer London, 2011, ch. Fault Tree Analysis, pp. 61–87.

[6] E. Ruijters and M. Stoelinga, "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools," *Computer Science Review*, vol. 15, pp. 29 – 62, 2015.

[7] W. E. Vesely, M. Stamatelatos, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, "Fault tree handbook with aerospace applications," NASA Office of Safety and Mission Assurance, Tech. Rep. Version 1.1, 2002. [Online]. Available: https://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf

[8] F. I. Khan and S. Abbasi, "Analytical simulation and {PROFAT} ii: a new methodology and a computer automated tool for fault tree analysis in chemical process industries," *Journal of Hazardous Materials*, vol. 75, no. 1, pp. 1 – 27, 2000.

[9] S. K. Shin and P. H. Seong, "Review of various dynamic modeling methods and development of an intuitive modeling method for dynamic systems," *Nuclear Engineering and Technology*, vol. 40, no. 5, pp. 375–386, 2008.

[10] B. Kaiser, C. Gramlich, and M. Förster, "State/event fault trees: A safety analysis model for software-controlled systems," *Reliability Engineering & System Safety*, vol. 92, no. 11, pp. 1521 – 1537, 2007.

[11] Z. Zhou and Q. Zhang, "Model event/fault trees with dynamic uncertain causality graph for better probabilistic safety assessment," *IEEE Transactions on Reliability*, vol. PP, no. 99, pp. 1–11, 2017.

[12] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, "Improving the analysis of dependable systems by mapping fault trees into bayesian networks," *Reliability Engineering & System Safety*, vol. 71, no. 3, pp. 249 – 260, 2001.

[13] M. Čepin and B. Mavko, "A dynamic fault tree," *Reliability Engineering & System Safety*, vol. 75, no. 1, pp. 83 – 91, 2002.

[14] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," *IEEE Transactions on Reliability*, vol. 41, no. 3, pp. 363–377, Sep 1992.

[15] ——, "Fault trees and markov models for reliability analysis of fault-tolerant digital systems," *Reliability Engineering & System Safety*, vol. 39, no. 3, pp. 291 – 307, 1993.

[16] K. D. Rao, V. Gopika, V. S. Rao, H. Kushwaha, A. Verma, and A. Srividya, "Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment," *Reliability Engineering & System Safety*, vol. 94, no. 4, pp. 872 – 883, 2009.

[17] L. Meshkat, J. B. Dugan, and J. D. Andrews, "Dependability analysis of systems with on-demand and active failure modes, using dynamic fault trees," *IEEE Transactions on Reliability*, vol. 51, no. 2, pp. 240–251, Jun 2002.

[18] J. B. Dugan, K. J. Sullivan, and D. Coppit, "Developing a low-cost high-quality software tool for dynamic fault-tree analysis," *IEEE Transactions on Reliability*, vol. 49, no. 1, pp. 49–59, Mar 2000.

[19] C. Y. Huang and Y. R. Chang, "An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees," *Reliability Engineering & System Safety*, vol. 92, no. 10, pp. 1403 – 1412, 2007.

[20] L. F. Rocha, C. L. T. Borges, and G. N. Taranto, "Reliability evaluation of active distribution networks including islanding dynamics," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1545–1552, March 2017.

[21] H. Lei and C. Singh, "Non-sequential monte carlo simulation for cyber-induced dependent failures in composite power system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1064–1072, March 2017.

[22] 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*, vol. 152, pp. 351 – 367, 2016.

[23] ——, "Maintenance strategy optimization for complex power systems susceptible to maintenance delays and operational dynamics," *IEEE Transactions on Reliability*, vol. PP, no. 99, pp. 1–22, 2017.

[24] H. George-Williams, M. Lee, and E. Patelli, "A framework for power recovery probability quantification in nuclear power plant station black-out sequences," in *Proceedings of the Probabilistic Safety Assessment and Management Conference*, vol. 13, 2016.

[25] A. Mosleh, D. M. Rasmuson, and F. M. Marshall, "Guidelines on modeling Commom-Cause Failures in probabilistic risk assessment," U.S. Nuclear Regulatory Commission, Tech. Rep. NUREG/CR-5485, 1998.

[26] H. George-Williams and E. Patelli, "Efficient availability assessment of reconfigurable multi-state systems with interdependencies," *Reliability Engineering and System Safety*, vol. 15, pp. 431–444, 2017.

[27] E. Patelli, M. Broggi, M. D. Angelis, and M. Beer, "Opencossan: An efficient open tool for dealing with epistemic and aleatory uncertainties," in *Vulnerability, Uncertainty, and Risk: Quantification, Mitigation, and Management - Proceedings of the 2nd International Conference on Vulnerability and Risk Analysis and Management, ICVRAM 2014 and the 6th International Symposium on Uncertainty Modeling and Analysis, ISUMA 2014*, 2014, pp. 2564 – 2573. [Online]. Available: http://dx.doi.org/10.1061/9780784413609.258

[28] E. Patelli, *Handbook of Uncertainty Quantification*. Springer International Publishing, 2017, ch. COSSAN: A Multidisciplinary Software Suite for Uncertainty Quantification and Risk Management, pp. 1–69.

Hindolo George-Williams received the B.Eng.(Hons.) degree in electrical/electronic engineering from the University of Sierra Leone, Freetown, Sierra Leone, in 2010, and the M.Sc.(Eng.) degree in energy generation from the University of Liverpool, Liverpool, U.K., in 2013. He is currently working toward the dual Ph.D. degree with the University of Liverpool and the National Tsing Hua University, Hsinchu, Taiwan. His Ph.D. research focuses on the probabilistic risk assessment of nuclear power plants.

Mr. George-Williams received the Best Project Award from the Sierra Leone Institute of Engineers in recognition of his outstanding execution of his final B.Eng. project. He also worked as a Maintenance Engineer (for a period of 30 months) for the Sierra Leone affiliate of the French oil giant, TOTAL.

Min Lee is a Distinguished Professor at the Department of Engineering and System Science (ESS) of National Tsing Hua University (NTHU), Hsinchu, Taiwan. He graduated from the Department of Nuclear Engineering of NTHU with a bachelor and master's degree in 1977 and 1979, respectively. He received his PhD in Nuclear Engineering from the Massachusetts Institute of Technology in 1985. He briefly worked at the Brookhaven National Laboratory after his PhD and joined the Department of Engineering and System Science of NTHU in 1989.

His research fields are probabilistic risk assessment of nuclear power plants, Light Water Reactor severe accident phenomenology and management, source term characterization of nuclear power plants, heat transfer, and system thermal-hydraulic analyses of Light Water Reactors.

Dr Lee has held several administrative positions at NTHU, including Chairman of ESS Department, Vice President and Chief of Staff, Vice President of General Affairs, and Vice President of Student Affairs. Dr Lee has also been on the board of directors of the Taiwan Power Company (a government-owned public utility) for 14 years and a member of the Nuclear Safety Committee of the same company for 12 years.

Edoardo Patelli is a member of the Institute for Risk and Uncertainty at the University of Liverpool, UK and a honorary member of the National Tsing Hua University, Taiwan. He is a Nuclear Engineering graduate from the Politecnico di Milano (Italy) and carried out his doctoral work in Radiation Science and Technology at the same Institute in the group of Professor Marzio Marseguerra and Enrico Zio. He then moved as a research associate to the University of Innsbruck (Austria) in the group of Professor Schuëller. Dr Patelli is co-Principal investigator of the Centre for Doctoral Training in Quantification and Management of Risk & Uncertainty in Complex Systems & Environments and a member of the Centre for Doctoral Training in "Next-Generation-Nuclear". Dr. Edoardo has published more than 200 contributions in international journals and proceedings of international conferences. He has supervised more than 20 PhD students on site and in collaboration with international partners. He is the Chair of the Technical Committee on Simulation for Safety and Reliability Analysis (ESRA - European Safety and Reliability Association) a guest-editor of international journals (e.g., the International Journal of Reliability & Safety and Structural Safety) and editorship of Springer's Encyclopaedia of Earthquake Engineering. He has also organised multi-disciplinary international conferences on risk and vulnerability (e.g., ASCE-ICVRAM-ISUMA 2014, IPW2015) and a number of Mini-symposia in different international conferences.