Chapter 7
Simulation Methods for the Analysis of Complex Systems

Hindolo George-Williams, T. V. Santhosh, and Edoardo Patelli

Abstract Everyday systems like communication, transportation, energy and industrial systems are an indispensable part of our daily lives. Several methods have been developed for their reliability assessment—while analytical methods are computationally more efficient and often yield exact solutions, they are unable to account for the structural and functional complexities of these systems. These complexities often require the analyst to make unrealistic assumptions, sometimes at the expense of accuracy. Simulation-based methods, on the other hand, can account for these realistic operational attributes but are computationally intensive and usually system-specific. This chapter introduces two novel simulation methods: **load flow simulation** and **survival signature simulation** which together address the limitations of the existing analytical and simulation methods for the reliability analysis of large systems.

7.1 Introduction

A system is classed as complex from one of two fronts—in terms of the functional relationships between its components and in terms of its structure. A structurally complex system does not conform to a series, parallel, or series-parallel configuration. Most real-world systems are composed of components that can operate at multiple

H. George-Williams
Institute of Energy and Sustainable Development, School of Engineering and Sustainable Development, De Montfort University, Oxford, United Kingdom
e-mail: hindolo.george-williams@dmu.ac.uk

T. V. Santhosh
Institute for Risk and Uncertainty, University of Liverpool, Liverpool, United Kingdom
e-mail: s.santhosh@liverpool.ac.uk

Bhabha Atomic Research Centre, Mumbai, India

E. Patelli (✉)
Centre for Intelligent Infrastructure, Civil and Environmental Engineering, University of Strathclyde, Glasgow, United Kingdom
e-mail: edoardo.patelli@strath.ac.uk

L. Aslett et al. (eds.), *Uncertainty in Engineering*,
SpringerBriefs in Statistics,
https://doi.org/10.1007/978-3-030-83640-5_7

performance levels or states and components with a functional coupling with other components. Such systems are deemed functionally complex, since their states cannot be directly deduced from their traditional two-state structure functions. They are characterised by multiple states, with the number of states determined by the diversity in the states of their components, structure and the functional relationships between their components [21]. In these systems, the number of performance levels may or may not be finite, depending on the performance measure under consideration and the type of system [21]. For instance, the power generated by a power plant may take any value between zero and its maximum achievable value, depending on the performance levels of its component and the demand on the grid. Complex systems may be standalone or form an indispensable part of some critical system like healthcare, safety-critical and industrial control systems. It is, therefore, important to be able to assess their susceptibility to failures, as well as quantify and predict the ensuing consequences, for effective planning of restoration and mitigation measures.

7.2 Reliability Modelling of Systems and Networks

In system reliability evaluation, the analyst has numerous techniques at their disposal, which can be classified as heuristic-, analytical- or simulation-based [1] and further as static or dynamic. In particular, dynamic techniques not only model the system based on the functional and structural relationships between its components, but also support dynamic relationships like inter-component and inter-system dependencies.

7.2.1 Traditional Approaches

Reliability Block Diagrams and **Fault Trees** have been extensively used in the reliability evaluation of binary-state systems. Both techniques have proven particularly useful for moderately sized systems with series-parallel configurations. However, they become difficult to apply with large or complex systems and often require additional techniques to decompose the system. The Reliability Graph [40] was, therefore, developed to overcome this difficulty and proved very efficient in modelling structural complexities. Reliability block diagrams, fault trees and reliability graphs, however, assume components to be statistically independent, which renders them inadequate for systems susceptible to restrictive maintenance policies and inter-component dependencies. However, techniques including but not limited to dynamic reliability block diagrams [10], dynamic fault trees [6], condition-based fault trees [35], dynamic flow graphs [2], Petri Nets [26] and other combinatorial techniques [38] have been developed to model these dynamic relationships. They have found application in a wide range of reliability engineering problems, including repairable systems with restrictive maintenance policies.

Though the earliest forms of these techniques including binary decision diagrams were applicable only to binary-state systems, numerous instances of their recent extension to multi-state systems exist, see, e.g. [39]. However, these extensions either *require state enumeration or the derivation of the minimal path or cut sets of the system, which is an NP-hard problem* [41].

The **extended block diagram technique** and **graph-based algorithms** share two common limitations. First, they define reliability with respect to the maximum flow through the system. Therefore, they are limited to systems with single output nodes and those with multiple output nodes where only the presence of flow at these nodes is relevant and not the relative magnitude of the flow. The second limitation arises from the assumption that there are no flow losses in the system, making them inapplicable to certain practical systems like energy systems and pipe networks, susceptible to losses in some failure modes. More recently, various researchers have made invaluable contributions to multi-state system reliability analysis, developing techniques applicable to a wide range of systems [22]. These techniques have mainly been based on either the structure function approach, stochastic process, simulation or the Universal Generating Function approach [21, 25].

The most popular stochastic process employed in system reliability analysis is the **Markov Chain (MC)**, which involves enumerating all the possible states of the system and evaluating the associated state probabilities [25]. This technique is only easily applicable to exponential transitions or distributions with simple cumulative distribution functions, requires complicated mathematics and becomes complex for large systems. For an M component binary-state system, the number of states in the model ranges from $M + 1$ for series systems, to 2^M for parallel systems. For large multi-state systems, the number of states increases exponentially, rendering the model difficult to construct and expensive to compute.

The **Universal Generating Function** was introduced to address the state explosion problem of the MC. It allows the algebraic derivation of a system's performance from the performance distribution of its components [21, 24]. However, both the Universal Generating Function and Markov Chain are limited in the number of reliability indices they can quantify. Also, like all multi-state system reliability evaluation techniques, they are maximum-flow-based and assume flow conservation across components. The Universal Generating Function, though straightforward for series/parallel systems, it requires a substantial effort for complex topologies.

Simulation methods are the most suitable for multi-state system reliability and performance evaluation, since they mimic the actual operation of systems. Their advantage over their analytical counterpart is due to the fact that they support any transition distribution, allow the effects of external factors on system performance to be investigated [43] and are easily integrated with other methods [36]. In particular, they allow the explicit consideration of the effects of uncertainty and imprecision on the system, providing a powerful tool for risk analysis and by extension, rational decision-making under uncertainty. They are, therefore, mostly used to analyse systems for which analytical approaches are inadequate. However, even some of the existing simulation methods [23, 43] require prior knowledge of the system's path set, cut set or structure function and are mostly limited to binary-state systems [42].

7.2.2 Interdependencies in Complex Systems

Engineers and system designers are under immense pressure to build systems robust and adequate enough to meet the ever-increasing human demand and expectation. Unavoidably, the resulting systems are complex and highly interconnected, which ironically constitute a threat to their resilience and sustainability [18]. Two systems are *interdependent* if at least a pair of components (one from each system) are coupled by some phenomena, such that a malfunction of one affects the other. In such systems, an undesirable glitch in one system could cascade and cause disruptions in the coupled system. The cascade could be fed back into the initiating system and the overall consequences may be catastrophic [5]. To minimise the effects of failures, some interdependent systems are equipped with *reconfiguration* provisions. This normally entails transferring operation to another component, rerouting flow through alternative paths, or shutting down parts of the system.

The achievement of maximum overall system performance is, in general, desirable. However, in many applications (nuclear power plants, for instance), it is more important to guarantee system availability and recovery in the shortest possible time, following component failure [16]. *Interdependencies* are manifested in engineering systems at two levels: between components (*inter-component*), which can be functional or induced and between systems/subsystems (*inter-system*) [15].

Functional dependencies are due to the topological and/or functional relationships between components. Induced dependencies, on the other hand, are due to a state change in one component (the initiator) triggering a corresponding state change in another (the induced), such that even when the initiator is reinstated, the induced does not reinstate, unless manually made to do so. Functional dependencies in standalone systems are intrinsically accounted for by the innate attributes of the system reliability modelling and evaluation technique while induced dependencies require explicit modelling. Inter-system dependencies, on the other hand, are due to functional or induced couplings between multiple systems. The functional dependencies in these systems, however, may require explicit modelling. This is the case for components relying on material generated by another system. For instance, an electric pump in a water distribution system relies on the availability of the electricity network.

Induced dependencies are further divided into *Common-Cause Failures* (CCF) [27] and cascading events, as summarised in Fig. 7.1. Common-cause failures are the simultaneous failure of multiple similar components due to the same root cause. Their origin is traceable to a coupling that normally is external to the system. Notable instances are shared manufacturing lines, shared maintenance teams, shared environments and human error. A group of components susceptible to the same CCF event is called a Common-Cause Group (CCG). An important point to note about common-cause failures is that, on occurrence of the failure event, there is a probability associated with multiple component failure and that the affected components fail in the same mode. Consequently, the number of components involved in the event ranges from 1 to the total number of components in the CCG. CCF events may affect an entire system or only a few of its components and, therefore, pose a consider-

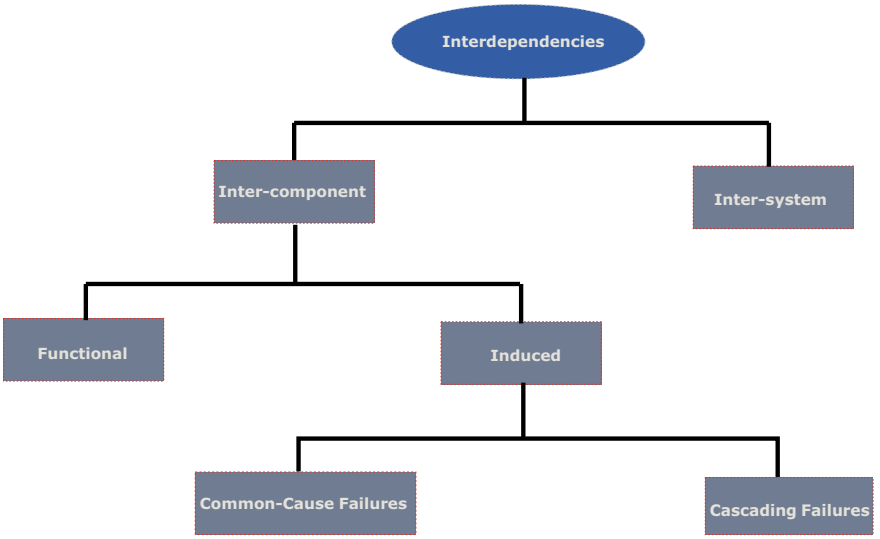

Fig. 7.1 Types of interdependencies in complex systems. Functional dependencies—such as when the failure of power supply forces the unavailability of connected components. Common-Cause Failures—due to earthquake excitation, vibration, environmental conditions (temperature, humidity, contaminants), shared maintenance. Cascading events such as the failure of one component might overload other components

able threat to the reliability of systems. CCF modelling and quantification attracts keen interest from system reliability and safety researchers, as well as practitioners. Examples of the work that has been done in this field can be found in [28, 33, 37]. Most of the methods presented in these publications, however, are built on reliability evaluation techniques that do not segregate the topological from the probabilistic attributes of the system. As such, they are computationally expensive for problems involving multiple reliability analysis of the same system. They also have yet to be applied to multi-state systems, as well as systems susceptible to both cascading and common-cause failures.

Cascading failures are those with the capacity to trigger the instantaneous failure of one or more components of a system. They can originate from a component or from a phenomenon outside the system boundary. The likelihood of the initiating event originating from within the system distinguishes them from CCF. Another point of dichotomy is that the affected components do not necessarily have to be similar or fail in the same mode. In addition, at the occurrence of the initiating event, the probability of all the coupled components failing is unity, same for the case when they are in a state rendering them immune [15, 18]. A few prominent examples of initiating events external to the system are extreme environmental events, natural disasters, external shocks, erroneous human-system interactions and terrorist acts. Various models have been developed to study the effects of cascading failures on complex systems [29]. However, a good number of these models only assess their response

to targeted attacks, variation in some coupling factor or the relative importance of system components. When faced with the additional situation of random component failures, a complete reliability and availability analysis should be performed [18]. Even methods that fulfill this requirement have their applicability hampered by components that undergo non-Markovian transitions, components susceptible to delayed transitions, and reconfigurable systems.

7.3 Load Flow Simulation

The load flow simulation is a recently proposed technique for the reliability and performance analysis of multi-state systems [17]. It is based on the fact that if the performance levels of a system's components are known, the performance levels of the system can be directly derived from its network model. In this formalism, each component is modelled as a semi-Markov stochastic process and the system as a directed graph whose nodes are the components of the system. The approach is intuitive and applicable to any system architecture and easily programmable on a computer. It outperforms other multi-state system reliability analysis approaches, since it does not require state enumeration or cut set definition. Efficient algorithms for manipulating the adjacency matrix of this directed graph to obtain the flow equations of the system are available in OpenCossan [31].

The operation of the system is simulated using Kinetic Monte Carlo method by initially sampling the state and time to the next transition (hereafter referred to as transition parameters) of each component. The simulation jumps to the smallest sampled transition time t_{min}, at which time the states of the components undergoing the transition are updated. Using the updated performance levels of the components of the system, the virtual flow across the system is computed via a linear programming procedure that employs the interior-point algorithm. The new transition parameters of the components undergoing a transition are then sampled and the simulation jumps to the next smallest transition time. This cycle of component transition parameter sampling, transition forcing and system performance computing continues until the mission time T is reached. The system performance computed at every component transition is captured and saved in counters, from which the performance indices of the system can be deduced. A component shutdown and restart procedure is incorporated to replicate the actual operating principles of most practical systems. In this procedure, the availability of each system component is tested against its predefined reference minimum input load level at every transition and the effects of functional interdependence on the failure probability of the components are accounted for. Figure 7.2 provides a high-level illustration of the load flow simulation procedure.

Ageing and component performance degradation is common in most systems. For such systems, techniques built around the flow conservation principle become obsolete, as the flow generated by sources can be dissipated in intermediate components in certain failure modes. For instance, consider a 100 MW power generator supplying a 95 MW load through a 125 MW transformer. If there are no power losses

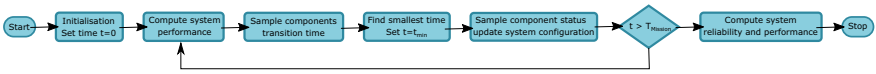

Fig. 7.2 Flowchart of the load flow simulation

in the transformer, 95 MW will be drawn from the generator and delivered to the load. However, if the efficiency of the transformer deteriorates to say 75%, it now takes all 100 MW from the generator but delivers only 75 MW to the load. In both cases, the apparent difference between the generation capacity and demand is the same but the power drawn from the generator increases while the effective power supplied to the load deteriorates. For this example, the demand would have to be slashed to 75 MW or less, to preserve the operational integrity of the generator. Other scenarios where component inefficiency affects system reliability are: a power transmission line prone to losses and an oil pipeline where a failure mode is a hole in a pipe or gasket failure at some flange [17].

The load flow simulation approach has been successfully applied to the availability assessment of a reconfigurable offshore installation [18], dynamic maintenance strategy optimization of power systems [19] and the probabilistic risk assessment of station blackout accidents in nuclear power plants [16].

Advantages Over Existing Techniques:

1. Inherits all the advantages of simulation approaches used for system reliability and performance evaluation.
2. Implements any system structure with relative ease, since it doesn't require knowledge of the minimal path or cut sets prior to system analysis.
3. Calculates the actual flow across every node of the system.
4. Models systems made up of multiple source and sink nodes with competing static or dynamic demand.
5. Models losses in components and across links.
6. Models component restart and shutdown.
7. Not limited to integer-valued node capacities and system demand, as required by other graph-based algorithms.

7.3.1 Simulation of Interdependent and Reconfigurable Systems

Load flow simulation allows the modelling of inter-component and inter-system dependencies, thereby supporting the reliability assessment of realistic engineering systems [18]. Components and external events that influence the operation of the

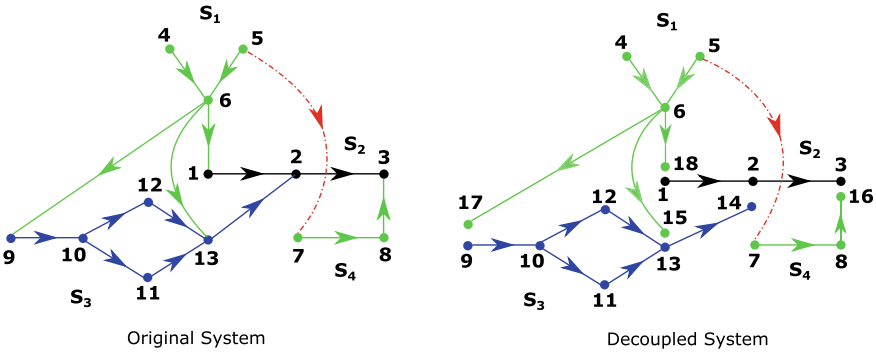

Fig. 7.3 Illustration of decoupling procedure for interdependent systems

system are identified and numbered, followed by the identification and modelling of all the inter-component dependencies in the system. The strategy is to decouple the interdependent system into its constituent systems (subsystems) as shown in [18]. The nodes associated with each subsystem are then identified and its directed graph obtained (i.e. only nodes with actual commodity flow are considered). The states of each node are then identified and modelled as described in [17].

For illustrative purposes, consider the original system in Fig. 7.3 (left panel). It is an interdependent four commodity system—each solid line transports a commodity and the broken line depicts an induced dependency in the direction of the arrow. Node 2 is part of subsystem S_2 and relies the commodity from subsystem S_3 to drive its operation. One would say it is functionally dependent on subsystem S_3 and exhibits a dual operation mode, operating both as a sink and an intermediate node. Its sink mode directly influences flow in S_3, while its transmission mode directly influences flow in S_2. It is, therefore, logical to separate node 2 into its constituent nodes, each representing a mode of operation. **Virtual nodes** representing the *sink modes* of dual nodes are created and assigned new IDs, creating a decoupled system (see Fig. 7.3 (right panel)). A load-source functional dependency exists between the decoupled nodes, since the transmission node is incapacitated if flow into the sink node is inadequate. Therefore, they make a load-source pair, with the transmission node being the load and the sink node, the local source node.

Local sources, otherwise known as *support nodes* in load-source pairs, are modelled as binary-state objects: state 1 (active) has capacity l, depicting the availability of the dependent node; State 2 (inactive) has capacity 0 and depicts its unavailability. l is the minimum level of support required to operate the dependent/sink node and in practical cases represents the load rating of that component. By applying the decoupling procedure described to all load dependency relationships in the system, the following load-source pairs; $\{2, 14\}$, $\{3, 16\}$, $\{1, 18\}$, $\{13, 15\}$ and $\{9, 17\}$ are obtained. $\mathbb{L}_i = \{j, l\}$ signifies that node i requires a minimum of l units of a certain commodity from node j to operate. If i has a load dependency relationship with

multiple nodes, $\mathbb{L}_i$ takes the form of a two-column matrix, with each row defining the node's relationship with another node.

Induced dependencies are defined by the parameter $\boldsymbol{D}_i = \{d_{j1}, d_{j2}, d_{j3}, d_{j4}\}_{u\times 4} \mid j = 1, 2, ..., u-1, u$, which defines the state change induced in other nodes as a result of a state change in node i. d_{j1} is the state of i triggering the cascading event, d_{j2}; the affected node, d_{j3}; the state the node has to be in to be affected, and d_{j4}; its target state on occurrence of the event. Each row of $\boldsymbol{D}_i$ defines the behaviour of an affected node, and u, the number of relationships. If node i and the affected node d_{j2} belong to different subsystems, the subsystem the latter belongs to is dependent on the subsystem of the former. For example, suppose state 2 of node 5 in Fig. 7.3 forces node 7 into state 3 if it is in state 1 at the time node 5 makes the transition to state 2. The induced dependency of node 7 on node 5 is defined by $\boldsymbol{D}_5$ as

$$\boldsymbol{D}_5 = \begin{pmatrix} 2 & 7 & 1 & 3 \end{pmatrix} \tag{7.1}$$

Once the system has been decoupled, the dependency tree depicting the relationships between its subsystems and their ranking is derived. The rank of a subsystem depends on its position on the tree relative to the reference subsystem. The independent subsystem, which is also the reference subsystem, is assigned rank 1 and the remainder ranked in ascending order of their longest distance from this reference. See [18] for the details of the ranking, reconfiguration and simulation procedures.

7.3.2 Maintenance Strategy Optimization

The load flow simulation approach can be exploited to optimise the maintenance strategies of complex systems. The multi-state semi-Markov models of components are extended to represent their behaviour under various maintenance strategies. The operation of the system is then simulated using a slightly modified version of the simulation procedure depicted in Fig. 7.2 and detailed in [19]. Non-Markovian component transitions associated with the operational dynamics imposed by maintenance strategies are implemented. For example, the maintenance of a failed component can only be initiated if there is an idle maintenance team, making the transition of the component from its failed to working state non-Markovian, since it is conditional on the availability of a maintenance team. Additional component states such as preventive maintenance, corrective maintenance, shutdown, diagnostics, idle and awaiting maintenance are included to model different maintenance activities.

To illustrate the derivation of the multi-state model of a component under various maintenance strategies, consider a binary-state component. The component is subject to both preventive and corrective maintenance and maintained by a limited number of maintenance teams. In addition, its corrective maintenance consists of two stages: a diagnosis stage and a restoration stage. Following diagnosis, the maintenance team could proceed with the actual repairs if spares are not required or make a spares request. There is a known probability associated with spares being needed for a repair

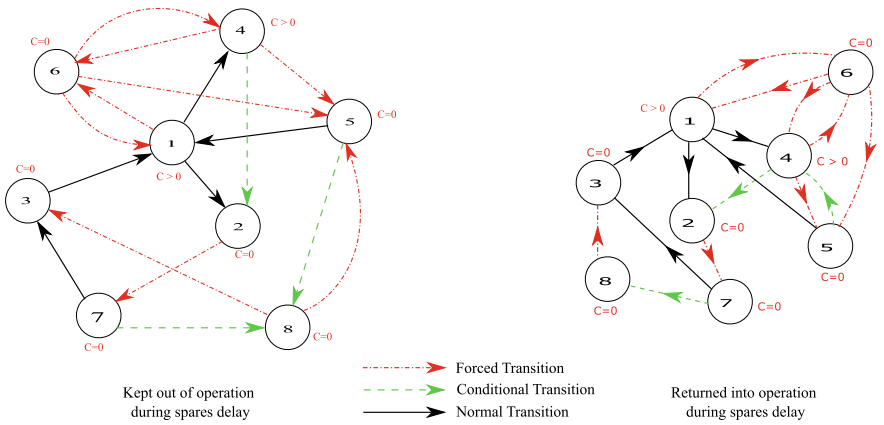

Fig. 7.4 Multi-state models of binary-state component under maintenance delays

and while the maintenance team awaits the spares, it could be assigned to another component. Similarly, there is a probability associated with spares being needed to complete the preventive maintenance of the component, which could be interrupted if these spares are not immediately available. The resulting multi-state models of the component under two contrasting maintenance strategies are shown in Fig. 7.4, with the component's state assignments and possible transitions. Transitions are either normal, forced or conditional. Normal transitions occur randomly and depend only on their associated time-to-occurrence distributions. Forced transitions occur purely as a consequence of events outside the component boundary, and their time-to-occurrence distributions are unknown. Conditional transitions, on the other hand, have a known time-to-occurrence distribution but are assigned a lower priority and only occur on fulfilment of a predefined probabilistic condition or set of conditions [19]. Unlike normal transitions in which the next state of the component depends only on its current state, the next state of the component under forced transitions may also depend on its previous state. As such, the multi-state component transition parameter sampling procedure presented in [17] cannot be used to determine the transition parameters of the component. For this, the set of procedures presented in [19] are required. The binary-state component models in Fig. 7.4 can be generalised for multi-state components by defining one 'Idle' state (if components are kept out of operation during spares delay), a 'Diagnosis' state (where necessary) and one 'Corrective Maintenance' state for each repairable failure mode.

With this approach, multiple contrasting complex maintenance strategies can be simulated without the need to modify the simulation algorithm, as the maintenance strategy is implemented at the component level. See, for instance, the optimal maintenance strategies for a hydroelectric power plant derived in [19].

7.3.3 Case Study: Station Blackout Risk Assessment

The complete lack of AC power at a nuclear power plant is critical to its safety, since AC power is required for its decay heat removal. Though designed to cope with these incidents, nuclear power plants can only do so for a limited time. The impact of station blackouts on a nuclear power plant's safety is determined by their frequency and duration. These quantities, however, are traditionally computed via a static fault tree analysis that deteriorates in applicability with increasing system complexity. The load flow simulation approach was used to quantify the probability and duration of possible station blackouts at the Maanshan Nuclear Power Plant in Taiwan, accounting for interdependencies between system components, maintenance, system reconfiguration, operator response strategies and human errors [16].

The Maanshan Plant is powered through two physically independent safety buses, which themselves are powered by six offsite power sources through two independent switchyards. Each safety bus has a dedicated backup diesel generator and both buses share a third diesel generator. Two gas turbine generators connected through the second switchyard power the plant's safety systems if all three diesel generators are unavailable. The gas turbine generators, however, take about 30 min to become fully operational, when powered on. The goal in this case study was to quantify the risk to the plant, of station blackouts initiated by the failure of the grid sources, as well as the switchyards and identify the best recovery strategy, to minimise this risk.

The load flow simulation approach was used to model the structural/functional relationships between the components of the system as described in Sect. 7.3 and the formalism described in Sect. 7.3.1 to model both the interdependencies between components and their dynamic behaviour under various recovery strategies. The full details of the solution approach and results are available in [16].

7.4 Survival Signature Simulation

For very large-scale systems and networks, the full system structure information (or structure function, minimal paths sets, etc.) might not be available or may be difficult to obtain. Having a compact representation of the system, therefore, is advantageous.

Survival signature [7] has been proposed as a generalisation of system signature [11, 12] to quantify the reliability of complex systems consisting of independent and identically distributed (iid) or exchangeable components, with respect to their random failure time. It has been shown in [8] how the survival signature can be derived from the signatures of two subsystems in both series and parallel configuration. The authors developed a non-parametric-predictive inference for system reliability using the survival signature. Aslett et al. [3] demonstrated the applicability of the survival signature to system reliability quantification via a parametric, as well as non-parametric approach. An efficient computational approach for computing approximate and exact system and survival signatures has been recently presented in [20, 34]. Feng et al. [13] developed an analytical method to calculate the sur-

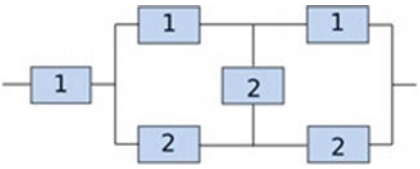

Fig. 7.5 Example of a bridge network composed of six-component of two types

Table 7.1 Survival signature for the system shown in Fig. 7.5

l_1	l_2	$\Phi(l_1, l_2)$	l_1	l_2	$\Phi(l_1, l_2)$
0	[0, 1, 2, 3]	0	2	[0, 1]	0
1	[0, 1]	0	2	2	1/3
1	2	1/9	2	3	2/3
1	3	1/3	3	[0, 1, 2, 3]	1

vival function of systems with uncertainty in the parameters of component failure time distributions. These methods are all useful but less practical for larger complex systems and not applicable to non-exponential transitions.

As an illustration, consider a six-component bridge network with two component types (Fig. 7.5), the survival function is given by Table 7.1.

Considering 2 working components of type 1; $l_1 = 2$ and 3 of type 2; $l_2 = 3$, there are three possible combinations in total but only two combinations lead to success (the survival of the system) of the system. Hence, the survival signature of the system is $\frac{2}{3}$, as shown in Table 7.1. Similarly, for $l_1 = 3$ and $l_2 = [0, 1, 2, 3]$, there are eight possible combinations in total, all of which result in success. Hence, the survival signature of the system in this case is equal to 1.0. Thus, knowing the success paths from the combinations of multiple types of active components, it is possible to compute the survival function of a complex system.

Exact analytical solutions are restricted to particular cases (e.g. systems with component failure times following the exponential distribution and non-repairable components). The survival function of a system with K component types is given by

$$P(T_s > t) = \sum_{l_1=0}^{m_1} \ldots \sum_{l_K=0}^{m_K} \phi(l_1, \ldots, l_K) P(\bigcap_{k=1}^{K} \{C_k(t) = l_k\}) \tag{7.2}$$

where

$$P(\bigcap_{k=1}^{K} \{C_k(t) = l_k\}) = \prod_{k=1}^{K} \binom{m_k}{l_k} [F_k(t)]^{m_k - l_k} [1 - F_k(t)]^{l_k} \tag{7.3}$$

Here, $C_k(t) \in \{0, 1, \ldots, m_k\}$ denotes the number of components of type k in the system which function at time t, and $F_k(t)$ represents the CDF of the random failure times of components of the different types. In this approach, we have a strong iid

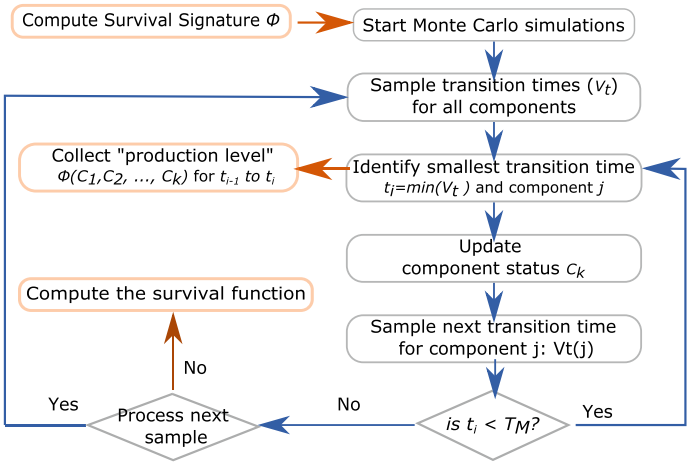

Fig. 7.6 Flow chart of the Monte Carlo simulation algorithm for complex systems with repairable components based on survival signature. Details of the simulation method are available in [30]

assumption of failure times within same components types. With this assumption, all state vectors [7] are equally likely to occur.

However, simulation methods can be applied to study and analyse any system, without introducing simplifications or unjustified assumptions. A Monte Carlo-based approach can be combined with survival signature, to estimate the reliability of a system in a simple and efficient way. A possible system evolution is simulated by generating random events (i.e. the random transition such as failure times of the system components) and then estimating the status of the system based on the survival signature (Eq. (7.2)). By counting the number of occurrences of a specific condition (e.g. the number of times the system is in working status), it is possible to estimate the survival function and reliability of the system.

The most generally applicable Monte Carlo simulation methods adopting the survival signature for multi-state component and repairable systems have been proposed in [30]. Its procedural steps are presented in Fig. 7.6.

7.4.1 Systems with Imprecision

The reliability analysis of complex systems requires the probabilistic characterisation of all the possible component transitions. This usually requires a large dataset that is not always available. To avoid the inclusion of subjective assumptions, imprecision and vagueness of the data can be treated by using imprecise probabilities that combine probabilistic and set theoretical components in a unified construct (see, e.g. [4, 9]). Randomness and imprecision are considered simultaneously but viewed separately at any time during the analysis and in the results [32].

Imprecision can occur at component level, where the exact failure distribution is not known or at system level, in the form of an imprecise survival signature. The latter occurs when part of the system can be unknown or not disclosed. Such imprecision leads to bounds on the survival function of the system, providing confidence in the analysis, in the sense that it does not make any additional hypothesis regarding to the available information. When the imprecision is at the component level, a naïve approach, employing a double loop sampling approach where the outer loop is used to sample realisations of component parameters, can be used. In other words, each realisation defines a new probabilistic model that needs to be solved adopting the simulation methods proposed above, from which the envelop of the system reliability is identified. However, since almost all systems are coherent (a system is coherent if each component is relevant, and the structure function is nondecreasing), it is only necessary to compute the system reliability twice, using the lower and upper bounds for all the parameters, respectively. If the imprecision is at the system level (i.e. in the survival signature), the simulation strategy proposed in Fig. 7.6 can be adopted without additional computational cost by collecting, in two separate counters, the upper and lower bounds of the survival signature at each component transition, as illustrated in [30]. Hence, imprecision at the component and system levels can be considered concurrently, without additional computational costs.

7.4.2 *Case Study: Industrial Water Supply System*

An industrial water supply system consisting of 13 components, as shown in Fig. 7.7, is chosen as a case study, to demonstrate the capability of the survival signature method. The system is expected to deliver water to at least one of the two tanks $T2$ or $T3$ from tank $T1$, through a set of motor-operated pumps and valves. The component failure data with the corresponding distributions are provided in Table 7.2. The survival signature method is employed to compute the reliability of the system.

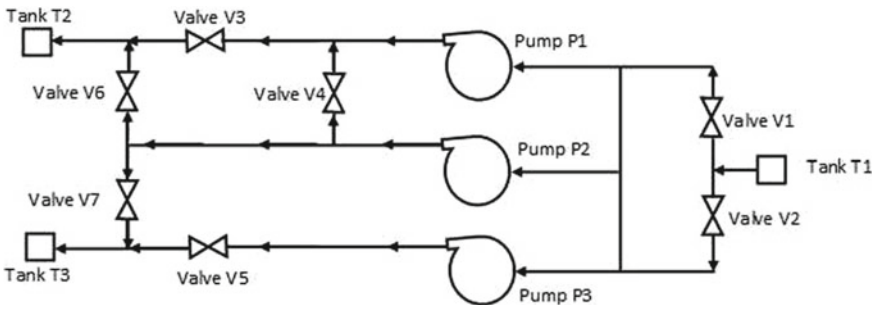

Fig. 7.7 Industrial water supply system

Table 7.2 Reliability parameters of the components of the water supply system

Component	Failure rate (h^{-1})	MTTR (h)	Repair rate (h^{-1})	Distribution type
T_1, T_2, T_3	$\lambda_1 = 5 \cdot 10^{-5}$	24	$\mu_1 = 0.0417$	Exponential
P_1, P_2, P_3	$\lambda_2 = 3 \cdot 10^{-3}$	17.4	$\mu_2 = 0.0575$	Exponential
$V_1, V_2, V_3, V_4, V_5, V_6, V_7$	$\lambda_3 = 2 \cdot 10^{-4}$	9	$\mu_3 = 0.111$	Exponential

Table 7.3 Survival signature (selected parts only) for the system shown in Fig. 7.7 computed with approach proposed in [20]

l_1	l_2	l_3	Φ	l_1	l_2	l_3	Φ
[0, 1]	∀	∀	0				
2	1	2	1/63	3	1	2	1/21
2	1	5	8/63	3	1	5	8/21
2	1	7	2/9	3	1	7	2/3
2	2	6	22/63	3	2	6	6/7
2	3	5	8/21	3	3	5	6/7
2	3	7	2/3	3	3	7	1

The components of the system are categorised into three types, namely, pumps, tanks and valves. The survival signature is given in Table 7.3. The survival function of the water system is then calculated analytically as shown below:

$$P(T_S > t) = \sum_{l_1=0}^{3} \sum_{l_2=0}^{3} \sum_{l_1=0}^{7} \Phi(l_1, l_2, l_3) \binom{3}{l_1} [1 - e^{-\lambda_1 t}]^{3-l_1} \left[e^{-\lambda_1 t}\right]^{l_1} \times \binom{3}{l_2} \left[1 - e^{-\lambda_2 t}\right]^{3-l_2} \left[e^{-\lambda_2 t}\right]^{l_2} \times \binom{7}{l_3} \left[1 - e^{-\lambda_3 t}\right]^{7-l_3} \left[e^{-\lambda_3 t}\right]^{l_3} \quad (7.4)$$

The resulting survival functions without repair and with repairable components are shown in Fig. 7.8.

As shown in Fig. 7.8, the results of the simulation method are in agreement with the analytical solution for both repairable and non-repairable components. The proposed simulation method is applicable to any distribution type, intervals or even probability boxes. It not only separates the system structure from its component failure time distributions, but also doesn't require the iid assumption between different component types, as illustrated in [14].

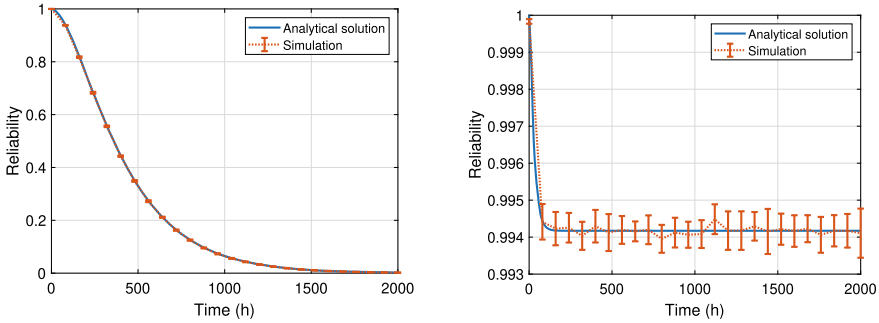

Fig. 7.8 Survival function without repairable (left panel) and with repairable components (right panel) computed using 10000 samples and verified by the analytical solutions

7.5 Final Remarks

System topological complexity, component interdependencies, multi-state component attributes and complex maintenance strategies inhibit the application of simple reliability engineering reasoning to systems. For systems characterised by these attributes, simulation-based approaches allow the realistic analysis of their reliability, despite the relatively higher computational costs of these approaches. This, however, is not a problem, with recent advancement in computing.

The load flow simulation approach is an intuitive simulation framework that is applicable to binary and multi-state systems of any topology. It does not require the prior definition of the structure function, minimal cut sets or the minimal path sets of the system. Instead, it employs a linear programming algorithm and the principles of flow conservation to compute the flow through the system. Thus, it can model flow losses and implement reconfiguration requirements relatively easily. It can model all forms of interdependencies in realistic systems, using intuitive representations. These attributes render the framework intuitive and generally applicable.

While the load flow simulation approach is optimised for multi-state systems, it may not be the best for binary-state systems with identical components. Since the survival signature is a function of the system topology only, it can be calculated only once and reused in multiple reliability analyses. This feature reduces the reliability evaluation of the system to the analysis of the failure probabilities of its components, which is computationally cheap. Efficient simulation methods based on system survival signature allow the reliability analysis of complex systems without resorting to simplifications or approximations.

The load flow and survival signature simulation approaches are not alternative to each other; instead, they can be coupled to take advantage of their unique features, especially for systems with multiple outputs and potentially, multi-state systems.

The algorithms and examples presented are available at: https://github.com/cossan-working-group/SystemReliabilityBookChapter.

References

1. M. Abd-El-Barr. *Design and analysis of reliable and fault-tolerant computer systems*. Hackensack, NJ, USA: World Scientific Publishing Co., 2006.
2. Ahmad W. Al-Dabbagh and Lixuan Lu. Reliability modeling of networked control systems using dynamic flowgraph methodology. *Reliability Engineering and System Safety*, 95(11):1202 – 1209, 2010.
3. L.J.M Aslett, F.P. Coolen, and S.P. Wilson. Bayesian inference for reliability of systems and networks using the survival signature. *Risk Analysis*, 2014.
4. Michael Beer and Edoardo Patelli. Editorial: Engineering analysis with vague and imprecise information. *Structural Safety*, 52:143, 2015.
5. Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, April 2010.
6. Sungil Byun, Inseok Yang, Moo Geun Song, and Dongik Lee. Reliability evaluation of steering system using dynamic fault tree. In *IEEE Intelligent Vehicles Symposium*, pages 1416 – 1420, 2013.
7. F.P. Coolen and T. Coolen-Maturi. Generalizing the signature to systems with multiple types of components. *Complex Systems and Dependability*, pages 115 – 30, 2012.
8. Frank P.A. Coolen and Tahani Coolen-Maturi. Predictive inference for system reliability after common-cause component failures. *Reliability Engineering & System Safety*, 135:27 – 33, 2015.
9. Alvarez DA. Infinite random sets and applications in uncertainty analysis. *Arbeitsbereich für Technische Mathematik am Institut für Grundlagen der Bauingenieurwissenschaften. Leopold-Franzens-Universität Innsbruck*, 2007.
10. Salvatore Distefano and Antonio Puliafito. Reliability and availability analysis of dependent-dynamic systems with drbds. *Reliability Engineering and System Safety*, 94(9):1381–1393, 2009.
11. S. Eryilmaz. Review of recent advances in reliability of consecutive k-out-of-n and related systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 224 (3):225 - 237, 2010.
12. Samaniego FJ. System signatures and their applications in engineering reliability. *Springer Science & Business Media*, 110.
13. M. Beer F. P. Coolen G. Feng, E. Patelli. Imprecise system reliability and component importance based on survival signature. *Reliability Engineering & System Safety*, 150:116 - 125, 2016.
14. Hindolo George-Williams, Geng Feng, Frank Coolen, Michael Beer, and Edoardo Patelli. Extending The Survival Signature Paradigm To Complex Systems With Non-repairable Dependent Failures. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 233(4):505–519, August 2019.
15. Hindolo George-Williams, Geng Feng, Frank PA Coolen, Michael Beer, and Edoardo Patelli. Extending the survival signature paradigm to complex systems with non-repairable dependent failures. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 233(4):505–519, 2019.

16. Hindolo George-Williams, Min Lee, and Edoardo Patelli. Probabilistic risk assessment of station blackouts in nuclear power plants. *IEEE Transactions on Reliability*, 67(2):494–512, June 2018.
17. Hindolo George-Williams and Edoardo Patelli. A hybrid load flow and event driven simulation approach to multi-state system reliability evaluation. *Reliability Engineering & System Safety*, 152:351–367, August 2016.
18. Hindolo George-Williams and Edoardo Patelli. Efficient Availability Assessment of Reconfigurable Multi-State Systems with Interdependencies. *Reliability Engineering & System Safety*, 165:431–444, September 2017.
19. Hindolo George-Williams and Edoardo Patelli. Maintenance Strategy Optimization for Complex Power Systems Susceptible to Maintenance Delays and Operational Dynamics. 66(4):1309–1330, 2017.
20. M. Beer J. Behrensdorf, M. Broggi. Imprecise reliability analysis of complex interconnected networks. *Safety and Reliability - Safe Societies in a Changing World - Haugen et al. (Eds), Taylor & Francis Group, London, ISBN 978-0-8153-8682-7 year = 2018.*
21. G. Levitin and A. Lisnianski. *Multi-state System Reliability Analysis and Optimization, in: Handbook of Reliability Engineering*, chapter 4, pages 61–90. Springer, 2003.
22. G. Levitin, L. Xing, H. Ben-Haim, and Y. Dai. Multi-state systems with selective propagated failures and imperfect individual and group protections. *Reliability Engineering & System Safety*, 96(12):1657–1666, 12 2011.
23. Jing-An Li, Yue Wu, Kin Keung Lai, and Ke Liu. Reliability estimation and prediction of multi-state components and coherent systems. *Reliability Engineering & System Safety*, 88(1):93 – 98, 2005.
24. A. Lisnianski and Y. Ding. Inverse lz-transform for a discrete-state continuous-time markov process and its application to multi-state system reliability. In *Applied Reliability Engineering and Risk Analysis*. Wiley, 2014.
25. Anatoly Lisnianski, Ilia Frenkel, and Yi Ding. *Multi-State System Reliability Analysis and Optimization for Engineers and Industrial Managers*. Springer-Verlag London Limited, 2010.
26. Manish Malhotra and Kishor S. Trivedi. Dependability modeling using petri-nets. *IEEE Transactions on Reliability*, 44(3):428 – 440, 1995.
27. A Mosleh, D M Rasmuson, and F M Marshall. Guidelines on modeling Commom-Cause Failures in probabilistic risk assessment. Technical Report NUREG/CR-5485, U.S. Nuclear Regulatory Commission, 1998.
28. Andrew O'Connor and Ali Mosleh. A general cause based methodology for analysis of common cause and dependent failures in system risk and reliability assessments. *Reliability Engineering & System Safety*, 145:341 – 350, 2016.
29. Min Ouyang. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, 121:43 – 60, 2014.
30. Edoardo Patelli. *Handbook of Uncertainty Quantification*, chapter COSSAN: A Multidisciplinary Software Suite for Uncertainty Quantification and Risk Management, pages 1–69. Springer International Publishing, 2017.
31. Edoardo Patelli, Hindolo George-Williams, Jonathan Sadeghi, Roberto Rocchetta, Matteo Broggi, and Marco de Angelis. OpenCossan 2.0: An efficient computational toolbox for risk, reliability and resilience analysis. In André T. Beck, Gilberto F. M. de Souza, and Marcelo A. Trindade, editors, *Proceedings of the Joint ICVRAM ISUMA UNCERTAINTIES Conference*, 2018.
32. Broggi M de Angelis M. Patelli E, Alvarez DA. Uncertainty management in multidisciplinary design of critical safety systems. *J Aerosp Inf Syst*, 12:140-69, https://doi.org/10.2514/1.I010273,2015.
33. Jose E. Ramirez-Marquez and David W. Coit. Optimization of system reliability in the presence of common cause failures. *Reliability Engineering & System Safety*, 92(10):1421 – 1434, 2007.
34. S. Reed. An efficient algorithm for exact computation of system and survival signatures using binary decision diagrams. *Reliability Engineering & System Safety*, 165:257 - 267, https://doi.org/10.1016/j.ress.2017.03.036.,2017.

35. Dan M. Shalev and Joseph Tiran. Condition-based fault tree analysis (cbfta): A new method for improved fault tree analysis (fta), reliability and safety calculations. *Reliability Engineering and System Safety*, 92:1231 – 1241, 2007.
36. Masoud Taheriyoun and Saber Moradinejad. Reliability analysis of a wastewater treatment plant using fault tree analysis and monte carlo simulation. *Environmental Monitoring and Assessment*, 187(1), 2015.
37. Matthias CM Troffaes, Gero Walter, and Dana Kelly. A robust Bayesian approach to modeling epistemic uncertainty in common-cause failure models. *Reliability Engineering & System Safety*, 125:13–21, 2014.
38. M. Veeraraghavan and K.S. Trivedi. A combinatorial algorithm for performance and reliability analysis using multistate models. *IEEE Transactions on Computers*, 43(2):229–234, Feb 1994.
39. Liudong Xing and Yuanshun Dai. A new decision-diagram-based method for efficient analysis on multistate systems. *Dependable and Secure Computing, IEEE Transactions on*, 6(3):161–174, July 2009.
40. Wei-Chang Yeh. An improved sum-of-disjoint-products technique for the symbolic network reliability analysis with known minimal paths. *Reliability Engineering & System Safety*, 92(2):260 – 268, 2007.
41. Wei-Chang Yeh. A fast algorithm for quickest path reliability evaluations in multi-state flow networks. *Reliability, IEEE Transactions on*, 64(4):1175–1184, Dec 2015.
42. Wei-Chang Yeh, Yi-Cheng Lin, Y.Y. Chung, and Mingchang Chih. A particle swarm optimization approach based on monte carlo simulation for solving the complex network reliability problem. *Reliability, IEEE Transactions on*, 59(1):212–221, March 2010.
43. Enrico Zio, Piero Baraldi, and Edoardo Patelli. Assessment of the availability of an offshore installation by monte carlo simulation. *International Journal of Pressure Vessels and Piping*, 83(4):312 – 320, 2006.