Reliability Engineering and System Safety 165 (2017) 431–444

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Efficient availability assessment of reconfigurable multi-state systems with interdependencies

Hindolo George-Williams[a,b], Edoardo Patelli[a,*]

[a] Institute for Risk and Uncertainty, Chadwick Building, University of Liverpool, Peach Street, Liverpool L69 7ZF, United Kingdom
[b] Institute of Nuclear Engineering & Science, National Tsing Hua University, Hsinchu, Taiwan

ARTICLE INFO

Keywords:
Multi-State system
Simulation
Interdependencies
Availability
Limited maintenance
Multi-Commodity

ABSTRACT

Realistic engineering systems often possess attributes that complicate their availability assessment. Notable examples being complex topology, multi-state behaviour, component interdependencies, and interactions with external phenomena. For such systems, analytical techniques have limited applicability, and efficient simulation techniques are, therefore, required. In this paper, a novel load-flow simulation approach is proposed to simplify the availability assessment of realistic engineering systems. The approach is simple and generally applicable to systems, including those with limited maintenance teams, reconfiguration requirements, and multiple commodity flows. A novel metric for assessing maintenance inadequacy and a real-time component ranking procedure are also introduced. In real-time ranking, failed components are assigned maintenance priorities during simulation in accordance with how much their availability improves system performance and how many idle maintenance teams there are. This eliminates the need for component importance ranking algorithms prior to simulation, which for some systems may be unnecessary. The applicability of the approach is demonstrated by analysing an offshore plant producing oil, gas, and water. The solution obtained is compared against another Monte Carlo simulation-based solution that requires the enumeration of the plant's cut-sets. The proposed approach is shown to be more intuitive, robust to human-induced errors, and require less human effort.

1. Introduction

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 resultant systems are complex and highly interconnected, which ironically constitute a threat to their resilience and sustainability. Majority of the systems we interact with on a day-to-day basis exist as multi-state interdependent systems. Two systems are interdependent if at least a pair of nodes (one from each system) are coupled by some phenomena, such that a malfunction of one affects the other. The coupling phenomenon could be proximity in space [1], functional dependence/interdependence [2], or both [3]. A water distribution network, where pumps and other electrical power-driven appliances rely on the reliability and performance of the power grid is a typical example.

The components of a system are normally prone to random failures arising from their intrinsic properties or induced failures stemming from targeted attacks [4], extreme environmental events [5], and erroneous human-system interactions. In interdependent systems, an undesirable glitch in one system could cascade and cause disruptions in coupled systems. The cascade could be fed back into the initiating system and the overall consequences may be catastrophic [1,6]. This was made clear by the massive blackout that struck Italy in September 2003, affecting the internet network in the process. In the same year, North America was hit by a blackout that lasted 4 days, affecting parts of USA and Canada [7]. To minimize the effects of these failures, some interdependent systems are equipped with reconfiguration provisions. This normally entails transferring operation to another node, rerouteing flow through alternative paths, or shutting down parts of the system. It is, therefore, vital to analyse the system's performance under the spectrum of possible vulnerability conditions, for adequate planning of defensive and contingency measures [8].

In general, the achievement of maximum overall system performance is desirable. However, in many applications, it is more important to recover the required system performance in the shortest possible time after component failure. This is the case, for instance, in nuclear power plant risk assessment, where the time-dependent recovery probability of off-site power is an important input to the overall safety of the plant [9]. Hence, system recovery time is not only a performance parameter, but

* Corresponding author at: Institute for Risk and Uncertainty, Chadwick Building, University of Liverpool, Peach Street, Liverpool L69 7ZF, United Kingdom
E-mail addresses: H.George-Williams@liv.ac.uk (H. George-Williams), epatelli@liverpool.ac.uk (E. Patelli).

http://dx.doi.org/10.1016/j.ress.2017.05.010
Received 7 June 2016; Received in revised form 3 March 2017; Accepted 3 May 2017
Available online 8 May 2017
0951-8320/

a fundamental safety parameter as well. Given the positive correlation between costs and resources (human, financial, and material) required to maintain a system, under economic constraints, there may not be sufficient resources for a speedy recovery. Therefore, an informed and robust decision making process would dictate that the decision support tool used is capable of modelling relevant realistic aspects of the system, including the possibility of limited recovery response.

Various models have been developed to study the effects of interdependencies on systems [8,10]. However, a good number of these only assess their response to targeted attacks, variation in some coupling factor, or the relative importance of system nodes [1,2,11]. According to Ouyang [10], these models alone cannot sufficiently analyse the performance of interdependent systems. He intimated that flow based approaches, taking into account material or service flow across the system were required. When faced with the situation of random node failures, a complete reliability and availability analysis should be performed. However, renown analytical multi-state system reliability evaluation techniques like Binary Decision Diagrams (BDD) [12,13], Sum-of-Disjoint-Products (SDP) [14], and the Universal Generating Function (UGF) [15–17] are of very little use to the evaluation of these systems. Their inapplicability is amplified if, nodes can undergo non-Markovian transitions, their restoration can be delayed, the system is reconfigurable, or in the case of BDD and SDP, the system is complex, such that state enumeration is infeasible. In spite of these challenges, there are a few successful attempts at their application to systems with some form of dependencies. Levitin, for instance, in [18] and [15], respectively applied the UGF approach to systems with lateral dependencies and systems prone to common-cause failures. Both instances, however, involved only one system with a single commodity. Stochastic Petri Nets [19,20] and Bayesian Networks [21] are another set of powerful computational tools for the reliability modelling of systems with dependencies. However, they also require state enumeration when applied to multi-state systems, which may be infeasible for some complex system architectures.

Certain realistic aspects of interdependent systems, as previously mentioned, are implementable only by simulation algorithms [22]. However, most multi-state system simulation algorithms rely either on the structure function of the system or enumeration of the system's path or cut sets [22,23]. Both procedures get cumbersome even for complex systems of moderate size, and with them, the shut down and restart of components (a type of reconfiguration) is non-intuitive [24].

1.1. Proposed approach

The authors recently presented a load-flow simulation technique for the analysis of multi-state systems [24]. In the technique, each system node is modelled as a semi-Markov stochastic process and the system structure as a directed graph. An event-driven simulation is used to reconstruct the random failure and repair events of system nodes. As nodes go through their cycle of failures and subsequent repairs, their capacities change, and the interior-point algorithm [25] is used to determine the performance of the system. The approach employs an adjacency matrix to define the structure of the system and derives the equations of flow across the entire system in the form of matrices. This particularly makes it suitable and intuitive for any system architecture and easily programmable on a digital computer. In terms of applicability, it outperforms other multi-state system analysis approaches, since it does not require state enumeration or cut set definition. It considers realistic system aspects like flow losses, reconfiguration, forced transitions, and multiple competing demands. The approach, however, is only applicable to homogeneous independent systems and does not consider restrictions on the number of simultaneous maintenance actions that can take place in the system.

In this work, the load-flow simulation approach is extended to support interdependencies, multi-commodity systems, and model limited maintenance team scenarios. Though largely built on the principles proposed in the original work [24], this work makes a series of new contributions as highlighted thus;

- We define a straight-forward procedure for uncoupling interdependencies in systems and propose an intuitive mathematical model for their adequate representation.
- Two recursive algorithms are proposed to accurately account for these interdependencies and compute the performance of the system during simulation.
- To enhance the efficient extraction of system availability and performance indices from the simulation result, easily implementable algorithms have been proposed. Availability, as used here, refers to the ability of a system to function as expected. It, therefore, encompasses the reliability, the output characteristics, and the recovery probability of the system after its deviation from expected performance.
- System reliability and output characteristics are already very common system availability indices. We use the recovery probability and a new metric for assessing the adequacy of the maintenance process as additional system performance indices.
- We also propose a real-time component ranking procedure to help decide the sequence of maintenance response that maximises system performance. In practice, the system operator would use this procedure whenever a scenario dictating preferential maintenance arises.
- Finally, a simple but important modification is also made to the original system flow calculation procedure, resulting in appreciable gains in computation time.

In summary, this work extends the applicability of the load-flow simulation approach and improves its computational efficiency.

1.2. Paper structure

The remainder of the paper is organised as follows; the next section is dedicated to providing an overview of the relevant modifications to the load-flow approach to include interdependencies. In this section, a generalised procedure for assessing the availability of interdependent multi-state systems is also presented. Details of the simulation procedure and availability assessment algorithms are respectively provided in Sections 3 and 4. Section 5 addresses the availability assessment problem of an offshore multi-commodity plant. The plant is used to illustrate the systematic roll out of the solution strategy developed in Section 2 to a practical problem of industrial relevance. The usefulness of the new metric for maintenance inadequacy and real-time component ranking are also illustrated here. The implication of the results, efficiency of the approach, and its limitations, climax this section. Finally, the closing remarks; drawing conclusions on the proposed approach, make up Section 6.

2. Implementation

In this section, the relevant principles governing the modelling of the system and its components are described. They are based on the earlier work presented in [24], as a result, premium is placed only on the necessary modifications. For this purpose, we use the arbitrary system shown in Fig. 1, which could be a binary-state system or a multi-state flow network [26]. It consists of 4 subsystems and 13 nodes, transporting 4 commodities. The number of subsystems is normally defined by the number of commodities or more generally by the number of closed-loops. This implies, a system could be composed of multiple subsystems even when only one commodity type is involved. Nodes 1, 2, and 3, transporting commodity-B, respectively require commodity, A, C and D to operate and nodes 9 and 13 in subsystem S_3 rely on flow from subsystem S_1. Also, a certain failure mode of node 5 in subsystem S_1, triggers the partial failure of node 7 in subsystem S_4. This type of interdependence is called one-way dependence, since the failure of node 5 affects node 7, but state change events in node 7 have no effect on node 5. Even for