Reliability Engineering and System Safety 163 (2017) 95–108

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

System design and maintenance modelling for safety in extended life operation

John Andrews*, Claudia Fecarotti

University of Nottingham, United Kingdom

ARTICLE INFO

Keywords:
Asset management
System reliability availability
Petri nets
Bayesian networks
Design
Maintenance
Aging systems

ABSTRACT

It is frequently the most cost effective option to operate systems and infrastructure over an extended life period rather than enter a new build programme. The condition and performance of existing systems operated beyond their originally intended design life are controlled through maintenance. For new systems there is the option to simultaneously develop the design and the maintenance processes for best effect when a longer life expectancy is planned. This paper reports a combined Petri net and Bayesian network approach to investigate the effects of design and maintenance features on the system performance. The method has a number of features which overcome limitations in traditionally used system performance modelling techniques, such as fault tree analysis, and also enhances the modelling capabilities. Significantly, for the assessment of aging systems, the new method avoids the need to assume a constant failure rate over the lifetime duration. In addition the assumption of independence between component failures events is no longer required. In comparison with the commonly applied system modelling techniques, this new methodology also has the capability to represent the maintenance process in far greater detail and as such options for: inspection and testing, servicing, reactive repair and component replacement based on condition, age or use can all be included. In considering system design options, levels of redundancy and diversity along with the component types selected can be investigated. All of the options for the design and maintenance can be incorporated into a single integrated Petri net and Bayesian network model and turned on and off as required to predict the effects of any combination of options selected. In addition this model has the ability to evaluate different system failure modes.

The integrated Petri-net and Bayesian network approach is demonstrated through application to a remote un-manned wellhead platform from the oil and gas industry.

1. Introduction

The performance of engineering safety systems is governed by both its initial design and also the maintenance strategy employed once it is in operation. The adequacy of any system is determined through the analysis of its predicted performance against target levels of safety and risk. The assessment process usually involves the identification of initiating events, which will produce potential hazards, and the response of the safety systems to prevent its escalation. Commonly the assessment of the system performance is carried out using an integrated combination of Event Tree Analysis [1] and Fault Tree Analysis [2–4]. The implementation of these techniques in commercial software require assumptions to be made regarding the system characteristics. Key assumptions are that the component failure events will be independent and (in the majority of commercial codes) that failures and repairs occur with constant rates. The limited range of models used to establish the failure probability of the components also restricts the ability of the method to investigate the benefits of the complex range of options which can be employed in maintaining the system. An extension of Fault Tree to include time requirements in order to capture the dynamic behaviour of systems is the Dynamic Fault Tree [5]. Dynamic Fault Tree has been used in [6] for the dependability analysis of safety and protection systems during standby and active operation phased. The authors combine an availability analysis of the system in standby mode and a reliability analysis for the active mode within the context of Dynamic Fault Trees. Although the use of Dynamic Fault Trees enables to account for time dependencies, their analysis still remains expensive when dealing with complex systems with many components and many possible events occurring. Approaches like Semi-Markov processes [7] enable to model systems characterised by non-constant rates processes, but the state-space explosion issue when considering systems with many components and many possible states still remains.

For many industries, when systems reach the end of their intended

* Corresponding author.

http://dx.doi.org/10.1016/j.ress.2017.01.024
Received 8 June 2016; Received in revised form 28 January 2017; Accepted 31 January 2017
Available online 02 February 2017

design life, it is more cost effective to continue operating the system, controlling its state through a comprehensive maintenance strategy, than to enter a new build programme. For new systems there is a strong driver to design for longer life expectancies. To establish the most effective performance, over extended life, a whole system, whole life view is required. In this approach the system structure (obtained through design) is considered simultaneously with the maintenance strategy. To adequately model the performance of this situation the restrictions featured in the tradition risk assessment methods need to be overcome.

As systems age their components, particularly mechanical components, experience non-constant (increasing) rates of failure. Maintenance strategies are a complex activity defined by parameters which govern the inspection/testing, servicing, reactive repair on failure, component replacement on age, use or condition and sub-system renewal. Opportunistic maintenance is also a possibility where work is carried out on components when the chance presents itself due to work required by other elements in the system. This introduces dependencies between the component conditions.

In formulating a maintenance strategy, the resource utilisation needs to be directed at the elements in the system where they can achieve most benefit. It is also expected that this distribution of resources will change over the life of the system as some parts age at faster rates than others. The system lifetime can be considered as a series of discrete time phases where different maintenance strategies are applied. This concept is similar to the use of phased mission analysis where the functional requirements change as a system mission progresses [8–10].

Fault tree and event tree methods are not capable of modelling non-constant failure rates that increases over time due to wear out, dependencies between component states or complex maintenance processes. Alternative methods have features to overcome these limitations. Petri nets (PNs) [11,12] have proved very effective in modelling systems which feature non-constant deterioration rates and can be used to represent very complex asset management processes [13–15]. PNs constructed to predict the system performance based on the system structure, along with the component deterioration process and the maintenance strategy frequently feature characteristics whose solution requires the use of the Monte Carlo technique [4]. It is therefore advantageous, in the interests of efficiency, to keep the size of such models to a minimum. This can be achieved through modularisation [16] enabling the analysis to be performed in small, independent sections. Bayesian Networks (BNs) [17–19] are capable of accounting for the dependencies in the maintenance process and modularising the analysis. The conditional probability tables can be derived from the results of the PN analysis. Maintenance phases can also be accommodated in the PN and BN methodologies. An integrated BN/PN approach, referred to as the BP-Net method, is developed in this paper and can be used to predict the system level response. An additional feature of this method is that several system failure modes can be considered in the same model.

Through setting the prior probabilities of the root nodes in the BN (to 1 and 0's) to reflect the required design and maintenance options selected, all different design and operational conditions can be investigated in a single model.

The approach is demonstrated in this paper by application to an unmanned wellhead platform used in the offshore oil and gas industry.

2. Safety system modelling

The performance of a safety system into extended life will be dependent upon both the design and the maintenance strategy employed. Ideally the model produced to assess the system performance should be capable of incorporating all options. The options, along with a discussion on how they can be incorporated into a single model, are considered below. It is also advantageous to be able to model several different system failure modes within a single model.

2.1. Design

The design of the system will determine its structure and which of the list of potential components which perform the same function will be selected.

System structure. This will determine how vulnerable the system is to the failure of its components. For safety critical systems, it is undesirable for a single component failure to result in system failure. Redundancy or diversity in the system structure are commonly employed to ensure an adequate level of fault tolerance. In addition, where possible, the system will be made to fail safe. Duplication of the same components (redundancy) or the provision of an alternative means to achieve the same function (diversity) can be implemented in a fully redundant (parallel) structure or a partially redundant (voting) structure. When systems are analysed using a fault tree, all of these design options can be incorporated in the same analysis through the use of house events. House events are incorporated into the fault tree diagram at the base level and are set to true or false in order to represent the selected design by turning on or off the relevant sections of the tree [20]. This type of feature also works well when the fault trees are analysed utilising Binary Decision Diagrams [21–23].

Component selection. There will usually be several options as to the component type selected to fulfil a specified function. Each component selection will imply different performance metrics, maintenance requirements and costs. As with the system structure, these choices can be incorporated into a single fault tree diagram using House events as indicated in reference [20].

These design options can also be included in a PN or BN analysis of the system. This is implemented using exactly the same mechanism as for fault trees and again turn on and off features in the analysis.

2.2. Maintenance strategy

A broad view of maintenance is taken in the context of the system modelling performed in this paper. It will have the effect of controlling the state of a system or asset once it becomes operational. Common maintenance features which need to be incorporated in the model are:

Inspection/testing this activity does not alter the state of any component. It simply reveals the component's condition and enables decisions to be made regarding the requirement to do work. For some components, the inspection can be a visual examination. For others a test can be performed, in some instances remotely.

Servicing is carried out to reduce the rate of failure rate of a component or sub-system. This includes activities such as the replacement of lubricants and filters and the painting of metal structures.

Reactive repair on failure. All components have the potential to fail and repair of the failed component to the working condition is carried out once its state is revealed through inspection or announces itself through its impact on system performance.

Component replacement on age, use or condition. This is usually the preferred means of controlling the system state by replacing components prior to their failure. This decreases the system failure occurrences and disruptions to the functionality of the system and can be conducted at times which are convenient. The trade-off is that early replacement wastes some of the component's operational life. For items where the condition can be measured and related to its failure then condition monitoring offers an effective means on which to base decisions on early component replacement. For items whose condition cannot be measured, the creation of its unreliability function through the study of historical failures can provide a replacement time which ensures that an acceptable risk of failure is experienced.

Sub-system renewal. A whole sub-system can be renewed when maintenance becomes an ineffective means of controlling its condition.

Opportunistic maintenance can be performed on a component when the opportunity presents itself due to work being performed on another component. It could be that the component requiring attention