International Journal of Approximate Reasoning 100 (2018) 29–55

Contents lists available at ScienceDirect

International Journal of Approximate Reasoning

www.elsevier.com/locate/ijar

A review of applications of fuzzy sets to safety and reliability engineering

Sohag Kabir *, Yiannis Papadopoulos

School of Engineering and Computer Science, University of Hull, Hull, HU6 7RX, UK

ARTICLE INFO

Article history:
Received 8 March 2018
Received in revised form 21 May 2018
Accepted 23 May 2018
Available online 26 May 2018

Keywords:
Safety
Reliability
Fuzzy set theory
Fault tree analysis
Bayesian network
Markov chain

ABSTRACT

Safety and reliability are rigorously assessed during the design of dependable systems. Probabilistic risk assessment (PRA) processes are comprehensive, structured and logical methods widely used for this purpose. PRA approaches include, but not limited to Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), and Event Tree Analysis (ETA). In conventional PRA, failure data about components is required for the purposes of quantitative analysis. In practice, it is not always possible to fully obtain this data due to unavailability of primary observations and consequent scarcity of statistical data about the failure of components. To handle such situations, fuzzy set theory has been successfully used in novel PRA approaches for safety and reliability evaluation under conditions of uncertainty. This paper presents a review of fuzzy set theory based methodologies applied to safety and reliability engineering, which include fuzzy FTA, fuzzy FMEA, fuzzy ETA, fuzzy Bayesian networks, fuzzy Markov chains, and fuzzy Petri nets. Firstly, we describe relevant fundamentals of fuzzy set theory and then we review applications of fuzzy set theory to system safety and reliability analysis. The review shows the context in which each technique may be more appropriate and highlights the overall potential usefulness of fuzzy set theory in addressing uncertainty in safety and reliability engineering.

1. Introduction

Safety critical systems are extensively used in many industries, including the aerospace, automotive, medical, and energy sectors. Systems that fall into this category range from airbags in cars to propulsion systems on spacecraft; however, they all share a common property — their failure has the potential to cause catastrophic effects on human life as well as the environment. For this reason, it is expected that safety critical systems possess a high level of safety and reliability. While safety is the avoidance of harm to people and the environment, reliability is the ability to perform the intended function uninterrupted by a failure, which is often a precondition for safety. Both properties are crucial, and as systems become more complex, their prediction via analysis plays a vital role in the successful design and development of the system; at the same time, with increasing complexity analyses become increasingly difficult.

Different probabilistic risk assessment (PRA) methods have been used to evaluate system safety and reliability. Fault tree analysis (FTA) is one of the most widely used PRA approaches to estimate system safety and reliability. In fault trees, the logical connections between faults and their causes are represented graphically. FTA is deductive in nature, meaning that the analysis starts with a top event (a system failure) and works backwards from the top of the tree towards the leaves of

* Corresponding author.
E-mail address: s.kabir@hull.ac.uk (S. Kabir).

https://doi.org/10.1016/j.ijar.2018.05.005
0888-613X/

the tree to determine the root causes of the top event. The results of the analysis show how different component failures or certain environmental conditions can combine together to cause the system failure.

After construction of a fault tree, the analyses are carried out at two levels: a qualitative level and a quantitative level. Qualitative analysis is usually performed by reducing fault trees to minimal cut sets (MCSs), which are a disjoint sum of products consisting of the smallest combinations of basic events that are necessary and sufficient to cause a hazardous situation, e.g., a system failure. In quantitative analysis, the probability of the occurrence of a system failure and other quantitative reliability indexes such as importance measures is mathematically calculated, given the failure rate or probability of individual system component. The results of quantitative analysis give analysts an indication about system reliability and also help to determine which components or parts of the system are more critical, so analysts can put more emphasis on the critical components or parts by taking necessary steps, e.g., including redundant components in the system model.

In addition to the FTA, Failure Mode and Effects Analysis (FMEA), Event Tree Analysis (ETA), Markov chains, Bayesian networks, and Petri nets are some of the other approaches that are used for safety and reliability evaluation of systems. In all the PRA approaches, the system failure probability is evaluated as a function of the failure probability of the system components (e.g. the basic events). Therefore, the applicability of these analysis methods for evaluating system safety and reliability is largely dependent on the availability of the components' lifetime data. Any uncertainties raised in the components failure probability will consequently propagate it to the results. On the other hand, unavailability of failure data would introduce degrees of uncertainty into the analysis results.

In the classical forms of the PRA approaches, failure rates, failure probabilities or other numerical data related to the failure behaviour of system components are usually considered known. But in large and complex systems, not all such data is known due to limited observation and scarcity of statistical data [127,209]. This situation is especially relevant in the early design stages, when the requirements and specifications of system components are incomplete, and in the case of new and complex software components. The failure probability of a relatively new component with insufficient historical failure data could, in theory, be estimated based on expert judgement or experience from similar components. Consequently, system safety and reliability could be evaluated based on generic statistical data, which may be taken from existing reliability databases. However, the use of generic data will add further uncertainty and imprecision to the results of the analysis.

By allowing imprecision and approximate analysis, fuzzy logic enables incorporating uncertainty in the analysis. Fuzzy set theory was firstly used in FTA for system reliability analysis in 1983 [216]. Since then, a number of researchers have developed different fuzzy set theory based FTA methodologies for system safety and reliability analysis, and many researchers have used these methodologies in a variety of application areas such as nuclear power plants, the process industries etc. Fuzzy set theory has also been applied in conjunction with dynamic extensions of the fault trees [232,96]. The application of fuzzy set theory in safety and reliability engineering has been extended to FMEA, ETA, Bayesian networks, and Petri nets.

The last two decades have seen the development of new techniques for model-based safety and reliability analysis, including HiP-HOPS [168,169], ALTARICA [9], and xSAP [17,23] which in various ways automate the production of analysis artefacts like fault trees and FMEAs. The issue of both aleatoric and epistemic uncertainties have not been addressed adequately in these new techniques. The aleatoric uncertainty is due to randomness of a physical system or natural variation, whereas the epistemic uncertainty is because of ambiguity, incompleteness, and lack of knowledge. We hope that this paper will provide some of the background to help stimulate research in addressing this issue.

This paper reviews different concepts of using fuzzy set theory in systems safety and reliability engineering, to reflect the current status of the fuzzy set theory based PRA methodologies, and their applications. The paper is organised as follows: Section 2 describes the fundamentals of fuzzy set theory. Fuzzy FTA, FMEA and ETA are reviewed in sections 3, 4 and 5 respectively. Fuzzy Bayesian networks, Markov chains, and Petri nets methodologies are reviewed in section 6. A discussion and future research directions are presented in section 7. Concluding remarks are provided in section 8.

2. Fundamentals of fuzzy theory

2.1. Fuzzy sets and numbers

Fuzzy set theory was introduced by Zadeh [269] to deal with imprecise, vague or partially true information. In classical set theory, membership of an element in a set is considered to be binary, i.e., either the element belongs to a set or does not belong to a set. However, fuzzy set theory allows an element of a set to have a membership value from the interval $[0, 1]$. Let X be a collection of object universe and its elements are represented by x. A fuzzy set A in X can be characterised by a membership function $\mu_A : X \to [0, 1]$. The value of function $\mu_A(x)$ represents the degree of membership of x in A. A membership value 1 means the element is completely in set A and 0 means the element is completely not in set A. On the other hand, values between 0 and 1 represent the partial membership, where the higher the value the stronger the degree of membership is.

A fuzzy number could be defined in different forms depending on the nature of the problem in hand. In [145], the authors have mentioned that any shape of membership function could be applied to reliability analysis of engineering systems. Among different shape of membership functions, the triangular and the trapezoidal shapes are widely used in reliability engineering to represent fuzzy failure rates or probabilities of system components.