Reliability Engineering and System Safety 150 (2016) 105–115

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A multiphase dynamic Bayesian networks methodology for the determination of safety integrity levels

Baoping Cai [a,b,*], Yu Liu [b,*], Qian Fan [a]

[a] College of Mechanical and Electronic Engineering, China University of Petroleum, Qingdao, Shandong 266580, China
[b] Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Received 8 July 2015
Received in revised form
24 January 2016
Accepted 27 January 2016
Available online 3 February 2016

Keywords:
Multiphase dynamic bayesian networks
Safety integrity level
Safety instrumented system
KooM architecture
KooMD architecture

ABSTRACT

A novel safety integrity levels (SILs) determination methodology based on multiphase dynamic Bayesian networks (MDBNs) for safety instrumented systems is proposed. Proof test interval phase and proof test phase are modeled separately using dynamic Bayesian networks, and integrated together to form the MDBNs. The unified structure models of MDBNs for *k*-out-of-*n* architectures are constructed, and the procedures of automatic creation of conditional probability tables are developed. The target failure measures, that is, probability of failure on demand, average probability of failure on demand, probability of failing safely, average probability of failing safely, and SIL of safety instrumented systems operating in a low demand mode, are evaluated using the proposed MDBNs. The effects of time interval of MDBNs, common cause weight, imperfect proof test and repair on model precision are researched. User-friendly SIL determination software is developed by using MATLAB GUI to assist engineers in determining the SIL value.

1. Introduction

Safety has always been an important property in the context of modern industry, which requires designers to address these technical specification challenges to improve reliability, maintainability, and availability constraints. For example, a triple redundant control system is required for subsea blowout preventers to ensure the safety of offshore oil and gas industry [26]. A reliable reconfigurable real-time operating system is used for fault-tolerant traction systems in railway applications [27]. Moreover, redundant controllers, sensors, and actuators are needed for flight-critical distributed systems in avionics applications [28]. Functional safety is a new aspect of safety and is becoming increasingly important, particularly with the introduction of IEC 61508 [1], which is a standard for the functional safety of electrical/electronic/programmable electronic safety-related systems. The standard is regulated in different fields, and various standards such as IEC 61511 in process industry [2], IEC 61513 in nuclear power plants [29], IEC 62061 in machinery [30], EN 50129 in railway applications [31], and ISO 26262 in road vehicles [32] are issued. The safety integrity level (SIL) of a safety instrumented system (SIS) is determined by the risk reduction factor provided by the SIS to the equipment under control. With the assumption that the SIS prevents all risks, it is a measure of the likelihood of a failure of the SIS. For example, in IEC 61508, SIL is determined by average probability of failure on demand (PFD_{avg}) for low demand mode and probability of failure per hour (PFH) for high demand mode; in ISO 26262, SIL is determined by random hardware failure target values; and in EN 50129, SIL is determined by tolerable hazard rate (THR). IEC 61508 is the general and fundamental standard, and it proposes several semi-quantitative and quantitative methods for SIL determination, such as reliability block diagram, fault tree, Markov chain, Petri net, risk graph, layer of protection analysis (LOPA), and hazardous event severity matrix. However, several of these methods are complex and difficult to apply [3], whereas others have important limitations for complex SISs, including binary variable problems [4] and state space explosion problems [5].

Research on SIL determination has attracted considerable attention, and significant results can be found in literature. Kim et al. [6] proposed an evaluation method for hardware SIL determination by using hazard analysis and risk assessment and failure modes, effects and diagnostic analysis. Dutuit et al. [7] proposed an evaluation method of PFD in relationship with SILs of SISs by introducing distributions for periodically tested components into fault tree models. Chang et al. [8] proposed a SIL determination procedure for risk graph method, Minimum SIL Table from OLF 070 and LOPA accounting for uncertainties. Khalil et al. [9] proposed a

* Corresponding author at: College of Mechanical and Electronic Engineering, China University of Petroleum, Qingdao, Shandong 266580, China. Tel.: +852 52264360/86 53286983500 8701.
E-mail addresses: caibaoping@upc.edu.cn, baoping.cai@cityu.edu.hk (B. Cai), lyu.12@my.cityu.edu.hk (Y. Liu).

http://dx.doi.org/10.1016/j.ress.2016.01.018
0951-8320/

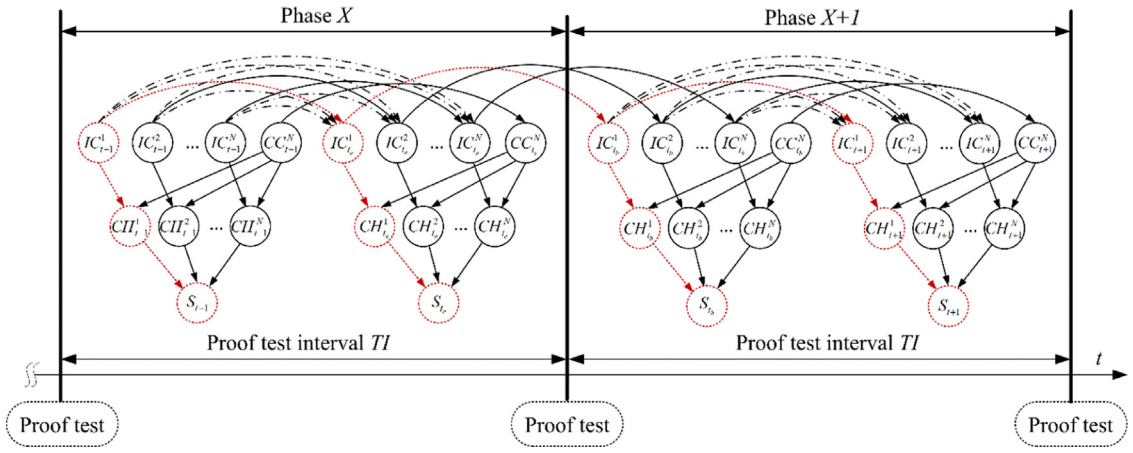

Fig. 1. Schematic diagram of MDBNs for SIL determination.

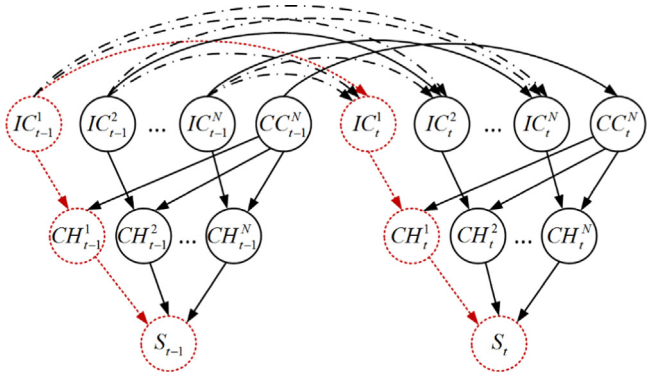

Fig. 2. DBNs for proof test interval phase.

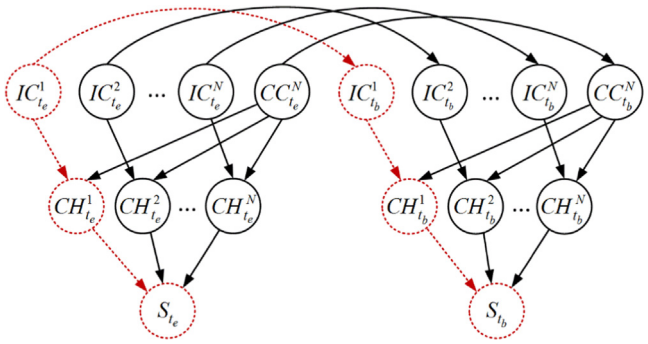

Fig. 3. DBNs for proof test phase.

cascaded fuzzy-LOPA model for SIL determination for certain hazardous scenarios in natural gas industry. Mechri et al. [10] proposed a holistic method for modeling the unavailability of SISs by using switching Markov chain and researching on the influences of several parameters on the performance of SISs, such as common cause failure, and imperfect proof testing. Ding et al. [11] proposed an approach for SIL determination based on system degradation by using reliability block diagram. Nait-Said et al. [12,13] proposed several modified risk graph methods to improve flexibility and reduce the subjective uncertainty. Shu et al. [14] proposed a simplified method for SIL determination for complex SISs by conducting Markov analysis on each channel and combining the results. Sallak et al. [15] proposed a fuzzy probabilistic method for SIL determination of SISs considering the uncertainty of failure rates of SIS components. Jahanian [23] conducted a detailed analysis and derived a generalized form of PFD formula for *K*-out-of-*M* (KooM) systems using the same makeup of PFD elements utilized by IEC 61508 standards. Ouache et al. [35] proposed a three-step mathematical model to compute the PFD of SISs and used Bowtie method to conduct the safety analysis of several scenarios by determining the PFD of safeguards. Innal et al. [36] established generic analytical formulations for the assessment of SIS performance in terms of safety integrity and operational integrity.

On another active research frontier, Bayesian networks (BNs) and dynamic Bayesian networks (DBNs) have attracted considerable attention in the field of system reliability, safety and risk evaluation. In recent years, they have been applied to study the reliability of various systems. Tsilipanos et al. [16] proposed a system of systems framework for the reliability evaluation of telecommunication networks based on a combination of hazard analysis techniques along with the BN model and sensitivity analysis. Doguc et al. [17] proposed an automated approach for the reliability assessment of grid systems by using BNs, which require no prior information of the grid system structure. Jiang et al. [18] proposed a BN-based probabilistic model, named hybrid relation model, for the reliability evaluation of programmable logic controller systems. Zhang et al. [19] proposed a fuzzy-BN-based systemic decision support method for safety risk analysis under uncertainty in tunnel construction. Daemi et al. [13,20] proposed a BN-based reliability evaluation method for composite power systems with emphasis on the importance of degree sequence of components in consideration of load variation and weather conditions. Baraldi et al. [39] applied BNs to handle the uncertainty problems of human reliability analysis and compare it with fuzzy expert system. O'Connor et al. [40] proposed a general dependency model (GDM) that used BNs to model the probabilistic dependencies between components for analysis of common causes and dependent failures in system risk and reliability assessments. Cai et al. [21,37,38] proposed BN-based reliability evaluation methods in consideration of common cause failure, imperfect coverage and intermittent faults, and DBN-based real-time reliability evaluation methodology for industrial systems. Ramírez et al. [22] proposed DBN-based evaluation method of life extension for ageing repairable systems. Flammini et al. [33] presented both a failure model for KooM systems based on BNs and a maintenance model based on continuous time Markov chains, which were combined according to a compositional multiformalism modeling approach to analyze the effect of imperfect maintenance on system safety. Moreover, the researchers proposed a BN-based method to evaluate the trustworthiness of 2oo3 decision fusion mechanisms in multi-sensor applications [41]. Weber et al. [34] applied BNs on circular and linear typical consecutive KooM: F system to estimate