Application of Bayesian Networks to Reliability Evaluation of Software System for Subsea Blowout Preventers

Baoping Cai, Yonghong Liu, Qian Fan and Yunwei Zhang

College of Mechanical and Electronic Engineering, China University of Petroleum, Qingdao, Shandong 266580, China
caibaoping987@163.com, liuyhupc@163.com, fanqian_upc@126.com, zhangyw1989@163.com

Abstract

The work develops a redundant software system for subsea blowout preventers, including control logics, human-machine interface (HMI) programs, remote access and redundant databases in order to meet the high reliability requirement of subsea drilling. The Bayesian networks (BN) for control logics, HMI programs and redundant databases are built and then the whole BN are established. The quantitative reliability evaluation is performed by using Netica software. The probability of software failure is evaluated via forward analysis, and the posterior probability given the failure is evaluated via backward analysis. The mutual information is researched in order to assess the important degree of basic events. The results show that the probability of software failure is 0.04%, which can meet the requirement of subsea drilling. The triple common cause failure should be paid more attention in order to improve the software performance. In addition, the control logics have the most important influences on software safety; the HMI programs have the least important influences; and the redundant databases are in between.

Key Words: *Software; Reliability; Bayesian networks; Subsea blowout preventers*

1. Introduction

Subsea blowout preventer (BOP) stack plays an extremely important role in providing safe working conditions for the drilling activities in 10000 ft ultra-deepwater region. Programmable logic controller (PLC) based triple modular redundancy system GE Fanuc Genius modular redundancy (GMR) is chosen to provide supervisory control and data acquisition due to the fact that the system can provide the tolerance against single component failures [1]. The operations of subsea BOP stack are performed totally by the software systems, including control logics, human-machine interface (HMI) programs, remote access and redundant databases. The reliability of control software is of vital importance to the safety of subsea operations.

The reliability of subsea BOP stacks for deepwater applications was evaluated using fault tree method [2, 3]. The system safety of well control equipment including BOP and hydraulic control systems was studied using failure modes and effects analysis and fault tree methods [4]. The performance of subsea BOP control systems and stacks with common-cause failures was evaluated by merging the independent Markov models with the Kronecker product approach [5, 6].

Recently, Bayesian networks (BN) are more and more used in reliability analysis due to the fact that the model can perform forward or predictive analysis as well as backward or diagnostic analysis. In predictive analysis, the probability of occurrence of any node is calculated on the basis of the prior probabilities of the root nodes and the conditional dependence of each node. In diagnostic analysis, the posterior probability of any given set of variables is calculated given some observation (the evidence), represented as instantiation of some of the variables to one of their admissible values [7-9]. The reliabilities of subsea BOP control systems including triple modular redundancy control system and double dual modular redundancy control system are evaluated by using BN models, taking into account common cause failure and imperfect coverage [10].

This work aims to research the reliability of software system for subsea BOP by using BN models. The paper is structured as follows: Section 2 describes software modules of subsea BOP. Section 3 presents the BN models for reliability analysis. Section 4 gives the analysis results. Section 5 summarized the paper.

2. Software Development

2.1. Subsea BOP Control System

A typical architecture of subsea BOP control system is shown in Figure 1. A triple GMR system, consisting of three Series 90-70 PLCs, is the kernel of the multiplex control system. Driller's computer, toolpusher's computer and work station provide for full control of the subsea BOP stack functions, and serves as primary, secondary and third control station, respectively. The three stations run the user-friendly HMI programs which are full of useful graphics and report tools. The database servers, virtual private network (VPN) server and control stations are connected to the PLCs via dual redundant Ethernet. Dual Ethernet cards run in each device. The PLCs are connected to blue and yellow subsea electronic modules (SEM) via Genius Bus. The two SEMs contain two sets of independent input and output subsystems. They control the blue pod and yellow pod, respectively. The VPN server is connected to Internet network through a third Ethernet card. The authorized operators in engineering offices, who has tunnel name, tunnel password, user name and user passwords, are permitted to remotely access the subsea BOP control processes through the VPN.

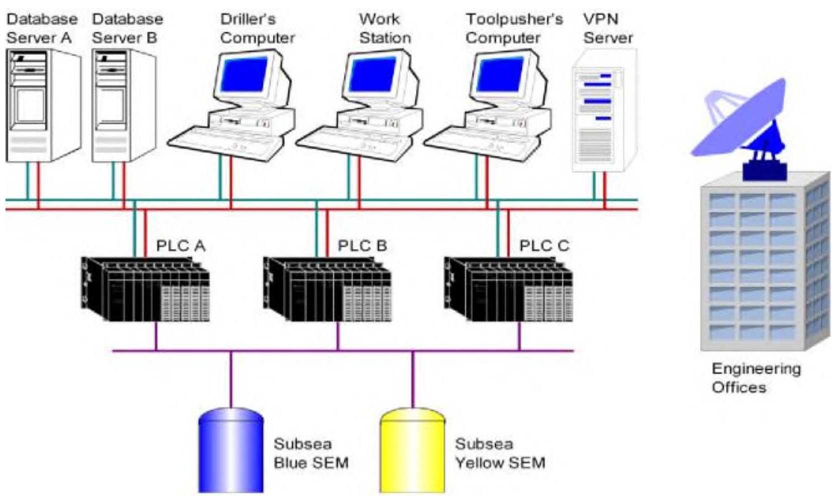


Figure 1. Architecture of Subsea BOP Control System

2.2. Control Logics

The control logics are developed using ladder language in Proficy Machine Edition Logic Developer (v.5.90), and all of the logics are downloaded to the three redundant PLCs. The control logics of subsea BOP system can work when at least one set of the logics works. Therefore, the three sets of control logics can be considered as parallel. The main logics are shown in Figure 2. The driller, toolpusher and manager can monitor and control the subsea BOP stack system with HMI programs running in driller's computer, toolpusher's computer and work station, respectively. It is developed using the Proficy Cimplicity HMI/SCADA (v. 7.50) software. It is similar to control logics that, the operators can control the subsea BOP when at least one set of HMI programs work. Therefore, the three sets of HMI programs can also be considered as parallel.

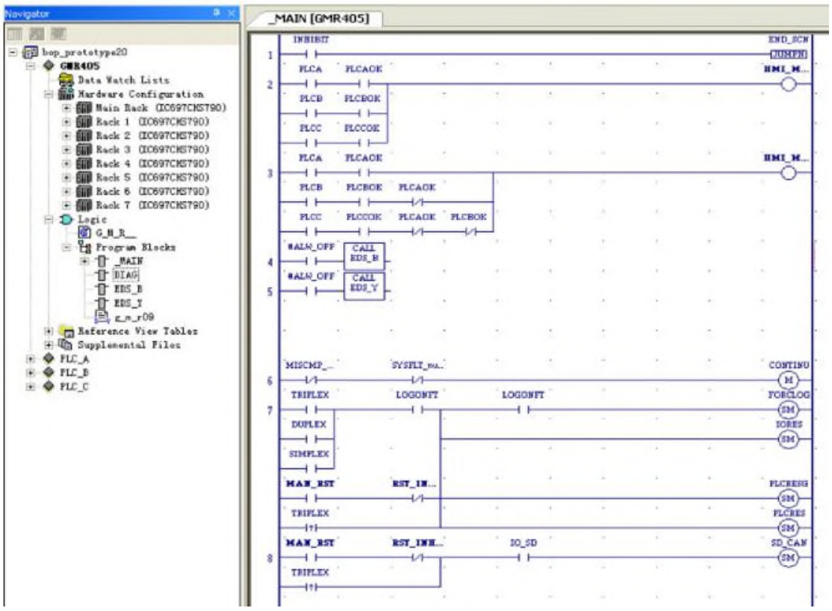


Figure 2. Main Logics of BOP Control System

2.3. HMI Programs and Remote Access

The driller, toolpusher and manager can monitor and control the subsea BOP stack system with HMI programs running in driller's computer, toolpusher's computer and work station, respectively. It is developed using the Proficy Cimplicity HMI/SCADA (v. 7.50) software. It is similar to control logics that, the operators can control the subsea BOP when at least one set of HMI programs work. Therefore, the three sets of HMI programs can also be considered as parallel.

The WebView function of Cimplicity HMI/SCADA makes authorized users can remotely view read-only points and alarm data for the project that is broadcasted to the web server through Internet. The broadcast session provides the means to broadcast a Cimplicity WebView screen to an unlimited number of users who can view it from remote locations. Therefore, the engineers in engineering offices can monitor the states and data of subsea

BOP system remotely. For example, the alarm list screen of subsea BOP stack can be read through Internet by using IE browser [1], as shown in Figure 3.

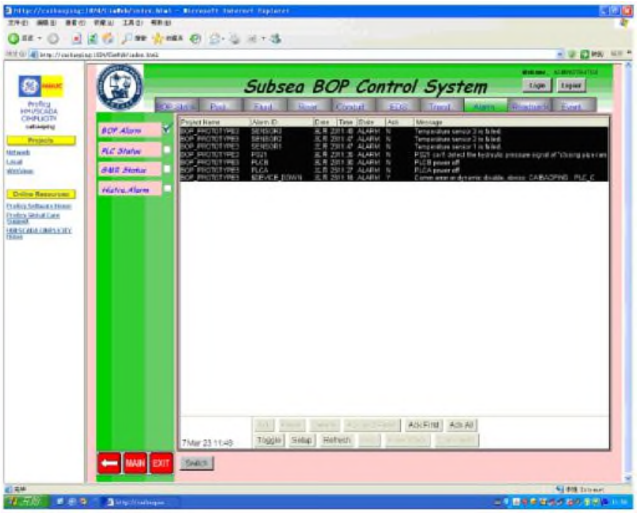


Figure 3. Remote-accessed Alarm List Screen of Subsea BOP

Stack 2.4. Redundant Databases

All the vital information during the drilling should be saved in the database, which is created using Microsoft SQL Server 2003. The database redundant servers involving a primary monitoring server and a secondary “Hot Standby” server are configured using Cimplicity server redundancy function within the Workbench on the primary server. Each primary server has one secondary server, and it is essentially a mirror image of the primary server. The operator accesses the database of primary server normally. Upon detection of failure of the primary server, the secondary server can assume control of data collection automatically, and allow user access with minimal loss of continuity. When the primary server comes back on line, control can be transferred back, and the secondary server will resume its backup role, as shown in Figure 4. Obviously, the two databases can be also considered as parallel.

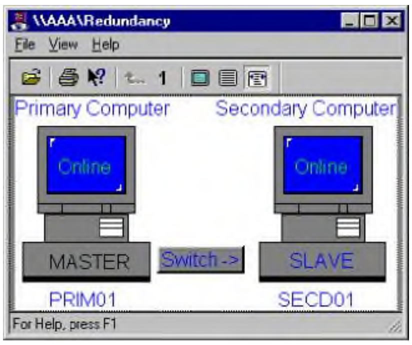


Figure 4. Database Redundancy Servers

The field data and alarms detected by system softwares are transmitted to database redundant servers via open database connectivity (ODBC), in order to share the information and generate report forms. Three information including event, alarm and data shown in Figure 5 are saved. The events such as log in, log out, logic download and alarm revision should be saved, the alarm such as BOP alarm, PLC alarm and GMR alarm should be saved, and the important data including pressure, temperature and flow rate should also be saved in database.

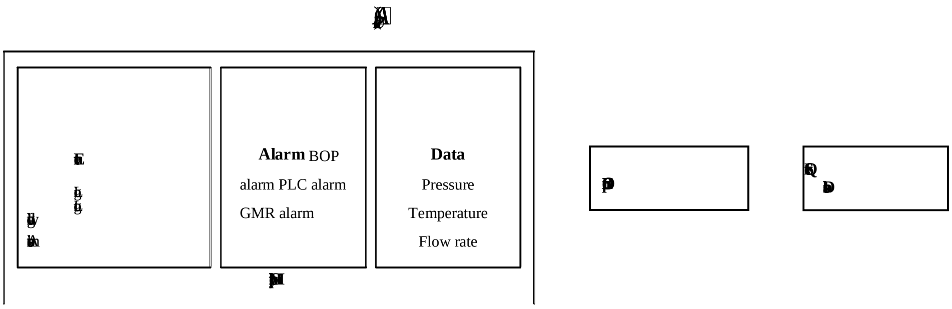


Figure 5. Database Logger Relationships

(| ( ))

3. BN Modeling for Reliability Analysis

3.1. Overview of Bayesian Networks

A Bayesian network is a directed acyclic graph (DAG) in which the nodes represent the system variables and the arcs symbolize the dependencies or the cause-effect relationships among the variables. The DAG represents the structure of causal dependence between nodes and gives the qualitative part of causal reasoning, thus the relations between variables and the corresponding states give the quantitative part, consisting of a conditional probabilistic table (CPT) attached to each node with parents [11].

According to the conditional independence and chain rule, the joint probability distribution of a set of variables $U=\{A_1, A_2,..., A_n\}$ can be determined by

n

E

(1)

where $Pa(A_i)$ are the parents of A_i in the Bayesian networks [12].

The probability distribution of a particular variable can be found by marginalizing the joint probability distribution with respect to the variable. This calculation is called marginalization, which can be used to compute the reliability of systems.

Given the observation of another set of variables E called *evidence*, the posterior probability distribution of a particular variable can be computed by using different classes of inference algorithms such as junction tree or variable elimination based on *Bayes' theorem* as [13].

(2)

The important degree of basic event to the system failure can be assessed by using Shannon's mutual information (entropy reduction), which is one of the most widely used measurement for ranking information sources [14]. It is assumed that uncertainty of system can be represented by entropy function as given

(3)

where $P(t)$ is the probability distribution of random variable T.

The mutual information is the total uncertainty-reducing potential of X, given the original uncertainty in T prior to consulting X. Intuitively, mutual information measures the information that T and X share: it measures how much knowing one of these variables reduces our uncertainty about the other [15]. The mutual information of T and X is given by

(4)

where $P(t, x)$ is the joint probability distribution function of T and X, and $P(t)$ and $P(x)$ are the marginal probability distribution functions of T and X, respectively.

3.2. BN Modeling for Software System

3.2.1. BN Modeling for Control Logics: For the redundant software, common cause failure (CCF) has significant influences on the software performance. CCF is defined as the failure of more than one hardware or software due to the same cause for redundant systems. Experience has shown that it has a dominant impact on accidents [16]. In the BN shown in Figure 6, different sources of shock are distinguished to model CCF of control logics. A shock from source A destroys logic A, a shock from source AB destroys logics A and B, and a shock from source ABC destroys logic A, B and C. Therefore, failure of logic A is the series of source A, AB and ABC. The system state of whole logics is the parallel of logics A, B and C due to the redundancy. The conditional probability tables are given in Figure 5. It is noted that the values of 1 and 0 denote the logic failure and logic working, respectively. The prior probabilities of logic shocks from sources are obtained based on the experience of operators.

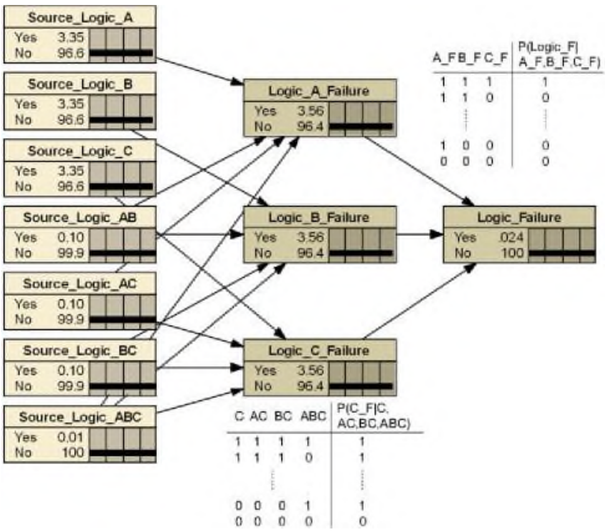


Figure 6. BN Modeling of Control Logics

3.2.2. BN Modeling for HMI Programs: The BN of HMI programs are similar to control logics except that they have different prior probabilities, as shown in Figure 7. This is because both of control logics and HMI programs have triple redundant software structures as described above. Obviously, HMI programs have lower prior probabilities than control logics. Therefore, the failure probability of HMI programs (0.006%) is lower than that of control logics (0.024%).

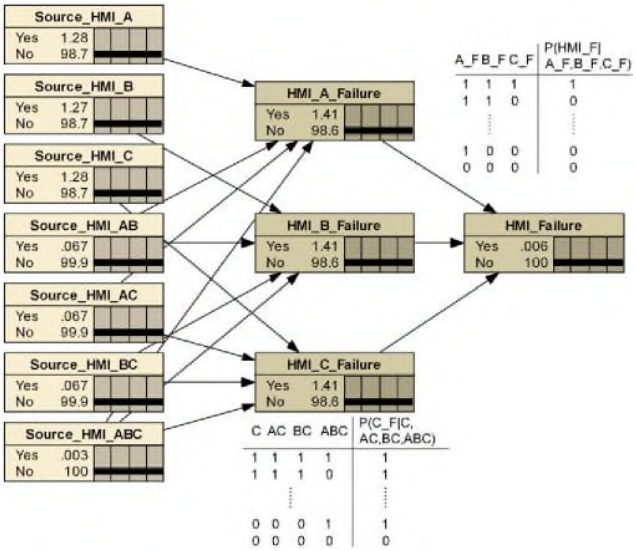


Figure 7. BN Modeling of HMI Programs

3.2.3. BN Modeling for Redundant Databases: The BN of redundant databases are shown in Figure 8. Although the failure of redundant databases has less influence on the safety of subsea drilling than control logics and HMI programs, the whole software is considered to be failed, once the redundant databases are failed, due to the fact that the control logics, HMI programs and redundant databases are integrated into a whole.

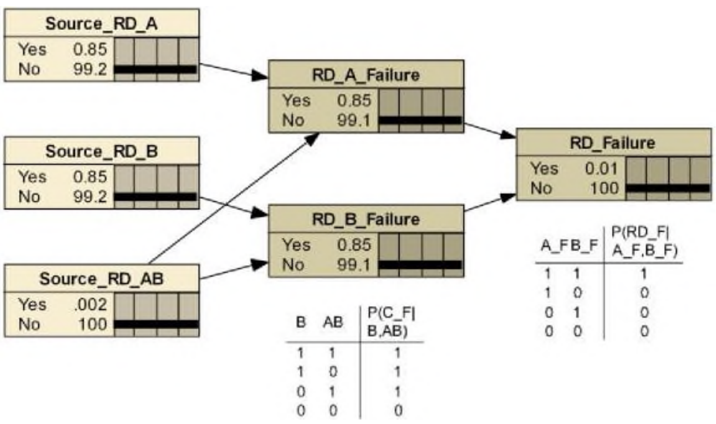


Figure 8. BN Modeling of Redundant Databases

3.2.4. The whole BN: According to the description above, either of the control logics, HMI programs and redundant databases is failed, the whole software is failed. Therefore, the three parts can be considered to be series. Subsequently, the whole BN is established, as shown in Figure 9.

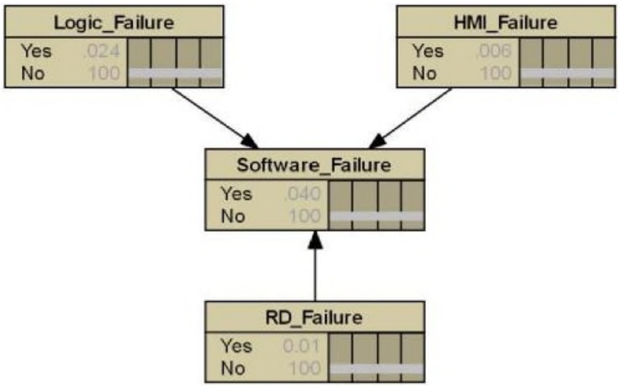


Figure 9. BN Modeling of Whole System

3.3. Reliability Evaluation

The quantitative reliability assessments of system software are performed using Netica software [17]. The software reliability can be evaluated via forward analysis, and the posterior probability for each event given the software failure is evaluated via backward analysis. The mutual information is also researched in order to assess the important degree of each event.

3.4. Validation of Modeling

Validation is an important aspect of a proposed model because it provides a reasonable amount of confidence to the results of the model. Several approaches are applied appropriately to the different aspects of a particular model, including sensitivity analysis, response analysis, response surface modeling, and external validation [18]. In order to carry out a full validation of the model the parameters used would need to be closely monitored for a long period to time. For the subsea BOP control system, it is obviously an impractical exercise. In the current work, a three-axioms-based sensitivity analysis method is therefore used for partial validation of the proposed DBN modeling. The following three axioms should be satisfied [19].

(1) A slight increase/decrease in the prior subjective probabilities of each parent node should certainly result in the effect of a relative increase/decrease of the posterior probabilities of child nodes;

(2) Given the variation of subjective probability distributions of each parent node, its influence magnitude to child node values should keep consistent;

(3) The total influence magnitudes of the combination of the probability variations from x attributes on the values should be always greater than the one from the set of x-y (y∈x) attributes.

4. Results and Discussions

4.1. Probability of Software Failure

The graphical representation of software failure with prior probabilities is shown in Figure 10(a). It can be seen that the probability of software failure is only 0.04%. The posterior probabilities of all the events given the software failure are shown in Figure 10(b), and the values are given in the 5th column of Table 1.

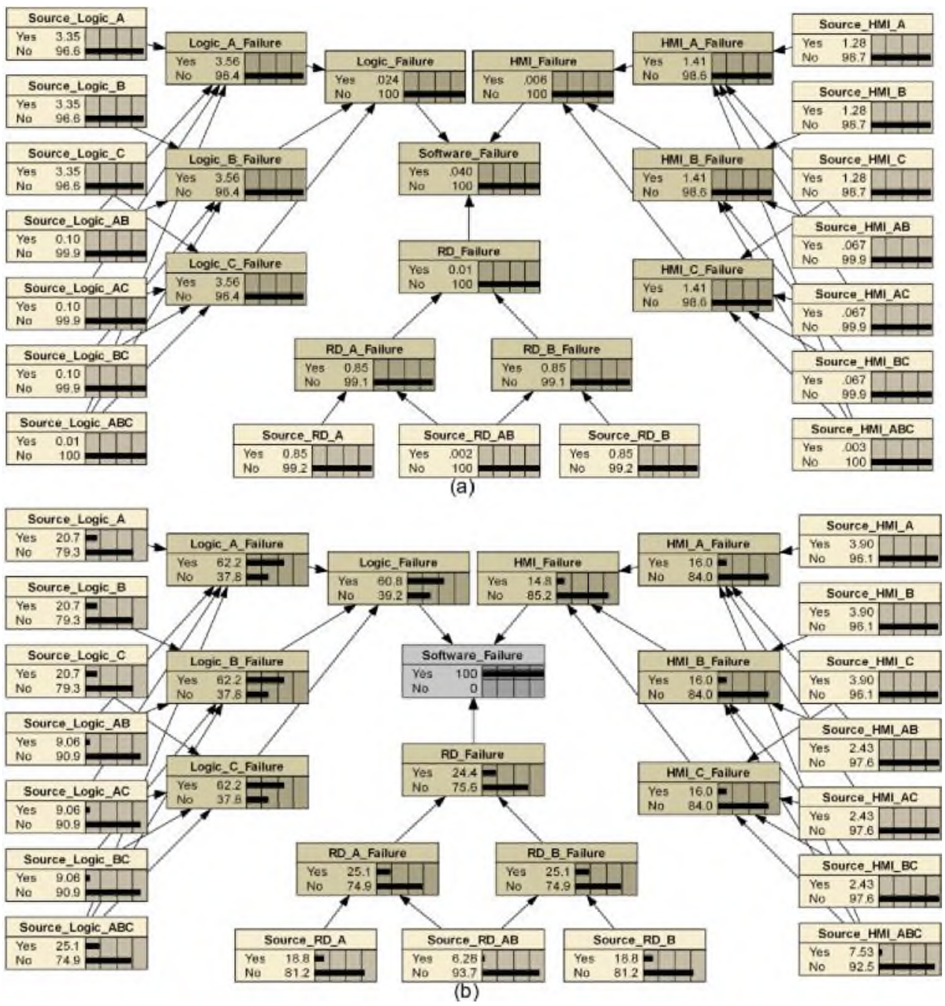


Figure 10. Graphical Representations of (a) Software Failure with Prior Probabilities and (b) Posterior Probability Given Software Failure

Table 1. Basic Events of Software Failure for Subsea BOP System

Software Modules	*Number*	*Basic Events*	*Prior Probability*	*Posterior Probability*
Control logics	C1	S_Logic_A(B,C)	3.35%	20.70%
	C2	S_Logic_AB(AC,BC)	0.10%	9.06%
	C3	S_Logic_ABC	0.01%	25.10%
HMI programs	H1	S_HMI_A(B,C)	1.28%	3.90%
	H2	S_HMI_AB(AC,BC)	0.07%	2.43%
	H3	S_HMI_ABC	0.00%	7.53%
Redundant databases	R1	S_RD_A(B)	0.85%	18.80%
	R2	S_RD_AB	0.00%	6.28%

4.2. Mutual Information Investigation

The individual contribution of each basic event to the software failure is described using mutual information, as shown in Figure 11. As indicated, "Source of logic ABC", "Source of logic A (B, C)", "Source of HMI ABC" and "Source of redundant database AB" have significant influences on the probability of whole software failure. Therefore, the triple CCF for all of control logics, HMI programs and redundant database should be paid more attention to improve the software system reliability.

The average values of mutual information for control logics, HMI programs and redundant databases are 7.6×10-4, 1.2×10-4 and 2.5×10-4, respectively. Obviously, the control logics have the most important influences on software safety; the HMI programs have the least important influences; and the redundant databases are in between. Therefore, the control logics should be paid more attention when developing the software for subsea BOP system.

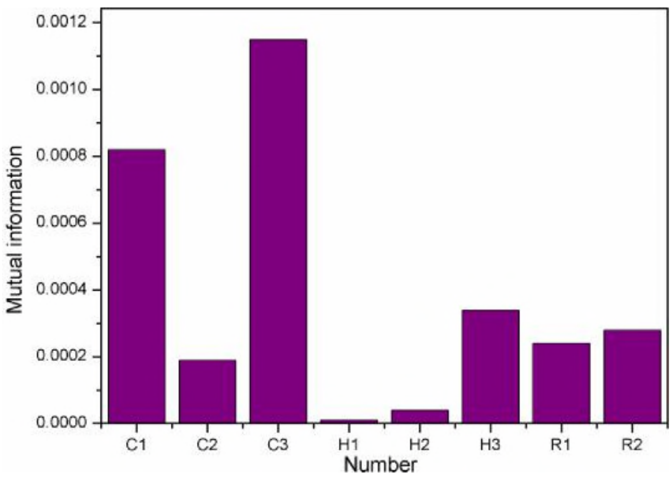


Figure 11. Mutual Information of Basic Events and "Software Failure"

4.3. Validation of the Model

Validation is an important task of demonstrating that the model is a reasonable representation of an actual system. A sensitivity analysis has been carried out in order to give a partial validation of the model. The model should at least satisfy the three axioms described in Section 3.4. Taking the child nodes of Logic_A_Failure shown in Figure 10 for example, when the state Yes of Source_Logic_A is set to 50% from 3.35%, the failure probability of software system increases to 0.14% from 0.04%. When both the change plus the state Yes of Source_Logic_AB are set to 50%, the failure probability of software system increases to 1.85%. When the two changes above plus the state Yes of Source_Logic_AC are set to 50%, the failure probability of software system increases to 26.8%. Finally, when the state Yes of last parent node Source_Logic_ABC is set to 50%, the failure probability of software system increases to 63.4%. The exercise of increasing each influencing node satisfies the axioms, thus giving a partial validation to the model.

5. Conclusions

A redundant software system for subsea BOP is developed, and the control logics, HMI programs, remote access and redundant databases are described. The BN of software system are established and the quantitative reliability assessments are performed.

(1) The probability of software failure for subsea BOP is 0.04%, which can meet the requirement of subsea drilling.

(2) The triple CCF for all of control logics, HMI programs and redundant database should be paid more attention in order to improve the software performance.

(3) The control logics have the most important influences on software safety; the HMI programs have the least important influences; and the redundant databases are in between.

(4) The sensitivity analysis partially validate the proposed DBN modeling is correct and rational.

Acknowledgments

This paper is a revised and expanded version of a paper entitled "Reliability research of software system for subsea blowout preventers" presented at the 1st International Conference on Software Technology in Cebu, Philippines on May 29-31, 2012.

The authors wish to acknowledge the financial support of the National High-Technology Research and Development Program of China (No.2007AA09A101), National Natural Science Foundation of China (No.50874115), Program for Changjiang Scholars and Innovative Research Team in University (IRT1086), Taishan Scholar Project of Shandong Province (TS20110823), Science and Technology Development Project of Shandong Province (2011GHY11520) and Incubation Programme of Excellent Doctoral Dissertation of China University of Petroleum (No.2010–02).

References

[1] B. P. Cai, Y. H. Liu, Z. K. Liu, F. Wang, X. J. Tian, Y. Z. Zhang, "Development of an automatic subsea blowout preventer stack control system using PLC based SCADA", ISA Trans., vol. 51, **(2012)**, pp. 198–207.

[2] P. Holand, "Reliability of subsea BOP systems for deepwater application, Phase II DW", Project report STF38 A99426, **(1999)**.

[3] P, Holand, "Deepwater kicks and BOP performance", Project report STF38 A01419, **(2001)**.

[4] J. H. Fowler, J. R. Roche, "System safety analysis of well-control equipment", SPE Drill. Completion, vol. 3, **(1994)**, pp. 193–198.

[5] B. P. Cai, Y. H. Liu, Z. K. Liu, X. J. Tian, Y. Z. Zhang and J. Liu, "Performance evaluation of subsea blowout preventer systems with common-cause failures", J. Pet. Sci. Eng., vol. 90–91, **(2012)**, pp. 18–25.

[6] B. P. Cai, Y. H. Liu, Z. K. Liu, X. J. Tian, H. Li and C. K Ren, "Reliability analysis of subsea blowout preventer control systems subjected to multiple error shocks", J. Loss Prev. Process Ind., vol. 25, **(2012)**, pp.

1044–1054.
[7] A. Bobbio, L. Portinale, M. Minichino and E. Ciancamerla, "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks", Reliab. Eng. Syst. Saf., vol. 71, **(2001)**, pp. 249–260.
[8] F. Flammini, S. Marrone, N. Mazzocca and V. Vittorinni, "A new modeling approach to the safety evaluation of N-modular redundant computer systems in presence of imperfect maintenance", Reliab. Eng. Syst. Saf., vol. 94, **(2009)**, pp. 1422–1432.
[9] B. Langseth and L. Portinale, "Bayesian networks in reliability", Reliab. Eng. Syst. Saf., vol. 92, **(2007)**, pp. 92–108.
[10] B. P. Cai, Y. H. Liu, Z. K. Liu, X. J. Tian, X. Dong and S. L. Yu, "Using Bayesian networks in reliability evaluation for subsea blowout preventer control system", Reliab. Eng. Syst. Saf., vol. 108, **(2012)**, pp. 32–41.
[11] P. Trucco, E. Cagno, F. Ruggeri and O. Grande, "A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation", Reliab. Eng. Syst. Saf., vol. 93, **(2008)**, pp. 823–34.
[12] F. V. Jensen and T. D. Nielsen, "Bayesian networks and decision graphs. 2nd ed", Springer, NY, **(2007)**.
[13] A. Darwiche, "Modeling and reasoning with Bayesian networks", Cambridge University Press, New York, **(2009)**.
[14] J. Pearl, "Probabilistic reasoning in intelligent systems: networks of plausible inference", Morgan Kaufmann Publishers, San Francisco, **(1988)**.
[15] Y. F. Wang, S. F. Roohi, X. M. Hu, M. Xie, "Investigations of human and organizational factors in hazardous vapor accidents", J. Hazard. Mater., vol. 191, **(2011)**, pp. 69–82.
[16] V. M. Hoepfer, J. H. Saleh, K. B. Marais, "On the value of redundancy subject to common-cause failures: Toward the resolution of an on-going debate", Reliab. Eng. Syst. Saf., vol. 94, **(2009)**, pp. 1904–16.
[17] Netica, Norsys Software Corporation, Netica version 4.16, http://www.norsys.com, **(2010)**.
[18] S. Rathnayaka, F. Khan and P. Amyotte, "Accident modeling approach for safety assessment in an LNG processing facility", J. Loss Prev. Process Ind., vol. 25, **(2012)**, pp. 414–423.
[19] B. Jones, I. Jenkinson, Z. Yang and J. Wang, "The use of Bayesian network modelling for maintenance planning in a manufacturing industry", Reliab. Eng. Syst. Saf., vol. 95, **(2010)**, pp. 267–77.

Authors

Baoping Cai

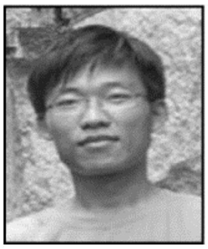
He was born in Hebei, China, in 1982. He received his B. S. and M. S. degree in Mechanical and Electronic Engineering from China University of Petroleum in 2006 and 2008 respectively. Currently, he is a Ph.D. candidate in Mechanical and Electronic Engineering in China University of Petroleum, China. His recent research interest is control system of subsea drilling equipments.

Yonghong Liu

He was born in Anhui, China, in 1965. He received his Ph.D. degree in Mechanical Manufacture from Harbin Institute of Technology, Harbin, China, in 1996.

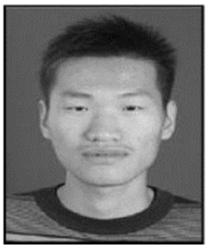
He is currently a professor and doctoral supervisor in College of Mechanical and Electronic, China University of Petroleum, China. He has published over 120 papers in some international or national journals and conferences. His current research interests include EDM of ceramics, expansion sand screen for sand control and control system of subsea drilling equipments. He is a member of China Nontraditional Machining Committee and Nontraditional Machining

Association of Shandong Province. He is Prominent Young and Middle-aged Specialist of Shandong Province and selected in New Century National Hundred, Thousand and Ten Thousand Talent Project.



Qian Fan

He was born in Shandong, China, in 1989. He received his B. S. degree in Mechanical engineering and automation from China University of Petroleum in 2012. Currently, he is a Master degree candidate in Mechanical and Electronic Engineering in China University of Petroleum, China. His recent research interest is diagnosis system of subsea drilling equipments.



Yunwei Zhang

He was born in Shandong, China, in 1989. He received his B. S. degree in Mechanical engineering and automation from China University of Petroleum in 2012. Currently, he is a Master degree candidate in Mechanical and Electronic Engineering in China University of Petroleum, China. His recent research interest is testing system of subsea drilling equipments.