Reliability Research of Software System for Subsea Blowout Preventers

Baoping Cai, Yonghong Liu, Zengkai Liu, Xiaojie Tian, Shilin Yu

College of Mechanical and Electronic Engineering, China University of Petroleum,
Dongying, Shandong 257061, China
caibaoping987@163.com; liuyhupc@126.com; liuzengk@163.com;
tianxj20050101@163.com; yushilin1988@sina.com

Abstract. In order to meet a high reliability requirement of subsea drilling, a redundant software system for subsea Blowout Preventers (BOP), including control logics, HMI programs, remote access and redundant databases are developed. The Bayesian networks for control logics, HMI programs and redundant databases are built and then the whole Bayesian networks are established. The quantitative reliability assessments are performed by using Netica software. 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.

Keywords: 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 [1]. 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 [2]. 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.

Recently, Bayesian networks are more and more used in performance assessment of software, due to the fact that the model can perform forward or predictive analysis as well as backward or diagnostic analysis [3]. This work aims to research the reliability of software system for subsea BOP by using Bayesian network models. The paper is structured as follows: Section 2 describes software modules of subsea BOP, including control logics, Human-Machine Interface (HMI) programs, remote access and redundant databases. Section 3 presents the Bayesian networks models for reliability analysis. Section 4 gives the analysis results. And 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 Fig. 1. A triple GMR system, consisting of three Series 90-70 PLCs, is the kernel of the multiplex control system, which runs the control logics for subsea functions. 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.

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 Fig. 2. The first three rungs of control logics, when activated, ensure that only one PLC communicates with the HMI programs. The submodules of control logics, such as Emergency Disconnect System (EDS) modules given in fourth and fifth rungs, can be added subsequently.

2.3 HMI programs and remote access

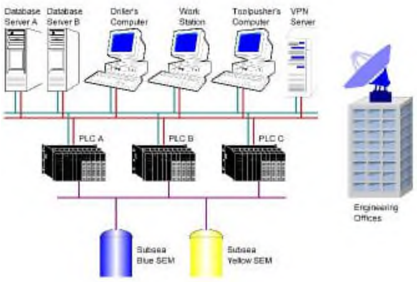
The driller, toolpusher and manager can monitor and control the subsea BOP stack system with HMI programs running in driller's computer, toolpusher's computer and work station, respectively. It is developed using the Proficy Cimplicity HMI/SCADA (v. 7.50) software. It is similar to control logics that, 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 subsea BOP stack screen and readback screen can be read through Internet by using IE browser.

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 secondary server can not be a primary configuration node, and does not support any configuration functions.

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. Obviously, the two databases can be also considered as parallel.



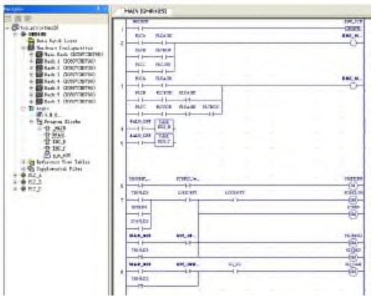


Fig. 1. Architecture of subsea BOP control system Fig. 2. Main logics of BOP control system

3 Bayesian networks modelling for reliability analysis

3.1 Bayesian networks modelling 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 [4]. In the Bayesian network shown in Fig. 4, 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 Fig. 4. 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.

3.2 Bayesian networks modelling for HMI programs

The Bayesian networks of HMI programs are similar to control logics except that they have different prior probabilities, as shown in Fig. 5. 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%).

3.3 Bayesian networks modelling for redundant databases

The Bayesian networks of redundant databases are shown in Fig. 6. 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.

3.4 The whole Bayesian networks

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. After establishing the whole Bayesian networks, the quantitative reliability assessments of subsea BOP software are performed using Netica software. 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.

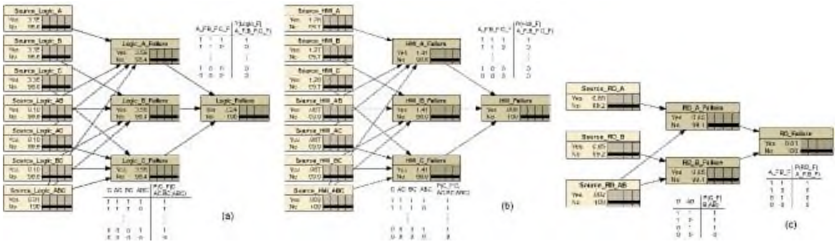


Fig. 3. Bayesian networks for (a) Control logics, (b) HMI programs, and (c) redundant databases

4 Results and discussions

The graphical representation of software failure with prior probabilities is shown in Fig. 7(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 Fig. 7(b), and the values are given in the 4th column of Table 1.

The mutual information and important degree sequence of all the parent nodes and the child node “Software failure” are given in the 5th and 6th columns of Table 1. It can be seen that “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 when developing and running the software.

The average values of mutual information and important degree sequence for each category of software are shown in 7th of Table 1. It can be seen that 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.

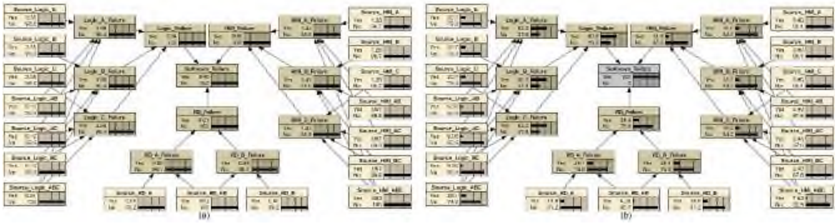


Fig. 4 Graphical representations of (a) Software failure with prior probabilities and (b) Posterior probability given software failure

Table 1. Mutual information of prior and posterior probabilities for each event

Events Modules	*Software*	*Prior Pro.*	*Posterior Pro.*	*Mutual Inform.*	*Imp. Deg.*	*Average value of MI*	*Imp. Deg.*
Control logics	S_Logic_A(B,C)	3.35%	20.70%	0.00082	2	0.00076	1
	S_Logic_AB(AC,BC)	0.10%	9.06%	0.00019	6		
	S_Logic_ABC	0.01%	25.10%	0.00115	1		
HMI programs	S_HMI_A(B,C)	1.28%	3.90%	0.00001	8	0.00012	3
	S_HMI_AB(AC,BC)	0.07%	2.43%	0.00004	7		
	S HMI ABC	0.00%	7.53%	0.00034	3		
Redundant databases	S_RD_A(B)	0.85%	18.80%	0.00024	5	0.00025	2
	S_RD_AB	0.00%	6.28%	0.00028	4		

5 Conclusions

A redundant software system for subsea BOP is developed, and the control logics, HMI programs, remote access and redundant databases are described in detail. The Bayesian networks for 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.

References

1. API 16D.: Specification for Control Systems for Drilling Well Control Equipment and Control Systems for Diverter Equipment. 2nd ed. API, Washington, DC (2004)
2. Cai, B., Liu, Y., Liu, Z., Wang, F., Tian, X., Zhang, Y.: Development of An Automatic Subsea Blowout Preventer Stack Control System Using PLC Based SCADA. ISA Trans. 51, 198--207 (2012)
3. Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E.: Improving the Analysis of Dependable Systems by Mapping Fault Trees into Bayesian Networks. Reliab. Eng. Syst. Saf. 71, 249--260 (2001)
4. Hoepfer, V.M., Saleh, J.H., Marais, K.B.: On the Value of Redundancy Subject to Common-Cause Failures. Reliab. Eng. Syst. Saf. 94, 1904--1916 (2009)