Research on the evaluation model of the software reliability for nuclear safety class digital instrumentation and control system

CHI Miao[1], and YANG Ming[2]

1. School of Economics & Management, Harbin Engineering University, 150001, P.R.China (chimiao@hrbeu.edu.cn)
2. College of Nuclear Science & Technology, Harbin Engineering University, 150001, P.R.China

Abstract: The method of evaluating software reliability (SR) of nuclear safety class digital instrumentation and control system (I&C) is investigated by reviewing international software design standards in order to build up the framework of the relevant standards. As the result of review of the NRC NUREG-0800 requirements it is first found out that the Digital I&C software standards should follow Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants (NUREG-0800 BTP7-14). Secondly, the quantitative evaluation models of SR should be constituted by using Bayesian Belief Network (BBN) to establish thirteen sub-model frameworks. Thirdly, each sub-models and the weight of corresponding indexes in the evaluation model are analyzed based on BBN. Finally the safety case was introduced. The reduced models are expected to lay a foundation for review and quantitative evaluation on the SR in nuclear safety class digital I&C.
Key words: safety class digital I&C system; software reliability; technical standard; Bayesian Belief Network

1 Introduction

Digital instrumentation and control (I&C) system being the nerve center of nuclear power plants, the performance of digital I&C system is greatly relevant to the safety and economy features of nuclear power plant[1]. Therefore, the nuclear industry has been raising an increased demand for safety and reliability of digital I&C system, where assessment on the reliability of nuclear safety class software becomes particularly important. Fukushima Daiichi accident in March 2011 sounded alarm bell to quicken the progress of the study.

This paper reviews international software design standards and establishes an evaluation model for the software reliability in nuclear safety class system. And this paper also presents interim results of on-going international joint research activities under the call of FP7-Fission-2010: Reliability and V&V of Nuclear Safety I&C Software (RAVONSICS). RAVONSICS tackles the problems of software reliability using Bayesian approaches that take into consideration all the information available, in particular evidence obtained by verification and validation (V&V).

2 General framework of software reliability by BBN

Received date: December 15, 2013
(Revised date: December 24, 2013)

BBN is a general model for probabilistic inference so that the conditional dependences between the random variables are presented in a directed acyclic graph. In the RAVONSICS context, the random variables are reliability claims related to the software and various pieces of evidence available for reliability assessment. BBNs have been suggested for software reliability estimation in several references by modeling features [2-5].The authors proposed an Evaluation Model of the Software Reliability in Nuclear Safety Class System.

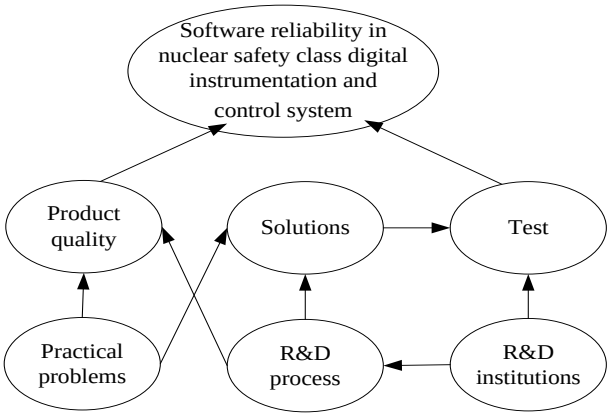


Fig. 1 Evaluation model of software reliability in nuclear safety class system.

The proposed model in Fig. 1 can be interpreted as to be composed by three parts: features part, practical problems part, and test part. The features part is to describe certain aspects of R&D institutions, R&D process, product quality and solutions to give influence software reliability. The nuclear safety class SR is influenced fundamentally by research

institutions and practical problems that need to be developed and measured. The features of R&D institutions influence the whole research process, and practical problems parts affect product quality and solutions, while the test part is determined by the research institutions' preparation for tests and the solutions.

As for the features part which affects the software reliability in nuclear safety class system, it is required to identify the differences between the features of software and the features of the relation between software and the environment. The features of software include the four types as described in the followings:

(1) The features of research institutions: reputation and experience of research institutions, warranty policy and the staff qualification.

(2) The features of research process: a high quality R&D process indicates that the software designing process is based on excellent software engineering experience. Besides, each R&D stage has archived files in integrity, consistency and traceability of the system.

(3) The features of product quality: the features of ultimate software product, such as reliability, simplicity, verifiability, and so on.

(4) The features of solutions: all activities about software development and validation, including examining model specifications, verifying documents and static analysis of code and testing system.

According to Shen, *et al*[6]. the modeling steps of the software reliability in nuclear safety class system to construct BBN are as shown in Fig. 2. The major steps of the modeling software reliability by BBN are as follows:

(1) Problem definition: the intermediate node among the target node "software reliability in nuclear safety class system", the basic nodes "practical problems part" and "research institutions" and other nodes in the network need to be identified.

(2) Establishing a network structure: based on experience or quantitative analysis techniques, establish a directed acyclic graph which describes qualitatively influencing relations of the effects of various factors Xs on a certain evaluation item Y.

(3) Definition of nodes probability table: to calculate the apriori probabilities of various nodes and to establish nodes probability table of the BBN based on experts experience and historical records. This is a quantitative description process of the influencing relationship among various nodes.

(4) Verifying BBN: to make predictions based on the established network and to make a qualitative comparison with the mainstream international nuclear safety software with engineering applications in order to verify the validity of the model and to determine whether or not revise apriori probabilities or various network nodes.

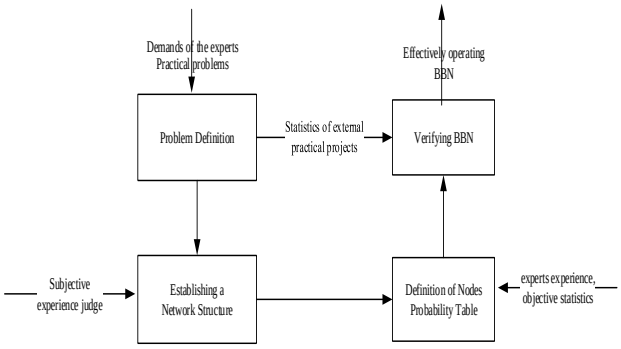


Fig. 2 Modeling steps of Bayesian Belief Network (BBN).

The rest of this paper will be how the authors' proposed method are applied for actual issues. However, the overview of the rest of this paper will be given below, prior to the details in the subsequent pats of this paper.

(1)Concerning appropriate evaluation model of software reliability in nuclear safety class system, a review analysis was conducted on the standards by R&D institutions in the process of software development. The results are obtained by referring to Chapter 7 of Standard Review Plan for the Review of Safety Analysis reports for Nuclear Power Plants Instrumentation and controls as an evaluation criterion of software reliability in nuclear safety class system (BTP7, NUREG-0800) [7]. BTP7-14 is also a guidance document used by the staff of U.S. Nuclear Regulatory Commission (NRC) for the review of nuclear power plant instrumentation and control system[8]. The detailed discussion will be given in Chapter 3 of this paper.

(2)Based on the above mentioned evaluation model by BBN and the U.S. NRC's BTP7-14, 13 sub-models on software reliability evaluation are constructed which can be applied for the software development process. The various indicators for the 13 sub-models are reduced and the index weights are obtained by means

of experts rating, BBN as well as the Hugin software. Currently in the literature, there are some popular commercial software packages available with deferent features and prices, and Hugin has its advantages being developed in full line of Bayesian network support products capable to build the BN models, providing mostly used inference algorithms including Junction Tree, and providing the capacity of full density estimation for CLG hybrid BN models [9].

If the target reliability is given, the influencing probability of each sub factors could be determined. The detailed discussion of this part will be given in Chapter 4.

(3)Final discussion will be on application example. By constructing BBN sub-models, the software development process is not only able to find out the weak links but also calculate quantitatively the influence of different factors in the case of the target reliability. Under different conditions, each sub-factors influence the probability at a target reliability. The detailed discussion of this part will be given in Chapter 5.

3 Design standard of nuclear safety class digital instrumentation and control system

3.1 Levels of standard

Since the digital instrumentation and control system particularly uses software technology, the former standard on the design principles for analog system by International Electro-technical Commission (IEC) become insufficient to provide adequate guidance on the safety design of digital instrumentation and control system. In order to adapt to the development of nuclear power plant digital instrumentation and control system, NRC set up a special working group in 2007 to study key issues on the examination of digital instrumentation and control system [10].

By reviewing the design principles of nuclear safety class digital instrumentation and control system as adopted by NRC working group, the authors of this paper divided various software standards issued by various international institutions in both foreign countries and China, into the following three groups: (i) quality assurance and configuration management, (ii) software development, and (iii) validation of software. The specific standards of every group are shown in Fig. 3. These standards included in Fig. 3 are the nuclear safety regulations (HAF) 003-1991, nuclear safety guidelines HAD 102/16 and the Appendix B of the Chapter 10 10CFR50 in U.S. Federal Regulations. Seven guidelines in Fig. 3 are RG1.152, RG1.168, RG1.169, RG1.170, RG1.171, RG1.172 and RG1.173, all of which mainly follow NUREG-0800 BTP7-14[11-21].

There are several reasons why the NRC staffs employ BTP7-14 as a safety software guideline [22]. They are : (1) it is the software review guideline of digital instrumentation and control system, (2) it confirms acceptable development plan of control software, (3) it shows that the implementation plan complies with the software life cycle, and (4) it shows that the design of development process is acceptable. The file of BTP7-14 provides guidance for evaluating whether or not the digital instrumentation and control system complies with the software life cycle.

3.2 Standard System

Generally speaking, various engineering standards have been established as the regulations and guidelines in accordance with the appropriate procedures set by individual organizations. And they are sometimes mutually utilized, cited and implemented in the individual standard system. For example, the international IEC standards are sometimes cited by the IAEA guidelines while the IEEE standards in the United States are sometimes included in the guidance from the United States Code of Federal Regulations (CFR) and the NRC guidelines (RG). As for China, GB and EJ are established under the guidance of HAF (HAD). Generally speaking, it is noteworthy that there exists fundamental distinction from the nature of MUST OBEY (law and regulation), GOOD TO FOLLOW (code and guideline) which exhibits LEVEL of standards, while there are international standards versus domestic standards.

The authors of this paper reviewed the natures and levels of existing standards by IEC, IEEE, IAEA and USNRC, and classified them into the two groups of (1) U.S. NUREG standards and (2)IEEE-IEC standards, and then reordered the both groups into three categories of (1)quality assurance and configuration management, (2)software development,

and (3)verification and validation. The result is shown in Fig. 3.

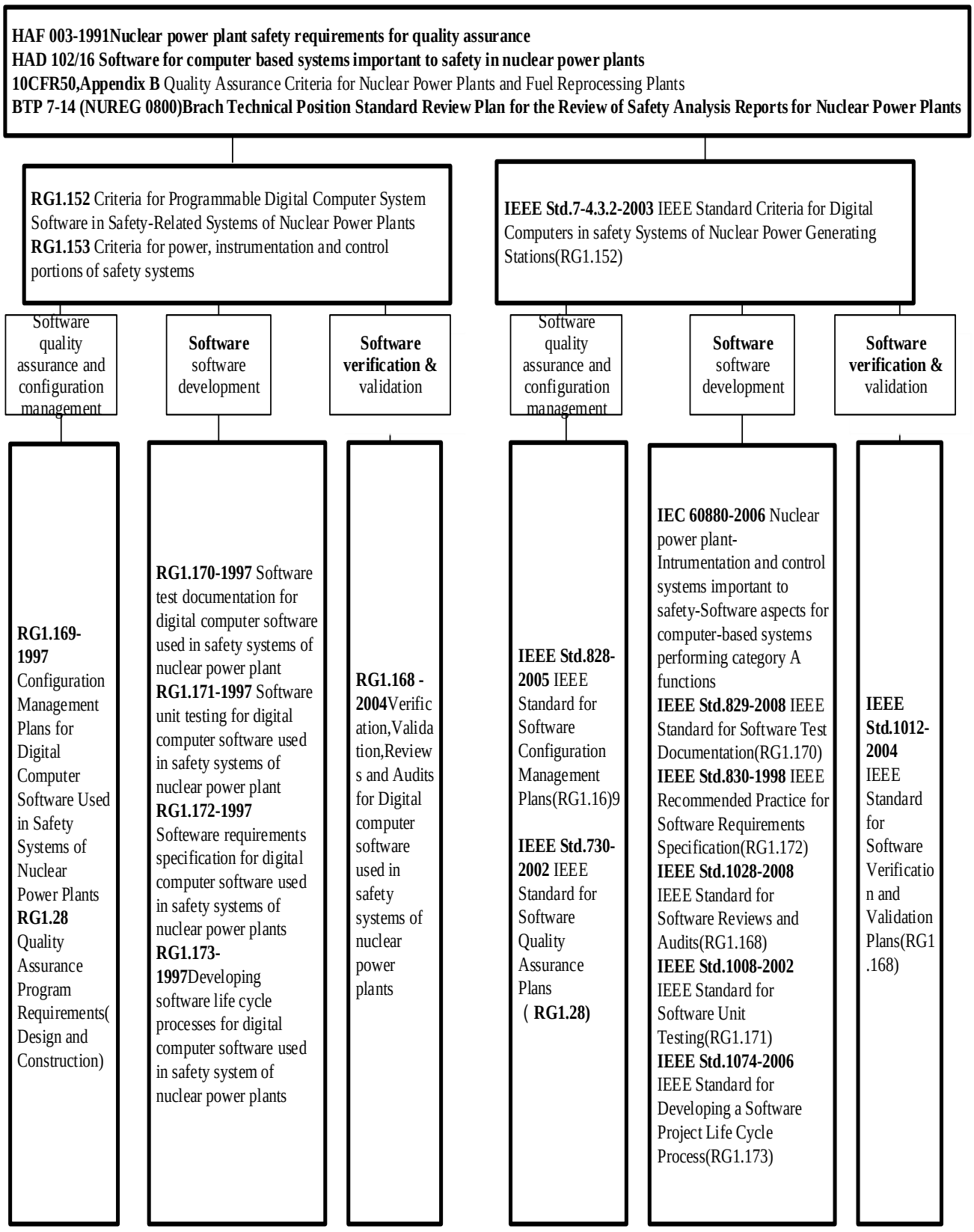


Fig. 3 Levels of Software Standards for Nuclear Safety Class Digital Instrumentation and Control System.

3.3 Existing Standards in China

In China, the current software standards for nuclear safety class digital instrumentation and control system borrow mainly from IEEE, IEC and other standards. Although still far away from perfect, China's main standards are shown in Table 1, where the correspondence between Chinese codes and the international ones is indicated [23].

Table 1 China's Standards for Nuclear Safety Class Instrumentation and Control System

Code	Version	Name	Referential Foreign Standards
EJ/T1058	1998	Computer Software of Safety System in Nuclear Power Plant	IEC-60880-1986
EJ/T1058-2	2005	Computer Software of Safety System in Nuclear Power Plant Part 2	IEC-60880-2-2000
GB/T13629	2008	Applicative Standards for Digital Computer of Safety System in Nuclear Power Plant	IEEE7-4.3.2-2003

4 Quantitative software evaluation model of nuclear safety class digital instrumentation and control system

Nuclear safety regulations and standards are accumulated in the development process of nuclear power [24]. Based on the method of constructing evaluation model by BBN and the U.S. NRC's BTP7-14 as mentioned in Chapter 2, 13 sub-models on software reliability evaluation were constructed which can be applied for the software development process. Table 2 shows all the 13 sub-models with individual relation to the attributes in Fig. 1.

Table 2 List of 13 sub-models for software reliability evaluation

No.	Name of sub-model	Attribute in Figure 1
1	management program	research institutions
2	requirements specification	research process
3	requirements safety analysis	
4	design instruction	
5	development program	
6	code safety	
7	integration program	
8	installation program	
9	maintenance program	
10	configuration management program	solutions
11	verification and validation program	test part
12	quality assurance program	product quality
13	safety program	

The detailed discussions on the two sub-models namely "the software evaluation of requirements specification" and "the software evaluation of management program" will follow in the subsequent subsections, and the other 11 sub-models are given in the appendix.

4.1 Frameworks of two sub-models

The degree of software requirements specification can be evaluated by the combination of several sub-indicators as shown in Fig. 4. As the ultimate outcome of product demands, the software requirements specification must be comprehensive, which means it must include all requirements. Developers and customers cannot make any assumptions. It describes all functional needs to be realized, various functional modules and their importance, business process and others from the viewpoint of customers. It also should list up the characteristics of the end-user which are important constraints of software design. The characteristics include constraints and impacts of requirements, all assumptions, dependencies and interface settings, all functional requirements and non-functional requirements, *etc*.

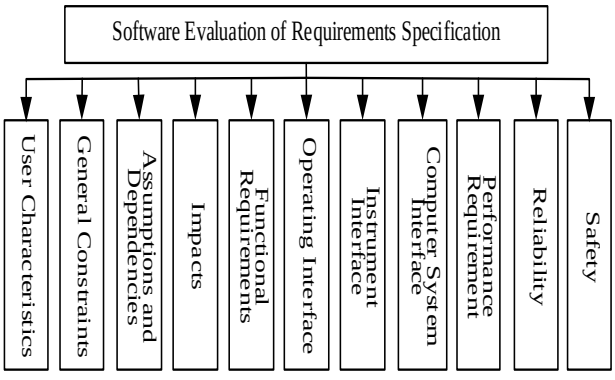


Fig. 4 Software evaluation of requirements specification.

The software management program can be evaluated via sub-indicators as shown in Fig. 5. It is the basic management profile in the whole software

development. Its main function is to supervise, control, report and evaluate about the entire project. This program emphasizes on the structural problems, especially on the process model, structural structure, boundary conditions, interfaces and project responsibility. The program describes management and technology-related procedural issues that influence safety. In some cases, the technology-related procedural issues would also be described in the software development program but in a different angle. While the management program emphasizes on human factors, the development program stresses on individual skills.

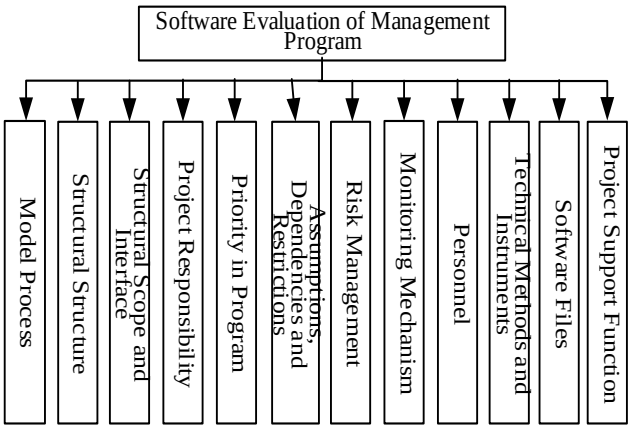


Fig. 5 Software evaluation of management program.

After the discussion on the above two sub-model frameworks, it is worth mentioning to pointing out some common issues which exist over many sub-indicators for different sub-models.

In order to evaluate the software reliability in nuclear safety class instrumentation and control system more accurately, the authors of this paper analyzed various indicators of sub-models and established a BBN evaluation model based on the IEC and IEEE standards by noticing the three parts, namely, "software quality assurance and configuration management", "software development", and "software verification and validation".

Figure 6 shows that one sub-indicator "structural scope and interface issues in the software development" could affect three different directions, in the part of "the software management program". That is, there are three affecting factors: (a) Are there any formal communication channel between the development institution and judges? (b)Whether the reporting channel is clear? , and (c) Whether the scope of a development institution is well defined?

The above three factors (a), (b), and (c) are independent of each other. The analysis here adopts the form of questions in order to plan a survey questionnaire via scoring by experts in the subsequent project. To ensure the integration of the model, the independence among various questions should be taken into consideration in order to avoid confusion by experts.

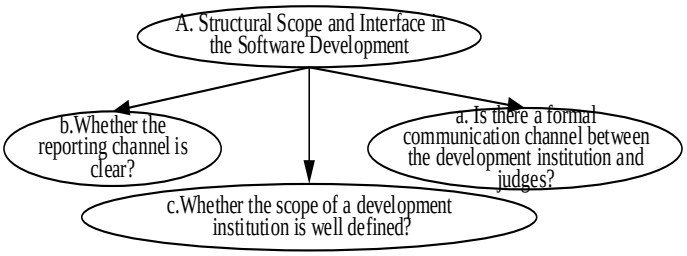


Fig. 6 Structural Scope and Interface Issues in the Software Development.

4.2 Weight Analysis

For evaluating the sub-model quantitatively, how to give weight for various sub-indicators in the model should be fully taken into consideration. Therefore, a list of questionnaires about every influencing factor in every sub-model is firstly prepared and then experts in different fields are invited according to different features. The invited experts could be roughly divided into three groups: experts on the standard itself, experts on the standard development, and experts on the evaluation about nuclear safety class instrument and control system. Then by conducting group brainstorming, a prior probability of each indicator and conditional probability table were determined.

If the probability is difficult to calculate, it is better to make full use of expert judgment. Normally, the expert group is supposed to give two kinds of conditional probabilities: one is probability with positive indicators and negative affecting factors and the other one is probability with negative indicators and positive affecting factors.

5 Application example analysis

In this chapter, the authors of this paper discuss on how to determine the BBN model in case for "structural scope and interface issues in the software development", one sub-indicator of evaluation of software reliability.

Just as shown in Fig. 6, three independent influencing sub-factors (a), (b) and (c), are assumed in the network. The probabilities of answering "Y" are set as 0.9 while the probabilities of answering "N" are set as 0.1. The conditional probabilities among factors are as shown in Table 3. After setting up in the Hugin software, the questions about "structural scope and interface issues in the software development" could be analyzed.

Table 3 Conditional probability table of structural scope and interface issues in software development

a. Whether the scope of a development institution is well defined?	Y				N			
b. Whether the reporting channel is clear?	Y		N		Y		N	
c. Is there a formal communication channel between the development institution and judges?	Y	N	Y	N	Y	N	Y	N
A Structural Scope and Interface in the Software Development (reliable)	0.99	0.85	0.95	0.87	0.93	0.84	0.8	0.7
A Structural Scope and Interface in the Software Development (reliable)	0.01	0.15	0.05	0.13	0.07	0.16	0.2	0.3

In the Hugin software, set the target node A "structural scope and interface issues in the software development" as an invalid state. As shown in Fig. 7, the probability of invalidity caused by (a) is 44.46% while the probability caused by (b) and (c) 21.61% and 27.19%, respectively. From the above statistical calculation, the question "whether the scope of a development institution is well defined" plays an essential factor in the invalidity of the target node A. As a result, the development institution is supposed to pay due attention on this question and try to improve it.

Then, according to the known a prior probability and conditional probability table, any posterior probability under any circumstance could be calculated by Hugin software. As shown in Figs. 8 and 9, if factors (a) and (b) are reliable, then probability of (c) invalidity is 0.00567 and the probability of a invalidity is 0.3387. Wherein the formula P (A, B) = P (A | B) P (B) P (A | B) = P (B | A) * P (A) / P (B) is given, then the posterior probability can be expressed as P (A | B) = P (A, B) / P (B). Combined with this Bayesian formula, we can conclude that

$$P(a=\mathrm{Y}, b=Y, c=\mathrm{N}/A=F)=P(a=Y, b=Y, c=N, A=F)/P(A=F)$$
$$=0.00567/0.3387=16.74\%$$

From the above result, if A is invalid as the premise and both (a) and (b) are reliable, then the probability of (c) invalidity is 16.47%.

In summary, through the establishment of BBN in the sub-models of nuclear safety class software reliability and the use of Hugin software, we cannot only find weak links in the software development process, but also calculate quantitatively the target reliability values influenced by different factors and find different influencing probabilities of sub-factors when the target reliability is given.

6 Conclusion

Within the international framework of China-EU cooperative projects on nuclear safety class digital instrument and control system, the authors of this paper presented their own developmental activity on the evaluation model of the software reliability for nuclear safety class digital instrumentation and control system. In this connection, 13 sub-models of the software reliability evaluation model were established by utilizing the BBN methodology. Various indicators used in those sub-models were reduced and the way of how to calculate weight factors of every indicators was proposed by using Hugin software for realizing the quantitative evaluation.

The proposed method has the advantage of distinguishing sub-indicators clearly in both qualitative and quantitative aspects. Furthermore, expert judgments could be obtained from the management level to the decision-making level, which makes use of accumulated skills and experience.

In the qualitative terms, the weak links in the software development can be found out in order to improve the program. In the quantitative aspect, the probability of software validity can be calculated through weight analysis made by the BBN model, which can evaluate the software development program and the software reliability. The disadvantage of this method lies in the subjectivity in scoring. The authors of this paper have been focusing on the research about the development process according to the task requirements at present, which would lay the foundation of further research such as modeling for practical problems.

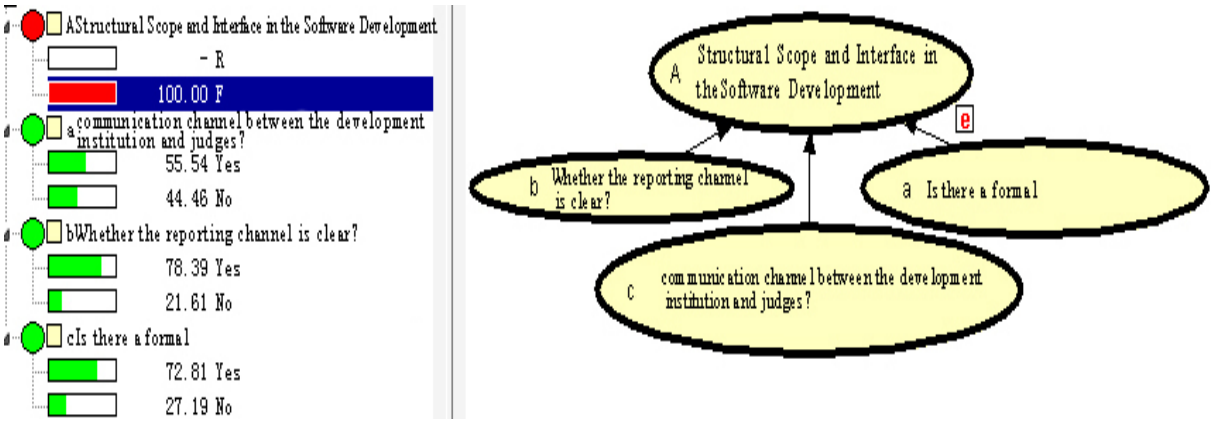


Fig. 7 Total invalid state of the structural scope and interface issues in the software development.

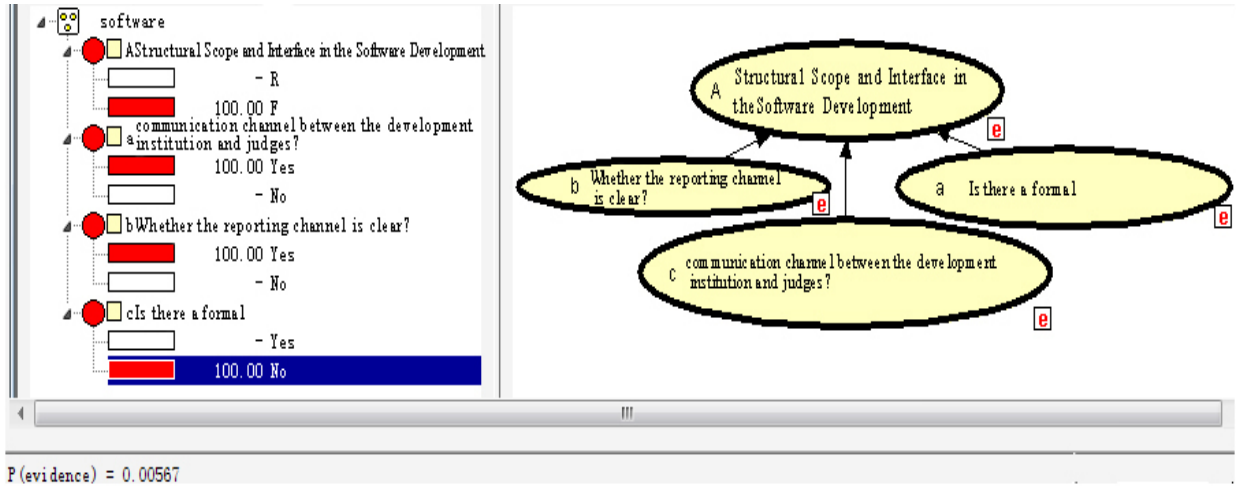


Fig.8 Setting the probability values of invalidity c and invalidity A when factors, a and b, are reliable.

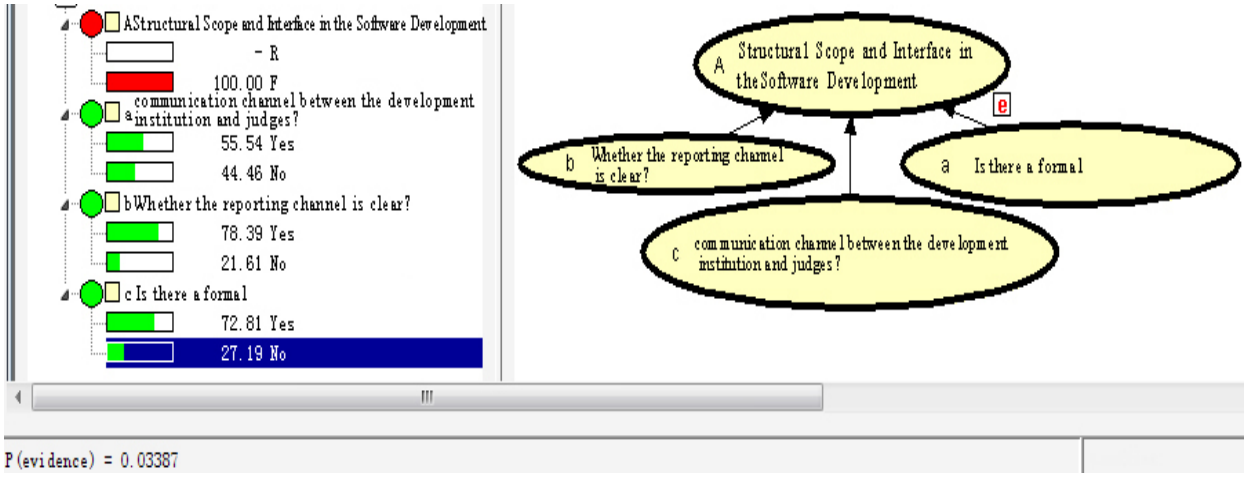


Fig. 9 Setting the probability value of invalidity A.

References

[1] WANG, J. S., HONG, Z. M, and HU, P.: Some Digital I &C System Application and Analyses in Nuclear Power Station Reconstruction, Chinese Journal of Nuclear Science and Engineering, 2005,25(3): 163-171. (In Chinese).

[2] AUTHÉN, S., BJÖRKMAN, K., HOLMBERG, J.-E., and LARSSON, J.: Guidelines for Reliability Analysis of Digital Systems in PSA Context — Phase 1 Status Report," NKS-230, Roskilde: Nordic Nuclear Safety Research, 2010.

[3] AUTHÉN, S., GUSTAFSSON, J., and HOLMBERG, J.-E.: Guidelines for Reliability Analysis of Digital Systems in PSA Context — Phase 2 Status Report, NKS-261, Roskilde: Nordic Nuclear Safety Research (NKS), 2012.

[4] HOLMBERG, J.-E., AUTHÉN, S., and AMRI, A.: Development of Best Practice Guidelines on Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PSA, Proc. of 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference, 25–29.6.2012, Helsinki, paper 10-Th4-1.

[5] BJORN, A. G.: The Use of Bayesian Belief Nets in Safety Assessment of Software Based Systems, International Journal on Intelligent Information Systems at FLINS'98, Int., .J. General Systems, 2000, 24 (2): 205-229,

[6] SHEN, G. G., DONG, L., and YE, D. S.: Research of Applying BBNs in Software Testing Process (in Chinese), Computer Engineering and Design, 2006, 20(3): 9-22.

[7] U.S Nuclear Regulatory Commission, Standard Review Plan for the Review of Safety Analysis reports for Nuclear Power Plants "Instrumentation and controls", NUREG-0800, Chapter7, rev.5[S], 2007.

[8] YANG, Y. F., and DING, Y.: The Manual of Verification and Validation of Digital Instrumentation and Control Software System in Nuclear Power Plant, Fujian Province: Xiamen University Press, 2010:8. (In Chinese).

[9] WEI Sun, CHEOL Young Park, and ROMMEL Carvalho: A New Research Tool for Hybrid Bayesian Networks using Script Language, Signal Processing, Sensor Fusion, and Target Recognition XX, Washington (2011).

[10] REN, Y. Z., and WANG, C. F.: Use of Digital Technology in Nuclear Power Plant Safety System, Instrument Standardization & Metrology, 2009,5(Important Issues):15-19. (In Chinese).

[11] National Nuclear Safety Administration, Nuclear Power Plant Safety Requirements for Quality Assurance (in Chinese), Guide, Series No. HAF003, Beijing (1991).

[12] National Nuclear Safety Administration, Computer-based Safety System Software in Nuclear Power Plant, Guide, Series No.102/16, Beijing (1988). (In Chinese).

[13] US Nuclear Regulation Commission, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, Appendix B to Part 50, Regulations, Series No. CFR50, Washington (2013).

[14] US Nuclear Regulation Commission, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, Guidelines, Regulatory Guide 1.152, Washington (1996).

[15] US Nuclear Regulation Commission, Verification, Validation, Reviews and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.168, Washington (2004).

[16] US Nuclear Regulation Commission, Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.169, Washington (1997).

[17] US Nuclear Regulation Commission, Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.170, Washington (1997).

[18] US Nuclear Regulation Commission, Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.168, Washington (1997).

[19] US Nuclear Regulation Commission, Software Requirement Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.172, Washington (1997).

[20] US Nuclear Regulation Commission, Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.173, Washington (1997).

[21] YANG, Y. F., and DING, Y.: The Manual of Verification and Validation of Digital Instrumentation and Control Software System in Nuclear Power Plant, Fujian Province: Xiamen University Press, 2010:12-16. (In Chinese).

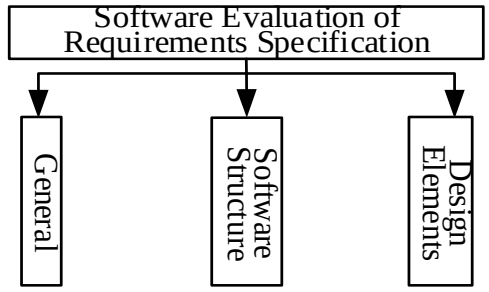
[22] YANG, Y. F., and DING, Y.: The Manual of Verification and Validation of Digital Instrumentation and Control Software System in Nuclear Power Plant, Fujian Province: Xiamen University Press, 2010:9. (in Chinese).

[23] ZHENG, W. Z., LI, X. J., ZHU, Y. M., and ZHANG, Y.: The Research on the Design Standards for Safety Class DI&C in Nuclear Power Plant, The Compilation of the First China Nuclear Instrument Control Technology Conference. Beijing, National Academy Press, 2012. (in Chinese).

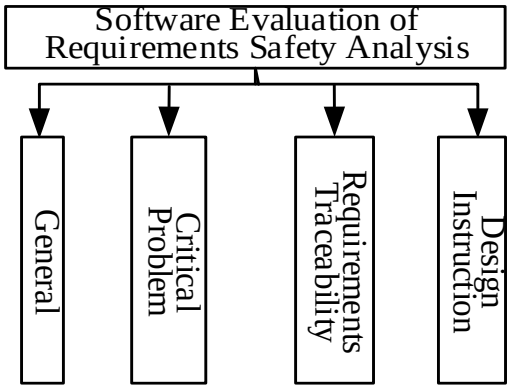
[24] ZHANG, J, Q., and WANG, G. S., Overview of the Standard System for Safety and Significant Instrumentation and Control Systems Used in Nuclear Power Plants, Process Automation Instrumentation, 2010, 20(09):40-43. (In Chinese).

Appendix: BBN models for the standards of I&C software development and evaluation

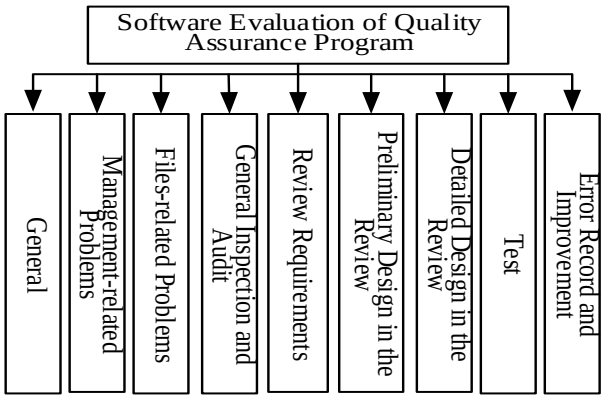
1. Requirement specification



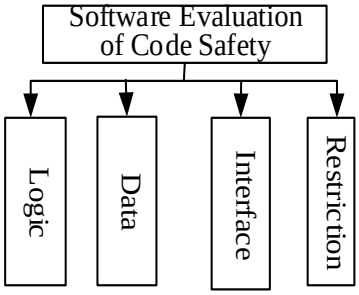
2. Requirement safety analysis



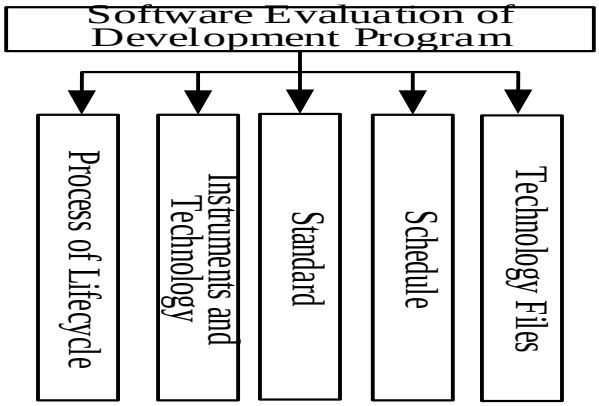
3. Quality assurance program



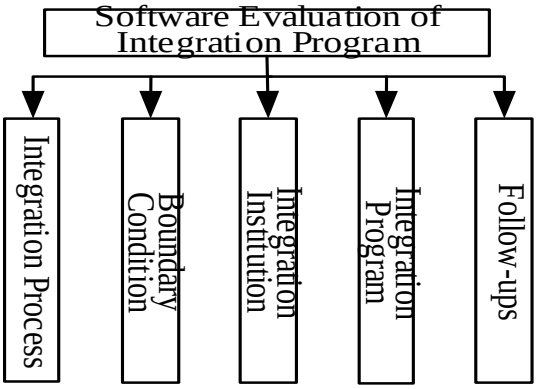
4. Code safety



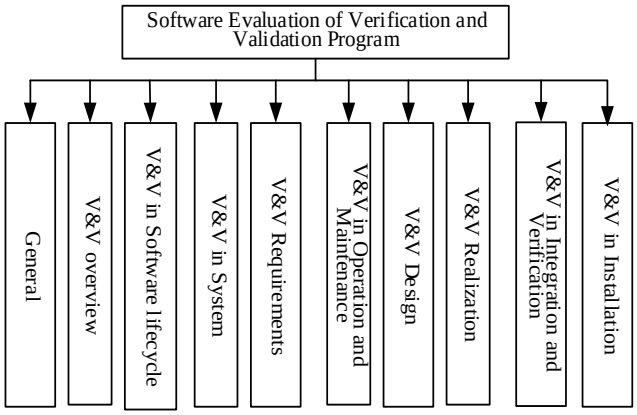
5. Development program



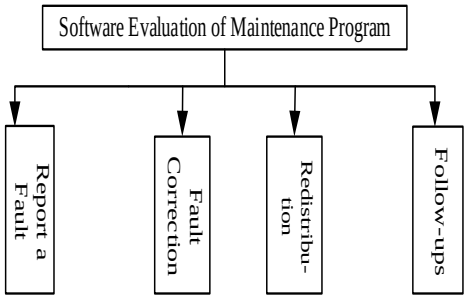
6. Integration program



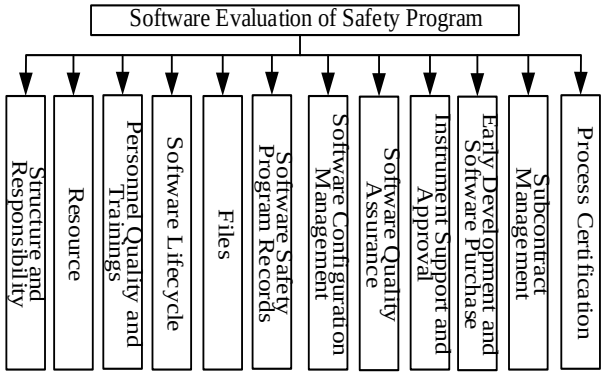
7. Verification and validation program



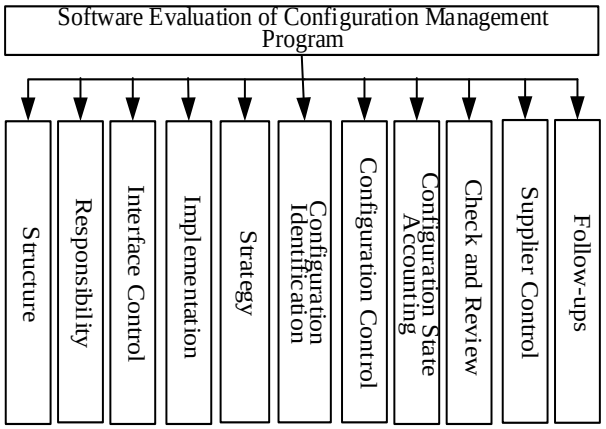
8. Maintenance program



9. Safety program



10. Configuration management program



11. Installation program