Guideline for Bayesian Net based Software Fault Estimation Method for Reactor Protection System

Heung-Seop Eom [a*], Gee-Yong Park [a], Seung-Cheol Jang [a]
[a]*Korea Atomic Energy Research Institute,1045 Daedeok-daero, Yuseong-gu, Daejeon*
[*]*Corresponding author: ehs@kaeri.re.kr*

1. Introduction

The purpose of this paper is to provide a preliminary guideline for the estimation of software faults in a safety-critical software, for example, reactor protection system's software. As the fault estimation method is based on Bayesian Net which intensively uses subjective probability and informal data, it is necessary to define formal procedure of the method to minimize the variability of the results. The guideline describes assumptions, limitations and uncertainties, and the product of the fault estimation method. The procedure for conducting a software fault-estimation method is then outlined, highlighting the major tasks involved. The contents of the guideline are based on our own experience and a review of research guidelines developed for a PSA.

2. Contents of the Guideline

2.1 Overview of the Method

Bayesian Belief Net (BBN) or Bayesian Net (BN) is a network-based formalism for representing and analyzing models involving an uncertainty [1]. The advantages of the BN can be utilized in the faults estimation of safety-critical software for nuclear power plants [2, 3]. The method in this guideline relies on BN to combine all the variables relevant to the reliability of software, and to consistently propagate the impact of these variables on the probabilities of the uncertain outcomes, for example, the fault number or reliability information. As the V&V governs development of safety-critical software in the nuclear field [4], the variables used in the BN model were mostly identified from V&V documents. Figure 1 represents the framework for the BN based reliability analysis of safety-critical software.

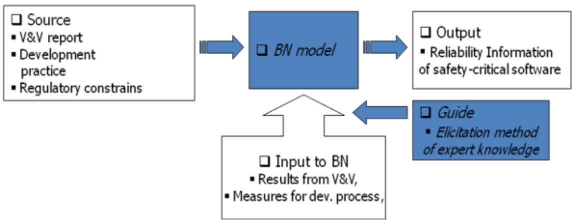

Fig. 1. Framework of BN based reliability analysis of a safety-critical software

2.2 Information Requirements

As the selection of variables (nodes in BNs) related to the fault introduction during the software development is the most critical part of the BN modeling, the software-reliability analyst should double-check to ensure that all the necessary variables are identified for the BN modeling.

The basic information to identify the variables needed for BN modeling are mostly included in V&V documents, such as V&V plan, V&V procedure, and V&V report. As all these V&V documents should be correct and formal, those documents must be produced under the formal process, such as software configuration management.

The software-reliability analyst must become familiar with the following fields:

- Basic probability theory
- Bayesian Nets (Bayesian Belief Nets)
- Software engineering (especially software reliability)
- V&V (plan, procedure, activities)
- International Standards and licensing requirements for a safety-critical software

Personnel familiar with V&V of a safety-critical software should be on call to provide information about the development documents and V&V activities such as plan, procedure, and assessment results.

The V&V experts and software developers are chiefly responsible for identifying the important variables, constructing the BN graphs, and defining the node probability of variables. Their close interaction with software reliability analysts will ensure that the modeling of faults introduction in the software development is correct. In quantifying these faults introduction, the underlying assumptions and limitations that apply to the models and data must be understood and not contradicted in their application to a PRA.

2.3 Procedure

A software development life-cycle (SDLC) basically consists of a requirement phase, a design phase, an implementation (coding) phase, an integration phase, and a validation phase. Most SDLCs employed for the development of a safety-critical software take form of any number and combination of these 5 phases. Thus, the sequence of the BN construction is ① compose "characteristic" BN by using the "characteristic" BN class, ② compose “fault estimation” BN for each SW development phase by using the “fault estimation” BN class. ③ construct all the development-phases BNs by using the previously composed “characteristic” BNs and a “faults estimation” BN, ④ finally, connect the development-phase BNs according to the development sequence, which leads to the SDLC BN. The SDLC BN is the final model that can estimate faults of the target software.

2.4 Methods of Documentation

The results of the software reliability analysis go directly into the system analysis. The only data that are used in the rest of the risk assessment are the information about the fault number in the target software. The important part of the final report is the assumptions in creating NPTs, so it is necessary to describe them in detail with proper evidence or back data. Other information included in the final report is not necessary as an input to the analysis itself, but is instead necessary as a reference on the performance of any particular software-reliability analysis.

The other software-reliability analysts must be able to trace through the analyses and to understand them fully. To obtain the necessary information, they must have access to the material on which the analysis was based. A copy of the final BN model and its calculation results should be included.

In short, the final report should include all information necessary for the system analyst to check the assumptions about all the variables. It should also include sufficient information so that another software-reliability analyst could analyze the same scenario and arrive at a similar result.

2.5 Display of Final Results

The most efficient method for displaying the results of the BN based software reliability analysis is to use the BN graphs. These graphs include most of the necessary information for the probabilities risk assessment (PRA) input. With these BN graphs and their attached NPTs, the system analysts can take reliability information for input into the fault trees. The BN graphs and their NPTs should have proper background information which the system analysts can understand. The background information should include the references and documents used for the construction of graphs and NPTs. This type of complete documentation of a software reliability analysis is important for PRAs to be performed at various times in the life of a plant. As the plant’s operation environments which generate input to the software changes over time, the PRAs need related information to reflect these changes.

2.6 Uncertainty

The BN based method requires lots of subjective judgment in eliciting the probabilities in constructing the BN model, so some degree of uncertainty is inevitable for the estimation of a software reliability calculation.

There are four major sources of uncertainty in estimating the probability of BN model for software reliability estimation.

(1) The conversion of qualitative V&V frame to the BN graph
(2) The elicitation of conditional probabilities in NPTs
(3) The conversion of qualitative V&V results to numbers for input of a BN model.
(4) The skill and knowledge of software reliability analysts

The first source, the conversion of qualitative V&V frame to BN graph, involves some abstraction and is subject to some interpretation on the part of the analyst. The second source, the elicitation of conditional probabilities in NPTs, is the most critical in building a BN model. Currently, the objective data for the most of NPTs are not available, so experts usually do the elicitation process. The third source, the conversion of qualitative V&V results to probabilities for input of a BN model, is also important and V&V experts usually perform the conversion process. The analyst is another source of uncertainty.

The way of handling uncertainties of the BN model in this guideline is the first approach and it uses the discrete probability distribution (DPD) method in which the distribution of fault number is graphed as a discrete histogram.

3. Conclusions

BN based software fault estimation method is promising but it uses lots of subjective probability and informal data. This fact requires an ordered guideline for the application of the method in the real fields. The proposed guideline is intended to assist researchers, reviewers, and software reliability analyst in the digital I&C field of nuclear power plants. We think that the guideline derived from our own experience will contribute the further research and the use of BN based method in the reliability assessment of a digital protection system in nuclear power plants.

REFERENCES

[1] F. V. Jenson, Introduction to Bayesian Networks, UCL Press, 1996

[2] Johnson, G., et al, 2000. Bayesian Belief Network Based Review of Software Design Documents, NIPC & HMIT, 2000.

[3] H.S. Eom, et al, A Study on the Quantitative Reliability Estimation of Safety-Critical Software for Probabilistic Safety Assessment, 4th NIPC & HMIT , 2004.

[4] G. Y. Park and K. C. Kwon, Software Verification & Validation for Digital Reactor Protection System, Information and Control Symposium, pp. 190-192, (2005).