# BBN based Quantitative Assessment of Software Design Specification

Heung-Seop Eom, Gee-Yong Park, Hyun-Gook Kang, Kee-Choon Kwon, Seung-Cheol Chang
*Korea Atomic Energy Research Institute, ISA Div., P.O.Box 105, Yuseong Daejeon, ehs@kaeri.re.kr*

## 1. Introduction

Probabilistic Safety Assessment (PSA), which is one of the important methods in assessing the overall safety of a nuclear power plant (NPP), requires quantitative reliability information of safety-critical software, but the conventional reliability assessment methods can not provide enough information for PSA of a NPP [1]. Therefore current PSA which includes safety-critical software does not usually consider the reliability of the software or uses arbitrary values for it [2]. In order to solve this situation this paper proposes a method that can produce quantitative reliability information of safety-critical software for PSA by making use of Bayesian Belief Networks (BBN). BBN has generally been used to model an uncertain system in many research fields including the safety assessment of software [3].

The proposed method was constructed by utilizing BBN which can combine the qualitative and the quantitative evidence relevant to the reliability of safety-critical software. The constructed BBN model can infer a conclusion in a formal and a quantitative way. A case study was carried out with the proposed method to assess the quality of software design specification (SDS) of safety-critical software that will be embedded in a reactor protection system. The intermediate V&V results of the software design specification were used as inputs to the BBN model.

## 2. Methods and Results

In this section BBN is briefly introduced and the principle of our BBN based quantitative assessment method is described. A case study was carried out to verify the possibility and the difficulties of the method when we use it in a real field. The experience of the case study is also discussed.

### *2.1 Bayesian Belief Networks (BBN)*

BBN is a network-based formalism for representing and analyzing models involving an uncertainty. Nowadays a number of efficient tools for a BBN modeling are available and BBN has become an widely used technology in many areas such as medical, military, financial, and the safety/reliability analysis of complicated systems such as digital systems. BBN consists of the following [4].

- A set of variables and a set of directed edges (arcs) between variables
- Each variable has a finite set of mutually exclusive states
- The variables together with the directed edges form a directed acyclic graph (DAC). A DAC is acyclic if there is no directed path A1 -> … An such that A1 = An
- To each variable A with parents B1 … Bn there is attached a conditional probability table P (A|B1…Bn).

The most useful advantage of BBN is that it allows us to employ both subjective probabilities and probabilities based on statistical data in a unified framework. The general process of BBN modeling is as follows.

- Step-1: Identify the main aspects that may influence the target variable(node)
- Step-2: Determination of relationships among nodes (topology structure)
- Step-3: Making of Node Probability Table
- Step-4: Collecting evidence
- Step-5: Computation of BBN

### *2.2 BBN- based Quantitative Assessment Method*

The proposed method relies on BBN to combine all the variables relevant to the reliability of SDS, and to propagate consistently the impact of these variables on the probabilities of the uncertain outcomes (in this example, the quality of SDS). The variables (nodes) used in the model were mostly identified from V&V procedures, V&V reports, and software design specification. Figure 1 represents the framework of the reliability assessment of safety-critical software in our proposed method. Assumption of the method is that the quantitative reliability feature of safety-critical software can be obtained by evaluating all the software product/process in the software's development lifecycle

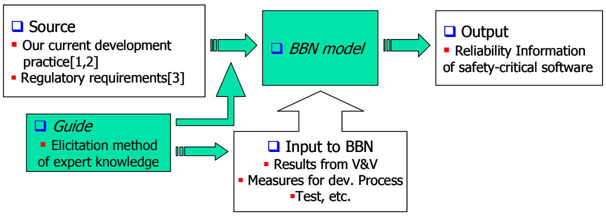
❑ Source
▪ Our current development practice[1,2]
▪ Regulatory requirements[3]
❑ BBN model
❑ Output
▪ Reliability Information of safety-critical software
❑ Guide
▪ Elicitation method of expert knowledge
❑ Input to BBN
▪ Results from V&V
▪ Measures for dev. Process
▪Test, etc.

Figure 1. Framework of reliability assessment of safety-critical software

### *2.3 Case Study: Assessment of Software Design Specification of a Reactor Protection System*

The purpose of the case study is to evaluate the SDS in a quantitative way with the proposed method. The basic documents which were used to develop the model are (i) Procedures for V&V [5], (ii) V&V report [6], and (iii) Software Design Specification. The constructed model consists of three sub-models. First sub-model is an architectural design model which assesses the architectural design of SDS. Second one is a license suitability model which is based on the current licensing criteria. Last one is an engineering decision model which is based on a technical point of view of V&V. Figure 2 shows the topology of BBN model. The properties of each sub-model are as follows.

- 8 properties for the software architecture design model: reliability, safety, security, timing, completeness, consistency, style, traceability, verifiability.
- 12 properties for the license suitability model: accuracy, reliability, robustness, safety, security, timing, completeness, consistency, correctness, style, traceability, verifiability.
- 4 properties for the engineering decision model: traceability, correctness, consistency, completeness

A total of 330 nodes and their node probability table (NPT) were developed. All the nodes converted from the checklists in the V&V reports have two states ("yes" and "no"). The conditional probabilities of the NPTs in the model were assigned by a V&V expert.

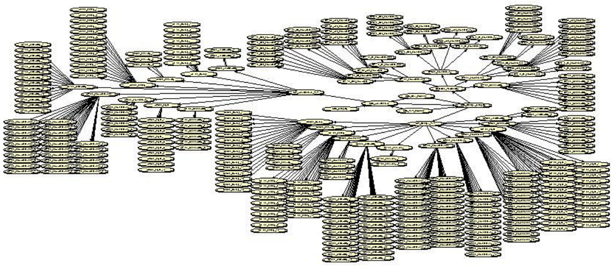

Figure 2. BBN topology used to assess software design specification of a reactor protection system

### *2.4 Analysis and Discussion*

Figure 3 shows the calculation results of the target variables of the whole model and two sub-models (the license suitability model and the engineering decision model.) The calculation results of the properties in the model are presented in Figure 4. As there was not enough information about the quality level of the development process and the V&V process, the model calculation was carried out according to two scenarios. First one is that the quality of the development process and the V&V process are unidentified, and the second one is that the development process and the V&V process are perfect.

Y axis in Figures 3 and 4 represents the variables' probability which indicates a sufficiency of a requirement for a variable. Since V&V of software architecture design was not completed yet, all the prior probabilities of the variables in the software architecture model were set to 50%, and the values in Figure 4 represent the posterior probabilities.

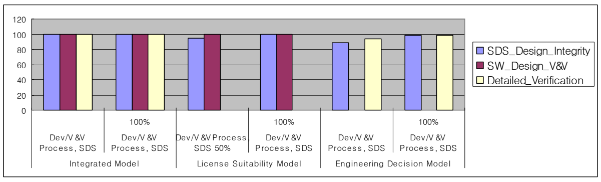

Figure 3. Calculation results of the target variables

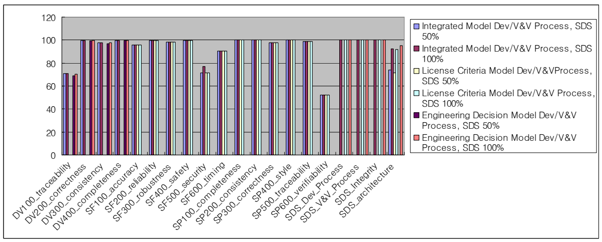

Figure 4. Calculation results of the properties

## 3. Summary and Conclusion

In order to support PSA we devised a BBN based method which can obtain quantitative reliability information of safety-critical software. The proposed method can combine disparate evidence which is gathered automatically during the development of software, and can infer a quantitative conclusion. The calculation results of the BBN model showed that its conclusion is mostly equivalent to those of the V&V expert for a given input data set. The method and the experience of the case study will be utilized in PSA of a digital safety system in NPPs. The method also showed that it can support the V&V expert's decision making process in controlling further V&V activities in KNICS.

## Acknowledgements

This research was supported by "The Mid and Long Term Nuclear R&D Program" of Ministry of Science and Technology, Korea.

## REFERENCES

[1] R.W. Butler, et al, The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software, IEEE Transactions on Software Engineering, 19(1), 1993

[2] H.G. Kang, et al, A Quantitative Study on Important Factors of the PSA of Safety-Critical Digital Systems, Nuclear Engineering and Technology, 33(6), 2001.

[3] Neil, M., et al, "Applying Bayesian Belief Networks to System Dependability Assessments," Proceedings of Safety Critical Systems Club, February 1996.

[4] Jensen, F., An Introduction to Bayesian Belief Networks, Springer-Verlag, New York, NY, 1996.

[5] G.-Y. Park, et al, V&V Procedure for Software Requirement Specification of Reactor Protection System, KNICS-RPS-SVP131, KAERI, KNICS, 2006.

[6] G.-Y. Park, V&V Validation Reports for Software Design Specification of Reactor Protection System, KNICS-RPS-SVR131-01, KAERI, KNICS, 2006.