Towards Easy Inspection and Effective Use of Formal Methods in NPP Software Fields

Seo Ryong Koo*, Han Seong Son*, Poong Hyun Seong*, Junbeom Yoo**, and Sung Deok Cha**

Korea Advanced Institute of Science and Technology

* Department of Nuclear Engineering

** Department of Electrical Engineering & Computer Science, Division of Computer Science

373-1 Gusong-dong, Yusong-gu, Daejeon, Korea 305-701

Dae Seong Son and Seong Soo Choi

Atomic Creative Technology

KAIST HTC #4408

62-1 Hwam-dong, Yusong-gu, Daejeon, Korea 305-348

I. Introduction

The use of digital systems is on increase in nuclear industry in recent years. Therefore, the importance of software verification and validation (V&V) is more emphasized in view of the nuclear safety. Inspection is widely believed to be an effective software V&V technique. However, software inspection is labor-intensive. In order to promote the application of software inspection, the authors have been developing a software inspection support tool, SIS-RT. SIS-RT is designed to partially automate the software inspection process so that the burden of software inspection may be reduced. SIS-RT also supports requirement traceability analysis, which is considered as one of important activities of software V&V. SIS-RT has four features; a document analysis, a traceability analysis, a formal analysis and an inspection meeting support. Though formal methods, such as Statechart [1], CPN [2], RSML [3], and SCR [4], are also considered as an effective V&V harness, they are not easy to be used properly in nuclear fields because of their mathematical nature. However, formal specification can lessen requirements errors by reducing ambiguity and imprecision and by clarifying instances of inconsistency and incompleteness. Therefore, this work suggests an integrated approach with inspection and formal methods in order to support easy inspection and effective use of formal specification method. This approach is expected to be a more effective requirement specification and analysis method in nuclear fields.

II. Approach for Easy Inspection and Effective Use of Formal Method

It is very difficult that requirement analyzer understands design documents written in natural language at once and then specifies software requirements from them formally. It is also difficult to assure the quality of the specification. This is because of the difference of domain knowledge between designer and

analyzer. Thus it is very important to fill this gap. Design documents written in natural language is mostly of large amount. It needs much time and efforts that analyzer understands and formally specifies the documents.

Using a software inspection support tool which fills the gap between natural language documents phase and formal specification phase, the approach proposed in this study helps a user perform easier inspection and compose formal specification efficiently. Figure 1 shows schematic diagram of the approach proposed in this study.

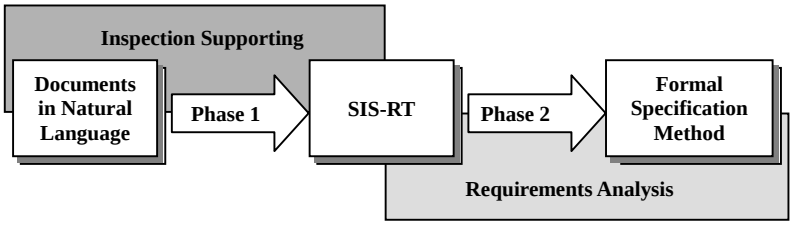

Figure 1. Schematic diagram of the approach

Phase 1 is inspection supporting to increase quality of the design documents written in natural language. As mentioned before, SIS-RT supports various V&V activity based on Fagan Inspection [5]. SIS-RT is a PC-based application designed for use by anyone who needs to manage requirements. A desirable attribute of inspections is rigor. Using computers to support the process helps provide this rigor, and improves the repeatability of the inspection process. Repeatability is essential if feedback from the process is to be used to improve it. In phase 1, SIS-RT can support easier inspection for user [6].

In phase 2, the document analysis feature of SIS-RT enables the effective transition into formal specification. Since it is difficult to generate a formal specification from a natural language document directly, it is necessary to extract useful information from design documents. SIS-RT supports the structural analysis of documents. Through the document analysis, we can obtain a refined document for formal specification and this document will be very useful to analyzer. The structure type from the analysis results is affected by formal methods that the analyzer uses for software requirements specification. For example, SCR-style SRS, composed by AECL, consists of Functional Overview Diagram (FOD) and Structured Decision Table (SDT). In this case, the structure type should be useful to draw FOD and SDT. With an Input-Process-Output structure type, the authors have successfully drawn FOD and SDT using SIS-RT.

III. Conclusions

Through the proposed approach, we can minimize some difficulties caused by the difference on domain knowledge between designer and analyzer. Furthermore, we can apply formal specification method more efficiently. There is, however, no formal specification method to be applied generally to nuclear fields and thus we cannot suggest generic structure type for the structural analysis. Now, we are

developing a formal specification method that can be used friendly in NPP software fields. Through further development efforts, SIS-RT will turn out to be a unique and promising software V&V tool.

[References]

[1] D. Harel, "Statecharts: A Visual Formalism for Complex Systems," Science of Computer Programming, vol. 8, pp.231-274, 1987.

[2] Kurt Jensen, “Coloured Petri Nets (Basic Concepts, Analysis Methods and Practical Use Volume 1), Second Edition”, Springer-Verlag Berlin Heidelberg, 1997.

[3] N.G. Leveson, M.P.E. Heimdahl, H. Hildreth, and J.D. Reese, "Requirements Specification for Process-Control Systems," IEEE Transaction on Software Engineering, vol.20, no.9, sept. 1994.

[4] C. Heitmeyer and B. Labaw, “Consistency Checking of SCR-style Requirements Specification”, International Symposium on Requirements Engineering, March, 1995.

[5] M.E. Fagan, “Design and Code Inspections to Reduce Errors in Program Development,” IBM system Journal, Vol. 15, No. 3, pp. 182-211, 1976.

[6] Han Seong Son and Poong Hyun Seong, "SIS-RT: An Integrated Software Inspection Support and Requirement Traceability Tool", Proceedings of the Korean Nuclear Society Autumn Meeting, 2000.