Software V&V Methodology for Embedded Real Time Kernel

Jang Yeol KIM[1], Young Jun LEE[2], Kyung Ho CHA[3], Se Woo CHEON[4],
Jang Soo LEE[5], Kee Choon KWON[6]

Korea Atomic Energy Research Institute (KAERI)
P.O. Box 105, Yuseong, Daejeon, 305-600, Republic of Korea
jykim@kaeri.re.kr[1], ex-yjlee426@kaeri.re.kr[2], khcha@kaeri.re.kr[3], swcheon@kaeri.re.kr[4],
jslee@kaeri.re.kr[5], kckwon@kaeri.re.kr[6]

1. Introduction

This paper addresses the Verification and Validation(V&V) process and methodology for embedded real time software of a safety-grade Programmable Logic Controller(PLC). This safety-grade PLC is being developed in the Korea Nuclear Instrumentation and Control System(KNICS) projects. KNICS projects are developing a Reactor Protection System(RPS) and an Engineered Safety Feature-Component Control System(ESF-CCS) as well as a PLC. Safety-grade PLC will be a major component that composes the RPS systems and ESF-CCS systems as nuclear instruments and control equipments. This paper describes V&V environment, V&V process and methodology, and the V&V tools by the KNICS projects.

2. V&V METHODS OF SAFETY-GRADE PLC

It describes the real-time operating system V&V experience which corresponds to the requirement analysis phase of the software development life cycle. Main activities of the real-time operating system Software Requirement Specification(SRS) V&V of the PLC are the technical evaluation, licensing suitability evaluation, inspection and traceability analysis, formal verification, software safety analysis, and software configuration management(Figure 1). We believe that we can achieve the functionality, performance, reliability and safety that are the V&V objective goals of a safety-grade PLC system at the requirement analysis phase during the software development life cycle through the suggested software V&V methods for a PLC.

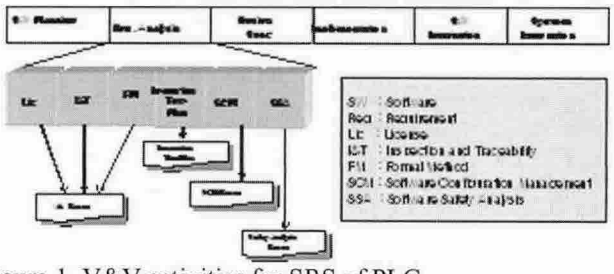

Figure 1. V&V activities for SRS of PLC

2.1Review of Licensing suitability

The purpose of the licensing suitability review confirms whether or not the software requirements which coincide with the criteria of the software, performance and safety requirements defined in the Safety-grade PLC. Software requirement detailed statement are suitable from the Code & Standard and technological viewpoint. According to SRP/BTP-14 criteria(USNRC, 1997), must satisfy all functionality characteristics and process characteristics.

2.2 Inspection and Traceability Analysis

Inspection and traceability analysis is performed via the three properties of completeness, correctness and consistency. Accuracy of definition, input/output accuracy, accuracy of software behavioral, and the accuracy of an interface of a software function are very impotant.

Traceability analysis for the requirements between the Software Requirement Specification(SRS) and Software Design Specification(SDS) using a SIS-RT tool for scheduling, task synchronization, ISR processing and time management that are major requirements of real time kernel was undertaken. Traceability analysis between the requirement specification and design specification has also been performed for scheduling and task management as shown in figure 2.

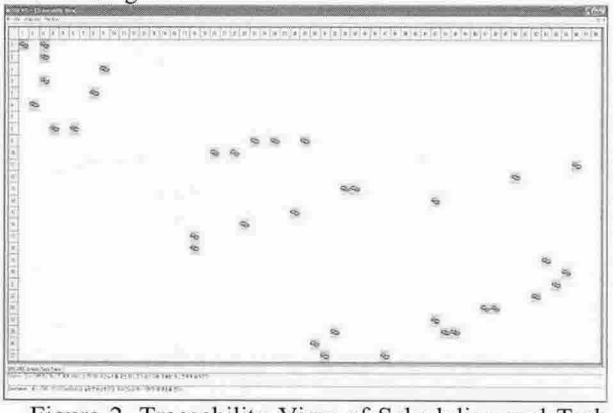

Figure 2. Traceability View of Scheduling and Task Management between SRS and SDS

2.3 Formal Verification

Verification can be performed automatically by the Model Checker/Model Certifier. Specification from model checking is usually based on the state machine

which is a model of the system. The procedure normally uses an exhaustive search of the state space of the system to determine if some specifications are true or not.

As consistency details the verification of the Safety-grade PLC operating system software requirement specification, verified to use commercially available Statemate Model Checker/Model Certifier tool supports. Verified about following six properties on Statechart based requirement specification that appear in as following.

a. Non-Determinism
b. Write/Write Race Condition
c. Range Violation
d. Drive to State
e. Drive to Config
f. Drive to Property

An error trace can be used as a counter example for the checked six properties and can help the verifier in tracking down where the error occurred.

2.4 Preparation for the Test Plan

Several test cases are necessary for testing the safety-grade PLC software. In the software requirement phase, a test plan should be prepared to satisfy the functional requirements and performance requirements of the safety-grade PLC.

The safety-grade PLC's verification environment schematic diagram is shown in figure 3. The real-time operating system and OSS/agents included the safety-grade PLC verified by using a Cantata++ Ver4.0 commercially available testing tool with Code Composer. The application program download for the safety-grade PLC will use pSET. pSET also checks the integrity of the memory value, status of register and special values inside the PLC.

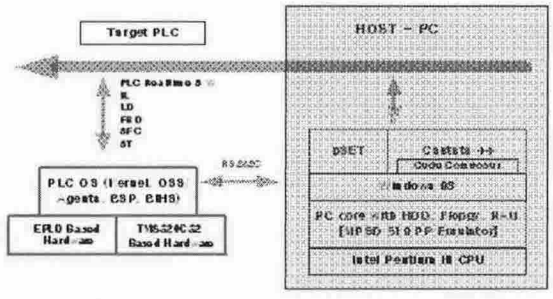

Figure 3 Test Environment Configuration for the PLC

2.5 Hazop Safety Analysis

At the requirement specification phase for the software development life cycle, present the HAZOP (Hazard and Operability) plan to achieve a hazard analysis. HAZOP is a technique that has been used successfully for a hazard analysis in industry such as a chemical factory. Achieved the software hazard analysis for developed guideline and checklist take advantage of this HAZOP concept in hazard analysis of the safety-grade PLC software requirement specification. After hazards and risks are collected, they are used in software verification and hazard analysis at the next step. Level of significance that is imposed on the various software requirements becomes necessary information to determine the resource to medicate in the development, verification, test etc.

3. Conclusion

Safety-grade PLC V&V's Systematic approach is a methodology, a tool and technique. Through the KNICS projects V&V methodology is established. The toolset used was a self-developed and a commercial available tool. The technique took advantage of the V&V techniques that use the formal verification technique. In this paper, at the requirement specification analysis phase, the suggested safety-grade PLC's V&V methodology, techniques and experiences were used. Introduced the software V&V experience at the requirement analysis phase using the proposed V&V methodology. V&V experiences are the licensing suitability evaluation, inspection and traceability analysis, formal verification, testing plan preparation, hazard analysis etc. The proposed V&V methodology satisfies the SRP/BTP-14 criteria for the safety software in nuclear power plants. The proposed V&V methodology is going to verify the upcoming software development life cycle in the KNICS projects

REFERENCES

[1] USNRC, *"BTP-14: Guidance on Software Reviews for Digital Computer-based I&C Systems,"* NUREG-0800 (1997).
[2] IEC 61131-3, "Programmable controllers - Part 3: Programming languages," (1993).
[3] IEEE Std-1012, "IEEE Standard for Software Verification and Validation Plans" (1986).
[4] IEEE Std-1028, "IEEE Standard for Software Reviews," (1997).
[5] Korea Atomic Energy Research Institute(KAERI), "Software Verification and Validation Plan(SVVP) for Software Requirement Specification(SRS) of Safety-grade Equipment and Device(SED)," KNICS-SED-(SRS) SVP121 (Rev. 00), Jan. 14, 2003. (In Korean)
[6] KAERI, "SVVP for Software Design Specification(SDS) of SED," KNICS-SED-(SDS) SVP131 (Rev. 00), Jan. 14, 2003. (In Korean)