Transactions of the Korean Nuclear Society Spring Meeting
Chuncheon, Korea, May 25-26 2006

Software Requirements V&V Works in KNICS Reactor Protection System

Gee Yong Park, Se Woo Cheon, and Kee Choon Kwon
Korea Atomic Energy Research Institue,150 Deokjin, Yuseong, Daejeon ,Korea
gypark@kaeri.re.kr, swcheon@kaeri.re.kr, kckwon@kaeri.re.kr

1. Introduction

A fully-digitalized reactor protection system (RPS), which is called the KNICS RPS in this paper, is being developed under the KNICS (Korea Nuclear Instrumentation & Control Systems) project in order to be used in newly-constructed nuclear power plants and also in the upgrade of existing analog-based RPS [1]. In the KNICS RPS, the trip functions such as signal comparison and voting logic are implemented on the software. Hence, the software in the KNICS RPS is crucial to nuclear power plants in that its malfunction may result in irreversible consequences and therefore, most of the software in RPS is classified into the safety-critical or safety-related class. In the KNICS project, the software used in a RPS is being developed under the rigorous procedure [1]. And also, an independent verification & validation (V&V) activities are arranged [2]. This paper presents V&V activities and main results performed at the requirements phase for the safety-critical software in the KNICS RPS.

2. V&V Activities at Requirements Phase

As is well known, the purpose of the software V&V process is to meet the nuclear regulatory requirements. For the S/W quality, the software life cycle process and the V&V tasks for the requirements phase are depicted in Fig.1. The V&V activities for KNICS RPS software requirements specification (SRS) are the review of the licensing suitability, the Fagan inspection [3], the formal verification, the S/W configuration management, the S/W safety analysis, and the integration test plan. In this section, among these activities, the former three activities are described.

2.1 Review of Licensing Suitability

The purpose of the review of the licensing suitability is to investigate the satisfaction of the S/W requirements to the acceptance criteria of the regulatory guide and codes/standards. In the V&V activities in the KNICS project, the acceptance criteria are established according to the BTP HICB-14 [4]. After the review process for the KNICS RPS SRS, the major review result was about the deficiency in the exceptional handling between processor test modes.

2.2 Inspection & Traceability

For a detailed inspection on the requirements in SRS, the method proposed by Fagan [3] was adopted. The inspection was performed with respect to the consistence, completeness, and correctness by the use of the well-defined checklists reflecting those three viewpoints. Fig.2 shows one of the checklist items and inspection results.

The traceability is to trace each requirement allocated onto the software in the system function requirements to the SRS, or reversely. In this process, the CASE tool, SIS-RT, proprietarily developed for the KNICS project was used as shown in Fig.3. Fig.3 displays the result of requirements traceability matrix for the bypass requirements related to CPC-CWP, where '∞' means there is a matching between both requirement items and '?' indicates there is no matching requirement.

2.3 Formal Methods

In order to improve the quality and attain the safety of safety-critical software in the early phase of the software development process, the KNICS RPS SRS written by natural language is specified by a formal specification method. For the formal specification and verification of the KNICS RPS SRS, the NuSRS tool was developed proprietarily for KNICS project. The overall configuration of NuSRS is depicted in Fig.4. The formal specification is performed by the formal specification language called NuSCR [5]. In the NuSCR, three formal specification types are provided: SDT (Structured Decision Table) for function-based operation such as the simple logic operation, FSM (Finite State Machine) for state-based operations such as the trip hysterisis, and TTS (Timed Transition System) for timing-based operations such as the trip delay. The formal specifications for a certain trip operation module can be converted automatically into the input file used for a model checker in NuSRS. Fig.5 shows the formal specifications for the pressurizer-low-pressure trip. The properties to be checked by the model checker are six cases where two (deadlock-freeness and non-determinism) are related to the model structure and the other four properties are operation-dependent. All the safety-critical function modules in the SRS were verified. The behaviors of all the requirements were satisfied but the exceptional case occurrence among test modes and the operation bypass function in the trip logic.

Besides the NuSRS, another verification process was performed in this KNICS RPS SRS. In this process, the HALDEN prover [6] was employed. Fig.6 shows the

HALDEN prover. The purposes of this verification process are two folds: One is to provide the verification process with the diversity viewpoint and the other is to simulate the behavior of the specifications. The Halden prover provides the simulation and theorem-proving functions. This could obviously compensate for the role of the model checker, i.e., from simulations, it was found that the "Setpoint Rising Bistable" logic in the KNICS RPS SRS had a defect in its own sequential logic such that the trip set point could not returned to its original value from the lower value by a trip hysterisis for a certain trend of measured signal. The theorems to be proved are almost same as those four properties in the NuSRS model checker.

3. Conclusion

All the V&V outputs performed at the requirement phase for KNICS RPS SRS are going to be reflected in the revision process of the software requirements and the iteration V&V procedure will be performed on the revised version of the SRS in order to proceed safely to the next software life cycle step, the design phase.

REFERENCES

[1] J. H. Park, D. Y. Lee, and C. H. Kim, "Development of KNICS RPS Prototype", Proceedings of ISOFIC 2005, Session 6, pp.160~161, Tongyeong, Korea, Nov. 1~4, 2005.
[2] G. Y. Park and K. C. Kwon, "Software Verification & Validation for Digital Reactor Protection System", Information and Control Symposium, pp.190~192, 2005.
[3] M. E. Fagan, "Design and Code Inspections to Reduce Errors in Program Development", IBM System Journal, vol.15, no.3, 1976.
[4] NUREG-0800, "Standard Review Plan: BTP HICB–14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" USNRC, 1997.
[5] J. Yoo and S. Cha, "A Formal Software Requirements Specification Method for Digital Plants Protection Systems", CS/TR 2003-191, KAIST, 2003.
[6] T. Sivertsen, Formal Development of the HRP Prover – Part 1: Syntax and Semantics, HWR-455, OECD Halden Reactor Project, 1996.

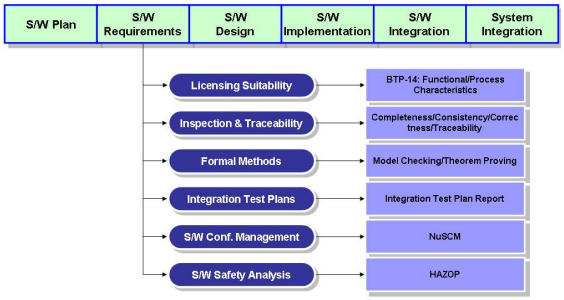

Figure 1. V&V tasks at requirements phase for KNICS RPS.

Item	R.G./Code/Std	Inspection Items		Inspection Results
Completeness of S/W Function Definitions	BTP HICB-14, Chap. 3.3a	Are all operational modes S/W shall perform described ? S/W functions and behaviors to be executed in each operational mode all described ?	Operation Bypass	NOT complete is CPC-CWP
			Setpoint Settings	NOT complete is trip hysteresis function in the manual reset variable setpoint module
			Test Mode	NOT complete is BP1 PT scheduler

Figure 2. One of checklist-based inspection result.

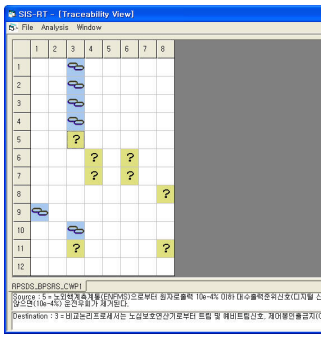

Figure 3. One result of requirements traceability by SIS-RT.

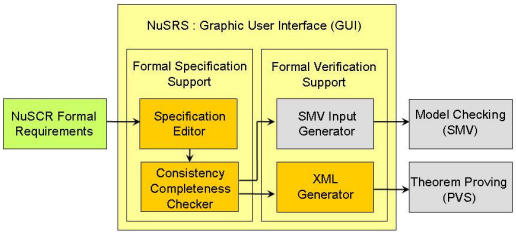

Figure 4. Configuration of NuSRS.

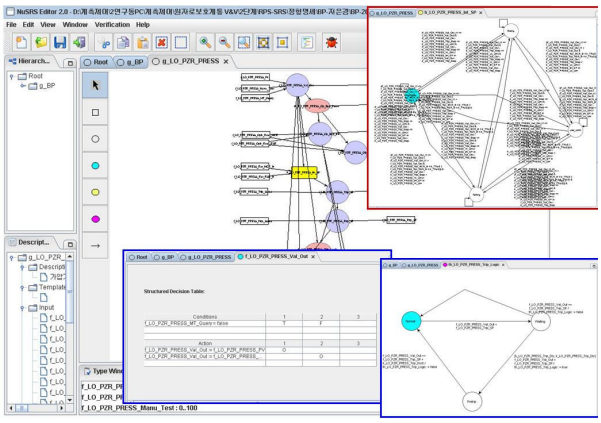
Figure 5. Formal specifications for the PZR_LO_P trip.

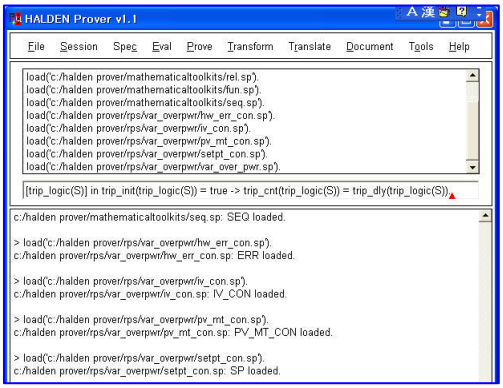

Figure 6. HALDEN prover.