Techniques and Tools for Software Qualification in KNICS

Kyung H. Cha, Yeong J. Lee, Se W. Cheon, Jang Y. Kim, Jang S. Lee, Kee C. Kwon
Instrumentation and Control·Human Factors Research Division, KAERI,
P.O. Box 105, Yuseong, Daejeon, 305-600, KOREA {khcha, ex-yjlee426,swcheon, jykim, jslee, kckwon}@kaeri.re.kr

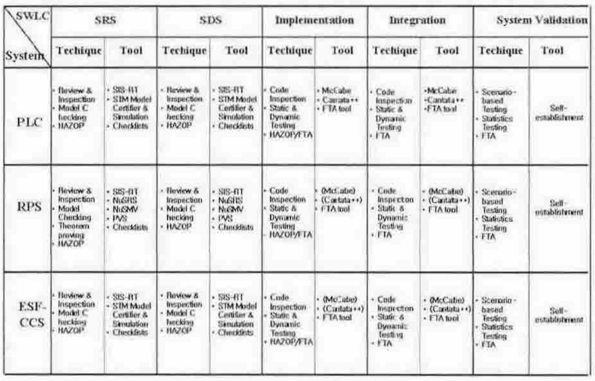
1. Introduction

This paper describes techniques and tools for qualifying safety software in Korea Nuclear Instrumentation and Control System (KNICS). Safety software are developed and applied for a Reactor Protection System (RPS), an Engineered Safety Features and Component Control System (ESF-CCS), and a safety Programmable Logic Controller (PLC) in the KNICS [1].

Requirements and design specifications of safety software are written by both natural language and formal specification languages. Statechart is used for formal specification of software of the ESF-CCS and the safety PLC while NuSCR [2] is used for formal specification of them of the RPS. pSET (POSCON Software Engineering Tool) as a software development tool has been developed and utilized for the IEC61131-3 based PLC programming.

The qualification of the safety software consists of software verification and validation (V&V) through software life cycle, software safety analysis, and software configuration management, software quality assurance, and COTS (Commercial-Off-The-Shelf) dedication.

The criteria and requirements for qualifying the safety software have been established with them in Software Review Plan (SRP)/Branch Technical Positions (BTP)-14 [3], IEEE Std. 7-4.3.2-1998 [4], NUREG/CR-6463 [5], IEEE Std. 1012-1998 [6], and so on. Figure 1 summarizes qualification techniques and tools for the safety software.



SWLC / System	SRS		SDS		Implementation		Integration		System Validation	
	Techique	Tool	Techique	Tool	Techique	Tool	Techique	Tool	Techique	Tool
PLC	· Review & Inspection · Model C hecking · HAZOP	· SIS-RT · STM Model Certifier & Simulation · Checklists	· Review & Inspection · Model C hecking · HAZOP	· SIS-RT · STM Model Certifier & Simulation · Checklists	· Code Inspection · Static & Dynamic Testing · HAZOP/FTA	· McCabe · Cantata++ · FTA tool	· Code Inspection · Static & Dynamic Testing · FTA	·McCabe ·Cantata++ ·FTA tool	· Scenario-based Testing · Statistics Testing · FTA	Self-establishment
RPS	· Review & Inspection · Model Checking · Theorem proving · HAZOP	· SIS-RT · NuSRS · NuSMV · PVS · Checklists	· Review & Inspection · Model C hecking · HAZOP	· SIS-RT · NuSRS · NuSMV · PVS · Checklists	· Code Inspection · Static & Dynamic Testing · HAZOP/FTA	· (McCabe) · (Cantata++) · FTA tool	· Code Inspecton · Static & Dynamic Testing · FTA	· (McCabe) · (Cantata++) · FTA tool	· Scenario-based Testing · Statistics Testing · FTA	Self-establishment
ESF-CCS	· Review & Inspection · Model C hecking · HAZOP	· SIS-RT · STM Model Certifier & Simulation · Checklists	· Review & Inspection · Model C hecking · HAZOP	· SIS-RT · STM Model Certifier & Simulation · Checklists	· Code Inspection · Static & Dynamic Testing · HAZOP/FTA	· (McCabe) · (Cantata++) · FTA tool	· Code Inspecton · Static & Dynamic Testing · FTA	· (McCabe) · (Cantata++) · FTA tool	· Scenario-based Testing · Statistics Testing · FTA	Self-establishment

·SIS-RT : Software Inspection Support and Requirements Traceability
·NuSRS: Nuclear Software Requirement Specification
·NuSDS: Nuclear Software Design Specification
·NuSMV: Nuclear Symbolic Model Verifier
·PVS: Prototype Verification System
·STM: Statemate MAGNUM

Figure 1. Techniques and tools for software qualification in KNICS

2. Techniques and Tools for Software Qualification

2.1 Review and Inspection (R&I)

Review and Fagan Inspection [2] are applied for verifying overall outputs through life cycle V&V activities.

The 3rd party review has been projected for qualifying the conceptual design and software requirements of the RTOS and the communication software for the safety PLC.

Checklists [7] were well structured within software V&V procedures and they are used for the R&I. Traceability analysis is also applied to software development life cycle (SDLC) activities. The R&I task scan be processed with the aids of SIS-RT (Software Inspection Support and Requirement Traceability) tool [2], focusing on the systematic software inspection and requirements traceability analysis for the whole software life-cycle based on natural language documents.

2.2 Interactive Formal Verification

Interactive formal verification is another technique for qualifying the software requirements and design. Model checking has been applied to verify the formal specifications of safety software. Figure 2 illustrates the model checking for the formal verification.

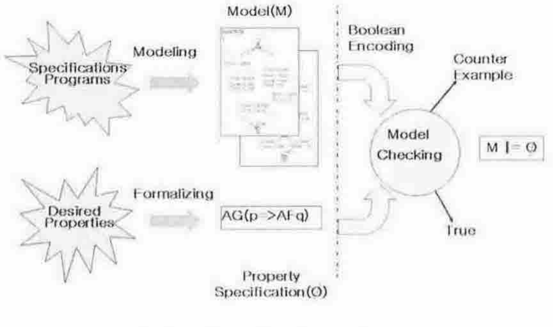


Figure 2. Model checking for formal verification

To support the interactive formal verification, Symbolic Model Verifier (SMV) and Prototype Verification System (PVS) tools have been tried to verify Nuclear Software Cost Reduction (NuSCR)-based software specification of the RPS, while Statemate MAGNUM (STM) Model Certifier has been applied to verify Statechart-based specification of software requirements for the safety PLC.

2.5 Automated Software Testing

Nuclear regulators tend to consider software testing as part of software V&V when they review a software-based I&C system. Accordingly, the V&V tasks for testing [6] shall be applied to test safety software for the RPS, the ESF-CCS, and the safety PLC in the KNICS.

Software testing tasks can be automated by automated software testing tools. To do save time and efforts for software testing, McCabe and Cantata++ tools are qualified and used for automating or supporting the software testing life cycle (STLC) tasks. In addition to these tools, an engineering simulator may be used for system testing of the safety software.

2.6 Software Safety Analysis

Software safety analysis (SSA) is required if software is applied to a safety I&C system, and the SSA shall be performed independently for the safety software through SDLC. SSA techniques include HAZOP (HAZard OPerability) methodology [8] and Fault-Tree Analysis (FTA). The HAZOP is based on the specialized checklists including guidewords and the FTA is to be supported by the pre-developed FTA tool developed and experienced by the PSA group at Korea Atomic Energy Research Institute.

2.7 Software Configuration Management

Evaluation of Software Configuration Management (SCM) is also required for design outputs through the life cycle V&V. The software configuration items, including software programs, are managed with the SCM procedure and supported by NuSCM tool.

28 Dedication of COTS Software

COTS (Commercial-Off-The-Shelf) software is applied partly for the safety PLC and the COTS dedication consists of the dedication work order, the dedication plan, the dedication processes, and the audit result report.

2.9 Quality Assurance (QA)

The QA plan and the QA procedure have been written for the KNICS project. Software QA is also applied to improve software quality for the KNICS through an audit of software. A software QA plan and a software QA procedure shall be written under the QA plan and manual and they are applied through the SDLC of the safety software.

3. Conclusions

The qualification of safety software for the KNICS has been performed for software verification and validation (V&V) through software life cycle, software safety analysis, software configuration management, software quality assurance, and COTS dedication. The various techniques and tools have also been qualified and applied for supporting the software qualification.

Our experience on the requirements V&V and the design V&V of safety software for the KNICS prototype shows that the techniques and their tools are very efficient for qualifying the safety software while we feel that the used checklists should be refined because they are very useful and important tool for the software qualification in the KNICS.

ACKNOWLEDGMENTS

This work has been performed for "Development of the Licensing Technology for Digital I&C" which is a part of the KNICS project and is supported by the Korean Ministry of Science and Technology (MOST) from 2001 to 2008. The authors would like to thank Dr. Han S. Son for his contributions on R&I and formal verification for recent 3 years.

REFERENCES

[1] Chang H. Kim and Jae B. Han, Software Development of Safety Systems for Nuclear Power Plant, Proceedings of the First Workshop on Development and Verification of Safety-Critical Software, Seoul, Korea, pp.11-25, Dec.3, 2003.

[2] Seo R. Koo, et al., Development of Software Requirement Analysis Tool for NPP Software Fields Based on Software Inspection and Formal Method, Proceedings of International Symposium on the Future I&C for NPP (ISPFIC 2002), Seoul, Korea, pp.159-164, Nov. 7-8, 2002.

[3] NUREG-0800, SRP/BTP-14: Guidance on Software Reviews for Digital Computer-based I&C Systems, USNRC, Washington D.C., July, 1997.

[4] ANSI/IEEE Std. 7-4.3.2-2003 (Revision of IEEE Std 7-4.3.2-1993), IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

[5] NUREG/CR-6463, Review Guidelines on Software Languages for Use in NPP Safety Systems, NRC, USA.

[6] IEEE Std. 1012-1998(Revision of IEEE Std 1012-1986), IEEE Standard for Software Verification and Validation Plans.

[7] Han S. Son, et al., Checklists Development for Software Verification of Reactor Protection System, Proceedings of the KNS 03 Spring Conference (CD Material), GyeongJu, Korea, May 29-30, 2003. (In Korean)

[8] Jang S. Lee, et al., HAZOP Methodology for Safety Analysis of Software Requirements Specifications, Proceedings of the KNS 03 Spring Conference (CD Material), GyeongJu, Korea, May 29-30, 2003. (In Korean)