The Qualification Experiences for Safety-critical Software of POSAFE-Q

Jang Yeol Kim[a*] , Kwang Seop Son[a], Se Woo Cheon[a], Jang Soo Lee[a], Kee Choon Kwon[a]
[a]Instrumentation and Control / Human Factors Division, Korea Atomic Energy Research Institute, 1045 Daedeok-daero, Yuseong-gu, Daejeon, Korea 305-353
[*]*Corresponding author: jykim@kaeri.re.kr*

1. Introduction

Programmable Logic Controllers (PLC) have been applied to the Reactor Protection System (RPS) and the Engineered Safety Feature (ESF)-Component Control System (CCS) as the major safety system components of nuclear power plants. This paper describes experiences on the qualification of the safety-critical software including the pCOS kernel and system tasks related to a safety-grade PLC, i.e. the works done for the Software Verification and Validation, Software Safety Analysis, Software Quality Assurance, and Software Configuration Management etc.

2. V&V Methods and Results

In this section some of the V&V techniques used in the KNICS Project are described. These techniques include a technical evaluation, licensing suitability evaluation, inspection and traceability analysis, formal verification, software safety analysis, software quality assurance, COTS dedication and its software configuration management etc.

2.1 Qualification organization

To perform the qualification work for a safety-critical software, it is very important to clearly define the responsibilities assigned to various groups of the assurance organization. The Development Team is responsible for producing design output during the entire software life cycle. The teams for the Software Verification & Validation(SVV) and Software Safety Analysis(SSA) are responsible for safety qualification of the design output produced by development team. First of all, prior to use Commercially Off The Shelf(COTS) software tool should be dedicated by quality assurance organization. The Software Configuration Management under Software Quality Assurance is responsible for configuration identification, status accounting, revision control on all of the design output and its verification results respectively. The well-structured qualification organization in KNICS project is shown in Figure 1.

2.2 Review of the licensing suitability

The safety-critical software qualification has been performed based on the following Code&STD framework shown in Figure2 where the most recent edition is used for each design output and verification. Thick line boxes in Figure 2 are closely related to software qualification criteria.

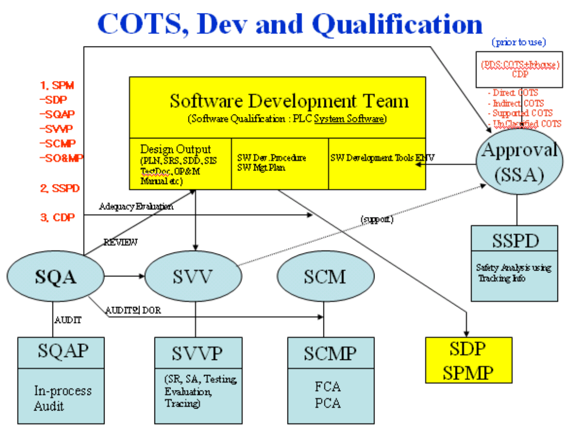

Fig. 1 Well-structured qualification organization for safety-critical system

(SPM : Software Program Manual, SDP: Software Development Plan, SQAP: Software Quality Assurance Plan, SVVP: Software Verification and Validation, SCMP : Software Configuration Management Plan, SO&MP : Software Operation and Maintenance Plan, SSPD : Software Safety Plan Description, CDP: Commercial Off the Shelf Dedication Plan, COTS: Commercial Off The Shelf Software, SQA: Software Quality Assurance, SVV: Software Verification and Validation, SCM: Software Configuration Management), SR: Software Review, SA: Safety Analysis, FCA: Functional Configuration Audit, PCA: Physical Configuration Audit)

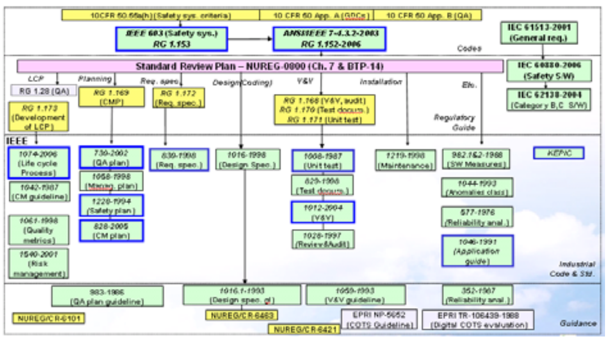

Fig. 2 Code and Standard framework for qualification of safety-critical system.

2.3 Inspection and Traceability Analysis

Through the traceability analysis and an inspection of the matrix style by using contents based KEY REQUIREMENTS, the missing requirements in the specifications ranging from the SRS to the SDS, including Implementation phase, Component Test, Integration Test and System Test have been easily found. Figure 3 shows one of the summarized results from the SRS to the SDS.

Fig 3. Traceability Martix

2.4 Software Testing

Software testing consisted of a component test, an integration test, and a system test. Running these tests execution produced a test plan generation, a test design generation, a test case generation and a test procedure generation according to the Software Test Life Cycle (STLC) as shown in Figure 4.

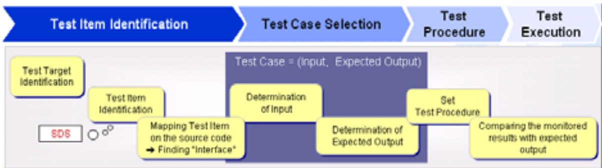

Fig. 4 Testing process by Test Life Cycle.
(Note, SDS : Software Design Specification.)

To determine the test objects for the integration test, the software design specification of the pCOS and system task were analyzed, and the software components and the hardware components have been identified. As shown in Fig 5, we focused on software integration test (SIT) and hardware integration test (HIT) of heterogeneous layers including hardware layer, OS layer, and application layer. The PLC applied in application layer will be implemented as an application software for Reactor Protection System(RPS).

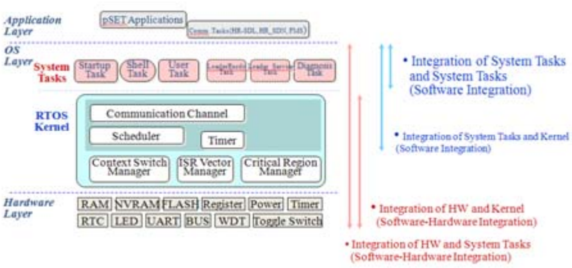

Fig. 5 Integration tree for pCOS and System Tasks

2.5 Software Configuration Management

Software Configuration Management (SCM) was performed following a software quality assurance policy during the whole software life cycle. Inconsistencies among the software configuration items have been found. Some of the reported anomalies have been resolved throughout the software configuration management process. Figure 6 shows as an example of the SCM processes.

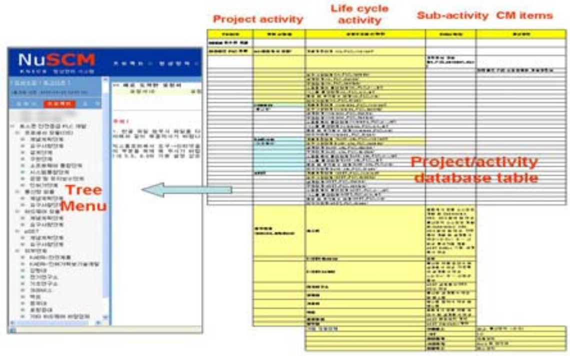

Fig 6. Software Configuration Management by NuSCM

3. Conclusions

Applied V&V approach for a safety-grade PLC have been used methodologies, tools and techniques. Our V&V scheme has been well set up through these works, i.e. through the KNICS project. The toolset used was either a self-developed or commercially available one. The technique took advantage of the V&V techniques using a formal verification technique. We have investigated and performed all the software V&V processes in the phase of the requirements, design, implementation, component testing, integration testing and system testing by using the V&V methodology described above. The major parts of our V&V works were the licensing suitability evaluation, inspection and traceability analysis, formal verification, hazard analysis, testing techniques including a component test, integration test and system test. The applied V&V methodology satisfies the SRP/BTP-14 criteria for the safety software in nuclear safety systems. Our V&V experience indicates the applied techniques and supporting tools used in the KNICS project were very efficient for qualifying the safety-grade PLC to be used for nuclear safety systems. Our V&V methodology will get improved through the upcoming related software qualification projects.

REFERENCES

[1] J.Y. Kim, S.W. Cheon, J.S. Lee, Y.J. Lee, K.H. Cha, and K.C. Kwon, "Software V&V Methods for a Safety Grade Programmable Logic Controller," Proceedings of the International Conference on Reliability, Safety and Hazards-2005, Dec. 1, 2005.

[2] K.H. Cha , J.Y. Kim, S.W. Cheon, J.S. Lee, Y.J. Lee, and K.C. Kwon, "Software Qualificaiton of a Programmable Logic Controller for Nuclear Instrumentation and Control Applications," 2006 WSEAS International Conferences(ISCGAV'06), Crete, August 2006.