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 ^aInstrumentation 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 safetycritical 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.

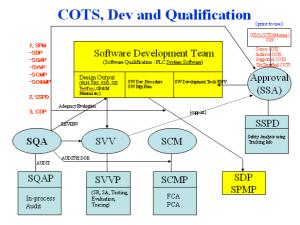


Fig. 1 Well-structured qualification organization for safetycritical system

(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

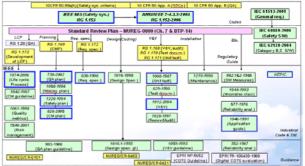


Fig. 2 Code and Standard framework for qualification of safety-critical system.

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.

	ARE40 27/77 14/0-101.000					AMEND 239 1008-508.84/00.38-385-505		
	645-5 00702-0052020049 64532949 :00702-00520 6359949		10	292	42U2	0238353		
		53	243 19 1 2947 125	492				
			GPLCS9 GHD: ++	435				
		11.4	2828749	435				
_	8400-20 #32882 213 839	12.0	2512742	632	-		-	-
5.1	2033 43 2342 2242 2252 4 653 000 242 M2530 004454452 922 4850 M70-20 82288 Pottes AUC			1001123 23.0329	9.±	82 5500 22590 00000 2 9 23	일양문제 프로토들이 영식제 기술요한	
53	다 104월 전문화5 동자02-70 등 다 22 동료 고 1-3 동경 문 보 2 가 3 4 명 2 가 8 가 로 요 요 요 요 요 요 요 요 요 요 요 요 요 요 요 요 요 요			#25%_03 # # # #	24	24	24	
5.2	환경 환 20 10 <td< td=""><td></td><td></td><td>2929 2959 2954 2954 29 2929 2929 2929</td><td>8.2</td><td>¥¥034म अ¥1034मन खभ</td><td>60208</td><td></td></td<>			2929 2959 2954 2954 29 2929 2929 2929	8.2	¥¥034म अ¥1034मन खभ	60208	
					6.2.1	응유에요리 X3M 급은받니	62328	
					6.2.3		69346	
					9,2,9	Transmitr_IIM(40(41 - QU)	60509	
					9,2,9	Send See To OB	eauxe	
5.3	10702-20 중32호급 2133 중3월 보 253 4 16 2 5 83 프로토운 // 중54 (1010) 호수리 프로토운 // (20140) 418월 17 2년 // 중50, 18702-20 중 22 중로 Patters, 3184,		625X8		1.2	●3 5008 22598 (MIN)2 2 9 23	일강류미 프로토콜이 정시미 기술수당	
5.1	승수권은 GIOIBIA 중국은 안문하기 책 IN CRC 같은 장면은 사용했다.		63848				080 경사 분개방영 유망	
61.2	0.28 00093 2576 28844 MA N292 25208 CACE /8 00		62028				아이 경기 관계학생 수학	

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.

Test Item Identification	Test Case Selection	Test Procedure	Test Execution				
Test Case = (Input, Expected Output)							
Identification Test Rem Identification	Determination	Set Test Procedure					
SDS 0 ° Mapping Test Iten on the source cod → Finding "Interfac	te Expected Oute	of Comp	oaring the monitored ults with expected output				

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).

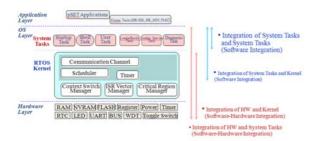


Fig. 5 Integration tree for pCOS and System Tasks

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 Qualification of a Programmable Logic Controller for Nuclear Instrumentation and Control Applications," 2006 WSEAS International Conferences(ISCGAV'06), Crete, August 2006.