원전 소프트웨어의 품질요건과 ISO 소프트웨어 표준의 적합성에 대한 분석

서용석*, 박희윤*, 김종명**, 김준엽**, 김현수***
*한국원자력연구소 계측제어・인간공학연구부
**삼창기업주식회사 제어기술연구소
***충남대학교 컴퓨터공학과
e-mail:yssuh@kaeri.re.kr

An Analysis of Compatability Between Software Quality Requirements for Nuclear Power Plants and ISO Software Standards

Yong-Suk Suh*, Heui-Youn Park*, Jong-Myoung Kim**, Joon-Yeop Kim**, Hyeon-Soo Kim***
*I&C and HF Div., Korea Atomic Energy Research Institute
**Control Tech. Research Inst., Samchang Enterprise Co., Ltd.
***Dept. of Computer Engineering, Chungnam National University

요 약

본 논문은 안전필수 소프트웨어라 할 수 있는 원전(원자력발전소) 소프트웨어의 품질요건을 원자력법, 시행규칙, 규제지침, 표준에 입각하여 분석하였고, 국제표준인 ISO(International Organization for Standardization) 소프트웨어 표준이 원전 소프트웨어 품질요건에 부합될 수 있는지를 ISO/IEC 12207을 중심으로 분석하였다. 현재는 요구되고 있지 않으나 앞으로 원전 소프트웨어 공급자에 대한 소프트웨어 개발능력 평가 시 소프트웨어 인증취득을 요구함으로써 원전 소프트웨어의 품질향상과 안전성을 도모할 수 있는 방법으로 제안하였다. 원전 소프트웨어에 요구되는 안전성분석에 대해서 검토하였다.

1. 서론.

원전의 안전기능을 수행하는 소프트웨어는 안전필수(safety critical) 소프트웨어로 분류된다. 안전필수 소프트웨어는 그 고장으로 인해 인간의 생명을 위협할 수 있는 소프트웨어를 의미한다. 국내 원전의 안전필수 소프트웨어는 과학기술부에서 제정한 원자력법을 준수하여 개발되어야 하며, 이러한 법적 요건을 확인하는 기관인 한국원자력안전기술원(KINS)에 의해 심사 및 인허가(licensing)를 득해야 원전에 사용될 수 있다.

품질은 제품 또는 용역이 사용자의 요구사항을 만족하기 위해 관여되는 총체적인 특성들의 집합이다. 품질은 포괄적이고 광의적인 의미로 사용되는 일반적인 용어이다. 소프트웨어 품질요건 역시 일반적인 품질요건을 벗어나지 않으며 소프트웨어 특성에 따른 요건이 추가되어 형성된다. 본 논문은 원전 소프트웨어 품질요건을 원자력법, 시행규칙, 규제지침, 표준에서 어떻게 명시하고 있는지 분석한다.

비정부단체인 ISO는 제품 또는 용역 등의 품질향상을 위해 그리고 세계무역에 있어서 국가 간 기술적 격차 해소 및 무역장벽 제거를 위해 국제표준을 제정한다. 이 단체는 소프트웨어 분야의 표준도 다수 제정하고 있는데 특별히 주목할 만한 표준으로 12207, 9001과 90003, 15504, 9126, 14598 등이 있다. 이러한 표준은 소프트웨어 품질향상을 목표로 하며 그동안 축적된 소프트웨어 공학적 사례(practice)를 반영하여 제정 및 개정된다. 이들 표준을 얼마나 정확하고 충분히 준용하여 소프트웨어 개발이 이루어지는지를 소프트웨어 전문가가 평가하는 과정이 인증(certification)이다. 국내 소프트웨어 산업에서 국제표준 인증의 중요성이 대두되고 있다.

원전 소프트웨어의 경우, 소프트웨어 인증의 필

요성이나 효과에 대해 아직까지는 크게 인식되고 있지 않은 실정이다. KINS는 원전 소프트웨어 심사 및 인허가 시, 소프트웨어 인증을 강력히 요구하고 있지 않다. 본 논문은 KINS가 원전 소프트웨어 수락기준으로서 소프트웨어 인증취득을 요구하게 되면 원전 소프트웨어의 품질이 향상되고 결국은 원전의 안전성에 기여할 수 있는 방법으로 제안한다.

원전 소프트웨어의 품질요건 중 특이사항은 안전성분석요건이다. 보편적으로 소프트웨어가 안전하다고 정량적으로 증명하는 방법이 소프트웨어 공학적인 기술측면에서 충분히 성숙되어 있지 않다고 판단되며 현재로선 정성적인 분석 노력이 최선인 것으로 인식되고 있다. 본 논문은 원전 소프트웨어 안전성 분석에 대한 현안사항을 검토한다.

2. 원전 소프트웨어 품질요건

국내 원자력법 제12조에 의하면 원전 소프트웨어 공급자는 원자력법 시행규칙을 만족하는 품질보증계획서를 KINS에 제출하여 심사를 받아야 한다. 그 계획서는 시행규칙의 제67조부터 85조까지 18조항에 걸쳐 언급하고 있는 품질보증기준을 만족하여야 한다. 그 기준의 주요 골자는 제반 품질관리, 문서화, 시험, 검사, 감사, 시정조치 등의 활동을 정의하고 명시하라는 것이다. 과학기술부 고시 제2001-47호는 위와 같은 기준을 보다 상세히 설명하고 있는 표준(또는 규격)인 한국전력산업기술기준(KEPIC)의 원자력품질보증기준(QAP)을 만족하는 품질보증계획서 작성을 권고하고 있다. KEPIC QAP-2 2.7에서는 소프트웨어 수명주기, 분석, 설계, 형상관리, 시험, 검사, 시정조치, 상용 소프트웨어 사용 등으로 구분하여 품질보증기준을 제시하고 있다. KEPIC QAP는 미국의 ASME에서 발행한 원자력품질보증기준(NQA)을 번안하여 제정된 것이다. 이와 같이 국내 원자력과 관련된 법적 사항들은 미국의 영향을 받고 있는 실정이다. 이는 국내 최초의 원전이 미국에 의해 건설된 이후 지금까지도 미국의 기술에 의해 많은 부분이 의존되어 건설되기 때문이다.

KINS는 원전 소프트웨어 심사 시 위와 같은 법적 요건을 만족하고 있는지 우선 확인한다. 추가적으로 KINS는 자체적인 원전 안전성 심사지침을 마련하여 원전 소프트웨어에 대한 심사기준을 갖고 있다 [1]. 이 심사기준에 따르면, 원전 소프트웨어 심사자는 소프트웨어 공급자가 원전 품질보증요건을 만족하고 동시에 소프트웨어 수명주기가 잘 정의된 품질보증계획을 수립하였는지 검토하고, 그 계획에 따라 소프트웨어 산출물이 생산되었는지 확인하는 것이다. 이 심사기준은 구체적인 지침을 언급하는 과정에서 미국의 원전규제지침(RG)을 심사근거로 삼고 있다. 원전 소프트웨어에 적용되는 RG로는 1.152와 1.168부터 1.173까지 총 7개의 RG를 들 수 있다. RG 1.152는 원전 소프트웨어의 품질은 IEEE 표준인 7-4.3.2에서 제시하는 품질기준을 만족하라고 권고하고 있다. 또한 RG 1.168은 소프트웨어 확인, 검증, 검토, 감사를 수행하는데 있어서 IEEE 1012와 1028을 참조할 것을 권고하며, RG 1.169는 형상관리를 수행하는데 IEEE 828, 1042를, RG 1.170은 시험문서를 작성하는데 IEEE 829를, RG 1.171은 단위시험을 수행하는데 IEEE 1008을, RG 1.172는 소프트웨어 요건명세서를 작성하는데 IEEE 830을, RG 1.173은 소프트웨어 수명주기 프로세스를 수립하는데 IEEE 1074를 참조할 것을 권고하고 있다. 이와 같이 원전 소프트웨어 규제지침은 소프트웨어의 품질보증에 필수적인 최소한의 요건을 명시하고 있고, 구체적인 내용은 IEEE 표준을 참조할 것을 권고하고 있다. 이와 같이 국내 원전 소프트웨어는 미국의 IEEE 표준을 준용하여 개발되어야 한다. 현재 소프트웨어 관련 IEEE 표준은 40여종 이상이 존재한다.

원전 소프트웨어 개발에 절대적으로 적용해야 하는 표준인 IEEE 7-4.3.2에서는 소프트웨어 품질기준으로 IEEE/EIA 12207.0에서 명시하는 품질보증활동이 만족되어야 함을 언급하고 있다. 물론 소프트웨어 품질보증표준인 IEEE 730도 만족해야 함을 요구하고 있다. 본 논문은 IEEE/EIA 12207.0 표준에 주목한다. 이 표준은 ISO/IEC 12207이라는 국제표준을 채택한 표준이다. 미국방성이 1998년도에 그동안 채택했던 소프트웨어 군용표준인 498을 취소하고 대신에 IEEE/EIA 12207.0을 사용한다는 내용에서도 이 표준은 신뢰성이 있는 표준이다 [2]. ISO/IEC 12207은 획득(acquisition), 공급(supply), 개발(development), 운영(operation), 유지보수(maintenance)라는 5개의 핵심(primary) 프로세스를 정의하고, 문서화(documentation), 품질보증(quality assurance), 형상관리(configuration management), 확인(verification), 검증(validation), 공동검토(joint review), 감사(audit), 문제해결(problem resolution)이라는 8개의 지원(support) 프로세스를 정의하고, 관리(management), 기반구조(infrastructure), 개선(improvement), 훈련(training)이라는 4개의 조직 수

명주기(organizational life cycle)이라는 프로세스를 정의한다. 이들 각각의 프로세스에는 고유의 활동(activity)들이 명시되어 있다. 따라서 이 표준은 소프트웨어 수명주기 전체에서 필요한 전반적인 활동을 명시하고 있다. 원전 소프트웨어 개발에도 이러한 활동이 수행되어야 함은 당연하다.

결론적으로 국내 원전 소프트웨어 품질요건은 다음과 같이 요약될 수 있다. 첫째, KEPIC QAP를 기본적으로 만족하라는 것이며, 둘째, IEEE 소프트웨어 표준을 준수하라는 것이며, 셋째, IEEE/EIA 12207과 동일한 ISO/IEC 12207에서 제시하는 소프트웨어 프로세스 모델을 만족하라는 것이다.

3. 원전 소프트웨어에 적용 가능한 국제인증

본 논문은 원전 소프트웨어 개발에 적용해야 하는 ISO/IEC 12207과 호환성을 갖는 SPICE(Software Process Improvement and Capability dEtermination), CMMI-SW(Capability Maturity Model Integration-Software), ISO 9001 인증에 대해 분석한다.

SPICE는 ISO 15504 표준을 의미하는 명칭이다. 이 표준은 프로세스를 평가하고 개선하는 활동을 통해 소프트웨어의 품질과 생산성이 향상될 수 있다는 소프트웨어 공학적 경험과 사례를 바탕으로 형성되었다. 과거 소프트웨어 산업에는 여러 종류의 프로세스가 각자 산재되어 형성되었는데, 이러한 프로세스를 통일된 기준으로 평가하자는 움직임과 산재된 프로세스들을 하나의 표준으로 제정할 필요가 있다는 움직임은 안전필수 소프트웨어가 요구되는 환경 예를 들어 군사용 소프트웨어에 대한 프로세스 요건으로부터 비롯되었다고 볼 수 있다. ISO는 이러한 요구를 충족하는 표준으로 15504를 제정하게 된다. 이 표준은 프로세스 능력수준을 <표 1>과 같이 6단계로 구분하여 평가할 수 있도록 지침을 제시한다.

<표 1> SPICE의 프로세스 능력수준

능력수준	의미
0	불완전한(incomplete) 프로세스임
1	초보적인(performed) 프로세스임
2	관리가 적용된(managed) 프로세스임
3	잘 정의된(established) 프로세스임
4	결과를 예측하는(predictable) 프로세스임
5	최적을 추구하는(optimizing) 프로세스임

이 표준은 구매자-공급자(customer-supplier), 엔지니어링(engineering), 지원(support), 관리(management), 조직(organization)이라는 5개의 프로세스 범주를 구분하여 총 38개의 프로세스와 249개의 사례를 정의하고 있다. 이 표준은 12207에서 정의된 프로세스와 호환성을 갖으며 이 프로세스를 평가하거나 개선하고자 하는 고객을 대상으로 지침을 제공한다. 안전필수 소프트웨어를 공급하려는 조직은 최소한 SPICE의 3단계 능력수준이 요구된다는 연구가 있었다 [3].

CMMI는 미국 카네기멜론대학의 소프트웨어공학센터에서 미국방성의 요구에 의해 프로세스 능력을 평가하는 모델을 명시한 것이다. CMMI는 과거 여러 종류의 CMM 모델을 2000년도에 통합하여 크게 CMMI-SE/SW/IPPD/SS라는 4개의 모델로 구분하여 명시하고 있다. 본 논문은 CMMI-SW에 대해서만 논한다. 이 모델은 국제표준은 아니지만 국내에서의 인지도는 SPICE와 동등하게 간주되고 있다. <표 2>와 같이 CMMI-SW는 과거 CMM의 5단계 성숙도와 SPICE의 6단계 능력수준을 통합한 모델이다. CMMI-SW가 SPICE와 호환성을 가짐으로써 이 모델은 12207의 프로세스와 밀접한 연관을 갖는다고 할 수 있다. 현재 미국방성은 주요 군용 소프트웨어 사업에 참가하는 업체는 최소한 CMMI-SW의 3단계 성숙도 인증취득을 요구하고 있다 [4].

<표 2> CMMI-SW의 프로세스능력수준과 성숙도

연속적 표현		단계적 표현	
능력수준	의미	성숙도	의미
0	Incomplete		
1	Performed	1	Initial
2	Managed	2	Managed
3	Defined	3	Defined
4	Quantitatively Managed	4	Quantitatively Managed
5	Optimizing	5	Optimizing

ISO 9001은 ISO 9000 시리즈(9000, 9001, 9004) 중의 하나이다. 이 표준은 임의의 조직 내부에 적용할 목적으로, 또는 인증의 수단으로 활용할 목적으로, 또는 계약서에 명시할 목적으로 사용할 수 있는 품질경영시스템에 대한 요구사항을 규정하고 있으며, 고객의 요구사항을 충족시키는데 있어서 필요한 품질경영시스템의 효과성에 중점을 두고 있다. 이 표준은 대부분의 산업체에 적용 가능하도록 일반적인 내용을 담고 있다. 이 표준을 소프트웨어 산업에 적용할 수 있도록 ISO/IEC 90003이 제정되었다. 90003은 9001의 모든 항목을 소프트웨어에 어떻게 적용할 것인가를 해석하고 있는데 대부분 12207의 해당 절에서 추가적인 정보를 얻을 수 있다고 언급

하고 있다. 이런 사실은 소프트웨어 산업에서 ISO 9001 인증을 획득하고자 한다면 먼저 12207을 만족하는 프로세스를 갖추어야 함을 알 수 있다.

결론적으로 SPICE, CMMI-SW, ISO/IEC 90003과 같은 표준은 12207에서 제시하는 소프트웨어 프로세스를 참조하고 있는 것으로 분석되었다. 이것은 원전 소프트웨어에서 요구하는 프로세스 모델을 만족한다고 할 수 있다. 원전 소프트웨어 공급자의 자격 심사 시 위와 같이 국제적으로 인지도가 높은 소프트웨어 인증을 취득하도록 요구한다면 원전 소프트웨어의 품질과 안전성이 향상될 수 있을 것이다.

4. 원전 소프트웨어 안전성분석 요건

원전 소프트웨어는 특별히 안전성분석 수행이 요구된다. 안전성이란 고장이 발생해도 안전한 상태가 유지될 수 있는 특성이며, 안전성분석이란 인간의 생명을 위협할 수 있는 위험요소(hazard)를 찾아내고 개선책을 제시하는 활동이다. 12207에는 소프트웨어 품질을 측정할 수 있는 메트릭과 프로젝트 위험(risk)을 관리하는 지침은 있지만 안전성분석에 대한 지침은 없다. 원전 소프트웨어에 적용하고 있는 IEEE 7-4.3.2는 정성적 분석기법으로 고장유형 및 영향분석(FMEA)과 고장수목분석(FTA)을 권고한다. 소프트웨어 공학적으로 소프트웨어의 신뢰도를 높일 수 있는 기법으로는 로직을 수학적으로 증명하는 정형기법 사용, 다양성 개발개념을 적용하는 N-버전 프로그래밍, 정량적 데이터 획득을 위한 신뢰도시험이 제시되고 있으나 이러한 기법은 소프트웨어의 복잡도가 증가함에 따라 비용이 급격히 증가되어 비현실적일 수 있다. KINS는 소프트웨어만 국한된 안전성분석보다는 소프트웨어와 하드웨어가 통합된 시스템에서 전체적인 안전성분석을 요구한다. 현재까지 조사한 바로는 안전필수 소프트웨어의 안전성분석을 위한 지침을 제시하는 국제표준은 존재하지 않은 것으로 파악되었다.

5. 결론

국내 원전 소프트웨어 품질요건에 대한 분석결과, 원전 소프트웨어는 미국 IEEE 소프트웨어 표준을 참조하여 개발되어야 하며, 특히 ISO/IEC 12207을 채택한 IEEE/EIA 12207.0의 프로세스 모델을 만족하여야 한다. 본 논문에서 ISO/IEC 12207과 호환성을 갖는 SPICE, CMMI-SW, ISO 9001 인증에 대한 분석결과, 이들은 원전 소프트웨어 품질요건에 부합하는 인증이며 원전 소프트웨어 공급자에게 이러한 인증을 취득하도록 요구한다면 원전 소프트웨어의 품질을 향상시킬 수 있고, 결국은 원전의 안전성을 도모할 수 있을 것이다. 따라서 국내 원전 심사 및 인허가 기관인 KINS가 이 사항을 원전 소프트웨어 공급자의 능력을 평가하는데 있어서 일차적인 기준으로 활용한다면 소프트웨어에 전문적인 지식이 없는 원전 심사자로 하여금 공급자의 자격 심사부담을 경감시킬 수 있는 효과를 얻을 것이다. 현재 원전 소프트웨어와 같은 안전필수 소프트웨어에 대한 국제인증제도가 충분히 성숙되어 있지 않은 실정이지만 위와 같은 인증을 원전 소프트웨어에서도 점진적으로 요구한다면 소프트웨어 인증제도를 더욱 활성화시킬 수 있는 계기가 될 것이다.

Acknowledgement

국내 원자력법 관련 내용은 www.kins.re.kr에서, 미국 원자력법은 www.nrc.gov에서, CMMI에 관련된 내용은 www.sei.cmu.edu에서 무료로 받을 수 있으며, ISO 표준은 www.iso.org에서 IEEE 표준은 www.ieeexplore.ieee.org에서 유료로 받을 수 있으므로 본 논문에서는 지면제약 때문에 참고문헌에서 명시하지 않았다.

참고문헌

[1] Software Review Plan: Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, NUREG-0800 BTP HICB-14, U.S. NRC, Rev. 4, 1997.

[2] Notice of Cancellation, Software Development and Documentation, MIL-STD-498, Notice 1, U.S. DoD, May 27, 1998.

[3] O Benediktsson, R B Hunter, A D McGettrick, Processes for Software in Safety Critical Systems, Software Process: Improvement and Practice, John Wiley and Sons Ltd., 2001, Vol. 6, issue 1, pp. 47-62.

[4] Memorandum for Component Acquisition Executives Director of Ballistic Missile Defense Organization, Software Evaluations for ACAT 1 Programs, U.S. DoD, 1999.