□ 기술해설 □

원전 계측제어 소프트웨어 안전성 국제표준 발전동향 분석

한국원자력연구소 이장수* · 엄흥섭** · 권기춘***

● 목 차 ●

1. 서 론

최근 전 세계 원자력 산업계에서는 종래의 원전 아날로그 계측제어계통의 디지털화를 위해 많은 노력을 기울이고 있으나, 원자력산업의 특수성인 안전성 확보에 필요한 소프트웨어 개발기준과 규제방법은 아직 정립되지 못하고 있다. 뿐만 아니라 디지털 계측제어계통의 핵심 기반기술인 필수안전(safety critical) 소프트웨어 개발 방법론이 확립되지 못하여 소프트웨어 공통모드고장 문제, 정량적인 소프트웨어 신뢰도와 안전성 보장 등을 위한 기준인 국제표준이 논란의 대상이 되고 있다.

원전 디지털 계측제어계통 개발의 안전성 확보와 밀접한 관계가 있는 규제방법과 고신뢰도 소프트웨어 개발방법론, 검증 및 확인(V&V, Verification and Validation)등에 대한 종합적인 분석은 한국원자력연구소 기술현황 분석 보고서[4]와 한국원자력학회지 기술보고[1] 그리고 소프트웨어 공학회지[3]에 보고 한 바 있다. 본 논문의 2장에서는 현재 원자력발전소 계측제어 계통을 개발하고 인허가할 때 사용되는 국제표준과 그 적용방법을 소개하고 3장에서는 국제원자력기구(IAEA, International Atomic Energy Agency)와 국제표준기구(ISO, International Organization for Standardization), 국제전기기술위원회(IEC, International Electrotechnical Commission)를 중심으로한 국제 표준의 변화추세를 분석하며 4장에서는 미국원자력규제위원회(NRC, Nuclear Regulatory Commission)와 IEEE(Institute of Electrical and Electronics Engineers)를 중심으로한 표준과 규제입장의 최근 추세를 분석하였다.

이러한 분석의 필요성은 현재 우리나라 원자력 산업의 현실과 국제적인 추세에 기인한다. 즉, 국제 원자력 산업 현실에서 모든 나라가 협력과 경쟁의 관계에 있지만, 이 분야 법규와 표준제정 및 기술력에 있어서는 미국 원자력규제위원회와 IEEE를 중심으로한 미국과 IAEA와 국제전기기술위원회를 중심으로한 국제기구로 나누어서 살펴볼 필요가 있다. 왜냐하면 우리나라 원자력 산업의 현실이 IEC 880-1986의 표준을 적용받는 발전소와 미국 원자력규제위원회의 규제입장과 IEEE 표준의 영향권에

* 정 회 원
** 비 회 원
*** 종신회원

있는 발전소가 모두 존재하기 때문이다. 따라서 이러한 두 줄기 추세를 면밀히 검토, 분석해 봄으로써 우리 고유의 기술자립 방향을 모색할 수 있을 것이다.

2. 원전 계측제어 소프트웨어 안전성 표준과 적용

2.1 원전 계측제어계통 안전성 국제표준

최근 원전의 아날로그 계측제어계통은 그 계통의 노후화로 운전 및 유지보수 비용의 증가와 디지털 기술의 빠른 발전에 의한 기술의 우수성 때문에 점차 디지털화 되어 가는 추세이다. 이러한 추세의 결과 종래 아날로그 하드웨어의 기능을 대폭 향상시킨 소프트웨어가 사용되게 되었으나 이는 소프트웨어 공통모드고장 문제와 소프트웨어 안전성 보장 문제 등을 야기시키고 있다.

사용자, 개발자와 규제자 모두가 인정하는 소프트웨어 검증 및 확인용 방법론과 표준들은 계측제어계통 소프트웨어의 품질을 보증할 수 있고 소프트웨어의 신뢰도를 높임으로써 전체 디지털계통의 품질을 보증한다. 소프트웨어의 설계와 개발 표준들은 일관성 있게 소프트웨어의 품질을 향상시킬 수 있고, 소프트웨어의 재사용 가능성을 높이며 소프트웨어 개발과 검증 및 확인을 자동화할 수 있는 도구 개발을 용이하게 한다. 원전 계측제어계통의 성공적인 디지털화를 위해서는 소프트웨어의 안전성 확보가 관건이며 필수안전 소프트웨어 검증 및 확인 기술 개발이 디지털화의 기반이고 핵심기술이다.

아직도 소프트웨어의 신뢰도와 안전성의 구분에 대해 정확한 구분이 되지 않고 사용되는 경우가 많다. 즉 소프트웨어의 결함만 최소화시키면 위험한 결과를 초래하지 않을 것이므로 안전한 소프트웨어란 신뢰도가 높은 소프트웨어이면 충분하다고 생각하는 것이다. 그러나 소프트웨어는 결함이 없지만 그 소프트웨어가 전체 계통차원에서 위험을 초래하거나 사고를 야기하는 경우가 있으며 반대로 결함이 많이 있지만 전체 계통에서는 전혀 위험을 야기하지 않는 안전한 소프트웨어도 있을 수 있다. 현재 전 세계적으로 소프트웨어의 안전성을 연구하는 학자들 사이에서는 소프트웨어의 안전성에 대한 이러한 의견에 대해 공감대를 형성하고 있으며 이것이 반영된 새로운 소프트웨어 안전성 관련 표준을 만들기 위해 소프트웨어 공학자와 계통공학자가 협력하여 작업을 하고 있다[16].

원전의 설계, 건설, 운영에 따른 규제요건은 원전의 안전을 최대로 확보하고 유지하려는 관점에서 추구되어 왔다. 새로운 원전을 건설하거나 기존의 원전 계통을 변경 또는 개선하려 할 경우 규제요건의 만족여부가 관건이 된다. 이러한 규제요건은 원전의 안전성을 확보하고 유지해 온 기반임은 사실이나, 한편으로는 규제요건이 기술발전 속도에 맞추어 정립되지 않아 유용한 기술을 원전에 적용하고자 할 때 오히려 장애요인으로 작용하는 측면도 있다.

원전 계측제어 고신뢰도 소프트웨어의 개발방법, 검증 및 확인방법, 표준 및 규제요건, 규제방법 등은 서로 밀접한 관계를 가지고 있다. 즉 소프트웨어의 안전성과 신뢰도 보장이라는 공통된 목표를 가지고 있기 때문에 적용 시점과 관점의 차이는 있으나 세부 기술적 내용과 현안은 같다고 할 수 있다. 따라서 본 절에서는 먼저 규제요건과 관련 표준들을 분석하고 미국 원자력규제위원회의 규제 방법을 알아보았으며 이를 위한 기술적 측면으로 고신뢰도 소프트웨어 개발방법, 검증 및 확인방법, 표준 및 규제요건, 규제방법에 대한 기술현안과 연구 현황을 서술하였다.

원전 계측제어계통과 관련하여, 현재 사용중인 규제요건과 규제 참고자료(STDs, Codes, CFRs)는 약 90여 가지가 있다. 그러나 특정 규제 대상 별로 적용하고 참고할 수 있는 규제자료의 분류 및 체계가 미흡하며, 계측제어계통의 디지털화에 따라 급변하는 기술발전 추세와 보조를 맞추기 위해서도 여러 가지 측면에서 개선되어야 할 필요가 있다. 이를 위해 미국 원자력규제위원회, EPRI(Electric Power Research Institute)[12][13], NIST(National Institute of Standards and Technology)[6], LLNL(Lawrence Livermore National Laboratory)[15]등 여러 기관에서 이러한 작업을 진행 중에 있다.

본 절에서는 미국 원자력규제위원회가 현재

원전 디지털 계측제어계통을 검토할 때 사용하는 규제요건들 중 안전관련 계통의 소프트웨어에 관한 것만 분석한다. 디지털 계측제어계통에서 소프트웨어는 종전 아날로그 계통에서 하드웨어적으로 해결하던 기능의 많은 부분을 대신하고 있다. 따라서 여기서 분석할 규제자료의 범위는 소프트웨어에 직접적인 것과 소프트웨어에 관련된 계통적인 규제요건들이며, 또한 다중방호 개념의 안전관련 규제요건을 포함한다. 현재 사용중인 디지털 계측제어계통 관련 규제 및 규제참고 자료 중에서 위에서 정한 분석 범위에 포함되는 국제표준들은 부록과 같다.

현재 미국 원자력규제위원회에서는 디지털계통을 검토할 때 Reg. Guide 1.152와 IEEE Std 7-4.3.2-1993을 사용한다. IEEE Std 1012-1986와 ASME NQA-2a-1990, Part 2.7 등이 주 참고 자료로 사용되며 그외 앞에서 언급된 모든 자료들이 참고로 사용된다. 따라서 피규제자는 궁극적으로 IEEE Std 7-4.3.2-1993를 만족시킬 의무가 있다. IEEE Std 7-4.3.2-1993는 규제자와 공급자 사이의 인터페이스, 검증 및 확인의 독립성, 검증 및 확인에 사용된 도구와 사람에 대한 자격, 하드웨어와 소프트웨어 및 계통의 요구사항, 소프트웨어 개발절차, 하드웨어 소프트웨어 통합, 검증 및 확인 방법 등을 기술하고 있다. 그러나 IEEE Std 7-4.3.2-1993에는 계통 및 하드웨어와의 통합을 고려하면서 주로 소프트웨어에 관련된 규제내용들이 원칙적인 측면에서 간략하게 기술되어 있다. 즉, IEEE Std 7-4.3.2-1993의 본문 내용에는 다른 규제지침서와 표준들로의 참고부분이 많으며 기술적으로 구체적인 내용은 대부분 부록에 수록되어 있다. 따라서 미국 원자력규제위원회에서는 많은 부분을 확대 해석하여 적용하고 있으며, 이에 따라 여러가지 규제 지침서들을 필요로 한다. IEEE Std 7-4.3.2-1993의 상위 규제요건이며 계측제어 안전계통 표준요건인 IEEE Std 603-1991의 Section 5.3과 5.4에 따라 엄격한 확인이 요구되며 세부 시험방법으로 IEEE Std 829-1983가 사용된다.

원전 보호계통은 10 C.F.R. Part 50, Appendix A, GDC 21, 22, 23에서 명시한 것처럼 고신뢰도와 고장시 안전을 보장하고 보호기능 손실이 없도록 하기 위해서 품질보증 개념과 다양성을 갖는 다중방호(Defense-In-Depth) 개념을 가지고 설계되어야 한다. 이러한 개념은 IEEE Std 603-1991, IEEE Std 379-1977, Reg. Guide 1.53, NUREG 0493[11] 등에 잘 나타난다. IEEE Std 7-4.3.2-1993와 이를 중심으로 한 지침서들을 최대한 활용하여 고신뢰도 소프트웨어를 개발하였어도 소프트웨어의 공통모드고장이 일어날 수 있을 때는 다중방호 개념에 따라 원자로를 안전하게 정지시킬 수 있는 예비 수단이 있어야 한다. 이를 위해 현재 미국 원자력규제위원회는 수동정지계통을 추가로 설치하여 사용할 것을 주장한다. 또한 단일사고기준(single failure criteria)을 만족시키기 위해 소프트웨어에 대해서도 고장모드 영향분석(FMEA, Failure Modes and Effect Analysis)를 수행해야 한다. 이러한 상황에서 미국 원자력규제위원회는 개발된 디지털 계측제어계통이 IEEE Std. 603, 279, 379, IEEE Std 7-4.3.2-1993와 Reg. Guide 1.152, 1.53의 만족여부와 그 상위요건인 10 CFR Part 50, Appendix A, GDCs 2, 4, 20, 21, 22, 23, 25 요구사항 만족여부를 검토한다. 이러한 규제요건들과 참고 지침서들은 적용범위와 사용된 용어를 정의하고 있으며 세부내용에서도 수직적, 수평적으로 서로의 관계를 가지고 있다.

2.2 기존 발전소 디지털화에 대한 표준적용

미국 원자력규제위원회는 기존 발전소에서 새로 디지털화되는 계측제어 안전계통을 인허가할 때 Reg. Guide 1.152와 IEEE Std 7-4.3.2-1993을 주로 사용하고 IEEE Std 1012-1986과 ASME NQA-2a-1990, Part 2.7을 참조한다. 미국 원자력규제위원회가 수행하는 규제 방법은 일반적으로 다음과 같다. 규제요원은 먼저 계통 설계 과정과 소프트웨어 검증 프로그램에 대해 자세히 검토하고 이전의 소프트웨어와 하드웨어 고장을 포함한 소프트웨어 및 하드웨어 고장 이력에 대한 모든 정보에 대해서 검토한다. 그리고 규제자는 소프트웨어 개발시 수행된 검증 및 확인작업에 대한 검토 작업을 아래와 같이 수행한다.

(1) 프로그램의 개발 단계를 점검한다.
(2) 공급자와 규제자 사이의 인터페이스를 점검하고 이에 대한 피드백 과정을 점검한다.
(3) 소프트웨어 문제/오류 보고서 등을 검토하고 정정 결과를 점검한다.
(4) IEEE Std 7-4.3.2-1993와 검증 및 확인 과정을 비교한다.
(5) 개발과정에 참여한 사람을 면담한다.
(6) 소프트웨어 확인자의 독립성을 점검한다.
(7) 기능요건과 이에 따른 소프트웨어 개발 문서를 점검한다.
(8) 소프트웨어의 개발 공정을 검토하고 앞으로의 공급자/규제자 사이의 인터페이스를 점검한다.
(9) 검증 및 확인 결과물을 점검한다.

그리고 규제요원은 소프트웨어의 성능과 신뢰도를 평가하기 위한 기준을 마련하기 위해서 모든 정보를 통합하고 대조한다.

2.3 개량형 경수로 디지털 계측제어계통에 대한 표준적용

디지털 신호가 아날로그 신호에 비해 더 많은 정보를 가지고 있고 디지털 장비가 아날로그 장비에 비해 월등한 정보처리 능력이 있기 때문에 계측제어 분야에서의 디지털 컴퓨터로의 변경은 원전 운전의 안전성과 신뢰성을 향상시킨다. 그러나 신뢰도를 달성하기 위해서는 계통 구조 설계와 특징에 대한 특별한 제약이 필요하고 계측제어계통의 설계, 구현, 설치, 운전, 유지보수, 수정 등 개발 주기의 각 단계에 관련된 고수준의 적용 요건이 필요하다. 미국 원자력규제위원회는 10 CFR Part 52의 일괄인허가(One-step licencing) 과정에서 15년 기간 동안 계측제어 분야를 포함한 원자력 발전소의 표준 설계를 승인하지만 승인 과정 중 공급자 사양을 요구하지는 않는다. 이는 계속 발전되어 가고 있는 디지털 기술의 장점을 이용할 수 있도록 융통성을 주기 위한 것인데 이에 따라 계통 설계 부분, 특히 소프트웨어 설계 부분은 상위단계만이 승인 대상이 된다. 이와 같이 미국 원자력규제위원회는 설계 승인 기간 동안에 진부해 질 수 있는 설계의 세부 사항은 제한하지 않고 설계 과정의 품질과 설계승인기준 (DAC, Design Acceptance Criteria), 제한사항, 제한치 등에 대해서만 제한 한다. 설계승인기준은 미국 원자력규제위원회가 검사, 시험, 분석 및 승인기준(ITAAC, Inspection, Tests, Analyses and Acceptance Criteria)을 통하여 설계 승인을 받는 통합승인(COL, Combined License)지원자가 수행한 설계 구현과 확인의 최종 안전성 평가를 하는 기준이 된다.

원전 계측제어계통이 디지털화 되면서 소프트웨어 공통모드고장 극복과 같은 소프트웨어 안전성 보장문제가 쟁점으로 부각되고 있다. 품질보장 측면에서의 노력에도 불구하고 공통모드고장이 발생할 가능성이 있기 때문에 다중방호 보장을 위한 설계에서의 다양성 제공이 필요하다. 기능적 다양성 개념은 "NUREG-0493 1979, A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System"[11]에 잘 나타나 있다.

원전 안전계통의 신뢰도 분석에 대한 일반적인 원칙은 IEEE/ANSI 352-1987에 소개되어 있으며 고장모드 영향분석과 고장수목분석(FTA, Fault Tree Analysis)과 같은 정성적인 신뢰도 분석방법과 수학적 모델링에 의한 정량적인 신뢰도 분석원칙을 설명하고 있다. 즉 신뢰도 분석에 대한 계통 차원에서의 이론들을 표준화한 것이다. 이렇게 표준화된 계통 차원의 이론들은 소프트웨어에 그대로 적용될 수 없으며 소프트웨어의 신뢰도 분석을 위한 정성적, 정량적 방법과 척도가 표준화되어야 한다.

이러한 표준화를 위한 노력의 일환으로 NUREG/CR-5930 'High Integrity Software Standards and Guidelines"[6]와 IEEE Std 1228-1994 'Standard for Software Safety Plan"이 만들어 졌다. NUREG/CR-5930에서는 고신뢰도 소프트웨어의 표준과 지침서들이 가져야 할 기준을 설명하고 기존 지침서들의 문제점을 분석하고 있다. 여기서는 고신뢰도를 요하는 소프트웨어의 안전성을 보장하기 위한 방법으로 소프트웨어 위험도분석에 대한 기준을 제시하고 있다. IEEE Std 1228-1994은 소프트웨어 안전성확보계획에 대한 방법들을 서술하고 있으며 현재 IEEE 소프트웨어 공학표준 위원회 산하의 소프트웨어 안전성 계획 그

룹에서는 이 표준을 소프트웨어 공학 전체 공정으로 구체화하기 위한 작업의 첫걸음으로 소프트웨어의 안전성 표준에 대한 현장을 준비하고 있다. 현재 10 CFR 52에 의거한 미국 원자력규제위원회의 단계별 소프트웨어 ITAAC에서 명시하는 문서들 중에는 이러한 소프트웨어 안전성확보계획과 소프트웨어 안전성분석 관련 문서들이 요구되고 있으나 이와 같은 문서를 작성하고 이를 검토할 때 필요한 표준과 지침서들이 미흡한 실정이다.

미국 원자력규제위원회는 안전성 관련 계측제어계통 설계과정 중에 각 단계에서 요구조건이 일치하는지 검증하기 위해 소프트웨어 ITAAC 구현을 감사 한다. 각각의 감사단계는 그림 1과 같고 각 단계별 주요 내용은 다음과 같다.

ITTAC의 구현 결과에 따라 미국 원자력규제위원회는 검사 보고서를 작성하고 문제에 대한 해결책을 제시한다. 해결되지 않은 중요한 현안사항(open item)에 대해서는 미국 원자력

planning Stage	Requirement Stage	Design Stage	Implementation Stage	Integration Stage	Validation Stage	Installation Stage	Operation & Maintenance Stage
Software Management Plan		Unit Test Plan	Integration Plan	Validation Plan	Installation Plan	Maintenance Plan	Regression Test Plan
Software Development Plan			Integration Test Plan	Validation Test Plan	Installation Test Plan	Operations Manuals	
Software QA Plan	Requirement Specification	H/W & Software Architecture	Code Listings	System Build	Training Plan	Installation Configuration Tables	
	Interface Specification	Design Specification			Operations Plan	Table Manuals	
		Interface Design Specification				Maintenance Manuals	
Software Safety Plan	Requirements Safety Analysis	Design Safety Analysis	Code Safety Analysis	Integration Test safety Analysis	Validation Test safety Analysis	Installation Test safety Analysis	Change Safety Analysis
Software V/V Plan	V/V Requirement Analysis Report	V/V Design Analysis Report	V/V Unit Test Report	V/V Integration	V/V Test & Analysis Test Report	V/V Test Installation Report	V/V Change Report Test Report
	V/V Anomaly Report	Report	V/V Anomaly Anomaly Rpt	V/V Test Anomaly Rpt	V/V Test Anomaly Rpt	V/V Test Anomaly Rpt	V/V Test
Software CM Plan	CM Requirement Report	CM Design Report	CM Implementation Report	CM Integration Report	CM Validation Report	CM Installation Report	CM Change Plan Report
	Revisions to Earlor Documents	Revisions to Earher Documents	Revisions to Earlier Documents	Revisions to Earlier Documents	Revisions to Earlier Documents	Revisions to Earher Documents	Revisions to Earher Documents
Planning Audit	Requirement Audit	Design Audit	Implementation Audit	Integration Audit	Validation Audit	Installation Audit	

그림 1 ITAAC 감사 단계

규제위원회가 결정을 내릴 수 있다. ITAAC의 각 단계에서 설계 개발은 승인된 설계 과정과 일치함이 증명되어야 하고 각 단계를 통하여 개발된 상세 설계는 승인 받은 설계를 만족시켜야 한다. 또한 ITAAC과 더불어 안전계통에 대한 다양한 시험이 요구된다.

현재 미국 원자력규제위원회는 원전 디지털 계측제어 및 보호계통과 같은 안전에 중대한 계통들에 사용된 소프트웨어의 건전성 평가 결과를 기초로 다음과 같은 다양성에 대한 입장을 발표하였다.

(1) 피규제자는 제안된 계측제어계통의 공통모드고장 취약성을 적절히 보완시켰다는 것을 입증하기 위해 다중방호와 다양성을 평가해야 한다. 이를 위한 참고 자료는 NUREG-0493[11]에 나타나 있으며 피규제자가 제안한 방법들은 따로 검토되어야 한다.

(2) 평가를 수행하는데 있어서 공급자와 피규제자는 안전성분석보고서(SAR, Safety Analysis Report)의 사고 분석에서 평가되는 각 사고에 대해 예상되는 공통모드고장을 평가해야 한다. 공급자와 피규제자는 이들 사고대비를 위해 적절한 다양성이 설계에 반영되었음을 보여주어야 한다.

(3) 만약 공통모드고장이 안전기능을 상실시킨다면 같은 기능을 수행하거나 다른 기능을 수행하는 다양한 수단이 제공되어야 한다. 그 계통이 관련된 사고 조건하에서 필요한 기능을 수행하기 위해 충분한 품질요건을 갖추었다면 비안전계통도 그 기능을 수행할 수 있다. 다양한 방법의 디지털과 비디지털계통들이 사용 가능하며 시간과 정보가 운전원에게 유용하다면 수동 조작도 가능하다. 다양성에 대한 형태와 종류는 설계에 따라 다양하며 각기 평가될 수 있다.

(4) 주제어실에 설치된 디스플레이와 제어기들은 안전 기능을 지원하는 변수를 감시하고 필수안전 기능의 수동 조작을 위해서 제공되어야 한다. 각각의 디스플레이와 제어기들은 앞의 (1), (3) 항목에서 언급하는 자동화된 안전계통과는 독립적이어야 한다.

원전 계측제어 소프트웨어들은 그 중요도의 정도와 소프트웨어의 종류에 따라 분류되며 이러한 분류에 따른 각각의 소프트웨어는 서로 다른 패러다임과 개발 방법론들이 적용되어야 한다. 이를 위해 IEEE Std 7-4.3.2-1993, IEEE Std 1228-1994 등과 같이 체계적인 요건들의 개발 및 보완 작업이 진행 중에 있다. 그러나 규제요건 및 표준들이 급격한 기술 발전을 효율적으로 수용하기 위해서는 각각의 요건들이 유연성과 확장성을 갖도록 보완되어야 하며 IEEE, ASME, ISO, 국제전기기술위원회 등 타 산업 표준들과 개발자 내부 지침서, 규제요건들의 유기적인 연계 체제를 갖추어야 한다.

3. 원전 계측제어 소프트웨어 안전성 국제표준 발전동향

국제전기기술위원회의 목적은 전기, 전자의 기술 분야에 있어서 표준화의 모든 문제와 관련사항에 관해 국제협력을 촉진하고 이에따라 국제적인 의사전달을 꾀하려고 하는 것이다. 이 목적은 각국의 총의를 가능한 표현하는 IEC 규격, 특히 국제규격의 형식에 따른 권고로 간행물을 발간하고 이것을 각국의 국가규격에 반영시키는 것으로 달성되고 있다.

국제전기기술위원회에서 개발된 표준중에 원자력발전소 안전계통에서의 컴퓨터 소프트웨어에 대한 표준으로 IEC 880-1986이 있다. 이 국제표준은 최근 디지털화 추세에 있는 원전 계측제어 계통의 개발과 안전 심의 기준으로, 캐나다 Darlington 원자력발전소와 프랑스 N4 원자력발전소 계측제어 계통개발에 사용됨으로써 세계적인 주목을 받고 있다. 그러나 이 표준은 개발된지 10년 가까이 지난 것으로, 급속도로 발전하고 있는 컴퓨터와 소프트웨어 관련 기술을 제대로 반영하지 못하고 있다. 뿐만 아니라 디지털 계통의 안전성을 보장하고 개발자와 규제자가 공감하는 심의 기준으로 사용되기 위해서는 많은 부분에서 연구와 개정을 필요로 하고 있다. 이에 따라 IEC/SC45A(국제전기기술위원회 원자로용측정장치) 분과에서는 약 2년 전부터 이의 개정을 위한 회의를 계속하고

SC45A/WGA3(Draft Chapeau)3 : Jan. 1995	NUCLEAR POWER PLANTS INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY : GENERAL REQUIREMENTS FOR COMPUTER BASED SYSTEMS
SC45A(Sec.)189 : July 1994	Software for computers important to safety for nuclear power plants : First supplement to IEC 880
SC45A/WGA3(j. Boulc'h)1 : Jan 1995	Software for Computers Important to Safety for Nuclear Power Plants : Second Supplement to Publication IEC 880 (1986)

있다. 1995년 프랑크푸르트회의에서는 현재 개발중인 다음과 같은 국제표준에 대한 각국의 의견을 검토하여 새로 개발되는 국제표준초안에 반영하였다.

상기 초안들 중 특히 CS45A(Sec.)189가 IEC 880-1986의 핵심부분에 대해 새로 개발되고 있는 초안으로서 다음 주제들을 다루고 있다.

(1) Defences against common mode failure
(2) Formal specification and design methods
(3) Automated tools for the development of software important to safety
(4) Use of pre-existing software products
(5) Safety-related applications

이들 5개 분야별로 자발적인 작업반을 만들어 각 국가에서 보내온 검토의견들을 재검토하여 국제표준 개발과정에 수용하거나 제외시키는 작업이 이루어졌다. 이 과정에서 국가별 의견을 수용하기는 쉬우나 제외시키기 위해서는 분명한 이유를 제시해야 하기 때문에 쉽지가 않았다. 즉 적극적으로 제안하는 국가의 의견이 국제표준으로 반영되는 경향이 있었다. 또한 이들 분야는 미국 IEEE에서도 많은 관심을 가지고 있으며 IEEE 소프트웨어 공학표준위원회 산하의 소프트웨어 안전성계획 그룹이 IEEE Std 1228-1994 'Software Safety Plan"을 계속 발전시키기 위한 공통의 연구분야 이기도 하다.

원전 계측제어계통 디지털화 추세에 의해, 컴퓨터 기반 안전계통을 위한 국제표준화 노력이 활발하였으며 앞으로 전개될 WTO 체제 하에서 국제표준의 중요성이 부각되고 있었다. 컴퓨터 기반 안전 계통에 대한 국제 표준인 IEC 880-1986을, 영국 Sizewell B Plant, 프랑스 Chooz B Plant, 캐나다 Darlington Plant와 같은 세계 최첨단의 디지털 제어기술을 적용한 발전소 설계에 대한 인허가 요건으로, 각국에서 채택하여 사용함에 따라 그 중요성이 한층 부각되었으며 미국의 IEEE 표준과는 경쟁관계에 놓여 있다.

국제 표준회의에서는 실제 원전 디지털 계측제어계통을 개발해 본 나라의 경험에서 나온 의견이 국제 표준에 가장 많이 반영되는 추세이고 그래서 프랑스, 영국, 캐나다측의 의견이 국제 표준에 많이 반영되고 있었으며, 미국도 웨스팅하우스사와 원자력규제위원회의 경험을 바탕으로 많은 영향력을 미치고 있다. 우리나라는 원전 계측제어계통에 디지털기술 적용시 현안문제로 등장한 소프트웨어 검증 및 확인분야와 주제어실의 설계개선을 위한 국제 표준을 제정하기 위한 검토 회의에 옵저버로 참여하는 정도에 머물고 있지만 각국에서 파견된 대표들과 의견을 교환하고 상호 협력할 수 있는 채널을 마련하였다. 우리나라도 우리의 원자력산업 규모에 맞게 국제표준 제정에 적극적으로 동참하는데 소홀히 해서는 안될 것이다.

4. 원전 계측제어 소프트웨어의 안전성 분야 미국표준 발전동향

IEEE Std 7-4.3.2-1993. Reg. Guide 1.152와 IEEE 379-1988, Reg. Guide 1.53을 중심으로 한 디지털 계측제어계통 소프트웨어 관련

규제요건들은 1980년대 전반기 이전에 작성된 것으로서 급격히 발전된 현재의 소프트웨어 기술 수준을 제대로 반영하지 못하고 있으며, 관련 규제요건 및 참고 지침들이 체계적으로 일원화되어 있지 못한 실정이다. 또한 종전 아날로그 계통에서의 하드웨어가 소프트웨어로 대체됨에 따라 하드웨어 및 계통 차원의 규제요건을 소프트웨어에 적용하여야 함에 따른 여러 가지 문제점이 발생되고 있다. 예를 들면 Class 1E 기기의 독립성 보장 요건 및 시험성 요건과 같은 아날로그 계통에서의 하드웨어 관련 요건들이 소프트웨어에도 적용되어야 한다. 소프트웨어 공통모드고장 대책을 정확히 검토할 수 있는 소프트웨어 고장모드영향분석, 고장수목분석과 같은 형식이론(formalism)의 도입, 위험도분석(Hazard Analysis) 방법서술, 보다 정량적인 규제 방법 등이 강구되어야 한다. 이에 대한 노력의 일환으로 IEEE Std 7-4.3.2-1993이 개발되었다. IEEE Std 7-4.3.2-1993에서는 컴퓨터를 구성하는 모든 요소들 즉 하드웨어, 소프트웨어, 펌웨어, 인터페이스 등에 관련된 세부 요건을 지정하고 있다. IEEE Std 7-4.3.2-1993은 안전요건만 만족한다면 발전하는 디지털 기술이나 방법 즉, "인공지능" 이나 "4세대 언어" 와 같은 신기술 적용을 제한하지 않고 있다. 또한 IEEE Std 603-1991의 요건과 기준을 보충하기 위한 세부 요건을 명시하고 있다. IEEE 7-4.3.2-1993은 컴퓨터계통이 안전계통의 요소로 사용될 때 안전계통 설계가 완벽하다는 것을 입증하기 위해 IEEE Std 603-1991과 병행해서 사용해야 한다. 현재 소프트웨어 도구 선정 규정이나 컴파일러, 운영체제, 라이브러리 등의 선택 기준에 대해서는 별도의 표준마련을 권고하고 있으며 IEEE Std 7-4.3.2-1993 범위에서는 제외되었다. 그리고 소프트웨어의 품질과 안전성 보장을 위해 다양성, 위험분석도, 신뢰도, 통신독립성, 상용 소프트웨어 검증, 소프트웨어 공통모드고장 대책에 대해서도 부록에서 자세히 언급하고 본문 요건의 범위에는 아직 포함시키지 않고 있다. 이와 같이 안전에 중대한 소프트웨어 개발 표준을 정립하기 위해 NUREG/CR-5930[6]에서는 고신뢰도 소프트웨어에 대한 기존의 표준과 지침서들의 문제점을 분석하고 있으며 소프트웨어 안전성 확보계획에 대한 표준이 IEEE Std 1228-1994로 개발 되었다.

원전 디지털 계측제어 소프트웨어계통은 그 중요도(criticality)의 정도에 따라 보호계통 소프트웨어, 제어계통 소프트웨어, 감시계통 소프트웨어와 그외 여러 가지 운전보조계통등으로 나눌 수 있다. 이들은 다시 안전관련 소프트웨어와 안전에 관련이 없는 소프트웨어로 나누어지며, 이들 소프트웨어를 개발하고 인허가를 수행할 때 현재 쟁점으로 부각되고 있는 것은 대중의 안전과 직결되는 안전계통 소프트웨어의 안전성과 신뢰도의 보장 문제이다.

구체적으로 말하자면 안전계통 소프트웨어의 공통모드고장 극복이 관건이며 이를 위해 소프트웨어 다중성, 주요 소프트웨어 격리, 소프트웨어 위험도분석, 고장허용 소프트웨어 개발, 형식이론의 도입 등 다양한 방법들이 제시되고 있다. 또한 원전에서 사용되는 모든 소프트웨어는 상당히 높은 수준의 품질과 신뢰도를 요구하므로, 고신뢰도 소프트웨어를 개발하고 검증 및 확인을 수행하며 이에 대한 인허가를 수행하기 위해서는 소프트웨어 개발공정 전 단계에 걸쳐서 기존의 소프트웨어 공학에서 연구되고 실용화되어 있는 소프트웨어 개발 방법론들이 매우 엄격하게 적용되어야 한다. 이러한 엄격함에도 불구하고 현재 소프트웨어의 신뢰도 측면에서 소프트웨어 공통모드고장 문제를 완전히 해결하지 못하고 있으며 한편으로는 인공지능 기법, 객체지향 프로그래밍, 실시간 프로그래밍 등 소프트웨어 관련 기술이 급속도로 발전하고 있다.

급격한 기술 발전은 소프트웨어 개발자에게 새로운 개발방법의 사용을 요구하며 규제기관에게는 새로운 규제요건의 개발과 새로운 규제방법을 요구하고 있다. 또한 소프트웨어 공학의 학문적인 측면에서도 고신뢰도 고품질의 소프트웨어를 적은 비용으로 효율적으로 개발할 수 있고 소프트웨어 공통모드고장을 극복하여 신뢰도를 보장할 수 있는 이론 정립과 도구 개발에 많은 노력을 하고 있으며, 이를 바탕으로 한 새로운 개발 방법론들을 제시하고 있다.

1976에 시작된 IEEE 소프트웨어 공학 표준

위원회에서는 전문적인 소프트웨어 공학 기술을 표준화하기 위하여 컨센서스 과정을 통해 표준들을 개발하고 있다. 1994년말까지 29가지 표준을 개발하였으며 이는 약 1200 페이지에 달한다. 현재 개발 진행중에 있는 표준이 24가지가 있으며 이중 5가지는 마지막 단계인 투표과정에 있다. 이외에도 1993년 5월에 완성된 IEEE 소프트웨어 공학 표준들의 발전 방향에 대한 마스터플랜에 따라 17개 계획 그룹이 현재 연구를 진행하고 있다. 특히 소프트웨어 안전성 계획 그룹은 소프트웨어의 안전성 확보를 위한 IEEE 표준의 발전 방향을 연구하고 있으며 1993년말 완성된 IEEE Std 1228-1994의 확대 개발을 기획하고 있다. 또한 국제표준기구인 IEC/SC45A/WG3, IEC/SC65A/WG9&10, ISO/IEC JTC SC7/WG9 등과 협조하고 있으며, 미국내부 UL(Underwriters Laboratory), NASA, US. DoD 등과도 공조체제를 이루고 있다. 이와같이 체계적으로 개발된 표준들은 현재 원자력 산업에서도 그대로 사용되고 있으며 미국 원자력 규제위원회의 감사에서도 많이 활용되고 있다. 특히 원전 디지털 계측제어 계통 개발 및 규제 시 적용되는 표준인 IEEE Std 7-4.3.2-1993에서도 많은 부분이 이와같은 IEEE 소프트웨어 공학 관련 표준들을 참고하고 있다.

현재 미국 미국 원자력규제위원회에서는 디지털 기술의 발전과 이에 따라 속속 개발되고 있는 표준들을 종합적으로 반영한 규제입장(branch technical position) 및 새로운 표준검토 계획(standard review plan)을 자문연구기관인 LLNL와 함께 1996년말을 목표로 개발하고 있다. 또한 미국 원자력규제위원회와 LLNL에서는 이러한 IEEE 소프트웨어 공학 표준과 대표적인 국제표준인 IEC 880-1986 및 관련 표준들에서의 적용범위와 내용상 불일치하는 점들을 분석하고 그 분석 결과를 반영한 새로운 규제 지침(Regulatory Guide)을 개발하고 있다.

5. 결 론

본 고에서는 원전 계측제어계통의 성공적인 디지털화를 위한 기반기술이자 핵심기술인 고신뢰도 소프트웨어 검증 및 확인 방법론을 우리 실정에 맞게 개발, 정립하기 위한 준비 단계로서 이 분야 현황을 규제 요건 즉 국제표준의 기술적 현안을 중심으로 기술하였다.

이와 같이 소프트웨어 안전성 보장이라는 목표를 달성하기 위해 현재 각계 각층에서 많은 노력을 기울이고 있다. 즉 산업표준을 정립하는 IEEE, ASME, IEC, ISO 등에서는 소프트웨어 안전관련 요건 정립 노력을 진행 중이며 규제를 시행하는 미국 원자력규제위원회, 카나다 원자력규제위원회 등 각국의 규제기관들에서도 규제시행 측면에서 소프트웨어 안전성 보장을 위한 연구를 수행 중에 있다. LLNL과 NIST 등 미국원자력규제위원회 자문기관들에서는 원자력 분야 소프트웨어의 안전성 보장을 위한 광범위한 연구와 디지털 계통 안전성 평가 업무를 수행 중이며 관련 기술이 가장 많이 축적된 것으로 알려지고 있다. 또한 카네기멜론대학의 Software Engineering Institute를 포함하여 학계에서도 안전에 중대한 소프트웨어에 대한 연구를 활발히 수행하고 있다. 미국 EPRI에서는 Upgrade Plan[13]에 따라 소프트웨어 검증 및 확인과 표준에 관련된 연구를 수행 중에 있으며 캐나다 Darlington 원자력발전소의 안전정지계통 소프트웨어의 안전성을 수학적인 방법으로 증명한 David Parnas, Computer Aided Software Engineering (CASE)와 같은 소프트웨어 개발 도구 회사들도 이러한 소프트웨어의 품질과 안전성을 보장하기 위한 연구 개발 노력을 아끼지 않고 있다. 이외에도 미국의 ABB-CE, 웨스팅하우스, 카나다원자력공사, 프랑스의 EdF 등 원전 공급업체들도 원전 디지털 계측제어계통의 핵심기술인 소프트웨어의 안전성 보장과 검증 및 확인 기술의 확보를 위해 많은 노력을 기울이고 있다. 현재 전세계적으로 소프트웨어의 안전성 관련 표준, 지침서등을 개발하고 있는 기구가 30여개가 되며 파악된 표준 및 지침서만 해도 250여가지가 된다[2].

이와 같은 종합적인 노력에 의해서 디지털 소프트웨어 계통의 안전성이 보장될 수 있고 원전에서 디지털 계측제어 기술이 정착할 수

있을 것이다. 후속기 원전에서 계측제어계통을 디지털화하고 기술자립을 추구하고 있는 우리도 이러한 상황에서 고신뢰도 소프트웨어 안전성 보장 기술과 검증 및 확인 기술과 같은 핵심 기반 기술의 확보가 필수적이다.

현재 추진 중인 원전 계측제어 계통의 디지털화 목표를 성공적으로 완수하고 디지털 계통 인허가 장벽을 원활히 극복하기 위해서 우리는 원전 계측제어 소프트웨어의 분류에 따른 모든 종류의 소프트웨어에 대한 고유의 완벽한 개발 방법론과 개발절차를 갖추고, 이러한 소프트웨어 개발에 필요한 도구들을 개발하며 개발 도구들의 유기적인 집합체인 CASE 환경과 같은 개발환경을 구축하는 것이 무엇보다도 우선되어야 하며, 규제요건과 규제방법의 세부 기술적인 측면에서의 지속적인 동향 파악과, 필수 안전 소프트웨어 관련 기반기술 연구를 적극적으로 수행하여야 하겠다.

참고문헌

[1] 이장수 외, "원전 계측제어 고신뢰도 소프트웨어 확인/검증 기술 현황." 한국원자력학회지, 제26권 제4호, 1994. 12월, pp. 600-610.

[2] 권기춘 외 "계측제어 시험검증기술 개발," KAERI/RR-1504/94, 한국원자력연구소, 1994, pp. 27-34.

[3] 이장수, "원전 계측제어 고신뢰도 소프트웨어 확인/검증 기술 현황." 소프트웨어 공학회지, 제7권, 제2호, 1994. 6월, pp. 96-103.

[4] 이장수 외 "원전 계측제어 고신뢰도 소프트웨어 확인/검증 기술 현황." KAERI/AR-411/94, 한국원자력연구소, 1994.

[5] IEEE Std 7-4.3.2-1993, 'Standard Criteria For Digital Computers In Safety Systems of Nuclear Power Generating Stations," IEEE, 1993.

[6] NUREG/CR-5930, 'High Integrity Software Standards and Guidelines," NIST, U. S. DoC. September 1992.

[7] NUREG/CR-4640, 'Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry," Pacific Northwest Laboratory, August 1987.

[8] NPX80-SQP-0101.0, 'Software Program Manual for NUPLEX 80+," ABB-CE, January 21, 1993.

[9] Digital Systems Reliability and Nuclear Safety Workshop. '(Draft) Operating Reactors Digital Retrofits Digital System Review Procedures." '(Draft) Branch Technical Position(HICB) Digital Instrumentation and Control Systems in Advanced Plants," NIST, U.S. DoC, September 1993.

[10] NUREG/CR-1462, 'Draft Safety Evaluation Report Related to the Design Certification of Combustion Engineering System 80+." U.S. NRC. September 1992.

[11] NUREG-0493, 'A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," U.S. NRC, March 1979.

[12] EPRI NP-4924. 'An Approach to the Verification of a Fault-Tolerant, Computer-Based Reactor Safety System : A Case Study Using Automated Reasoning," EPRI, January 1987.

[13] EPRI NP-7343, 'Integrated Instrumentation and Control Upgrade Plan," EPRI, February 1992.

[14] IEEE/ANSI 352-1987, 'IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generation Station Safety System," IEEE, October 13, 1987.

[15] NUREG/CR-6101, 'Software Reliability and safety in Nuclear Reactor Protection Systems," LLNL, J. D. Lawrence, November 1993.

[16] Nancy G. Leveson, 'SAFEWARE," Addison Wesley. 1995. pp. 164-168, pp. 433-437.

[17] Glanford J. Myers, 'The Art of Software Testing," John Wiley & Sons, Inc., 1979.

[18] Boris Beizer, 'Software Testing Techniques," 2nd Edition, Van Nostrand Reinhold, 1990.

부 록

Protection and Safety Systems

IEEE 279	Criteria for Protection Systems for Nuclear Power Generating Stations [IEEE has replaced this standard with IEEE 630, but 279 is mentioned specifically in 10 CFR 50.55a(h), Nov. 1988]
IEEE/ANSI 379-1988	Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety System
IEEE/ANSI 603-1991	Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE/ANSI 1033-1985	Recommended Practice for Application of IEEE Std 828 to Nuclear Power Generating Stations
IEEE/ANSI 7-4.3.2-1993	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

IEEE Software Engineering Standards

IEEE/ANSI 610.12-1990	Glossary of Software Engineering Terminology
IEEE/ANSI 730.1-1989	Standard for Software Quality Assurance Plans
IEEE/ANSI 828-1983	Standard for Software Configuration Management Plans
IEEE/ANSI 829-1983	Standard for Software Test Documentation
IEEE/ANSI 830-1984	Guide for Software Requirements Specifications
IEEE/ANSI 982.1-1988	Standard Dictionary of Measures to Produce Reliability SW
IEEE/ANSI 982.2-1988	Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software
IEEE/ANSI 983-1986	Guide for Software Quality Assurance Planning
IEEE/ANSI 1008-1987	Standard for Software Unit Testing
IEEE/ANSI 1012-1992	Standard for Software Verification and Validation Plans
IEEE/ANSI 1016-1987	Recommended Practice for Software Design Descriptions
IEEE/ANSI 1016.1-1993	Guide to Software Design Descriptions
IEEE/ANSI 1028-1988	Standard for Software Reviews and Audits
IEEE/ANSI 1042-1987	Guide to Software Configuration Management
IEEE/ANSI 1044-1993	Standard for Classification of Software Anomalies
IEEE/ANSI 1045-1992	Standard for Software Productivity Metrics
IEEE/ANSI 1058.1-1987	Standard for Software Project Management Plans

IEEE/ANSI 1059-1993	Guide for Software Verification and Validation
IEEE/ANSI 1061-1992	Standard for a Software Quality Metrics Methodology
IEEE/ANSI 1062-1993	Recommended Practice for Software Acquisition
IEEE/ANSI 1063-1987	Standard for Software User Documentation
IEEE/ANSI 1074-1991	Standard for Developing Software Life Cycle Processes
IEEE/ANSI 1175-1991	Standard Reference Model for Computing System Interconnections
IEEE/ANSI 1209-1992	Recommend Practice for the Evaluation and Selection of CASE Tools
IEEE/ANSI 1219-1992	Standard for Software Maintenance
IEEE/ANSI 1228-1993	Standard for Software Safety Plans
IEEE/ANSI 1298-1992	Software Quality Management System, Part 1 : Requirements

International Standards

IEC 557-1982	IEC Terminology in the Nuclear Reactor Field
IEC 639-1979	Nuclear Reactor. Use of the Protection System for Non-safety Purposes.
IEC 643-1979	Application of Digital Computers to Nuclear Reactor I&C
IEC 671-1980	Periodic Tests and Monitoring of the Protection System of Nuclear Reactors
IEC 709-1981	Separation within the Reactor Protection System
IEC 812-1985	Analysis Techniques for System Reliability - Procedure for FMEA
IEC 880-1986	Software for Computers in the Safety Systems of Nuclear Power Stations
IEC 960-1988	Functional Design Criteria for a Safety Parameter Display System for Nuclear Power Stations
IEC 987-1989	Programmed Digital Computers Important to Safety for Nuclear Power Stations
IEC 1014-1989	Programs for Reliability Growth
IEC 1025-1990	Fault Tree Analysis
IEC 1226-1993	The Classification of Instrumentation and Control Systems Important to Safety for Nuclear Power Plants
IEC 8631-1989	Information Technology - Program Constructs and Conventions for Their Representations
IEC 9126-1991	Information Technology - Software Product Evaluation - Quality Characteristics and Guidelines for Their Use

Nuclear Regulatory Commission

R.G. 1.22	Periodic Testing of Protection System Actuation Functions. [Basis for implementing GDC 21 and IEEE 279.]
R.G. 1.53	Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems. Basis for Implementing GDC 21 and IEEE 279, Section 4.2.[IEEE 379 implements the R.G. 1.53]
R.G. 1.152	Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants. [This guide endorses IEEE 7432.]

U.S.A Code of Federal Regulations

10 CFR 50 Appendix A, General Design Criteria for Nuclear Power Plants.
This is a partial list of GDC. Others may apply to I&C upgrade.

GDC 1 Quality standard and records
GDC 2 Design Bases for Protection Against Natural Phenomena
GDC 4 Environmental and Missile Design Bases
GDC 12 Suppression of Reactor Power Oscillations
GDC 13 Instrumentation and Control
GDC 15 Reactor Coolant System Design
GDC 19 Control Room
GDC 20 Protection System Functions
GDC 21 Protection System Reliability and Testability
GDC 22 Protection System Independence
GDC 23 Protection System Failure Modes
GDC 24 Separation of Protection and Control Systems
GDC 25 Protection System Requirements for Reactivity Control Malfunctions
GDC 26 Reactivity Control System Redundancy and Capability
GDC 29 Protection Against Anticipated Operations Occurrences

ASME/ANSI Standards

ASME/ANSI NQA-1	Quality Assurance Program Requirements for Nuclear Facilities
ASME/ANSI NQA-2	Quality Assurance Requirements for Nuclear Facility Applications

IEEE and ISO Local Area Network Standards :

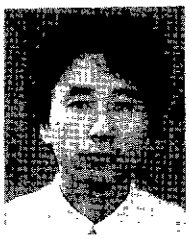
ISO 8802.2 : 1989	Information Processing Systems-Local Area Networks Part 2 : Logical Link Control. (Supersedes IEEE 8022-1985)
ISO 8802.3 : 1989	Information Processing System-Local Area Networks Part 3 : Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.
IEEE 802.4-1985	Token-Passing Bus Access Method and Physical Layer Specification
IEEE 802.5-1989	Standard for Local Area Networks : Token Ring Access Method and Physical Layer Specifications

이 장 수

1983 경북대학교 전자공학과 (공학사)
1986 한국과학기술원 전산학 (이학석사)
1994～현재 한국과학기술원 전산학과 박사과정
1991 정보처리기술사
1986～현재 한국원자력연구소 선임연구원
1995～현재 IEC TC45/SC45A 한국대표
1995～현재 IEEE SESC Software Safety Planning Group member

관심 분야 : 소프트웨어 안전성, 실시간 시스템 등

엄 홍 섭



1974～1979 중앙대학교 경영학과, 학사
1979～현재 한국원자력연구소 인공지능분야

관심분야 : 소프트웨어 안전성, 인공지능기술의 원전 적용,

권 기 춘

1974～1980 경북대학교 전자공학과, 학사
1984～1989 한국과학기술원 전산학과, 석사
1993～현재 한국과학기술원 전산학과, 박사과정
1980～현재 한국원자력연구소 계측제어연구팀 분야책임자

관심분야 : 고신뢰도 소프트웨어 검증 및 확인방법론, 인공지능기술 원전 적용, 실시간 시뮬레이션