Journal of the Korean Nuclear Society
Volume 26, Number 4, December 1994

《기술보고》

원전 계측제어 고신뢰도 소프트웨어 확인 / 검증 기술 현황

이장수 · 권기춘 · 동인숙
한국원자력연구소
(1994. 4. 25 접수)

요 약

원자력산업계에서는 원전 계측제어계통의 디지털화를 위해 많은 노력을 기울이고 있으나, 원자력산업의 특수성인 시스템 안전성 확보에 필요한 소프트웨어 개발기준과 규제방법이 정립되지 못하고 있다. 뿐만 아니라 디지털 계측제어계통의 핵심 기반기술인 고신뢰도 소프트웨어 개발 방법론이 확립되지 못하여 소프트웨어 공통모드고장 문제, 정량적인 소프트웨어 신뢰도 보장 문제 등이 논란의 대상이 되고 있다. 이와 같이 원전 계측제어계통 디지털화 성공을 위해서는 소프트웨어 신뢰도 확보가 관건이며 고신뢰도 소프트웨어 확인 및 검증 기술 개발이 절실히 요구된다.

본 기술보고에서는 디지털 계측제어계통 소프트웨어에 대한 규제요건을 소프트웨어 신뢰도 보장을 위한 개발자, 사용자, 규제자 사이의 합의 기준측면에서 분석하였다. 또한 최근의 미국 원자력규제위원회의 디지털 계측제어계통 소프트웨어에 대한 규제방법과 규제동향을 살펴보았으며 마지막으로 고신뢰도 소프트웨어 개발과 확인 및 검증 방법, 규제 요건, 규제 방법 등에서 공통적으로 고려해야 할 기술적 측면의 현안과 이의 해결을 위한 연구 현황등을 파악하였다.

1. 서 론

소프트웨어 확인 및 검증(Software Verification and Validation : S /W V&V)이란 시스템이 실제로 요구된 기능을 완벽하고 신뢰성 있게 수행함을 소프트웨어 개발공정 단계별로 확인(Verification)하는 절차이며, 그 소프트웨어 시스템이 요구 사항대로 설계되었음을 검증(Validation)하는 절차이다.

최근 원전의 아날로그 계측제어계통은 그 시스템의 노후화로 인한 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 신뢰도 보장 문제 등을 야기시키고 있다.

사용자, 개발자와 규제자 모두가 인정하는 소프트웨어 확인 및 검증용 방법론과 도구들은 계측제어계통 소프트웨어의 품질을 보증할 수 있고 소프트웨어의 신뢰도를 높임으로써 전체 디지털시스템의 품질을 보증한다. 소프트웨어의 설계와 개발 표준들은 일관성 있게 소프트웨어의 품질을 향상시킬 수 있고, 소프트웨어의 재사용 가능성을 높이며 소프트웨어 개발과 확인 및 검증을 자동화할 수 있는 도구 개발을 용이하게 한다. 또한 원전의 신경계통이라 할 수 있는 계측제어계통의 디지털화와 제어 기술의 고도화를 위해 지능형 소프트웨어의 개발이 상당한 비중을 차지할 것으로 예상되어 이에 대한 확인 및 검증 기술의 개발을 서둘러야 할 것이다. 원전 계측제어계통의 성공적인 디지털화를 위해서는 소프트웨어의 신뢰도 확보가 관건이며 고신뢰도 소프트웨어 확인 및 검증 기술 개발이 디지털화의 기반이고 핵심기술이다.

원전의 설계, 건설, 운영에 따른 규제요건은 원전의 안전을 최대로 확보하고 유지하려는 관점에서 추구되어

왔다. 새로운 원전을 건설하거나 기존의 원전을 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 작용하고 있다.

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

2. 규제요건 분석

2.1. 분석 범위

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 Nuclear Regulatory Commission (NRC), Electric Power Research Institute (EPRI), National Institute of Standards and Technology (NIST) 등 여러 기관에서 이러한 작업을 진행중에 있다.

본 절에서는 신뢰도와 권위를 가진 미국 NRC가 현재 원전 디지털 계측제어계통을 검토할 때 사용하는 접근에 따른 규제요건들중 안전관련 시스템의 소프트웨어에 관한 것만 분석한다.

디지털 계측제어계통에서 소프트웨어는 종전 아날로그 시스템에서 하드웨어적으로 해결하던 기능의 많은 부분을 대신하고 있다. 따라서 여기서 분석할 규제자료의 범위는 소프트웨어에 직접적인 것과 소프트웨어에 관련된 시스템적인 규제요건들이며, 또한 다중방호 개념의 안전관련 규제요건을 포함한다. 현재 사용중인 디지털 계측제어계통 관련 규제 및 규제참고 자료중에서 위에서 정한 분석 범위에 포함되는 자료는 다음과 같다.

Protection and Safety Systems

ANSI /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]

ANSI /IEEE 379-1888 Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety System ANSI /IEEE 603-1991 Standard Criteria for Safety Systems for Nuclear Power Generating Stations

ANSI /IEEE 1033-1985 Recommended Practice for Application of IEEE Std 828 to Nuclear Power Generating Stations ANSI /IEEE 7-4.3.2-1993 IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

IEEE Software Engineering Standards

ANSI /IEEE 729-1983 Glossary of Software Engineering Terminology

ANSI /IEEE 730. 1-1989 Standard for Software Quality Assurance Plans

ANSI /IEEE 828-1983 Standard for Software Configuration Management Plans

ANSI /IEEE 829-1983 Standard for Software Test Documentation

ANSI /IEEE 830-1984 Guide for Software Requirements Specifications

ANSI /IEEE 982. 1-1988 Standard Dictionary of Measures to Produce Reliability SW

ANSI /IEEE 982. 2-1988 Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software

ANSI /IEEE 983-1986 Guide for Software Quality Assurance Planning

ANSI /IEEE 1008-1987 Standard for Software

Unit Testing
ANSI /IEEE 1012-1986 Standard for Software Verification and Validation Plans
ANSI /IEEE 1016-1987 Recommended Practice for Software Design Descriptions
ANSI /IEEE 1042-1987 Guide to Software Configuration Management
ANSI /IEEE 1058. 1-1987 Standard for Software Project Management Plans
ANSI /IEEE 1063-1987 Standard for Software User Documentation

International Standards

IEC 880-1986 Software for Computers in the Safety Systems of Nuclear Power Stations
IEC Pub. 557(1982) IEC Terminology in the Nuclear Reactor Field
IEC Pub. 639(1979) Nuclear Reactor. Use of the Protection System for Non-safety Purposes.
IEC Pub. 643(1979) Application of Digital Computers to Nuclear Reactor I&C
IEC Pub. 671(1980) Periodic Tests and Monitoring of the Protection System of Nuclear Reactors

Nuclear Regulatory Commission (NRC)

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.]

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-Carrier
Part 3 : 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

2.2. 규제요건 현황

현재 NRC에서는 디지털시스템을 검토할 때 Reg. Guide 1. 152와 ANSI /IEEE 7-4.3.2-1993을 사용한다. ANSI /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 ANSI /IEEE 7-4.3.2를 만족시킬 의무가 있다. ANSI /IEEE 7-4.3.2는 규제자와 공급자 사이의 인터페이스, V&V의 독립성, V&V에 사용된 도구와 사람에 대한 자격, 하드웨어와 소프트웨어 및 시스템의 요구사항, 소프트웨어 개발 절차, 하드웨어 소프트웨어 통합, 확인 및 검증방법 등을 기술하고 있다. 그러나 ANSI /IEEE 7-4.3.2에는 시스템 및 하드웨어와의 통합을 고려하면서 주로 소프트웨어에 관련된 규제내용들이 원칙적인 측면에서 간략하게 기술되어 있다. 즉, ANSI /IEEE 7-4.3.2-1993의 본문 내용에는 다른 규제지침서와 표준들로의 참고부분이 많으며 기술적으로 구체적인 내용은 대부분 부록에 수록되어 있다. 따라서 NRC에서는 많은 부분을 확대해석하여 적용하고 있으며, 이에 따라 여러 가지 규제지침서들을 필요로 한다.

ANSI /IEEE 7-4.3.2의 상위 규제요건이며 계측제어 안전계통 표준 요건인 ANSI /IEEE Std 603-1991의 Section 5.3과 5.4에 따라 엄격한 확인이 요구되며 세부 시험방법으로 ANSI /IEEE 829가 사용된다. 이와 같이 ANSI /IEEE 7-4.3.2를 중심으로 디지털 계측제어계통 소프트웨어의 개발과정과 그 결과물의 건전성 평가에 사용되는 지침서들의 관계는 [그림 1]의 QUALITY 부분과 같다.

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 ANSI /IEEE 603-1991, ANSI /IEEE 379-1977, Reg. Guide 1.53, NUREG 0493 등에 잘 나타난다. ANSI /IEEE 7-4.3.2와 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 NRC는 수동정지계통을 추가로 설치하여 사용할 것을 주장한다. 또한 단일사고기준(Single Failure Criteria)을 만족시키기 위해 소프트웨어에 대해서도 고장모드영향분석(Failure Modes and Effect Analysis, FMEA)를 수행해야 한다. 이와 같은 다중방호 개념과 관련된 지침서들의 관계도는 [그림 1]의 SAFETY 부분과 같다. 이러한 상황에서 NRC는 개발된 디지털 계측제어계통이 ANSI /IEEE Std. 603, 279, 379, 7-4.3.2와 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.

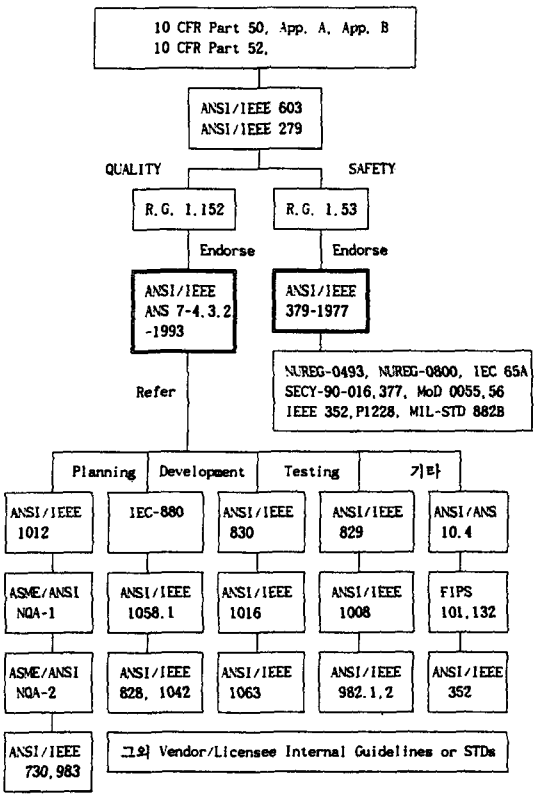

그림 1. 디지털 보호계통 소프트웨어 규제요건 체계

2.3. 규제방법

2.3.1. 기존 발전소 디지털화에 대한 NRC 규제 방법

NRC는 기존 발전소에서 새로 디지털화되는 계측제어 안전계통을 인허가 할 때 Reg. Guide 1.152와 ANSI/IEEE 7-4.3.2-1993을 주로 사용하고 ANSI/IEEE 1012-1986과 ASME NQA-2a-1990, Part 2.7을 참조한다. NRC가 수행하는 규제 방법은 대략 다음과 같다. 규제요원은 먼저 시스템 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 확인 및 검증 작업에 대한 검토 작업을 아래와 같이 수행한다.

(1) 프로그램의 개발 단계를 점검한다.
(2) 공급자와 규제자 사이의 인터페이스를 점검하고 이에 대한 피드백과정을 점검한다.
(3) 소프트웨어 문제/오류 보고서 등을 검토하고 정정 결과를 점검한다.
(4) ANSI/IEEE ANS-7-4.3.2와 V&V 과정을 비교한다.
(5) 개발과정에 참여한 사람을 인터뷰한다.
(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) V&V 결과물을 점검한다.

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

2.3.2. 개량형 경수로(ALWR)의 디지털 계측제어 시스템에 대한 NRC 규제 입장

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 시스템 구조 설계와 특징에 대한 특별한 제약이 필요하고 계측제어계통의 설계, 구현, 설치, 운전, 유지보수, 수정 등 개발 주기의 각 단계에 관련된 고수준의 적용 요건이 필요하다. NRC는 10 CFR Part 52의 일괄인허가(One-step licencing) 과정에서 15년 기간 동안 계측제어 분야를 포함한 원전의 표준 설계를 승인하지만 승인 과정중 공급자 사양을 필요로 하지 않으므로, 계속 발전되어 가고 있는 디지털 기술의 장점을 이용하기 위한 융통성을 갖는 것이 바람직하기 때문에 시스템 설계 부분, 특히 소프트웨어 설계 부분은 상위단계만 요구된다. 이와 같이 NRC는 설계 승인 기간 동안에 진부해 질 수 있는 설계의 세부 사항은 'lock-in' 하지 않고, 오히려 10 CFR 52의 설계 승인 접근 방법에서는 설계 과정의 품질과 설계승인기준(Design Acceptance Criteria, DAC), 제한 사항, 제한치 등에 대해 'lock-in'을 하기 위한 것이다. DAC의 개념은 NRC가 Inspection, Tests, Analysis and Acceptance Criteria (ITAAC)을 통하여 설계 승인을 받는 Combined License (COL) 지원자에 의한 설계 구현과 확인의 최종 안전성 평가를 할 수 있게 해준다.

NRC는 안전성 관련 계측제어계통 설계과정중에 각 단계에서 요구조건이 일치하는지 검증하기 위해 소프트웨어 ITAAC 구현을 감사(Audit) 한다. 각각의 감사 단계는 [그림2]와 같다. 이 결과에 따라 NRC는 검사보고서를 작성하고 문제에 대한 해결책을 제시한다. 해결되지 않은 중요한 현안사항 (Open Issue)에 대해서는 NRC가 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 ITAAC 과 더불어 안전계통에 대한 다양한 시험이 요구된다. 현재 NRC는 원전 디지털 보호계통과 같은 안전에 중대한 시스템들에 사용된 소프트웨어의 건전성 평가 결과를 기초로 다음과 같은 다양성에 대한 입장을 발표하였다.

(1) 피규제자는 제안된 계측제어계통의 공통모드고장의 취약성을 적절히 보완시켰는 것을 입증하기 위해 다중방호와 다양성을 평가해야 한다. 이를 위한 참고 자료는 NUREG-0493에 나타나 있으며 피규제자가 제안한 방법들은 따로 검토되어야 한다.
(2) 평가를 수행하는데 있어서 공급자와 피규제자는 안전성분석보고서(SAR)의 사고 분석에서 평가되는 각 사고에 대해 예상되는 공통모드고장을 평가해야

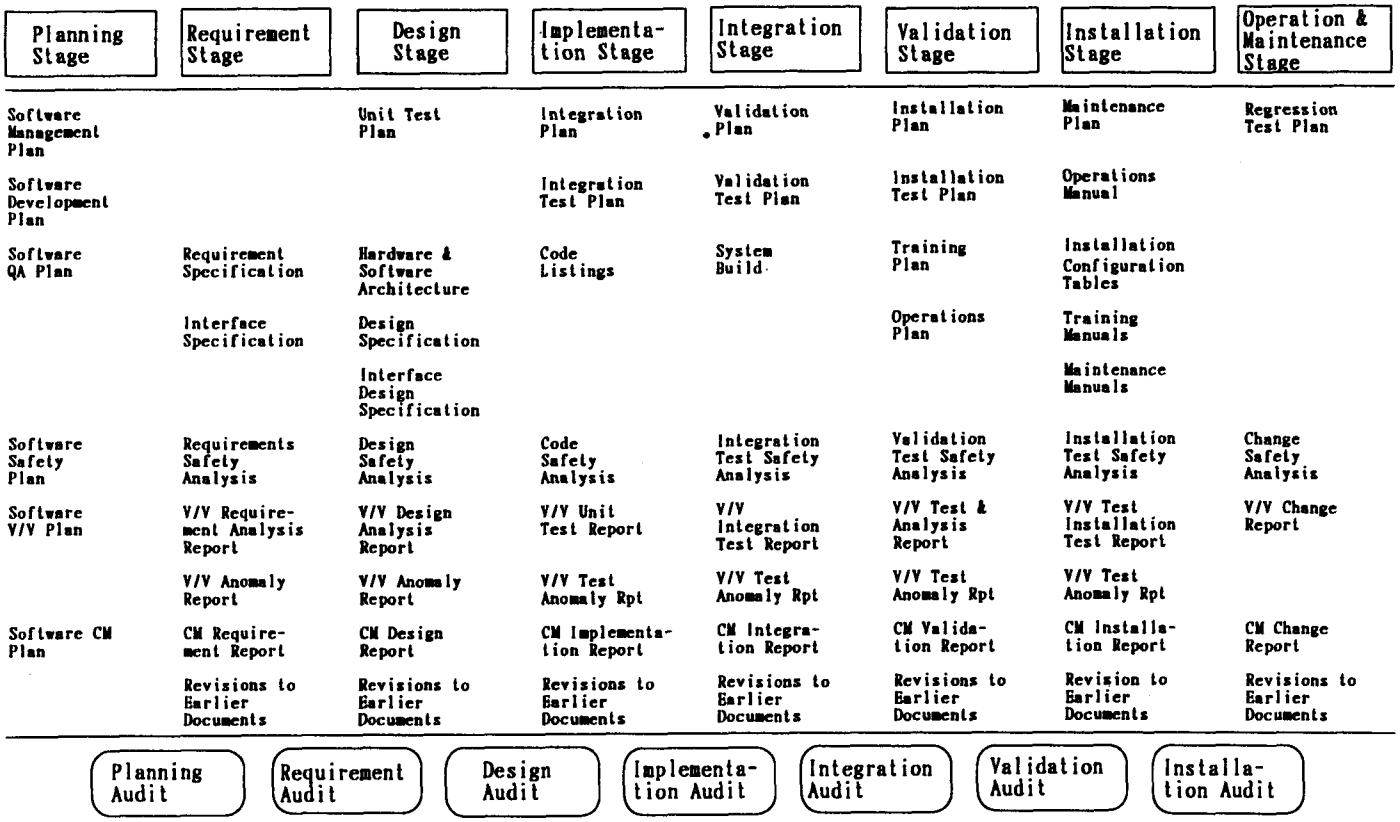

그림 2. Flow of Documents Through the Software Cycle

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 시스템이 관련된 사고 조건하에서 필요한 기능을 수행하기 위해 충분한 품질요건을 갖추었다면 비안전계통도 그 기능을 수행할 수 있다. 다양한 방법의 디지털과 비디지털 계통들이 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 안전기능을 지원하는 변수를 감시하고 필수안전 기능의 수용하기 위해서는 각각의 요건들이 유연성과 확장성을 갖도록 보완되어야 하며 IEEE, ASME등 타 산업 표준들과 개발자 내부 지침서, 규제요건들의 유기적인 연계체제를 갖추어야 한다.

3.2. 품질과 안전성 보장을 위한 문제점 고찰

3.2.1.품질 보증 측면

3.2.1.1. 계획 단계

이 단계에서는 Project Management Planning, Configuration Management Planning, 소프트웨어 Safety Planning, 소프트웨어 V&V Planning, 소프트웨어 Quality Assurance Planning 등이 수행되며 이와 관련하여 ANSI /IEEE 1058.1, ANSI /IEEE 828, ANSI /IEEE 730.1, ANSI /IEEE 1012, P1228 등의 Standards(Stds)들이 있다. NRC에서는 소프트웨어 개발 Life cycle 전단계에 대하여 감사와 검토를 수행하며 이 때 필요한 문서의 종류를 밝히고 있다.

그러나 NRC의 규제방법에서는 ANSI /IEEE 7-4.3.2-1993를 중심으로 상하의 관련된 Codes and Stds를 참고하여 규제를 시행하며 검토에 필요한 문서의 종류를 밝히고 있으나, 세부 기술적인 면에서 구체적이고 명확한 기준과 한계를 세우지 못하고 있는 실정이다. 예를 들면 Project Management Plan에서 개발 팀과 V&V 팀의 독립성에 대한 명확한 정의, 소프트웨어 Safety Plan에서 모든 종류의 소프트웨어에 대한 정량적인 신뢰도 명시, 요구되어지는 문서들이 가져야 할 세부적인 기술사항에 대한 구체적인 언급이 없다.

3.2.1.2. 요구분석 단계

이 단계에서는 요구사양을 작성하고 분석할 때 수학적인 formalism을 도입하여 품질과 신뢰도를 높여 보고자 하는 것이 최근의 추세이다. 요구사양을 형식에 맞게 작성함으로써 다음 단계인 설계를 수행할 때보다 완벽하게 요구사항을 반영할 수 있고 요구분석을 수동 혹은 자동으로 수학적인 증명을 할 수 있다. 그리고 결함을 개발공정 초기에 발견하여 수정할 수 있음으로써 개발비용을 절감할 수 있는 장점이 있다. 그러나 이 단계의 주목적이 사용자 혹은 시스템 엔지니어와 소프트웨어 엔지니어사이의 의견교환을 통해서 정확한 요구사항을 수립하는 것인데, 이러한 Formalism의 도입은 자연언어를 사용한 통신보다는 의사 전달이 부자유스러운 단점이 있다.

이러한 정형화된 요구조건으로부터 Test case를 자동 생성할 수 있고 요구사양 자체를 실행할 수 있는 자동화 도구를 만들어 요구분석 단계에서 개발하고자 하는 시스템의 동작을 시뮬레이션해 봄으로써 결함을 조기 발견, 해결하고자 하는 노력을 진행 중에 있다. 이외에도 Requirement Traceability의 완벽한 시행 및 자동 점검방법 등에 대한 연구와 상품화가 진행 중에 있다.

3.2.1.3. 설계 단계

여기서도 앞 단계에서와 같은 Formalism 도입이 시도되고 있으며 설계 방법론에서도 이제까지의 구조적 설계 방법론에서 점차 객체지향 설계 방법론으로 바뀌어 가고 있다. Module Coupling, Cohesion등 Modularity, Information Hiding등 그 동안의 소프트웨어 공학에서의 연구 결과들이 점차 객체지향 설계 방법론으로 초점이 맞춰지고 있다. 이러한 객체지향 설계 방법은 재사용성을 높여 개발하는 소프트웨어 시스템의 신뢰도를 높이고 V&V 비용을 낮출 수 있다.

3.2.1.4. 구현 단계

개발에 사용되는 프로그래밍 언어가 점차 어셈블리 언어에서 'C', 'Ada'와 같은 고수준 언어로 바뀌어 가고 있으며 앞으로는 'C++'과 같은 객체지향 언어가 사용될 전망이다. 프랑스의 N4 시스템의 소프트웨어 개발에는 Ada가 사용되었다. 이러한 프로그래밍 언어의 선택과 소프트웨어 공통모드고장 극복을 위한 다양성을 언

어와 컴파일러에 적용하고 있다. 또한 컴파일러, 운영체제, 시험 도구, 에디터등 개발에 사용되는 모든 도구들에 대한 Prequalification이 문제가 되고 있다. 소프트웨어 개발 회사들은 자체적으로 코딩 지침서등을 작성하여 사용하고 있으나 표준화가 되어 있지 못한 형편이다. 완벽한 예외사항 처리등 고장허용 프로그래밍이 요구되고 있으며 고장허용 소프트웨어의 개발은 요구분석 단계부터 고려되어야 할 기술적인 사항이 매우 많다. 이를 위해 현재 시도되고 있는 기술들 중 대표적인 것으로 소프트웨어 개발공정 전 단계에 걸쳐 다양성을 고려하는 N-version 프로그래밍 기법과 Recovery Block 기법이 사용되고 있으나 소프트웨어 복잡도 증가에 따른 안전성 위해요소가 있어 많은 논란이 제기 되고 있다.

3.2.1.5. 통합, 확인 및 검증 단계

검증이란 소프트웨어 개발의 각 단계에서 그 소프트웨어가 요구사항을 만족하는가를 평가하는 것이며, 확인은 소프트웨어 개발공정 전체 단계에서 해당 단계의 결과물이 전단계의 결과물과의 일관성, 완벽성, 정확성을 만족하는가를 확인하는 것이다. 요구분석 단계, 설계 단계, 구현 단계를 거치면서 세부 모듈의 프로그래밍이 되고 나면, 이러한 break-down의 역순으로 모듈들을 통합하여 시스템을 완성하고 통합 순서에 따라 확인과 시험이 이루어진다. 이러한 시험은 모듈시험, 통합시험, 기능시험, 시스템 시험, 인수시험, 설치시험의 순서로 이루어진다. 시험의 각 단계에서 사용될 수 있는 기법과 도구에 대한 대표적인 서적으로 G.J. Myers의 "The Art of Software Testing"과 B. Beizer의 "Software Testing Techniques"등이 있으며 관련 연구 논문들이 계속해서 나오고 있기 때문에 이들의 선택과 사용에 세심한 주의를 기울여야 하며, 요구되는 신뢰도에 따라 시험계획 작성과 시험종료시점이 달라지며 고신뢰도 소프트웨어 일수록 시험비용이 올라간다. 근본적으로 소프트웨어의 완벽한 시험은 불가능하며 확인 및 검증의 독립성, 자가시험, 확인 및 검증의 정도등이 주 관심사이다. 현재 사용중인 시험관련 Standard에는 ANSI /IEEE 829와 ANSI /IEEE 1008이 있으며 확인 및 검증과 관련하여 ANSI /IEEE 1012가 있다.

3.2.1.6. 설치, 운영 및 유지보수 단계

이 단계에는 설치문서, 운전 및 유지보수 지침서, 훈련지침서등 각종 문서들을 정확히 갖추어야 하며 개발과정에서 발견하지 못한 결함을 보완하기 위한 유지 및 보수계획, Regressing 시험계획과 이에 따른 Configuration Management Change, V&V Anomaly Report, Safety Analysis Change 등이 중요하다. 특히 소프트웨어 유지보수는 계측제어계통이 하드웨어에서 소프트웨어로 바뀜에 따라 현장에서 느끼는 가장 심각한 애로 사항으로 부각되고 있어 소프트웨어 시스템에 대한 시험가능성 여부는 새로운 문제로 제기되고 있다.

3.2.2. 안전성측면

원전 계측제어계통이 디지털화 되면서 소프트웨어 공통모드고장 극복과 같은 소프트웨어 안전성 보장문제가 쟁점으로 부각되고 있다. 품질보증 측면에서의 노력에도 불구하고 공통모드고장이 발생할 가능성이 있기 때문에 다중방호 보장을 위한 설계에서의 다양성 제공이 필요하다. 기능적 다양성 개념은 NUREG-0493 1979에 잘 나타나 있다.

원전 안전계통의 신뢰도 분석에 대한 일반적인 원칙은 ANSI /IEEE 352-1987에 소개되어 있으며 고장모드영향분석과 고장수목분석과 같은 정성적인 신뢰도 분석방법과 수학적 모델링에 의한 정량적인 신뢰도 분석원칙을 설명하고 있다. 즉 신뢰도 분석에 대한 시스템 차원에서의 이론들을 표준화한 것이다. 이렇게 표준화된 시스템 차원의 이론들은 소프트웨어에 그대로 적용될 수 없으며 소프트웨어의 신뢰도 분석을 위한 정성적, 정량적 방법과 척도가 표준화 되어야 한다.

이러한 표준화를 위한 노력의 일환으로 NUREG /CR-5930와 IEEE /P-1228등이 만들어졌다. NUREG /CR-5930에서는 고신뢰도 소프트웨어의 Standards와 Guidelines이 가져야 할 기준을 설명하고 기존 지침서들의 문제점을 분석하고 있다. 여기서는 고신뢰도를 요하는 소프트웨어의 안전성을 보장하기 위한 방법으로 소프트웨어 위험도분석에 대한 기준을 제시하고 있으며 이러한 기준 전체에 대한 설명은 다음절에서 하고자 한다. 초안으로 발표된 IEEE /P-1228은 소프트웨어 안전성 확보계획에 대한 방법들을 서술하고 있으나, 명확히 하고 수정해야 할 내용이 많은 것으로 NUREG /CR-5930에서는 분석하고 있다. 현재 10 CFR 52에 의거한 NRC의 단계별 소프트웨어 ITAAC에서 명시하는 문서들 중에는 이러한 소프트웨어 안전성확보계획과 소프트웨어 안전성분석 관련 문서들이 요구되고 있으나 이와 같은 문서를 작성하고 이를 검토할 때 필요한 Standard나 Guideline이 없는 실정이다.

3.3. 고신뢰도 소프트웨어 확인검증 기준

고신뢰도의 소프트웨어 시스템을 개발하기 위해서는 개발자, 감리자, 사용자가 공동으로 사용할 수 있는 고신뢰도 소프트웨어 공학 분야의 객관적 이론이나 기술적 근거가 있어야 한다. 그러나 타 공학 분야와는 달리 소프트웨어 공학 분야의 이러한 이론들은 Standard나 핸드북 형태의 체계적이고 종합적인 문서화가 미흡한 실정이다. 본 절에서는 Standard가 체계적으로 문서화되고 대상 소프트웨어의 객관적인 측정도구로 사용될 수 있기 위한 기준을 설명하고자 한다. 이에 대한 연구는 미국의 NIST가 NRC 과제로 수행하였으며 그 연구결과인 NUREG/CR-5930 내용중 기준에 관련된 핵심적인 것만을 요약하고자 한다.

3.3.1. 중요도/ 보증의 수준

인적, 물적 중요도의 정도에 따라 개발하고자 하는 소프트웨어의 요구사항, 개발에 사용된 도구, 방법론 등이 달라져야 한다. 이와 같은 것들은 중요도이외에도 인공지능 기법과 같은 신기술의 사용, 소프트웨어가 가지는 임무의 중요도, 프로젝트의 크기 등에 의해서도 달라지지만 NUREG/CR-5930에서는 소프트웨어 결함에 따른 결과의 심각성만을 고려하여 각 방법론의 기준을 설명하고 있다.

3.3.2. Life cycle Phases

Standard가 Life cycle의 단계를 갖는 것이 소프트웨어 개발공정 각 단계에서 생산되는 문서의 범위를 분명히 하기에 용이하다. 여러 가지 Life cycle 모델이 있고 각 모델에서의 단계에 대한 표현도 다양하지만 일반적으로 계획(초기), 요구분석, 설계, 구현, 통합 및 시험, 설치, 운영 및 유지보수등으로 이루어진다.

3.3.3. 문서화

소프트웨어 문서화는 개발자, 사용자, 감리자, 검사자, 인허가자 각각에게 서로 다른 여러 가지 목적을 부여한다. 따라서 Standard는 문서의 요구사항이 얼마나 철저한가?, 문서화에 묘사되어야 할 내용과 항목이 제대로 명시되어 있는가?, 정량적인 특성 묘사가 있는가? 등을 반영하여야 한다.

3.3.4. 위험대비 소프트웨어 기능성

시스템 위험도분석은 시스템 동작에 급작스럽게 영향을 줄 수 있는 위험요소의 종류에 대한 정보를 제공한다. 특정 소프트웨어는 이러한 위험요소를 발견하고 완화하며 극복하는 기능을 가질 수 있으며 고신뢰도 소프트웨어 Standard에서는 이와 같이 위험요소를 대비하기 위한 소프트웨어의 방호 기능을 고려하여야 한다.

3.3.5. 소프트웨어 공학 실행

소프트웨어 공학의 실제기술들의 적절한 사용이 고신뢰도 소프트웨어 개발에 필수적이며 Standard에 정확하게 명시되어야 한다. 즉 정형화된 명세서, Component Isolation, Modularity, 언어와 컴파일러 선택, 부동 소숫점 계산과 인터럽트를 사용하지 않는 프로그래밍, Quality Attributes 등이 반영되어야 한다.

3.3.6. 보증활동

소프트웨어 개발공정 전체에서의 문제점 발견을 위한 활동들인 소프트웨어 확인 및 검증, 소프트웨어 품질보증, Software Configuration Management, 소프트웨어 위험도분석 등에 관하여 Standards가 가져야 할 기준을 명시하고 이에 대한 공정을 수행한다. 소프트웨어 품질보증은 Product가 기술적 요구사항을 만족한다는 믿음을 제공하기 위한 계획적이고 체계적인 행동양식이다. Software Configuration Management는 소프트웨어 개발과 유지보수를 할 때 항목들의 특성을 식별하여 문서화하고 Baseline 화하며, Configuration Identification, Configuration Control, Configuration Status Control, Configuration Audit 등이 주된 임무이다.

4. 결 론

본 기술보고에서 사용된 중요한 소프트웨어 공학 용어 두가지를 다시 한번 분명히 하면 다음과 같다. 먼저 확인 및 검증이란 소프트웨어 시스템이 요구사항대로 설계되었는지를 보장하는 절차이며 그 시스템이 실제로 요구된 기능을 완벽하고 신뢰성 있게 수행함을 개발공정 단계별로 확인하는 절차이다. 다음으로 방법론이란 소프트웨어 개발 전형에 따른 life cycle의 설정, 설정된 life cycle에 따른 개발 지침서, 확인 및 검증지침서, 개발도구를 포함한 체계적인 개발환경 등을 의미하며 소프트웨어 개발 철학 및 개발자 윤리까지도 포함된다.

본 기술보고에서는 원전 계측제어계통의 성공적인 디지털화를 위한 기반기술이자 핵심기술인 고신뢰도 소프트웨어 확인 및 검증 방법론을 우리 실정에 맞게 개발, 정립하기 위한 준비 단계로서 이 분야 기술 현황을 규제요건, 규제 방법, 규제 접근 방법등에서의 기술적 현안을 중심으로 기술하였다. 이러한 기술적 현안을 해결하기 위한 연구 노력들을 NRC를 중심으로 살펴보았고, 고신뢰도 소프트웨어 규제요건이 갖추어야 할 기준을 서술하였다.

원자력 산업에서의 계측제어계통 디지털화와 이를 위한 고신뢰도 소프트웨어의 성공적 개발을 위해 개발자, 규제자, 사용자등 각계 각층에서 체계적이고 종합적인 노력을 기울이고 있다. 본 기술보고에서도 이러한 노력의 일환으로 디지털 계측제어계통 소프트웨어에 대한 규제요건을 규제나 인허가 측면이 아니라 소프트웨어 신뢰도 확보 관점에서 개발자, 사용자, 규제자가 공감하는 합의기준이 되기 위해 필요한 기술적인 측면을 파악해 봄으로써 규제요건이 정립되어야 할 방향을 제시하고자 하였다.

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 NRC, AECB 등 각국의 규제기관들에서도 규제시행 측면에서 소프트웨어 안전성 보장을 위한 연구를 수행 중에 있다. Lawrence Livermore National Laboratory와 National Institute of Standard and Technology등 NRC 자문기관들에서는 원자력 분야 소프트웨어의 안전성 보장을 위한 광범위한 연구와 디지털 시스템 안전성 평가 업무를 수행 중이며 관련 기술이 많이 축적된 것으로 알려지고 있다. 또한 CMU의 Software Engineering Institute를 포함하여 학계에서도 안전에 중대한 소프트웨어에 대한 연구를 활발히 수행하고 있다. EPRI에서는 Upgrade Plan에 따라 소프트웨어 확인 및 검증과 표준에 관련된 연구를 수행 중에 있다. 캐나다 Darlington 발전소의 안전정지계통 소프트웨어의 안전성을 수학적인 방법으로 증명한 David Parnas의 회사와 같은 전문용역업체들과 Computer Aided Software Engineering(CASE)와 같은 소프트웨어 개발 도구 회사들도 이러한 소프트웨어의 품질과 안전성을 보장하기 위한 연구 개발 노력을 아끼지 않고 있다. 이외에도 ABB-CE, Westinghouse, AECL, EdF 등 원전 공급업체들도 원전 디지털 계측제어계통의 핵심기술인 소프트웨어의 안전성 보장과 확인 및 검증 기술의 확보를 위해 많은 노력을 기울이고 있다.

이와 같은 종합적인 노력에 의해서 디지털 소프트웨어 시스템의 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 확인 및 검증 기술과 같은 핵심 기반기술의 확보가 필수적이다.

현재 추진 중인 원전 계측제어 시스템의 디지털화 목표를 성공적으로 완수하고 디지털 시스템 인허가 장벽을 원활히 극복하기 위해서는 원전 계측제어 소프트웨어의 분류에 따른 모든 종류의 소프트웨어에 대한 고유의 개발 방법론과 개발절차를 갖추어야 한다. 나아가서 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, 고신뢰도 소프트웨어 관련 기반기술 연구를 적극적으로 수행하여야 한다.

참고문헌

1. 본문 2.1 분석 범위에 표시된 모든 Codes and Standards.
2. NUREG/CR-5930, "High Integrity Software Standards and Guidelines," NIST, U.S. DoC, September 1992.
3. NUREG/CR-4640, "Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry," Pacific Northwest Laboratory, August 1987.
4. NPX80-SQP-0101.0, "Software Program Manual for NUPLEX 80+," ABB-CE, January 21, 1993.
5. Digital Systems Reliability and Nuclear Safety Workshop, "(Draft) Operating Reactors Digital Retrofits Digital System Review Procedures," "(Draft) Branch Technical Position(HICB) Digital Instrumentation and Con-

trol Systems in Advanced Plants," NIST, U. S. DoC, September 1993.
6. NUREG-1462, "Draft Safety Evaluation Report Related to the Design Certification of Combustion Engineering System 80+," U.S. NRC, September 1992.
7. NUREG-0493, "A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," U.S. NRC, March 1979.
8. ANSI/ANS-10. 4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry," American Nuclear Society, May 1987.
9. 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.
10. EPRI NP-7343, "Integrated Instrumentation and Control Upgrade Plan," EPRI, February 1992.
11. ANSI/IEEE Std 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generation Station Safety System," IEEE, October 13, 1987.
12. Glanford J. Myers, "The Art of Software Testing," John Wiley & Sons, Inc., 1979.
13. Boris Beizer, "Software Testing Techniques," 2nd Edition, Van Nostrand Reinhold, 1990.
14. 권기춘외 "원전 계측제어 고신뢰도 소프트웨어 확인/검증 기술 현황," KAERI/AR-411/94, 한국원자력연구소, 1994.
15. ANSI/IEEE 7-4.3.2-1993, "Standard Criteria For Digital Computers In Safety Systems of Nuclear Power Generating Stations," Draft 8, 1993.
16. IEEE/P-1228, "Standard for Software Safety Paln," Draft k, Sep. 1993.