'99 추계학술발표회 논문집
한국원자력학회

차세대 원전 디지털 계측제어계통의 소프트웨어 건전성 등급 평가 방법

Evaluation Method of Software Integrity Level Usable for KNGR I&C System

이우준, 박현신, 정학영
한국전력공사 전력연구원,
대전광역시 유성구 문지동 103-16

요 약

디지털 기술이 발전에 따라 기존의 아날로그 방식의 계측제어계통이 컴퓨터 기반의 디지털 계측제어계통으로 전환되면서 소프트웨어의 고장(Fault)으로 인한 안전성저해 때문에, 규제기관에서는 소프트웨어 개발에 관한 요건을 철저히 준수할 것을 요구하며, 이는 개발자에 노력 및 비용면에서 부담이 되고 있다. 이러한 상황에서, 소프트웨어 등급분류는 효과적인 수명주기 활동, 특히 소프트웨어 확인 및 검증활동을 위한 절차마련에 중요한 기반이 된다. 본 보고서는 소프트웨어 등급을 결정하는 기존의 인자(Factor)들을 검토하고 차세대 원전 디지털 계측제어계통에 적용할 수 있는 수정된 소프트웨어 등급분류 기준을 제안하고 있다. 본 논문에서 제안한 분류기준은 정성적이지만, 근사적으로는 상대적 위험도를 반영하고 있다.

Abstract

The analog-based nuclear instrumentation and control(I&C) system have been replaced with computer-based system. Due to the possible safety impact of the software failure, it is strictly required to follow rigorous software development procedure based on software engineering, which in general necessitates a great amount of effort and cost. Under this situation, it is highly recommended to develop a software classification which can guide for the cost-effective software life cycle activities, especially for software verification and validation activities. This paper reviews several attributes and factors proposed for determining the software category and then, suggests a classification criteria usable for KNGR(Korean Next Generation Reactor) digital I&C system softwares, putting more importance on the plant availability in the evaluation of software integrity level(SIL). While the proposed classification is qualitative, it reflects the risk ranking.

1. 배 경

원자력 발전소의 계측제어계통(Instrumentation and Control; I&C)에서 사용되는 Analog 방식의 기기들은 대개 20 내지 30년 된 기기들이여서 고장확률이 증가하고 유지 및 보수비용이 증대된다. 뿐만 아니라 기기 단종으로 인해 유지/보수하는데 어려움이 있다. 이러한 문제점이 과거 1970년대 말, 1980년대 초에 제기되어 전세계의 많은 원자력 발전소들이 기존의 Analog 방식의 계측제어계통을 Computer를 기반으로 하는 디지털 방식의 계측제어계통(이하 디지털 계측제어계통)으로 전환하는 추세이다. 디지털 계측제어계통으로 전환되면서 Analog 방식의 기기들이 가지고 있었던 기능적 문제점들이 제거되거나 향상된 기능을 제공하고 있다.

반면에 소프트웨어와 관련한 문제점들이 적지 않다. 즉, 소프트웨어의 오류로 인한 전 디지털 계통의 마비가 그것이다. 이와 관련하여, Leveson(1995)은 소프트웨어 설계에 있어서 문제점을 다음과 같이 설명하고 있다. 첫째, 소프트웨어는 Analog의 기능을 단지 Discrete하게 모사할 뿐이고 그 과정에서 부정확하고 복잡한 작업이 불가피하다는 것이다. 둘째, 유연성(Flexibility)으로부터 초래된 문제이다. 저자는 Flexibility가 이점이 될 수도 있지만 소프트웨어는 물리적 제한(Physical Limitation) 또는 자연법칙(Natural Law)이 적용되지 않아 복잡한 소프트웨어를 임의적으로 설계할 수 있고 그로 인해 쉽게 오류가 발생할 수 있다고 지적하고 있다. 셋째, 소프트웨어의 복잡성 및 보이지 않는 연계관계이다. 즉 복잡하게 얽힌 연계관계로 인해 수행도중 발생할 수 있는 오류를 쉽게 예측할 수 없다는 것이다. 마지막으로, 과거의 운영 정보의 부족이다. 다시 말하면, 소프트웨어는 해당 목적에 국한되어 설계되기 때문에 측정, 평가 혹은 설계 개선을 위한 가용한 운영경험정보들이 축적되어 있지 않다는 것이다.

결국, Computer를 동작하는 소프트웨어의 예측할 수 없는 비물리적 원인에 의한 계측제어계통의 마비는 심각한 사고로 연결될 수 있고 처리/보수비용은 경우에 따라서는 막대한 경제적 부담을 가져다 줄 수 있다. 규제기관에서는 이러한 가능성을 방지하기 위해 다양성을 가진 계통을 추가로 설치하도록 요구하고 있지만 소프트웨어의 오류로 인한 위험성을 근본적으로 해결하기 위해 엄격한 소프트웨어 개발요건을 마련하여 소프트웨어 설계 검토 및 요건 준수 감시활동을 강화하고 있는 실정이다.

현재 디지털 계측제어계통, 특히 안전성관련 소프트웨어에 대한 규제요건과 관련한 산업표준규격 또는 유사한 지침서들은 다양한 소프트웨어 개발 모델을 제시하고 있다. 또한 NUREG-0800 및 관련된 지침서들(예를 들면 IEEE Standard 또는 IEC Guideline 등)은 일련의 체계적인 소프트웨어 수명주기 활동(Software Life Cycle Activity)을 중심으로 개발 절차를 제시하고 있다. KINS에서도 디지털 계측제어계통설계에 대한 안전성 심사기준을 마련하여 차세대원전설계에 적용하고 있는데 1) 컴퓨터 소프트웨어의 신뢰성 2) 컴퓨터 하드웨어의 성능검증 3) 심층방어 설계 개념의 적용 등 3가지 인허가 심사 현안을 중심으로 기준을 마련하고 있다[윤원영, 1997]. 특히 소프트웨어 개발과 관련한 소프트웨어 수명주기 활동의 수행여부를 검증하는 것에 그 초점을 두고 있다.

이러한 소프트웨어에 대한 엄격한 규제요건은 그 고장으로 인한 위험성을 고려할 때 타당한 면이 있으며, Leveson이 지적한 4가지 문제점들에 비추어 보면 Software 개발요건은 그러한 문제점을 최대한 해결할 수 있는 노력들이 반영되어 있는 것은 사실이다. 또한 현 상황에서 소프트웨어의 신뢰성을 확보하기 위한 적절한 요건으로 사료된다. 그러나 소프트웨어 수명주기 활동에 대한 지침서가 다양하고 절차 및 방법론에 대한 기준이 정립되어있지 않은 상태에서 개별적 요건이 요구하는 수행활동의 범위(Scope) 및 깊이(Depth)는 소프트웨어 개발자에 따라 다양하게 해석될 수 있는 여지를 남겨 놓고 있다. 예를 들면, 차세대원자로 상세안전요건에서는

> '컴퓨터-기반 보호계통의 소프트웨어는 소정(所定)의 보호기능을 수행할 수 있도록 철저한 소프트웨어 개발공정에 따라 개발되어야 한다. 특히 소프트웨어와 하드웨어의 통합 그리고 통합된 컴퓨터시스템을 보호계통에 통합시키는 개발 공정이 철저히 지켜져야 하며, 그리고 소프트웨어 개발, 상업용 컴퓨터 검증, 소프트웨어 개발툴, 확인 및 검증(V&V), 형상관리(CM) 등에 관한 요건들을 만족하여야 한다(9.2.4.5절 3항).'

> '안전관련 계측제어계통은 그것이 지원하고 있는 안전계통 또는 안전관련설비의 설계기준을 원칙적으로 따라야 한다. 그 설계기준은 일반적으로 수행하는 안전기능의 중요도에 따라 다르지만, 최소한 다음과 같은 사항들을 포함하여야 한다. 컴퓨터-기반 계측제어계통은 또한 컴퓨터에 관한 시스템 설계기준들을 고려하여야 한다(9.3.3.1절)'

고 기술할 뿐 보호계통과 안전관련 계측제어계통간에 구별된 차별적 요건을 기술하고 있지 않다. 즉, 여러 규제 및 연구기관에서 제시하는 Computer를 기반으로 하는 계측제어계통의 안전성에 대한 근거가 정성적이고 결정론적(Deterministic)이며 보수적인 측면이 적지 않아 개발자들에게 상당한 부담이 되고 있기도 하다. 이와 같은 요건에 부합되는 소프트웨어 개발비용의 증대 및 소프트웨어 유지 및 보수비용의 증가로 인하여 디지털 계통의 교체함으로써 기대할 수 있는 경제성 효과는 뚜렷이 입증되지 않고 있으며 다소 위축되는 경향이 없지 않다.

계통에 속한 소프트웨어의 성격에 따른 차별적 요건적용이 개발자의 책임사항이라면 개발자(혹은 기관)에서 소프트웨어 개발절차에 대한 차별적 기준마련 및 근거를 제시하고 이 기준이 소프트웨어 신뢰성 및 안전성을 충분히 만족할 수 있음을 보일 필요가 있다. System 80+에 대한 FSER(Final Safety Evaluation Report)에서도 "비안전관련 소프트웨어도 안전관련 소프트웨어의 개발 방법과 유사한 구조적 방법으로 개발하여야하지만, 안전관련 소프트웨어에 대한 요건을 엄격히 준수할 필요는 없다" [NUREG-1462, 1994]라고 기술하고 있어 개발 절차 및 방법 그리고 심도(Depth)는 개발자가 구체적이고 합리적으로 정립할 필요가 있다.

이와 같은 소프트웨어의 차별적 개발 절차를 마련하기 위해서는 소프트웨어의 등급분류가 선행되어야 한다. 즉, 소프트웨어 수명주기 활동을 포함한 개발 절차 및 요건들을 선택적으로 적용하거나 심도(Depth)를 다르게 적용할 수 있는 등급분류 기준이 필요하다. 이를 위해서는, Software Integrity Level(SIL)을 부여하여 소프트웨어 개발 요건에 준용하는 방법 및 절차 그리고 그 깊이 등을 Level에 따라 등급별로 적용하여 요구되는 Integrity Level을 성취하는 것이 효과적일 수 있다. 여기서 SIL은 설계, 확인 및 검증방법 및 절차에 대한 요건의 심도를 반영하는 것으로서

Level이 높을수록 수명주기 활동을 철저하게 수행하여 품질(Quality)을 보장하는 것을 의미한다. 따라서, 낮은 SIL의 소프트웨어라고 해서 낮은 품질을 목표로 하는 것이 아니라 품질을 보장하기 위한 문서 및 수명주기 활동의 정도가 낮은 것을 의미한다. 불필요한 개발절차를 지양하되 필요할 경우에는 비안전 계통의 소프트웨어라 할 지라도 철저하게 설계 및 확인/검증 절차를 수행할 수 있는 근거를 마련하는 것이 바람직할 것이다. 현재 몇 몇 기관에서는 안전등급을 기초로 하여 소프트웨어를 분류하고 차별적으로 소프트웨어 개발 요건을 적용하고 있지만 그 기준에 대한 기술적 기반(Technical Basis)의 타당성 및 적용성을 재검토할 필요가 있다. 따라서 본 보고서에서는 EPRI 등에서 제안하는 소프트웨어 분류방법을 분석하고 이를 원전 디지털 계측제어계통에 적용할 수 있도록 문제점을 보완하고 결과적으로 수정된 소프트웨어 분류기준을 제안하고자 한다.

2. 소프트웨어 분류기준

현재까지 알려진 소프트웨어 분류 방법은 주로 EPRI 및 AECL에 제안 된 것이 대표적인 예인데 AECL은 CANDU PHWR(가압중수로) 소프트웨어 개발에 적용하고 있다.

EPRI에서는 먼저 계통을 안전기능에 따라 분류하는데 설계요건이 결정론적 방법으로 확립되었거나 확률적 방법으로 확립되었을 경우 모두에 대해서 적용할 수 있다. 결정론적 방법의 경우에 있어서는 발생확률을 고려하지 않고 개시사건(Initiating Event) 및 계통의 고장으로 인한 결과만을 고려하여 분류하며, 확률적 방법인 경우 개시사건의 확률 및 계통의 신뢰성을 고려한 Risk ranking에 따라 분류 할 것을 제안하고 있다[EPRI TR-103291]. 계통분류 후에는 등급에 비례한 SIL을 잠정적으로 부여하고, 세부적으로 Adjusting Factor를 고려한 SIL을 조정할 것을 제안하고 있다 (Level 1이 가장 높은 등급을, Level 4는 가장 낮은 등급을 의미함). Adjusting Factor로는 다양성(Diversity), 소프트웨어 고장 결과(Software Failure Consequences), 기능적 복잡성(Functional Complexity)의 3가지를 제안하고 있다. [Adjusting Factor에 대한 자세한 내용은 동보고서 참조]

AECL의 분류 방법은 Risk-Based 분류방식이라 할 수 있는데, 먼저 Plant System 안전 중요도를 결정(Phase I)한 후 소프트웨어의 고장으로 인한 영향을 유형별로 결정(Phase II)하여 소프트웨어를 분류하고 있다[G. Archinoff 등, 1995]. Phase I에서 고장확률 및 고장의 결과로 평가하는데 계통의 Unavailability Requirement(Q) (안전/완화 계통 및 감시/시험계통에 대해서) 또는 Initiating Event Frequency Limit(f) (공정계통에 대해서)를 이용하여 계통의 안전 중요도를 High, Medium, Low로 평가하고 있다.

Phase II에서는 소프트웨어 고장 모드 및 영향을 분석하여 소프트웨어가 Phase I에서 결정된 계통의 안전기능에 미치는 정도에 따라 Type I, II, III로 나누고 있다. 이 과정에서 계통의 등급보다 낮은 등급을 소프트웨어에 부과할 지를 결정하고 있다. 결과적으로 표 1과 같이 계통의 안전중요도 및 소프트웨어 고장유형을 두 인자로 하여 Software Integrity Level(1-4)을 부과하고 있다.

표 1. Software Category as a Function of Safety Significance and Impact Type

Plant System Safety Significance	Software Failure Impact Type		
	Type I	Type II	Type III
High	1	2	4
Medium	2	3	4
Low	3	3	4

위에서 살펴본 바와 같이 소프트웨어 분류 방법들은 각각의 기술적 근거를 배경으로 제안되었기 때문에 어느 한 기준을 일반화하기는 어렵다. 위에서 언급된 분류 기준의 개별적 항목을 차세대 원전 디지털 계측제어계통에 대비하여 문제점을 분석하고 최종적으로는 차세대 원전 디지털 계측제어계통에 적절한 소프트웨어 분류기준을 제안하고자 한다.

2.1 계통분류(System Classification)

계통의 안전등급분류는 먼저 Plant Licensing Basis(Regulatory Basis) 및 대상원전의 DBE(Design Basis Event)에서 출발하여 Plant-level Function, 계통 및 부품에까지 이르게 된다. 안전등급은 기본적으로는 안전에 중요한 기능을 기반으로 안전관련(Safety-related: SR)과 비안전관련(Non-safety-related: NSR)으로 분류된다. 안전관련(Safety-related) 구조물, 계통, 혹은 부품은 10 CFR 21.3, 10 CFR 50.49 및 10 CFR 100 Appendix A에 정의되어 있다 [등급분류에 대한 일반적 사항은 EPRI NP-6895 참조].

현재 과기처 고시는 ANSI/ANS 51.1을 준용하고 있으며 안전관련기능의 중요성에 따라 Safety Class 1, 2 및 3로 분류하고 있다. 이후에 발행된 ANSI/ANS 58.14에서는 Safety Classification외에 Pressure Integrity Classification을 추가하고 있다. 국내에서는 과기처 고시 제 94-10호 "원자로 시설의 안전등급과 등급별 규격에 관한 규정"에서 안전기능에 따라 원자로 시설 및 설비에 대하여 안전등급 1, 2, 3 및 비안전등급으로 분류하고 계측제어계통은 안전등급 3으로 분류하였다. 그후 차세대원전 규제요건에서는 IAEA 안전등급분류를 기초로 계측제어계통을 안전성계통 및 비안전성계통으로 분류하였으나 정성적 기능 기반으로 분류하였다.

IEC-1226에서는 FSEs(Functions, Systems, and Equipments)의 안전 중요도에 따라 Category A, B, C 및 안전에 중요하지 않은 등급등 4등급으로 분류하고 있다. 이 방식은 IAEA 기준 하에서 안전 및 안전 관련(safety or safety-related) 의 이분법적인 방식을 탈피하여 안전 중요도를 기준하여 다단계적으로 분류한 방식이다. 그러나 동 보고서에서의 분류 기준 역시 안전을 유지하는 데 주 역할(Primary Role), 보조적인 역할(Complementary Role) 간접적인 역할(Indirect Role)을 수행하는 FSE 등 정성적인 기준을 제시하고 있다.

IEC-1226 분류방식은 기능기반(혹은 분류에서는 대상계통이 담당한 안전과 관련된 기능적 측면만을 고려하여 그 계통의 고장으로 인한 결과의 심각성을 분류기준으로 한다. 따라서 계통의 고

장확률을 정량적으로 고려한 Risk Ranking을 기초로 한 분류라고 할 수는 없기 때문에 결정론적(Deterministic) 분류 방식이라 할 수 있다. 이러한 결정론적인 분류 방식은 첫째, 어떤 계통의 기능적인 면만을 고려하기 때문에 계통고장이 안전 미치는 영향을 정확히 가름할 수 없다. NRC가 SECY-91-292에서 언급하였듯이 운전경험자료, 즉 사건들 중에는 비안전계통의 고장으로 인해 원전 설비의 Defense-In-Depth에 손상을 주는 경우가 많이 있다는 것이 그 실례가 된다. 둘째, 안전등급에 속한 기기/계통이라 할 지라도 그 기능에 따라서는 상대적 중요도가 존재하는데 그것과는 상관없이 모든 기기/계통이 안전에 관련한 기준을 적용함으로써 불필요한 개발비용이 증가할 가능성이 있다는 점이다. 살펴본 바와 같이 다단계 안전등급분류를 시도하였어도 결국 '안전에 중요한' 계통에 대해서는 일반적으로 Class 1E의 규정에 지배되는 경향이 있어 요건들의 차별적 적용이 뚜렷하지 않다.

반면에 IAEA 50-SG-D8에서는 발전소 기기를 안전중요도에 따라 2가지 범주로, 즉 Items Important to Safety 와 Items Not Important to Safety로 분류하고 있으나(Items Important to Safety는 위에서 분류한 안전관련에 해당된다. Safety-Related 계측제어 계통의 안전 중요도 평가를 위한 6가지 기준을 권고하고 있으며 이 기준들은 위험도 기반(Risk-Based)의 디지털 계측제어 계통분류 기준의 근거를 제시하고 있다(IAEA 보고서의 Safety-Related System은 Items Important to Safety 중 Safety System을 제외한 기기를 말함. 따라서 2.1절의 서두에서 언급한 Safety-Related와 구별됨). 다만, 평가를 위해서는 디지털 계통의 고장확률 추정이 필요하지만 현재까지 이에 대한 일반적 방법론이 부재한 상태이다.

이와 같이 결정론적 분류 방식에서 탈피하기 위해서는 디지털 계통의 고장 확률 추정이 필수적임을 알 수 있다. 디지털 계통의 고장확률 추정의 필요성은 NRC(Nuclear Research Council) Study에서도 강조된 사항이다[Nuclear Research Counsil, 1997] 즉, 새로운 설계개념으로 인한 Component Control 개념 변화, 디지털 기기의 채용으로 인한 유지/보수 전략 변화, 그리고 Cost-effective 분석의 기반으로서 PRA(Probabilistic Risk Assessment) 방법등을 사용하여 디지털 I&C 계통의 고장이 전체 System에 미치는 상대적 영향정도를 결정할 필요가 있는 것으로 권고하고 있다.

IAEA 보고서등에서 정의하는 '안전'은 인간 및 환경에 피해를 주는 예상하지 않은 방사선누출을 초래하는 사건의 발생을 방지할 수 있는 정도를 의미하며 계측제어 계통의 고장이 안전에 미치는 심각성도 이 안전개념 기준으로 평가된다. 그러나 이와 더불어 고려해야할 사항은 Plant Availability이다. 예상 초기 사건에 대해서 적절한 방어가 수행된다 하더라도, 예를 들면 원자로 정지가 성공적으로 수행되고 Post Trip Activity가 적절히 수행되어도 Plant Availability 측면에서는 바람직하지 않다. 즉 원전 불시정지(Forced Outage)는 안전에 영향을 미치지 않는다 하더라도 Plant Availability의 가장 심각한 장애가 된다. 계측제어의 입장에서는 어떤 계통의 고장으로 인한 Plant Availability 손실을 고려해야 한다. 자료에 의하면 1978년부터 1996년까지 국내 원전의 발전정지 사례중 계측제어설비의 고장으로 인한 불시 정지가 상당한 부분(24.6%)을 차지하고 있는 것을 알 수 있다[원자력 발전 연보, 1996].

원자로 불시정지와 같은 최악의 Plant Availability 손실 이외에도 출력 감발의 경우도 한 예가 될 수 있다. 예를 들면, 정보처리계통(Information Processing System: IPS)의 경우 핵비등이탈비(Departure from Nuclear Boiling Ratio: DNBR) 와 국부출력 밀도(Local Power Density: LPD)의 Margin을 계산하기 위해 노심운전 제한치감시계통(Core Operating Limit Supervisory System: COLSS) program을 실행하는데, 만약 COLSS Program이 고장났을 경우 Technical Specification은 운전제한치(Operating Limit)의 Margin의 감시(Surveillance)를 CPC Data를 이용하여 수동으로 수행하도록 요구하고 있다. 이때, 충분한 Margin을 유지하기 위해 원자로 출력을 감발할 필요가 있다. 이와 같이 비안전 감시계통도 보호계통 보다는 덜 심각하지만 Plant Availability의 손실을 초래할 수 있어 이러한 요소를 소프트웨어의 분류시 고려할 필요가 있다.

K-URD(Korean Utility Requirements Document) 10장의 3.5.2.1절에서는 설계목표에 대한 정량적인 기준의 하나로서 MMIS 기기의 고장으로 인한 불시정지의 빈도를 50 Reactor Year동안 1번 이하로 규정하고 있고, 3.5.2.2절에서는 Plant Availability 감소를 초래할 수 있는 M-MIS 기기의 MTBF(Mean Time Between Failure)가 5년 이상이 되도록 규정하고 있다. 이 정량적인 수치들을 MMIS 계통설계에 직접 반영하기에는 몇 가지 어려움이 있지만(특히 디지털 계측제어계통의 정량적 신뢰성분석을 위한 효과적 방법 부재와 특히 소프트웨어 신뢰성을 정량적 추정방법 부재가 주 어려움이다) 계통고장으로 인한 원자로 정지 빈도(Trip Frequency)한계의 설정을 통해 MMIS 설계의 신뢰성을 평가할 수 있는 기준이 되고 있다.

이러한 의미에서 AECL 의 분류방식은 바람직한 분류 방식이라 할 수 있다. 그러나 이를 적용하기 위해서는 계통의 Unavailability Requirement 또는 Initiating Event Frequency Limit 가 선행되어야 하기 때문에 현 차세대 원전 설계요건에서 이와 같은 정량적 기준을 도출하는 것이 어려운 실정이다. 일견으로는, Utility가 자체 분석을 통하여 제한치를 설정하고 이를 기준으로 설계를 수행하고 그 결과에 대한 근거를 Utility에서 제시하고 인허가 기관에서 이를 인정하는 절차를 마련하는 것도 한 방법이 될 수 있다. 이는 Risk-Informed 기반 인허가 규제 추세에 대비할 수 있는 근거도 될 수 있다.

2.2 다양성 인자

EPRI 보고서에서는 한 계통의 다양성 수단이 마련되어있으면 두 계통의 Software의 Integrity Level을 하향 조절하도록 제안하고 있다. 이때 두 계통은 같은 안전등급일 경우 적용할 필요가 있지만 한 계통이 낮은 안전등급으로 분류된 경우에는 적용할 수 없다. 예를 들면, 차세대 원전의 경우 보호계통에 대해서는 다양성 설비인 DPS(Diverse Protection System)가 마련되었지만 DPS는 비안전 등급으로 분류되어 있고 그 기능도 보호계통의 일부 기능만 수행하기 때문에 EPRI에서 제안한 다양성 인자를 고려하기는 부적절하다. 다시 말하면, 다양성인자를 적용하기 위해서는 두 계통이 기능적으로 동일하다는 판단근거 마련이 선행되어야 한다.

2.3 복잡성 인자

적용되는 계통의 기능적 복잡성은 소프트웨어 등급분류의 중요한 요소로서 소프트웨어의 개발 및 검증/확인 분야 등에서 강조되고 있는 사항 중의 하나이다. 이것은 소프트웨어가 복잡할수록 개발 및 분석이 어려워지고 오류가 연루될 가능성이 커지므로 확인 및 검증활동의 필요가 증대되며 철저하게 수행하여야 한다는 관점이다[Leveson, 1995]. 심지어는 소프트웨어의 복잡성이 고장확률과 비례한다는 관점에서 고장확률 대신에 복잡성의 정도를 이용하여 Risk를 평가하는 경우도 있다[EPRI TR-102106, 1993]. EPRI TR-103291 Vol 3에서는 기능적 복잡성(Functional Complexity)만 고려하고 설계 및 구현의 복잡성(Design/Implementation Complexity)은 Adjusting Factor와 분리하여 고려할 것을 제안하고 있는데 반하여, EPRI TR-103916(1995)에서는 신뢰성 및 요건을 만족하는 계통의 등급별 확인 및 검증의 깊이(Depth)를 결정하는 중요 인자로 System Complexity를 사용하고 있다. 다만, 각 인자들에 대해서 High, Medium, Low 중 하나로 평가된 결과를 기초로 평균적 Complexity Level을 결정하는 방법이 결여되어 있다. [계통의 Complexity를 평가할 수 있는 여러 6개 Factor 들의 정의는 동보고서 참조] 원전 계측제어 계통을 EPRI TR-103916(1995)의 기준을 기초로 복잡성을 분석할 때, 각 계통들은 안전기능의 중요도와는 상관없이 비슷한 정도로 나타나고 있어, 차세대 원전 계측제어계통에서는 SIL에 영향을 주는 중요한 인자로 채택하기가 어렵다.

2.4 소프트웨어 고장 유형(Software Failure Impact Type) 인자

소프트웨어 고장 유형평가의 핵심은 소프트웨어 고장모드 및 영향평가이다. EPRI TR-103291 Vol. 3에서는 Adjusting Factor의 한 인자로서 Software failure Consequence 분석 결과에 따라 SIL을 조정하도록 제안하고 있는 반면에, AECL 기준에서는 Special Safety Systems & Mitigating Systems 및 Process System, 그리고 Monitoring/Test System에 대해 Type I, II, III로 분류할 수 있는 기준을 명시하고 있다.

근본적으로, 두 분류 기준은 소프트웨어 고장이 안전기능에 미치는 영향이 적을수록 SIL이 낮아지도록 한 점에서는 공통적이지만 EPRI의 기준을 적용할 때 바람직하지 않은 측면도 있다. 예를 들면, 만약 소프트웨어오류가 발생할 때 실패-안전(Fail-Safe)과 같은 내고장성 설계 개념이 적용되었을 경우 안전에 미치는 영향만을 고려하면 SIL을 하향조절할 수도 있지만 안전에 중요한 계통이 높은 신뢰성을 갖고 정상적으로 기능을 수행하도록 높은(숫자로는 낮은) SIL로 설계하는 것이 내고장성보다 우선되어야하기 때문에 하향조절 기준으로서 부적절하다. 다시 말하면, SIL 평가는 높은 안전등급의 계통에 대해서는 높은 SIL을 부여하여 요구되는 기능을 보장하는 것이 주목적이기 때문이다. 또한 앞에서 언급하였듯이, 높은 안전등급의 소프트웨어의 고장시 완화계통으로 인해 안전성은 보장된다 하더라도 Plant Availability에 손상을 주는 것은 바람직하지 않다. 대신에 기능적으로는 안전 기능과 관련이 적어 소프트웨어의 고장이 주 계통의 안전 기능 수행에 영향을 미치지 않을 경우 SIL을 하향하는 것이 적당하다. 또한 소프트웨어가 새로운 고장모드 위험성이 있으면 SIL을 상향 조절하도록 제시하고 있는데 이는 소프트웨어 고장예측이 어려운 것을 감안하면 판단하기 어려운 기준이다.

일반적으로, 디지털 계측제어계통은 아날로그 계통보다는 자료전송 네트워크를 공유하거나 제어기기를 공유하는 경향이 크기 때문에 한 계통의 고장이 여러 계통의 고장으로 파급되는 위험(공통 모드 고장)에 대한 우려가 크며, 사실상 소프트웨어 개발 요건은 이러한 가능성을 최소화하는 것이 주목표라고 할 수 있을 정도이기 때문에 위에서 언급한 고장 영향 결과에 대한 적절한 평가는 매우 중요한 분류 작업이다. 이와 같이, 두 분류기준에서 살펴보았듯이 낮은 SIL의 소프트웨어는 어떤 방식으로든 높은 SIL의 소프트웨어의 실행을 방해하지 않아야 된다.

3. 차세대 원전 계측제어 계통 소프트웨어 분류 기준

지금까지 논의한 사항들을 정리하면 Software Integrity Level을 평가하기 위한 적절한 절차는 첫째, 위험도(Risk) 평가이다. 즉, 계통의 고장 확률 및 그 고장이 안전에 미치는 영향 정도를 평가하여 계통의 안전 중요도를 Risk Ranking에 따라 분류하는 방법이다. 이를 위해서는 정량적 신뢰성(Reliability) 및 고장영향(Failure Effect) 분석이 가능해야 한다. 둘째는, Plant Availability를 고려하여야 한다. 즉, 소프트웨어의 고장으로 인한 위험도 평가와 더불어 소프트웨어의 고장으로 인한 Plant Availability 손실 평가가 수반되어야 한다. Utility 자체가 Unavailability Requirement를 마련하는 것도 한 방법이 될 수 있다. 또한 Technical Specification을 근거로 Plant Availability에 대한 간접적인 평가도 한 방법이 될 수도 있다.

그러나, 현재로서는 위험도(Risk)를 정량적으로 분석할 수 있는 기반이 미비하고 설혹 그것이 가능하더라도 인허가 요건이 그러한 기준을 수용할 수 있는 여지를 마련하여야 할 것이다. 더욱이 Plant Availability를 기준으로 한 분류기반도 미비하여 정량적 기준 마련이 어렵다.

따라서 이상과 같은 제한적 상황 때문에, 계통분류를 먼저 국내 규제 요건에서 정의하는 기능 기반의 안전등급 분류에 준하고 이어서 각 계통의 소프트웨어들에 대해서 SIL을 부여하되 소프트웨어가 안전기능에 미치는 영향정도와 Plant Availability를 부분적으로 반영한 분류 방식으로 귀결된다.

SIL에 영향을 주는 여러 가지 인자들의 타당성 및 적용성을 디지털 계측제어계통에 비추어 분석한 결과, 소프트웨어가 안전기능에 미치는 영향정도가 SIL 결정의 가장 주요한 인자임을 알 수 있다. 내용적으로는 소프트웨어의 기능 및 소프트웨어의 독립성 여부가 그 영향정도의 중요한 판단 기준이 될 수 있다. 다양성 인자 및 복잡성 인자 그리고 내고장성 등과 같은 고장완화수단 인자들도 경우에 따라서는 고려의 대상이 될 수 있지만 근본적인 SIL 평가 기준으로는 불완전함을 알 수 있다. 이외에도 다른 인자들을 고려할 수 있지만, 본 분류기준에서는 Plant Availability를 추가로 고려하였다.

표 2는 본 보고서에서 제안한 2단계의 분류기준을 보여준다. 먼저, 가로축을 차세대원전 계측제어계통의 안전등급분류를 기준으로 하고 세로축을 각 계통에 속한 소프트웨어 고장이 안전기능에 미치는 영향정도에 따라 Type I, II, III로 설정하고 SIL을 부여하였다. 이 Type의 분류기준에 Plant Availability를 반영하였는데 구체적인 분류 기준은 다음과 같다.

Type I:
계통 고유의 기능을 직접적으로 수행 하는 소프트웨어로 계통 고유의 논리 및 연산을 담당하여 그 소프트웨어의 고장이 계통의 고유 안전기능의 완전한 상실을 초래하거나 즉각적인 원자로 정지(Shutdown) 또는 원자로 불시 정지(Trip)가 요구되는 소프트웨어

Type II:
Type I의 소프트웨어를 직접적으로 혹은 간접적으로 보조하는 소프트웨어로 Type I의 소프트웨어의 기능 수행에 필요한 정보를 교환하거나 자료를 처리하는 소프트웨어. 그러나 그 소프트웨어의 고장이 계통의 고유 안전기능의 상실에 영향을 주지 않고 다만 일정한 시간이후에 운전절차에 따라 원자로 출력감발이 요구되는 소프트웨어

Type III:
소프트웨어의 고장이 Type I 또는 Type II 소프트웨어의 실행에 영향을 주지 않으며 수동 혹은 자동 원자로 불시 정지 및 출력감발이 요구되지 않는 소프트웨어

표 2. 차세대 원전 계측제어계통 Software Integrity Level 분류

소프트웨어 고장영향 유형	안전성계측제어 계통		비안전성 계측제어 계통	
	보호계통	안전관련계통	다양성계통	비안전관련계통
Type I	1	2	3	4
Type II	1	2	3	4
Type III	2	3	4	4

2단계 분류의 결과로 생긴 4x3의 공란(Slot)에 SIL을 부여한 방법은 다음과 같다. 먼저, 보호계통, 안전관련 및 비안전성 계측제어 계통의 SIL을 각각 1, 2, 3으로 하고 비안전성 계측제어계통의 다양성계통의 Type II는 안전기능의 정도가 높은 것을 고려하여 상향 조절하였다(4에서 3으로). (비)안전성 계측제어계통에서 Type II에 대해 SIL을 Type I과 동일하게 부여하고 III에 대해 SIL을 Type II보다 한 단계씩 하향하되 SIL이 5이상 되는 것을 피하였다.

Type II 소프트웨어가 비록 계통의 안전기능에는 영향을 주지 않지만 Plant Availability의 중요성을 강조하기 위해 Type I의 SIL을 유지하였다. Type II 소프트웨어의 부동작시(예를 들면, 특별한 이유없이 "Halt" 되는 경우) 대게 재기동(Reboot) 등의 방법으로 정상상태로 회복할 수 있다. 그러나 아직도 몇 몇의 경우는 해결책이 없어 "Random Event" 성격의 부동작이 목격된다[Tang, 1992]. 이 경우 정상상태 회복을 위한 조치 중에 인적오류 발생 가능성이 크고, 또한 만약 소프트웨어의 설계오류인 경우 대게 주어진 시간 내에 보수가 불가능할 것으로 예측되기 때문에 개발단계에서 철저하게 관리하는 것이 개발비용이 다소 증가하더라도 Plant Availability를 고려할 때 더 효과적일 수 있다.

4. 결론 및 향후 방향

현재의 원전 사업자는 디지털 계통의 타당성을 인정하는 반면 디지털 계통의 소프트웨어의 위험성을 불식하고 요건에 충족한 소프트웨어의 개발을 위한 경제적 부담을 최소화하여야 하는 입장에 있다. 이러한 상황에서 계측제어계통의 소프트웨어 분류기준 개발은 경제적(Cost-effective) 소프트웨어 개발, 특히 효율적인 확인 및 검증을 위한 방법론 수립에 일조할 수 있다.

본 논문에서는 차세대 원전 계측제어계통의 소프트웨어 분류기준을 도출하기 위해 기존에 제안된 몇 몇 기준들을 분석하고 관련 지침서 및 보고서 그리고 인허가 요건등을 통하여 적용성 여부를 분석하였다. 계측제어계통의 결정론적 소프트웨어의 분류기준을 탈피하고 위험도 기반 혹은 정량적 기준에 근거한 분류기준을 마련하는 것은 현시점에서는 어려운 것으로 판단된다. 다만 소프트웨어의 상대적 안전중요도와 Plant Availability를 고려한 분류기준을 제시하였다.

본 보고서에서 제안한 분류기준을 다른 기준들과 비교할 때 Plant Availability를 강조하여 계통의 본래 기능을 수행하는 소프트웨어와 동일하게 취급하고 있다. 이는 개발 단계에서는 비용의 증가를 가져올 수 있으나 원자로 출력 감소로 인한 손실과 비교할 때 바람직한 방향으로 판단된다. 소프트웨어의 특성상 설계오류인 경우 개발자만이 보수할 수 있는 제한성 때문에 운전절차서상의 일정시간 내에 정상상태로 회복하기가 불가능할 것으로 예측된다. 이 경우 막대한 운영상의 손실을 초래할 수 있기 때문에 이를 방지하기 위한 노력이 개발 초기부터 이루어져야 한다.

SIL 평가기준은 정량적 평가에 근거하기보다는 정성적으로 설정하였다. 근본적으로는 현재 국내 가압경수로(PWR)에 대해서는 정량적 기준을 적용할 수 있는 근거가 미약하고 안전기능의 중요성에 따라 계통이 분류되어 있어서 그 제한성을 초월할 수 없다. 따라서 해석의 차이가 발생할 수 있는 여지가 있고 계통분류가 Risk Ranking을 완벽하게 반영하지는 않더라도 High Consequence에 대한 분석을 적절하게 수행하여 SIL을 부여할 수 있으면 본래의 Risk의 의미를 근사적이나마 비례적으로 반영할 것으로 판단된다.

본 소프트웨어의 분류의 목적이 소프트웨어의 수명주기 활동의 수행정도를 차별화하고 특히 검증/확인 절차의 효율적 적용을 위한 기준마련에 있는 만큼 차별적 SIL을 결정한다 하더라도 그 계통의 신뢰성 혹은 운영성을 유지하는 것이 중요하다. 이를 위해서는 SIL과 일관된 소프트웨어 개발 절차를 확립하는 것이 더욱 중요하다.

보다 기술적으로 합리적인 분류를 위해서는 디지털 계통의 고장모드 및 영향분석 그리고 정량적 신뢰성 분석이 선행된 심층적 Risk Analysis 와 Technical Specification분석을 통한 Plant Availability 분석, 나아가 Cost-benefit Analysis를 포함한 다각적인 분석이 필요하다. 이는 인허가 기관보다는 Utility 자체에서 IAEA의 권고대로 위험도 기반 과 운영성 및 보수성을 고려한 보다 정량적인 기준을 마련하는 것이 소프트웨어 개발분야 뿐 만 아니라 디지털 계통의 신뢰성을 향상시키고 Risk-Informed Based Regulation 추세에 대응하고 나아가서는 원자력 발전소의 국제적 경쟁력을 향상시키는 데도 필요한 작업이다.

참고문헌

[1]윤원영, "원전 디지털 계측제어계통의 개발현황 및 규제동향, 원전디지털 계측제어계통 규제기술동향 분석세미나," pp. 1-17, 한국전력공사, 1997.

[2]"원자력 발전 연보," 한국 전력 공사, 1996.

[3]"차세대원자로 상세안전요건", 원자력안전기술원, 개정중.

[4]ANSI/ANS 51.1, "American National Standard Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," 1983

[5]ANSI/ANS 58.14, "Safety and Pressure Integrity Classification Criteria for Light Water Reactors," 1993

[6]G. Archinoff, D. Lau, J. Grosbois, and W. Bowman, "Guideline for Categorization of Software in Nuclear Power Plant Safety, Control, Monitoring and Testing Systems," Rev. 1.0, COG-95-264, AECL, 1995.

[7]Nuclear Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues," National Academy Press, Washington, 1997.

[8]EPRI NP-6895, "Guidelines for the Safety Classification of Systems, Components, and Parts Used in Nuclear Power Plant Applications(NCIG-17)," 1991.

[9]EPRI TR-102106, "Survey and Assessment of Conventional Software Verification and Validation Techniques," 1993.

[10]EPRI TR-103291, "Handbook for Verification and Validation of Digital Systems," Vol. 3, Topical Reviews, 1994.

[11]EPRI TR-103916, "Verification and Validation Guidelines for High Integrity Systems," Vol. 1, Main Report, 1995.

[12]IAEA 50-SG-D8, "Safety-Related Instrumentation and Control Systems for Nuclear Power Plants," 1984.

[13]IEC 1226, "Classification of Instrumentation and Control Systems Important to Safety of Nuclear Power Plants," 1993.

[14]K-URD, Korean Utility Requirements Document

[15]R. Kunzig, "Europe's Dream," Discover, pp. 96-103, May 1997.

[16]N. Leveson, "Safeware: System Safety and Computers," Addison Wesley, 1995.

[17]NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design," Vol. 1, pp. 7-4, U. S. NRC, 1994.

[18]NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants"

[19]SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors"

[20]D. Tang, "Analysis and Modelling of Correlated Failures in Multicomputer Systems," IEEE Transactions on Computers, Vol. 41, No. 5, 1992.