KAERI/TR-2668/2004

안전소프트웨어의 정량 V&V 방안 연구

A Study on Quantitative V&V of Safety-Critical Software

한 국 원 자 력 연 구 소

제 출 문

한국원자력연구소장 귀하

본 보고서를 2003 연도 “정지/저출력 및 디지털 계통의 위험도 평가기술 개발” 과제의 기술보고서로 제출합니다.

2004. 3.

부서명 : 종합안전평부

주 저 자 : 엄흥섭

공 저 자 : 손한성

강현국

장승철

하재주

요 약 문

최근 원자력발전소의 안전을 평가하는 중요한 수단 중의 하나인 확률론적 안전성 평가(Probabilistic Safety Assessment: PSA)에 사용하기 위하여 소프트웨어 신뢰도의 정량적인 정보에 대한 실용적인 요구가 생겨나고 있다. 그러나 기존의 소프트웨어 신뢰도 정량평가 방법들은 PSA가 요구하는 충분한 정보를 제공할 수 없기 때문에 현재는 디지털 시스템을 포함하는 PSA의 경우 소프트웨어 부분을 배제하거나 또는 임의의 값을 사용하고 있는 실정이다. 본 보고서에서는 최근 불확실성을 포함하는 시스템의 모델링에 많이 활용되고 있는 Bayesian Belief Networks 기법을 이용하여 규칙 기반의 정성적인 소프트웨어 평가 방법론을 Bayesian Belief Networks로 모델링하고 PSA가 요구하는 정보를 생산할 수 있는 기본체제 연구와 사례연구에 대하여 기술하였다.

제안된 기본 체제는 안전 소프트웨어의 신뢰도에 관계된 정성적인 증거와 정량적인 증거 모두를 결합하여 정형적이고 정량적인 방법으로 결론을 추론할 수 있는BBN의 특성을 활용하여 구축되었다. 그리고 사례연구로서 연구된 방법론을 원자로 보호 계통에 탑재될 안전 소프트웨어 요구명세서의 품질을 평가하는 데 적용하였는데, 전문가에 의해 수행된 확인 및 검증 결과들이 모델의 입력으로 사용되었다. 만들어진 BBN 모델의 결과와 분석 내용은 전문가의 정성적인 판단과 유사하게 나타났으며 분석 내용들은 추후의 V&V 활동에 대한 의사 결정에 활용될 예정이다.

SUMMARY

Recently practical needs have required quantitative features for the software reliability for Probabilistic Safety Assessment (PSA) which is one of the important methods being used in assessing the overall safety of nuclear power plant (NPP). But the conventional assessment methods of software reliability could not provide enough information for PSA of NPP, therefore current assessments of a digital system which includes safety-critical software usually exclude the software part or use arbitrary values. This paper describes a Bayesian Belief Networks (BBN) based method that models the rule-based qualitative software assessment method for a practical use and can produce quantitative results for PSA.

The framework was constructed by utilizing BBN that can combine the qualitative and quantitative evidence relevant to the reliability of safety-critical software and can infer a conclusion in a formal and a quantitative way such as human experts' do. The case study was performed by applying the method for assessing the quality of software requirement specification of safety-critical software that will be embedded in reactor protection system. The V&V results were used as inputs for the model. The calculation results of the BBN model showed that its conclusion is mostly equivalent to those of the V&V expert for a given input data set, and it will also support the V&V expert's decision making process in controlling further V&V activities.

목 차

<표 차례>

<그림 차례>

제1 장. 서론

바람직하지 못한 위험을 회피하거나 통제하려는 노력에도 불구하고 원전의 디지털 계측제어 기기와 같은 새로운 기술을 사용함에 따라 관리하기에 어려운 새로운 위험이 나타나고 있다. 지금까지 새로운 위험문제가 생길 때마다 이런 위험들을 감소시키는 효과적인 방법을 발견하거나 이를 위해 한정된 자원을 할당하는 노력이 이루어져 왔는데, 현재 중요한 문제들 중의 하나는 디지털 안전 계통에 사용되는 안전 중요 소프트웨어의 신뢰도 분석이다. 그런데 원전 안전 시스템에 사용되는 소프트웨어의 신뢰도 평가는 고장의 원인이 설계 결함에 주로 기인하고 또 입력에 대해 비선형적 출력을 가지는 소프트웨어의 특성으로 인하여 시험이나 신뢰도 성장모델과 같은 기존의 정량적 방법으로는 불충분하다는 것이 현재의 정설이다[1][2]. 이에 따라 각종 국제 표준이나 각 국의 원자력 규제 기관들은 소프트웨어의 신뢰도에 관계되는 모든 활동과 자료들을 종합적으로 판단하여 신뢰도를 평가하는 규칙 기반의 정성적 평가에 의존하고 있는데[3][4][5], 최근에 디지털 시스템이 원전의 안전계통에 사용되고 이에 따라 확률론적 안전성 평가(Probabilistic Safety Assessment, PSA)와 같이 소프트웨어의 신뢰도를 정량적으로 평가해야 하는 현실적 필요성이 대두되고 있다.

본 연구의 최종적인 목표는 PSA에 사용할 수 있는 안전 소프트웨어의 정밀한 신뢰도 정보를 획득하는 체계적인 체제를 개발하는 것이다. 이 목표를 달성하고 또 안전 소프트웨어의 신뢰도 정량평가에 내재된 문제들을 해결하기 위하여 BBN 기술을 이용한 방법론을 연구하였다 이 방법은 안전 소프트웨어의 신뢰도 평가에 필요한 정량적인 증거와 정성적인 증거 모두를 종합할 수 있고 이들 증거를 근거로 엄밀한 수학적 논리를 통하여 합리적인 결론을 추론할 수 있는 장점이 있다. 그리고 연구된 방법론의 실용적 가능성을 결정하기 위하여 사례연구를 수행하였다.

제2 장. BBN과 소프트웨어 신뢰도 정량평가 기본체제

제1 절. BBN 방법론

1990년대 초 Bayesian Belief Networks(또는 BBN, Belief Networks, Bayesian Networks, Causal Probabilistic Networks, 등)는 학계 뿐 아니라 산업계에서도 많은 주목을 받았다. BBN의 이론적인 개발은 1970년대로 거슬러가지만 그 당시에는 효과적인 알고리즘의 결여와 도구가 없었던 관계로 실용적인 적용은 어려운 실정이었다. 그러나 효과적인 도구가 많이 만들어진 요즈음에는 BBN은 의료, 군사, 금융, 안전과 신뢰도 평가와 같은 많은 분야에서 활용되는 기술로 되어가고 있다.

Bayesian Belief Networks(BBN)는 대상 시스템의 관련된 변수들을 인과관계에 의해 모델링하고 변수들 간의 종속성 정도를 조건부 확률로 나타낸 다음 관찰된 여러 가지의 증거를 만들어진 BBN 모델에 입력한 후 베이스(Bayes) 확률 정리를 비롯한 확률 법칙을 적용하여 계산하고 정량적 결과를 이끌어 내는 방법론이다.

BBN은 그래프 상에서 원으로 표시되는 노드(Node)와 노드들 사이를 연결하는 연결선(arcs 또는 directed edges) 그리고 각 노드에 속한 확률 테이블(Node Probability Tables: NPT 또는 Conditional Probability Table: CPT)로 구성되어 있다. 노드는 모델에 포함된 변수들을 나타내며 노드 연결선은 노드간의 인과관계를 나타낸다. 각 노드는 무작위 변수로서 몇 개의 상태를 가지고 있으며(예: "Yes"와 "No"의 상태) 각 상태의 확률 값의 합은 1이 된다. 각 노드에 연결된 노드 확률 테이블은 노드간의 연결 강도를 결정하며 모 노드(parent node)의 각 상태에 대한 조건부 확률로 표현된다.

BBN의 구성은 다음과 같다[6].

○ A set of variables and a set of directed edges (arcs) between variables

○ Each variable has a finite set of mutually exclusive states

○ The variables together with the directed edges form a directed acyclic graph(DAC). A DAC is acyclic if there is no directed path A1 -> An such that A1 = An

○ To each variable A with parents B1 Bn there is attached a conditional probability table P(A|B1Bn).

BBN 상의 노드들은 목표노드(target node), 관찰가능 노드(observable node) 그리고 중간 노드(intermediate node)로 구분할 수 있다[7].

○ 목표 노드는 모델에서 평가 목적에 해당하는 노드로서 "프로그램의 무결함" 등이 될 수 있다.

○ 관찰가능 노드는 직접 관찰 가능한 노드로서 "N 번 테스트 중 M번 실패" 또는 "ISO 9000 품질요건 만족" 등이 될 수 있다. 이들 관찰가능 노드들은 정량화 된 수치이거나 또는 측정 가능해야 하는데 이 측정은 판단에 의한 주관적 확률 값도 가능하다.

○ 중간 노드는 제한된 정보나 믿음(belief)을 나타내는 것으로 "개발 과정의 품질" 또는 "제작자의 명성" 등이 여기에 해당된다.

BBN의 모델링 순서는 다음과 같다

1 단계: 노드(변수) 확인 (in a target system)

2 단계: 그래프 작성

3 단계: 노드 확률 테이블(NPT) 작성

4 단계: 증거 확보(명세서 평가 결과, 시험 결과, V&V 결과 등)

5 단계: 계산 및 분석(추론)

BBN을 안전소프트웨어 신뢰도의 정량적 평가에 사용하는 근거는 다음과 같다[8][9].

○ 안전 소프트웨어의 신뢰도/안전성 평가와 같이 필연적으로 불확실성을 내포하고 또 의사결정을 위한 충분한 증거를 얻는 것이 현실적으로 불가능한 문제의 해결에 적합한 것으로 나타남.

○ 현재, 이와 같은 문제에 대한 해결은 전문가가 다양한 형태(정성적 형태 및 정량적 형태)의 관련 증거들을 근거로 하여 정성적으로 판단을 하는 것이 유일한 방안으로 되어있는데, BBN은 이들 다양한 형태의 증거들을 정형적으로 결합하고 평가 시 수반되는 불확실성들을 명시적으로 도입하여 그 결과를 정량화 하는 방안을 제시할 수 있다는 점이 가장 큰 가능성.

○ 또 실제로 전문가에 의하여 평가 시 사용되고 있으나 기존의 정량적 평가 기법들로는 구현하기 어려운 내용들, 예를 들면 측정할 수 없는 신뢰도 관련 특성들(개발팀의 품질 등급 등)에 대한 정성적 평가를 일관된 평가 프레임 안에서 정량적 평가에 도입할 수 있다는 점도 타 방법론에 비하여 장점으로 나타남.

○ 이 외에도:

(i) 복잡하고 애매함이 함축된 평가 내용들이 BBN의 그래프와 NPT를 통하여 명시적이고 이해하기 쉽게 나타나므로 평가 전문가들이나 관련 전문가(개발팀, 시험 팀)들 사이의 의사소통과 토론이 용이하게 되고,

(ii) 기존의 소프트웨어 공학에서 사용되는 각종 메트릭스 또는 확인 및 검증 결과나 시험 결과를 활용하여 모델링 할 수 있어 새로운 측정 방법을 추가로 개발할 필요가 없으며,

(iii) 결여된 자료가 있어도 결과 값을 구할 수 있어 개발 초기단계부터 사용이 가능

(iv) 모델에 사용된 각 변수들이 상황에 따라 어떻게 변화하는지 쉽게 알 수 있어 신뢰도에 중요한 영향을 주는 변수들을 확인할 수 있다는 점과,

(v) 복잡한 확률 계산을 용이하게 해주는 도구들이 있다.

제2절. 안전소프트웨어 신뢰도 정량평가 기본 모델

원자력발전소의 안전을 평가하는 중요한 수단 중의 하나인 확률론적 안전성 평가(PSA)에 사용하기 위하여 소프트웨어 신뢰도의 정량적인 정보에 대한 실용적인 요구가 생겨나고 있다. 그러나 기존의 소프트웨어 신뢰도 정량평가 방법들은 PSA가 요구하는 충분한 정보를 제공할 수 없는 실정이다. 이런 문제를 해결하기 위하여 정성적인 증거와 정량적인 증거를 함께 결합할 수 있고 이들을 근거로 정형적이며 정량적인 방법으로 결론을 추론하는 방안을 BBN을 이용하여 연구하였다.

그림 1은 안전 소프트웨어의 정량적인 신뢰도 정보를 획득하는 전반적인 체제를 BBN 그래프를 이용하여 보여주고 있다. 이 그래프는 안전 소프트웨어의 정량적인 신뢰도 정보들을 그 소프트웨어의 각 개발 단계에서 생성되는 생산물의 품질을 평가함으로서 획득할 수 있다는 가정하고 있다. 소프트웨어 생산물은 소프트웨어 요구명세서, 소프트웨어 설계명세서, 소프트웨어 코드 그리고 이진 형태로 된 최종 소프트웨어들을 들 수 있다. 그림 1의 “Test_Result”는 결함이 발견되지 않은 상태에서의 시험 회수 또는 결함이 발견되지 않은 상태에서의 시험 기간이 될 수 있다.

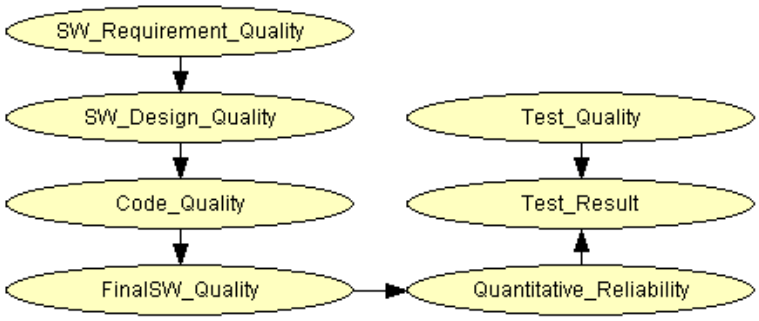

그림 1 안전소프트웨어 신뢰도 정량평가를 위한 기본 BBN 그래프

소프트웨어 개발 각 단계에서 나오는 소프트웨어 생산물을 평가하기 위한 모델은 그림 2의 일반 모델[10]을 사용하였다. 소프트웨어 생산물의 품질은 그 생산물에 관련된 특성들과 그것을 개발한 과정 그리고 소프트웨어 공학 척도들을 고려함으로서 측정될 수 있다. 그림 2는 소프트웨어 개발 단계 중 하나인 요구명세 작성 단계의 소프트웨어 생산물의 품질을 평가하는 BBN 모델이다.

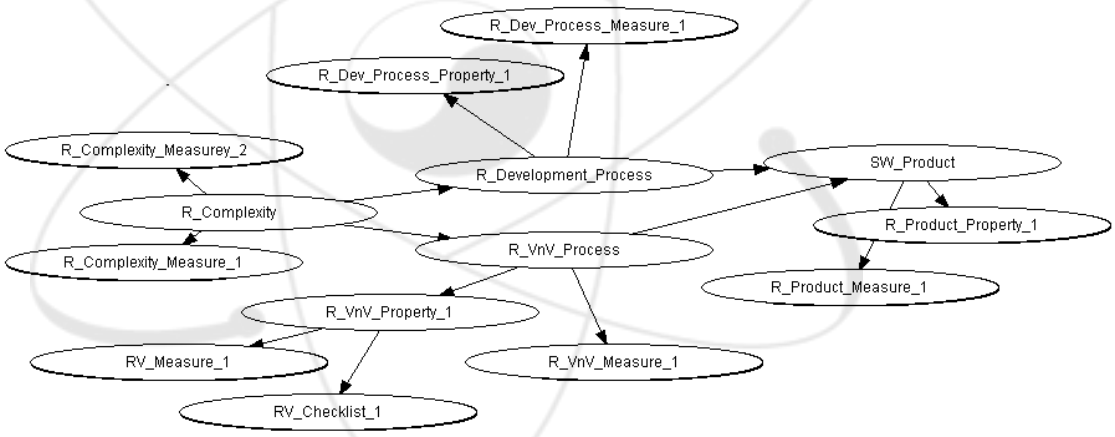

그림 2 요구명세 단계의 생산물(요구명세서)를 평가하기 위한 일반 BBN 모델

여기에서 소프트웨어의 특성들은 각종 척도와 체크리스트 등을 통하여 평가될 수 있는데 소프트웨어 요구명세 단계에서 사용될 수 있는 척도로는 다음과 같은 것들이 있다[11].

- ○ Reviews, Inspection and Walkthroughs -> V&VProcess
- ○ Man hours per major defect detected -> Product, V&V Process
- ○ Cause and effect graphing -> Product
- ○ Function point analysis (FPA) -> Product

○ Project initiation reliability prediction -> Prior reliability

○ software CMM -> V&V, Development

제3 장. KNICS 원자로보호계통 SW V&V를 위한 BBN

제1 절. KNICS 소프트웨어 확인 및 검증

KNICS 소프트웨어 확인 및 검증 절차는 BTP-14에 준하여 표-1과 같이 기능적 특성과 공정 특성으로 분류하여 안전에 중요한 소프트웨어의 요구사항을 검증하는 절차로 되어있다[12].

표 1 소프트웨어 요구사항 명세 검토 내용

기능 특성	공정 특성
정확도	완전성
기능성	일관성
신뢰성	정확성
강인성	스타일
안전성	추적성
보안성	명확성
타이밍	확인가능성

○ 정확도(accuracy): 센서와 운전원의 입력에서 오류가 생기지 않는 정도, 근사치 또는 측정치에서 보여진 정확함의 정도, 그리고 작동기 출력에서 오류가 생기지 않는 정도이다.

○ 기능성(functionality): 소프트웨어에 의해서 수행되어야 할 동작이다. 기능이라 함은 일반적으로 원자로 운전에 영향을 미치는 입력 정보를 출력 정보로 변환하는 것이다. 입력은 센서류, 운전원, 다른 장비, 또는 다른 소프트웨어에서 받게 된다. 출력은 작동기, 운전원, 다른 장비 또는 다른 소프트웨어로 보내진다.

○ 신뢰도(reliability): 어떤 소프트웨어 시스템이나 기기가 고장 없이 동작하는 정도이다. 이 정의는 고장의 결말은 고려하지 않고 고장 발생만을 고려한 것이다.

○ 강인성(robustness): 어떤 소프트웨어 시스템이나 기기가 부정확한 입력 또는 응력의 환경조건을 받더라도 소정의 기능을 정확하게 발휘해 내는 능력이다. 이것은 그 명세서의 가정사항과 어느 정도 다를지라도 정확하게 기능을 수행해 내는 능력도 포함한다.

○ 안전성(safety): 시스템의 안전성 고려사항에 직접 영향을 미치거나 또는 상호 연관되는 소프트웨어 시스템의 성질이나 특성이다. 이 SLCP에서 논의된 다른 특성은 소프트웨어-기반 안전계통의 전체 안전성에 미치는 중요한 기인자이지만, 그것은 일차적으로는 소프트웨어의 내적 동작에 관련된다. 그러나 안전성 특성은 소프트웨어가 시스템의 재해에 미치는 영향과 그러한 재해를 통제하기 위해 취해지는

수단에만 관련된다.

○ 보안성(security): 무단적이고, 불필요하고 불안전한 침투를 방지하기 위한 능력이다. 그러한 침투가 소프트웨어의 안전관련 기능에 영향을 줄 수 있는 한 보안은 안전성 현안이다.

○ 타이밍: 사용 중인 계산시스템에 의해 부과된 그 타이밍 목적을 하드웨어 제약조건 내에서 달성해 내는 소프트웨어 시스템의 능력이다.

○ 완전성(completeness): 소프트웨어에서 요구되는 기능을 완전하게 구현해 내는 계획문서, 구현공정문서 및 설계 결과물의 속성이다. 소프트웨어가 수행해야 할 기능은 안전계통의 일반기능요건과 전체시스템의 설계에서 소프트웨어에 배정된 기능요건들로부터 비롯된다.

○ 일관성(consistency): 어떤 소프트웨어 시스템에 대한 여러 종류의 문서들과 기기 간에 서로 상반된 것이 없는 정도이다. 두 가지 관점의 일관성이 있다. 내적 일관성은 어떤 기기의 서로 다른 부분 내에서의 일관성으로서 예를 들면, 어떤 소프트웨어 설계는 만약 설계 구성요소들이 서로 상반되지 않는다면 내적으로 일관된 것이라고 말할 수 있다. 외적 일관성은 한 기기와 다른 기기 간의 일관성으로서 예를 들면, 소프트웨어 요건과 그 코드가 만약 서로 간에 상반되지 않는다면 일관된 것으로 보아야 한다.

○ 정확성(correctness): 어떤 설계 결과물이 그 명세서, 설계, 그리고 구현에서 결함이 생기지 않을 정도이다. 정확성과 정확도 및 완전성과 같은 다른 특성 간에 서로 중첩하는 것이 바람직하다.

○ 스타일(style): 계획문서, 설계공정문서 및 설계 결과물의 형태와 구조이다. 문서 스타일은 어떤 문서의 구조와 형태를 말한다. 이것은 이해성(understandability), 판독성(readability), 그리고 수정성(modifiability)을 함축한 말이다. 프로그래밍 스타일은 소프트웨어의 프로그래밍 언어와 프로그래밍 그 자체의 특성을 말한다.

○ 추적성(traceability): 한 생명주기 제품의 각 요소가 어떤 선행 생명주기 제품의 하나 또는 그 이상의 요소들로 거슬러서 추적될 수 있고, 그리고 어떤 후행 생명주기 제품의 하나 또는 그 이상의 요소로 추적될 수 있는 정도이다.

○ 명확성(unambiguity): 그 제품의 각 요소와, 모든 요소들이 서로 합쳐지더라도 한가지의 해석만을 갖는 정도이다.

○ 확인성(verifiability): 소프트웨어 계획문서, 설계공정문서 및 설계 결과물이 확인

기준의 수립과 그러한 기준이 만족되었는지를 결정하기 위한 분석, 검토, 혹은 시험의 수행을 쉽게 할 수 있도록 서술 또는 제공되는 정도이다

제2절. 사례연구: 원자로보호계통 SW 요구명세서 평가

BBN을 이용한 안전소프트웨어 신뢰도 정량평가 방안의 실용성과 PSA에의 활용 가능성을 확인하기 위하여 사례연구를 수행하였다. 사례 연구의 범위는 원자로 보호계통 소프트웨어의 요구명세서의 품질을 평가하는 것으로 한정하였다. BBN 모델링에 사용된 문서는 공학적안전설비-기기제어계통 소프트웨어 개발계획서[13], 원자로보호계통 소프트웨어 요구사항명세 검증절차서[12], 원자로보호계통 소프트웨어 요구명세 검증보고서[14]이다. 이들 문서는 현재 KNICS에서 원자로 보호계통의 안전소프트웨어를 개발하기 위해서 사용 중인 문서들이다.

1. 요구명세서품질에영향을미치는변수의확인

BBN을 이용한 요구명세서의 품질 평가 방안은 품질에 관련된 모든 증거들을 결합하고 이들 변수들의 영향을 일관되게 전체 네트워크에 전파시키는 것이다. 따라서 모델링의 첫 작업은 요구명세서의 품질에 관련된 모든 변수들을 확인해야 하는데 이렇게 확인된 변수들은 일반적으로 BBN에서 노드로 사용된다. 요구명세서의 품질을 평가하기 위한 모델의 변수들은 대부분 확인 및 검증 절차서[12]과 소프트웨어 개발 계획서[13]에서 추출되었으며 이들을 요약하면 다음과 같다.

○ 소프트웨어 요구명세서의 14개 특성으로 앞에서 나타난 표 1과 같다.

○ 각 특성에 대한 질문들. 각 특성은 체크리스트를 가지고 있는데 이 체크리스트상의 질문들은 소프트웨어 요구명세서의 품질을 평가하는 내용들이다. 모델에 사용된 총 질문의 수는 150여개이고 부록 A에 질문 내용이 기술되어 있다.

○ 개발 과정, 확인 및 검증 과정, 그리고 복잡성

2. BBN그래프와 노드확률테이블 작성

소프트웨어 요구명세서의 품질에 관련된 변수들의 확인이 완료되면 다음 단계는 이들 변수들을 가지고 그래프를 그리고 또 각 변수들에 대하여 노드확률테이블(NPT)를 작성하게 된다. 이 단계의 목적은 관련된 모든 정보를 네트워크로 결합하는 것이다. BBN의 구축은 일반적으로 3단계로 나누어지는데 노드를 준비하고 이들을 연결하고 NPT를 작성하는 것이다.

○ 노드의 준비: 전 단계에서 확인된 변수들은 소프트웨어 요구명세서의 품질을 평

가하는데 필요한 기본 정보들이며, 따라서 이들은 BBN의 중심 노드들이 된다. 모델에 사용된 전체 노드 수는 166개이다.

○ 노드의 연결: 노드들을 연결하는 방법은 여러 가지가 있다. 가장 일반적인 방법은 그들의 인과관계에 따라 연결하는 것이다. 이러한 인과관계가 분명하지 않을 때는 보다 추상적인 노드에서 구체적인 노드로, 또는 보다 일반적인 노드에서 상세한 노드로 연결한다. 또 하나의 일반적인 연결 방법은 목표 노드에서 시작하여 이것에 영향을 미치는 노드로 연결하는 방법이다. 목표 노드는 네트워크에서 값을 구하고자 하는 노드(들)이다. 그림 3은 이렇게 작성된 소프트웨어 요구명세서 품질 평가용 BBN의 최상위 레벨 그래프인데 이것은 14개의 요구명세서 특성과 그림 2와 같은 원칙을 기반으로 작성되었다.

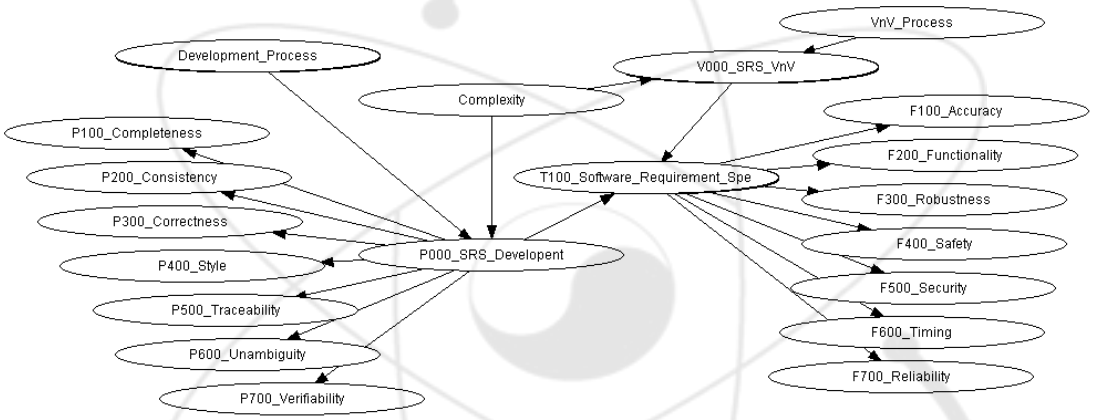

그림 3 소프트웨어 요구명세서 품질 평가를 위한 최상위 레벨 BBN 그래프

기술된 바와 같이 각 특성들은 이들을 평가하기 위한 체크리스트를 가지고 있고 체크리스트는 수 개의 질문으로 구성되어 있다. 이들 특성들과 질문들을 가지고 다음과 같이 14개 하위 레벨의 그래프를 작성하였다.

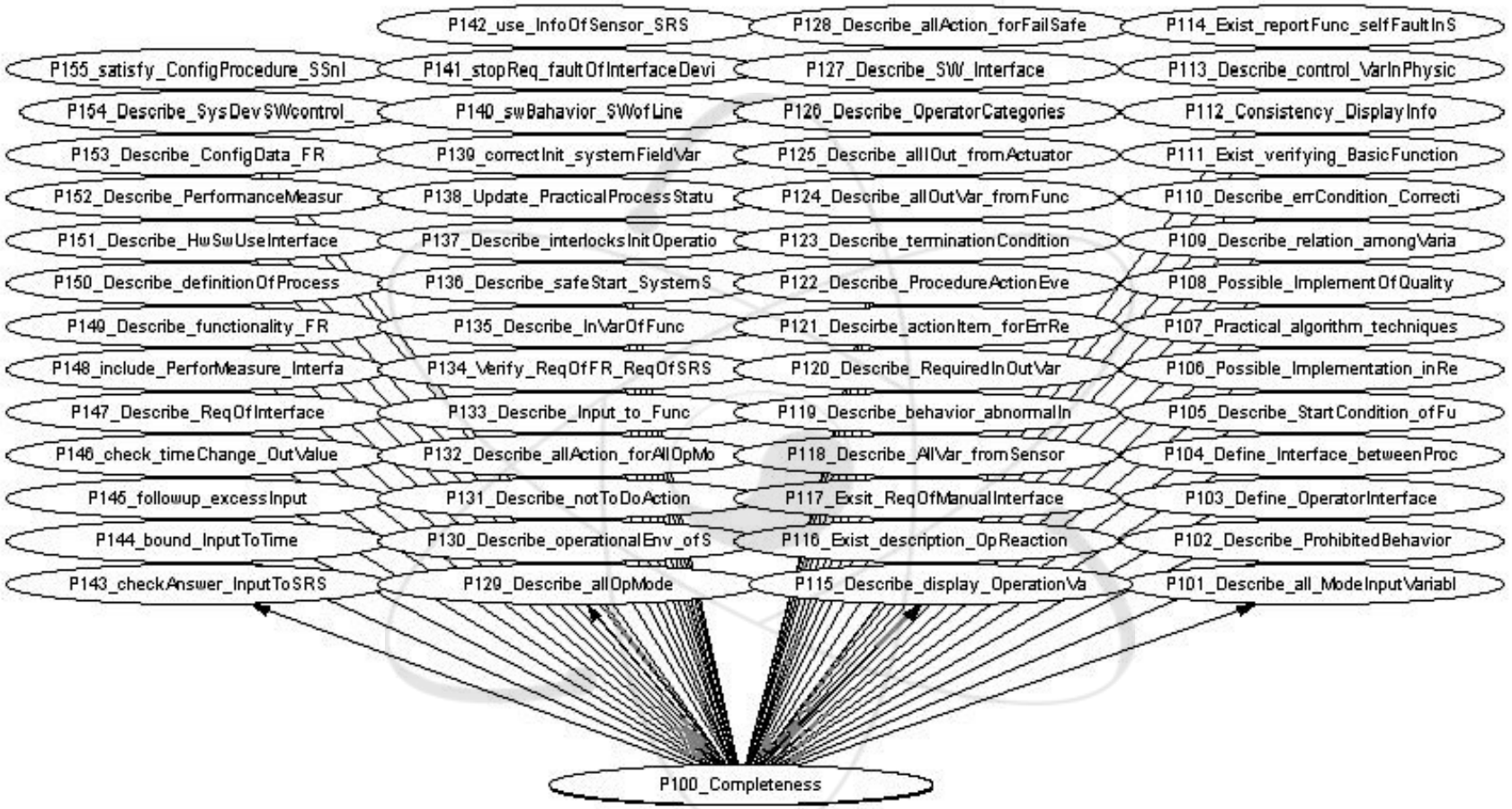

그림 4 Completeness 노드의 서브 그래프

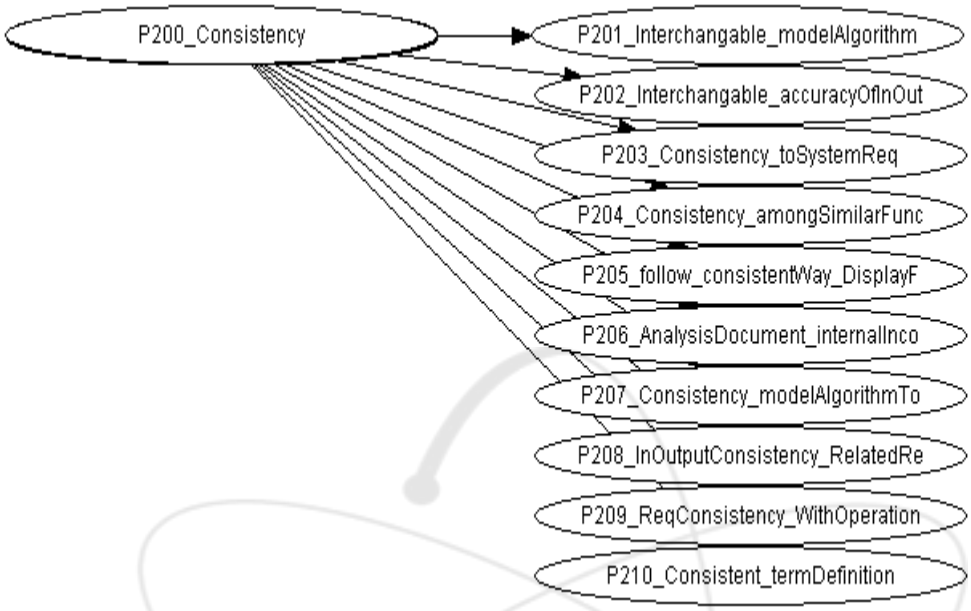

그림 5 Consistency 노드의 서브 그래프

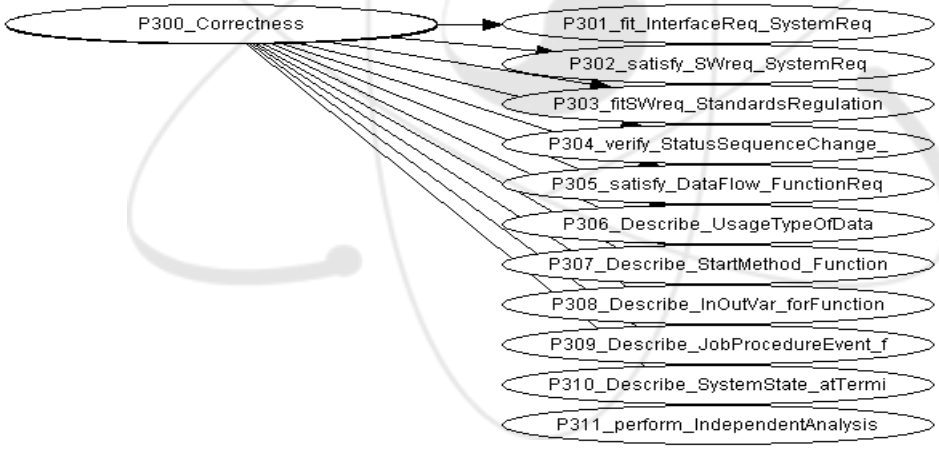

그림 6 Correctness 노드의 서브 그래프

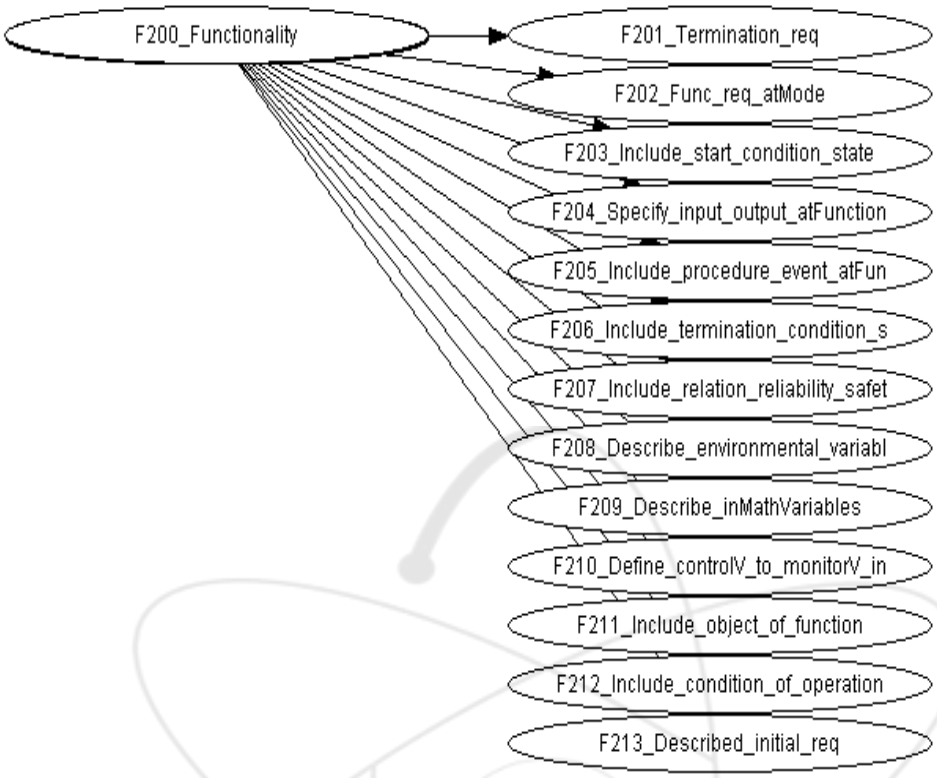

그림 7 Functionality 노드의 서브 그래프

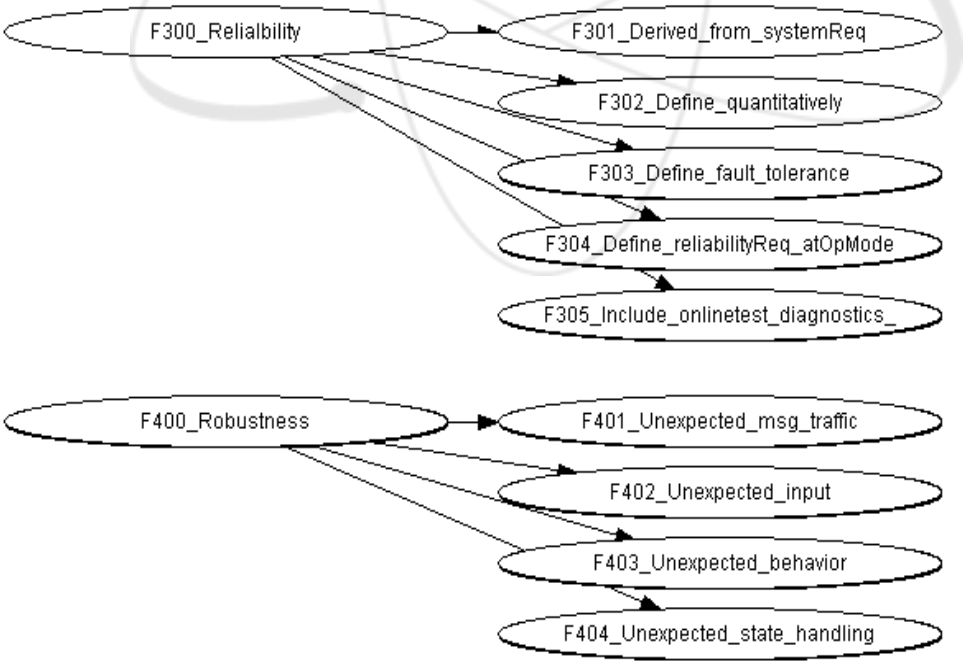

그림 8 Reliability, Robustness 노드의 서브그래프

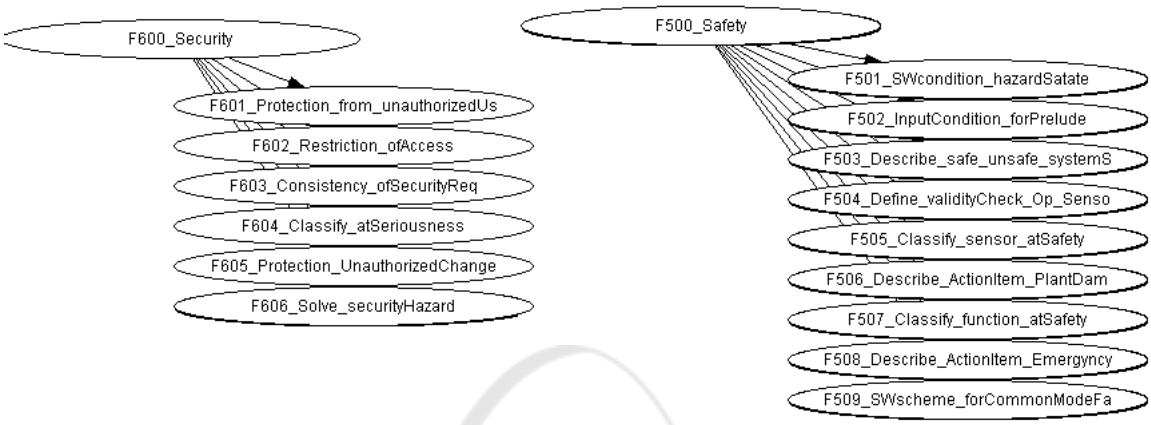

그림 9 Security, Safety 노드의 서브그래프

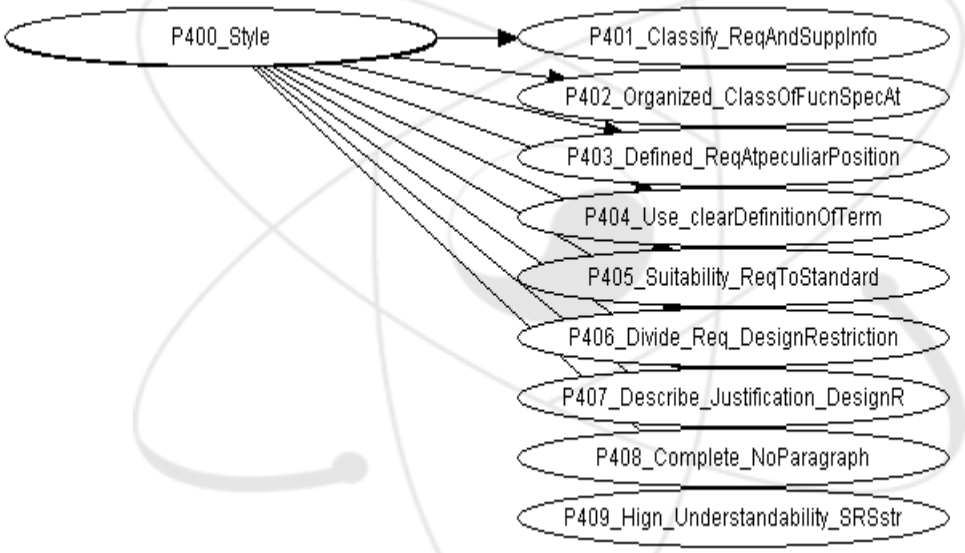

그림 10 Style 노드의 서브그래프

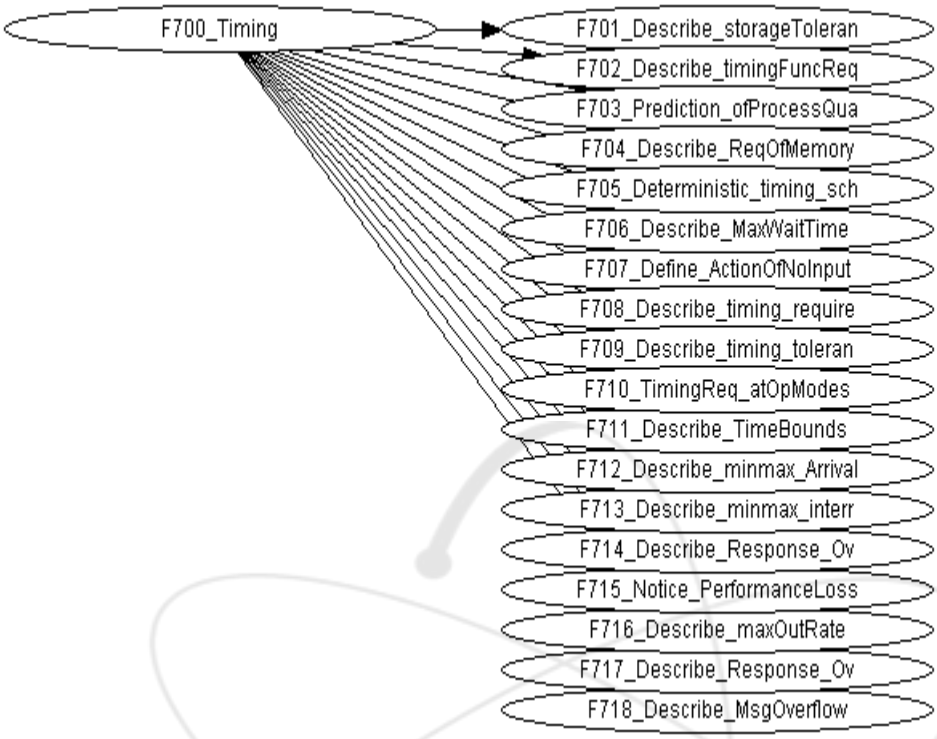

그림 11 Timing 노드의 서브그래프

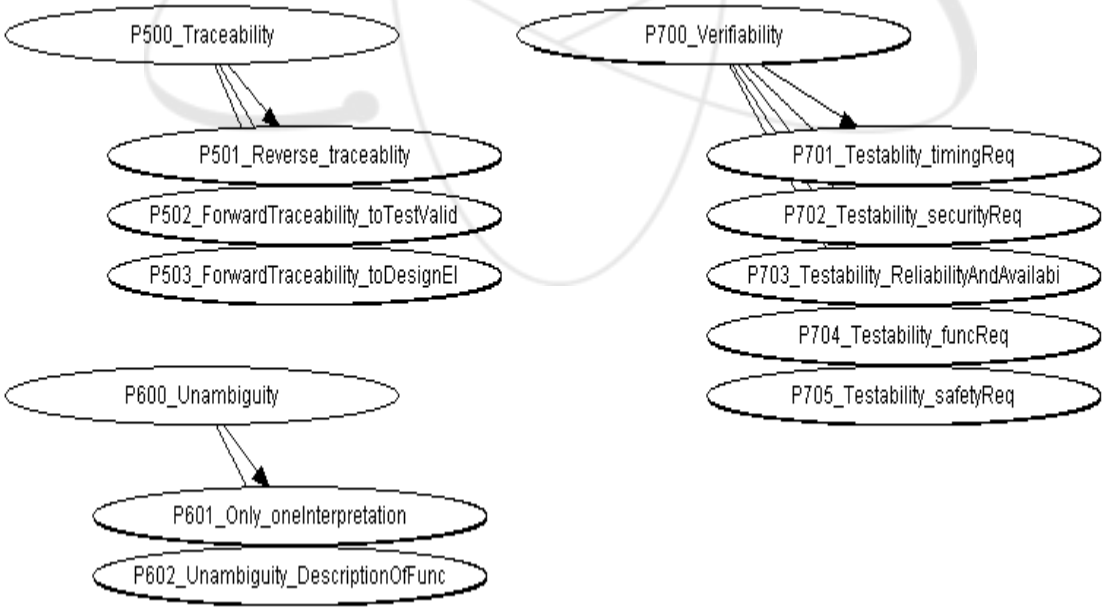

그림 12 Traceability, Unambiguity, Verifiability 노드의 서브그래프

○ 노드의 확률 값 설정

노드들을 모두 연결시켜 네트워크를 완성시킨 다음에는 각 노드의 NPT를 작성해야 한다. NPT는 연결된 노드 간의 연결 강도를 나타낸다. NPT의 확률 값을 작성하는 방법은 여러 가지가 있을 수 있다. 예를 들면, 기존에 관찰된 빈도를 근거로 확률을 정할 수도 있고 이런 통계적인 자료가 없는 경우에는 전문가의 주관적인 판단에 근거한 확률 값을 설정할 수도 있다.

소프트웨어 요구명세서의 품질을 평가하기 위해 작성된 본 연구의 BBN에서 목표 노드는 "T100_Software_Requirement_Specificaion"인데 이 노드는 "acceptable"과 "unacceptable" 두 개의 상태를 가지고 있다. 이 노드의 상태들은 소프트웨어 요구명세서의 품질을 나타낸다. 체크리스트로부터 만들어진 모든 노드들은 두 개의 상태 "yes"와 "no"를 가지고 있다. NPT의 확률들은 V&V 전문가가 작성하였는데 일반적인 작성 기준은 다음과 같다.

(1) 노드확률테이블 형식

◇ 노드확률테이블 형식-1

Self \ Pt	good	bad
yes		
no		

◇ 노드확률테이블 형식-2

Node-1		Good		Poor	
Node-2		Good	Poor	Good	Poor
Node-3	Acceptable				
	Not_Acceptable				

(2) 노드확률테이블의 확률 값 설정 방안

◇ 가능한 값 조합

(1.0, 0.0) (0.99, 0.01) (0.95, 0.05) (0.9, 0.1) (0.8, 0.2) (0.7, 0.3) (0.6, 0.4)

(3) 두 노드 사이의 연결 강도(조건부 확률)에 따른 값 부여 기준

◇ 결정론적인 연결

Self \ Pt	good	bad
yes	1.0	0.0
no	0.0	1.0

◇ 가장 확실한 연결

Self \ Pt	good	bad
yes	0.99	0.01
no	0.01	0.99

◇ (구체적and세부적) 사항에 대한 연결

Self \ Pt	good	bad
yes	0.95	0.05
no	0.05	0.95

◇ (구체적and종합적) or (추상적and세부적) 사항에 대한 연결

Self \ Pt	good	bad
yes	0.90	0.10
no	0.10	0.90

◇ (추상적and종합적) 사항에 대한 연결

Self \ Pt	good	bad
yes	0.8	0.2
no	0.2	0.8

◇ 추상적이고 종합적인 사항에 대한 느슨한 연결

Self \ Pt	good	bad
yes	0.7	0.3
no	0.3	0.7

◇ most loosely coupled connection

Self \ Pt	good	bad
yes	0.6	0.6
no	0.4	0.4

이와 같은 기준으로 작성된 NPT는 부록 B에 기술되어 있다.

3. 노드 입력 값 (항목 평가치) 설정

BBN의 목적은 관찰된 증거들에 근거하여 목표 노드의 값을 계산하는 것이다. 따라서 모든 관찰 가능한 노드들의 값을 얻는 것이 필요하다. 물론 BBN에서는 일부 또는 전체 관찰 가능 노드에 값을 입력하지 않고도 목표 노드의 값을 계산하는 것이 가능하다. 이들 관찰 가능 노드들에 입력할 값은 정성적인 형태나 또는 정량적인

형태로 얻어진다. 그런데 BBN에 사용되는 모든 값은 확률의 형식으로 표현되어야 하므로 정성적인 증거 값들은 정량 형태로 변환하는 것이 필요하다. 소프트웨어 요구명세서의 품질을 평가하기 위한 본 BBN 모델에서는 V&V 전문가가 모든 관찰 가능 노드들의 입력 값을 직접 작성하였으며 그 작성 기준은 다음과 같다.

(1) 질문 형태

질문	yes	no
알고리즘(논리/공식)이 정확한가?		

(2) 가능한 입력 값 샘플

(1.0, 0.0) (0.99,).01) (0.95, 0.05) (0.9, 0.1) (0.8, 0.2) (0.7, 0.3) (0.6, 0.4) (0.5, 0.5)

(3) 노드 상태 값 부여 방법

(가) 질문 형태별로 부여할 수 있는 노드 상태(node state)의 <u>최대 값</u>

◇ 결정론적(deterministic)인 질문에 대한 응답

(1.0, 0.0)

◇ (구체적and세부적) 질문에 대한 응답

(0.99, 0.01)

◇ (구체적and종합적) or (추상적and세부적) 질문에 대한 응답

(0.9, 0.1)

◇ (추상적and종합적) 질문에 대한 응답

(0.8, 0.2)

(나) 특별 케이스

◇ 답을 알 수 없는 경우의 응답(가장 불확실한 상황)

(0.5, 0.5)

◇ 단일 값으로 평가가 곤란한 경우에는 범위(range)값, max-min 값 형태를 사용.

(다) 일반적 값 부여 기준

확률 값을 부여하는 일반적 기준은 표-2의 Sherman Kent의 등급척도를 참조하였

다.

표 2. Sherman Kent의 등급 척도

Order of Likelihood	Synonyms	Chances in 10	Percent
Nearly Certain	Virtually certain		99
	We are convinced	9	
	Highly probable		
	Highly likely	8	80
Probable	Likely		
	We believe		
	We estimate	7	
	Chances are good		
	It is probable	6	60
Even Chance	Chances slightly better than even		
	Chances about even	5	
	Chances slightly less than even	4	40
Improbable	Probably not		
	Unlikely	3	
	We believe not	2	20
Nearly Impossible	Almost impossible		
	Only a slight chance	1	
	Highly doubtful		10

이 외에 확률 값 설정에 관련된 참고 자료는 "안전 SW의 신뢰도 정량평가 BBN을 위한 전문가 지식추출 지침(KAERI/TR-2662/2004)“을 사용하였다.

최종적으로 작성된 각 노드 별 입력 값은 부록 D에 첨부된 “ KNICS 원자로보호계통 소프트웨어 확인 및 검증 평가 값: 상세항목“ 과 같다.

4. 모델의 계산 및 분석

전 단계에서 수집된 증거들을 가지고 BBN의 계산을 수행하면 소프트웨어 요구명세서의 품질을 평가할 수 있다. 이 증거는 BBN의 관찰가능 노드들의 입력항목이 된다. 계산 결과는 BBN의 모든 노드들의 확률분포이다. 본 BBN 모델의 목적은 목표 노드인 소프트웨어 요구명세서 품질의 “acceptable″상태의 확률 분포를 구하는 것이지만 BBN에서는 그 외에도 여러 가지 유용한 분석을 할 수 있는데 본 연구에서는 2 개의 시나리오를 설정하여 그 계산과 분석을 수행하였다. BBN의 계산은 매우 복잡하여 수작업으로는 거의 불가능하므로 적절한 컴퓨터 도구를 사용해야 하는데 본 연구에서는 HUGIN[15]을 사용하였다.

본 연구에서 설정한 시나리오는 다음과 같다.

(1) V&V 전문가의 평가 값을 입력하여 계산한 결과

(2) 측정가능 노드의 계산 값과 14개 중간변수 평가 항목의 비교분석

각 시나리오 별 계산 결과와 분석은 다음과 같다.

(1) V&V 전문가의 평가 값을 입력하여 계산한 결과

표 3. V&V 전문가의 평가 값을 입력하여 계산한 결과

노드 이름	상태 값(%)	비고
T100_Software_Requirement_Spec	acceptable: 0	요구명세서 품질
F100_Accuracy	good: 0.06	정확도
F200_Functionality	good: 0.04	기능성
F300_Reliability	good: 0.09	신뢰성
F400_Robustness	good: 6.61	강인성
F500_Safety	good: 0	안전성
F600_Security	good: 0	보안성
F700_Timing	good: 0	타이밍
P100_Completeness	good: 81.56	완전성
P200_Consistency	good: 0.08	일관성
P300_Correctness	good: 0	정확성
P400_Style	good: 6.89	스타일
P500_Traceability	good: 0	추적성
P600_Unambiguity	good: 0.05	명료성
P700_Verifiability	good: 0.26	확인가능성

표 4. 시나리오-1의 중간 노드 값

노드 이름	상태 값(%)	비고
CMM_Level	<Level3: 79.04	SW CMM등급
Complexity	low: 29.09 medium: 33.94 high: 36.97	요구명세서 복잡성
Development_Process	good: 6.39	개발 공정
SRS_Development	good: 0	개발 구현
SRS_V&V	good: 33.32	확인 및 검증 구현
VnV_Process	good: 35.34	확인 및 검증 공정

목표 노드 “Software_Requirement_Specification”의 “acceptable″ 상태의 확률이 매우 낮게 나왔는데 이것은 현재 요구명세서가 여전히 개발 단계이고, 그래서 전체 체크리스트 중 약 30% 만이 긍정적으로 평가되었기 때문이다. 이 시나리오는 추후 V&V 활동을 결정하는 기준으로도 사용할 수 있는데, 예를 들면, 평가 대상이 된 소프트웨어 요구명세서의 잠정적인 완료 기준을 목표 노드 ”acceptable″ 상태의 확률을 95% 이상으로 설정하는 것 등이다.

표5는 전문가가 평가한 각 질문의 평가치들(예를 들어, (1,0) (0.99, 0.01), (0.9,0.1) (0.8, 0.2))을 모두 (1,0)로 대치하여 계산한 결과이다. 이 계산의 목적은 0.99 또는 0.9와 같은 복잡한 정량화 단계를 보다 단순화시켰을 경우의 결과와 본래의 평가치를 사용했을 경우의 결과를 비교하기 위한 것이다.

표 5. 평가치를 “1”로 대치하여 계산한 결과

노드 이름	상태 값(%)	비고
T100_Software_Requirement_Spec	acceptable: 0	요구명세서 품질
F100_Accuracy	good: 0	정확도
F200_Functionality	good: 0	기능성
F300_Reliability	good: 0.02	신뢰성
F400_Robustness	good: 21.52	강인성
F500_Safety	good: 0	안전성
F600_Security	good: 0	보안성
F700_Timing	good: 0	타이밍
P100_Completeness	good: 0.28	완전성
P200_Consistency	good: 0.09	일관성
P300_Correctness	good: 0	정확성
P400_Style	good: 5.54	스타일
P500_Traceability	good: 0	추적성
P600_Unambiguity	good: 0.01	명료성
P700_Verifiability	good: 0.03	확인가능성

표 6. 시나리오-1, 평가값 “1”로 대치한 경우의 중간 노드 값

노드 이름	상태 값(%)	비고
CMM_Level	<Level3: 79.04	SW CMM등급
Complexity	low: 29.09 medium: 33.94 high: 36.97	요구명세서 복잡성
Development_Process	good: 6.39	개발 공정
SRS_Development	good: 0	개발 구현
SRS_V&V	good: 33.32	확인 및 검증 구현
VnV_Process	good: 35.34	확인 및 검증 공정

평가치를 (1,0)으로 대치하여 계산한 경우에도 전체적인 계산 결과는 본래의 평가치를 사용하여 계산한 결과와 거의 유사하고 목표 노드의 값도 동일하다. 다만 P100_completeness 노드의 상태 값은 거의 반대로 나타나고 있다는데, 이것은 모두 (1,0)로 응답을 한 경우(표-5)는 개수에 비례하는 경향이 강하므로 P100_completeness의 “Bad” 상태 값이 크게 나왔으나 표-4의 경우에는 yes로 응답한 질문에 (0.99)의 값이 no의 응답 경우(4개)보다 상대적으로 많은 13개가 나왔으므로 P100_completeness의 “Good” 상태 값이 크게 나온 것이다. P100_completeness 노드의 정보는 다음과 같다.

- o P100_completeness노드의 전체 질문 개수: 55
- o yes 응답개수->23, no 응답개수->32
- o 0.99로 된 응답개수 : yes->13, no->4 이고 나머지는 0.9로 응답

P100_completeness 노드와 같이 자노드(child node)를 가진 노드는 자노드에 서로 상반되는 값이 입력 될 경우 특정한 경계(서로 상반되는 입력값을 가지는 자노드 개수 비례, 예를 들면 3:2 또는 5:4 등)에서 모노드의 값이 급격하게 변하는 현상을 나타내는데 이것은 모노드와 자노드간의 연결강도(조건부 확률 값이)가 높을수록 그 변화가 심하다.

(2) 측정가능 노드의 계산 값과 14개 특성 변수 평가 항목의 비교분석

다음의 표는 부록-C와 같이 전문가가 14개 특성에 대해 개별적으로 평가 값을 부여한 것과 BBN계산 결과를 비교한 것이다.

표 7. 모델 계산 값과 전문가 평가 값 비교

노드 이름	계산 값(%)	전문가 평가 값(%)
F100_Accuracy	good: 0	good: 20
F200_Functionality	good: 0	good: 40
F300_Reliability	good: 0.02	good: 20
F400_Robustness	good: 21.52	good: 60
F500_Safety	good: 0	good: 40
F600_Security	good: 0	good: 0
F700_Timing	good: 0	good: 20
P100_Completeness	good: 0.28	good: 30
P200_Consistency	good: 0.09	good: 50
P300_Correctness	good: 0	good: 20
P400_Style	good: 5.54	good: 50
P500_Traceability	good: 0	good: 20
P600_Unambiguity	good: 0.01	good: 10
P700_Verifiability	good: 0.03	good: 20

모델의 계산 값은 전문가의 평가 값에 비하여 매우 낮게 나타났다. 이것은 BBN 모델의 특성 상 노드 간에 종속성이 생겨 한 노드의 값이 다른 노드에 영향을 주기 때문이다. 예를 들어 F100_Accuracy 노드의 경우를 보면 이 노드에 속한 질문의 20% 정도에 긍정적 평가치가 입력되더라도 나머지 80%의 부정적 평가치와 또 다른 13개의 특성 노드들의 자노드에 입력되는 부정적 평가치(bad: 0.9 등)들이 F100_Accuracy에 계속적으로 영향을 주어 결국에는 good: 0과 같은 값이 된 것이다. 그런데 전문가의 정성적 평가는 이와 같은 종속성에 따른 영향을 모델에 비하여 적게 고려하므로 모델 계산 결과에 비하여 상대적으로 높은 평가 값을 준 것으로 보여 진다.

제4 장. 요약 및 결론

원자력발전소의 PSA에 사용하기 위하여 안전 소프트웨어의 신뢰도 정보를 획득할 수 있는 체계적인 방안을 개발하고 부분적인 사례연구를 수행하였다. 이 방안은 안전 소프트웨어의 신뢰도에 관련된 정성적인 증거와 정량적인 증거를 함께 결합할 수 있고 또 이들 증거에 근거하여 정형적이고 정량적으로 결론을 추론할 수 있는 BBN을 기반으로 구축하였다. 사례연구로서 KNICS에서 현재 개발 중인 원자로보호계통 소프트웨어의 요구명세서 품질 평가에 적용하였고 동 문서의 V&V 결과를 모델의 입력 자료로 사용하였다. BBN모델의 계산 결과는 V&V 전문가의 판단과 유사하게 나타났으며, 또한 이 모델은 추후의 V&V 활동에 대한 의사결정을 할 때 필요한 자료를 제공할 수 있을 것으로 보인다.

추후의 연구내용은 소프트웨어 개발 각 단계에서 생산되는 해당 결과물(설계명세서, 코드, 이진형태의 코드 등)의 품질 평가용 상세 BBN모델을 구축하는 것과 이로부터 최종적으로 안전 소프트웨어 신뢰도의 정량적인 값을 추론하는 모델을 구축하는 것이다.

참고문헌

[1] B. Littlewood and L. Strigini, Validation of Ultrahigh Dependability for Software-Based Systems, Communication of the ACM, 36(11), 1993

[2] R.W. Butler and G.B. Finelli, The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software, IEEE Transactions on Software Engineering, 19(1), 1993

[3] NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," (SRP). The updated SRP Chapter7

[4] RTCA. Software considerations in airborne systems and equipment certification, DO-178B, Requirements ad Technical Concepts for Aeronautics, 1992.

[5] 경수로형 원전 안전심사지침, 한국원자력안전기술원, 1998

[6] Jensen, F., An Introduction to Bayesian Belief Networks, Springer-Verlag, New York, NY, 1996.

[7] Bjorn Axel Gran and Gustav Dahll, Estimating dependability of programmable systems using bayesian belief nets, OECD HALDEN rector project, HWR-627, 2000 May

[8] B. Littlewood and L. Strigini, Examination of Bayesian Belief Networks for Safety Assessment of Nuclear Computer-based Systems, ESPRIT DeVa Project 20072, 1998

[9] Neil, M., et al, "Applying Bayesian Belief Networks to System Dependability Assessments," Proceedings of Safety Critical Systems Club, February 1996.

[10] Gary Johnson, Bayesian Belief Networks based Review of Software Design Documents, International Topical Meeting on Nuclear Instrumentation, Control, and Human-Machine Technologies(NPIC & HMIT 2000), Washington DC, Nov. 2000

[11] Gary Johnson, Assessment of software reliability measurement method, LLNL, 1999

[12] HanSung, S., et al, 2003. V&V Procedure for Software Requirement

Specification for Reactor Protection System, KNICS-RPS-(SRS)-SVP121, KAERI KNICS, 2003.

[13] Du-Hwan, K., et al, 2001. Software Development Plan for Engineering Safety Features, KNICS-ESF-SDP101, KAERI KNICS, 2001.

[14] HanSung, S., 2004. V&V Validation Reports for Software Requirement Specification for Reactor Protection System, KNICS-RPS-(SRS)-SVR121, KAERI KNICS, 2004.

[15] Hugin, www.hugin.dk, Aalborg, Denmark

부록 A. KNICS 원자로보호계통 소프트웨어 확인 및 검증용 BBN의 질문 리스트
부록 B. KNICS 원자로보호계통 소프트웨어 확인 및 검증용 BBN의 NPT
부록 C. KNICS 원자로보호계통 소프트웨어 확인 및 검증 평가 값: 종합항목
부록 D. KNICS 원자로보호계통 소프트웨어 확인 및 검증 평가 값: 상세항목

부록 A. 소프트웨어 요구명세서 V&V를 위한 질문 목록

소프트웨어 요구명세서 V&V를 위한 질문들은 14개의 특성으로 구성되어 있고 이들 특성은 다음의 표와 같이 기능특성과 공정 특성으로 나눌 수 있다.

표 A-1. 소프트에어 요구사항 명세 검토 내용

기능 특성/코드	공정 특성/코드
정확도/F1	완전성/P1
기능성/F2	일관성/P2
신뢰성/F3	정확성/P3
강인성/F4	스타일/P4
안전성/F5	추적성/P5
보안성/F6	명료성/P6
타이밍/F7	확인가능성/P7

A-1. 기능 특성 검증

◇ 정확도 검증(Accuracy)에 관한 질문 목록

노드명/노드확률테이블		질문
정확도: F100_Accuracy		
1	F101_Accuracy_req_atNVariables	수치 값을 갖는 각 입력변수 및 출력 변수에 대해서 정확도 요구사항이 존재하는가?
2	F102_Accuracy_req_atVariables	모든 입력과 출력 변수에 대하여 정확도 요구사항이 존재하는가?
3	F103_Describe_in_quantitatively	각 정확도 요구사항이 정량적으로 기술되어 있는가?
4	F104_Describe_physical_unit	각 정확도 요구사항에 물리적 단위가 기술되어 있는가?
5	F105_Describe_error_range	각 정확도 요구사항에 오차 허용범위가 포함되어 있는가?
6	F106_define_data_type_size	모든 정확도 요구사항들은 데이터 형식과 데이터 크기가 포함되어 있는가?

◇ 기능성(Functionality) 검증

노드명/노드확률테이블		질문
F200_Functionality		
1	F201_Termination_req	출력다운과 가동중지 순서와 같은 종결(termination) 요구사항이 명세되어 있는가?
2	F202_Func_req_atMode	시스템 설계 문서(SDD)와 안전분석보고서에서 식별된 모든 운전모드들에 대한 기능 요구사항들이 완전하게 명세 되어 있는가?
3	F203_Include_start_condition_state	모든 기능 요구사항들이 시작 조건 및 각 기능 개시에서의 시스템의 상태를 포함하고 있는가?
4	F204_Specify_input_output_atFunction	기능 요구사항들이 각 기능에 요구되는 입, 출력 변수들을 모두 명세하고 있는가?
5	F205_Include_procedure_event_atFunc	기능 요구사항들이 각 기능을 수행하는데 필요한 작업 순서, 조치사항, 이벤트 등을 포함하고 있는가?
6	F206_Include_termination_condition_state	모든 기능 요구사항들이 종결 조건 및 각 기능 종결 시 시스템의 상태를 포함하고 있는가?
7	F207_Include_relation_reliability_safety	기능 요구사항들이 시스템의 신뢰도 및 안전성에 대한 각 기능의 연관성을 직, 간접적으로 포함하고 있는가?
8	F208_Describe_environmental_variables	SRS가 소프트웨어가 감시 또는 제어하는 물리적 환경에서의 변수(온도나 압력 등)를 식별하고 있는가?
9	F209_Described_inMathVariables	SRS가 물리적 환경의 변수들을 수학적 변수로 나타내고 있는가?
10	F210_Define_controlV_monitorV_inFunc	SRS가 제어변수(controlled variables)의 요구되는 행위들을 수학적 함수를 이용한 감시변수(monitored variables)로서 정의하고 있는가?
11	F211_Include_object_of_function	기능 요구사항들이 각 기능의 목적을 포함하고 있는가?
12	F212_Include_condition_of_operation	기능 요구사항들이 각 기능을 동작하도록 하는 야기 조건(trigger conditions)을 포함하고 있는가?
13	F213_Describe_initial_req	변수의 초기값, 기동 및 출력 상승 절차와 같은 초기화 요구사항들이 명시되어 있는가?

◇ 신뢰성(Reliability) 검증

노드명/노드확률테이블		질문
신뢰성(Reliability) 검증		
1	F301_Derive_from_systemReq	소프트웨어 신뢰성 요구사항이 시스템 설계 사양(SDD)의 신뢰성 요구사항으로부터 도출되는가?
2	F302_Define_quantitatively	소프트웨어 신뢰성 요구사항이 고장율이나 고장 기준에 대한 평균시간과 같이 정량적으로 정의되어 있는가?
3	F303_Define_fault_tolerance	고장허용이나 점차적인 노후(graceful degradation) 등에 대한 요구사항이 정의되어 있는가?
4	F304_Define_reliabilityReq_atOpMode	각 운전모드에 대한 신뢰성 및 가용성 요건이 주어졌는가?
5	F305_Include_onlinetest_diagnostics_req	소프트웨어 요구사항 명세가 시험 및 진단에 대한 요구사항을 포함하고 있는가?

◇ 강인성(Robustness) 검증

노드명/노드확률테이블		질문
강인성(Robustness) 검증		
1	F401_Unexpected_msg_traffic	SRS가 예기치 못한 메시지 트래픽 상황에서 소프트웨어 거동을 명세하고 있는가?
2	F402_Unexpected_input	SRS가 예기치 않은, 부정확한 또는 부적절한 입력 데이터 또는 다른 비정상 조건하에서 소프트웨어 거동을 명세하고 있는가?
3	F403_Unexpected_behavior	SRS가 예기치 않은, 부정확한 또는 부적절한 하드웨어 및 소프트웨어 거동 하에서 소프트웨어 거동을 명세하고 있는가?
4	F404_ProperAction_UncorrectState	SRS가 시스템 작동 상 임의의 절차에서 빠져 나온 후의 상태 체크와 부정확한 상태가 검출되었을 경우에 대한 적절한 조치를 요구하고 있는가?

◇ 안전성(Safety) 검증

노드명/노드확률테이블		질문
F500_Safety: 안전성(Safety) 검증		
1	F501_SWcondition_hazardState	시스템이 위험한 상태에 이르게 하는 소프트웨어의 조건이 SRS에서 명세 되어 있는가?
2	F502_InputCondition_forPrelude	SRS가 소프트웨어 초기 보호 조치(initiating protective actions)에 대한 전조(prelude)로서 필요한 입력 조건과 계산들을 명시하고 있는가?
3	F503_Describe_safe_unsafe_systemStatus	SRS가 시스템의 안전한 상태 및 비 안전 상태를 명시하고 있는가?
4	F504_Define_validityCheck_Op_SensorIN	SRS에서 운전원과 센서 입력에 대한 검증 체크(validity checks)에 대해 정의하고 있는가?
5	F505_Classify_sensor_atSafety	SRS가 안전 중요도에 따라 센서와 actuator를 분류하고 있는가?
6	F506_Describe_ActionItem_PlantDamage	SRS가 발전소 손상을 막기 위해 필요한 소프트웨어 조치사항(필요한 계산과 물리적인 백그라운드 포함)을 명세하고 있는가?
7	F507_Classify_function_atSafety	소프트웨어 요구 사항 명세가 중요도에 따라 기능을 분류하고 있는가?
8	F508_Describe_ActionItem_Emergency	SRS가 원자로의 비상정지를 수행하기 위해 필요한 소프트웨어 조치사항(필요한 계산과 물리적인 백그라운드 포함)을 명세하고 있는가?
9	F509_SWscheme_forCommonModeFailure	시스템 설계 사양(SDD) 및 안전분석보고서(SAR)에 의해 요구되는 잠재적인 공통모드 고장에 대한 소프트웨어의 대처방안이 명시되어 있는가?

◇ 보안성(Security) 검증

노드명/노드확률테이블		질문
보안성(Security) 검증		
1	F601_Protection_from_unauthorizedUser	SRS가 승인되지 않은 사람이 소프트웨어 시스템을 다루는 것을 금지하는 요구사항을 부여하고 있는가?
2	F602_Restriction_ofAccess	SRS가 운전원, 매니져 및 기타 직원에 대한 접근제한(access restriction)을 부여하고 있는가?
3	F603_Consistency_ofSecurityReq	보안성 요구사항이 전체적으로 상호 일관성(mutually consistent)이 있는가?
4	F604_Classify_atSeriousness	컴퓨터 시스템에 대한 잠재적 보안 위협이 심각성과 가능성에 따라 식별 및 분류되고 문서화되는가?
5	F605_Protection_UnauthorizedChange	SRS가 소프트웨어 시스템에 대한 승인되지 않은 변경을 방지하는 요구사항을 부여하고 있는가?
6	F606_Describe_securityHazard	SRS에서 보안 위협을 강조하기 위한 요구사항을 명시하고 있는가?

◇ 타이밍(Timing) 검증

노드명/노드확률테이블		질문
타이밍(Timing) 검증		
1	F701_Describe_storageTolerances	SRS가 저장장소 허용(storage tolerances)을 명시하고 있는가?
2	F702_Describe_timingFuncReq	SRS가 시간에 중요한 기능과 그 기능에 대한 시간 요건을 명시하고 있는가?
3	F703_Prediction_ofProcessQuantity	소프트웨어에 대한 처리량 예상이 주어져있는가?
4	F704_Describe_ReqOfMemorySize	메모리 크기 요구사항이 명백하게 표현되어 있는가?
5	F705_Deterministic_timing_schedule	소프트웨어 시스템이 결정론적 타이밍으로 동작하도록 되어 있는가?
6	F706_Descirbe_MaxWaitTime	Error로 표시되어 예외처리로 들어가기 전에, 컴퓨터가 처음 입력을 기다릴 최대시간이 명시되어 있는가?
7	F707_Define_ActionOfNoInput	정해진 시간 동안 입력이 없을 때 시스템이 취할 행동이 정해져 있는가?
8	F708_Describe_timing_requirement	타이밍 요구사항이 명백하게 표현되어 있는가?
9	F709_Describe_timing_tolerance	SRS가 타이밍 허용치를 명시하고 있는가?
10	F710_TimingReq_atOpMode	최대, 최소 타이밍 요구사항이 각 운전모드에 대하여 모두 명시되어 있는가?
11	F711_Describe_TimeBounds	명시된 허용 시간한계 (Time bounds)를 벗어나 들어오는 입력에 대한 시스템의 행동이 각 운전모드에 대해 명시되어 있는가?
12	F712_Describe_minmax_ArrivalRate	입력의 최대 최소 도착률이 명시되어 있는가?
13	F713_Describe_minmax_interruptR	인터럽트의 최대, 최소 발생률이 명시되어 있는가
14	F714_Describe_Response_Overflow	예상 입력률 (또는 인터럽트 발생률)을 초과 했을 때 시스템 응답이 명시 되어 있는가?
15	F715_Notice_PerformanceLoss	과부하 상태에 대해 시스템이 성능 감소를 보일 때, 이러한 성능감소가 점진적인가? 또 이 상황이 운전원에게 통보 되는가?
16	F716_Describe_maxOutRate	최대 출력률이 명시되어 있고 연결된 장비와 호환하는가?
17	F717_Describe_Response_OverOutR	예상 출력률을 초과 했을 때 시스템 응답이 명시되어 있는가?
18	F718_Describe_MsgOverflow	사용자 인터페이스 명세가 정보의 출력이 사용자의 정보 이해력을 초과하는 발생을 방지하도록 명세 하는가?

A-2. 공정 특성 검증에 관한 질문 목록

◇ 완전성(Completeness) 검증

노드명/노드확률테이블		질문
완전성(Completeness) 검증		
1	P101_Describe_all_ModeInputVariables	시스템에 요구되는 모든 행위가 모든 운전 모드 및 모든 가능한 입력변수에 대해서 기술하고 있는가?
2	P102_Describe_ProhibitedBehavior	소프트웨어가 실행해서는 안 되는 행위도 기술해야 하며 실행되는 환경까지도 기술하고 있는가?
3	P103_Define_OperatorInterface	운전원 연계 (키보드 입력, 제어 판넬, 제어기 및 디스플레이 위치 및 배치, 운전원 응답 및 의사결정 시간, 디스플레이 장치의 색상, 볼드체, 밑줄 및 깜빡임 사용, 메뉴 기법 등)가 충분히 정의되는가?
4	P104_Define_Interface_betweenProcess	각 프로세서간의 연계가 모두 정의되어있는가?
5	P105_Describe_StartCondition_ofFunc	각 기능적 요구사항이 해당 기능이 어떻게 시작되는가 기술되어 있는가?
6	P106_Possible_Implementation_inResource	필요한 안전관련 기능들이 기존의 활용 가능한 자원(예산, 스케쥴, 맨파워, 기기 및 소프트웨어 도구)을 가지고 정확하게 구현 가능한가?
7	P107_Practical_algorithm_techniques	명세된 모델이나 알고리즘, 또는 산술 기법(numerical techniques)들이 실질적이며 현재 사용되는 기법인가?
8	P108_Possible_ImplementOfQualityAttrib	소프트웨어에 대하여 명세된 품질 속성(quality attributes)이 각 소프트웨어 유니트 및 완전하게 통합된 소프트웨어 시스템에 대해 달성 가능한가?
9	P109_Describe_relation_amongVariables	감시변수와 입력변수 사이의 관계 및 출력변수와 제어변수 사이의 관계가 정확하게 기술되어 있는가?
10	P110_Describe_errCondition_CorrectiveAct	오류 조건(error conditions)이 요구되는 조치사항(corrective actions)과 함께 기술되어 있는가?
11	P111_Exist_verifying_BasicFunciton	운전원이 시스템의 기본 기능이 동작하는가를 확인할 수 있도록 허용하는 요구사항이 존재하는가?

노드명/노드확률테이블		질문
12	P112_Consistency_DisplayInfo	색상 사용, 디스플레이 스크린에 대한 정보 위치, 아이콘, 플래싱 신호 및 경보 신호에 대한 요구사항들이 일관적인 체계를 따르고 있는가?
13	P113_Describe_control_VarInPhysicalEnv	물리적 환경에 있는 변수들을 소프트웨어가 완전히 감시하고 제어하도록 명세되어 있는가?
14	P114_Exist_reportFunc_selfFaultInSystem	컴퓨터 시스템이 자체의 결함이나 고장을 운전원에게 보고할 수 있도록 하는 요구사항이 존재하는가?
15	P115_Describe_display_OperationVar	운전원에게 운전변수들을 정확하게 표시해 주고 수정할 수 있도록 하는 요구사항이 기술되어 있는가?
16	P116_Exist_description_OpReaction	의사결정을 하기 위해 가용한 시간을 포함해서 소프트웨어에서 발생한 메시지에 대해서 운전원의 반응을 기술하는 요구사항들이 있는가?
17	P117_Exist_ReqOfManualInterface	수동 연계가 규정된 안전 범위를 초과하여 기본적인 안전 조치사항을 지연시키지 않아야 한다는 요구사항이 존재하고 있는가?
18	P118_Describe_AllVar_fromSensor	각 센서로부터 오는 가능한 각 입력에 대해서 완전하게 기술하고 있는가?
19	P119_Describe_behavior_abnormalInput	SRS가 비정상적인 입력에 대한 소프트웨어의 거동(behavior)을 명시하고 있는가?
20	P120_Describe_RequiredInOutVar	각 기능적 요구사항이 그 기능에 의해 요구되는 입력변수와 출력변수들을 명시하고 있는가?
21	P121_Describe_actionItem_forErrRecovery	오류 극복(error recovery)을 위해 컴퓨터 시스템에서 요구되는 조치사항들이 완전하게 기술되어 있는가?
22	P122_Describe_ProcedureActionEvent	각 기능적 요구사항이 그 기능을 수행하는데 요구되는 태스크 순서, 조치사항 및 이벤트들을 명시하고 있는가?
23	P123_Describe_terminationCondition	각 기능적 요구사항이 종결 조건(termination conditions)이나 기능 완수 시 시스템 상태에 대해서 명시하고 있는가?
24	P124_Describe_allOutVar_fromFunc	기능들로부터 모든 출력변수들이 완전하게 기술되어 있는가?
25	P125_Describe_allOut_fromActuator	각 조작장치(actuator)로의 가능한 모든 출력을 기술하고 있는가?

노드명/노드확률테이블		질문
26	P126_Describe_OperatorCategories	예상되는 경험 수준에 따라 분류된 운전원들의 범주(categories)에 대해서 SRS에서 기술하고 있는가?
27	P127_Describe_SW_Interface	SRS에서 소프트웨어의 연계(하드웨어, 기성 소프트웨어, COTS 소프트웨어 및 운전원)에 대해서 모두 명시하고 있는가?
28	P128_Describe_allAction_forFailSafe	Fail-safe 조치사항에 대해서 컴퓨터 시스템에서 요구되는 모든 조치가 완전하게 기술되어 있는가?
29	P129_Describe_allOpMode	소프트웨어가 수행해야 하는 모든 운전모드들에 대해서 기술되어 있는가?
30	P130_Describe_operationalEnv_ofSW	SRS가 프로그램이 구동되어야 할 운전 환경(operational environment)에 대해서 기술하고 있는가?
31	P131_Describe_notToDoAction	SRS에서 소프트웨어가 수행하지 않아야 할 것에 대해서 언급하고 있는가?
32	P132_Describe_allAction_forAllOpMode	모든 운전 모드에 대해 컴퓨터 시스템에서 요구되는 모든 조치들이 완전하게 기술되어 있는가?
33	P133_Describe_Input_toFunc	기능에 대한 모든 입력이 완전하게 기술되어 있는가?
34	P134_Verify_ReqOfFR_ReqOfSRS	FR에기술된 모든 기능적 요구사항들이 SRS에 기능으로 기술되었는지를 확인한다
35	P135_Describe_InVarOfFunc	기능에 대한 모든 입력 변수들이 완전하게 기술되어 있는가?
36	P136_Describe_safeStart_SytemSW	시스템과 소프트웨어가 안전한 상태에서 시작되도록 기술되어 있는가?
37	P137_Describe_interlocksInitOperation	연동(interlocks)은 시스템 기동시에 초기화되거나 가동할 수 있도록 기술되어 있는가
38	P138_Update_PracticalProcessStatus	공정의 내부적인 소프트웨어 모델은 초기 기동과 일시적인 정지 후에 실질적인 공정 상태를 반영하도록 업데이트 되도록 되어 있는가?
39	P139_CorrectInit_systemFieldVar	모든 시스템과 현장 변수들이 클락을 포함해서 기동 시에 정확하게 초기화되도록 되어 있는가?
40	P140_SwBehavior_SWoffLine	정지 후 기동 전 또는 컴퓨터가 공정 (오프라인)에서 일시적으로 해제되었을 때 받은 입력 값에 대한 소프트웨어 거동을 명기하도록 되어 있는가?
41	P141_StopReq_faultOfInterfaceDevice	연계 장치 고장 시 위험한 기능들을 정지시킬 수 있도록 요구사항에서 기술하고 있는가?

노드명/노드확률테이블		질문
42	P142_Use_InfoOfSensor_SRS	센서로부터 오는 모든 정보가 SRS의 어떤 부분에서 사용되도록 되어 있는가?
43	P143_CheckAnswer_InputToSRS	SRS에서 입력되는 모든 값들이 체크되고 범위를 초과하거나 예상치 않은 이벤트 시에 대응조치가 기술되어 있는가?
44	P144_Bound_InputToTime	모든 입력들은 시간에 대해서 완전하게 bound되어 있는가? 제한치가 초과하거나 예상한 입력이 전해지지 않았을 경우에 올바른 거동이 기술되어 있는가?
45	P145_Followup_ExcessInput	SRS에서 과도한 입력(부하 가정에 대한 위배)에 대한 조치가 기술되어 있는가?
46	P146_Check_TimeChange_OutValue	SRS에서 안전-중요 출력 값들의 적절함과 위험한 값들에 대해 시간에 따른 변화를 체크하도록 하는 요구사항이 존재하는가?
47	P147_Describe_ReqOfInterface	S/W 인터페이스 완전성 분석을 위해 각각의 인터페이스 요구사항이 빠짐없이 기술되어 있는가?
48	P148_Include_PerforMeasure_InterfaceReq	각 인터페이스 요구사항이 데이터 형태와 성능 척도들 (타이밍, 대역폭, 정밀도, 안전성, 보안성)을 포함하는가?
49	P149_Describe_Functionality_FR	SRS와 FR에서 기능성 (알고리즘, 상태 및 모드 정의, 입/출력 검증, 예외 처리, 보고, 기록)에 대해서 기술되어 있는가?
50	P150_Describe_FefinitionOfProcess	SRS와 FR에서 프로세스 정의 및 스케줄링에 대해서 기술되어 있는가?
51	P151_Describe_HwSwUserInterface	SRS와 FR에서 하드웨어, 소프트웨어 및 사용자 인터페이스에 대한 설명이 기술되어 있는가?
52	P152_Describe_PerformanceMeasure_FR	SRS와 FR에서 성능 척도 (timing sizing, 속도, 용량, 정확도, 정밀도, 안전성, 보안성)에 대한 기술이 되어 있는가?
53	P153_Describe_ConfigData_FR	SRS와 FR에서 주요 형상 데이터에 대한 기술이 되어 있는가?
54	P154_Describe_SysDevSWcontrol_SRSfR	SRS와 FR에서 시스템, 장치 및 소프트웨어 제어 (초기화, 트랜잭션 및 상태 감시, 자가 시험)에 대한 기술이 되어 있는가?
55	P155_Satisfy_ConfigProcedure_SRSnIRS	완전성 검증을 위해서는 SRS와 IRS가 관련 형상관리 절차를 만족하는가?

◇ 일관성(Consistency) 검증

노드명/노드확률테이블		질문
P200_Consistency_1		일관성(Consistency) 검증
1	P201_Interchangable_ModelAlgorithm	SRS에서 명시된 모델, 알고리즘 및 계산 기법들이 수학적으로 서로 상호 일치(mutually consistent) 하는가?
2	P202_Interchangable_SccuracyOfInOutData	입력, 계산 및 출력 데이터들에 요구되는 정확도(accuracies)가 상호 호환성(mutually compatible)을 갖고 있는가?
3	P203_Consistency_toSystemReq	개별적인 요구사항들이 SDD(System Design Description) 및 SAR(Safety Analysis Report)의 요구사항들과 일치하는가?
4	P204_Cosistency_amongSimilarFunctions	유사한 기능들에 대한 요구사항들은 서로 상호 일치하는가?
5	P205_Follow_ConsistentWay_DisplayFactorReq	색상, 디스플레이 스크린에 대한 정보 위치, 아이콘, flashing 신호 및 altering 신호들 사용에 대한 요구사항들이 일관된 방식을 따르고 있는가?
6	P206_AnalysisDocument_InternalInconsistency	SRS가 내부 모순에 대해 분석이 수행되었고 이 분석에 대해서 문서화 되었는가?
7	P207_Consistency_ModelAlgorithmToRefData	SRS에서 명시된 모델, 알고리즘 및 계산 기법들이 적용 가능한 표준 참고문헌과 일치하는가?
8	P208_InOutputConsistency_RelatedReqOfOther	SRS에서 명시된 입력 및 출력 사양이 하드웨어 또는 기성 소프트웨어 등에 의해 부여된 연계 요구사항들과 일치하는가?
9	P209_ReqConsistency_WithOperationEnv	개별적인 요구사항들이 프로그램이 맞추어야 할 운전 환경에 대한 문서화된 기술사항과 알려진 성질들과 일치하고 있는가?
10	P210_Consistent_TermDefinition	SRS를 통해서 통일되고 일치되는 전문 용어 (terminologies) 및 정의(definitions)들을 사용하고 있는가?

◇ 정확성(Correctness) 검증

노드명/노드확률테이블		질문
P300_Correctness		정확성(Correctness) 검증
1	P301_Fit_InterfaceReq_SystemReq	외부 및 내부 소프트웨어 인터페이스 요구사항이 계통 요구사항의 문맥과 잘 부합 하는가?
2	P302_Satisfy_SWreq_SystemReq	시스템에 대한 제약사항 및 가정사항들을 고려하여 소프트웨어 요구사항들이 소프트웨어와 관련된 시스템 요구사항들을 모두 만족 하는가?
3	P303_Fit_SWreq_StandardsRegulation	소프트웨어 요구사항들이 표준, 참조, 규제, 정책, 프로젝트 운영 방침 등에 잘 부합 하는가?
4	P304_Verify_StatusSequenceChange_Code	적용분야의 전문지식, 시제품 결과, 공학적 원리 및 기타 근거와 결합된 논리 및 자료 흐름을 사용하는 원시코드 컴포넌트의 상태 순서 및 상태 변경에 대해서 검증하였는가?
5	P305_Satisfy_DataFlow_FunctionReq	데이터 및 제어흐름이 기능 및 성능요건을 만족하는가?
6	P306_Descirbe_UsageTypeOfData	데이터 사용처와 형식에 대한 기술이 되어 있는가?
7	P307_Describe_StartMethod_FunctionalReq	기능적 요구사항들이 각 기능이 어떻게 개시되는가를 정확하게 기술하고 있는가?
8	P308_Describe_InOutVar_forFunction	각 기능적 요구사항이 그 기능에 요구되는 입력변수와 출력변수를 정확하게 명시하고 있는가?
9	P309_Describe_JobProcedureEvent_forProcess	각 기능적 요구사항이 그 기능을 수행하는 데 요구되는 작업 순서, 행위 및 사건들을 정확하게 명시하고 있는가?
10	P310_Describe_SystemState_atTermination	각 기능적 요구사항이 종결 조건이나 기능의 종료 시 시스템의 상태에 대해 정확하게 명시하고 있는가?
11	P311_Perform_IndependentAnalysis	알고리즘의 정확성을 검증하기 위한 SRS에서 기술된 알고리즘에 대한 독립적 분석이 수행되었는가?

◇ 스타일(Style) 검증

노드명/노드확률테이블		질문
P400_Style		스타일(Style) 검증
1	P401_Classify_ReqAndSuppInfo	SRS가 소프트웨어 요구사항 자체와 기타 보완적 정보(설계 제약사항, 하드웨어 플랫폼, 코딩 표준 등)를 서로 구분하고 있는가?
2	P402_Organized_ClassOfFuncSpecAtMode	SRS의 기능적 명세 부분이 각 운전모드에 따라 요구사항들이 분류되도록 구성되어 있는가?
3	P403_Defined_ReqAtpeculiarPosition	각 요구사항들이 SRS내에 특정하고 또한 완전하게 어떤 한 위치에서 정의되어 있는가?
4	P404_Use_ClearDefinitionOfTerm	소프트웨어 요구사항 명세가 각 기술적 용어와 약어에 대해서 정확한 정의를 하고 있는가?
5	P405_Suitability_ReqToStandard	소프트웨어 요구사항 명세가 벤더 또는 소프트웨어 개발자에 의해 부여된 표준에 따르고 있는가?
6	P406_Divide_Req_DesignRestriction	SRS에서 요구사항과 설계 제약사항을 서로 구분하고 있는가?
7	P407_Describe_Justification_DesignRestriction	SRS에 포함된 각 설계와 각 시행 제약사항에 대해서 정당성(justification)에 대한 기술이 있는가?
8	P408_Complete_NoParagraph	SRS에서 빈 절, 구가 없이 완전한가?
9	P409_High_Understandability_SRSstructure	SRS의 구조와 형태가 이해성, 판독성, 수정성이 높은가?

◇ 추적성(Traceabiltiy) 검증

노드명/노드확률테이블		질문
P500_Traceability		추적성(Traceabiltiy) 검증
1	P501_Reverse_Traceability	각 요구사항들이 시스템 설계 기술(System Design Description)이나 안전분석보고서(Safety Analysis Report)내 특정 요소로 역방향 추적이 가능한가?
2	P502_ForwardTraceability_TotestValidation	각 요구사항들이 그들이 만족하는지를 확증하는데 사용될 특정한 시험(test) 또는 검증 기준(validation criteria)으로 순방향 추적이 가능한가?
3	P503_ForwardTraceability_toDesignElement	각 요구사항들이 특정 설계 요소로 순방향 추적이 가능한가?

◇ 명료성(Unambiguity) 검증

노드명/노드확률테이블		질문
P600_Unambiguity		비-모호성(Unambiguity) 검증
1	P601_Only_OneInterpretation	모든 요구사항이 오직 한가지로(in one and only one way) 해석 될 수 있는가
2	P602_Unambiguity_DescriptionOfFunction	기능설명이 애매모호하지 않는가?

◇ 확인가능성(Verifiability) 검증

노드명/노드확률테이블		질문
P700_Verifiability		확인가능성(Verifiability) 검증
1	P701_Testability_TimingReq	각 타이밍 요구사항이 시험 가능한가?
2	P702_Teatability_SecurityReq	각 보안성 요구사항이 시험 가능한가?
3	P703_Testability_ReliabilityAndAvailability	각 신뢰성 및 가용성 요구사항이 시험 가능한가?
4	P704_Testability_FuncReq	각 기능적 요구사항이 시험 가능한가?
5	P705_Testability_SafetyReq	각 안전성 요구사항이 시험 가능한가?

B. 원자로 보호계통 SW 요구사항 명세 검토를 위한 BBN의 노드확률테이블

B-1. Root node NPTs(Unconditional pdfs)

Node name \ State	Good	Poor
VnV_Process	0.5	0.5

Node name \ State	Good	Poor
Development_Process	0.5	0.5

Node name \ State	Low	Medium	High
Complexity	0.33	0.34	0.33

B-2. NPTs of High level network

P000_SRD_Development		Good		Poor	
SRS_VnV		Good	Poor	Good	Poor
T100_Software_Requirement_Spec	Acceptable	0.99	0.5	0.5	0.01
	Not_Acceptable	0.01	0.5	0.5	0.99

Development_Process		Good		Poor	
VnV_Process		Good	Poor	Good	Poor
CMM_Levle	< Level 3	0.99	0.5	0.5	0.01
	+> Levle 3	0.01	0.5	0.5	0.99

Complexity		Low		Medium		High	
VnV_Process		Good	Poor	Good	Poor	Good	Poor
SRS_VnV	Good	0.99	0.1	0.95	0.05	0.9	0.01
	Poor	0.01	0.9	0.05	0.95	0.1	0.99

Complexity		Low		Medium		High	
Development_Process		Good	Poor	Good	Poor	Good	Poor
P000_SRS_Development	Good	0.99	0.1	0.95	0.05	0.9	0.01
	Poor	0.01	0.9	0.05	0.95	0.1	0.99

T100_Software_Requirement_Spec		Acceptable	Not_Acceptable
F100_Accuracy	good	0.9	0.1
	bad	0.1	0.9

T100_Software_Requirement_Spec		Acceptable	Not_Acceptable
F200_Functionality	good	0.99	0.01
	bad	0.01	0.99

T100_Software_Requirement_Spec		Acceptable	Not_Acceptable
F300_Reliability	good	0.95	0.05
	bad	0.05	0.95

T100_Software_Requirement_Spec		Acceptable	Not_Acceptable
F400_Robustness	good	0.95	0.05
	bad	0.05	0.95

T100_Software_Requirement_Spec		Acceptable	Not_Acceptable
F500_Safety	good	0.99	0.01
	bad	0.01	0.99

T100_Software_Requirement_Spec		Acceptable	Not_Acceptable
F600_Security	good	0.9	0.1
	bad	0.1	0.9

T100_Software_Requirement_Spec		Acceptable	Not_Acceptable
F700_Timing	good	0.95	0.05
	bad	0.05	0.95

P000_SRD_Development		Acceptable	Not_Acceptable
P100_Completeness	good	0.99	0.01
	bad	0.01	0.99

P000_SRD_Development		Acceptable	Not_Acceptable
P200_Consistency	good	0.99	0.01
	bad	0.01	0.99

P000_SRD_Development		Acceptable	Not_Acceptable
P300_Correctness	good	0.99	0.01
	bad	0.01	0.99

P000_SRD_Development		Acceptable	Not_Acceptable
P400_Style	good	0.8	0.2
	bad	0.2	0.8

P000_SRD_Development		Acceptable	Not_Acceptable
P500_Traceability	good	0.99	0.01
	bad	0.01	0.99

P000_SRD_Development		Acceptable	Not_Acceptable
P600_Unambiguity	good	0.9	0.1
	bad	0.1	0.9

P000_SRD_Development		Acceptable	Not_Acceptable
P700_Verifiability	good	0.8	0.2
	bad	0.2	0.8

B-3. NPTs of low level networks

B-3-1. 기능특성 검증 항목의 NPTs

◇ 정확성 검증(Accuracy) 서브네트워크의 노드확률테이블

F100_Accuracy		good	bad
F101_accuracy_req_atNVariables: 수치 값을 갖는 각 입력변수 및 출력 변수에 대해서 정확도 요구사항이 존재하는가?	yes	0.95	0.05
	no	0.05	0.95

F100_Accuracy		good	bad
F102_accuracy_req_atVariables: 모든 입력과 출력 변수에 대하여 정확도 요구사항이 존재하는가?	yes	0.80	0.20
	no	0.20	0.80

F100_Accuracy		good	bad
F103_describe_quantitatively: 각 정확도 요건이 정량적으로 기술되어 있는가?	yes	0.80	0.20
	no	0.20	0.80

F100_Accuracy		good	bad
F104_describe_physical_unit: 각 정확도 요건에 물리적 단위가 기술되어 있는가?	yes	0.80	0.20
	no	0.20	0.80

F100_Accuracy		good	bad
F105_describe_error_range: 각 정확도 요건에 오차 허용범위가 포함되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

F100_Accuracy		good	bad
F106_define_data_type_size: 모든 정확도 요구사항들은 데이터 형식과 데이터 크기가 포함되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

◇ 기능성 검증 서브네트워크의 노드확률테이블

F200_Functionality		good	bad
F201_termination_req: 출력다운과 가동 중지 순서와 같은 종결(termination) 요구사항이 명세 되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

F200_Functionality		good	bad
F202_func_req_atMode: 시스템 설계 문서(SDD)와 안전분석보고서에서 식별된 모든 운전 모드들에 대한 기능 요구사항들이 완전하게 명세 되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

F200_Functionality		good	bad
F203_Include_start_condition_state: 모든 기능 요구사항들이 시작 조건 및 각 기능 개시에서의 시스템의 상태를 포함하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

F200_Functionality		good	bad
F204_Specify_input_output_atFunction: 기능 요구사항들이 각 기능에 요구되는 입, 출력 변수들을 모두 명세하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

F200_Functionality		good	bad
F205_Include_procedure_event_atFunc: 기능 요구사항들이 각 기능을 수행하는데 필요한 작업 순서, 조치사항, 이벤트 등을 포함하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

F200_Functionality		good	bad
F206_Include_termination_condition_state: 모든 기능 요구사항들이 종결 조건 및 각 기능 종결 시 시스템의 상태를 포함하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

F200_Functionality		good	bad
F207_Include_relation_reliability_safety: 기능 요구사항들이 시스템의 신뢰도 및 안전성에 대한 각 기능의 연관성을 직, 간접적으로 포함하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F200_Functionality		good	bad
F208_Describe_environmental_variables: SRS가 소프트웨어가 감시 또는 제어하는 물리적 환경에서의 변수(온도나 압력 등)를 식별하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F200_Functionality		good	bad
F_209_Described_inMathVariables: SRS가 물리적 환경의 변수들을 수학적 변수로 나타내고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F200_Functionality		good	bad
F210_Define_controlV_to_monitorV_inFunc: SRS가 제어변수(controlled variables)의 요구되는 행위들을 수학적 함수를 이용한 감시변수(monitored variables)로서 정의하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F200_Functionality		good	bad
F211_INclude_object_of_function: 기능 요구사항들이 각 기능의 목적을 포함하고 있는가?	yes	0.80	0.20
	no	0.20	0.80

F200_Functionality		good	bad
F212_Include_condition_of_operation: 기능 요구사항들이 각 기능을 동작하도록 하는 야기 조건(trigger conditions)을 포함하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F200_Functionality		good	bad
F213_Described_initial_req: 변수의 초기값, 기동 및 출력 상승 절차와 같은 초기화 요구사항들이 명시되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

◇ 신뢰성(Reliability) 검증 서브네트워크의 노드확률테이블

F300_Reliability		good	bad
F301_Derived_from_systemReq: 소프트웨어 신뢰성 요구사항이 시스템 설계사양(SDD)의 신뢰성 요구사항으로부터 도출되는가?	yes	0.90	0.10
	no	0.10	0.90

F300_Reliability		good	bad
F302_Defined_quantitatively: 소프트웨어 신뢰성 요구사항이 고장율이나 고장 기준에 대한 평균시간과 같이 정량적으로 정의되어 있는가?	yes	0.80	0.20
	no	0.20	0.80

F300_Reliability		good	bad
F303_Defined_fault_tolerance: 고장허용이나 점차적인 노후(graceful degradation) 등에 대한 요구사항이 정의되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F300_Reliability		good	bad
F304_Defined_reliabilityReq_atOpMode: 각 운전모드에 대한 신뢰성 및 가용성 요건이 주어졌는가?	yes	0.90	0.10
	no	0.10	0.90

F300_Reliability		good	bad
F305_Include_test_diagnostics_req: 소프트웨어 요구사항 명세가 시험 및 진단에 대한 요구사항을 포함하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

◇ 강인성(Robustness) 검증 서브네트워크의 노드확률테이블

F400_Robustness		good	bad
F401_Unexpected_msg_traffic: SRS가 예측하지 못한 메시지 교통량에 대한 소프트웨어의 행위를 명시하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

F400_Robustness		good	bad
F402_Unexpected_input: SRS가 예기치 않은, 부정확한 또는 부적절한 입력 데이터 또는 다른 비정상 조건하에서 소프트웨어 거동을 명세하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

F400_Robustness		good	bad
F403_Unexpected_behavior: SRS가 예기치 않은, 부정확한 또는 부적절한 하드웨어 및 소프트웨어 거동 하에서 소프트웨어 거동을 명세하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F400_Robustness		good	bad
F404_ProperAction_UncorrectState: SRS가 시스템 작동 상 임의의 절차에서 빠져 나온 후의 상태 체크와 부정확한 상태가 검출되었을 경우에 대한 적절한 조치를 요구하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

◇ 안전성(Safety) 검증 서브네트워크의 노드확률테이블

F500_Safety		good	bad
F501_SWcondition_hazardState: 시스템이 위험한 상태에 이르게 하는 소프트웨어의 조건이 SRS에서 명세되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

F500_Safety		good	bad
F502_InputCondition_forPrelude: SRS가 소프트웨어 초기 보호 조치(initiating protective actions)에 대한 전조(prelude)로서 필요한 입력 조건과 계산들을 명시하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F500_Safety		good	bad
F503_Describe_safe_unsafe_systemStatus: SRS가 시스템의 안전한 상태 및 비 안전 상태를 명시하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

F500_Safety		good	bad
F504_Define_validityCheck_Op_SensorIN: SRS에서 운전원과 센서 입력에 대한 검증 체크(validity checks)에 대해 정의하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F500_Safety		good	bad
F505_Classify_sensor_atSafety: SRS가 안전 중요도에 따라 센서와 actuator를 분류하고 있는가	yes	0.90	0.10
	no	0.10	0.90

F500_Safety		good	bad
F506_Describe_ActionItem_PlantDamage: SRS가 발전소 손상을 막기 위해 필요한 소프트웨어 조치사항(필요한 계산과 물리적인 백그라운드 포함)을 명세하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F500_Safety		good	bad
F507_Classify_function_atSafety: 소프트웨어 요구 사항 명세가 중요도에 따라 기능을 분류하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F500_Safety		good	bad
F508_Describe_ActionItem_Emergency: SRS가 원자로의 비상정지를 수행하기 위해 필요한 소프트웨어 조치사항(필요한 계산과 물리적인 백그라운드 포함)을 명세하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F500_Safety		good	bad
F509_SWscheme_forCommonModeFailure: 시스템 설계 사양(SDD) 및 안전분석보고서(SAR)에 의해 요구되는 잠재적인 공통모드 고장에 대한 소프트웨어의 대처방안이 명시되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

◇ 보안성(Security) 검증 서브네트워크의 노드확률테이블

F600_Security		good	bad
F601_Protection_from_unauthorizedUser: SRS가 승인되지 않은 사람이 소프트웨어 시스템을 다루는 것을 금지하는 요구사항을 부여하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

F600_Security		good	bad
F602_Restriction_ofAccess: SRS가 운전원, 매니져 및 기타 직원에 대한 접근제한(access restriction)을 부여하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F600_Security		good	bad
F603_Consistency_ofSecurityReq: 보안성 요구사항이 전체적으로 상호 일관성(mutually consistent)이 있는가?	yes	0.90	0.10
	no	0.10	0.90

F600_Security		good	bad
F604_Classify_atSeriousness: 컴퓨터 시스템에 대한 잠재적 보안 위협이 심각성과 가능성에 따라 식별 및 분류되고 문서화되는가?	yes	0.90	0.10
	no	0.10	0.90

F600_Security		good	bad
F605_Protection_UnauthorizedChange: SRS가 소프트웨어 시스템에 대한 승인되지 않은 변경을 방지하는 요구사항을 부여하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

F600_Security		good	bad
F606_Solve_securityHazarde: SRS에서 보안 위협을 강조하기 위한 요구사항을 명시하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

◇ 타이밍(Timing) 검증 서브네트워크의 노드확률테이블

F700_Timing		good	bad
F701_Describe_storageTolerances: 소프트웨어 요구사항 명세가 저장장소 허용(storage tolerances)을 명시하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F702_Describe_timingFuncReq: 소프트웨어 요구사항 명세가 시간에 중요한 기능과 그 기능에 대한 시간 요건을 명시하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

F700_Timing		good	bad
F703_Prediction_ofProcessQuantity: 소프트웨어에 대한 처리 량 예상이 주어져 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F704_Describe_ReqOfMemorySize: 메모리 크기 요구사항이 명백하게 표현되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F705_Deterministic_timing_schedulee: 소프트웨어 시스템이 결정론적 타이밍으로 동작하도록 되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

F700_Timing		good	bad
F706_Descirbe_MaxWaitTime: Error로 표시되어 예외처리로 들어가기 전에, 컴퓨터가 처음 입력을 기다릴 최대시간이 명시되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F707_Define_ActionOfNoInput: 정해진 시간 동안 입력이 없을 때 시스템이 취할 행동이 정해져 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F708_Describe_timing_requirement: 타이밍 요구사항이 명백하게 표현되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F709_Describe_timing_tolerancet: 소프트웨어 요구 사항 명세가 타이밍 허용치를 명시하고 있는가?	yes	0.95	0.05
	no	0.05	0.99

F700_Timing		good	bad
F710_TimingReq_atOpMode: 타이밍 요구사항이 각 운전모드에 대하여 모두 명시되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F711_Describe_TimeBounds: 명시된 허용 시간한계 (Time bounds)를 벗어나 들어오는 입력에 대한 시스템의 행동이 각 운전모드에 대해 명시되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F712_Describe_minmax_ArrivalRate: 입력의 최대 최소 도착률이 명시되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F713_Describe_minman_interruptR: 인터럽트의 최대, 최소 발생률이 명시되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F714_Describe_Response_Overflow: 예상 입력률 (또는 인터럽트 발생률)을 초과 했을 때 시스템 응답이 명시 되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F715_Notice_PerformanceLoss: 과부하 상태에 대해 시스템이 성능 감소를 보일 때, 이러한 성능감소가 점진적인가? 또 이 상황이 운전원에게 통보 되는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F716_Describe_maxOutRate: 최대 출력률이 명시되어 있고 연결된 장비와 호환하는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F717_Describe_Response_OverOutR: 예상 출력률을 초과 했을 때 시스템 응답이 명시 되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

F700_Timing		good	bad
F718_Describe_MsgOverflow: 사용자 인터페이스 명세가 정보의 출력이 사용자의 정보 이해력을 초과하는 발생을 방지하도록 명세하는가?	yes	0.90	0.10
	no	0.10	0.90

B-3-2. 공정특성 검증 항목의 NPTs

◇ 완전성(Completeness) 검증 서브네트워크의 노드확률테이블

P100_Completeness		good	bad
P101_Describe_all_ModeInputVariables: 시스템에 요구되는 모든 행위가 모든 운전모드 및 모든 가능한 입력변수에 대해서 기술하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P102_Describe_ProhibitedBehavior: 소프트웨어가 실행해서는 안 되는 행위도 기술해야 하며 실행되는 환경까지도 기술하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P103_Define_OperatorInterface: 운전원 연계 (키보드 입력, 제어 판넬, 제어기 및 디스플레이 위치 및 배치, 운전원 응답 및 의사결정 시간, 디스플레이 장치의 색상, 볼드체, 밑줄 및 깜빡임 사용, 메뉴 기법 등)가 충분히 정의되는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P104_Define_Interface_betweenProcess: 각 프로세서간의 연계가 모두 정의되어있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P105_Describe_StartCondition_ofFunc: 각 기능적 요구사항이 해당 기능이 어떻게 시작되는가 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P106_Possible_Implementation_inResources: 필요한 안전관련 기능들이 기존의 활용 가능한 자원(예산, 스케쥴, 맨파워, 기기 및 소프트웨어 도구)을 가지고 정확하게 구현 가능한가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P107_Practical_algorithm_techniques: 명세된 모델이나 알고리즘, 또는 산술 기법(numerical techniques)들이 실질적이며 현재 사용되는 기법(the state of the art)인가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P108_Possible_ImplementOfQualityAttrib: 소프트웨어에 대하여 명세된 품질 속성(quality attributes)이 각 소프트웨어 유니트 및 완전하게 통합된 소프트웨어 시스템에 대해 달성 가능한가?	yes	0.80	0.20
	no	0.20	0.80

P100_Completeness		good	bad
P109_Describe_relation_amongVariables: 감시변수와 입력변수 사이의 관계 및 출력변수와 제어변수 사이의 관계가 정확하게 기술되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P110_Describe_errCondition_CorrectiveActr: 오류 조건(error conditions)이 요구되는 조치사항(corrective actions)과 함께 기술되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P111_Exist_verifying_BasicFunciton: 운전원이 시스템의 기본 기능이 동작하는가 확인할 수 있도록 허용하는 요구사항이 존재하는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P112_Consistency_DisplayInfo: 색상 사용, 디스플레이 스크린에 대한 정보 위치, 아이콘, 플래싱 신호 및 경보 신호에 대한 요구사항들이 일관적인 체계를 따르고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P113_Describe_control_VarInPhysicalEnv: 물리적 환경에 있는 변수들을 소프트웨어가 완전히 감시하고 제어하도록 명세 되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P114_Exist_reportFunc_selfFaultInSystem: 컴퓨터 시스템이 자체의 결함이나 고장을 운전원에게 보고할 수 있도록 하는 요구사항이 존재하는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P115_Describe_display_OperationVar: 운전원에게 운전변수들을 정확하게 표시해주고 수정할 수 있도록 하는 요구사항이 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P116_Exist_description_OpReaction: 의사결정을 하기 위해 가용한 시간을 포함해서 소프트웨어에서 발생한 메시지에 대해서 운전원의 반응을 기술하는 요구사항들이 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P117_Exist_ReqOfManualInterface: 수동 연계가 규정된 안전 범위를 초과하여 기본적인 안전 조치사항을 지연시키지 않아야 한다는 요구사항이 존재하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P118_Describe_AllVar_fromSensor: 각 센서로부터 오는 가능한 각 입력에 대해서 완전하게 기술하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P119_Describe_behavior_abnormalInput: SRS가 비정상적인 입력에 대한 소프트웨어의 거동(behavior)을 명시하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P120_Describe_RequiredInOutVar: 각 기능적 요구사항이 그 기능에 의해 요구되는 입력변수와 출력변수들을 명시하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P121_Describe_actionItem_forErrRecovery: 오류 극복 (error recovery)을 위해 컴퓨터 시스템에서 요구되는 조치사항들이 완전하게 기술되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P122_Describe_ProcedureActionEvent: 각 기능적 요구사항이 그 기능을 수행하는 데 요구되는 태스크 순서, 조치사항 및 이벤트들을 명시하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P123_Describe_terminationCondition: 각 기능적 요구사항이 종결 조건(termination conditions)이나 기능 완수 시 시스템 상태에 대해서 명시하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P124_Describe_allOutVar_fromFunc: 기능들로부터 모든 출력변수들이 완전하게 기술되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P125_Describe_allOut_fromActuator: 각 조작장치(actuator)로의 가능한 모든 출력을 기술하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P126_Describe_OperatorCategories: 예상되는 경험 수준에 따라 분류된 운전원들의 범주(categories)에 대해서 SRS에서 기술하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P127_Describe_SW_Interface: SRS에서 소프트웨어의 연계(하드웨어, 기성 소프트웨어, COTS 소프트웨어 및 운전원)에 대해서 모두 명시하고 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P128_Describe_allAction_forFailSafe: Fail-safe 조치사항에 대해서 컴퓨터 시스템에서 요구되는 모든 조치가 완전하게 기술되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P129_Describe_allOpMode: 소프트웨어가 수행해야 하는 모든 운전 모드들에 대해서 기술되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P130_Describe_operationalEnv_ofSW: SRS가 프로그램이 구동되어야 할 운전 환경(operational environment)에 대해서 기술하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P131_Describe_notToDoAction: SRS에서 소프트웨어가 수행하지 않아야 할 것에 대해서 언급하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P132_Describe_allAction_forAllOpMode: 모든 운전 모드에 대해 컴퓨터 시스템에서 요구되는 모든 조치들이 완전하게 기술되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P133_Describe_Input_toFunc: 기능에 대한 모든 입력이 완전하게 기술되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P134_Verify_ReqOfFR_ReqOfSRS: FR에기술된 모든 기능적 요구사항들이 SRS에 기능으로 기술되었는지를 확인한다	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P135_Describe_InVarOfFunc: 기능에 대한 모든 입력 변수들이 완전하게 기술되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P136_Describe_safeStart_SytemSW: 시스템과 소프트웨어가 안전한 상태에서 시작되도록 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P137_Describe_interlocksInitOperation: 연동(interlocks)은 시스템 기동시에 초기화되거나 가동할 수 있도록 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P138_Update_PracticalProcessStatus: 공정의 내부적인 소프트웨어 모델은 초기 기동과 일시적인 정지 후에 실질적인 공정 상태를 반영하도록 업데이트 되도록 되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P139_correctInit_systemFieldVar: 모든 시스템과 현장 변수들이 클락을 포함해서 기동 시에 정확하게 초기화되도록 되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P140_swBehavior_SWoffLine: 정지 후 기동 전 또는 컴퓨터가 공정(오프라인)에서 일시적으로 해제되었을 때 받은 입력 값에 대한 소프트웨어 거동을 명기하도록 되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P141_stopReq_faultOfInterfaceDevice: 연계 장치 고장 시 위험한 기능들을 정지시킬 수 있도록 요구사항에서 기술하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

P100_Completeness		good	bad
P142_use_InfoOfSensor_SRS: 센서로부터 오는 모든 정보가 SRS의 어떤 부분에서 사용되도록 되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P143_checkAnswer_InputToSRS: SRS에서 입력되는 모든 값들이 체크되고 범위를 초과하거나 예상치 않은 이벤트 시에 대응조치가 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P144_bound_InputToTime: 모든 입력들은 시간에 대해서 완전하게 bound되어 있는가? 제한치가 초과하거나 예상한 입력이 전해지지 않았을 경우에 올바른 거동이 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P145_followup_excessInput: SRS에서 과도한 입력(부하 가정에 대한 위배)에 대한 조치가 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P146_check_timeChange_OutValue: SRS에서 안전-중요 출력 값들의 적절함과 위험한 값들에 대해 시간에 따른 변화를 체크하도록 하는 요구사항이 존재하는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P147_Describe_ReqOfInterface: S/W 인터페이스 완전성 분석을 위해 각각의 인터페이스 요구사항이 빠짐없이 기술되어 있는가?	yes	0.99	0.01
	no	0.01	0.99

P100_Completeness		good	bad
P148_include_PerforMeasure_InterfaceReq: 각 인터페이스 요구사항이 데이터 형태와 성능 척도들 (타이밍, 대역폭, 정밀도, 안전성, 보안성)을 포함하는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P149_Describe_functionality_FR: SRS와 FR에서 기능성 (알고리즘, 상태 및 모드 정의, 입/출력 검증, 예외 처리, 보고, 기록)에 대해서 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P150_Describe_definitionOfProcess: SRS와 FR에서 프로세스 정의 및 스케줄링에 대해서 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P151_Describe_HwSwUserInterface: SRS와 FR에서 하드웨어, 소프트웨어 및 사용자 인터페이스에 대한 설명이 기술되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P152_Describe_PerformanceMeasure_FR: SRS와 FR에서 성능 척도 (timing sizing, 속도, 용량, 정확도, 정밀도, 안전성, 보안성)에 대한 기술이 되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P153_Describe_ConfigData_FR: SRS와 FR에서 주요 형상 데이터에 대한 기술이 되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P154_Describe_SysDevSWcontrol_SRSfR: SRS와 FR에서 시스템, 장치 및 소프트웨어 제어 (초기화, 트랜잭션 및 상태 감시, 자가 시험)에 대한 기술이 되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P100_Completeness		good	bad
P155_satisfy_ConfigProcedure_SRSnIRS: 완전성 검증을 위해서는 SRS와 IRS가 관련 형상관리 절차를 만족하는가?	yes	0.90	0.10
	no	0.10	0.90

◇ 일관성(Consistency) 검증 서브네트워크의 노드확률테이블

P200_Consistency		good	bad
P201_Interchangable_modelAlgorithm: SRS에서 명시된 모델, 알고리즘 및 계산 기법들이 수학적으로 서로 상호 일치(mutually consistent) 하는가?	yes	0.95	0.05
	no	0.05	0.95

P200_Consistency		good	bad
P202_Interchangable_accuracyOfInOutData: 입력, 계산 및 출력 데이터들에 요구되는 정확도(accuracies)가 상호 호환성(mutually compatible)을 갖고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P200_Consistency		good	bad
P203_Consistency_toSystemReq: 개별적인 요구사항들이 SDD(System Design Description) 및 SAR(Safety Analysis Report)의 요구사항들과 일치하는가?	yes	0.99	0.01
	no	0.01	0.99

P200_Consistency		good	bad
P204_Cosistency_amongSimilarFunctions: 유사한 기능들에 대한 요구사항들은 서로 상호 일치하는가?	yes	0.99	0.01
	no	0.01	0.99

P200_Consistency		good	bad
P205_follow_consistentWay_DisplayFactorReq: 색상, 디스플레이 스크린에 대한 정보 위치, 아이콘, flashing 신호 및 altering 신호들 사용에 대한 요구사항들이 일관된 방식을 따르고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P200_Consistency		good	bad
P206_AnalysisDocument_internalInconsistency: SRS가 내부 모순(internal contradictions)에 대해 분석이 수행되었고 이 분석에 대해서 문서화되었는가?	yes	0.80	0.20
	no	0.20	0.80

P200_Consistency		good	bad
P207_Consistency_modelAlgorithmToRefData: SRS에서 명시된 모델, 알고리즘 및 계산 기법들이 적용 가능한 표준 참고문헌과 일치하는가?	yes	0.90	0.10
	no	0.10	0.90

P200_Consistency		good	bad
P208_InOutputConsistency_RelatedReqOfOther: SRS에서 명시된 입력 및 출력 사양이 하드웨어 또는 기성 소프트웨어 등에 의해 부여된 연계 요구사항들과 일치 하는가?	yes	0.99	0.01
	no	0.01	0.99

P200_Consistency		good	bad
P209_ReqConsistency_WithOperationEnv: 개별적인 요구사항들이 프로그램이 맞추어야 할 운전 환경에 대한 문서화된 기술사항과 알려진 성질들과 일치하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P200_Consistency		good	bad
P210_Consistent_termDefinition: SRS를 통해서 통일되고 일치되는 전문 용어 (terminologies) 및 정의(definitions)들을 사용하고 있는가	yes	0.90	0.10
	no	0.10	0.90

◇ 정확성(Correctness) 검증 서브네트워크의 노드확률테이블

P300_Correctness		good	bad
P301_fit_InterfaceReq_SystemReq: 외부 및 내부 소프트웨어 인터페이스 요구사항이 계통 요구사항의 문맥과 잘 부합 하는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P302_satisfy_SWreq_SystemReq: 시스템에 대한 제약사항 및 가정사항들을 고려하여 소프트웨어 요구사항들이 소프트웨어와 관련된 시스템 요구사항들을 모두 만족 하는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P303_fit_SWreq_StandardsRegulation: 소프트웨어 요구사항들이 표준, 참조, 규제, 정책, 프로젝트 운영 방침 등에 잘 부합 하는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P304_verify_StatusSequenceChange_Code: 적용분야의 전문지식, 시제품 결과, 공학적 원리 및 기타 근거와 결합된 논리 및 자료 흐름을 사용하는 원시코드 컴포넌트의 상태 순서 및 상태 변경에 대해서 검증하였는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P305_satisfy_DataFlow_FunctionReq: 데이터 및 제어흐름이 기능 및 성능요건을 만족하는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P306_Descirbe_UsageTypeOfData: 데이터 사용처와 형식에 대한 기술이 되어 있는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P307_Describe_StartMethod_FunctionalReq: 기능적 요구사항들이 각 기능이 어떻게 개시되는가를 정확하게 기술하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P308_Describe_InOutVar_forFunction: 각 기능적 요구사항이 그 기능에 요구되는 입력변수와 출력변수를 정확하게 명시하고 있는가?	yes	0.99	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P309_Describe_JobProcedureEvent_forProcess: 각 기능적 요구사항이 그 기능을 수행하는 데 요구되는 작업 순서, 행위 및 사건들을 정확하게 명시하고 있는가?	yes	0.99	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P310_Describe_SystemState_atTermination: 각 기능적 요구사항이 종결 조건이나 기능의 종료 시 시스템의 상태에 대해 정확하게 명시하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P300_Correctness		good	bad
P311_perform_IndependentAnalysis: 알고리즘의 정확성을 검증하기 위한 SRS에서 기술된 알고리즘에 대한 독립적 분석이 수행되었는가?	yes	0.99	0.01
	no	0.01	0.99

◇ 스타일(Style) 검증 서브네트워크의 노드확률테이블

P400_Consistency		good	bad
P401_Classify_ReqAndSuppInfo: SRS가 소프트웨어 요구사항 자체와 기타 보완적 정보(설계 제약사항, 하드웨어 플랫폼, 코딩 표준 등)를 서로 구분하고 있는가?	yes	0.95	0.05
	no	0.05	0.95

P400_Consistency		good	bad
P402_Organized_ClassOfFuncSpecAtMode: SRS의 기능적 명세 부분이 각 운전모드에 따라 요구사항들이 분류되도록 구성되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

P400_Consistency		good	bad
P403_Defined_ReqAtpeculiarPosition: 각 요구사항들이 SRS내에 특정하고 또한 완전하게 어떤 한 위치에서 정의되어 있는가?	yes	0.95	0.05
	no	0.05	0.95

P400_Consistency		good	bad
P404_Use_clearDefinitionOfTerm: 소프트웨어 요구사항 명세가 각 기술적 용어와 약어에 대해서 정확한 정의를 하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P400_Consistency		good	bad
P405_Suitability_ReqToStandard: 소프트웨어 요구사항 명세가 벤더 또는 소프트웨어 개발자에 의해 부여된 표준에 따르고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P400_Consistency		good	bad
P406_Divide_Req_DesignRestriction: SRS에서 요구사항과 설계 제약사항을 서로 구분하고 있는가?	yes	0.90	0.10
	no	0.10	0.90

P400_Consistency		good	bad
P407_Describe_Justification_DesignRestriction: SRS에 포함된 각 설계와 각 시행 제약사항에 대해서 정당성(justification)에 대한 기술이 있는가?	yes	0.90	0.10
	no	0.10	0.90

P400_Consistency		good	bad
P408_Complete_NoParagraph: SRS에서 빈 절이나 구가 없이 완전한가?	yes	0.90	0.10
	no	0.10	0.90

P400_Consistency		good	bad
P409_High_Understandability_SRSstructure: SRS 의 구조와 형태가 이해성, 판독성, 수정성이 높은가?	yes	0.90	0.10
	no	0.10	0.90

◇ 추적성(Traceabiltiy) 검증 서브네트워크의 노드확률테이블

P500_Traceability		good	bad
P501_Reverse_traceability: 각 요구사항들이 시스템 설계 기술(System Design Description)이나 안전분석보고서(Safety Analysis Report)내 특정 요소로 역방향 추적이 가능한가?	yes	0.99	0.01
	no	0.01	0.99

P500_Traceability		good	bad
P502_ForwardTraceability_TotestValidation: 각 요구사항들이 그들이 만족하는지를 확증하는데 사용될 특정한 시험(test) 또는 검증 기준(validation criteria)으로 순방향 추적이 가능한가?	yes	0.95	0.05
	no	0.05	0.95

P500_Traceability		good	bad
P503_ForwardTraceability_toDesignElement: 각 요구사항들이 특정 설계 요소로 순방향 추적이 가능한가?	yes	0.99	0.01
	no	0.01	0.99

◇ 명료성(Unambiguity) 검증 서브네트워크의 노드확률테이블

P600_Unambiguity		good	bad
P601_Only_oneInterpretation: 모든 요구사항이 오직 한가지로(in one and only one way) 해석 될 수 있는가?	yes	0.99	0.01
	no	0.01	0.99

P600_Unambiguity		good	bad
P602_Unambiguity_DescriptionOfFunction: 기능설명이 애매모호하지 않는가?	yes	0.90	0.10
	no	0.10	0.90

◇ 확인가능성(Verifiability) 검증 서브네트워크의 노드확률테이블

P700_Verifiability		good	bad
P701_Testability_timingReq: 각 타이밍 요구사항이 시험 가능한가?	yes	0.90	0.10
	no	0.10	0.90

P700_Verifiability		good	bad
P702_Teatability_securityReq: 각 보안성 요구사항이 시험 가능한가?	yes	0.90	0.10
	no	0.10	0.90

P700_Verifiability		good	bad
P703_Testability_ReliabilityAndAvailability: 각 신뢰성 및 가용성 요구사항이 시험 가능한가?	yes	0.90	0.10
	no	0.10	0.90

P700_Verifiability		good	bad
P704_Testability_funcReq: 각 기능적 요구사항이 시험 가능한가?	yes	0.90	0.10
	no	0.10	0.90

P700_Verifiability		good	bad
P705_Testability_safetyReq: 각 안전성 요구사항이 시험 가능한가?	yes	0.90	0.10
	no	0.10	0.90

C. 원자로 보호계통 소프트웨어 요구사항 명세 체크리스트의 입력 값

C-1. 기능특성 검증 항목의 평가 값

◇ 정확성 검증(Accuracy)에 관한 질문의 평가 값

F100: 정확성(accuracy) 검증에 대한 질문	Yes	No
F101: 수치 값을 갖는 각 입력변수 및 출력 변수에 대해서 정확도 요구사항이 존재하는가?		0.9
F102: 모든 입력과 출력 변수에 대하여 정확도 요구사항이 존재하는가?		0.9
F103: 각 정확도 요건이 정량적으로 기술되어 있는가?		0.9
F104: 각 정확도 요건에 물리적 단위가 기술되어 있는가?		0.9
F105: 각 정확도 요건에 오차 허용범위가 포함되어 있는가?		0.9
F106: 모든 정확도 요구사항들은 데이터 형식과 데이터 크기가 포함되어 있는가?	0.9	

◇ 기능성 검증에 관한 질문의 평가 값

F200: 기능성(Functionality) 검증	Yes	No
F201: 출력다운과 가동 중지 순서와 같은 종결(termination) 요구사항이 명세 되어 있는가?		0.99
F202: 시스템 설계 문서(SDD)와 안전분석보고서에서 식별된 모든 운전 모드들에 대한 기능 요구사항들이 완전하게 명세 되어 있는가?		0.9
F203: 모든 기능 요구사항들이 시작 조건 및 각 기능 개시에서의 시스템의 상태를 포함하고 있는가?		0.9
F204: 기능 요구사항들이 각 기능에 요구되는 입, 출력 변수들을 모두 명세하고 있는가?	0.99	
F205: 기능 요구사항들이 각 기능을 수행하는데 필요한 작업 순서, 조치사항, 이벤트 등을 포함하고 있는가?	0.99	
F206: 모든 기능 요구사항들이 종결 조건 및 각 기능 종결 시 시스템의 상태를 포함하고 있는가?		0.9
F207: 기능 요구사항들이 시스템의 신뢰도 및 안전성에 대한 각 기능의 연관성을 직, 간접적으로 포함하고 있는가?		0.9
F208: SRS가 소프트웨어가 감시 또는 제어하는 물리적 환경에서의 변수(온도나 압력 등)를 식별하고 있는가?	0.9	
F209: SRS가 물리적 환경의 변수들을 수학적 변수로 나타내고 있는가?	0.9	
F210: SRS가 제어변수(controlled variables)의 요구되는 행위들을 수학적 함수를 이용한 감시변수(monitored variables)로서 정의하고 있는가?	0.9	
F211: 기능 요구사항들이 각 기능의 목적을 포함하고 있는가?		0.9
F212: 기능 요구사항들이 각 기능을 동작하도록 하는 야기 조건(trigger conditions)을 포함하고 있는가?		0.9
F213: 변수의 초기값, 기동 및 출력 상승 절차와 같은 초기화 요구사항들이 명시되어 있는가?		0.9

◇ 신뢰성(Reliability) 검증에 관한 질문의 평가 값

F300: 신뢰성(Reliability) 검증에 대한 질문	Yes	No
F301: 소프트웨어 신뢰성 요구사항이 시스템 설계사양(SDD)의 신뢰성 요구사항으로부터 도출되는가?		0.9
F302: 소프트웨어 신뢰성 요구사항이 고장율이나 고장 기준에 대한 평균시간과 같이 정량적으로 정의되어 있는가?		0.9
F303: 고장허용이나 점차적인 노후(graceful degradation) 등에 대한 요구사항이 정의되어 있는가?		0.9
F304: 각 운전모드에 대한 신뢰성 및 가용성 요건이 주어졌는가?		0.9
F305: 소프트웨어 요구사항 명세가 시험 및 진단에 대한 요구사항을 포함하고 있는가?	0.9	

◇ 강인성(Robustness) 검증에 관한 질문의 평가 값

강인성(Robustness) 검증에 대한 질문	Yes	No
F401: SRS가 예기치 못한 메시지 트래픽 상황에서 소프트웨어 거동을 명세하고 있는가?		0.9
F402: SRS가 예기치 않은, 부정확한 또는 부적절한 입력 데이터 또는 다른 비정상 조건하에서 소프트웨어 거동을 명세하고 있는가?	0.9	
F403: SRS가 예기치 않은, 부정확한 또는 부적절한 하드웨어 및 소프트웨어 거동 하에서 소프트웨어 거동을 명세하고 있는가?	0.9	
F404: SRS가 시스템 작동 상 임의의 절차에서 빠져 나온 후의 상태 체크와 부정확한 상태가 검출되었을 경우에 대한 적절한 조치를 요구하고 있는가?		0.9

◇ 안전성(Safety) 검증에 관한 질문의 평가 값

안전성(Safety) 검증에 대한 질문	Yes	No
F501: 시스템이 위험한 상태에 이르게 하는 소프트웨어의 조건이 소프트웨어 요구사항 명세에 명시되어 있는가?		0.99
F502: SRS가 소프트웨어 초기 보호 조치(initiating protective actions)에 대한 전조(prelude)로서 필요한 입력 조건과 계산들을 명시하고 있는가?		0.9
F503: SRS가 시스템의 안전한 상태 및 비 안전 상태를 명시하고 있는가		0.99
F504: SRS에서 운전원과 센서 입력에 대한 검증 체크(validity checks)에 대해 정의하고 있는가?	0.99	
F505: SRS가 안전 중요도에 따라 센서와 actuator를 분류하고 있는가		0.9
F506: SRS가 발전소 손상을 막기 위해 필요한 소프트웨어 조치사항(필요한 계산과 물리적인 백그라운드 포함)을 명세하고 있는가?	0.9	
F507: 소프트웨어 요구 사항 명세가 중요도에 따라 기능을 분류하고 있는가?	0.9	
F508: SRS가 원자로의 비상정지를 수행하기 위해 필요한 소프트웨어 조치사항(필요한 계산과 물리적인 백그라운드 포함)을 명세하고 있는가?		
F509: 시스템 설계 사양(SDD) 및 안전분석보고서(SAR)에 의해 요구되는 잠재적인 공통모드 고장에 대한 소프트웨어의 대처방안이 명시되어 있는가		0.9

◇ 보안성(Security) 검증에 관한 질문의 평가 값

보안성(Security) 검증에 대한 질문	Yes	No
F601: SRS가 승인되지 않은 사람이 소프트웨어 시스템을 다루는 것을 금지하는 요구사항을 부여하고 있는가?		0.99
F602: SRS가 운전원, 매니져 및 기타 직원에 대한 접근제한(access restriction)을 부여하고 있는가?		0.9
F603: 보안성 요구사항이 전체적으로 상호 일관성(mutually consistent)이 있는가?		0.9
F604: 컴퓨터 시스템에 대한 잠재적 보안 위협이 심각성과 가능성에 따라 식별 및 분류되고 문서화되는가?		0.9
F605: SRS가 소프트웨어 시스템에 대한 승인되지 않은 변경을 방지하는 요구사항을 부여하고 있는가?		0.99
F606: SRS에서 보안 위협을 강조하기 위한 요구사항을 명시하고 있는가?		0.9

◇ 타이밍(Timing) 검증에 관한 질문의 평가 값

타이밍(Timing) 검증에 대한 질문	Yes	No
F701: 소프트웨어 요구사항 명세가 저장장소 허용(storage tolerances)을 명시하고 있는가?		0.9
F702: 소프트웨어 요구사항 명세가 시간에 중요한 기능과 그 기능에 대한 시간 요건을 명시하고 있는가?	0.99	
F703: 소프트웨어에 대한 처리 량 예상이 주어져 있는가?		0.9
F704: 메모리 크기 요구사항이 명백하게 표현되어 있는가?		0.9
F705: 소프트웨어 시스템이 결정론적 타이밍으로 동작하도록 되어 있는가?	0.99	
F706: Error로 표시되어 예외처리로 들어가기 전에, 컴퓨터가 처음 입력을 기다릴 최대시간이 명시되어 있는가?		0.9
F707:정해진 시간 동안 입력이 없을 때 시스템이 취할 행동이 정해져 있는가?		0.9
F708: 타이밍 요구사항이 명백하게 표현되어 있는가?		0.9
F709: 소프트웨어 요구 사항 명세가 타이밍 허용치를 명시하고 있는가?		0.9
F710: 최대, 최소 타이밍 요구사항이 각 운전모드에 대하여 모두 명시되어 있는가?	0.9	
F711: 명시된 허용 시간한계 (Time bounds)를 벗어나 들어오는 입력에 대한 시스템의 행동이 각 운전모드에 대해 명시되어있는가?	0.9	
F712: 입력의 최대 최소 도착률이 명시되어 있는가?		0.9
F713: 인터럽트의 최대, 최소 발생률이 명시되어 있는가?		0.9
F714: 예상 입력률 (또는 인터럽트 발생률)을 초과 했을 때 시스템 응답이 명시 되어 있는가?		0.9
F715: 과부하 상태에 대해 시스템이 성능 감소를 보일 때, 이러한 성능감소가 점진적인가? 또 이 상황이 운전원에게 통보 되는가?		0.9
F716: 최대 출력률이 명시되어 있고 연결된 장비와 호환하는가?		0.9
F717: 예상 출력률을 초과 했을 때 시스템 응답이 명시되어 있는가?		0.9
F718: 사용자 인터페이스 명세가 정보의 출력이 사용자의 정보 이해력을 초과하는 발생을 방지하도록 명세 하는가?		0.9

C-2. 공정특성 검증 항목의 평가 값

◇ 완전성(Completeness) 검증에 관한 질문의 평가 값

완전성(Completeness) 검증에 대한 질문	Yes	No
P101: 시스템에 요구되는 모든 행위가 모든 운전모드 및 모든 가능한 입력변수에 대해서 기술하고 있는가?	0.99	
P102: 소프트웨어가 실행해서는 안 되는 행위도 기술해야 하며 실행되는 환경까지도 기술하고 있는가?		0.9
P103: 운전원 연계 (키보드 입력, 제어 판넬, 제어기 및 디스플레이 위치 및 배치, 운전원 응답 및 의사결정 시간, 디스플레이 장치의 색상, 볼드체, 밑줄 및 깜빡임 사용, 메뉴 기법 등)가 충분히 정의되는가?	0.99	
P104: 각 프로세서간의 연계가 모두 정의되어있는가?	0.99	
P105: 각 기능적 요구사항이 해당기능이 어떻게 시작되는가 기술되어 있는가?		0.9
P106: 필요한 안전관련 기능들이 기존의 활용 가능한 자원(예산, 스케쥴, 맨파워, 기기 및 소프트웨어 도구)을 가지고 정확하게 구현 가능한가?		0.9
P107: 명세된 모델이나 알고리즘, 또는 산술 기법(numerical techniques)들이 실질적이며 현재 사용되는 기법(the state of the art)인가?	0.9	
P108: 소프트웨어에 대하여 명세된 품질 속성(quality attributes)이 각 소프트웨어 유니트 및 완전하게 통합된 소프트웨어 시스템에 대해 달성 가능한가?		0.8
P109: 감시변수와 입력변수 사이의 관계 및 출력변수와 제어변수 사이의 관계가 정확하게 기술되어 있는가?	0.99	
P110: 오류 조건(error conditions)이 요구되는 조치사항(corrective actions)과 함께 기술되어 있는가?	0.9	
P111: 운전원이 시스템의 기본 기능이 동작하는가를 확인할 수 있도록 허용하는 요구사항이 존재하는가?	0.9	
P112: 색상 사용, 디스플레이 스크린에 대한 정보 위치, 아이콘, 플래싱 신호 및 경보 신호에 대한 요구사항들이 일관적인 체계를 따르고 있는가?		0.9
P113: 물리적 환경에 있는 변수들을 소프트웨어가 완전히 감시하고 제어하도록 명세되어 있는가?	0.99	
P114: 컴퓨터 시스템이 자체의 결함이나 고장을 운전원에게 보고할 수 있도록 하는 요구사항이 존재하는가?		0.9
P115: 운전원에게 운전변수들을 정확하게 표시해주고 수정할 수 있도록 하는 요구사항이 기술되어 있는가?	0.9	
P116: 의사결정을 하기 위해 가용한 시간을 포함해서 소프트웨어에서 발생한 메시지에 대해서 운전원의 반응을 기술하는 요구사항들이 있는가?		0.9
P117: 수동 연계가 규정된 안전 범위를 초과하여 기본적인 안전 조치사항을 지연시키지 않아야 한다는 요구사항이 존재하고 있는가?	0.9	
P118: 각 센서로부터 오는 가능한 각 입력에 대해서 완전하게 기술하고 있는가?	0.99	

완전성(Completeness) 검증에 대한 질문	Yes	No
P119: SRS가 비정상적인 입력에 대한 소프트웨어의 거동(behavior)을 명시하고 있는가?	0.9	
P120: 각 기능적 요구사항이 그 기능에 의해 요구되는 입력변수와 출력변수들을 명시하고 있는가?	0.99	
P121: 오류 극복(error recovery)을 위해 컴퓨터 시스템에서 요구되는 조치사항들이 완전하게 기술되어 있는가?	0.9	
P122: 각 기능적 요구사항이 그 기능을 수행하는 데 요구되는 태스크 순서, 조치사항 및 이벤트들을 명시하고 있는가?	0.9	
P123: 각 기능적 요구사항이 종결 조건(termination conditions)이나 기능 완수 시 시스템 상태에 대해서 명시하고 있는가?		0.9
P124: 기능들로부터 모든 출력변수들이 완전하게 기술되어 있는가??	0.99	
P125: 각 조작장치(actuator)로의 가능한 모든 출력을 기술하고 있는가?	0.99	
P126: 예상되는 경험 수준에 따라 분류된 운전원들의 범주(categories)에 대해서 SRS에서 기술하고 있는가?		0.8
P127: SRS에서 소프트웨어의 연계(하드웨어, 기성 소프트웨어, COTS 소프트웨어 및 운전원)에 대해서 모두 명시하고 있는가?		0.99
P128: Fail-safe 조치사항에 대해서 컴퓨터 시스템에서 요구되는 모든 조치가 완전하게 기술되어 있는가?	0.9	
P129: 소프트웨어가 수행해야 하는 모든 운전모드들에 대해서 기술되어 있는가?	0.99	
P130: SRS가 프로그램이 구동되어야 할 운전 환경(operational environment)에 대해서 기술하고 있는가?		0.9
P131: SRS에서 소프트웨어가 수행하지 않아야 할 것에 대해서 언급하고 있는가?		0.9
P132: 모든 운전 모드에 대해 컴퓨터 시스템에서 요구되는 모든 조치들이 완전하게 기술되어 있는가?	0.99	
P133: 기능에 대한 모든 입력이 완전하게 기술되어 있는가?		0.99
P134: FR에 기술된 모든 기능적 요구사항들이 SRS에 기능으로 기술되었는지를 확인한다?		0.99
P135: 기능에 대한 모든 입력 변수들이 완전하게 기술되어 있는가?		0.99
P136: 시스템과 소프트웨어가 안전한 상태에서 시작되도록 기술되어 있는가		0.9
P137: 연동(interlocks)은 시스템 기동 시에 초기화되거나 가동할 수 있도록 기술되어 있는가?		0.9
P138: 공정의 내부적인 소프트웨어 모델은 초기 기동과 일시적인 정지 후에 실질적인 공정 상태를 반영하도록 업데이트 되도록 되어 있는가?		0.9
P139: 모든 시스템과 현장 변수들이 클락을 포함해서 기동 시에 정확하게 초기화되도록 되어 있는가?		0.9
P140: 정지 후 기동 전 또는 컴퓨터가 공정 (오프라인)에서 일시적으로 해제되었을 때 받은 입력 값에 대한 소프트웨어 거동을 명기하도록 되어 있는가?		0.9
P141: 연계 장치 고장 시 위험한 기능들을 정지시킬 수 있도록 요구사항에서 기술하고 있는가?		0.9

완전성(Completeness) 검증에 대한 질문	Yes	No
P142: 센서로부터 오는 모든 정보가 SRS의 어떤 부분에서 사용되도록 되어 있는가?	0.99	
P143: SRS에서 입력되는 모든 값들이 체크되고 범위를 초과하거나 예상치 않은 이벤트 시에 대응조치가 기술되어 있는가?	0.9	
P144: 모든 입력들은 시간에 대해서 완전하게 bound되어 있는가? 제한치가 초과하거나 예상한 입력이 전해지지 않았을 경우에 올바른 거동이 기술되어 있는가?		0.9
P145: SRS에서 과도한 입력(부하 가정에 대한 위배)에 대한 조치가 기술되어 있는가?		0.9
P146: SRS에서 안전-중요 출력 값들의 적절함과 위험한 값들에 대해 시간에 따른 변화를 체크하도록 하는 요구사항이 존재하는가?		0.9
P147: S/W 인터페이스 완전성 분석을 위해 각각의 인터페이스 요구사항이 빠짐없이 기술되어 있는가?	0.99	
P148: 각 인터페이스 요구사항이 데이터 형태와 성능 척도들 (타이밍, 대역폭, 정밀도, 안전성, 보안성)을 포함하는가?		0.9
P149: SRS와 FR에서 기능성 (알고리즘, 상태 및 모드 정의, 입/출력 검증, 예외 처리, 보고, 기록)에 대해서 기술되어 있는가?		0.9
P150: SRS와 FR에서 프로세스 정의 및 스케줄링에 대해서 기술되어 있는가?		0.9
P151: SRS와 FR에서 하드웨어, 소프트웨어 및 사용자 인터페이스에 대한 설명이 기술되어 있는가?		0.9
P152: SRS와 FR에서 성능 척도 (timing sizing, 속도, 용량, 정확도, 정밀도, 안전성, 보안성)에 대한 기술이 되어 있는가?		0.9
P153: SRS와 FR에서 주요 형상 데이터에 대한 기술이 되어 있는가?		0.9
P154: SRS와 FR에서 시스템, 장치 및 소프트웨어 제어 (초기화, 트랜잭션 및 상태 감시, 자가 시험)에 대한 기술이 되어 있는가?		0.9
P155: 완전성 검증을 위해서는 SRS와 IRS가 관련 형상관리 절차를 만족하는가?		0.9

◇ 일관성(Consistency) 검증에 관한 질문의 평가 값

일관성(Consistency)에 대한 질문	Yes	No
P201: SRS에서 명시된 모델, 알고리즘 및 계산 기법들이 수학적으로 서로 상호 일치(mutually consistent) 하는가?	0.9	
P202: 입력, 계산 및 출력 데이터들에 요구되는 정확도(accuracies)가 상호 호환성(mutually compatible)을 갖고 있는가?		0.9
P203: 개별적인 요구사항들이 SDD(System Design Description) 및 SAR(Safety Analysis Report)의 요구사항들과 일치하는가?	0.99	
P204: 유사한 기능들에 대한 요구사항들은 서로 상호 일치하는가?		0.99
P205: 색상, 디스플레이 스크린에 대한 정보 위치, 아이콘, flashing 신호 및 altering 신호들 사용에 대한 요구사항들이 일관된 방식을 따르고 있는가?		0.9
P206: SRS가 내부 모순 (internal contradictions)에 대해 분석이 수행되었고 이 분석에 대해서 문서화되었는가?	0.9	
P207: SRS에서 명시된 모델, 알고리즘 및 계산 기법들이 적용 가능한 표준 참고문헌과 일치하는가?	0.9	
P208: SRS에서 명시된 입력 및 출력 사양이 하드웨어 또는 기성 소프트웨어 등에 의해 부여된 연계 요구사항들과 일치 하는가?		0.99
P209: 개별적인 요구사항들이 프로그램이 맞추어야 할 운전 환경에 대한 문서화된 기술사항과 알려진 성질들과 일치하고 있는가?	0.9	
P210: SRS를 통해서 통일되고 일치되는 전문 용어 (terminologies) 및 정의 (definitions)들을 사용하고 있는가?		0.9

◇ 정확성(Correctness) 검증에 관한 질문의 평가 값

P300: 정확성(Correctness) 에 대한 질문	Yes	No
P301: 외부 및 내부 소프트웨어 인터페이스 요구사항이 계통 요구사항의 문맥과 잘 부합 하는가?		0.9
P302: 시스템에 대한 제약사항 및 가정사항들을 고려하여 소프트웨어 요구사항들이 소프트웨어와 관련된 시스템 요구사항들을 모두 만족 하는가?		0.9
P303: 소프트웨어 요구사항들이 표준, 참조, 규제, 정책, 프로젝트 운영 방침 등에 잘 부합 하는가?		0.9
P304: 적용분야의 전문지식, 시제품 결과, 공학적 원리 및 기타 근거와 결합된 논리 및 자료 흐름을 사용하는 원시코드 컴포넌트의 상태 순서 및 상태 변경에 대해서 검증하였는가?		0.9
P305: 데이터 및 제어흐름이 기능 및 성능요건을 만족하는가?	0.9	
P306: 데이터 사용처와 형식에 대한 기술이 되어 있는가?		0.9
P307: 기능적 요구사항들이 각 기능이 어떻게 개시되는가를 정확하게 기술하고 있는가?		0.9
P308: 각 기능적 요구사항이 그 기능에 요구되는 입력변수와 출력변수를 정확하게 명시하고 있는가?		0.99
P309: 각 기능적 요구사항이 그 기능을 수행하는 데 요구되는 작업 순서, 행위 및 사건들을 정확하게 명시하고 있는가?		0.99
P310: 각 기능적 요구사항이 종결 조건이나 기능의 종료 시 시스템의 상태에 대해 정확하게 명시하고 있는가?		0.9
P311: 알고리즘의 정확성을 검증하기 위한 SRS에서 기술된 알고리즘에 대한 독립적 분석이 수행되었는가?	0.99	

◇ 스타일(Style) 검증에 관한 질문의 평가 값

스타일(Style) 검증에 대한 질문	Yes	No
P401: SRS가 소프트웨어 요구사항 자체와 기타 보완적 정보(설계 제약사항, 하드웨어 플랫폼, 코딩 표준 등)를 서로 구분하고 있는가?		0.9
P402: SRS의 기능적 명세 부분이 각 운전모드에 따라 요구사항들이 분류되도록 구성되어 있는가?	0.9	
P403: 각 요구사항들이 SRS내에 특정하고 또한 완전하게 어떤 한 위치에서 정의되어 있는가?	0.9	
P404: 소프트웨어 요구사항 명세가 각 기술적 용어와 약어에 대해서 정확한 정의를 하고 있는가?		0.9
P405: 소프트웨어 요구사항 명세가 벤더 또는 소프트웨어 개발자에 의해 부여된 표준에 따르고 있는가?	0.9	
P406: SRS에서 요구사항과 설계 제약사항을 서로 구분하고 있는가?		0.9
P407: SRS에 포함된 각 설계와 각 시행 제약사항에 대해서 정당성(justification)에 대한 기술이 있는가?		0.9
P408: SRS에서 빈 절, 구가 없이 완전한가?		0.9
P409: SRS 의 구조와 형태가 이해성, 판독성, 수정성이 높은가?	0.9	

◇ 추적성(Traceabiltiy) 검증에 관한 질문의 평가 값

추적성(Traceabiltiy) 검증에 대한 질문	Yes	No
P501: 각 요구사항들이 시스템 설계 기술(System Design Description)이나 안전분석보고서(Safety Analysis Report)내 특정 요소로 역방향 추적이 가능한가?		0.99
P502: 각 요구사항들이 그들이 만족하는지를 확증하는데 사용될 특정한 시험(test) 또는 검증 기준(validation criteria)으로 순방향 추적이 가능한가?	0.9	
P503: 각 요구사항들이 특정 설계 요소로 순방향 추적이 가능한가?		0.99

◇ 명료성(Unambiguity) 검증에 관한 질문의 평가 값

명료성(Unambiguity) 검증에 대한 질문	Yes	No
P601: 모든 요구사항이 오직 한가지로(in one and only one way) 해석 될 수 있는가?		0.99
P602: 기능설명이 애매모호하지 않는가?		0.9

◇ 확인가능성(Verifiability) 검증에 관한 질문의 평가 값

확인가능성(Verifiability) 검증에 대한 질문	Yes	No
P701: 각 타이밍 요구사항이 시험 가능한가?		0.9
P702: 각 보안성 요구사항이 시험 가능한가?		0.9
P703: 각 신뢰성 및 가용성 요구사항이 시험 가능한가?		0.9
P704: 각 기능적 요구사항이 시험 가능한가?	0.9	
P705: 각 안전성 요구사항이 시험 가능한가?	0.9	

D. 기능 특성과 공정 특성 검증 항목의 14개 특성 평가 값

D-1. 기능 특성의 평가

◇ 정확도(Accuracy)

정확도 요건	정확도 검토의견	입력 값
정확도 요구사항은 모든 입력과 출력에 대하여 부여되어야 하며, 수치적으로 물리적 단위와 오차 허용 범위를 포함하여 기술한다. 또한 각 입력 및 울력의 자료형과 자료크기가 포함되어야 한다.	모든 입력 및 출력에 대하여 물리적 단위와 오차 범위를 포함한 수치적 기술이 나타나 있지 않다. 각 입력 및 출력의 타입에 대해서는 시스템적인 관점에서의 타입 - 예를 들어 디지털 입력인지 아날로그 입력인지 - 은 요구사항 명세서가 참조하고 있는 연계사양서에 잘 명세되어 있으나 소프트웨어적 관점에서의 데이터타입에 대한 명세는 전무한 상태이다. 데이터의 크기에 대한 명세도 현재는 나타나 있지 않다.	0.2

◇ 기능성(Functionality)

기능성 요건	기능성 검토의견	입력 값
기능성은 각 운전 모드에서 수행되어야 할 운전이 완전히 기술되는 것을 요구하고 있다. 기능은 기능에 대한 입력, 기능에 의해서 수행되는 변환(transformations) 및 기능에 의해서 발생되는 출력으로 기술되어야 한다.	전반적으로 비교논리 프로세서, 동시논리 프로세서, 자동시험 및 연계 프로세서의 각 기능들을 상세 명세 수준까지 잘 기술하고 있으며 각 기능에 필요한 입력 및 발생되는 출력에 대해서도 잘 명세하고 있다. 그러나 일부 기능의 상세 명세가 빠져 있으며 (예: 비교논리 프로세서 박동신호 논리, AD conversion 논리, 운전우회상태 결정 논리) 기술된 상세 논리 중에서도 일부 고려해야 할 사항들 (예: 비교논리 예비 트립 기능에서도 신호 검증 부분이 있어야 할 것으로 보임)이 나타나있지 않은 경우도 있었다. 또한 입력 및 출력이 모두 정의되어 있기는 하나 그들 각각의 속성들 데이터 타입, source 나 destination 에 대해서 시스템적 관점에 대해서만 기술하고 있어서 소프트웨어적 관점에서 그러한 특성들을 명세할 필요가 있다고 생각된다	0.4

◇ 신뢰성(Reliability)

신뢰성 요건	신뢰성 검토의견	입력값
신뢰성은 고장 허용 및 고장모	입력 모듈 고장으로 인한 비정상적 입력에 대한	0.2

드에 대한 모든 요구사항들이 각 운전모드에 대하서 충분히 기술되도록 요구한다. 컴퓨터 시스템 고장으로부터 해석 및 복구에 대한 요구사항을 포함하는 하드웨어와 소프트웨어 고장을 취급하기 위한 소프트웨어 요구사항들이 제공되어야 한다. 온라인 서비스 시험 및 진단에 대한 요구사항들이 제공되어야 한다.	대처방법이나 프로세서 모듈의 고장에 대한 조치는 요구사항으로서 언급하고 있으나, 개별 point의 stuck 이나 watchdog timer의 고장, 노외중성자속 감시계통의 고장 시 대처 방안에 대해서는 언급하고 있지 않다.	

◇ 강인성(Robustness)

강인성 요건	강인성 검토의견	입력값
강인성에서는 예기치 않은, 부정확한 또는 부적절한 입력, 하드웨어 양상 또는 소프트웨어 양상 하에서 소프트웨어 양상을 모두 명세할 것을 요구한다. 예기치 않은 높은 또는 낮은 메시지 트래픽 하에서 소프트웨어의 양상이 특별한 관심사이다.	입력변수의 유효성 여부를 판단하는 논리가 기술되어 있으나 예비트립 논리에는 signal validation 논리가 표현되어 있지 않으며 좀 더 상세한 기술이 필요할 것으로 보인다. 현재는 신호가 valid 인지 invalid 인지만 판단하고 있는데. 입력 신호의 range, type, unit 등을 바탕으로 신호의 유효성 여부를 판단하는 과정에 대한 상세한 기술이 필요하다. 하드웨어나 소프트웨어의 오류 및 고장에 대해서는 적절한 감지 및 경보 요구사항을 기술하고 있으며 그러한 고장이 계통 수준의 안전 기능을 방해하지 못하도록 하는 요구사항도 기술하고 있다.	0.6

◇ 안전성(Safety)

안전성 요건	안전성 검토의견	입력값
안전성은 안전의 중요도에 따라 소프트웨어 기능, 운전 절차, 입력, 출력을 분류하도록 하고 있다. 안전에 중요한 요구사항은 SRS에서 식별되어야 한다. 안전 항목의 식별은 안전분석보고서 요구사항뿐만 아니라 Reg. Guide 1.152에서 기술된 비정상 조건 및 이벤트에 대해서도 포함해야 한다.	시스템의 hazardous state를 야기 시키는 소프트웨어 조건, 예를 들어 - 순환적 의존관계 - 서로 다른 계열 사이의 호출 - Function의 정상적 개시 및 완료를 방해하는 조건 등에 대해 identify하고 있지 않다.(그러나 이것은 FMEA나 PSAR에서 다루어야 할 내용이 아	0.4

	닌지?) 또한 계열 1과 2의 응용 프로그램은 동일한 것을 사용한다고 되어있는데 이것이 common mode failure를 일으키는 원인이 되지 않는지 분석할 필요가 있다. 그 밖에 ATIP에서 *5.3.1.2 ATIP이 하나의 PM으로 이루어졌다면 자신이 고장일 때 PM:ERR 신호를 발생시킬 수 없는 경우는 발생하지 않는지에 대해 검토할 필요가 있다.	

◇ 보안성(Security)

보안성 요건	보안성 검토의견	입력값
보안성은 컴퓨터 시스템에 대한 보안 위협을 식별하고 심각성(severity)과 가능성(likelihood)에 따라 분류할 것을 요구한다. 소프트웨어가 이와 같은 위협을 감지, 방지 또는 완화시키는데 필요한 조치사항들이 접근통제 제한을 포함해서 명시되어야 한다.	보안성에 대한 언급 없음	0.0

◇ 타이밍(Timing)

타이밍 요건	타이밍 검토의견	입력 값
타이밍에서는 특정 타이밍 제약사항 하에서 운전되어야 하는 기능들이 식별되고 타이밍 기준이 각각에 대해서 명기되어야 한다. 타이밍 기준은 각 운전 모드에 대해서 제공되어야 한다. 타이밍 요구사항은 안전조치사항에 대한 stimulus와 response 사이의 시간 지연이 정상 및 예견되는 고장 조건 하에서 결정적이어야 한다. BTP HICB-21에서는 실시간 수행도에 대해서 추가적인 절차를 제공하고 있다.	모든 논리들의 behavior를 기술함에 있어 정적인 관점을 취하고 있어서 timing에 대한 고려사항을 찾아 볼 수 없으며 타이밍에 대한 고려가 없이는 소프트웨어의 behavior가 비결정적이 될 수 있어서 이에 대한 보완이 필요하다고 사료된다.	0.2

D-2. 공정 특성 평가

◇ 완전성(Completeness)

완전성 요건	완전성 검토의견	입력 값
완전성에서는 전산 시스템에서 요구되는 모든 행위들이 모든 운전 모드와 모든 가능한 입력 변수들의 값에 대해서 충분히 기술되어야 함을 요구하고 있다. SRS는 소프트웨어가 수행되지 않아야 할 모든 행위들도 기술해야 한다. 소프트웨어가 돌아가는 운전 환경이 기술되어야 한다. 소프트웨어가 감시되고 제어되어야 할 물리적 환경 내 모든 변수들이 충분히 명세되어야 한다.	일부 기능의 상세 명세가 기술도지 않았으며 입출력의 정의가 완전하지 않았다. o General -입력의 source와 출력의 destination에 대한 기술이 빈약하거나 전혀 없음. o Bistable Processor -그림 5.1-1에 표현된 기능 블록 각각에 대한 상세명세를 기술하고 있으나, 박동신호 논리에 대한 상세 논리가 없음 -그림 5.1-1에는 없으나 추가적으로 AD conversion에 대한 상세논리가 필요할 것으로 사료됨. -그림 5.1-3의 예비트립 논리에도 signal validation이 있어야 하지 않는지? -5.1.3.2의 2항 트립채널우회신호를 받아서 전송하는 것도 하나의 function인데 5.1.4절에 빠져 있음. -5.1.4.7.1 운전우회상태 결정에 대한 상세 논리 없음. -5.1.4.7.1 운전우회상태 결정에 대한 상세 논리가 없는 이유로, 정상운전에서 운전우회 상태로 전이되는 조건에 대한 명세가 완전하지 못함. -온라인 상태에서 설정치 변화가 일어나는 조건에 대해서는 상세논리로 잘 기술되어 있으나 오프라인 상태에서 EWS로설정치를 변화시키는 과정에 대한 명세는 필요치 않은가? o ATIP -그림 5.3-2: 논리가 어떻게 시작되는지에 대한 명세 없음 -그림 5.3-13: 오차와 관련된 논리에서 설정치는 고정치이지만 공정변수는 가변치이므로 최대값	0.3

	과 최소값이 존재해야 하는데, 이에 대한 기술이 없음	

◇ 일관성(Consistency)

일관성 요건	일관성 검토의견	입력값
일관성은 소프트웨어 요구사항 명세의 내용이 시스템 요구사항 및 설계와 일관되는가를 요구한다. 일관성은 다음과 같은 점검 항목으로 검증한다. 요구사항 자체의 일관성은 모든 용어들과 개념들이 일관되게 문서화 되었는가, 기능의 상호작용과 가정이 일관되는가, 소프트웨어 요구사항 들간의 일관성이 유되는가 및 시스템 요구사항과 일관되는가를 검증하는 것이다.	o 일반 의견 -신호 및 데이터의 정확성 자체가 정의되어 있지 않아 입력, 계산 및 출력 자료들에 요구되는 정확성들이 상호 호환이 가능한가를 확인할 수 없었다. -신호 정의의 일관성 부족: 같은 신호 (값)으로 보이나 서로 다른 이름들을 사용하는 경우가 명세 전체에서 빈번히 발견됨 o 일관성10(용어 일관성) -channel error, module error, value error (5.1.4.1.1, 5.1.4.2.1, 5.1.4.3.1) 채널 오류, 모듈 오류, 공정변수값 오류(?) -모듈 에러, 체널 에러, 공정변수의 valid 모듈 오류, 채널 오류, 공정변수의 유효성 -trip set-point, trip hysterisis, trip logic, pre-trip set-point, pre-trip hysterisis, bypass, time delay 트립 설정치, 트립 히스테리시스, 트립 논리, 예비트립 설정치, 예비트립 히스테리시스, 운전우회상태, 시간 지연 -5.3 절에 사용되는 '캐비닛운전원모듈' 등과 같은 고유명사의 띄어 쓰기 -'자동시험 및 프로세서 모듈' '자동시험 및 연계프로세서 모듈', '연계 및 시험 프로세서' '통신 및 연계시험 프로세서', '에러' '오류' 으로 변경 -통신망의 용어 일관성 : ICN 채널내부통신망, ICDN 채널간 데이터 통신망, SDL 안전데이터링크 등으로 영어를 사용하지 말고, 한글어로 사용하여 일관성 유지 -본문 중 ESF-CCS, RTSG, COM 은 해당되는	0.5

	한글사용하여 용어 일관성 유지 (ESF은 ESF-CCS로 변경) -용어의 일관성 유지 : 건전성 감시 및 진단, 수동개시 자동시험, 수동시험 o General -신호 및 데이터의 정확성 자체가 정의되어 있지 않아 입력, 계산 및 출력 자료들에 요구되는 정확성들이 상호 호환이 가능한가를 확인할 수 없었다. -신호 정의의 일관성 부족: 같은 신호 (값)으로 보이나 서로 다른 이름들을 사용하는 경우가 명세 전체에서 빈번히 발견됨. o Bistable Processor -DS 101 표 1의 입력신호명과 SRS 표 4-1의 트립신호명 사이에 일관성 없음. -표 4-1의 No 15, 16: DS 101에의하면 NR은 고압력, WR은 고고압력임. 그러나, SRS에는 반대로 기술됨 o ATIP -전체적으로 자연어 spec과 NuSCR spec사이의 추적성이 부족함 (예: 입/출력이 무엇을 의미하는가가 추적이 안 됨. 각 기능에 대한 명세가 자연어 spec의 어디에 해당하는가가 나타나지 않음) -입/출력의 의미에 대해 자연어 spec과 NuSCR 사이에 추적이 안 됨. -5.3.2 자동시험 및 연계프로세서 입력: IR101과의 일관성 위해 BP, CP, OM's, ILC 및 ESF-CCS, 캐비닛 기기, x-ATIP's들로부터 입력신호를 받는다는 것을 명시 바람. -IR101의 표 6.3.3에는 자체 프로세서 상태 입력에 대한 언급이 없음. -IR101과의 일관성 측면에서 5.3.3에 아날로그 출력에 대해 기술할 필요가 있다고 생각됨.	

	-5.3.4.1.1: IR101에는 COM으로부터의 박동신호 입력이 없음. -5.3.4.1.1의 출력들이 IR101에 정의되어 있지 않음. -5.3.4.1.2, 5. 출력: IR101 표 6.3.6을 참조하고 있는 것으로 생각되나 정확히 표의 어떤 신호인지 대응되지 않음.	

◇ 정확성(Correctness)

정확성 요건	정확성 검토의견	입력 값
정확성 검증의 목표는 전산 시스템에서 요구되는 action에 대한 기술사항에 결점이 없어야 할 것과 그 외의 다른 오구사항들은 기술되지 않아야 함을 요구한다.	o Bistable processor - 5.1.4.1 고정설정치 하강트립 (fixed setpoint rising trip)을 5.1.4.1 고정설정치 하강트립(fixed setpoint falling trip)으로 정정 요망 - 31페이지와 32페이지의 delta T 구분 요망 - 5.1.4.3.3, 5.1.4.4.2,에서 'Module_Error' -> 'f_Module_Error'로 정정 요망 - 그림 5.1-20 'th_SURCE_SECTION' -> 'th_SOURCE_SELECTION'으로 정정 요망 - 그림 5.1-3의 예비트립 논리에도 signal validation이 있어야 함 - 표 4-1 No 15, 16: NR은 고압력, WR은 고고압력임 - 그림 4-2 입출력의 시작/도착점이 부정확함 (ex. SOE 시작점?) - 그림 4-2 Network 이름이 빠진 부분이 있음 o Coincidence processor - 5.2.4.5에서 LCB가 아니라 LSB 아닌가? o ATIP - 5.3.1에서 인용한 참고문서 1.4.2가 reference에 없음 - 5.3.1.1에서 '연동되어 있어야 한다'라는 표현이 모호함	0.2

	- 5.3.1.2 ATIP이 하나의 PM으로 이루어졌다면 자신이 고장일 때 PM:ERR 신호를 발생시킬 수 없는 경우는 발생하지 않는가?	

◇ 스타일(Style)

스타일 요건	스타일 검토의견	
스타일은 SRS의 내용이 이해 가능할 것(understandable)을 요구한다	명세서의 전체적인 구성은 각 기능별로 잘 나뉘어져 있으나 신호 정의의 일관성 부족과 각 논리간의 선후과계 설명 부족으로 인해 understandability가 부족한 경향이 있다.	0.5

◇ 추적성(Traceability)

추적성 요건	추적성 검토의견	
추적성은 SRS 상의 요구사항들과 안전 시스템 요구사항 및 설계 사이의 양방향 추적(two-way trace)이 가능할 것을 요구한다. 추적성은 다음과 같은 점검항목으로 검증한다. SRS내 각 요구사항으로부터 이 요구사항이 만족하는지를 확인하기 위해 사용되는 특정 인스펙션, 분석 또는 시험으로부터의 순방향 추적을 포함해서 SRS 내 각 요구사항과 소프트웨어 설계 사이의 양쪽 방향으로의 추적이 되어야 한다.	전반적으로 시스템 레벨의 설계 명세 내용과 소프트웨어 레벨의 요구사항 및 소프트웨어 요구사항의 정형 명세 사이의 순방향, 역방향 추적이 용이하나, ATIP의 경우 전체적으로 자연어 명세와 NuSCR 명세 사이의 추적성이 부족하다. (예: 입출력이 무엇을 의미하는가가 추적이 안됨. 각 기능에 대한 명세가 자연어 명세의 어디에 해당하는가가 나타나지 않음)	0.2

◇ 명료성(Unambiguity)

명료성 요건	명료성 검토의견	입력 값
명료성은 각 소프트웨어 요구사항 또는 모든 요구사항들이 전체적으로 단 한가지의 해석을 가질 것을 요구한다.	전체적으로 몇몇 요구사항들을 제외하고 명료성을 가진다. o Bistable processor	0.1

	- 5.1.4.2.2 "최저값으로 설정된 트립 및 예비트립 설정치는 공정변수가 최저값으로 설정되기 바로 전의 트립 및 에비트립 설정치에 도달할 때까지는 계속 최적값을 유지한다."라는 요구사항을 이해하기 힘듬 o ATIP - 5.3.1.1에서 '연동되어 있어야 한다'라는 표현이 모호함. 무엇과 어떻게 연동되어야 하는 것인가?	

◇ 확인가능성(Verifiability)

확인가능성 요건	확인가능성 검토의견	입력값
확인 가능성은 각 소프트웨어 요구사항이 만족되는가를 결정하기 위한 특정한 분석, 검토 또는 시험을 수행하는 것이 가능할 것을 요구한다.	각 요구사항들이 정형적(혹은 수학적)으로 표현되어 있어서 전반적인 확인가능성은 높다고 할 수 있다.	0.2

서 지 정 보 양 식

수행기관보고서번호	위탁기관보고서번호	표준보고서번호	INIS 주제코드
KAERI/TR-2668/2004			

제목 / 부제	안전소프트웨어의 정량 V&V 방안 연구
연구책임자 및 부서명 (주저자)	엄흥섭 (종합안전평가부)
연 구 자 및 부 서 명	강현국 (종합안전평가부), 장승철(종합안전평부), 하재주(종합안전평가부), 손한성(KNICS)

출 판 지	대전	발행기관	KAERI	발행년	2004. 2.
페 이 지	85 p.	도 표	있음(○), 없음( )	크 기	21×29.7cm
참고사항					
비밀여부	공개(○), 대외비( ), __ 급비밀		보고서종류	기술보고서	
연구위탁기관			계약 번호		

초록

최근 원자력발전소의 안전을 평가하는 중요한 수단 중의 하나인 확률론적 안전성 평가(Probabilistic Safety Assessment: PSA)에 사용하기 위하여 소프트웨어 신뢰도의 정량적인 정보에 대한 실용적인 요구가 생겨나고 있다. 그러나 기존의 소프트웨어 신뢰도 정량평가 방법들은 PSA가 요구하는 충분한 정보를 제공할 수 없기 때문에 현재는 디지털 시스템을 포함하는 PSA의 경우 소프트웨어 부분을 배제하거나 또는 임의의 값을 사용하고 있는 실정이다. 본 보고서에서는 최근 불확실성을 포함하는 시스템의 모델링에 많이 활용되고 있는 Bayesian Belief Networks 기법을 이용하여 규칙 기반의 정성적인 소프트웨어 평가 방법론을 Bayesian Belief Networks로 모델링하고 PSA가 요구하는 정보를 생산할 수 있는 기본체제 연구와 사례연구에 대하여 기술하였다.제안된 기본 체제는 안전 소프트웨어의 신뢰도에 관계된 정성적인 증거와 정량적인 증거 모두를 결합하여 정형적이고 정량적인 방법으로 결론을 추론할 수 있는BBN의 특성을 활용하여 구축되었다. 그리고 사례연구로서 연구된 방법론을 원자로 보호 계통에 탑재될 안전 소프트웨어 요구명세서의 품질을 평가하는 데 적용하였는데, 전문가에 의해 수행된 확인 및 검증 결과들이 모델의 입력으로 사용되었다. 만들어진 BBN 모델의 결과와 분석 내용은 전문가의 정성적인 판단과 유사하게 나타났으며 분석 내용들은 추후의 V&V 활동에 대한 의사 결정에 활용될 예정이다.

주제명 키워드 (10단어내외)	안전 소프트웨어, 신뢰도, Bayesian Belief Nets, BBN, V&V

BIBLIOGRAPHIC INFORMATION SHEET

Performing Org. Report No.	Sponsoring Org. Report No.	Standard Report No.	INIS Subject Code
KAERI/TR-2662/2004			

Title / Subtitle	A Study on Quantitative V&V of Safety-Critical Software
Project Manager and Department	H.S. Eom (Integrated Safety Assessment Division)
Researcher and Department	H.G. Kang (ISA), S. C. Chang(ISA), J. J, Ha(ISA), H.S. Son(KNICS)

Publication Place	Daejon	Publisher	KAERI	Publication Date	2004. 2.
Page	85 p.	Ill. & Tab.	Yes(○), No ( )	Size	21× 29.7cm
Note					
Classified	Open(○),Restricted( ),-___ Class Document		Report Type	Technical Report	
Sponsoring Org.			Contract No.		

Abstract(15-20 Lines)

Recently practical needs have required quantitative features for the software reliability for Probabilistic Safety Assessment which is one of the important methods being used in assessing the overall safety of nuclear power plant. But the conventional assessment methods of software reliability could not provide enough information for PSA of NPP, therefore current assessments of a digital system which includes safety-critical software usually exclude the software part or use arbitrary values. This paper describes a Bayesian Belief Networks based method that models the rule-based qualitative software assessment method for a practical use and can produce quantitative results for PSA. The framework was constructed by utilizing BBN that can combine the qualitative and quantitative evidence relevant to the reliability of safety-critical software and can infer a conclusion in a formal and a quantitative way. The case study was performed by applying the method for assessing the quality of software requirement specification of safety-critical software that will be embedded in reactor protection system.

Subject Keywords (About 10 words)	Safety critical software, Bayesian Belief Nets, BBN, V&V