2001 추계학술발표회 논문집
한국원자력학회

확률론적 안전성평가를 위한 정성적 소프트웨어 신뢰도 평가의 정량화 방안

A Bayesian Belief Nets Based Quantification Method of Qualitative Software Reliability Assessment for PSA

엄흥섭, 김장열, 성태용, 이기영

한국원자력연구소
대전광역시 유성구 덕진동 150

요약

현재 원전 안전 시스템에 사용되는 소프트웨어의 신뢰도는 규칙기반의 정성적 평가에 의하고 있으나 원자력발전소의 안전성 평가를 위한 중요한 수단으로 사용되고 있는 확률론적 안전성 평가(PSA)에 디지털 시스템을 포함시켜야 하는 현실적 요구를 충족시키기 위해서는 소프트웨어 신뢰도의 정량화가 요구된다. 본 논문에서는 기존에 사용되고 있는 소프트웨어의 정성적인 평가 방법을 Bayesian Belief Nets 을 이용하여 정형적으로 모델링 하고 PSA 에서 요구하는 정량화 된 결과를 구하는 한 가지 방안에 대하여 논의하였으며 원전 상용소프트웨어 인정 프로세스를 논의된 방안에 적용하여 동 방안의 PSA 활용 가능성을 검토하였다.

Abstract

Current reliability assessments of safety critical software embedded in the digital systems in nuclear power plants are based on the rule-based qualitative assessment methods. But practical needs require the quantitative features of software reliability for Probabilistic Safety Assessment (PSA) that is one of important methods being used in assessing the whole safety of nuclear power plant. This paper discusses a Bayesian Belief Nets (BBN) based quantification method that models current qualitative software assessment in formal way and produces quantitative results required for PSA. Commercial Off-The-Shelf (COTS) software dedication process was applied to the discussed BBN based method for evaluating the plausibility of the method in PSA.

1. 서론

PSA 는 원전의 안전성을 종합적이며 정량적으로 평가하기 위한 중요한 안전성 평가 수단

으로 신규 원자력발전소 건설 시 인허가 사항으로 제출이 요구되며 최근에는 미국을 중심으로 PSA 결과를 현재까지 사용되던 결정론적인 규제의 보완 수단으로 사용하고 있는데 국내에서도 이의 채택이 적극적으로 검토되고 있다. 그러나 기존 원전에 적용되어 왔던 PSA 방법론을 그대로 디지털 시스템에 적용하여 시스템의 안전성을 정량화 하는 데에는 아직까지 해결되지 못하고 있는 다음과 같은 몇 가지 문제점이 있다[1].

- Modeling the multi-tasking of digital systems
- Estimating software failure probability
- Estimating the effect of software diversity and V&V efforts
- Estimating the coverage of fault-tolerant features
- Estimating the CCF probability in hardware
- Modeling the interactions between hardware and software
- Failure mode of digital systems
- Environmental factors
- Digital system induced initiating events including human errors

위의 문제점들 중 원전 안전 시스템에 사용되는 안전 소프트웨어의 신뢰도 평가는 고장의 원인이 설계 결함에 주로 기인하고 또 입력에 대해 비 선형적 출력을 가지는 소프트웨어의 특성으로 인하여 시험이나 신뢰도 성장모델과 같은 기존의 정량적 방법 단독으로는 불충분하다는 것이 현재의 정설이다. 따라서 각국의 규제기관은 소프트웨어의 신뢰도에 관계되는 모든 활동과 자료들을 종합적으로 판단하는 규칙 기반의 정성적 평가에 의존하고 있다.

본 논문에서는 규칙이나 절차 기반의 정성적 평가 절차에 근거한 현행 방법을 Bayesian Belief Nets 을 이용하여 정량적 결과를 얻을 수 있는 방안에 대하여 논의하였고 상용소프트웨어의 인정 프로세스를 시험케이스로 적용하여 동 방안의 PSA 적용 가능성을 검토하였다.

상용 소프트웨어는 기본적으로는 안전 디지털 시스템의 제작자가 만든 안전 소프트웨어와 동일한 특성을 가지고 있으나 개발 과정의 평가가 거의 불가능하고 또 각 개발 단계별 생산 문서를 평가 전문가가 쉽게 얻을 수 없다는 특이성 때문에 보다 정성적인 평가에 의존하고 있는 실정이다[2].

2. 원전 상용 소프트웨어 인정 프로세스

BBN 을 이용하여 문제를 해결할 때 일반적으로 전문가의 추론 과정을 추출하여 사용하거나 또는 표준이나 가이드라인의 절차나 기준을 따르게 된다. 본 논문에 제시된 BBN 모델의 기본은 상용 소프트웨어 인정(dedication) 방법 4 가지 중 method 2 인 공급자 조사 방법에 의 상용 소프트웨어 인정 프로세스에 관하여 NUREG/CR-6421 의 기본 개념을 바탕으로 하고 EPRI/TR-106439 기준을 적용하여 절차적 관점에서 상용 등급 조사(commercial grade survey) 방법에 의한 상용 소프트웨어 인정 프로세스를 사용하였다. 모델을 위해 사용된 상용 소프트웨어 인정 프로세스는 9 단계로 되어 있으며 각 단계별로 세부적 검토 항목이 정해져 있

다. 각 단계별 주요 내용은 다음과 같다[2].

단계 1: 조사 전 사전회의(pre-survey meeting)

정보공학 방법론에 따른 소프트웨어 엔지니어링 절차를 준수하여 소프트웨어를 개발 하였는지 여부를 검토하며 ISO 9001 Part 3 의 준수 여부가 중요한 판단의 기준이 된다. “ISO 9001 Part 3 에서 규정한 항목 검토” 외에 3 개의 중분류 검토 항목이 있다.

단계 2: 제품 설명서 검토

제조 회사가 제공할 수 있는 모든 제품 설명서를 검토하는 단계로 “새로운 기능의 추가 및 변경 정의” 외에 3 개의 세부 검토 항목이 있다.

단계 3: 시스템 및 소프트웨어 기능 요건 조사

소프트웨어의 요구사양명세를 검토하는 단계로 상위 레벨의 시스템 명세로부터 소프트웨어 요구사양 명세까지 추적성 분석의 개념을 근간으로 “기능요건 명세서 존재 여부” 외에 4 개의 중분류 검토 항목이 있다.

단계 4: 소프트웨어 설계 조사

소프트웨어의 설계 요건을 조사하는 단계로 “설계 과정의 검토” 외에 9 개의 중분류 검토 항목이 있다.

단계 5: 소프트웨어 개발에 관한 조사

소프트웨어 품질 보증 목표와 계획 그리고 계획의 준수 여부를 검토한다. “소프트웨어 품질보증 계획의 검토” 외에 1 개의 중분류 검토 항목이 있다.

단계 6: 하드웨어 및 소프트웨어 통합 조사

하드웨어와 소프트웨어의 통합계획 여부, 통합 시험 절차 및 관련 승인기준 여부, 형상시험 여부, 통합 변경 제어 여부를 검토하는 단계이다.

단계 7: 시스템 검증 조사

시스템 검증에 대한 시험계획 여부, 테스트 절차서 존재 및 완결성 여부, 확인 과정에서 나타난 결과 검토, 시스템 테스트와 관련된 사항을 검토하며 “상세 유형 시험 절차” 외에 1 개의 중분류 검토 항목이 있다.

단계 8: 사용자 문서 조사

회사로부터 취득 가능한 모든 매뉴얼에 대하여 요구사양 및 설계 요건 부합 여부를 평가하고 이들의 일관성, 명확성, 정확성 유지를 검토한다.

단계 9: 소프트웨어 유지보수 조사

최초의 배포(original release)가 이루어진 이래 발생된 문제점들을 어떻게 해결 했는가를 검토하고 관련 기록 정보를 평가한다. 또 제품에서 발견된 오류들이 어떻게 사용자들에게 통지되었는지 여부를 점검하고 이들 자료의 형상관리 여부를 검토한다. "변경통지 절차에 대한 감사 계획 여부" 외에 2 개의 중분류 검토 항목이 있다.

3. 상용소프트웨어 인정 프로세스 BBN 모델

3.1 BBN

BBN 은 관련된 변수들을 인과관계에 의해 구성하여 모델링하고 변수들 간의 종속성 정도를 조건부 확률로 나타낸 다음 관찰된 여러 가지의 증거에 입력한 후 베이시안(Bayesian) 확률 정리를 적용하여 정량적 결론을 이끌어 내는 방법론이다. BBN 은 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 구성되는데 노드는 모델에 포함된 변수들을 나타내며 노드 연결선은 노드간의 인과관계를 나타낸다. 각 노드는 무작위 변수로서 몇 개의 상태를 가지고 있으며(예: "Yes"와 "No") 각 상태의 확률 값의 합은 1 이 된다. 각 노드에 연결된 노드 확률 테이블은 노드간의 연결 강도를 결정하며 모 노드(parent node)의 각 상태에 대한 조건부 확률로 표현된다[3].

BBN 상의 노드들은 목표노드(target node), 관찰가능 노드(observable node) 그리고 중간 노드(intermediate node)로 구분된다[4]. 목표 노드는 모델에서 평가 목적에 해당하는 노드로서 "프로그램의 무 결함" 등이 될 수 있고, 관찰가능 노드는 직접 관찰 가능한 노드로서 "N 번 테스트 중 M 번 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[4].

3.2 상용소프트웨어 인정 프로세스를 위한 BBN 그래프

BBN 을 이용하여 문제 해결을 위한 모델링을 할 때 일반적으로 가장 먼저 해야 할 작업은 모델 구축에 필요한 모든 관련된 증거들을 확인하는 것이다. 이 증거들은 관련된 변수(과정, 제품, 자원 등)들과 그들의 속성 또는 특성에 대한 서술이며 이것들이 BBN 의 변수(노드)가 된다. 논의된 BBN 모델에서는 제 2 장에서 기술된 인정 프로세스 9 단계를 기본 레벨의 변수들로 설정하였고 목표 노드는 "상용 소프트웨어 승인"으로 설정하였다. 기본 레벨의 노드들은 다시 자 노드들을 가지고 있는데 이들 노드는 제 2 장에서 기술된 각 단계별 중분류 검토 항목을 근거로 하여 작성하였다. 이와 같이 하여 만들어진 BBN 기본 그래프는 그림 1 과 같다.

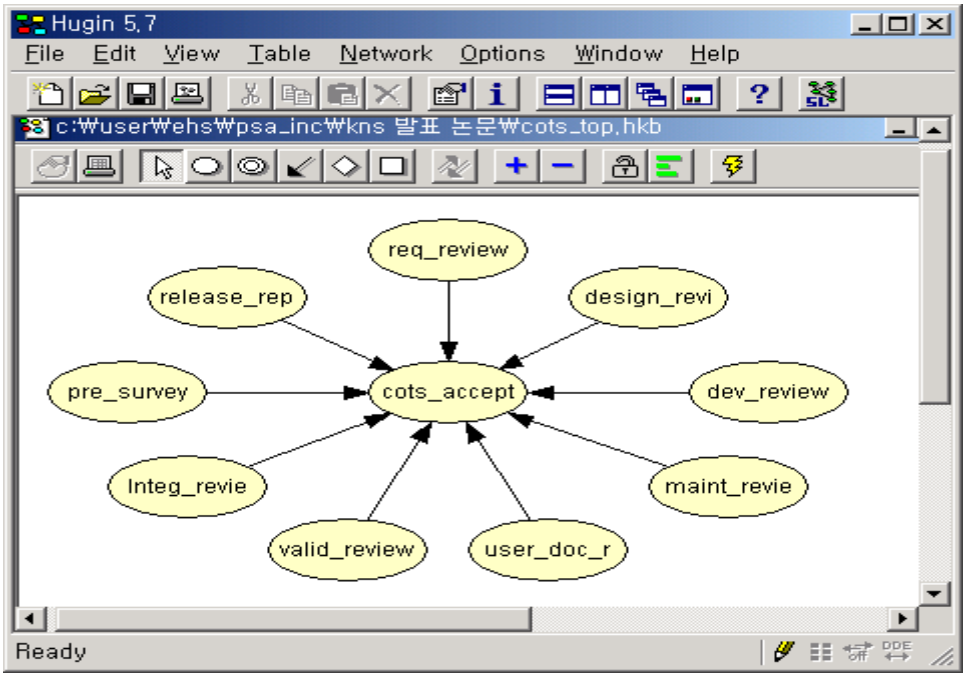

그림 1. 상용소프트웨어 인정 프로세스 기본 BBN 그래프

그림 1 "상용소프트웨어 인정 프로세스 기본 BBN 그래프" 상의 각 노드는 다시 각 단계에 포함되어 있는 중분류 검토 항목을 근거로 자 노드들을 가진다. 예로, 상용소프트웨어 인정 프로세스 단계 3 에 해당하는 "시스템 및 소프트웨어 기능 요건 검토" 노드의 BBN 그래프는 이 단계에서 검토되는 5 개의 중분류 검토 항목을 자 노드로 설정하여 그림 2 와 같이 만들어졌다.

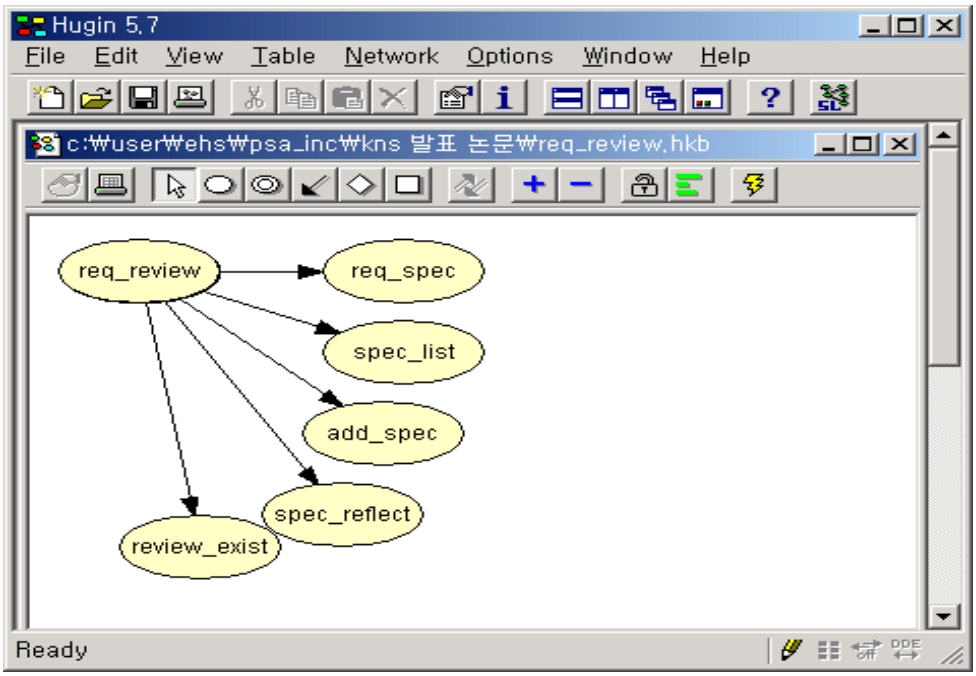

그림 2. "시스템 및 소프트웨어 기능 요건 검토" 노드의 BBN 그래프

위와 같은 방법으로 만들어진 상용소프트웨어 인정 프로세스의 전체 BBN 그래프는 그림 3 과 같다.

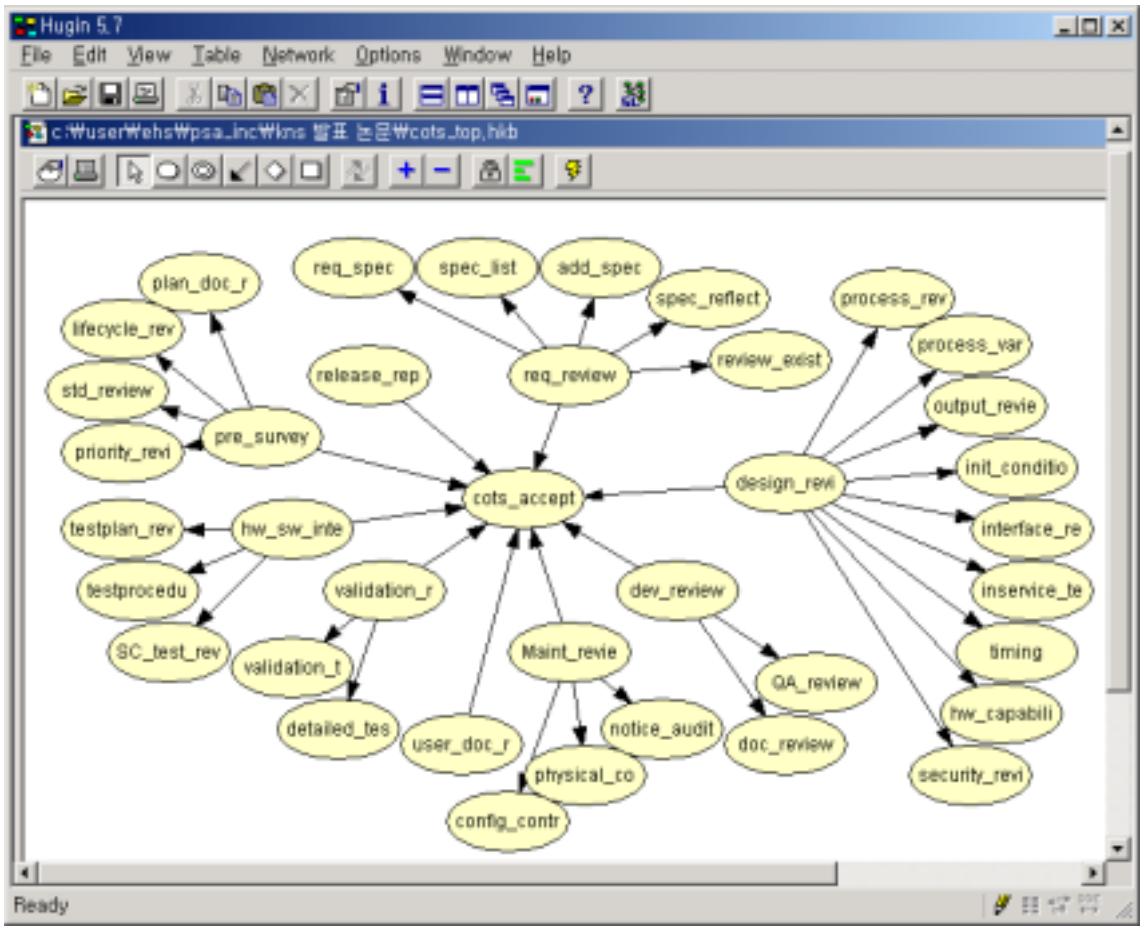

그림 3. 상용소프트웨어 인정 프로세스 전체 BBN 그래프

3.3 BBN 노드들의 노드 확률 테이블 작성

BBN 그래프의 작성이 완료되면 다음 단계는 각 노드별로 노드 확률 테이블을 정의하는 것인데 이것은 (a) 각 노드의 상태를 정의하는 것과 (b) 각 상태별 확률 값을 구하는 것으로 나누어진다. 그림 3 에서 나타난 BBN 그래프 상의 각 노드들의 확률 테이블은 다음과 같이 정의되었다.

O 목표 노드 “COTS_ACCEPTANCE” : [>1x10^{-4} pfd]와 [=<1x10^{-4} pfd] 두 개의 상태

O 중간 노드 전체 : [acceptance]와 [no acceptance] 두 개의 상태

O 관찰가능 노드 전체 : [Yes]와 [No] 두 개의 상태

목표 노드에서 설정된 두 개의 상태가 의미하는 것은 관찰 가능 노드에 측정/획득된 값을 입력한 후 전체 네트(Net)를 조건부 확률 계산과 Bayesian 확률 정리를 사용하여 계산을 수행했을 때 목표 노드의 각 상태가 어떤 확률 값을 가지고 있나를 추론하기 위한 것이다. 즉 목표 노드가 [>1x10^{-4} pfd]인 상태가 될 확률과 [=<1x10^{-4} pfd]가 될 확률을 구할 목적으로 정

의한 것이다. 여기에서 두 상태를 구분하는 기준 값 "$1x10^{-4}$ pfd"은 BBN 에서 직접적으로 구해지지 않는데 이것은 BBN 이 시험(Testing)이나 신뢰도 성장 모델과 같은 통계적 기법을 사용하여 직접적인 고장 확률 값을 구하는 것이 곤란한 문제의 해결에 적용되었기 때문이다. 따라서 이 값은 (a) PSA 를 신뢰도 배분을 위한 도구로 사용하여 역으로 목표 값을 구하거나 (b) 시스템 요구 사항에서 결정된 수치를 사용하거나 (c) 전문가가 전체 시스템의 안전성 분석을 고려하여 적절하다고 판단한 값을 사용하게 된다. (a)와 목적은 다르지만 방법상으로는 유사하게 PSA 로부터 목표 수치를 구하는 방법의 예로는 PSA 를 사용하여 원전 안전계통 소프트웨어의 시험횟수를 결정하는 방법에 대한 연구[5]가 있었고 (b)의 예로는 Sizewell B 원전의 소프트웨어 기반 보호계통의 요구사항($1x10^{-3}$ pfd)이 있으며 (c)의 예로는 Westinghouse AP600 의 보호 및 안전계통 PSA 예($1.1x10^{-5}$ pfd)와 월성 원전 SDS2 의 소프트웨어 고장수목 분석 예($1x10^{-4}$: constant probability)가 있다.

중간 노드의 상태 [acceptance]와 [no acceptance]는 직접적으로 측정 가능한 것이 아니고 제한된 정보나 믿음을 표현하는 것인데 일반적으로 자 노드인 관찰가능 노드들의 상태 값에 의해서 결정된다.

관찰 가능 노드의 상태 [Yes]와 [No]는 모두 측정 가능한 변수들이다. 이들 변수들은 정량적인 값으로 구해질 수도 있고 전문가의 판단에 의한 주관적 확률 값으로 측정될 수도 있다. BBN 은 이런 정량적 성질의 증거들과 정성적 성질의 증거들을 정형적(formal)으로 결합하여 일관된 방식으로 결론을 추론하는 특징을 가지고 있다.

여기에서 논의된 BBN 모델의 관찰가능 노드들은 모두 정성적인 것들이어서 [yes]/[no]와 같은 상태로 표현 되었고 또 목표 노드도 두 가지 상태에 대한 확률로 표현 되었지만, 정량적인 값(예를 들어 확률 등)을 구할 수 있는 관찰가능 노드들로 이루어진 BBN 에서는 그 정량적인 값들을 사용하여 목표노드로부터 구체적인 고장확률과 같은 point value 를 구할 수 있다. 예를 들면, PSA 에서 사용되는 고장수목 분석법(FTA)과 같은 방식으로 BBN 을 모델링 할 수 있는데 이렇게 하면 FTA 에 사용된 기본사건의 값들을 BBN 의 관찰가능 노드에 입력해서 FTA 의 정점 사건의 값과 동일한 결과를 BBN 의 목표 노드로부터 얻을 수 있다.

3.4 BBN 모델의 사용

BBN 그래프를 완성하고 노드 확률 테이블의 정의가 완료되면 각 노드에 관찰된 값을 입력하여 구하고자 하는 목표 노드의 값을 계산하게 된다. BBN 모델의 일차적인 목적은 관찰 및 획득된 증거에 근거한 목표 노드의 값을 구하는 것이지만 BBN 이 가진 특성과 확률 계산을 자동으로 해 주는 BBN 도구[7]를 이용하여 What if 분석 또는 시나리오 분석이 가능하므로 이를 활용하여 평가 뿐 아니라 소프트웨어 생명 주기의 모든 단계에서 최적화 문제를 비롯한 여러 가지 문제의 해결에 사용될 수 있다[6]. 표 1 은 만들어진 상용소프트웨어 인정 프로세스 BBN 에 여러 가지 입력(증거) 조합을 가정한 시나리오를 만들어 계산한 결과의 일부이다. 표 1 에서 나타난 목표 노드의 값은 실제적인 증거에 근거하여 계산된 것이 아니고 또 노드 확률 테이블의 확률을 정의하는데 전문가의 지식이 완전하게 반영되지 않았기

때문에 값에 대해 실질적인 의미를 부여할 수는 없다. 그러나 여러 경우에 대한 시나리오 분석의 결과 만들어진 BBN 모델은 전문가의 판단과정을 유사하게 모의하고 있고 또 시나리오 별 계산 결과도 일반적으로 적절한 결론을 제시한 것으로 나타났다.

표 1. 증거 입력 조합별 시나리오와 BBN 목표 노드 상태 값

시나리오	목표 노드 상태 값	
	Accept [=<1x10^{-4} pfd]	No Accept [>1x10^{-4} pfd]
1. 증거가 입력되지 않은 초기 상태	0.6914	0.3086
2. 모든 증거가 긍정적	0.9251	0.0749
3. 1 개 증거를 제외한 모든 증거가 긍정적	0.8999	0.1001
4. 2 개 증거를 제외한 모든 증거가 긍정적	0.8714	0.1286
5. 3 개 증거를 제외한 모든 증거가 긍정적	0.8646	0.1354

그림 4 는 시나리오 #3 을 BBN 모델링 도구 Hugin[7]을 사용하여 계산한 결과를 보여준다. “plan_doc_review” 노드에는 부정적 증거가 발견되어 노드 상태 [no]의 확률이 1 로 설정되었고 다른 모든 관찰 노드들은 [yes]상태의 확률 값이 1 로 설정된 시나리오다.

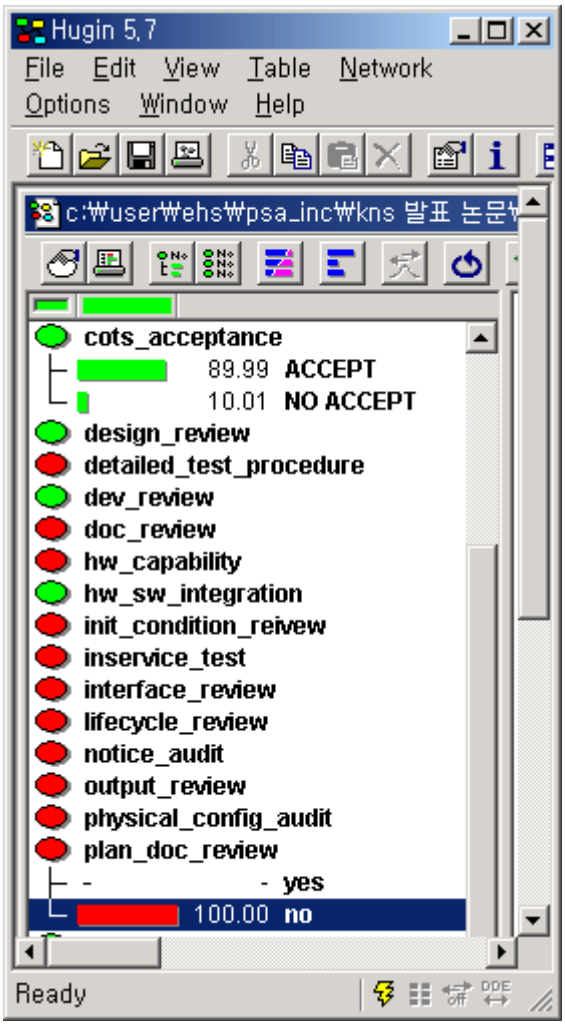

그림 4. 시나리오 #3 계산 결과

4. 요약 및 결론

원자력발전소의 안전성 평가를 위한 중요한 수단으로 사용되고 있는 확률론적 안전성 평가에 안전 계통 디지털 시스템을 포함시켜야 되는 현실적인 요구가 있고 이를 위해서는 안전 소프트웨어의 정량적인 신뢰도 평가가 필요하다. 그러나 시험이나 신뢰도 성장 모델과 같은 기존의 정량적 소프트웨어 신뢰도 평가 방법 단독으로는 원전 안전 계통 디지털 시스템에 사용되는 소프트웨어의 신뢰도를 구하기 어려운 것이 현재의 기술 수준이며 따라서 원자력분야를 비롯한 타 산업분야의 안전성/신뢰도 관련 표준들이나 각국의 규제 기관들은 규칙기반의 정성적 평가 방식을 따르고 있다.

본 논문에서는 안전 소프트웨어의 특성으로 인하여 만족할 만한 새로운 정량적 신뢰도 평가 방법이 가까운 장래에 나오기 어려우나 디지털 시스템의 확률론적 안전성 평가와 같은 현실적인 필요성은 당장 대두되고 있는 현재의 상황에서, 하나의 대안으로 기존에 채택되고 있는 소프트웨어의 정성적인 평가 방법을 Bayesian Belief Nets 방법론을 이용하여 정형적으로 모델링 하고 PSA 에서 요구하는 정량화 된 결과를 구하는 방안을 원전 상용소프트웨어 인정 프로세스를 시험케이스로 적용하여 논의하였다. 논의된 방안의 시험 적용 결과 나타난 문제점은;

(1) 만들어진 모델이 기존 규칙 기반의 정성적 평가 시스템을 완전하게 반영했는가에 대한 검증 문제와

(2) BBN 을 적용하는 대상들은 정량화 된 값을 구하기 어려운 불확실성이 많이 포함된다는 특성으로 인해 변수(노드) 간의 연결 강도를 나타내는 노드 확률 테이블을 전문가의 판단으로부터 확률 형태로 추출하여 정의해야 하는데 따르는 문제점인데,

이런 문제점들은 BBN 기반 방법론의 공통적인 문제점인데 원자력분야를 비롯해서 항공분야나 군수분야에서 디지털 시스템의 안전성 평가의 일부로 이에 대한 연구가 현재 진행중에 있다[6].

한편, 나타난 유용성으로는;

(1) 신뢰도 평가에 관련된 다양한 증거들(과정, 제품 정보, 경험적 자료, 전문가의 판단, 불완전한 정보 등)을 일관된 평가체제 안에서 정형적으로 결합하여 결론을 추론할 수 있고

(2) 모델의 직관적 그래프 형태가 평가에 관련된 복잡한 연관 관계와 감추어진 가정들을 명시적으로 나타내어 결론이 도출되는 과정에 대한 투명도와 감사도(auditability)를 높일 수 있으며

(3) 불확실하거나 애매한 증거들이 필연적으로 포함되는 신뢰도 평가에 있어서 “what if” 분석을 가능하게 해주므로 의사결정에 있어 효과적인 도구로 사용될 수 있다는 점이다.

감사의 글

이 논문은 대한민국 과학기술부에서 시행하는 원자력연구개발 중장기사업의 지원으로 수행되었습니다.

참고문헌

[1] T. Sung, H.G. Kang, “Intermediate Probabilistic Safety Assessment Approach for Safety Critical Digital Systems,” Proceeding of ICON9, Nice, France, 2001.

[2] 김장열 외, 공급자 조사 방법에 의한 원전 상용소프트웨어 인정 프로세스, 한국원자력학회 추계학술발표회, 2000.

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

[4] G. Dahll et al, “The Use of Bayesian Belief Bets in Safety Assessment of Software Based Systems,” *Int. J. General Systems*, Vol. 29(2), pp 205-229, 2000.

[5] 강현국 외, PSA 를 이용한 원전 안전계통 소프트웨어 시험횟수 결정, 한국원자력학회 추계학술발표회, 2000.

[6] 엄흥섭 외, 원전 안전 소프트웨어의 정량적 신뢰도 평가를 위한 Bayesian Belief Nets 기술 분석, KAERI/AR-594/2001, 한국원자력연구소, 2001

[7] HUGIN Expert A/S., http://www.hugin.dk