2003 춘계학술발표회 논문집
한국원자력학회

BBN을 이용한 안전 소프트웨어의 정량적 신뢰도 평가에 대한 연구

A Study on the Quantitative Evaluation of the Reliability for Safety Critical Software Using Bayesian Belief Nets

엄흥섭, 장승철, 하재주
한국원자력연구소
대전광역시 유성구 덕진동 150

요약

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. 시험이나 확인 및 검증과도 같은 많은 활동들이 소프트웨어의 설계 단계에서 수행되고 있으나 종래의 소프트웨어 신뢰도 분석 기법들을 디지털 안전 시스템에 적용하기에는 충분하지 못한 까닭에 안전 중요 소프트웨어의 신뢰도를 정량적으로 평가하는 방법은 아직까지 개발되지 못한 실정이다. 본 논문에서는 디지털 안전 시스템에 사용되는 안전 중요 소프트웨어의 신뢰도를 정량적으로 추정하기 위한 Bayesian Belief Nets의 적용성에 대하여 논의하였고 이를 위하여 원자력 연구소에서 작성된 상용 소프트웨어 인정 프로세스를 기본으로 BBN 모델을 구축하였다. 결론적으로 BBN 기술의 채용은 원전에 사용되는 안전 중요 소프트웨어의 신뢰도 평가 과정을 용이하게 하고 또 실용적 관점에서의 소프트웨어 신뢰도 평가와 관련해서는 what-if 분석과 같은 유용한 정보를 제공할 수 있는 것으로 나타났다.

Abstract

Despite the efforts to avoid undesirable risks, or at least to bring them under control in the world, new risks that are highly difficult to manage continue to emerge from the use of new technologies, such as the use of digital instrumentation and control (I&C) components in nuclear power plant. Whenever new risk issues came out by now, we have endeavored to find the most effective ways to reduce risks, or to allocate limited resources to do this. One of the major challenges is the reliability analysis of safety-

critical software associated with digital safety systems. Though many activities such as testing, verification and validation (V&V) techniques have been carried out in the design stage of software, however, the process of quantitatively evaluating the reliability of safety-critical software has not yet been developed because of the irrelevance of the conventional software reliability techniques to apply for the digital safety systems. This paper focuses on the applicability of Bayesian Belief Net (BBN) techniques to quantitatively estimate the reliability of safety-critical software adopted in digital safety system. In this paper, a typical BBN model was constructed using the dedication process of the Commercial-Off-The-Shelf (COTS) installed by KAERI. In conclusion, the adoption of BBN technique can facilitate the process of evaluating the safety-critical software reliability in nuclear power plant, as well as provide very useful information (*e.g.*, 'what if' analysis) associated with software reliability in the viewpoint of practicality.

1. 서론

원전 안전 시스템에 사용되는 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 방법으로는 불충분하다는 것이 현재의 정설이다[1]. 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 있다[2][3]. 그러나 최근에 디지털 시스템이 원전의 안전계통에 사용되고 이에 따라 확률론적 안전성 평가(Probabilistic Safety Assessment, PSA)와 같이 소프트웨어의 신뢰도를 정량적으로 평가해야 하는 현실적 필요성이 대두되어 이를 해결하기 위한 여러 가지 연구가 각 산업분야에서 수행되고 있다[4].

본 논문에서는 기존에 사용되고 있는 규칙이나 절차 기반의 정성적 평가에 근거한 소프트웨어의 신뢰도 평가 방법을 Bayesian Belief Net 을 이용하여 정형적으로 모델링하고 이를 통하여 정량적 결과를 얻을 수 있는 방안에 대하여 논의하였다. 한국원자력연구소에서 연구 중인 상용소프트웨어의 인정 프로세스[5]를 시험케이스로 3 가지 BBN 모델을 만들고 그 중 하나의 모델에 대해서는 현실적으로 가능한 시나리오를 작성하여 적용하였다.

2. Bayesian Belief Nets

2.1 개요

Bayesian Belief Nets(BBN)의 이론적인 개발은 1970 년대로 거슬러가지만 그 당시에는 효과적인 알고리즘의 결여와 도구가 없었던 관계로 실용적인 적용은 어려운 실정이었다. 그러나 효과적인 도구가 많이 만들어진 요즈음에는 의료, 군사, 금융, 안전과 신뢰도 평가와 같은 많은 분야에서 활용되는 기술로 되어가고 있다. BBN 은 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.

2.2 BBN 모델링 샘플

간단한 예를 통하여 BBN 의 개념과 활용 방식을 소개한다. 여기에서 사용된 예는 “Introduction to Bayesian Networks[6]”에서 나온 내용을 각색한 것이다.

2.2.1 불확실성을 포함하는 문제의 모델링

BBN을 이용하여 모델을 만들고자 하는 지식(knowledge)은 다음과 같다.

[미스터 홈즈는 로스엔젤레스에 산다. 어느 날 아침 홈즈가 집을 나설 때 그는 자기 집 정원의 잔디가 젖어있는 것을 발견한다(변수 H-wet). 이것은 비(변수 Rain) 때문일까? , 아니면 스프링클러(변수 Sprinkler) 때문일까? 양쪽 사건에 대한 홈즈의 믿음은 모두 높아진다. 그 다음 홈즈는 이웃에 사는 왓슨 집 정원의 잔디(변수 W-wet)를 보고 그것도 역시 젖어있다는 것을 알게 된다. 여기서 홈즈는 간밤에 비가 왔다는 것을 거의 확신하게 된다.]

위의 상황에서 홈즈의 추론은 다음과 같다.

추론-1: 홈즈는 자기 집 정원의 잔디가 젖은 것을 보고 비와 스프링클러의 가능성을 높인다.

추론-2: 홈즈는 비가 온 것에 대한 가능성이 높아지자 왓슨 집 정원의 잔디도 젖었을 것이라는 가능성을 높인다.

추론-3: 그래서 홈즈는 왓슨 집 정원의 잔디를 검사하게 되고, 그것이 젖어있는 것을 발견하자 간밤에 비가 온 것에 대한 가능성을 급격하게 높이는 반면 스프링클러의 가능성은 초기의 값으로 낮춘다.

2.2.2 BBN에서 지식의 표현 방식

BBN 은 노드(node), 화살표 모양의 연결선 그리고 노드확률테이블(node probability table, NPT)로 구성되어있다. 노드는 이산 무작위 변수를 표현하는데, 위의 예에서 “Rain" "Sprinkler" "W-wet" "H-wet"가 여기에 속한다. 모든 변수는 상태(states)를 가지고 있는데, 변수 “Rain"의 경우에는 두 가지 상태(yes 와 no)를 가지고 있다. 연결선은 변수 간의 인과관계를 표시한다. 스프링클러는 홈즈 집 정원의 잔디가 젖게 되는 원인이기 때문에 이 관계는 노드 "Sprinkler"에서 노드 “H-wet" 방향으로 연결선이 그려지게 된다. 그림 1 은 위의 예에서 서술된 지식을 표현하는 BBN 그래프이다.

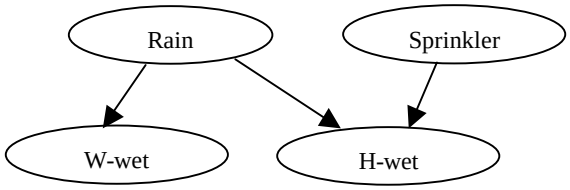

그림 1. 2.2.1에서 서술된 지식의 BBN graph 표현

불확실성에 대한 추론을 하기 위해서는 각 노드에 대하여 NPT 를 만들어야 한다. 위의 예에서, 노드 "W-wet"의 NPT 는 다음의 표와 같이 작성할 수 있다.

표 1. 노드 “W-wet”의 노드확률테이블

	‘Rain’ = yes	“Rain” = no
Pr(W-wet = yes)	1	0.2
Pr(W-wet = no)	0	0.8

이 표의 값들은 변수 “Rain"에 대한 변수 “H-wet"의 조건부 확률 값들을 보여주며 그 의미는 다음과 같다.

만약 비가 오면, 왓슨 집 정원의 잔디는 반드시 젖는다 : 확률 값 = 1

만약 비가 오지 않는 경우에는, 왓슨 집 정원의 잔디는 젖을 확률이 낮다. : 확률 값 = 0.2

같은 방식으로 변수 “H-wet"과 이 변수의 원인이 되는 두 노드 (Rain, Sprinkler) 사이의 관계는 다음의 표와 같이 표현될 수 있다.

표 2. 노드 “H-wet”의 노드확률테이블

Rain	Yes		No	
Sprinkler	Yes	No	Yes	No
Pr(H-wet = yes)	1	1	0.9	0
Pr(H-wet = no)	0	0	0.1	1

변수 “Rain"과 변수 “Sprinkler"의 NPT 는 성질이 다르다. 이런 노드들은 모노드(parent node)가 없기 때문에 노드의 각 상태에 대하여 초기 값을 설정해 주어야 한다. 여기의 예에서는 Pr(Rain = yes) = 0.2, Pr(Sprinkler = yes) = 0.1 로 값을 설정하였다.

2.2.3 증거의 입력과 추론

2.2.1 에서 기술된 추론들은 2.2.2 에서 만들어진 BBN 의 계산에 의하여 자동적으로 이루어진다. BBN 은 각 변수들의 결합확률분포의 간결한 표현이며, 주어진 무작위 변수 집합에 대하여 가장 완전한 정보를 나타낸다. 다음의 표는 위의 BBN 모델 예에서 나타난 각 노드의 사전 확률 값을 보여준다.

표 3. 노드들의 사전 확률

Sprinkler	Rain	W-wet	H-wet
0.1	0.2	0.036	0.272

BBN 의 주된 용도는 실제의 증거(각 사건의 관찰 결과)에 입각하여 각 변수의 상태 확률 값을 갱신하는 것이다. 위에서 기술된 예의 정형적 추론은 다음과 같이 된다.

[증거 -> 홈즈가 자기 집 정원의 잔디가 젖은 것을 본다.]

이 사건은 BBN 에서 Pr(H-wet = yes)을 1 로 설정하고 BBN 을 계산하면 되는데 결과를 보면 Pr(Rain = yes)은 0.2 에서 0.735 로 높아졌고, Pr(Sprinkler = yes)는 0.1 에서 0.338 로 높아졌다. 이 결과는 2.2.1 에서 기술된 정성적 추론과 모순되지 않는다. 그리고 Pr(W-wet = yes)은 0.036 에서 0.788 로 높아졌는데 이 결과 2.2.1 의 추론-2 와 일치하고 있다.

[증거 -> 홈즈가 왓슨 집 정원의 잔디를 검사하고 그것이 젖어있는 것을 발견한다.]

BBN 모델에서 이 증거는 Pr(H-wet = yes)을 1 로 설정하고 BBN 을 계산하면 되는데 결과를 보면, Pr(Rain = yes)은 0.735 에서 0.933 으로 높아졌고, Pr(Sprinkler = yes) 은 0.338 에서 0.16 으로 낮아졌다. 이 결과는 2.2.1 의 추론-3 과 일치하고 있다.

위의 예에서 나타난 것처럼 BBN 방법론의 가장 큰 유용성은 획득된 증거의 영향을 확률법칙에 의거하여 일관되게 불확실한 결과의 확률에 전파하는 것이다. BBN 의 또 하나의 이점은 정성적인 표현(예를 들면, 가능하다, 아닐 것 같다, 약간 증가한다 등)을 사용하는 것에 비해 보다 정밀한 추론을 가능하게 해 준다는 점이다. 또 다른 이점은 하나의 통일된 체계(framework) 내에서 주관적 확률과 통계적 자료에 근거한 확률 모두를 채용할 수 있고 따라서 추론을 하는데 있어서 정성적인 척도와 정량적인 척도를 결합할 수 있다는 점이다.

3. BBN 모델링 방법과 COTS 인정 프로세스

3.1 BBN 모델링 방법

일반적인 BBN 구축 절차는 모델링 대상 시스템의 변수들을 확인하고 이들 확인된 변수들을 BBN 의 노드로 사용하여 그래프를 작성한 후 각 노드들의 노드확률테이블을 작성하고 마지막으로 관찰된 값을 모델에 입력하여 관심 노드(변수)들의 계산된 결과를 분석하는 것인데 일반적으로 4 단계로 이루어진다.

◇ 단계-1: BBN 모델에 사용되는 변수들의 확인

모델을 구축하는데 필요한 모든 관련된 증거들을 확인/작성하는 단계이다. 이 증거들은 관련된 변수(실체: 과정, 제품, 자원 등)들과 그들의 속성 또는 특성에 대한 서술(description)이며, 추후 구축하려는 BBN 상에서 노드가 된다. 이 단계에서는 이들 실체와 속성들 간의 연결 관계는 고려하지 않아도 되며 단순히 나열하기만 하면 된다. 또한 관련된 표준들이나 생명주기가 반드시 고려되어야 한다.

◇ 단계-2: 확인된 변수들을 사용하여 그래프 작성

모델에 필요한 변수들이 모두 확인되면 다음 단계는 이들 변수들의 관계를 고려하여 그래프를 작성한다. BBN 의 그래프에서 가능한 노드의 그래프 연결 형태는 직렬연결, 분기연결, 수렴연결의 3 가지가 있다. BBN 모델링에 사용될 노드(변수)들을 사용하여 목표 노드의 값을 구하기 위해서는 각 노드들의 연결 관계를 확인해야 한다. 이들 노드들의 연결관계는 인과 관계적 결정(causal determination), 통계적 결정(statistical determination), 구조적 결정(structural determination) 등의 추론 형태를 가지는데 이들 추론 형태에 적합하도록 3 가지 그래프 형태를 적용하여 전체 BBN 그래프를 작성한다.

◇ 단계-3: 각 변수들의 노드확률테이블 작성

BBN 그래프가 완성된 다음 각 노드의 노드 확률 테이블(NPT)을 정의하는 단계로서 먼저 노드의 상태를 정의한 다음 각 상태에 대한 확률 값을 정하게 된다. BBN 모델에서 가장 중요한 부분중의 하나이며 또 만들기 어려운 부분이 노드 확률 테이블이다. 대부분의 경우 노드 확률 테이블을 작성하기 위하여 분야 전문가에게 의존해야 되고 해당 전문가는 각 노드의 상태별 확률 값을 추출해야 한다. 노드의 상태별 확률 값을 작성하는 방법은

(a) 실험 값 또는 통계적 자료와 같은 객관적 자료를 사용하여 작성하는 경우와

(b) 전문가의 주관적 판단에 의거하여 작성하는 경우가 있다.

◇ 단계-4: 해당 노드에 관찰된 값을 입력한 후 계산

BBN 그래프와 NPT 가 모두 만들어지면 마지막 단계로 각 노드에 값을 입력한 후 목표 노드 및 관심 노드의 값을 계산하고 분석한다. 최근에 복잡한 계산을 신속하게 해 주고 또 모델의 작성과 분석을 용이하게 해주는 도구들이 개발되어 BBN 을 실용적 문제 해결에 적용하는 것이 가능하게 되었다.

3.2 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 대상은 원자력연구소에서 작성된 상용 소프트웨어 인정 프로세스인데, 이것은 상용 소프트웨어 인정(dedication) 방법 4 가지 중 method 2 인 공급자 조사 방법에 의한 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) 방법을 활용하여 만들어졌다. 이 상용 소프트웨어 인정 프로세스는 다음과 같이 9 단계로 되어 있으며 각 단계별로 세부적 검토 항목을 포함하고 있다.

단계 1: 조사 전 사전회의(pre-survey meeting)
단계 2: 제품 설명서 검토
단계 3: 시스템 및 소프트웨어 기능 요건 조사
단계 4: 소프트웨어 설계 조사
단계 5: 소프트웨어 개발에 관한 조사
단계 6: 하드웨어 및 소프트웨어 통합 조사
단계 7: 시스템 검증 조사
단계 8: 사용자 문서 조사
단계 9: 소프트웨어 유지보수 조사

4. 안전 소프트웨어 평가 방법론

4.1 기본 BBN 모델

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. 본 논문에서 제안한 기본 BBN 모델은 3.2 에서 기술된 상용 소프트웨어 인정 프로세스 9 단계와 “상용 소프트웨어의 운전 이력”을 기본 레벨의 변수들로 설정하였고 목표 노드는 "상용 소프트웨어 승인"으로 설정하였다. 그리고 기본 레벨의 변수 9 개와 상용 소프트웨어의 운전이력 변수는 4 개의 그룹으로 분류하였다. 상용 소프트웨어 인정 프로세스를 구성하는 9 단계와 운전이력 변수는 프로세스 각 단계에서 검토되는 세부 질문 항목들을 가지고 있는데 이들 세부 질문 항목들을 각 기본 레벨 변수의 하위 변수로 설정하였다. 이와 같은 방법에 의하여 만들어진 상용 소프트웨어 평가용 BBN 그래프는 첨부된 그림 A-1 과 같다.

4.2 BBN 을 이용한 평가 방안

안전 소프트웨어의 신뢰도 평가할 경우 현실적으로 가능성이 있는 3 가지 경우에 대하여 각각 BBN 모델을 이용한 평가 방안을 작성하였다.

◇ 방법-1 : 특정 신뢰도 값의 충족 여부 판단을 위한 BBN

가. 개요

어떤 소프트웨어가 특정한 신뢰도 값의 범위 내에 드는지 여부를 판단해야 할 경우가 있다. 이 경우 소프트웨어의 정성적인 평가를 통해 얻어진 여러 가지 증거(평가 자료)와 해당 소프트웨어의 특정한 신뢰도 값의 관계를 BBN 을 이용하여 구축할 수 있고 이 BBN 모델을 활용하여 평가 자료에 입각한 신뢰도 값 충족 여부를 판단하는 방법이다. 여기서 목표 노드에 설정되는 특정한 신뢰도 값(예를 들면, "1x10-4E pfd")은 다음과 같은 것들이 사용될 수 있다.

(a) PSA 를 신뢰도 배분을 위한 도구로 사용하여 전체 안전계통 디지털 시스템의 목표 신뢰도 값으로부터 역으로 계산된 소프트웨어 신뢰도 값
(b) 시스템 요구 사항에서 결정된 값(수치)
(c) 전체 시스템의 안전성 분석을 위하여 전문가가 판단하여 설정한 값

(a)의 예로는 목적은 다르지만 방법상으로는 유사하게 확률론적 안전성 평가(PSA)로부터 목표 수치를 구한 방법의 예로는 PSA 를 사용하여 원전 안전계통 소프트웨어의 시험횟수를 결정하는 방법에 대한 연구[7]가 있었고, (b)의 예로는 Sizewell B 원전의 소프트웨어 기반 보호계통의 요구사항(1x10-3E pfd)이 있으며, (c)의 예로는 Westinghouse AP600 의 보호 및

안전계통 PSA 예(1.1x10-5E pfd)와 월성 원전 SDS2 의 소프트웨어 고장수목 분석 예(1x10-4E)가 있다.

나. 그래프

방법-1 의 상위 레벨 BBN 그래프는 다음의 그림 2 와 같다.

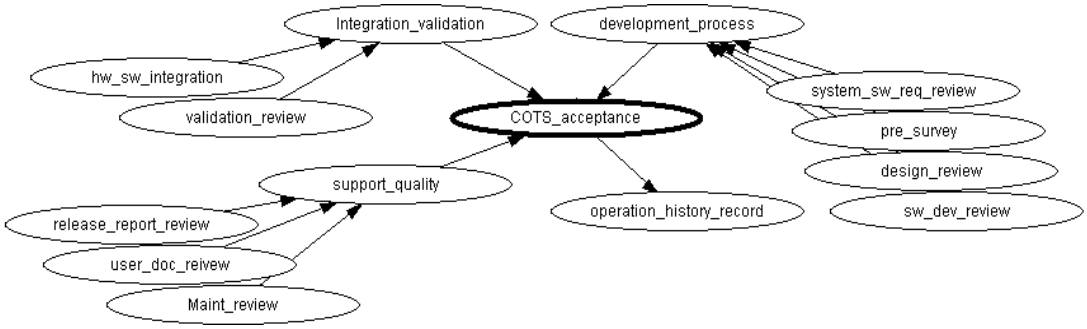

그림 2. 방법-1 의 특정 신뢰도 값 충족 여부 판단을 위한 BBN

상용 소프트웨어 인정 프로세스의 9 단계 및 운전 이력 기록이 모두 변수(노드)로 설정되었고 이들 노드는 다시 4 개의 그룹으로 분류되어 목표 노드인 “COTS_acceptance"에 연결되었다. 프로세스의 9 단계 노드와 운전 이력 기록 노드의 자노드(child node) 연결 상태는 그림 A-1 의 기본 BBN 그래프와 동일하다.

다. 노드확률테이블

목표 노드 "COTS_ACCEPTANCE"는 특정한 신뢰도 값 “1x10-4E pfd”을 가지고 있는데 이 값보다 같거나 작은 경우와 큰 경우 두 가지 경우를 상태(state)로 가지고 있고 [accept]와 [not accept]로 표시되었다. 따라서 본 BBN 에서 목표 노드는 다음의 표 4 와 같은 형태를 가진다.

표 4. 목표 노드 “COTS_ACCEPTANCE" 의 노드확률테이블

목표노드 상태	설정된 신뢰도 값
accept	=<1x10 -4E pfd
not accept	>1x10 -4E pfd

이렇게 목표 노드 “COTS acceptance"에 설정된 두 개의 상태와 그 값이 의미하는 것은 상용 소프트웨어 인정 프로세스의 각 단계별로 조사를 통해 획득한 증거들을 관찰 가능 노드에 입력한 후 전체 네트(Net)의 계산을 수행했을 때 목표 노드의 각 상태가 어떤 확률 값을 가지고 있는지 추론한 다음, 그 결과에 따라 설정된 신뢰도 값의 사용 여부를 판단하기 위한 것이다. 즉 목표 노드가 [>1x10-4Epfd]인 상태가 될 확률과 [=<1x10-4E pfd]가 될 확률을 구해서 해당 상용 소프트웨어의 신뢰도 값으로 사용할 수 있는지 여부를 판단하는 목적으로 정의한 것이다.

◇ 방법-2 : 운전이력을 신뢰도 값으로 사용할 경우의 BBN

가. 개요

상용 소프트웨어는 기본적으로는 안전 디지털 시스템의 제작자가 직접 개발한 소프트웨어와 유사하지만 해당 소프트웨어의 운전(사용) 이력을 얻을 가능성이 많은 반면 해당 소프트웨어의 개발에 관련된 문서는 충분치 않을 가능성이 높다. 이 경우 운전 이력에서 구해진 신뢰도 값이 판단의 대상이 되고 상용 소프트웨어 인정 프로세스에 있는 모든 단계에서 검토되는 항목들의 평가 결과는 운전 이력 기록의 품질에 대한 평가 결과와 함께 운전이력에서 추출된 동 소프트웨어의 신뢰도 값을 어느 정도 믿을 수 있는가에 영향을 미치는 하나의 요소로 볼 수 있다. 이와 같은 상황에서는 목표 노드를 상용 소프트웨어의 개발자나 제 3 자가 제공하는 운전 이력 자료의 값으로 설정하고, 상용 소프트웨어 인정 프로세스에 있는 모든 단계에서 검토되는 항목들의 평가 결과의 조합과 운전 이력 기록의 품질을 목표 노드에 영향을 미치는 변수(노드)로 설정하여 운전 이력을 신뢰도 값으로 사용 여부를 판단하는데 BBN 을 활용할 수 있다.

나. 그래프

상용 소프트웨어 인정 프로세스 9 단계를 기초로 한 기본 레벨 노드 9 개와 그 하위 노드 그래프는 방법-1 의 BBN 그래프와 동일하다. 또 이들 9 개 기본 레벨 노드를 그룹으로 분류하여 만든 노드들도 기본 BBN 과 동일하다. 새로 만들어지는 노드는 “COTS_quality"로 이 변수는 상용 소프트웨어 인정 프로세스에 있는 모든 단계에서 검토되는 항목들의 평가 결과가 조합된 것이다. “operation_record_quality" 노드는 소프트웨어의 제시된 신뢰도 수치에 대한 확신의 정도를 나타내는 변수로서 기본 BBN 의 ”operation_history_record"와 동일하다. 방법-2 의 상위 레벨 BBN 그래프는 다음 그림 3 과 같다.

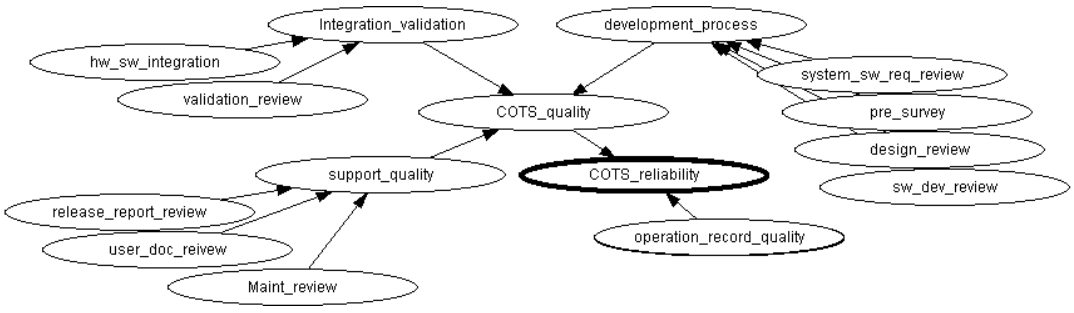

그림 3. 방법-2 의 운전이력을 신뢰도 값으로 사용할 경우의 BBN

다. 노드 확률 테이블

목표 노드 “COTS_reliability”의 상태 값은 운전이력으로부터 추출된 해당 상용 소프트웨어의 신뢰도 값이거나 또는 소프트웨어 개발 회사에서 제시한 신뢰도 값이다. 여기서는 “0.0001 pdf"가 예로서 사용되었다. “상용 소프트웨어 인정 프로세스의 평가

결과(COTS_quality)”와 “운전 이력 및 오류 관리의 품질(operation_record_quality)” 두 변수는 목표 노드에 직접 연결되므로 목표 노드 “COTS_reliability"의 노드확률테이블은 아래의 표와 같은 형태가 된다.

표 5. 목표노드 “COTS_reliability”의 노드확률테이블

operation_record_correctness		Good			Bad		
COTS_quality		good	aver.	Bad	good	aver.	bad
COTS_reliability (pdf)	<=0.0001	0.9	0.7	0.6	0.4	0.3	0.1
	>0.0001	0.1	0.3	0.4	0.6	0.7	0.2

새로 만들어진 “COTS_quality" 노드는 운전 이력에 관련된 부분을 제외하고 상용 소프트웨어 인정 프로세스를 기본으로 만들어진 BBN 의 최종 결과가 조합되는 노드로서 그룹 노드인 “development_process", "integration_validation", "support_quality”를 모노드로 가지며 설정된 노드확률테이블은 아래의 표와 같다.

표 6. COTS_quality 노드의 노드확률테이블

development_process		good				Bad			
support_quality		good		bad		good		bad	
integration_validation		good	bad	good	bad	good	bad	good	bad
COTS_quality	good	0.8	0.5	0.5	0.1	0.5	0.1	0.1	0.0
	average	0.2	0.4	0.4	0.4	0.4	0.4	0.4	0.2
	bad	0.0	0.1	0.1	0.5	0.1	0.5	0.5	0.8

소프트웨어의 운전이력 및 오류관리를 의미하는 변수 “operation_record_quality" 노드는 제시된 소프트웨어 신뢰도 수치의 확실성(credibility)을 나타내며 이 노드에 연결된 세부 검토 항목(BBN 그래프에서는 자 노드들)의 평가 결과에 따라 그 상태 값이 결정된다.

◇ 방법-3 : 신뢰도 구간 값을 구할 경우의 BBN

가. 개요

이것은 방법-1 BBN 의 경우와 같이 특정 신뢰도 값의 충족 여부를 구하는 것이 아니라 해당 소프트웨어가 어떤 신뢰도 값(구간 값)을 가질 것인가를 구하는 것이 목적이다. 상용 소프트웨어 인정 프로세스 뿐 아니라 여타의 소프트웨어 개발 방법이나 품질 등과 같은 정성적인 평가 결과와 그 소프트웨어의 정량적인 신뢰도 값의 상관관계를 파악하는 것은 어렵다. 그 이유는 지금까지 특정한 개발 과정(또는 방법론)을 사용하여 만들어진 소프트웨어가 실제 운전 상황에서 운영되었을 때의 경험적 정량적 신뢰도 값이 발표된 적이 드물고 또 실제 운전 상황으로부터 나온 특정 소프트웨어어의 신뢰도 값이 있더라도 소프트웨어의 운전 상황이 달라지면 그 값을 그대로 채용하는데 불확실성이 내포되기 때문이다. 그러나 적절한 소프트웨어 개발 방법론을 준수하여 소프트웨어를 개발하면 그 소프트웨어는 각 산업이나 응용분야에서 요구하는 신뢰도 요구사항을 만족할 수 있다는 것이 소프트웨어 신뢰도에 대한 일반적 인식이고 원자력 산업과 항공산업을 비롯한 각 산업 분야의 국제 표준이나 규제 기관들도 기본적으로는 이런 방침을 취하고 있다. 이 점은 소프트웨어의 정성적인 평가 결과(예를 들면 V&V 에 의한 평가결과)와 그 소프트웨어의 정량적 신뢰도 값의 상관관계를 정량적으로 명확하게 알기는 힘들지만 관계가 밀접하다는

것을 암시적으로 인정하고 있다고 볼 수 있다. 따라서 소프트웨어의 정성적인 평가 결과를 BBN 과 같은 정형적 방법으로 정량적인 신뢰도 값과 연결시켜 이를 분석하는 것은 의미가 있으며 다른 평가 방법들과 더불어 의사결정의 자료로 유용하다고 보여진다.

나. 그래프

그래프는 방법-1 의 BBN 그래프인 그림 3 과 동일하다.

다. 노드확률 테이블

목표 변수(노드)를 제외한 모든 변수와 그래프 그리고 NPT 는 방법-1 과 동일하다. 그러나 여기서는 상용 소프트웨어 인정 프로세스 각 단계에 있는 세부 검토 항목들의 평가 결과를 이용하여 방법-1 의 BBN 과 같이 목표 노드의 각 상태 값(특정 신뢰도 값이 될 확률)을 구하는 것이 아니라 해당 소프트웨어가 어떤 신뢰도 값(구간 값)을 가질 것인가를 구하는 것이 목적이므로 목표 노드 “ COTS_acceptance"의 NPT 는 아래와 같은 형태로 만들어진다.

표 7. 목표 노드 "COTS_acceptance"의 노드확률테이블

operation_history_record		good							
development_process		Good				bad			
Support_quality		Good		Bad		good		bad	
integration_validation		good	Bad	good	bad	good	bad	good	bad
COTS_ acceptance	<0,0.00001]	0.7	0.1	0.1	0.0	0.1	0.0	0.0	0.0
	<0.00001,0.0001]	0.25	0.45	0.45	0.2	0.45	0.2	0.2	0.0
	<0.0001,0.001]	0.04	0.35	0.35	0.25	0.35	0.25	0.25	0.1
	<0.001,0.01]	0.01	0.1	0.1	0.4	0.1	0.4	0.4	0.2
	<0.01,0.1]	0.0	0.0	0.0	0.15	0.0	0.15	0.15	0.6
	<0.1,1]	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1

operation_history_record		Bad							
development_process		Good				Bad			
Support_quality		Good		Bad		good		Bad	
integration_validation		good	Bad	good	bad	good	bad	good	Bad
COTS_ acceptance	<0,0.00001]	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	<0.00001,0.0001]	0.45	0.2	0.2	0.0	0.2	0.0	0.0	0.0
	<0.0001,0.001]	0.35	0.25	0.25	0.1	0.25	0.1	0.1	0.0
	<0.001,0.01]	0.1	0.4	0.4	0.2	0.4	0.2	0.2	0.0
	<0.01,0.1]	0.0	0.15	0.15	0.6	0.15	0.6	0.6	0.1
	<0.1,1]	0.0	0.0	0.0	0.1	0.0	0.1	0.1	0.9

5. BBN 모델의 활용

여기에서는 방법-3 의 상용 소프트웨어 인정 프로세스 BBN 모델에 현실적으로 시나리오에 따른 증거(입력 값)를 만들어 계산한 결과와 그에 대한 논의를 기술하였다. 계산 결과로 나타난 목표 노드의 값은 실제 케이스의 평가 결과에 근거하여 계산된 것이 아니고 또 NPT 의 확률에 전문가의 지식이 충분히 반영되지 않았기 때문에 계산된 결과 값에 대해 절대적인 의미를 부여할 수는 없으나, 시나리오의 계산 결과에 이하면 모델은 전문가의

판단과정을 유사하게 모의하고 있고 일반적으로 예상할 수 있는 결과와 모순되지 않게 나타났다.

5.1 시나리오

시나리오는 다음의 표 8 과 같이 작성되었다.

표 8. 시나리오

시나리오 이름		시나리오 내용	BBN 모델에서 증거 입력 상태
D	D-1	평가 결과 중 1 개의 부정적 결과가 나왔을 경우	1 개의 측정 가능 노드에 부정적 값(no 상태가 100%)이 사용된 경우
	D-2	2 개의 부정적 결과	2 개의 측정 가능 노드에 부정적 값 사용
	D-3	3 개의 부정적 결과	3 개의 측정 가능 노드에 부정적 값 사용
	D-4	4 개의 부정적 결과	4 개의 측정 가능 노드에 부정적 값 사용
	D-5	5 개의 부정적 결과	5 개의 측정 가능 노드에 부정적 값 사용
	D-6	6 개의 부정적 결과	6 개의 측정 가능 노드에 부정적 값 사용

5.2 시나리오 별 계산 결과와 논의

시나리오 적용 대상은 방법-3 의 BBN 이며 하나의 기본 레벨에 시나리오 D-1, D-2, D-3, D-4, D-5, D-6 을 적용한 경우 목표노드의 계산 결과는 아래의 표 9 와 같다.

표 9. 하나의 기본 레벨에 적용한 경우 목표노드 “COTS_acceptance" 계산 결과

목표 노드: COTS_acceptance		시나리오 D 의 경우 목표노드 값					
		D-1	D-2	D-3	D-4	D-5	D-6
상태	<0,0.00001]	0.6919	0.6908	0.6854	0.5257	0.4718	0.4578
	<0.00001,0.0001]	0.2527	0.2530	0.2548	0.3072	0.3249	0.3294
	<0.0001,0.001]	0.0442	0.0447	0.0475	0.1295	0.1573	0.1644
	<0.001,0.01]	0.0112	0.0114	0.0122	0.0371	0.0455	0.0476
	<0.01,0.1]	0.0000	0.0000	0.0000	0.0005	0.0007	0.0007
	<0.1,1]	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

◇ 각 기본 레벨에 속한 세부 검토 항목의 일부(1 개)에 부정적 결과를 적용한 경우에는 목표 노드의 긍정적 상태 “accept" 값이 best case 와 큰 차이가 없는 것으로 나타났다. 이것은 정성적 평가기준을 사용한 전문가의 최종판단과 유사하다고 보여진다.

각기 다른 기본 레벨에 시나리오 D-1, D-2, D-3, D-4, D-5, D-6 을 적용한 경우 목표노드 “COTS_acceptance" 계산 결과는 아래의 표 10 과 같다.

표 10. 다른 기본 레벨에 적용한 경우의 목표노드 “COTS_acceptance" 계산 결과

목표 노드: COTS_acceptance		시나리오 D 의 경우 목표노드 값					
		D-1	D-2	D-3	D-4	D-5	D-6
상태	<0,0.00001]	0.6919	0.6915	0.6915	0.6837	0.5820	0.5720
	<0.00001,0.0001]	0.2527	0.2528	0.2528	0.2554	0.2883	0.2905
	<0.0001,0.001]	0.0442	0.0444	0.0444	0.0484	0.1004	0.1050
	<0.001,0.01]	0.0112	0.0113	0.0113	0.0125	0.0288	0.0314
	<0.01,0.1]	0.0000	0.0000	0.0000	0.0000	0.0006	0.0012
	<0.1,1]	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

◇ 부정적 관찰 결과를 한 개의 기본 레벨 노드에 적용한 결과와 여러 개의 기본 레벨 노드에 분산하여 적용한 계산 결과에서 나타난 사항은 다음과 같다.

(a) 부정적 관찰 결과를 각 기본 레벨 노드에 분산하여 적용할 경우에는 목표 노드의 상태 값에 큰 변화가 없다(표 9 및 그림 4(a) 참조).

(b) 그러나 부정적 관찰 결과를 하나의 기본 레벨 노드에 적용할 경우에는 목표 노드의 상태 값에 상대적으로 큰 변화가 생긴다. 특히 부정적 값의 입력 대상이 되는 기본 레벨의 전체 검토 항목 수의 절반을 초과하여 부정적 관찰 결과를 입력했을 때는 목표 노드의 상태 값이 상대적으로 많이 변한다(표 10 및 그림 4(b)참조).

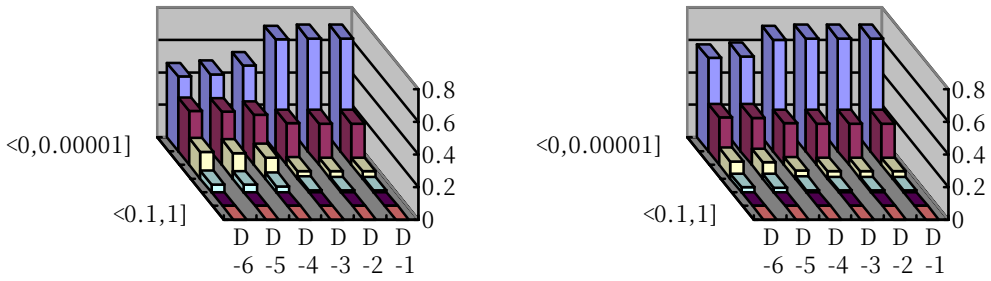

그림 4. (a) 하나의 기본레벨 적용 경우 (b) 다른 기본레벨 적용 경우

위의 예에서 나타난 시나리오 같이 실제의 상황에서도 특정 단계에 집중적으로 부정적 평가 결과들이 나올 경우와 각 단계에 분산되어 부정적 평가 결과들이 나올 수 있다. 위와 같은 방식으로 만들어진 BBN 에서는 부정적 평가 결과가 나온 세부 검토 항목의 개수가 같더라도 그 항목들이 하나의 기본 단계에 집중되어 있는가 아니면 각기 다른 단계에 분산되어 있는가에 따라 최종 평가(목표 변수의 상태 값)가 달라진다. 따라서 평가 대상이 되는 시스템(상용 소프트웨어)의 특성을 고려하여 사전에 각 노드의 조건부 확률(노드 사이의 관계 강도)을 조정하는 것이 필요하다고 보여진다.

6. 결론 및 추후 연구내용

기존에 채택되고 있는 소프트웨어의 정성적인 평가 방법을 BBN 을 이용하여 PSA 에서 필요로 하는 정량화 된 결과를 구하는 방안을 원전 상용소프트웨어 인정 프로세스를 시험케이스로 시험적 연구를 수행하였다. 안전소프트웨어의 신뢰도 평가에 BBN 방법론을 적용한 이유는 (a) 신뢰도 평가에 관련된 다양한 증거들(과정, 제품 정보, 경험적 자료, 전문가의 판단, 불완전한 정보 등)을 일관된 평가체제 안에서 정형적으로 결합하여 정량적 결론(확률)을 추론할 수 있고 (b) 모델의 직관적 그래프 형태가 평가에 관련된 복잡한 연관 관계와 감추어진 가정들을 명시적으로 나타내어 결론이 도출되는 과정에 대한 투명도를 높일 수 있으며 (c) 불확실하거나 애매한 증거들이 필연적으로 포함되는 신뢰도 평가에 있어서 "what if" 분석을 가능하게 해주므로 의사결정에 있어 효과적인 도구로 사용할 수 있기 때문이었으며 본 시험적 연구를 통하여 이를 확인할 수 있었다.

본 연구의 최종 목표는 원전의 안전계통에 사용되는 디지털 시스템의 위험도 평가에 필요한 안전 소프트웨어의 신뢰도를 구하는 방안을 마련하는 것이며 이를 위하여 앞으로 연구되어야 할 내용과 고려사항은 다음과 같다.

◇ BBN 방법론 분야

만들어진 BBN 모델이 기존 규칙 기반의 정성적 평가 시스템을 적절하게 반영했는가에 대한 검증과 BBN에 사용되는 주관적 확률 값 설정에 대한 연구가 필요하다.

◇ BBN 모델의 대상이 되는 안전 소프트웨어의 신뢰도 평가 틀(frame) 선정

BBN 모델의 대상이 되는 소프트웨어 평가 틀을 선정할 때, 규제나 표준 틀을 모델 대상으로 할 경우에는 범용성이 있고 검증이 상대적으로 용이하나, 특정 소프트웨어는 개발팀이나 조직에서 자체적으로 만든 검증/평가 문서(지침서 등)에 따라 검증이나 평가가 수행되므로 얻어진 평가 자료를 모델에 사용하기 어려운 점이 있다. 반면, 개발 조직이나 특정 시스템의 개발/검증 틀을 모델 대상으로 할 경우에는 평가 결과 자료와 모델의 연계성은 좋지만 모델의 기반이 되었던 해당 개발/검증 틀이 적절한가에 대한 2 차적 검증을 고려해야 한다.

감사의 글

이 논문은 대한민국 과학기술부에서 시행하는 원자력연구개발 중장기사업의 지원으로 수행되었습니다.

참고문헌

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

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

[3] 경수로형 원전 안전심사지침, 한국원자력안전기술원, 1998

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

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

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

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

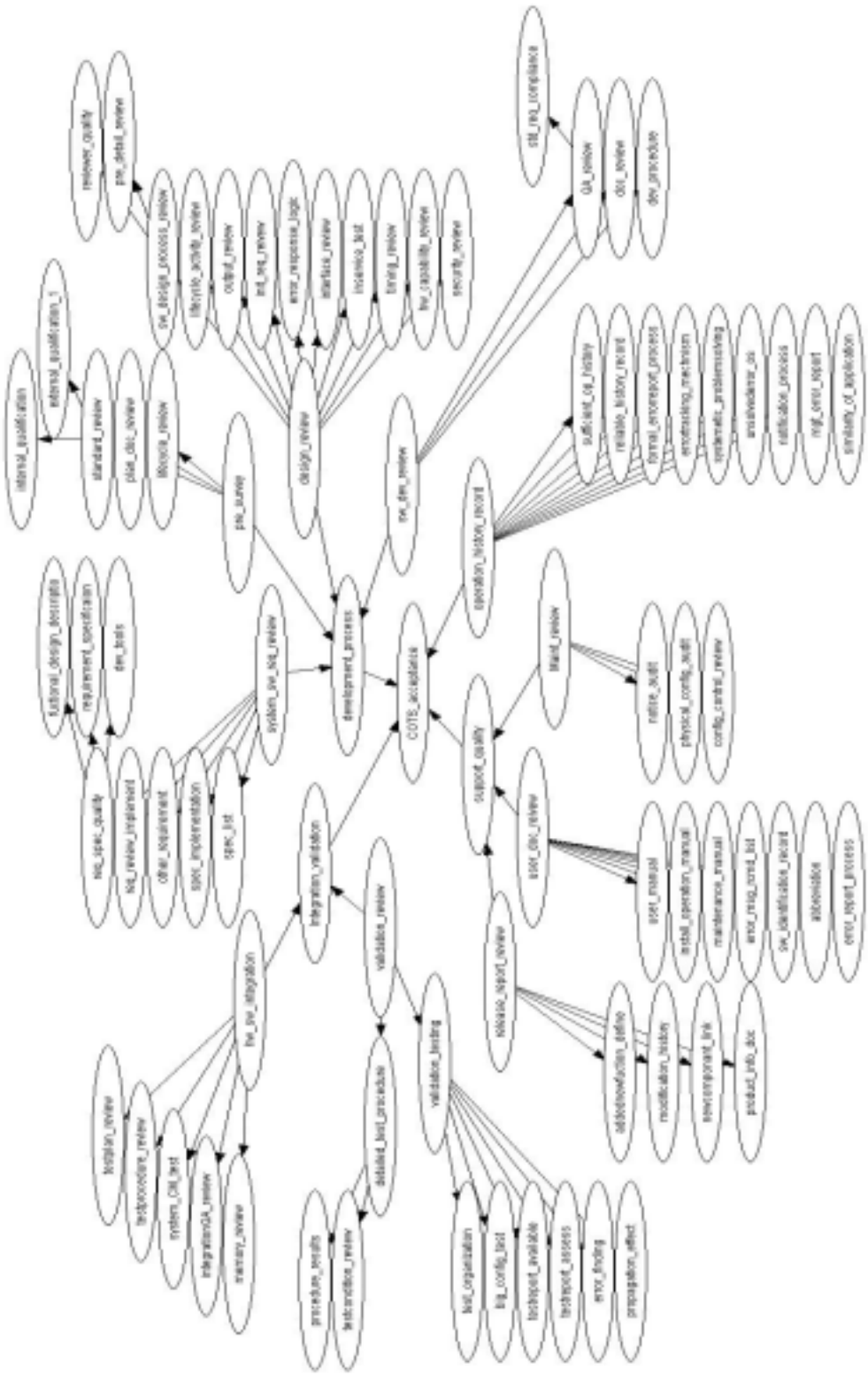

그림 A-1. 상용 소프트웨어 평가용 기본 BBN 그래프