STPA와 Petri Nets의 연계: 음성인식 기반 제조 안전시스템 사례 연구

임태형, 김두환, 양상운
한국정보통신기술협회
thyim@tta.or.kr, enghks0605@tta.or.kr, sangoon@tta.or.kr

Integration of STPA and Petri Nets: A Case Study of Speech Recognition-based Safety System for Manufacturing

Taihyong Yim, Doohwan Kim, Sangoon Yang
Telecommunications Technology Association

요 약

본 논문은 위험 분석 기법인 STPA와 정형 분석 이론인 Petri Nets의 연계 방안을 제안한다. 음성인식 기반 제조 안전 시스템의 사례 연구를 통해 STPA의 정성 분석과 Petri Nets의 정량 분석을 상호보완적으로 활용하면, STPA를 단독으로 사용할 때와 비교하여 위험 분석의 객관성과 신뢰도가 향상될 수 있음을 확인하였다. 시스템 이론에 기반한 STPA로 시스템의 동작 맥락에서 예외적, 돌발적 사고 시나리오를 도출하고, 이를 Petri Nets의 불변량 분석, 도달성 그래프 분석, 시뮬레이션으로 분석하면 위험 요인을 통제·관리하기 위한 객관적이고 명확한 기준을 수립할 수 있다.

Ⅰ. 서 론

시스템 규모가 커지고, 복잡해지면서 STPA(System Theoretic Process Analysis)[1]가 주목받고 있다. STPA는 운영 환경을 포함한 시스템의 동작 맥락에서 구성요소 사이의 상호작용에 초점을 맞춤으로써 기존 위험분석 기법이 찾지 못한 예외적이고, 돌발적인 시스템 반응을 일으키는 위험요인을 찾을 때 효과적이다.

반면, STPA는 정성 분석 기법이므로 식별된 여러 위험 요인의 발현율, 파급력 등을 측정·비교하는 정량 분석을 제공하지 않는다. 여러 위험 요인이 존재할 때, 모든 위험 요인이 동일 발현율, 파급력을 갖지 않으므로 위험 요인을 구분하여 제한된 자원을 잘 분배하고, 위험 대책을 마련해야 한다. STPA로 위험 분석을 수행하더라도 위험 요인의 우선순위를 결정하거나, 위험 요인의 조건, 상태 변화가 안전에 얼마나 영향을 끼치는지 등을 분석할 때 다른 분석이 추가로 요구된다. 본 논문은 음성인식 기반 제조 안전 시스템의 사례 연구를 통해 위험 분석 기법인 STPA와 정형 분석 이론인 Petri Nets[2]의 연계 방안을 제안한다.

Ⅱ. 본론

위험 분석 대상 시스템은 음성인식 기반 제조 안전 시스템이다. 제조 설비를 운행하는 작업자가 위험 상황에서 음성인식 기능으로 설비를 긴급 중단시킬 수 있다. 제조 환경에서 작업자 안전을 위해 도입된 음성인식 시스템은 가정용 음성인식 시스템보다 음성인식의 정확도, 시스템의 가용성, 반응 속도 등 다양한 측면에서 높은 성능 수준을 요구한다. 따라서 개발 단계 초기부터 위험 분석을 실시하여 시스템이 요구수준을 충족시킬 수 있는지 확인하는 것이 매우 중요하다. 본 논문에서는 STPA와 Petri Nets을 연계하여 위험 분석을 실시하였다. 제안하는 STPA와 Petri Nets의 연계 방법은 다음과 같다.

① STPA로 음성인식 오작동과 관련한 사고 시나리오를 도출
② 도출된 사고 시나리오를 Petri Nets 모델로 개발
③ Petri Nets 모델의 불변량 분석, 도달성 그래프 분석, 시뮬레이션 실시
④ Petri Nets 분석 결과를 활용하여 위험 대책 수립 및 위험 관리

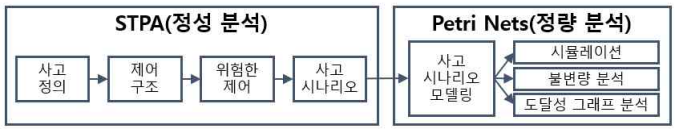

그림 1. STPA와 Petri Nets의 연계 방안

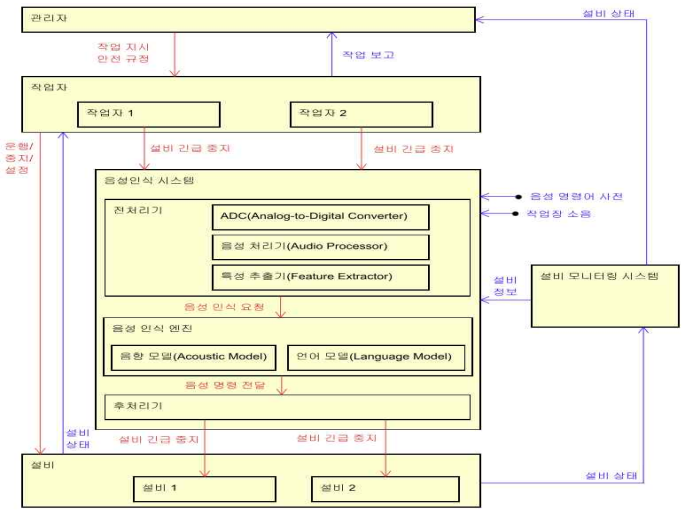

그림 2. STPA 제어 구조

표 1. STPA 분석 결과 도출된 사고 시나리오 유형

사고 시나리오 유형	건수	비율
시스템 외부 환경요인	9	31.03%
잘못된 제어 조치 입력 또는 제어 조치 누락	7	24.14%
지연 제어	5	17.24%
제어 충돌	4	13.79%
상황 인지 오류	2	6.90%
제어 명령 훼손 또는 손실	2	6.90%
합계	29	100.00%

STPA 분석 결과 <표 1>과 같이 여러 유형의 사고 시나리오가 도출되었으며, 외부 환경요인으로 사고가 발생하는 시나리오가 29건 중 9건(31.03%)으로 가장 많이 도출되었다. 이에 해당하는 '교육 실패', '이상 소음', '안전 장비'의 3가지 사고 시나리오를 Petri Nets 분석 대상으로 선정하였다.

- 사고 시나리오 1. 작업자에게 음성인식 시스템 사용 교육이 제대로 제공되지 않아 긴급 상황에서 음성인식 시스템을 활용하지 못하고, 설비가 계속 운행되어 사고가 발생함
- 사고 시나리오 2. 위험 상황에서 작업장 이상 소음으로 음성인식이 실패하고 설비가 계속 운행되어 사고가 발생함
- 사고 시나리오 3. 안전장비(마스크, 방청귀마개)를 착용한 작업자가 위험 상황에서 음성인식으로 설비 운행 정지를 시도했으나, 음성인식이 실패하여 사고가 발생함

각 시나리오는 사고가 발생하는 독립 사건이지만, 동시에 발생할 수도 있다. 또한, 각 시나리오의 원인이 발현될 확률은 각각 다를 수 있다. 실제 운영 환경을 가정하여 위험 요인들의 발현율을 설정하고 Petri Nets 모델을 개발했으며, 불변량 분석, 도달성 그래프 분석, 시뮬레이션을 수행하였다.

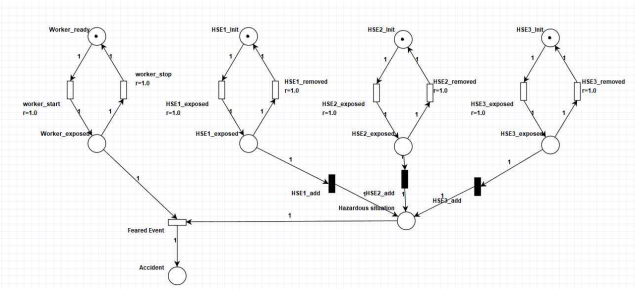

그림 3. Petri Nets 사고 모델

Petri Nets 불변량 분석과 도달성 그래프 분석은 사고가 발생하는 과정을 모델의 구조로 해석한다. 사고를 일으키는 특정 사건이 교착 관계나 무한 루프를 형성하는지, 고정된 순서나 패턴이 있는지 등의 구조적 특성을 불변량 분석과 도달성 그래프로 확인할 수 있다. 1개의 위험 요인만 고려한 Petri Nets 모델의 경우, 작업자는 사고 모델의 구조 상 위험 요인이 존재하지 않는 상태, 위험 요인이 생성된 상태, 사고 상태 중 하나의 상태에만 머물며, 여러 상태를 동시에 겪을 수 없다. 사고는 작업자가 작업 중이고, 위험 요인이 발현된 상태에서만 발생하고, 위험 요인이 생성되더라도 작업자가 대기 중이면 사고가 발생하지 않으며, 작업자의 작업 시작과 위험 요인의 발생은 순서 관계없이 사고를 일으킬 수 있다. 위험 요인이 2개, 3개로 늘어나면 <그림 4, 5>와 같이 더욱 복잡한 구조적 특성을 분석할 수 있다. 이러한 분석 결과는 작업자가 어떤 상태에 오래 머물지 예측할 수 있는 견고한 수학적 근거가 된다.

구조 해석이 완료된 사고 시나리오에 대해 Petri Nets 시뮬레이션을 수행하여 위험 요인의 발현율과 위험 요인의 중첩이 사고 발생에 끼치는 영향을 정량적으로 확인하였다. 이는 STPA의 정성 분석으로 찾은 위험 요인을 모니터링하고 통제·관리하는 객관적이고, 명확한 기준을 제공해주며, 위험 대책을 마련하는 중요한 근거를 제공한다. 시뮬레이션 결과, 위험 요인의 발현율 증가와 위험 요인의 중첩은 사고 발생 확률을 증가시키지만, 개별 위험 요인의 발현율이 위험 요인의 중첩보다 사고 발생에 더 큰 영향을 끼침을 알 수 있다. 즉, 발현율이 낮은 위험 요인은 여러 위험 요인이 동시에 발현되는 것까지 고려할 필요 없지만 발현율이 높은 위험 요인이 하나라도 존재한다면 해당 위험 요인을 적극 모니터링하고, 다른 위험 요인과의 동시 발현 상황까지도 고려한 종합적인 위험 대책이 필요하다.

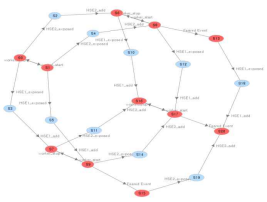

그림 4. Petri Nets 도달성 그래프(위험 요인 2개)

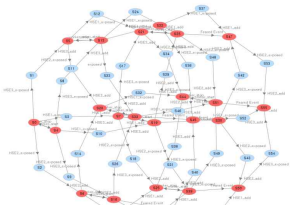

그림 5. Petri Nets 도달성 그래프(위험 요인 3개)

표 2. 위험 요인 발현율에 따른 사고 발생 영향도

위험 요인 발현율	평균 토큰 수	
	위험 요인 노출 상태	사고 상태
1회/1개월	0.0041	0.00205
1회/1일	0.04412	0.01472
1회/8시간	0.15	0.05
1회/4시간	0.5	0.1667
1회/1시간	0.5	0.25

표 3. 위험 요인 중첩에 따른 사고 발생 영향도

위험 요인 수	위험 요인 발현율	평균 토큰 수	
		위험 요인 노출 상태	사고 상태
1개	1회 / 1개월 (교육 실패) 1회 / 1시간 (이상 소음) 5회 / 1시간 (안전 장비)	0.0041	0.00205
2개		0.33333	0.33333
3개		0.25113	0.55556

Ⅲ. 결론

STPA의 정성 분석과 Petri Nets의 정량 분석을 상호보완적으로 활용하면, STPA를 단독으로 사용할 때와 비교하여 위험 분석 결과의 객관성과 신뢰도가 향상된다. STPA는 시스템 관점에서 다양한 위험 요인을 찾도록 돕지만 식별된 사고 시나리오가 어느 정도의 확률로 발생할지 등의 정량 분석은 제공하지 않는다. STPA의 정성 분석 결과는 위험 대책 범위와 방향 결정에 도움을 주지만 어느 위험에 더 많은 자원을 투입해야 할지는 답하지 못한다. Petri Nets의 정형 분석은 STPA의 정성 분석으로 찾은 위험 요인을 모니터링하고 통제·관리하는 객관적이고, 명확한 기준을 제공해주며, 위험 대책을 마련하는 중요한 근거를 제공한다. STPA와 Petri Nets의 연계는 독립적인 여러 위험 요인들이 동시에 발현되는 상황에서의 사고 발생 확률까지 분석하여 위험 요인을 개별적으로 취급하지 않고, 시스템 이론에 기반한 종합적인 사고 대책을 마련하는데 좋은 접근방법이다.

참 고 문 헌

[1] N. G. Leveson and J. P. Thomas, "STPA Handbook," Cambridge, MA, USA: MIT Press, 2018, (http://psas.scripts.mit.edu/home/materials/)

[2] Jean F.A., Nicolae B., Mohammed H. M., "Systems Dependability Assessment: Benefits of Petri Net Models," Wiley-ISTE, 2016