STPA를 활용한 누수 탐지 시스템의 위험분석 사례 연구

김나영, 안신미, 임해찬

한국정보통신기술협회

nykim@tta.or.kr, smahn226@tta.or.kr, ohaechano@tta.or.kr

A Case Study on Risk Analysis of Leak Detection System Using STPA

Kim Na Young, Ahn Shin Mi, Im Hae Chan

Telecommunications Technology Association

요 약

본 논문은 상수도관에서 발생하는 누수를 탐지하기 위한 누수 탐지 시스템에 잠재된 위험을 분석하고, 시스템에서 발생할 수 있는 위험에 대한 안전 대책이 충분히 반영되어 있는지 검증하는 방안을 소개한다. STPA 기법을 활용하여 누수 탐지 시스템의 구성요소 간의 제어 관계를 통해 불안전 제어 조치를 식별하고, 이에 대한 손실 시나리오를 식별하였다. 최종적으로 손실 시나리오가 가장 많이 식별된 시스템 구성요소를 대상으로 시스템에 위험에 대한 안전 대책이 충분히 반영되어 있는지를 검증하였다.

Ⅰ. 서 론

지하 깊숙한 곳에 매설된 상수도관에서 발생하는 누수를 탐지하기 위한 누수 탐지 시스템(Leak Detection System, LDS)은 인공지능 기술을 활용하여 굴착 없이 원격으로 누수 발생 여부와 누수가 발생한 위치를 탐지하는 기능을 제공한다. LDS가 정상 동작할 경우, 누수를 신속하고 정확하게 탐지하여 누수로 인한 피해를 최소화하고, 상수도 시스템 운영의 효율성을 향상한다.

반면, LDS가 누수 발생을 적시에 탐지하지 못하거나 누수가 발생한 위치를 잘못 판단할 경우, 상수도의 공급이 중단되거나 불필요한 상수도 운영 비용이 발생하는 등의 손실이 발생한다. 즉, LDS는 재산상의 큰 손실을 유발하는 안전 필수 시스템(Safety-critical System)이므로 위험분석이 필수적으로 요구된다.

최근 LDS의 구성과 로직이 복잡해지면서 FMEA(Failure Mode and Effect Analysis)나 FTA(Fault Tree Analysis)만으로는 위험분석을 수행하는 데에 한계가 있다. 본 논문은 STPA(System Theoretic Process Analysis)[1] 기법을 활용하여 시스템에 잠재된 위험을 분석하고, 최종적으로 시스템에서 발생할 수 있는 위험에 대한 안전 대책이 충분히 반영되어 있는지 검증한다.

Ⅱ. 적용 대상 시스템

위험분석 적용 대상인 LDS는 상수도관에서 누수가 발생한 위치와 누수의 심각한 정도를 판별하여 관리자가 조기에 사고에 대응할 수 있도록 지원한다. LDS는 누수음 수집 센서와 상수관망 및 지리 정보를 포함하는 국가 지리 정보 시스템(GIS)이 연동되어 동작한다. 센서로부터 수집된 누수음 진동 데이터는 GIS 데이터와 함께 LDS로 전달되어, 실시간으로 누수 발생 여부와 누수가 발생한 위치를 판단한 후, 관리자에게 대시보드를 통해 분석 결과가 제공된다. LDS는 외부 시스템과의 연계, 딥러닝 기술을 활용한 누수 탐지, 대시보드를 통한 누수 탐지 결과의 시각화 등으로 인해 기존의 누수 탐지 시스템보다 높은 성능이 요구된다.

Ⅲ. STPA 적용 결과

STPA는 사고 및 위험을 정의하는 것에서 시작된다. 이후 시스템 구성요소 간의 제어 관계에 따라 도식화한 후에 불안전한 제어 조치를 식별하고, 마지막으로 불안전 제어 조치에 대한 손실 시나리오를 식별한다.

① 사고, 손실 및 위험 정의

LDS에서 가장 치명적인 사고는 심각한 상수도 누수 발생으로 인해 상수도 공급이 중단되거나, 불필요한 상수도 누수 탐사로 인해 상수도 운영 비용 손실 피해가 발생하는 것이다.

표 1. STPA 분석 결과 도출된 사고 목록

ID	사고(Accident) 목록
A-1	심각한 상수도 누수가 발생함
A-2	불필요한 상수도 누수 탐사(굴착)를 수행함

표 2. STPA 분석 결과 도출된 손실 목록

ID	손실(Loss) 목록
L-1	상수도 공급이 중단됨
L-2	상수도 운영 비용이 손실됨

표 3. STPA 분석 결과 도출된 위험 목록

ID	위험 목록(System-level Hazard)	관련 손실
H-1	누수 미탐	L-1
H-2	누수 오탐 · 상수도의 누수를 잘못 감지 · 상수도의 누수를 감지했으나, 잘못된 위치가 측정됨	L-1, L-2

② 제어구조(Control Structure) 도식화

제어구조는 누수를 탐지하는 LDS와 제어 대상인 상수도관을 포함하여 누수음 수집 센서, 상수도 누수 관리자 및 국가 지리 정보 시스템으로 구성된다. 제어구조에서 제어 조치(Control Action)는 최종 의사결정권자인 관리자가 LDS로부터 제공되는 누수 위치와 누수 상태를 전달받아 현장 탐사를 수행하는 것이다.

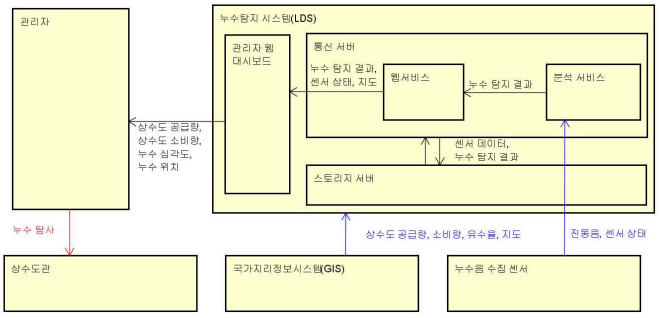

그림 1. STPA 분석 결과 도출된 제어구조

③ 불안전 제어 조치(Unsafe Control Action) 식별

제어구조의 제어 명령에 대한 불안전 제어 조치는 다음과 같다.

표 4. STPA 분석 결과 도출된 불안전 제어 조치 목록

제어조건	위험 제어 조치			
	필요 제어 미제공	불필요 제어 제공	늦은/이른 제어	과잉/불충분 제어
검출해야 할 누수가 발생할 때	UCA1	-	UCA2	-
검출해야 할 누수이나, 위치 오차가 발생할 때	-	UCA3	-	-
검출이 불필요한 누수가 발생할 때	-	UCA4	-	-

* UCA1: 검출해야 할 누수가 발생할 때, 관리자가 누수를 탐사하지 않음
* UCA2: 검출해야 할 누수가 발생할 때, 관리자가 누수를 늦게 탐사함
* UCA3: 검출해야 할 누수이나 위치 오차가 발생할 때, 관리자가 누수를 탐사함
* UCA4: 검출이 불필요한 수준의 누수가 발생할 때, 관리자가 누수를 탐사함

④ 손실 시나리오(Loss Scenarios) 식별

불안전 제어 조치에 대한 여러 유형의 손실 시나리오를 식별한 결과, 제어 결정 결함으로 인해 사고가 발생하는 시나리오가 170건 중 61건(35.88%)으로 가장 많이 도출되었다.

(시나리오 1) 검출해야 할 수준의 누수가 발생했을 때, 누수 분석 서비스에서 모델의 과적합으로 인해 누수 판단 오류가 발생하여 웹서비스에 누수 탐사 제어 조치가 전달되지 않아 관리자가 누수를 탐사하지 않음

(시나리오 2) 검출해야 할 수준의 누수이나 위치 오차가 발생했을 때, 누수 분석 서비스에서 평가 데이터의 독립성 가정 위반으로 인해 누수 판단 오류가 발생하여 웹서비스에 누수 탐사 제어 조치가 전달되어 관리자가 불필요하게 누수를 탐사함

(시나리오 3) 검출이 불필요한 수준의 누수가 발생했을 때, 누수 분석 서비스에서 학습 데이터의 수량 부족으로 인해 누수 판단 오류가 발생하여 웹서비스에 누수 탐사 제어 조치가 전달되어 관리자가 불필요하게 누수를 탐사함

표 5. STPA 분석 결과 도출된 손실 시나리오 유형

손실 시나리오 유형	건수	비율
센서 결함	10	5.88%
피드백 정보 훼손 또는 손실	6	3.53%
피드백 정보 지연	19	11.18%
제어기 결함	29	17.06%
상황 인지 결함	11	6.47%
제어 결정 결함	61	35.88%
잘못된 제어 입력	32	18.82%
제어 입력 누락	2	1.18%
합계	170	100.00%

표 6. STPA 분석 결과 도출된 시스템 요소별 손실 시나리오 유형

시스템 구성요소	건수	비율
누수음 수집센서	13	7.60%
관리자	17	10.00%
관리자 대시보드	7	4.10%
분석 서비스	68	40.00%
웹 서비스	7	4.10%
통신서버	19	11.20%
스토리지 서버	17	10.00%
누수음 수집센서 및 통신서버 간 통신	11	6.50%
국가지리정보시스템 및 통신서버 간 통신	11	6.50%
합계	170	100.00%

Ⅳ. 안전대책 검증 결과

LDS에 STPA를 적용한 결과, 8개의 시스템 구성요소 중에서 분석 서비스에서 가장 큰 손실 시나리오(68건, 40%)가 식별되었다. 분석 서비스는 센서 데이터를 주파수로 변환하여 주파수 신호와 누수량, 수압 데이터의 상관분석을 통해 누수 발생 여부(확실, 의심, 정상)를 판단하므로, 분석 서비스에 적용된 인공지능(Artificial Intelligence, AI) 모델과 AI 데이터 관련 위험에 대한 안전대책이 충분히 반영되어 있는지 검증하였다.

AI 데이터는 모델의 학습용과 평가용에 따라 누수 발생 여부를 기준으로 분류된다. AI 데이터는 구조 및 형식의 적합성 통계적 다양성, 구문 및 의미적 정확성에 대한 품질 검증이 요구되며, 검증 결과는 <표 7>과 같다.

표 7. AI 데이터의 안전대책 검증 결과

검증 항목		결과
적합성	데이터 포맷 불일치	0%
	데이터 형식 불일치	0%
다양성	클래스 불균형(확실, 의심, 정상)	30.24%, 18.77%, 51.00%
정확성	데이터 결측	0%
	데이터 라벨링 오류	1.34%

AI 모델은 주파수 데이터를 입력받아 누수 발생 여부를 출력한다. AI 모델은 기존의 평가용 데이터를 활용한 모델 성능과 변조된 평가용 데이터를 활용한 모델의 강건성 검증이 요구되며, 검증 결과는 <표 8>과 같다.

표 8. AI 모델의 안전대책 검증 결과

검증 항목		결과
성능	정확도(Accuracy)	99.2%
강건성	T-검정(T-검정 통계량, P-value)	0.083, 0.74
	모델 정확도	60.86%

Ⅴ. 결론

누수 탐지 시스템은 누수로 인한 상수도 공급 중단 및 불필요한 누수 탐사에 따른 운영 비용 손실이 발생하는 안전 필수 시스템으로, 복잡한 컴포넌트와 로직으로 구성되어 있어 STPA 기법을 활용한 위험분석이 효과적이다. 본 논문에서는 누수 탐지 시스템의 개발 및 운영 측면에서의 안전을 확보하기 위해 STPA 기법을 적용하여 정성적인 위험분석 결과를 도출하고, 시스템에 위험에 대한 안전 대책이 충분히 반영되어 있는지를 검증하였다. 그 결과, 누수 발생 여부를 판단하는 분석 서비스에서 가장 많은 손실 시나리오가 식별되었으며, 분석 서비스에 활용된 AI 데이터의 클래스 불균형 및 AI 모델의 강건성 오류에 대한 대책이 필요함을 확인하였다. 향후에는 누수 탐지 시스템에 사용되는 AI 데이터의 불균형 개선 및 AI 모델의 강건성 확보를 위한 AI 데이터 수집 전략에 대한 연구를 진행할 예정이다.

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/)