정형기법을 통한 위기대응 매뉴얼 신뢰성 향상

정금택, 이 혁, 서 석, 최진영
고려대학교 컴퓨터학과
e-mail: {jkt76, hlee, choi}@formal.korea.ac.kr, s_suh@korea.ac.kr

Security Improvement of Crisis Response Manual using Formal Methods

Kum-Taek Jeong, Hyuk Lee, Suk Seo, Jin-Young Choi
Dept. of Computer Science & Engineering, Korea University

요 약

위기대응 매뉴얼은 지진, 태풍 등 상황에 적절하게 적용되며 신뢰성 있게 작동한다는 것이 보장되어야 한다. 따라서 위기대응 매뉴얼의 검증은 필수적이며, 이를 위해 본 논문에서는 정형기법 도구인 Statemate를 이용한 명세, 검증 및 신뢰성 개선방안을 제시한다. 모델체킹을 통해서 매뉴얼 사용자들의 임의적인 판단을 일의킬 수 있는 Non-Determinism과 대응 매뉴얼이 달성하고자 하는 목표의 도달여부에 대해 검증을 수행할 수 있으며, 이외에도 사용자가 원하는 검증 속성을 Temporal Logic으로 작성해서 검증할 수 있다. 또한 도구에서 지원하는 시뮬레이션을 통해 제한적이지만 조치내용의 적절성 여부와 추가적으로 발생 가능한 트리거를 찾음으로써 위기대응 매뉴얼의 신뢰성을 향상시킬 수 있다.

1. 서론

+정상사고(Normal Accident) 사례 중의 하나인 쓰리마일섬 핵 발전소 사고의 경우와 같이 상황별 대응매뉴얼이 만들어졌다 하더라도 예상치 못한 상황이 발생하거나[1], 대구 지하철 사고와 같이 대응매뉴얼이 부적절한 경우, 그리고 조치절차가 하나의 동일상황에 대해 두 가지 이상의 판단이 수행될 수 있는 경우 위기상황에 대한 피해규모는 커질 수 있다. 2003년 대구지하철 사고를 계기로 정부 각 부처는 발생의 빈도는 낮지만 발생시 큰 피해가 예상되는 안보, 재난, 국가핵심기반 등의 분야에 대해 즉각적으로 수행해야 할 행동절차와 조치사항을 구체적으로 규정한 '위기대응 실무매뉴얼'을(총 272개) 2005. 11월 완성하였다.

위의 사례들을 통해서도 알 수 있듯이 위기대응 매뉴얼은 의도된 상황에 적절히 적용되며 신뢰성 있게 작동된다는 것이 보장되어야 한다. 따라서 대응매뉴얼의 보장을 위한 검증은 필수지만 실제 검증을 수행한 사례는 발견하기 어렵다. 위기대응 매뉴얼 검증 방안으로 실제 유사한 환경을 구축해서 매뉴얼을 적용해 보는 방안이 있지만 시간, 비용, 기술적 문제 등의 제약으로 수행하는데 어려움이 따른다. 이에 대한 대안으로 시뮬레이션과 정형명세를 통한 검증이 있다. 시뮬레이션은 상황이 발생할 수 있는 유사한 환경을 컴퓨터로 구현해서 실제 매뉴얼을 적용해 보는 것이며, 정형명세를 통한 검증은 추상화된 모델을 명세한 후 정형검증을 수행하는 방법이다. 본 논문에서는 위기대응 매뉴얼의 검증방안으로 정형기법 도구를 활용한 명세 및 검증방안을 제시하고 검증결과를 통해 위기대응 매뉴얼의 신뢰성을 향상하고자 한다.

+ 찰스페로우가 1984년에 발표한 서적으로 정상사고이론에 따르면 현대사회 시스템의 상호작용에 대한 복잡도가 높아지고 결합도가 강해짐에 따라 사고는 피할 수 없으며 이는 지극히 정상적이라는 이론

2. 관련 연구

2.1 정형 기법

정형기법은 소프트웨어 시스템의 명세, 디자인, 검증을 위해 수학적 모델을 사용하는 기술 및 도구들의 집합으로 정형명세와 정형검증이 있다. 정형명세의 사용은 위기대응 매뉴얼에 내포되어 있을 수 있는 에러를 줄이고 모호성을 줄이기 위해서 사용된다. 정형검증은 정형명세를 분석하여 무모순성, 정확성을 검증하거나 설계가 주어진 가정에서 요구사항을 만족하였는지를 검증하는 기법이다[2].

2.2 STATEMATE

STATEMATE는 시스템을 기능적, 행위적, 구조적 관점으로 명세하고 시뮬레이션 할 수 있는 Reactive 시스템 명세에 적합한 직관적인 언어이다. 위의 세 가지 관점에 따라 액티비티 챠트, 상태 챠트, 모듈 챠트로 나눌 수 있다[3]. 액티버티 챠트는 기능의 입·출력을 명세하며, 각 액티버티는 입·출력이 발생하는 이벤트, 조건 및 그 행위를 명세하는 상태챠트를 통해 통제받게 된다. 모듈챠트는 구조적 관점에서 시스템을 명세함으로써 시스템의 물리적 구성을 제시해 준다. 명세언어를 통해 모델이 완성되면 시뮬레이션을 할 수 있으며, 검증하고자 하는 속성에 대해 모델체킹이 가능하다.

3. 위기대응 실무매뉴얼 모델

3.1 위기대응 실무매뉴얼 명세

위기대응 매뉴얼의 정형명세 과정은 대응매뉴얼이 달성해야 할 목표 즉 속성을 식별하고 속성을 만족할 수 있도록 지속적으로 명세를 수정하는 것이다. 또한 매뉴얼이 실행되는 환경의 컴포넌트를 식별하고 이들 컴포넌트간의 입·출력되는 데이터를 파악하며, 적절하게 추상화된 모델을 통해 효과적인 검증이 수행되도록 한다[4]. 모든 위기대응 매뉴얼은 작성 목표, 대응체계도(부서별 임무), 조치사항, 조치 세부내용의 공통된 프레임워크를 가지고 있는데 이는 <표 1>과 같이 Statemate 구조적, 기능적, 행위적 관점의 챠트로 대응시킬 수 있다.

<표 1> 위기대응 매뉴얼 구성에 따른 Statemate 명세

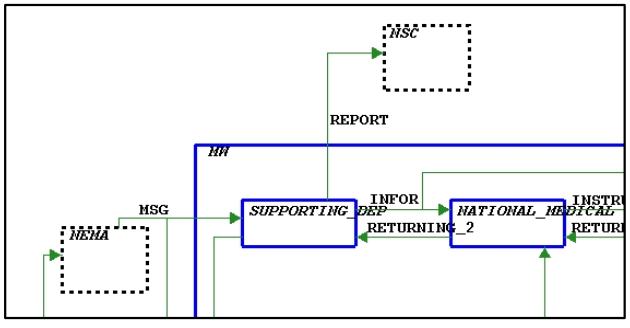
위기대응 매뉴얼	STATEMATE
작성 목표	검증 속성
대응 체계도(조직도)	모듈(Module) 챠트
조치 사항	액티비티(Activity) 챠트
조치 세부내용	상태(State) 챠트

3.2 적용 사례

272개 매뉴얼 중 “지진-의료지원”분야를 대상으로 실제 적용해보면 지진발생에 따른 위기대응 매뉴얼의 작성목표는「피해 범위/규모 등의 신속한 상황파악 및 초동조치」로써 조치사항은 크게 지진상황 파악 및 전파, 대응조직 구성 및 초동조치, 긴급 대응조치, 복구 또는 후속조치의 4단계로 구성되어 있으며 각 단계별로 조치 세부내용이 있다. 각 조치사항은 조치 세부내용을 통해 수행 시기/조직/내용 등이 상세히 기술된다. 대응목표와 조치내용을 Statemate의 각 챠트로 실제 적용해 보면 다음과 같으며 [5] 논문의 명세를 위기대응 매뉴얼 구성과 같이 4단계 조치목록으로 재구성하였다.

○ 검증 속성
- 인명피해를 접수 받게 되면 응급치료를 수행하는 상태에 반드시 도달한다.
- 지진 발생시 매뉴얼 대로 수행하면 보고를 수행하는 상태에 도달할 수 있다.

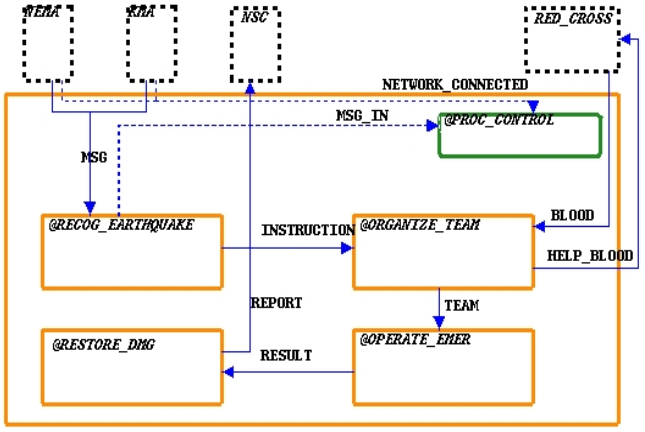
○ 모듈 챠트(Module-Chart)



(그림 1) 대응조직 모듈 챠트

(그림-1)은 지진발생시 긴급 의료지원을 수행하는 조직의 대응체계도 일부를 모듈챠트로 나타낸 것으로 외부환경과 내부 컴포넌트간의 주고받는 메시지를 명세한다. (그림-1)에서 외부환경은 소방방재청(NEMA), 국가안전보장회(NSC)이고 매뉴얼 수행주체인 내부조직은 지원반(SUPPORTING_DEP), 국립의료원(NATIONAL_MEDICAL) 등으로 소방방재청으로부터 지진 메시지를 받고 국가안전보장회로 보고를 수행함을 나타내고 있다.

○ 액티비티 챠트(Activity-Chart)



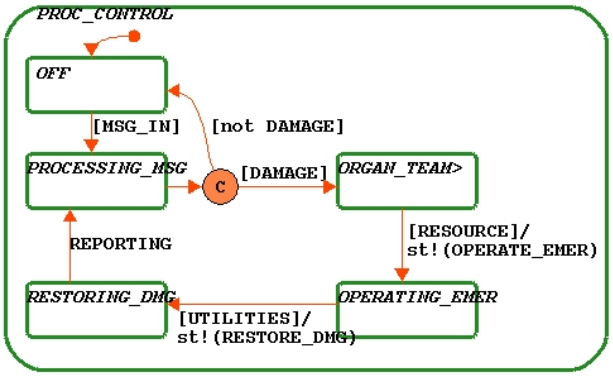
(그림 2) 조치목록 액티비티 챠트

(그림-2)는 <표 2>의 조치목록을 액티비티 챠트로 나타낸 것으로 위기상황 접수 단계(RECOG_ EARTHQUAKE)에서는 소방방재청(NEMA)과 기상청(KMA)의 메시지를 입력받아 대응조직을 구성하는 지시를 내리고 대응조직을 구성하는 액티비티(ORGANIZE_TEAM)에서는 적십자에 혈액을 요청(HELP_BLOOD)하며 대응조직(TEAM)을 긴급대응조치 액티비티로 보내는 것을 알 수 있다. 4개의 액티비티 내에는 각각의 하부 액티비티를 가지고 있어 예를 들어 대응조직을 구성하는 액티비티(ORGANIZE_TEAM)에는 <표 2>의 현장응급 의료반 지원준비 및 출동, 응급의료기관 진료준비 등의 하부 액티비티가 포함되어 있다.

<표-2> 지진발생시 조치목록 (긴급 의료지원)

조치 사항	액티비티	하부 조치사항
위기상황 접수/보고	-RECOG_ EARTHQUAKE	○ 지진발생 정보의 접수/전파 ○ 피해상황 접수 및 전파
대응조직 구성·운영	- ORGANIZE_TEAM	○ 현장응급의료반 지원준비 및 출동 ○ 응급의료기관 진료준비
긴급대응 조치	- OPERATE_EMER	○ 대응조직의 구성·운영 ○ 응급의료 활동 실시 ○ 처리상황 보고 및 전파
복구활동	- RESTORE_DMG	○ 부상자 진료, 회복상태 확인 ○ 의료지원 및 전염병 예방 ○ 간병 봉사자 활동 실태 확인

○ 상태 챠트(State-Chart)



(그림 3) 세부 조치내용 상태 챠트

(그림-2)의 각각의 액티비티는 (그림-3)의 상태 챠트를 통해서 통제되어 활성화 및 비활성화 되는데 예를 들어 메시지를 처리하는 상태(PROCESSING_MSG)는 지진상황 파악 단계(RECOG_EARTHQUAKE)를 통제한다. 또한 하부 액티비티를 가지고 있는 상위 액티비티는 하부 액티비티를 통제하기 위한 상태챠트를 각각 가지고 있다.

4. 위기대응 실무매뉴얼 검증 및 개선

4.1 모델체킹을 통한 검증 및 개선

위기대응 매뉴얼 조치절차의 결정에 있어 모호성 여부의 검증과 작성목표 달성여부에 대해서는 모델체킹을 이용한다. Statemate 모델체커는 Non-Determinsm, Drive to State (해당되는 State에 도달할 수 있는지를 검증), Drive to Property(사용자가 정의한 속성을 만족하는지를 검증) 외 여러 가지를 검증할 수 있지만 위에서 언급한 속성검증은 3가지 방법을 사용한다. 우선 사용자 판단에 모호함을 줄 수 있는 절차에 대해서는 'Non-Determinism 검사'를 이용해서 사용자가 두 가지 이상으로 판단할 수 있는 부분이 있는지를 검증한다. 위에서 다루었던 예제를 검증한 결과 Non-Determinism이 두 곳에서 검출되었는데 한 가지 예는 팀이 출동을 위한 장비 또는 혈액이 없는 경우 롤백을 위한 트리거가 제시되지 않은 경우였다.

매뉴얼 작성목표의 달성여부에 대한 검증은 'Drive to State' 방법(Liveness 검증)을 이용하며 도달해야 될 상태만을 지정해 주면 모델체커가 자동적으로 검증을 수행한다. 본 논문에서는 '피해지역에서 응급치료를 수행하는 상태에 도달 가능한지'와 '보고를 수행하는 상태'에 도달 가능한지를 검증하였으며 결과는 전이를 위한 트리거가 모두 충족한 경우에는 도달 할 수 있음이 검증되었다. 'Drive to Property'를 통해서는 사용자가 검증하고자 하는 속성을 직접 기술해서 검증할 수 있다. 예를 들어 '대응팀이 혈액이 없다 하더라도 현장에서 응급치료 활동은 수행 할 수 있다'의 경우 Temporal Logic으로 작성해서 검증할 수 있다.

4.2 시뮬레이션을 통한 검증 및 개선

대응 매뉴얼 조치내용의 적절성과 추가적으로 발생가능한 상황을 찾는 것은 도구에서 지원하는 시뮬레이션을 이용한다. 시뮬레이션은 액티비티 챠트를 기준으로 상태챠트와 연동되어 수행되며 하부 액티비티 챠트도 활성화되어 시뮬레이션이 진행된다. 스텝별로 진행시키면서 개발자와 도메인 사용자는 시각적인 추적을 통해 조치내용의 적절성을 판단하며, 명세에 포함되지 않았지만 추가적으로 발생 가능한 트리거를 고려하고 이로 인한 분기를 찾는데 유용하게 활용될 수 있다. 예를 들어 국립의료원은 응급의료기관에 재난상황을 전파하는 책임이 있지만 국립의료원이 지진 발생 등으로 통신을 수행할 수 없는 경우 대책이 없음을 고려할 수 있었다.

5. 결론 및 향후 과제

위기대응 매뉴얼은 특성상 의도된 상황에 적용 가능하며 신뢰할 수 있게 작동할 수 있다는 것이 보장되어야 한다. 따라서 위기대응 매뉴얼의 검증은 필수적이며 이를 위해 본 논문에서는 정형기법 도구를 활용한 명세 및 검증을 수행하고 검증결과를 토대로 위기대응 매뉴얼의 신뢰성을 개선하는 방안을 제시하였다. 위기대응 매뉴얼의 목록은 Statemate의 명세언어(3가지 챠트)로 각각 대응되어 묘사가 용이함을 알 수 있었다. 또한, 모델체커를 통해서 조치결정에 있어 모호성(Non-Determinism)과 작성목표 달성여부(Liveness) 검증을 수행했으며, 시뮬레이션을 통해서는 제한적이지만 추가적으로 발생가능한 이벤트에 대한 분기를 찾는데 유용함을 알 수 있었다. 하지만 Statemate 도구를 이용한 위기대응 실무매뉴얼의 검증에도 한계는 있어서 시간소비를 고려한 속성 검증은 제한적이며 (예를 들어 '지진이 발생 후 4시간 내에는 현장에 출동하고 8시간 이내에는 조치보고가 이루어져야 한다'), 조치절차 자체의 적절성에 대한 자동화된 검증도 한계가 있다. 따라서 향후에는 시간의 고려가 가능한 정형도구를 이용해 검증속성을 확장하면 매뉴얼을 더욱 보완할 수 있으리라 판단된다.

참고문헌

[1] Charles Perrow, "Normal Accidents : living with high-risk technologies", Princeton Univ., 1984.

[2] Edmund M. Clarke and Jeannette M. Wing, "Formal Methods: State of the Art and Future Directions", ACM Computing Surveys, 1996.

[3] David Harel and M. Politi, "Modeling Reactive Systemswith Statecharts", McGraw-Hill, 1998.

[4] A. Lamsweerde, "Formal Specification: a Roadmap", In The Future of Software Engineering, ACM Press, 2000.

[5] 정금택, 이진호, 서석, 최진영, "정형기법을 적용한 위기대응 실무매뉴얼 명세 및 검증", 한국정보과학회 학술발표논문집 제37권 제1호, pp. 116~119, 2010.