정형기법을 적용한 위기대응 실무매뉴얼 명세 및 검증

정금택○ 이진호 서석 최진영
고려대학교 컴퓨터학과
{jkt76○, jhlee, choi}@formal.korea.ac.kr, s_suh@korea.ac.kr

Specification and Verification of Crisis Response Manual using Formal Methods

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

요 약

안보, 재난, 국가핵심기반 분야에 위기발생시 즉각적인 조치를 위한 '위기대응 실무매뉴얼'이 정부기관별로 작성되어 있지만 조치사항에 대한 정량적 검증이 부족하다. 오류가 내포된 조치절차는 피해를 확대 시킬 수 있으므로 위기대응절차에 대한 검증이 요구되며 이를 위해 본 논문에서는 Statemate의 구조적, 기능적, 행위적 관점의 언어를 활용해서 정형기법(formal methods)을 수행함으로써 위기 대응 실무매뉴얼의 모델링 방법을 제안하고 매뉴얼에 기술되어 있는 조치절차의 검증결과를 제시하였다

1. 서 론

2010. 1월 남미에 위치한 작은 나라 아이티는 7.0 강진에 20만명 이상이 사망하고, 2008. 5월에는 중국 쓰촨성 대지진으로 약 8만여명 이상이 사망하는 일이 발생했다. 이를 계기로 국내에서도 소방방재청 주관으로 지진 시뮬레이션을 수행한 결과 서울 인근에서 규모 6.3의 지진이 일어날 경우 사상자는 2만3천여명이 발생할 것이라고 예측되었다[1]. 지진의 경우 발생 빈도는 낮지만 발생할 경우 피해가 커질 수 있어 국가 차원에서 지진발생에 대응하기 위한 절차를 사전에 수립해 놓고 있다. 이렇듯 발생시 큰 피해가 예상되는 안보, 재난, 국가핵심기반 등의 분야에 대해 정부 각 부처가 즉각적으로 수행해야할 행동절차와 조치사항을 구체적으로 규정한 '위기대응 실무매뉴얼'이(총 272개) 2005. 11월 완성되어 정부 각 기관에서 활용되고 있다.

위기대응 매뉴얼은 평소에 경험하기 힘들고 긴박한 사항에 대한 절차인 점을 감안하면 조치내용 확인에 장시간이 소요되거나, 조치내용이 부적절한 경우, 실무자가 임의로 판단할 수 있는 모호한 조치들이 내포된 경우에 피해규모는 기하급수적으로 커질 가능성이 있다. 따라서 대응절차에 대한 검증은 반드시 요구되지만 현재 수립된 위기대응 매뉴얼에 대한 검증사례, 검증방안 등과 관련된 내용은 발견되지 않아 본 논문에서는 정형기법을 활용해서 위기대응 절차를 명세하고 검증하고자 한다. 이에 대한 검증사례로 본 논문에서는 "지진발생시 응급의료활동"을 대상으로 STATEMATE 명세언어를 활용하였다

2. 관련 연구

2.1 정형기법

정형기법은 소프트웨어 시스템의 명세, 디자인, 검증을 위해 수학적 모델을 사용하는 기술 및 도구들의 집합으로 정형명세(formal specification)와 정형검증(formal verification)이 있다. 정형명세는 정형논리 또는 수리에서 사용되는 기호 등을 이용하여 요구사항을 기술하는 것이며, 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 직관적인 언어로써 Reactive 시스템 명세에 적합하며, 각 관점별로 Activity-Chart, State-Chart, Module-Chart로 나눌 수 있다[3]. Activity-Chart는 기능의 입·출력을 명세하며, 각 Activity는 입·출력이 발생하는 이벤트, 조건 및 그 행위를 명세하는 State-Chart를 통해 통제받게 된다. Module-Chart는 구조적 관점에서 시스템을 명세함으로써 시스템의 물리적 구성을 제시해 준다. 각 챠트는 독립적으로 사용도 가능하지만 Module>Activity>State 챠트간의 계층구조(hierarchy)를 가진 명세도 가능하다. 명세에 대한 검증은 시뮬레이션과 모델체킹을 통해 수행될 수 있는데 본 논문에서는 대응절차의 검증을 위해 시뮬레이션과 모델체킹을 모두 사용하였다.

2.3. 위기대응 실무매뉴얼

정부기관 대부분이 운용하는 위기대응 실무매뉴얼은 발생가능한 위기 예상 시나리오에 대한 조치사항을 작성한 것으로 구성은 위기대응 목표, 대응체계도(부서별 임무), 조치사항, 조치 세부내용으로 되어 있어 Statemate의 구조적, 기능적, 행위적 관점의 챠트에 각각 대응할 수 있어 Statemate로 명세가 용이하다

3. '위기대응 실무매뉴얼' 명세

3.1 대 상

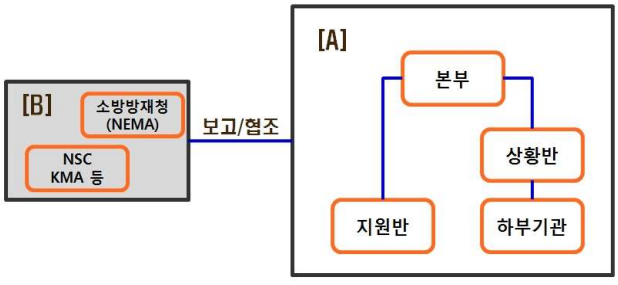
272개 분야 중 지진에 대해 의료지원을 담당하는 기관의 대응매뉴얼로 한정하였으며 해당기관에서 작성한 조치내용을 기준으로 명세하였다. 조치내용을 간략히 요약하면 다음과 같다.

> 지진발생 및 피해상황이 소방방재청으로 부터 접수되면 해당 기관은 관련 하부기관에 전파하고 대응반(국립의료원, 응급의료기관 등)을 준비시킨다. 또한 필요한 자원(혈액, 장비 등)을 지원해주고 응급의료 활동을 수행하며 피해상황 및 부상자들의 회복상태를 확인해서 NSC, 재난안전대책본부 등 주요기관에 보고를 수행한다

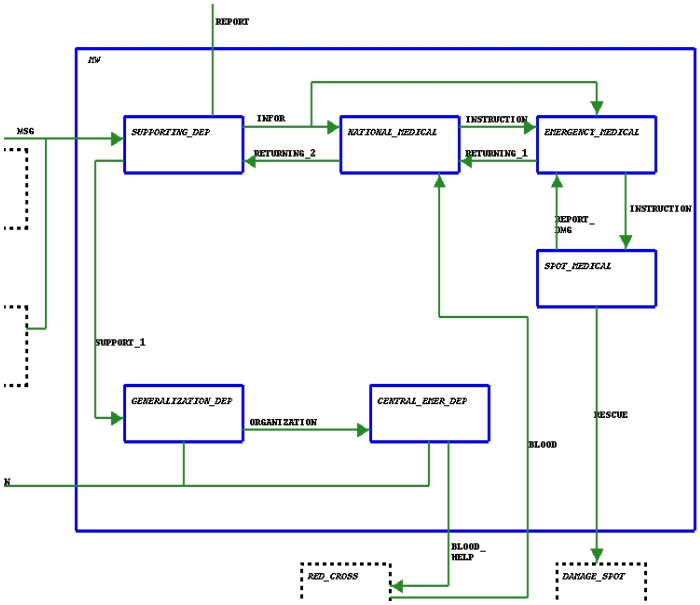
3.2 관점별 명세

◦물리적 구성

매뉴얼의 대응체계도를 살펴보면 (그림-1)과 같이 내부조직인 [A]와 보고 및 협조 관계에 있는 외부기관[B]로 나뉘어 있는데 모델링은 [A]인 내부기관에 대해서만 수행하고 외부기관인 [B]는 환경으로 설정해서 주고받는 정보를 정한다. 이러한 과정을 통해 (그림-2)와 같은 Module-Chart를 명세할 수 있으며, 이 챠트를 통해 사용자는 기관간의 주고받는 정보를 파악할 수 있다.



(그림-1) 위기대응 실무매뉴얼 대응 체계도



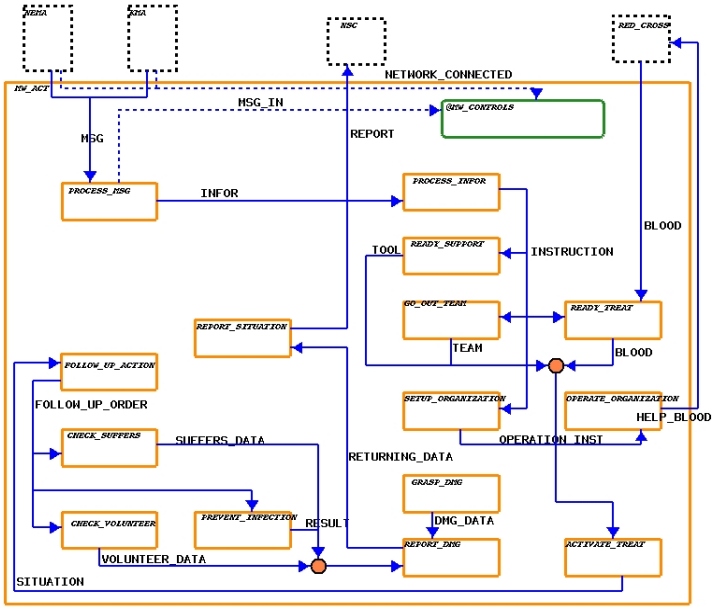
(그림-2) Module-Chart

◦시스템 수행기능 명세

대응 매뉴얼은 사건 발생시 조치사항을 기술한 것으로 대응매뉴얼에 명세된 조치목록과 그에 대응하는 Activity를 만들어서 [표-1]과 같이 작성한다. 여기에 각 Activity간의 관계 및 진행순서와 입·출력되는 정보를 정한다. 여기에 Module-Chart에서 정해진 내부와 외부기관간의 전달되는 정보를 반영하면 (그림-3)과 같은 Activity-Chart를 명세할 수 있다. 예를 들면 "피해상황 접수 및 전파"에 해당되는 액티비티(PROCESS_INFOR)는 피해정보(INFOR)를 입력받아 초동조치를 수행하는 지시(INSTRUCTION)를 출력함을 알 수 있다. 또한 소방방재청(NEMA)과 기상청(KMA)에서는 메시지(MSG)를 받고 NSC 등에 보고를 수행함을 알 수 있다.

[표-1] 지진발생시 의료지원 조치목록

조치 사항	세부 내용	액티비티
위기상황 접수/보고	◦지진발생 정보의 접수/전파	-PROCESS_MSG
초동조치	◦피해상황 접수 및 전파 ◦현장응급의료반 지원준비 및 출동 ◦응급의료기관 진료준비	- PROCESS_INFOR - READY_SUPPORT GO_OUT_TEAM - READY_TREAT
긴급대응 조치	◦인명피해 상황파악 및 보고 ◦대응조직의 구성·운영 ◦응급의료 활동 실시 ◦처리상황 보고 및 전파	- GRASP_DMG - SETUP_ORGA' OPERATE_ORGA' - ACTIVATE_TR' - REPORT_DMG
후속조치	◦부상자 진료 및 회복상태 확인 ◦의료지원 및 전염병 등 예방강화 ◦간병 봉사자 활동 실태 확인	- CHECK_SUF' - PREVENT_INF' - CHECK_VOLUN'



(그림-3) 조치목록 Activity Chart

◦시스템 행위(Behavior) 명세

(그림-3)의 각 Activity는 "@MW-CONTROL"이라는 Control-Activity에 의해서 통제되어 활성화 되거나 비활성화 되는데 이 Control Activity는 State-Chart를 통해서 명세된다. State-Chart는 상태(State)와 전이(Transition)로 구분되는데, 이때 전이를 일으키는 것은 전이에 붙은 레이블(이벤트[조건]/액션)이 된다[4,5].

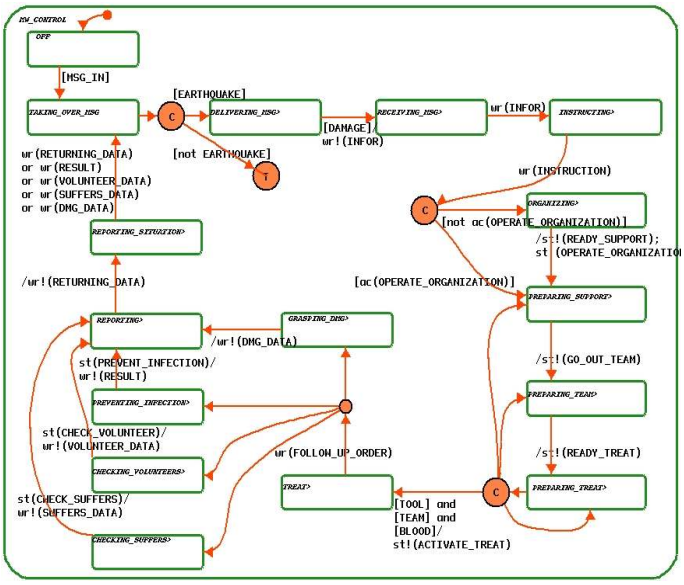
'@MW-CONTROL'을 내부를 명세한 State-Chart (그림-4)를 대략적으로 살펴보면 다음과 같다.

- (그림-4)에서 메시지에 피해내용([DAMAGE])이 있으면 메시지를 수령하는 상태(RECEIVE_MSG)로 전이되고 "PROCESS_INFOR"(그림-3)는 활성화된다.
- (그림-3)의 "READY_SUPPORT", "GO_OUT_TEAM", "READY_TREAT", "READY_ORGANIZATION"은 (그림-4)의 지시(INSTRUCTION)가 트리거 되면 활성화되고 구조팀, 구조도구, 혈액이 모두 준비되면 치료상태 (TREAT)로 전이된다.

4. '위기대응 실무매뉴얼' 검증

4.1 검증속성

검증속성은 대응매뉴얼의 대응목표에 해당되는 내용으로 '지진으로 인한 피해발생시 사태수습을 위해 응급치료를 수행하는 상태에 도달할 수 있는가'와 '피해상황에 대한 보고를 수행하는 상태에 도달할 수 있는지'를 알아보는 생존성(Liveness) 속성에 대해 검증하고, 사용자에게 부적절한 결정을 야기시킬 수 있는 Non-Determinism의 두 가지에 대해서 검증하기로 한다. 이를 위해 본 논문에서는 시뮬레이션과 모델체킹 두 가지 검증방안에 대해 모두 수행하였다.



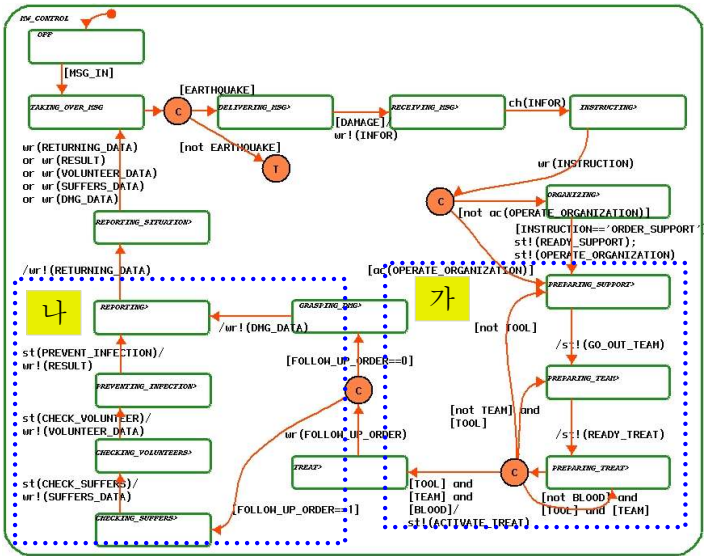
(그림-4) 조치목록 State-Chart

4.2 시뮬레이션

시뮬레이션은 Activity_Chart와 State_Chart에 대해 병렬로 진행할 수 있으며 두 챠트간의 상관관계를 스텝별로 진행하면서 경과 상황을 관찰할 수 있다. 또한 시뮬레이션을 수행하면 시각적인 추적이 가능하고 스텝별로 이벤트와 조건을 변경시켜서 그 변화를 관찰할 수 있으며, Non-determinism이 발생되는 경로에서는 사용자가 이를 인지하고 경로를 선택해서 진행 할 수 있는 장점이 있다. 현재의 대응매뉴얼대로 명세 후 시뮬레이션을 수행한 결과 도구(TOOL), 혈액(BLOOD), 구조인력(TEAM) 중의 한 가지라도 없는 경우 이에 대해서 전이되는 State가 결정되지 않음을 알 수 있었으며, 부상자 진료 및 회복상태 확인(CHECKING_SUFFERS), 봉사자 실태 확인(CHECKING_VOLUNTEERS) 등을 수행하기 위한 트리거가 제시되지 않음을 발견할 수 있었다. 따라서 시뮬레이션을 통해 발견된 Non-Determinism에 대해 (그림-5)의 <가>와 같이 도구, 혈액, 구조인력 중의 하나라도 충족되지 않으면 롤백이 이루어지는 상태를 조건별로 지정하고, <나>에서 보는것과 같이 후속조치 명령(FOLLOW_UP_ODDER) 이후에 트리거를 제시해 주고 상태 간에 순서를 정함으로써 이 문제를 해결하였다.

상태간의 전이에 있어 모든 조건을 참으로 전제하고 모델의 생존성(Liveness) 속성을 검증한 '지진으로 인한 피해발생시 응급치료를 수행하는가'와 '피

해상황 및 진행현황에 대한 보고를 수행하는지'의 속성은 만족하였음을 알 수 있었다.



(그림-5) 조치목록에 대한 수정된 State-Chart

4.3 모델체킹

모델체킹은 유한상태 병렬 시스템을 검증하기 위한 기술로 자동화된 검증방법이다[6]. Statemate 모델체커는 설계상에서 속성에 대한 동적행위를 체크하는 기술로 모델체커에서 제공하는 검증속성에는 Range Violation, Non-Determinism, Race Condition, Drive to State(해당되는 State에 도달할 수 있는지를 검증), Drive to Property(사용자가 정의한 속성을 만족하는지를 검증)가 있다. 사용자의 모호한 판단 배제와 조치매뉴얼의 수립 목적인 치료 및 보고수행 여부 검증을 위해서 'Non-Determinism'과 'Drive to State' 검증 모드를 이용했으며, 수정된 State-Chart(그림-5)를 대상으로 검증한 결과는 [표-2]와 같다.

[표-2] Statemate 모델체커 검증결과

	Name	Type	Scope	Result
1	AFTER_Non_Det	Non-Determinism	All	No Non-Determinism
2	After_Reach_Report	Drive to State	User Defined	0 of 2 States reached

보는바와 같이 Non-Determinism은 발견되지 않았지만 Drive to State는 치료와 보고의 2개의 State모두에 진입하지 않을 수 있음을 보여주고 있다. 이는 어떠한 경우에 있어서는 '치료상태와 보고상태'로 진입되지 않을 수 있음을 의미한다. 시뮬레이션과 다른 결과를 보여주는 것은 시뮬레이션 때에는 이벤트와 조건이 참이 되는 경우를 사용자가 직접 입력했지만 모델체킹시에는 거짓인 조건을 포함한 모든 경우를 모델체커가 자동적으로 고려하므로 이러한 결과가 도출되었다. 한 가지 예로 (그림-5)의 <가> 영역에서 도구, 팀, 혈액 중의 한 가지라도 없는 경우 조건이 만족될 때까지 계속적으로 루프(Loop)가 발생되어 "치료(TREAT) 및 보고(REPORTING)"상태에 진입할 수 없는 경우가 있으므로 모델체킹 결과가 도달할 수 없는 경우도 있는 것으로 판명되었다

5. 결론 및 향후 과제

안보, 재난, 국가핵심기반 등의 분야에 대해 정부 각 부처 기관이 즉각적으로 수행해야할 행동절차와 조치사항을 구체적으로 규정한 '위기대응 실무매뉴얼'은 특성상 반드시 검증이 이루어져야 한다. 이를 위해 실제 환경을 만들어 연습을 수행하는 방법도 있지만 모델링을 통해 시뮬레이션을 수행해보고 검증을 수행하는 것도 하나의 방법이다. 따라서 본 논문에서는 위기대응 매뉴얼의 체계도, 조치사항, 세부 조치내용을 Statemate의 Module, Activity, State의 3가지 챠트로 대응시켜 명세하였으며, 시뮬레이션 및 모델체킹을 통해 매뉴얼에 대한 검증을 수행함으로써 조치절차에서 보완이 요구되는 부분을 도출하였다.

정형기법을 통한 위기대응 실무매뉴얼 검증은 매뉴얼에 대한 검증을 정성적 판단이 아닌 정량적으로 수행할 수 있는 장점이 있으므로 향후에는 특정 기관으로 한정된 조치절차의 검증에서 기관별 상호관계를 고려한 검증을 통해 보완사항을 도출하는 것도 의미있는 연구가 될 것이다.

6. 참고문헌

[1] http://news.kukinews.com/article/view.asp?page=1&gCode=kmi&arcid=0003374507&cp=nv
[2] Edmund M. Clarke and Jeannette M. Wing, "Formal Methods: State of the Art and Future Directions", ACM Computing Surveys, 1996
[3] http://www.ilogix.com
[4] David Harel, "Statecharts a visual formalism for complex systems, Science of Computer Programming 8, 1987
[5] David Harel and Amnon Naamad, "The STATEMATE semantics of statecharts", ACM Transactions on Software Engineering and Methodology(TOSEM), volume 5, issue 4,1996
[6] E. M. Clarke,O Grumberg, D. A. Pelad, Model Checking, MIT Press, 1999