상태차트를 이용한 철도제어시스템 요구사항 명세

이혁 O* 황대연* 윤용기** 황종규** 조현정** 최진영*

*고려대학교

{hlee O, dyhwang , choi}@formal.korea.ac.kr

**한국철도기술연구원

{ykyoon , jghwang , hjjo}@krri.re.kr

Specification of Requirements of Railroad Control System using Statechart

Hyuk Lee O*, Dae-Yon Hwang*, Jin-Young Choi*

*Korea University

Yong-Ki Yoon** , Jong-Gyu Hwang** , Hyun-Jeong Jo**

**Korea Railroad Research Institute (KRRI)

요 약

시스템 운영 중에 오류가 발생하면 치명적인 인적, 물적 피해를 초래하는 안전필수 시스템은 안전성과 신뢰성을 확보하기 위한 요구명세의 정형적인 명세와 검증이 요구된다. 철도 차량의 진로와 속도를 제어하는 철도제어 시스템은 안전필수 시스템임에도 불구하고 요구사항이 자연어로 표현되어 있다. 자연어로 명세 된 요구사항은 자연어의 모호한 특성으로 인하여 오류의 위험으로부터 안전하지 못하다. 본 논문에서는 자연어로 명세 되어있는 철도제어 시스템의 요구사항을 도식적인 설계언어인 상태차트(Statechart)를 이용하여 정형적으로 명세함으로써 철도제어 시스템의 안전성과 신뢰성을 향상하고자 한다.

1. 서 론

안전필수 시스템인 철도제어 시스템은 안전성 및 신뢰성 향상을 위해 요구사항과 설계에 대한 정형적인 명세가 요구된다. 또한 무모호성, 간결성, 일관성, 완전성, 검증 가능성 등과 같이 안전한 시스템이 갖추어야 할 요소들은 정형적으로 검증되어야 한다. 자연어로 명세 된 요구사항은 자연어의 모호성으로 인하여 안전한 시스템이 갖추어야 할 요소들을 보장하기 힘들다. 전세계적으로 높은 안전 등급의 시스템을 명세할 때는 수학이나 논리에 기반한 정형명세 언어를 사용하여 명확하게 명세 하고 필요한 속성들을 검증하는 것을 요구하는 추세이다[1]. 하지만 우리나라는 권고만을 하고 있고 철도제어 시스템의 요구사항 또한 자연어로만 명세 되어 있다[2].

본 논문에서는 자연어로 기술된 철도제어시스템의 간격제어모듈 요구 명세를 상태차트[3]라는 정형적 언어로 기술하여 자연어 명세가 가지는 모호한 점을 없애고자 한다. 또한 이러한 정형적 명세를 통해 자연어 명세에서는 찾기 힘든 명세의 완전성과 일관성을 찾아서 자연어 요구 명세에서 기술하지 않은 요소들이 무엇인지 파악하여 보충할 수 있도록 하며, 명세 상에서의 모순이 없도록 하고자 한다.

본 논문은 정형 명세언어인 상태차트에 대해 설명하고, 자연어로 된 철도제어 시스템의 요구사항을 상태차트를 이용하여 정형적으로 명세한다. 그리고 정형적으로 기술한 상태차트 명세의 완전성과 일관성을 검사하여 요구 명세 정확히 기술되었음을 보인다. 마지막으로 결론과 향후 연구로 마무리 한다.

2. 연구배경

Harel에 의해 처음 제안되었던 상태차트는 뛰어난

본 연구는 한국철도기술연구원의 지원을 받아 수행 되었음

가독성을 특징으로 하며 복잡한 반응형 시스템의 행위적인 부분을 효과적으로 명세할 수 있는 도식적 정형명세 언어로 직관적인 이해가 매우 편한 동시에 동시성 및 계층성을 표현하기에 용이한 장점을 갖는다[4]. 상태차트는 현재 UML에 포함되어 매우 널리 쓰이고 있다. 상태차트는 시스템의 요구와 설계사항을 상태들과 전이들로 표현하며, 상태들에는 더 이상 내부에 하위 상태를 가지지 않는 상태와 내부에 하위 상태를 가지는 상태들이 있다.

상태간의 전이는 E[C]/A 형태로 표기된다. E는 전이를 유발시키는 이벤트이다. 이벤트들은 Broadcast 되는 특성으로 특정 전이를 대상으로 발생하지 않고, E의 범위 내에 있는 모든 전이가 동시에 발생된 이벤트를 감지한다. C는 Condition의 약자로 상태 변화의 조건이 된다. 즉, C에 제시된 상태들이 만족되고 E에 해당되는 이벤트들이 발생하게 되면 전이가 이루어지게 된다. A는 Action으로 해당 전이가 일어나면 데이터 값이나 Condition 값의 변화를 발생시키거나 이벤트들을 발생시킨다. E, C, A 모두 필수가 아닌 선택적이며 E와 C가 모두 없으면 무조건 다음 시간 단위에 전이를 하게 된다.

상태차트의 특징은 다음과 같이 표현할 수 있다.
Statechart = State-diagrams + Depth + Orthogonality + Broadcast-communication

3. 철도 제어시스템의 자연어 요구사항

철도제어 시스템은 필수기능과 비(非)필수기능으로 나뉘어 진다. 여기서 필수기능은 안전과 직결되는 부분으로 열차의 진로제어와 이동권한 설정 및 방호 기능 등을 포함한다.

다음은 열차제어시스템의 필수기능을 담당하는 간격제어 모듈의 요구 명세 요약이다.

철도제어시스템의 간격제어 모듈(DCM, Distance Control Module)은 이동권한 설정 기능과 궤도의 개방 및 폐쇄 기능, 임시속도 제한 기능을 담당한다.

열차의 이동권한 설정이란, 열차가 이동할 궤도에 대해 권한을 설정하고 열차에게 전송하여 설정된 권한에 따라 열차의 속도를 제어하는 것이다. 권한의 종류는 적색, 황색, 녹색의 세가지 경우가 존재한다.

각 색상의 권한은 다음과 같이 설정되어 있다.

녹색: 최대 목표속도로 진행
황색: 궤도 내에서 반드시 정지
적색: 궤도 내로 진입 금지

권한의 설정 기준은 다음과 같다.

간격제어 모듈은 각 열차 사이 및 다음과 같은 장애물 사이에 허용이동권한이 적색으로 설정된 궤도와 황색으로 설정된 궤도를 최소한 각 한 개씩 설정함으로써 안전한 열차 분리가 이루어질 수 있도록 한다.

1. 다른 열차가 점유하고 있는 궤도
2. 특정 이유로 열차 운행이 차단된 궤도
3. 선로전환기 설정이 열차의 운행과 맞지 않는 궤도

궤도의 개방 및 폐쇄 기능은 보수 작업이나 비상시에 열차보호를 위해 특정 궤도 혹은 전체 궤도를 개방하거나 폐쇄하는 기능이다. 궤도의 개방 및 폐쇄 명령은 자동열차감시장치 (ATS, Automatic Train Supervision)로부터 온다. 궤도폐쇄 명령이 간격제어 모듈로 전달되면, 간격제어 모듈은 해당궤도에 무조건적인 적색 허용이동권한을 설정하여 해당궤도를 폐쇄하고 인접한 궤도도 이에 준하여 허용이동권한을 설정한다

임시속도제한 기능은 특정구간에 속도제한을 설정하는 것으로서, 임시속도제한은 특정블록 또는 모든 블록에 적용될 수도 있다. 임시속도제한이 지정된 블록을 통과하는 열차는 지정한 속도를 초과할 수 없게 된다.

4. 철도 제어시스템의 요구사항에 대한 정형적 명세

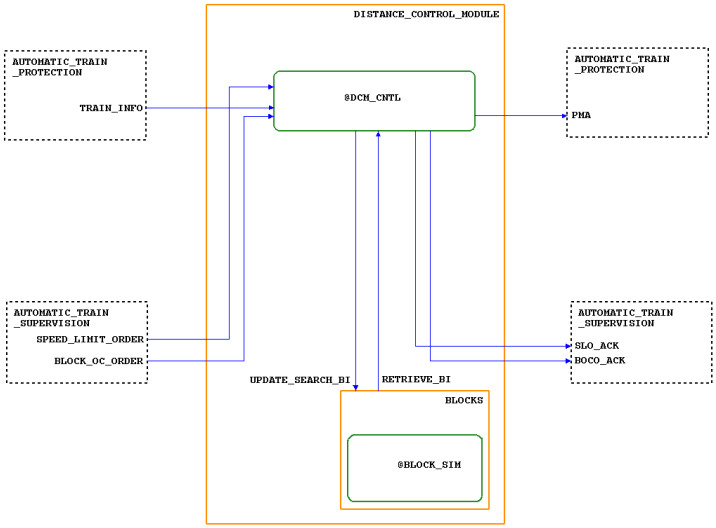
본 논문에서 명세 시 사용되는 정형적 명세언어로는 STATEMATE의 상태차트를 사용하였다. STATEMATE는 상태차트 도구 중 현재 가장 널리 알려진 상용화 도구이다.

명세의 대상은 철도제어시스템의 필수기능에서 가장 중요한 간격제어 모듈에서 이동권한 설정과 궤도의 개방 및 폐쇄와 임시속도제한 명령 처리 기능을 명세하였다.

4.1 엑티비티차트 (Activity Chart)를 이용한 명세

엑티비티차트는 명세 대상의 기능적인 측면을 보여주는 상위 단계의 차트이다. 여기서는 간격제어 모듈을 엑티비티차트를 사용하여 다음과 같이 나타내었다.

DISTANCE_CONTROL_MODULE 엑티비티는 간격제어 기능을 나타내고, 좌우로 있는 점선의 엑티비티들은 외부 엑티비티들을 나타낸다. 여기서 명세범위를 간격제어 모듈로 한정했기 때문에 외부 엑티비티들의 행위들은 명세에서 제외되었다. 열차를 나타내는 열차자동 보호장치(ATP, Automatic Train Protection)와 자동열차감시장치 (ATS, Automatic Train Supervision)가 외부 엑티비티로 명세되었다.



[그림 1] 간격제어 모듈의 엑티비티차트

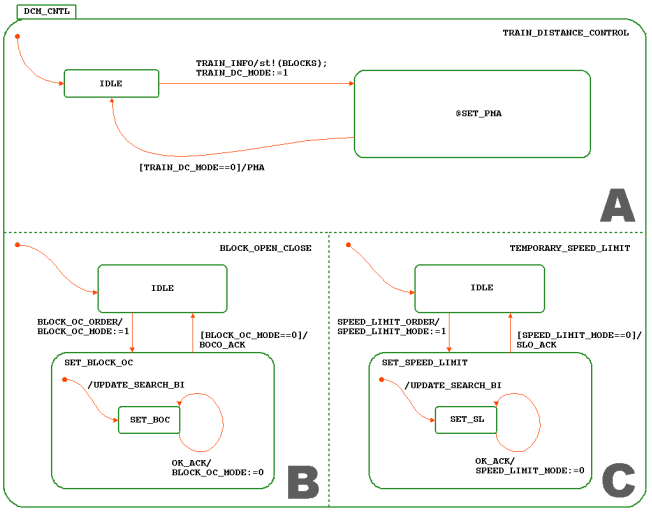
[그림 1]의 엑티비티차트에서 열차는 간격제어 모듈에서 열차정보와 이동권한 요청을 하고 이에 대해 간격제어 모듈은 허용이동권한을 생성하여 보내준다. 자동열차감시장치는 궤도의 개방 및 폐쇄 명령과 임시속도제한 명령을 간격제어 모듈로 보내고, 이에 대해 간격제어 모듈은 명령이 처리되었음을 알리는 응답을 한다.

4.2 상태차트를 이용한 요구사항 명세

상태차트는 엑티비티차트로 표현된 기능에 대한 행위를 보여준다. 상태차트 중에는 엑티비티차트와 동일한 수준에서 전체 엑티비티의 행위를 나타내는 컨트롤 차트가 있다. [그림 2]는 간격제어 모듈의 컨트롤 차트이며 점선으로 나뉘어진 세 부분은 각각 이동권한 설정([그림 2]의 A: TRAIN_DISTANCE_CONTROL), 궤도 개방 및 폐쇄([그림 2]의 B: BLOCK_OPEN_CLOSE), 임시속도제한(([그림 2]의 C: TEMPORARY_SPEED_LIMIT)을 나타내고 있다. 이동권한 설정 상태는 열차로부터 열차정보/이동권한요청이 들어오면 유휴(IDLE)상태에서 SET_PMA 상태로 전이하게 되고 열차에게 보내줄 허용이동권한을 생성하여 열차에게 보내준 뒤에 유휴상태로 돌아가는 것을 보여준다.

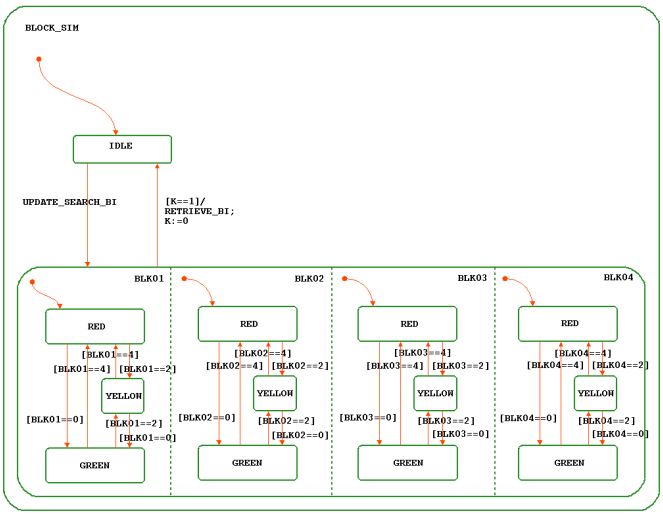
궤도 개방 및 폐쇄 상태는 유휴상태에서 자동열차감시장치로부터 궤도 개방 및 폐쇄 명령이 들어오면 SET_BLOCK_OC 상태로 전이하게 되고 명령을 처리한 후에 처리 결과를 보낸 뒤에 유휴상태로 돌아가는 것을 보여준다.

임시 속도 제한 상태는 자동열차감시장치로부터 임시속도제한 명령이 들어오면 유휴상태에서 TEMPORARY_SPEED_LIMIT 상태로 전이하게 되고 명령을 처리한 후에 처리 결과를 보낸 뒤에 유휴상태로 돌아가는 것을 보여준다.



[그림 2] 간격제어 모듈의 컨트롤차트

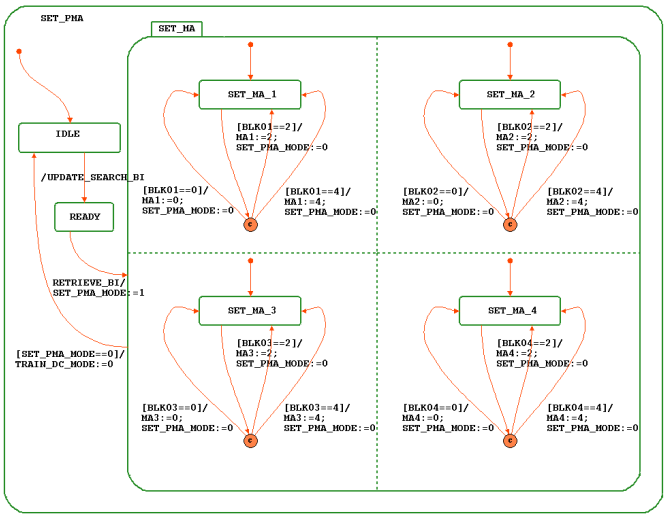
열차의 이동권한 설정, 궤도 개방 및 폐쇄, 임시속도제한은 모두 열차의 이동을 통제하는 것이며, 이것을 위한 궤도의 상태정보는 특정한 저장소에 저장된다. 이 저장소를 엑티비티차트의 BLOCKS 엑티비티로 나타내었다. 궤도 개방 및 폐쇄와 임시속도제한은 단방향 명령으로 간격제어 모듈로 이와 같은 명령이 오면 BLOCKS 엑티비티에 해당 명령의 사항을 갱신하게 된다. 이동권한 설정 명령은 열차로부터 열차정보/이동권한요청이 들어오면 BLOCKS 엑티비티에 열차가 점유하고 있는 궤도의 정보(위치정보)를 갱신하고 요청된 궤도의 상태를 확인하여 허용이동권한을 생성한 뒤에 열차에게 넘겨주게 된다.



[그림 3] SET_PMA의 상태차트

[그림 3]은 SET_PMA 상태의 행위를 보여주는 상태차트이다. 열차로부터 열차정보/이동권한 요청이 들어와서 SET_PMA 상태로 전이됨과 동시에 SET_PMA는 열차 정보와 이동권한 요청정보를 BLOCKS 엑티비티로 보내고 유휴상태로 전이한다.

BLOCKS 엑티비티로부터 이동권한 요청정보에 대한 궤도정보는 받게 되면 SET_PMA는 궤도정보에 따라 허용이동권한을 설정하여 그림 2와 같이 열차에게 보내주게 된다.



[그림 4] BLOCK_SIM의 상태차트

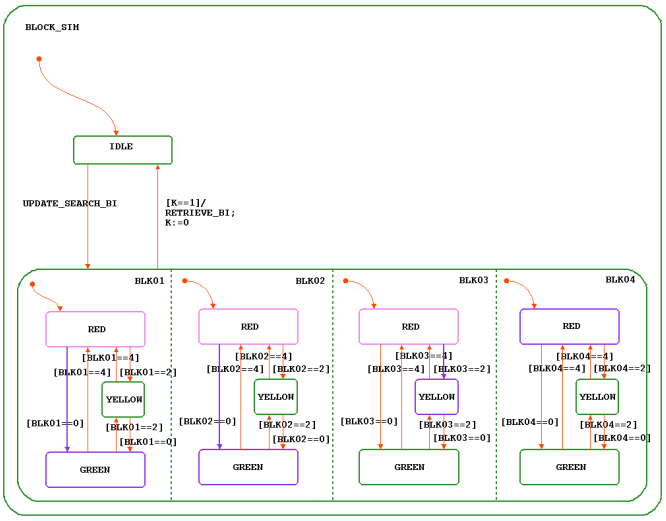
[그림 4]는 BLOCKS 엑티비티의 행위를 나타내는 상태 차트이다. BLOCK_SIM 상태는 초기화 됨과 동시에 유휴상태에 머무르고 있다가 열차 정보와 이동권한 요청정보가 들어오면 궤도 설정 상태로 전이하게 되고 이동권한 요청이 들어온 궤도의 상태정보를 내보낸다.

5. 시뮬레이션을 통한 기능 검사

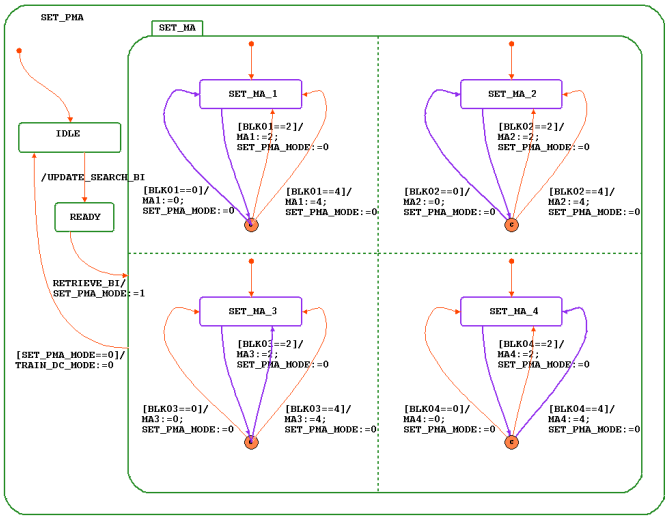
4장의 간격제어 모듈의 명세가 자연어 요구 사항에서 기술된 속성들을 만족시키는지에 대해 시뮬레이션을 통하여 만족여부를 볼 수 있다.

속성 1. 궤도 상태에 따른 허용이동권한의 정확함
속성 2. 임시속도제한이 설정된 궤도에 대한 허용 이동권한의 정확함
속성 3. 폐쇄된 궤도는 적색 상태로 개방 전까지 사용불가 (이동권한 요청, 임시 속도제한 불가)

시뮬레이션을 통하여 간격제어 모듈이 위의 세가지 속성을 만족하는지를 알아낼 수가 있었다.

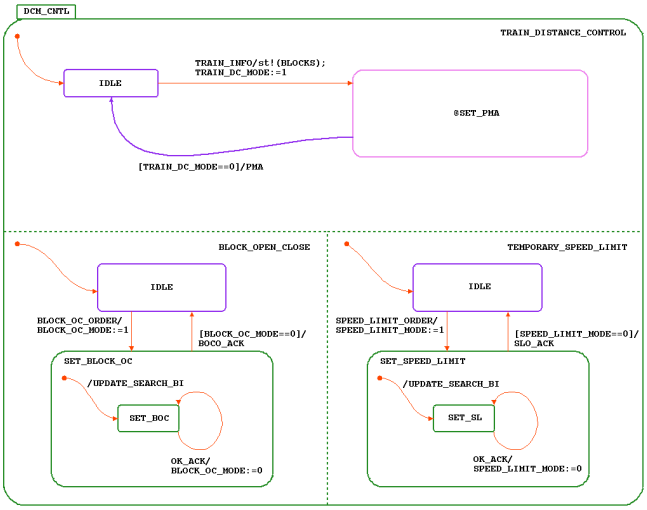


[그림 5] 궤도 정보의 수정



[그림 6]. 허용이동권한의 설정

[그림 5]는 궤도 정보가 초기화되는 전이상태이며 궤도들의 초기 상태는 적색이다. [그림 5]와 같은 궤도 상태에 이동권한 요청을 하였을 때에 궤도 상태가 올바르게 허용이동권한으로 설정이 되는지는 [그림 6]으로 확인할 수가 있었다. 허용이동권한을 설정한 후에 허용이동권한을 열차에게 보내도 유휴상태로 돌아가는 간격제어 모듈을 [그림 7]에서 확인할 수가 있었다.



[그림 7] 허용이동권한 전송 후 유휴 상태로 전이

6. 결론 및 향후 연구

본 논문에서는 자연어로 명세 된 상태차트를 이용하여 철도제어시스템의 간격제어 모듈을 명세하였다. 이와 같이 요구사항을 분석하여 만든 정형적 상태차트 명세를 시뮬레이션 함으로써 요구사항이 명확하게 작성되었는지를 확인할 수가 있었고, 나아가서 자연어 명세에서 기술하지 않았던 사항들을 찾아내어 한층 안전한 요구 명세를 작성할 수 있었다.

참고문헌

[1] Jame F. Peters, Witold Pedrycz, “Software Engineering – An Engineering Approach}, Wiley, 2000

[2] IEC. IEC-61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems. International Electrotechnical Commission, 1999.

[3] David Harel, “Statecharts: A Visual formalism for Complex Systems”, Science of Computer Programming. Vol. 8, issue 3, pp. 231-274, 1987

[4] David Harel and Ammon Naamad, “The STATEMATE Semantics of Statecharts”, ACM Trans. Soft. Eng. Method, Oct. 1996.

[5] Gerald Luttgen and Michael von der Beeck and Rance Cleaveland, “A Compositional Approach to Statecharts semantics”, Report 12, Institute for Computer Applications in Science and Engineering (ICASE 2000)