1999년도 대한전기학회 하계학술대회 논문집 1999 7 19-21

Grafcet을 이용한 연동로직 분석

황 종 규, 이 종 우, 이 재 호, 최 규 형
한국철도기술연구원, 철도신호통신팀

Analysis of Interlocking Functions using Gragcet Language

Jong-Gyu Hwang, Jong-Woo Lee, Jae-Ho Lee, Gyu-Hyung Choi
Korea Railroad Research Institute(KRRI)

Abstract - Recently, the computer based control systems instead of conventional relays circuitry are widely used to industrial applications, and also those technology is available to railway signaling which are safety-critical systems. However, the safety and reliability of software for those systems are harder to demonstrate than in traditional relays circuitry because the faults or errors can not be analyzed and predicted to those systems. So, the safety problems are crucial more and more in computer based control system. In this paper, the GRAFCET(*GRA*phe *F*onctionnel de *C*ommande *E*tape/*T*ransition) language is used as a analysis and verification tool for safety-critical interlocking logic. The general description for Grafcet notation are provided and the general modeling for interlocking logic is presented.

1. 서 론

최근들어 컴퓨터를 이용한 제어시스템의 설계 및 제작 기술이 산업계 각 분야에서 실용화되어지고 있으며, 높은 레벨의 안정성·신뢰성이 요구되는 철도분야에서도 기존의 계전기를 이용한 논리회로가 컴퓨터를 이용한 제어스템으로 대체되어가고 있다.

기존의 계전기 등은 소자 자체의 Fail-safe 동작특성을 이용하여 높은 레벨의 안전성과 신뢰성을 확보할 수 있었지만 컴퓨터를 이용한 제어시스템은 기존의 계전기를 사용한 시스템만큼의 안전성 레벨을 확보하기가 어렵다. 이 높은 레벨의 요구사항을 만족할 수 있도록 하드웨어를 중복(Redundancy)으로 구성하는 등 하드웨어에 의한 안전성 확보방안들이 다양하게 제안 및 적용되고 있으며, 또한 상당부분 소프트웨어에도 그 역할을 요구하고 있다.

이에 따라 고장이나 오류의 발생을 최대한으로 줄일 수 있도록 소프트웨어가 개발되어져야 하며, 이를 위해서는 제어시스템 소프트웨어의 동작특성에 대한 사양을 엄격하게 정하여 로직상의 오류를 최대한으로 줄일 수 있도록 하여야 한다. 소프트웨어의 신뢰성 향상이 제어시스템 전체의 신뢰성을 확보하는데 중요한 부분이 된다. 이러한 노력의 하나로 철도 선진국에서는 높은 안정성을 요구하는 제어시스템의 소프트웨어 개발에 정형기법(Formal Method)을 적용하려는 연구가 진행 중에 있다[1]-[3]. 이는 소프트웨어 로직 및 그 동작특성을 수학적 표현을 기반으로 하는 엄격한 논리체계를 바탕으로 정의 및 표현하고 이를 검증함으로서 소프트웨어의 높은 신뢰성을 확보하는 것이다. 하지만 이러한 방법은 많은 개발기간을 필요로 하고 개발비용이 과다해지며 대규모의 전체시스템에 적용하기에는 다소 무리가 따른다. 특히 철도신호분야에도 철도 선진국에서는 연구가 진행 중에 있으나 아직은 연구차원에 머무르고 있다.

본 연구에서는 높은 안전성과 신뢰성이 절대적으로 요구되는 전자연동장치의 연동소프트웨어의 분석을 위한 표준화된 제어언어인 GRAFCET을 검토하였다. 또한 이 언어를 사용하여 연동로직을 모델링 하고 분석하는 방법을 설명한다[4].

2. Grafcet의 기본 표현

철도신호제어분야에서 기존의 계전기 로직에서 마이크로프로세서로 대체되어가면서 상대적으로 로직에 대한 안정성 및 신뢰성에 대한 부분이 더욱 중요하게 되었다. 이는 제어시스템이 전자화되어감에 따라 고장모드 분석 및 예측에 어려움이 있기 때문이다. 이에 따라 높은 안전성과 신뢰성을 요구하는 신호시스템, 특히 전자연동장치의 경우, 설계단계에서부터 높은 신뢰성과 안전성을 갖는 연동로직과 동작사양을 확보하여야 한다.

이처럼 시스템의 동작사양의 분석, 시뮬레이션 및 검증에 현재 일부에서는 페트리 네트(Petri-net)가 사용되고 있다[1]. 이 페트리 네트는 제어의 흐름과 상태의 변화를 모델링하고 시뮬레이션 하는데 유용하게 이용되어질 수 있다. 또한 80년대 후반 프랑스에서 이 페트리 네트의 특성을 그대로 가지면서 좀더 쉽게 표현하고 사용할 수 있는 Grafcet이 소개되었다[5][6]. 이는 프로차트 형식의 그래픽 언어로서 IEC 61131-3 규격으로 채택되었으며, 현재 유럽을 중심으로 제어로직의 표현 및 시뮬레이션, 제어시스템 구성 등에 많이 활용하고 있다.

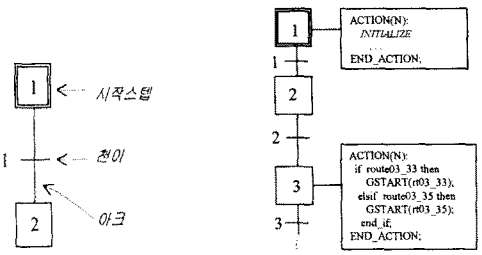

그림 1. Grafcet의 기본구조

이 Grafcet은 제어의 흐름 등을 그대로 프로차트 형식으로 표현하는 언어로서 조건이나 데이터 처리의 흐름이 직관적으로 이해되며, 상태의 변화 등의 관찰이 매우 용이하다. 또한 전체에서 톱다운시켜 프로그램을 전개할 수 있어 제어로직의 분석 및 검증에 용이하다. 본 장에서는 이러한 Grafcet 언어의 기본적인 표현방식을 살펴보고자 한다.

Grafcet은 일련의 제어동작을 여러 개의 스텝별로 프로그램 흐름과 조건들의 명확한 표현이 가능하도록 하는 제어로직의 동작사양을 모델링하고 표현할 수 있는 언어로서, 스텝(Step), 천이(Transition), 링크(Link), 제어액션(Control Action) 등으로 구성되어진다. 그 그

래프의 기본적인 표현은 그림1와 같이 페트리 네트와 거의 유사하다.

스텝은 활성화 상태와 비활성화 상태를 가지며 제어토큰이 표시된 스텝이 활성화 스텝이 된다. 스텝들 중 프로그램이 시작될 때 맨 처음 시작하는 스텝을 초기스텝이라 하며 이중 사각형으로 표시한다. 제어액션은 스텝에 대응하는 것으로 스텝이 활성화되면 수행되어지는 부분으로 각 스텝 옆에 사각형 내에 수행할 내용들을 표시하게 된다. 이 제어액션은 IEC에서 표준으로 정한 ST, IL, LD 등 어느 언어로도 표현이 가능하며, 모든 스텝들이 반드시 제어액션을 가질 필요는 없다. 천이는 스텝들을 활성화 또는 비활성화 시키도록 하는 것으로 천이의 점화조건을 만족하면 바로 전 스텝을 비활성화 시키고 다음 스텝을 활성화시키도록 하는 역할을 한다. 즉, 이 조건에 따라 제어토큰이 한 스텝에서 다른 스텝으로 이동하게 된다. 이 천이의 점화조건은 논리변수나 논리연산자, 타이머 등의 여러 가지 형태로 표현이 가능하다. 제어로직의 동작사양 표현시 이 천이의 점화조건이 프로그램의 제어흐름을 결정하는 중요한 부분이 된다.

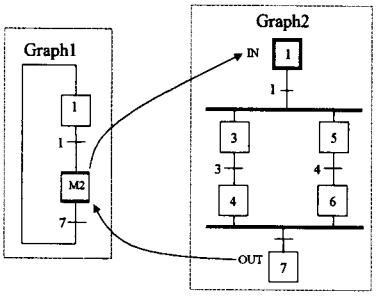

그림 2. 매크로스텝의 표현

또한 Grafcet은 좀더 효율적으로 로직의 제어흐름을 표현할 수 있도록 수렴OR(OR Convergence), 분산OR(OR Divergence), 수렴AND(AND Convergence) 및 분산AND(AND Divergence)에 의해 선택 시컨스와 병렬 시컨스가 가능하다. 결합OR은 여러 개의 천이 조건들 중 하나 이상이 만족하면 다음 스텝이 활성화되는 것이고, 분산 OR는 스텝의 출력이 여러 개의 천이조건으로 분기하는 것으로 여러 개의 천이조건들 중 하나를 만족하면 그 스텝으로 분기하게 된다. 이 결합 및 분산 OR는 여러 가지로 분기하고자하는 선택적인 로직 프로세스에 효과적으로 이용될 수 있다. 마찬가지로 결합 AND는 모든 스텝이 활성화되어야 만이 제어토큰이 다음 천이로 넘어갈 수 있으며, 천이가 점화되면 모든 입력 스텝들이 동시에 비활성화 된다.

그림2와 같은 매크로스텝(Macro Step)은 복잡한 제어로직을 계층적인 간략화된 그래프로 표현할 수 있도록 해 준다. 즉 복잡한 그래프를 매크로 스텝으로 표시하면 전체 제어흐름을 이해하기에 편리할 것이다.

3. 연동로직의 표현

전자연동장치는 열차집중제어장치나 조작반(LCP : Local Control Panel)으로 부터의 제어명령을 수신하여 선로변에 진로제어 신호를 발생시키고 또한 안전한 진로의 확보를 위한 각종 쇄정로직을 처리하는 열차의 안전운행을 마지막으로 책임지는 장치이다. 이러한 연동장치는 높은 안정성과 신뢰성의 연동로직의 확보가 매우 중요하다.

전자연동장치는 진로제어, 감시기능, 보호기능 등 여러 기능들을 수행하지만, 연동장치 고유기능은 안전한 진로제어이다. 이 진로제어에는 진로설정, 진로해정, 전철기 제어, 신호기 제어 등으로 다시 분류될 수 있는데 이러한 기능들을 수행함에 있어서 안전한 진로의 확보 및 보호가 되도록 진로쇄정, 전철기 쇄정, 철사쇄정, 접근쇄정 등의 각종 안전로직들을 필요로 한다.

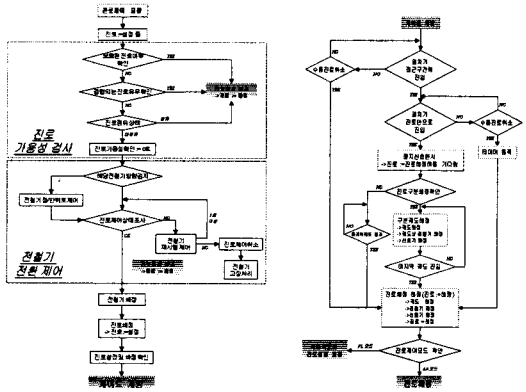

그림 3. 진로설정 및 해정 프로차트

그림3은 연동장치의 진로설정 및 해정을 위한 프로차트를 나타낸 것이다. CTC나 LCP로부터 진로요청이 있으면 요청된 진로가 제어가능한지를 우선적으로 검사하게 된다. 이 가용성 검사가 완료되면 진로상의 모든 전철기들의 위치를 확인하고 원하는 위치로 제어하게 된다. 그리고 나서 설정된 진로의 보호를 위해서 쇄정을 하게 된다. 이러한 일련의 과정이 모두 마무리되면 요청된 진로의 사용이 유효하게 되고 신호기나 마커로 게이트 개방신호를 전송하게 된다. 진로를 해정할 경우에도 궤도회로의 점유상태, 진로의 상태, 열차의 위치 등 해정조건을 우선적으로 검사하여야 한다. 즉 접근구간에 열차가 운행중일 때 진로취소 요구를 하게 되면 일정 시간 대기후 진로해정을 하는 접근해정이나 운행효율을 위해 구간별로 해정하는 진로구분해정 등이 해정시에 요구된다.

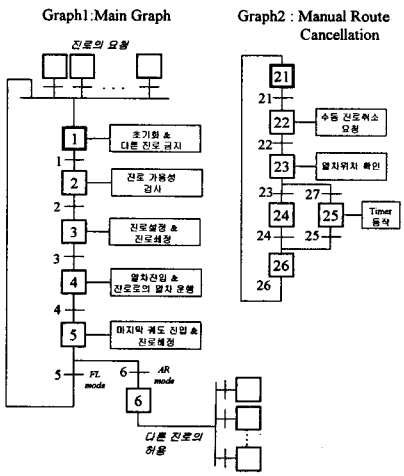

그림 4. Grafcet에 의한 개략적인 표현

그림3과 같은 프로차트의 완벽성과 좀더 실제적인 제어로직의 확보를 위해 본 연구에서는 이들 로직들을 앞장에서 검토한 Grafcet으로 모델링하여 시뮬레이션 및 상태변화의 관찰 등을 통하여 로직을 분석하고 있다. 그림4는 진로설정 및 해정의 개략적인 프로세스를 Grafcet으로 표현한 것이다. 그림은 첫 번째 단계의 그래프이고 각 각 단계별로 좀 더 세부적으로 모델링 이 되어지게 된다. 이 그림은 Graph1과 Graph2로 나뉘

어져 있는데 이는 Grafcet 언어의 병렬처리 특성을 활용한 것으로서, Graph1은 주 그래프이고 Graph2는 수동으로 진로 취소 요청이 될 경우의 그래프이다. 즉 초기 스텝인 스텝1과 21은 프로그램 시작과 동시에 수행되어지고, 그래프2는 수동진로 취소요구가 발생시까지 스텝22에 대기하고 있다가 요청시 그래프를 전개시키게 된다.

4. 연동로직 분석 시스템

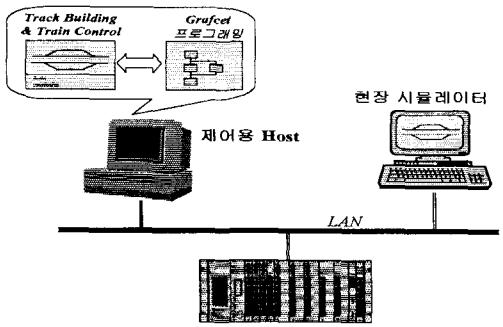

그림 5. 연동로직 분석을 위한 시스템 구성

전자연동장치의 연동로직 분석을 위한 시스템 구성은 그림5와 같다. 제어용 호스트에서는 그림6과 같은 궤도회로 편집 및 제어 입력을 위한 프로그램에서 선로변의 신호상태를 편집하게 되며, Grafcet 프로그램과 DDE 통신을 통해 데이터 교환을 하게 된다. 즉 그림6과 그림7 같은 윈도우를 이용하여 제어입력을 하고 이 입력을 바탕으로 Grafcet 프로그램에서 연동로직을 수행하게 된다.

이 Grafcet 로직이 LAN을 통해 VME 시스템으로 전송되어 처리되고 그 결과가 현장 시뮬레이터로 반영되게 된다. Grafcet 프로그램은 그림8처럼 프로그램의 전개과정을 직관적으로 확인할 수 있고 각 변수들의 상태변화가 별도의 윈도우를 통해 모니터링 가능하다. 이를 통해 제어 프로세스의 흐름 및 상태변화의 파악에 용이하여, 로직의 분석 및 검증에 유용하게 활용될 수 있다.

현재는 각각 모듈별로 프로그램이 진행 중에 있으며, 특히, 연동로직을 Grafcet으로 모델링 작업이 중점적으로 진행되고 있다.

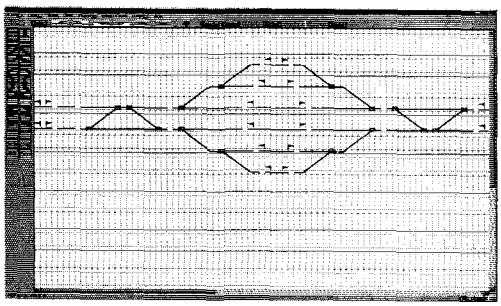

그림 6. 궤도회로 편집 및 제어용 윈도우 예

5. 결론

높은 레벨의 안정성과 신뢰성이 요구되는 전자연동장치 연동로직의 분석 및 검증을 위하여 Grafcet이라는 언어를 사용하였다. 이는 제어시스템의 상태변화 및 제어의 흐름을 그래픽적으로 모델링 할 수 있고, 또한 제어의 흐름을 이해하기가 쉽게 되어있어 제어로직과 동작사양의 분석, 표현 및 검증에 적절하다. 본 논문에서 이 언어의 기본적인 표현방법을 설명하였고 이 언어를 사용하여 연동로직의 일부를 모델링 하고 있다.

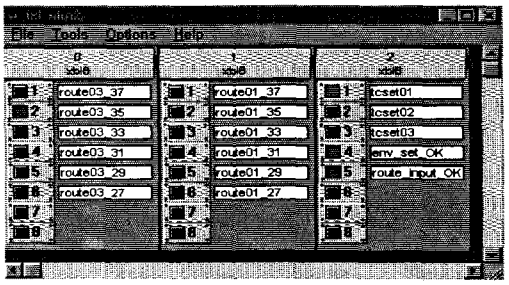

그림 7. 시뮬레이션 I/O 윈도우

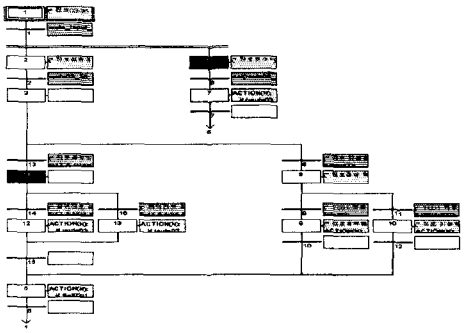

그림 8. Grafcet의 전개

이러한 Grafcet을 이용한 로직 분석 및 검증방법은 제어대상의 규모가 커지면 변수 및 상태의 수가 비약적으로 증가하므로 어느 정도의 역까지 가능한지에 대한 검토가 필요하다. 이러한 문제를 염두해 두고 현재 더욱 복잡한 연동로직의 모델링 중에 있다. 이 Grafcet 프로그램과 궤도회로 편집프로그램과 연계한 프로그램을 구성하여 높은 안전성과 신뢰성을 달성할 수 있는 연동로직 분석 및 검증을 위한 툴의 개발이 최종적인 목표이다.

[참 고 문 헌]

[1] 福岡 博, 福田 光芳, 'ペトリネットによる連動仕様の検証', RTRI Report Vol. 9, No. 11, pp. 19-24, 1995.

[2] J. Rushby, 'Formal Methods and the Certification of Critical Systems', Technical Report CSL-93-7, pp. 14-105, December 1993.

[3] Ian Mitchell and etc., 'Formal Mathematics for Signalling - A Tutorial Example', Report of an IRSE Seminar, pp. 17-30, 15th. April 1996.

[4] 황종규, '연동소프트웨어의 안전성 확보를 위한 시뮬레이션 기법', 한국철도학회 춘계학술대회, 5. 1999.

[5] Rene David, 'Grafcet : A Power Tool for Specification of Logic Controllers', IEEE Trans. on Control System Technology, Vol. 3, No. 3, pp. 253-268, 1995.

[6] P. Baracos, 'Tutorial Reference Guide to the Grafcet Automation Language : Grafcet Step by Step', Famic Technologies 2000 In., 1992.