한국철도학회논문집 제20권 제1호 ▌pp. 55-63 (2017년 2월)
JOURNAL OF THE KOREAN SOCIETY FOR RAILWAY VOL.20, NO.1 ▌pp. 55-63 (February 2017)
ISSN 1738-6225(Print)
ISSN 2288-2235(Online)

전자연동장치 S/W 안전성 확보를 위한 Z 방법표현에 관한 연구

Study on Z specification for S/W Safety of Computer Based Interlocking Systems

안 진 · 이종우*
Jin Ahn · Jongwoo Lee

Abstract Railway interlocking systems which are safety-critical systems are rapidly changed from relay-based systems to computer-based systems which have high flexible. Computer-based interlocking systems (CBI) are consisted of hardware and software in which system safeties arise one of important problems. The interlocking software of the CBI influences directly to the system safeties. “z” notation is one of formal methods have been used for system software specification to secure system safety. In this paper, the specification of interlocking logics for CBI systems is realized using “z” notation and verifies it with Z/EVES.

Keywords : Forma Methods, Z, PES, Interlocking, safety-critical

초 록 철도에 사용되고 있는 Safety critical systems 중 하나인 연동장치는 relay-based systems에서 computer-based systems으로 급속히 변환되고 있다. computer-based interlocking systems (CBI)의 안전성확보가 중요한 문제 중 하나로 떠오르고 있다. CBI를 구성하는 연동논리 software는 시스템 안전성에 직접적으로 영향을 미치는 부분 중 하나이다. Formal methods 중 하나인 “Z”notation은 이 software 안전성 확보를 위해 software 명세에 많이 사용되고 있다. 본 논문에서는 “Z”notation을 이용하여 연동논리 일부분을 구현하였으며, Z/EVES를 이용하여 검증을 하였다.

주요어 : 정형기법, Z, PES, 연동장치, 안전성

1. 서 론

일반적으로 자연언어를 이용하여 요구사항과 같은 공학적인 내용을 표시하는 경우에 확실성, 정밀성 등을 확보하기가 어렵다[1]. CBI(Computer based Interlocking)와 같은 장치를 개발하기 위해서 요구사항을 자연언어로 나타내면 시스템 복잡도가 높은 경우 요구사항이 불안정하거나 모순이 발생하는 경우가 많다[1,2].

시스템 검증을 위한 시험 시나리오는 사람이 만들어 낼 수 있는 경우 수가 한계가 있으며, 아무리 많은 수의 테스팅을 수행한다 하더라도 그것이 시스템의 안정성을 100% 보장한다고는 말할 수 없다. 따라서 근래에는 최대한 많은 수의 시나리오를 자동으로 생성해 내기 위한 연구가 많이 진행되고 있으며, 이러한 방법 중 하나가 정형기법(Formal Methods)이다[3,4].

정형기법은 수학과 논리학에 기반 하기 때문에 표현이 명확하고, 기계적이고 논리적인 증명 절차에 따라 가능한 모든 경우에 대한 증명을 수행하여 신뢰할 수 있는 시스템의 구현에 도움을 준다.

전자연동장치와 관련되어 수학적 모델링을 하여 안전성을 검증하는 시도가 많이 이루어지고 있다[5,6,7]. 전자연동장치를 set theory[8]를 이용하여 모델링하고, 그 모델을 이용하여 다양한 정형기법을 이용하여 안전성을 검증하고 있다. 연동논리의 소프트웨어 구현은 표준화가 되어 있지 않기 때문에 현재에도 다양한 방법으로 전자연동장치의 논리를 모델링 하고, 정형기법을 이용하여 증명하고 있다. 본 논문에서도 set theory를 이용하여 연동논리를 모델링하고, “Z”notation 이용하여 논리를 증명하였다. 본 논문의 구성은 2장에서 전자연동장치에 기본에 대해서 기술하였으며, 3장에는 일부 진로제어 연동논리를 set theory로 모델링을 하였으며, 4장에서는 그 모델링을 “Z/EVES”를 이용하여 “Z”notation의 진로제어 명세로 기술하고, 이 기술이 논리적 오류가 없음을 증명하였다[9].

*Corresponding author. E-mail: saganlee@seoultech.ac.kr.

https://doi.org/10.7782/JKSR.2017.20.1.55

2. 전자연동장치 요구명세

2.1 전자연동장치

Computer Based Interlocking System인 전자연동장치는 하드웨어와 소프트웨어로 구성되어 있다. 전자연동장치를 구현하는 방법으로는 각 역의 특성에 따라서 연동장치의 로직을 직접 소프트웨어로 구현하는 방법과 연동장치논리를 해석할 수 있는 코어프로그램과 각각의 역의 특성을 나타내는 데이터베이스를 이용하는 방법이 있다[1]. 전자의 방법으로 역의 논리를 직접 구현하는 이유는 릴레이 로직으로 논리의 완벽성을 검증한 후에 그 논리를 그대로 전자연동장치에 적용시키는 방법이다. 후자는 현재 많이 사용하고 있는 방법으로 유연성이 높아 모든 역에 쉽게 적용할 수 있다. 대부분의 전자연동장치는 하드웨어와 소프트웨어로 구성되어 있으며, 하드웨어는 선로변 장치와 인터페이스를 담당하고, 소프트웨어는 하드웨어에서 논리처리를 한다. 소프트웨어는 코어에 해당하는 연동논리 소프트웨어와 각역의 특성을 나타내는 그래픽 프로그램으로 구성되어 있다.

전자연동장치는 안전기능을 수행하기 때문에 요구사상의 정확성이 필요하다. 전자연동장치는 하드웨어와 소프트웨어가 결합되어 경우의 수가 combinatoric하게 증가하게 되고, 이러한 복잡성으로 인하여 요구사항을 정확하게 검증하는 것은 상당히 많은 작업을 동반한다[2]. 본 논문에서는 formal methods를 이용하여 전자연동장치의 요구사항 완벽성을 검증하는 방법을 제시하였다.

2.2 전자연동장치의 특성

2.2.1 전자연동장치의 구성요소

전자연동장치는 열차의 진로를 제어하는 장치이다. 진로는 하나의 폐색과 다음 폐색 간의 궤도 구간을 따라 진행하는 경로로서, 궤도회로, 선로전환기 및 신호기들로 구성되어 있으며, 서브진로를 갖고 논리적 특성을 갖는다. 어떤 진로 R_i에 대해서 진로개통은 열차가 그 진로에 진입할 수 있도록 진로 신호기가 통과신호를 현시한 것을 말하며, 진로차단은 그 진로신호기가 정위로 복귀되어 정지신호를 현시하여 그 진로 R_i에 진입할 수 없는 것을 말한다.

전자연동장치에서 진로를 설정하는 프로세스는 Fig. 1과 같다. 진로를 설정하기 위해서는 진로요청에 따라서 진로선별모듈에서 진로개통 가능여부를 판단하고 진로개통이 가능할 때 진로를 설정하고 신호기를 통과신호로 현시한다.

전자연동장치는 진로를 구성하는 실제적인 장치인 궤도회로, 선로전환기 및 신호기와 논리적으로 설정된 진로를 다음과 원칙에 의해서 동작을 한다.

① 진로는 경합하지 않는다. 즉 모든 궤도회로는 주어진 시간에 오직 한 진로에만 할당되어 쇄정되어, 다른 진로에는 절대로 할당되지 않는다.

② 선로전환기(point machine)를 포함하는 궤도구간에 걸쳐있는 서브진로가 한 진로에 대해서 쇄정되어 있다면, 선로전환기는 그 서브진로에 맞게 설정되어 있다.

③ 진로가 설정되면, 그에 해당하는 서브진로는 모두 쇄정된다.

④ 철사쇄정 : 선로전환기가 포함되어있는 궤도회로가 점유되어 있다면, 그 선로전환기는 쇄정된다.

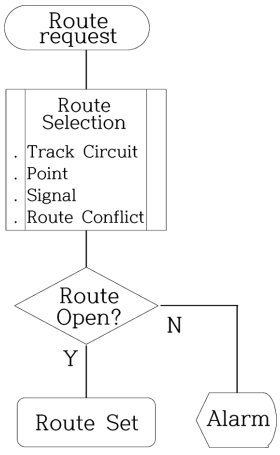

Fig. 1. Process of route setting.

⑤ 진로연쇄 : 한 진로에 대한 서브진로가 쇄정되었다면, 그 진로에서 선행구간의 모든 진로는 쇄정된다.
전자연동장치는 선로변 장치, 논리적 진로 및 진로를 제어하는 원칙으로 구성되어 있다.

2.2.2 전자연동장치 요구명세 및 검증

전자연동장치의 요구명세를 도출하기 위해서는 앞 절에서 언급한 전자연동장치의 원칙을 이용한다. 잘못된 명세에 의한 작업은 개발과정이 충실하다 하더라도 쓸모없는 시스템이 된다. 현재까지 대부분 사용자의 요구명세는 자연어(natural language)로 표시된다. 정형화는 자연어 요구명세를 정형 명세로 mapping하는 것이다. 정형화는 수학적 표기법을 이용하여 시스템의 특성 및 기능을 서술하여, 증명 가능하도록 하는 방법이며, 이 방법은 수학적 완전성(completeness), 정확성(correctness) 및 일관성(consistency) 등을 가지고 있다[3,4].

2.3 전자연동장치의 정형화

2.3.1 정형화 방법

정형명세를 위한 확실한 방법은 정해져 있지 않다. 소프트웨어는 한 가지의 통일된 수학이론으로 나타낼 수 없다. 이것은 소프트웨어 언어 기준 및 이론의 다양성으로 인해 많은 프로그래밍 언어가 존재하는 것과 같다. 각기 다른 사람들은 같은 문제를 푸는데 서로 다른 프로그래밍언어를 사용한다.

정형기법의 핵심은 요구명세의 개념을 찾는 것이다. 요구명세는 데이터를 변경시키는 작업으로서, 어떻게 데이터를 처리된 데이터로 변경시키는가에 대한 서술이다. 정형명세에는 시스템 모델 동작특성 및 목표시스템의 동작특성에 대한 2가지 방법이 있다.

-모델화된 시스템의 동작특성은 연산(operation), 가능한 기능, 혹은 동작(action) 등으로 표시된다. 핵심적인 요소는 모델화된 시스템의 초기 상태에서 각각의 동작에 의해서 데이터가 변경되는 것에 대한 분명한 정의이며, 이 방식을 상태기반 혹은 모델기반 요구명세 언어라고 한다.

- 목표 시스템의 동작특성은 처리된 데이터 즉 그 데이터가 어떻게 처리되는 것 혹은 그것에 관련된 방법에 집중되어 있으며, 이 요구명세는 대수 요구명세(algebraic specification) 혹은 공리 요구명세(axiomatic specification)이다.

모델기반 요구명세는 상태변환 시스템(transition system), 추상 상태머신(abstract state machine), 집합기반 요구명세 등이 있으며, 목표시스템의 내부 상태의 개념(notion)을 기술하는 능력, 혹은 어떻게 시스템의 동작이 시스템의 상태를 변경시키는가에 의해서 결정된다. 이 방법에는 집합이론(set theory), 분류이론(category theory), 및 논리이론, 오토마타 기반 모델링 등이 있다[9].

2.3.2 연동논리 정형화

진로의 물리적 구성은 궤도회로, 선로전환기 및 신호기로 되어 있고, 이 시스템들의 상태에 의해서 어떤 특정진로를 결정할 수 있으며, 연동장치는 진로개통(open)과 차단(closed)을 수행한다. 연동장치는 진로의 개통과 차단을 수행하기 위해서 일련의 시퀀스를 통하여 반복적으로 수행을 한다. 따라서 전자연동장치의 동작요구명세(behavior specification)는 진로개통과 차단을 반복적으로 수행하는 일련의 시퀀스가 포함되어야 한다.

상태변화를 나타내는 경우, 아날로그 시스템은 연속이 되고, 전자연동장치의 경우는 이산형이 된다. 대부분의 방법은 상태변화 사이의 상태를 결정하는 원인으로 외부 혹은 내부를 구분하지 않고 관측점을 사용한다. 상태변화는 결정하고자 하는 사건과 연관되며, 이것을 레이블 혹은 동작이다. 동작 시퀀스는 동작이 주기적으로 수행되며, 동작의 초기상태에서 동작이 완료되는 종료상태가 반복된다. 따라서 전자연동장치는 상태변환 시스템(transition systems)으로 나타낼 수 있다. 상태변환 시스템은 상태공간, 초기상태 혹은 초기 상태의 집합 및 상태 간의 변환 집합 등으로 나타낼 수 있다. 전자연동장치의 진로 구성 요건은 진로를 구성하는 궤도회로가 차량에 의한 점유가 아닌 상태이거나 혹은 다른 진로에서 사용하지 않아야 하며, 선로전환기가 진로방향으로 전환되어야 한다. 그러므로 전로 구성에 대한 연동논리 정형화는 궤도회로, 선로전환기, 다른 진로(신호기)의 상태변환 집합이다.

3. 진로제어의 명세 정형화

3.1 전자연동장치 모델링

전자연동장치 모델링은 진로를 모델링하는 것이다. 전자연동장치의 진로는 여러 개의 진로 즉 큰 역의 경우는 수백 개의 진

로, 아주 작은 역의 경우는 10개 이내의 진로로 구성되는 경우도 있다. 진로는 신호기와 신호기 사이의 선로이며, 기본 단위는 궤도회로(track circuits), 선로전환기(point machines) 및 신호기(signals)로 구성되어 있다. 1개의 진로는 다수의 궤도회로 및 선로전환기를 가질 수 있고, 단지 하나의 신호기만을 갖는다. 각각의 진로는 궤도회로, 선로전환기를 공유하여 진로를 구성할 수 있다. 각 진로는 서로 공유된 시스템을 배타적으로 사용하여, 진로를 설정한다[7].

3.2 전자연동장치의 시스템 모델링

전자연동장치의 모델링은 선로를 구성하는 궤도회로(track circuits), 선로전환기(points) 및 신호기(signals) 등과 같은 물리적인 서브시스템과 2개의 신호기 사이의 궤도로 구성된 진로(routes), 부분진로(sub-routes) 논리 시스템이 이용된다.

이 기본 시스템은 다음과 같이 정의된다.

$$TCircuits = \{T_i^s \mid i \in I, s = f \vee o\} \tag{3.1}$$

$$Points = \{P_i^{d,s} \mid i \in I, d = n \vee r, s = f \vee l \vee o\} \tag{3.2}$$

$$Signals = \{S_i^s \mid i \in I, s = p \vee s\} \tag{3.3}$$

$$Routs = \{R_i^s \mid i \in I, s = f \vee l \vee o\} \tag{3.4}$$

$$SubRoutes = \{r_i^s \mid i \in I, s = f \vee l \vee o\} \tag{3.5}$$

TCircuits, *Points* 및 *Signals*은 실제적인 시스템이다. *Routes* 및 *Subroutes*는 논리적인 구성이다. *SubRoutes*는 궤도회로 T_i와 일대일로 연결이 되며, 식 (3.6)과 같이 궤도회로 방향에 따라 서브진로가 달라진다.

$$r_i^s = \{T_i^{ab}, T_i^{ba} \mid i = 1 \cdots n,\ ab,\ ba\text{: direction of track circuit}\} \tag{3.6}$$

TCircuits, *Points*, *Signals*, *Routes* 및 *SubRoutes*는 indexed set이며, "*i*", "*s*" 및 "*d*"는 set의 index이다.

$$i = \{i \mid i \in I,\ i : number\ of\ each\ set\} \tag{3.7}$$

$$s = \{f,\ l,\ o,\ pf,\ s,\ p \mid l : lock,\ o : occupied,\ pf : partailly\ free,\ s : stop,\ p : pass\} \tag{3.8}$$

$$d = \{n,\ r,\ ab,\ ba \mid n : normal,\ r : reverse,\ ab : a\ to\ b\ direction,\ ba : b\ to\ a\ directi\ o\ n\} \tag{3.9}$$

진로를 구성하면 *TCircuits*, *Points*, *Signals*, *Routes* 및 *SubRoutes*의 시스템들 사이에 Fig. 2 와 같이 상호연관 관계(relation)가 있다. 5개의 시스템은 ${}_5P_2$의 관계가 있으며, 각 시스템 자체의 관계를 고려하면, 30개의 관계가 성립된다. 1개의 진로는 *TCircuits*, *Points*, *Signals*, *Routes* 및 *SubRoutes*를 구성하는 member들의 조합에 의해서 나타낼 수 있다.

TCircuits, *Points*, *Signals*, *Routes* 및 *SubRoutes*의 member들의 조합은 power set $\mathbb{P}(\cdots)$으로 나타냈으며, ${}^S()$는 power set을 나타낸다.

$${}^S T = \mathbb{P}(TCircuits) \tag{3.10}$$

$${}^S P = \mathbb{P}(Points) \tag{3.11}$$

$${}^S S = \mathbb{P}(Signals) \tag{3.12}$$

$${}^S R = \mathbb{P}(Routes) \tag{3.13}$$

$${}^S r = \mathbb{P}(SubRoutes) \tag{3.14}$$

Proposition 1: 진로 R_i는 신호기 S_i와 S_j 사이를 나타내며, 그 사이에 신호기 $S_k (i \neq j \neq k)$가 존재하지 않는다.

proof: $\forall R_i$ 는 두 신호기 사이를 정의하는 것으로 S_i와 S_j 사이에 신호기 S_k가 있다면 S_i와 S_k 혹은 S_k와 S_j사이가 새로운 진로 R_i가 된다.

Proposition 2: $\exists R_i$ 는 궤도회로가 반드시 있으며, 그 궤도회로 power set ${}^{S}T$의 부분 집합 ${}^{S}T_i$이며, ${}^{S}T_i$는 1개 이상의 T_i^S가 물리적으로 연속적으로 연결된 T_i^S로 구성된다.
proof : ${}^{S}T$는 식 (3.10) 집합의 power set이며, 모든 경우의 수를 포함하므로, 그 부분 집합 ${}^{S}T$는 ${}^{S}T_i \subseteq {}^{S}T$이며, 진로 R_i는 연속된 궤도회로 나타낼 수 있으므로 ${}^{S}T_i$로 나타낼 수 있다.

Proposition 3: $\exists R_i$ 는 구성하는 선로전환기(point)들은 ${}^{S}P_i$로 나타낼 수 있다.
proof: ${}^{S}P_i$는 ${}^{S}P_i \subseteq {}^{S}P$이다.

따라서 진로 R_i는 ${}^{S}T_i$, ${}^{S}P_i$ 및 S_i의 부분 집합으로 식 (3.15) 과 같이 나타낼 수 있다.

$$R_i = \{{}^{S}T_i,\ {}^{S}P_i,\ S_i,\ S_j | {}^{S}T_i \subseteq {}^{S}T,\ {}^{S}P_i^d \subseteq {}^{S}P,\ (S_i,\ S_j) \subseteq {}^{S}S\} \tag{3.15}$$

부분집합 ${}^{S}T_i$의 "n"개의 원소도 indexed subset로 나타낼 수 있다.

Proposition 4: $\exists R_i$ 를 구성하는 ${}^{S}T$는 물리적으로 연속적으로 연결된 T_i^S로 구성되며, 연속적으로 연결된 것을 ordered ${}^{S}T_i$를 ${}^{S}T_{i,j}^{s}$ 이라 하며, 식 (3.16)와 같이 나타낼 수 있다.

$${}^{S}T_{i,j}^{s} = \{{}^{S}T_{i,j}^{s} :\ {}^{S}T_{i,j}^{s} \in {}^{S}T_i | 1 \le j \le n,\ n :\ element\ number\ of\ {}^{S}T_i\} \tag{3.16}$$

proof: $\forall {}^{S}T_{i,j} \in {}^{S}T_i$ 이므로 $({}^{S}T_{i,j} \in {}^{S}T_i) \equiv ({}^{S}T_i \in {}^{S}T_i)$ 이다.

Proposition 5: $\exists R_i$ 를 구성하는 선로전환기(point)들은 ${}^{S}P_i$를 ordered ${}^{S}P_i$를 ${}^{S}P_{i,j}^{d}$ 로 식 (3.17)과 같이 나타낼 수 있다.

$${}^{S}P_{i,j}^{d} = \{{}^{S}P_{i,j}^{d} :\ {}^{S}P_{i,j} \in {}^{S}P_i | 1 \le j \le n,\ n :\ element\ number\ of\ {}^{S}P_i\} \tag{3.17}$$

proof: $({}^{S}T_{i,j} \in {}^{S}T_i) \equiv ({}^{S}T_i \in {}^{S}T_i)$ 이므로, ${}^{S}T_{i,j} \equiv {}^{S}T_i$ 이다.

Proposition 6: R_i를 구성하는 ${}^{S}T_{i,j} \cong {}^{S}r_{i,j}$ 로 대체할 수 있으며, 식 (3.16)를 식 (3.18)와 같이 변환할 수 있다.

$${}^{S}r_{i,j}^{d} = \{{}^{S}r_{i,j}^{d} :\ {}^{S}r_{i,j} \in {}^{S}r_i | 1 \le j \le n,\ n :\ element\ number\ of\ {}^{S}r_i\} \tag{3.18}$$

proof: $T_i \cong r_i$ 이므로 ${}^{S}T_{i,j} \cong {}^{S}r_{i,j}$ 이다.

따라서 진로 R_i는 식 (3.15)에서 식 (3.19)로 나타낼 수 있다.

$$R_i = \{{}^{S}r_i^{s},\ {}^{S}P_i^{d}, S_i, S_{k_i} \mid {}^{S}r_i \subseteq {}^{S}r,\ {}^{S}P_i^{d} \subseteq {}^{S}P, (S_i, S_k) \subseteq {}^{S}S\} \tag{3.19}$$

Fig. 2는 각 부분집합들 사이에 관계(relation)가 있음을 보여주며, 30가지의 관계가 있다. 진로구성에 따른 관계를 정의하기 위해서 시스템의 "요소관계"와 "제어관계"(control conditions)로 나누었으며, 요소관계는 "element", "be consisted of", "overlap", "linked", "neighbor" 및 "match"를 도출하고, 제어관계를 나타내는 "lock", "direction" 및 "signal"을 도출하였다.

요소관계에서 "element"는 "$x \in M$", "be consisted of"는 "$\{x|E(x)\}$"인 집합, "overlap"은 "$\cap$"의 intersection, "linked"와 "match"는 "bijection"의 관계를 가지고 있다. 제어관계는 시스템의 상태가 다른 시스템에 미치는 영향이 있는 것을 정의 하였다. 제어관계는 각 시스템들 간에 상태에 의해서 종속되는 관계를 나타내며, control은 "lock", "direction" 및 "signal"이다.

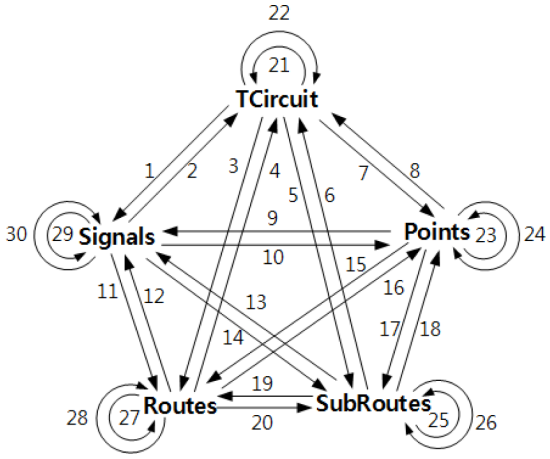

Fig. 2 Relations between systems.

Fig. 2에 의해서 각 시스템간의 관계 "ℝ"를 간단하게 정의할 수 있다.

$$element = {}^{S}r_i \ \mathbb{R} \ R_i \tag{3.20}$$

$$lock = {}^{S}r_i \ \mathbb{R} \ R_i \tag{3.21}$$

$$be\ consisted\ of = R_i \ \mathbb{R} \ ({}^{S}r_i \wedge {}^{S}P_i) \tag{3.22}$$

$$linked = T_i \ \mathbb{R} \ P_i \tag{3.23}$$

$$signal = (f : R_i^l \Rightarrow S_i^p \ \text{if} \ R_i \Rightarrow R_i^l) \vee (f : R_i^l \Rightarrow S_i^s \ \text{if} \ R_i \Rightarrow R_i^l) \tag{3.24}$$

$$\begin{aligned} status = {} & (f : r_i^d \Rightarrow r_i^f \vee r_i^o \vee r_i^l) \vee (f : R_i^d \Rightarrow R_i^f \vee R_i^o \vee R_i^l) \\ & \vee (f : P_i \Rightarrow P_i^{d,f} \vee P_i^{d,o} \vee P_i^{d,l}) \vee (f : S_i \Rightarrow S_i^s \vee S_i^p) \end{aligned} \tag{3.25}$$

3.3 연동논리

열차가 진로 R_i를 통과하는 event를 E_i라 정의한다. 열차진로통과 E_i를 위해서는 R_i에 대해서 각 시스템의 설정, 쇄정, 개통 후에, 열차의 진입 및 통과의 절차가 필요하며, 통과 후에는 그 진로를 재개통하기 위해서 쇄정된 시스템을 해정해야 한다. 진로 R는 항상 차단이 되어 있어, 진입을 허가하는 신호기 S는 항상 정지신호를 현시 하므로 식 (3.23), 식 (3.26)과 같이 나타낼 수 있다.

$$status \ : S_i \in R_i \Rightarrow S_i^s \tag{3.26}$$

1) 진로설정 및 개통

간략화된 연동논리에 의해 진로 R_i를 개통하기 위해서는 첫 번째로 식 (3.28)을 만족해야 한다.

$$R_i \cap R_j^l = \varnothing, \ \forall j, i \neq j \tag{3.27}$$

$$ran(status: \ R_i) = {}^{S}r_i^f \wedge {}^{S}P_i^{d,f} \wedge S_i^s \Rightarrow R_i^f \tag{3.28}$$

$$ran(signal: \ R_i^f) = S_i^p \tag{3.29}$$

$$(ran(status: \ R_i) = R_i^f) \wedge (ran(status: \ S_i) = S_i^p) \tag{3.30}$$

2) 진로차단

진로가 차단 되는 것은

$$ran(status:\ R_i) = {}^{S}r_i^{o} \vee {}^{S}P_i^{d,o} \Rightarrow R_i^{o} \tag{3.31}$$

$$ran(status:\ R_i^{o}) = S_i^{o} \tag{3.32}$$

$$(ran(status:\ R_i) = R_i^{o}) \wedge (ran(status:\ R_i^{o}) = S_i^{s}) \tag{3.33}$$

3) 부분해정

$$ran(status:\ {}^{s}r_i) = r_{i,j-1}^{f} \wedge r_{i,j}^{o},\ (1 < j \le n) \tag{3.34}$$

4) 철사쇄정

$$(ran(linked:\ T_i) = P_i) \wedge (ran(status:\ T_i) = T_i^{o}) \tag{3.35}$$

4. “Z”의 진로제어의 명세

4.1 “Z” Notation

“Z” notation은 정형기법 중의 하나이며, 집합이론 및 1차 술어(1st order predicate) 수학적 논리를 이용하여 모델링하는 특수 언어이다. “Z” notation을 이용하여, sets and types, declarations, 변수, expression 및 연산자, predicates, equation 및 laws 등을 나타낼 수 있으며, formal reasoning을 수행할 수 있다.

4.2 전자연동장치의 시스템 “Z” 모델링

전자연동장치를 구성하는 시스템을 “Z” notation을 이용하여 식 (3.36)과 같이 나타낼 수 있다.

$$[TCircuit,\ Points,\ Signals,\ Routes,\ Subroute] \tag{3.36}$$

TCircuit, Point, Signals, Routes 및 Subroutes의 power set은 “Z” notation의 schema를 이용하여 다음과 같이 나타낼 수 있다. 전자연동장치를 구성하는 시스템을 Fig. 3과 같이 나타낼 수 있다.

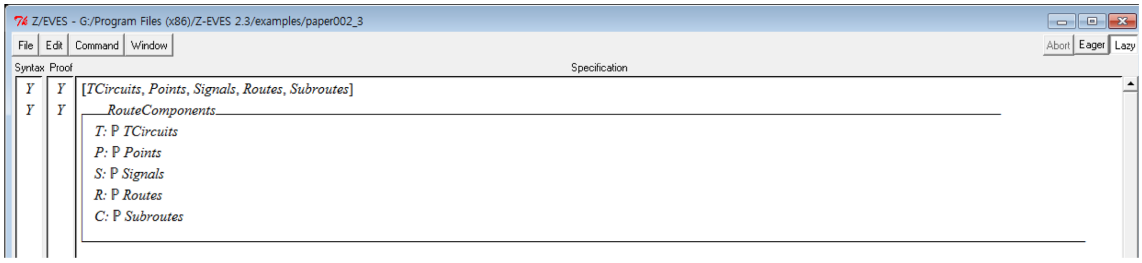

Fig. 3 “Z” Notation for systems definition of interlocking systems.

전자연동장치에 진로 R_i를 구성하는 시스템은 Fig. 4와 같이 나타낸다.

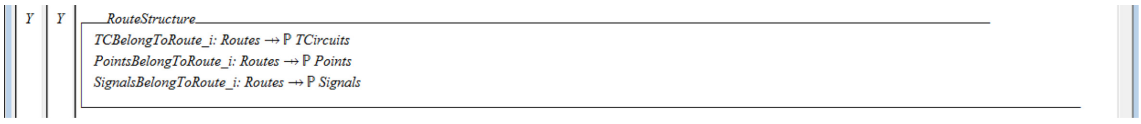

Fig. 4. “Z” Notation of route structure.

진로 R_i의 연동논리는 Fig. 5와 같이 나타낸다.

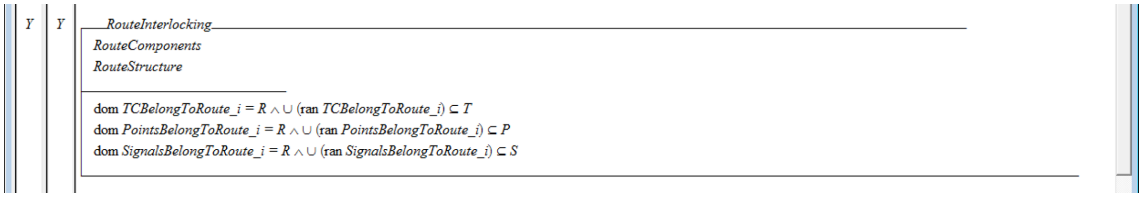

Fig. 5. "Z" Notation of route interlocking.

진로 R_i의 설정, 개통 및 차단에 대한 "z" notation은 Fig. 6과 같이 나타낸다.

Fig. 6. "Z" Notation of route set, open, and close.

Fig. 3에서 "syntax"와 "proof"가 각각 "Y"로 표시된 것은 "Z" notation으로 정확하게 표시되었다는 것을 나타내고, "proof"의 "Y"는 논리적으로 증명되었다는 것을 나타낸다.

정형기법으로 전자연동장치의 명세를 나타내는 것은 시스템의 상태 즉 시스템 데이터가 어떻게 변화되는 것을 나타낸 것이다.

5. 결 론

전자연동장치의 진로구성에 관한 논리를 "Z" notation을 이용하여 구현하였다. "Z" notation으로 구현하기 위해서 집합이론을 이용하였으며, 그 집합 모델링을 "Z" notation을 이용하여 구현하였다. 연동논리를 구성하기 위해서 궤도회로, 선로전환기, 신호기, 진로 및 서브진로를 모델링했으며, 궤도회로, 선로전환기를 set theory의 power set을 이용하여 나타냈으며, "Z/EVES"툴을 이용하여 "Z" notation으로 모델링하고 증명을 하였다.

전자연동장치 모델링은 시스템의 power set으로 모델링을 하였으나, 전자연동장치를 구성하는 시스템을 정확하게 일치시키기에는 set theory로 한계가 있었다. set theory를 이용하여 진로를 구성하는 궤도회로의 순차적인 모델링, 부분진로의 부분 해정 등을 indexed set을 이용하여 나타낼 수는 있지만, "Z" notation을 이용하여 정확하게 구현하기에 어려움이 있었다. 향후 연구과제로는 set theory를 이용하여 모델링한 부분집합의 원소들을 "Z" notation으로 구현하는 방법의 개발이 필요하다.

전체적으로 전자연동장치의 연동논리의 구현은 궤도회로, 선로전환기 및 신호기와 같은 물리적인 서브시스템과 2개의 진로(routes), 부분진로(sub-routes) 논리 시스템 전체를 포함하는 방법으로 구현을 하였으며, 연동논리의 일부 진로제어의 "Z" notation 표현이 논리적인 모순이 없다는 것을 증명하였다. 이를 통해 "Z" notation이 전자연동장치의 연동논리를 안전성이 확보된 소프트웨어로 구현할 수 있음을 보여준다.

후 기

본 연구는 2016년도 서울과학기술대학교 산학협력단의 지원에 의하여 이루어진 "전자연동장치 S/W 안전성 확보를 위한 Z 방법표현에 관한 연구"에 대한 연구로서, 관계부처에 감사드립니다.

References

[1] D.K. Shin, K.H. Shin, K.M. Lee, J.H. Lee (2011) Study on the specification development of the safety-critical Korean high-speed rail interlocking equipment (in Korea), *2011 Spring Conference of the Korean Society for Railway*, Hoengseong, pp. 101-108.
[2] K.Y. Song, J.S. Choi, J.K. Choi, S.Y. Heo (2012) Interlocking Types (in Korea), Korea Rail Network Authority, KR S-06020 Rev.4
[3] J. Jacky (1996) *The way of Z : Practical programming with formal methods*, Cambridge university press, Cambridge.
[4] B. Potter, J. Sinclair, D. Till (1996) *An Introduction to Formal Specification and Z*, Prentic Hall, New Jersey.
[5] S.A. Khan, N.A. Zafar (2009) Towards the Formalization of Railway Interlocking System using Z-Notations, *2009 2nd International Conference on Computer, Control and Communication*, Karachi Sindh, Pakistan.
[6] K. Kanso, A. Setzer (2009) Specifying Railway Interlocking Systems, *Ninth International Workshop on Automated Verification of Critical Systems*, Swansea, UK.
[7] A. Janota (2000) Using Z Specification for Railway Interlocking Safety, *Periodica Polytechnica Transportation Engineering*, 28(1-2), pp. 39-53.
[8] http://people.umass.edu/gmhwww/595t/text.htm (Accessed 1 November 2016).
[9] M. Saaltink (1999) *The Z/EVES 2.0 User's Guide*, ORA Canada, Ottawa, Ontario.

(Received 2 February 2017; Revised 13 February 2017; Accepted 16 February 2017)

Jin Ahn : jinahn@daeati.co.kr
Department of Railway Electrical & Signaling Engineering, Graduate School of Railway, Seoul National University of Science and Technology, 232 Gongneung-ro Nowon-gu, Seoul 139-743, Korea
Jong-Woo Lee : saganlee@seoultech.ac.kr
Department of Railway Electrical & Signaling Engineering, Graduate School of Railway, Seoul National University of Science and Technology, 232 Gongneung-ro Nowon-gu, Seoul 139-743, Korea