設 計 自 動 化 91－12
(1999. 2. 5)

モデル検査法を用いた鉄道信号システムの連動仕様検証

川村 正

三菱電機(株)先端技術総合研究所
〒661-8661 兵庫県尼崎市塚口本町 8-1-1
Tel：06-6497-7138
E-mail：kawamura@sys.crl.melco.co.jp

鉄道信号システムは、障害や誤動作が重大な事故につながるため、安全性に関して厳しい基準が求められている。特に駅構内の交通は輻輳するため、安全の確保のためには複雑な運行制御が必要となる。駅構内の信号機や転轍器の制御を行う装置は連動装置と呼ばれ、保安機能の実現に関して中心的な役割を果たす。一方、安全性・信頼性の高いシステムを実現するための技術として形式的手法が近年注目されている。本研究では、連動装置の制御仕様の形式的検証を行う方法を提案する。連動装置や駅構内の機器の動作を有限状態機械で、これらの装置の動作が満たすべき性質を時相論理式で記述し、有限状態機械上で時相論理式が成り立つかどうかを、モデル検査法と呼ばれる方法で検証する。

キーワード：形式的検証、試験、鉄道システム、信号システム、時相論理

Verification of Railway Interlocking Specifications by a Model Checking Method

Tadashi Kawamura

Advanced Technology R&D Center, Mitsubishi Electric Corporation
8-1-1, Tsukaguchi-Honmachi, Amagasaki, Hyogo, 661-8661
phone : +81-6-6497-7138
email : kawamura@sys.crl.melco.co.jp

The verification of safety requirements is a fundamental problem in railway signaling system design. Especially, specifications of railway inter-locking systems, which control railway signals and points in a station in a safety-critical manner, become very complex and hard to verify. Recently in this fields, formal verification is expected to be a promising technique for verifying safety requirements. This paper describes how to verify a railway inter-locking specifications by a formal verification method. A railway inter-locking system is described by a finite state machine and safety requirements are described by temporal logic formulas. Then, by a model checking method, the formal verification of the temporal logical specification is done.

Key Words : Formal Verification, Testing, Railway System, Signaling, Temporal Logic

1．はじめに

鉄道信号システムは、列車の位置検知と転轍器（分岐器）の制御を行い、制御盤からの操作に従って信号機等で列車に進行・停止の指示を与えることによって列車の運行制御を行う。特に駅構内では交通が輻輳するため、連動装置と呼ばれる装置によって列車運行の安全を確保している。鉄道信号システムは、障害や誤動作が重大な事故につながるため、安全性に関して厳しい基準が求められている。中でも連動装置は鉄道信号システムの保安機能に関して中心的な役割を果たしているが、連度装置の行う制御は比較的小規模な駅でも複雑になり、その設計・検査には膨大なコストがかけられている。本研究では、モデル検査法を用いて連動装置の制御論理の形式的検証を行う方法を提案する。

2．連動装置

2．1 連動装置の概要

駅構内には多くの線路が集中・分岐し、列車運行に必要な進路を構成できるようになっている。そのため、線路が分岐・交錯する点には多数の転轍器が設置され、また進行すべき進路を指示するために多数の信号機や標識が設置されている。衝突・脱線・接触などの事故を引き起こすことなく、かつ能率良く列車運行を行うためにはこれらの信号機や転轍器を適切に取扱うことが必要である。

列車の本数が少なく、速度も遅かった時代にはオペレータが安全を確認しながら操作することによって運行制御を行うことが可能であったが、現在では人手に頼ったまま安全を確保し、能率良く運行することはほとんど不可能になっている。そこで、列車の進行に際しては以下のような制御を行う。

（1）進路上に他の列車がいない、分岐器が必要な方向を向いている、他の列車の進路と交錯していないことをチェックした上で信号機に進行信号を表示させる。

（2）進行信号が現示されている間は、オペレータが誤った操作をしても進路上の転轍器は転換しない。

（2）のように信号機やその他の機器、列車の状態によって転轍器を転換できないようにすることを鎖錠と呼び、鎖錠を解くことを解錠と呼ぶ。このように信号機と転轍器を関係づけて動作させることにより、オペレータの負担を減らし、またオペレータが誤った操作をしても危険な状態に陥らないようにしている。このような機能を連動と呼び、オペレータの操作に従って連動機能を実現するシステムを連動装置と呼ぶ。また連動装置の制御の仕様を連動仕様と呼ぶ。

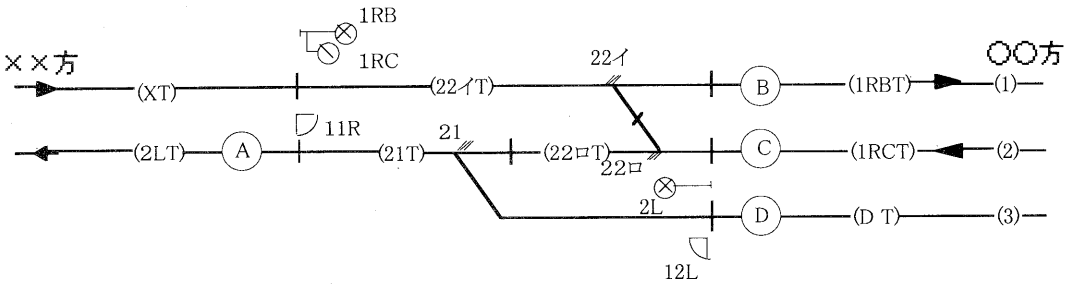
連動装置の働きの具体例は次節で示す。

2．2 連動図表

連動仕様は連動図表と呼ばれる図と表で表わされる。連動図表の例を図1に示す。

連動図は機器及びその配置を表わしている。実線は線路を表わす。線路上の縦線で区切られた各区分には軌道回路が設置され、区分内の列車の有無を検知する。区分内の記号XT、2LT、21Tなどはその区分に設置された軌道回路を表わす（便宜上、軌道回路の記号でその区分を表わすこともある）。1RC、1RD、2Lは信号機に付けられた番号を、各番号傍の記号は信号機の設置場所を表わす。また、11R、12Lは入換標識に付けられた番号を、各番号傍の記号は入換標識の設置場所を表わす。信号機及び入換標識は、列車の進入がないときには、原則として停止信号を現示する。

21イ、21ロ、22は転てつ器に付けられた番号及びその設置場所を表わす。転てつ器は列車の進入がないときは番号傍の毛羽三本の方向に進路を取るよう設定されている。列車の進入がない時に転てつ器が設定されている方向を転てつ器の定位と呼ぶ。また、定位と反対の方向を反位と呼ぶ。第1図では、転てつ器21の定位は21Tと22ロTを結ぶ方向であり、反位は21TとDTを結ぶ方向である。転てつ器22イと22ロは連動しており、両方とも定位か、両方とも反位に設定される。このような転てつ器を2動の転てつ器と呼び、同一の番号に添字を付けることでこれを表わす。2動の転てつ器の場合、2つの転てつ器とも動作・制



名称		番号		鎖錠	信号制御	進路鎖錠	接近鎖錠
場内信号機	XT-1番線	1R	B	22	22イT、1RBT	(22イT)	XT ((90秒))
	XT-2番線		C	22	22イT、22ロT,1RCT	(22イT)(22ロT)	
場内信号機	2番線-2LT	2L	A	22、21 11RC	22ロT,21T,2LT	(22ロT)(21T)	1RDT ((90秒))
入換標識	2LT-2番線	11R	C	21、22 2L		(21T)(22ロT)	2LT ((30秒)
	2LT-3番線		D	21 12L		(21T)	
入換標識	3番線-2LT	12L	A	21 11RD		(21T)	DT ((30秒))

図1 連動図表

御が同じであることから、1つの転てつ器のように取り扱うことがある。この場合、22イと22ロを合わせて22というように、共通の番号のみで呼ぶ。

連動表は各進路ごとに現場機器の連動仕様を記述する。1行目はXTから1番線及び2番線（それぞれ連動図中の(1)及び(2)）に至る進路に関する記述であり、これらの進路はそれぞれ番号欄の信号機1RBと1RCに進行現示を表示させることによって設定される。これらの進路は信号機の記号1RB、1RCで表わす。3行目の入換標識の欄は、1台の入換標識 11Rによって2LTから2番線及び3番線 （連動図中の(3)） へ至る2つの進路を設定することを表わす。便宜上、これらの進路を11RC及び11RDと表わす。鎖錠欄以降は後述する。

次に、図1の連動図を用いて連動装置の働きの具体例を説明する。○○方から2番線（図中の(2)）に列車が進入してくる場合、以下のチェックを行った後、信号機2Lに進行現示を出す。

(1-1) 進路上の転轍器21、22が必要な方向を向き、鎖錠されている。

(1-2) 交錯する進路1RC、11RC、11RD、12Lが設定されていない。

(1-3) 進路上の軌道回路22ロT、21LT、2LTは列車を検知していない。

また、列車の進行に際しては以下のように進路上の転轍器の鎖錠・解錠が行われれる。

(2-1) 列車の進行中は、進路上の区分22ロT、21T内の転轍器は鎖錠されている。

(2-2) 列車運行の能率を上げるため、列車が22ロTを通過すると、22ロT内の転轍器はすぐ

に解錠される。21Tについても同様である。

上の(2-1)(2-2)のように、進路区分内の転轍器を鎖錠・解錠することを、その進路区分を鎖錠・解錠するという。

連動図表の鎖錠欄は例の(1-1)(1-2)に対応し、チェックすべき転轍器と進路が記入される。例えば図1の連動表の3行目の2Lに関する鎖錠欄には転轍器21、22と進路11RCが記入される（転轍器番号をそのまま記入した場合は定位、○囲みで記入した場合は反位を表わす）。ここで2Lと交錯する進路1RCが鎖錠欄に記入されていないが、これは1RCを設定するには転轍器22を2Lの場合とは逆方向に設定し、鎖錠する必要があるので、22の方向をチェックしておけば1RCのチェックは必要ないためである。進路11RD、12Lが記入されていないのも同様の理由による。

信号制御欄は(1-3)に対応し、チェックすべき進路上の軌道回路が記入される。図1の進路2Lの場合は連動表の3行目にあるように22ロT、21LT、2LTが記入される。

進路鎖錠欄は(2-1)(2-2)に対応し、進路上を列車が通過し、解錠される順に進路区分名が記入される。図1の進路2Lの場合は22ロT、21Tの順に記入される。接近鎖錠欄については本稿では説明を省略する。

連動図表については文献[7,8]に詳しい。

2．3 連動装置の種類

連動装置には、継電連動装置と電子連動装置の2種類がある。

継電連動装置は、リレー回路によって構成されている。継電連動装置のリレー回路に関しては標準結線が定められており[7]、連動仕様を構成する各パターンごとにリレー回路の標準的な構成が定めれらている。

電子連動装置はマイクロコンピュータ制御によるもので、日本では1985年にはじめて導入された。電子連動装置の連動機能の構成法は、細部に違いがあるものの、大筋では継電連動装置の構成を引き継いでおり、その標準結線をプログラム化したものである。

3．モデル検査法を用いた連動仕様の形式的検証

3．1 形式的検証

鉄道システムのように、事故や障害が重大な被害を生む恐れを持つシステムでは、要求された機能をいかに正確に実現するかが重要な課題となる。しかしながら、システムの大規模複雑化に伴い、システムの安全性・信頼性を保証することはますます困難になりつつある。

この問題に対する一つの答えとして、形式的検証が注目されつつある。形式的検証は、システムが仕様通りに動作するかどうかを数学的方法を用いて保証する技術で、システムの安全性や信頼性を高い精度で保証するものとして期待されている。

形式的検証は古くから研究されてきたが、検証のために膨大な計算時間を必要とすることから、長年実用性のない研究とみなされてきた。しかし、計算機の処理能力の向上とそれに伴う検証の効率化技術の発達により、近年では実用化技術として盛んに研究されている。

鉄道システムの分野でも、鉄道総研が事務局となり安全性技術に豊富な経験を持つ専門家の参加によって1996年に作成されたガイドライン「列車運転制御システムの安全性技術指針」の中で、事前安全性解析のための技術として形式的手法が推奨されている[6]。特に、連動仕様の設計については比較的小規模の駅でも非常に複雑なものとなるが、現在その設計・試験はすべて人手で行われており、そのコストは膨大なものとなっている。このため、この分野では特に形式的手法への期待が大きく、実際、形式的仕様記述や検証についていくつかの試みがなされている[1,4,5]。本研究では、連動図表で表わされた連動仕様の形式的検証を試みる。

3．2 モデル検査法

本研究では、モデル検査法と呼ばれる形式的検証法を用いる。モデル検査法は論理回路

検証の分野で成功を納め、他分野でも注目を集めている形式的検証法である[2,7]。

モデル検査法は、仕様記述言語として時相論理の一種であるＣＴＬ（Computation Tree Logic)を用いる。ＣＴＬ式の意味は、Kripke構造と呼ばれる有向グラフ上で定義される。Kripke構造は有限状態機械のモデルと考えられるので、検証するシステムを有限状態機械で記述し、ＣＴＬ式で記述した性質がこの有限状態機械上で成り立つかどうかを証明することにより、システムがこの性質を満たすかどうかを検証することができる。

3.2.1 時相論理ＣＴＬ

ＣＴＬは、通常の命題論理の命題演算子 +(論理和)、&(論理積)、!(論理否定)、→(含意）などに加え、時相演算子を持つ。時相演算子は、Ａ（全称記号）及びＥ（存在記号）と、時間に関する性質を表わす演算子Ｘ（next)、Ｆ(Future)、Ｇ(Global)、Ｕ(Until)を組み合わせて用いる。時相演算子の直観的な意味は以下の通りである。

ＥＸｐ(ＡＸｐ)：現状態から遷移できるある（すべての）状態でｐが成立する。

ＥＧｐ(ＡＧｐ)：現状態からのある（すべての）遷移系列において常にｐが成立する。

ＥＦｐ(ＡＦｐ)：現状態からのある（すべての）遷移系列においていつかｐが成立する。

Ｅ[ｐＵｑ](Ａ[ｐＵｑ])：現状態からのある（すべての）遷移系列において、いつかｑが成立し、かつ最初にｑが成立するまではｐが成立し続ける。

3.2.2 ＣＴＬのモデル検査

与えられたＣＴＬ式が有限状態機械Ｋ上のすべての初期状態で成り立つかどうかを判定することをモデル検査と呼ぶ。モデル検査法の詳細は文献[2,7]を参照されたい。本稿では、例として、有限状態機械Ｋ上でＥＧｐの形の命題が成り立つかを検査するアルゴリズムを示す。

(1) ｐが成り立つすべての状態の集合をＴとする。

(2) Ｐが成り立ち、かつＴに含まれる状態への遷移が少なくとも一つある状態の集合をＵとする。

(3) Ｕ＝Ｔならば(5)へ進む。

(4) Ｔ：＝Ｕとし、(2)へ戻る。

(5) ＴがＫの初期状態を含んでいればＥＧｐが成り立つ。含んでいなければＥＧｐは成り立たない。

ＥＧｐはある状態遷移系列上のすべての状態でｐが成り立つことを要求するので、ｐが成り立つ状態から遷移を逆にたどって常にｐが真となる状態遷移系列を求める。このような遷移系列のうち初期状態から始まるものがあることを(5)で求める。他の形の式も同様に検査する。

実用規模のシステムは状態数が非常に大きくなるため、上の検査法をそのまま適用するのは現実的ではない。この問題を解決するために、様々な手法が研究されている[3]。本研究では記号モデル検査法を採用したシステムSMV[7]を用いる。

3．3 連動仕様の検証

連動仕様検証の概要を図２に示す。連動図表で記述した連動仕様と、信号機・転轍器・軌道回路などの現場機器や制御盤上の入力機器及び列車のモデルから有限状態機械を構成する。検証項目はＣＴＬ式で記述し、これが有限状態機械上で成り立つかを検証する。検証に失敗した場合、モデル検査法では反例となる状態遷移系列を返すことができるので、これをデバッグのための情報として用いる。

3.3.1 連動仕様の記述

2.3 節で述べたように継電連動装置は連動仕様に対してリレー回路の標準結線が定められており、電子連動装置の場合は一部違いがあるものの、大筋では継電連動装置の構成を引き継いでいる。本研究では連動仕様検証の第一段階として、連動図表を継電連動装置の標準結線に基づいて解釈し、これを有限状態

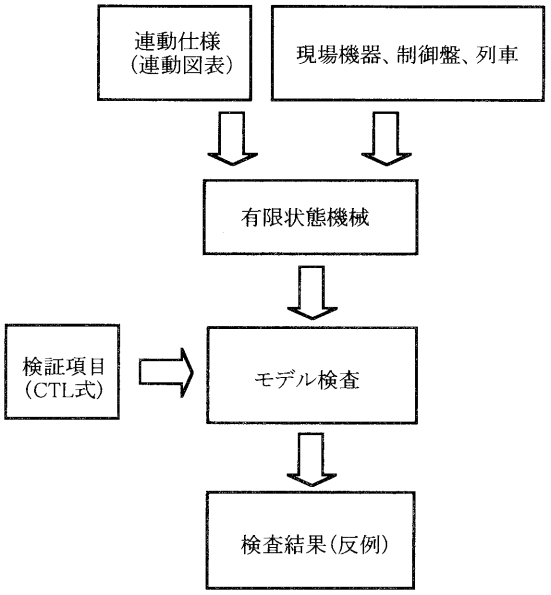


図2 連動仕様の形式的検証

機械によって記述する。

図１の連動図表のうち、進路2Lの進路鎖錠を実現するリレー回路（の一部）を図３に示す。 22ロTLSRは22ロTの進路鎖錠リレーと呼ばれ、このリレーが落下すると22ロT が鎖錠されるように構成されている。進路鎖錠リレーは一つの進路区分に対して右行進路用（TRSR）と左行進路用（TLSR）の二つが設けられる。22ロTLSRは左行進路用であり、進路2Lの設定・確保のために用いられる。 2LASRは制御盤から2Lの進路設定要求がなされた時、転轍器の方向など一定の条件が満たされていると落下し、進路解除要求がなされると動作する。 22ロTRは列車が22ロTにあるときは落下し、列車がないときは動作する。この回路によると、2Lの進路を設定するとまず 2LASRが落下するので、それによって22ロTLSRも落下し、22ロTが鎖錠される。 進路2Lを解除すると2LASRが動作するが、このとき列車が 22ロTに進入していると 22ロTRが落下しているので22ロTLSRは動作しない。 列車が22ロTを通過すると22ロTRが動作するので22ロTLSRも動作し、22ロTが解錠される。 ここで22ロTRと並行に22ロTLSRが挿入され、自己保持接点として構成されているが、これは 1RCが設定されて逆方向から列車が 22ロTに進入してきたときに22ロTLSRを落下させないようにするためである。

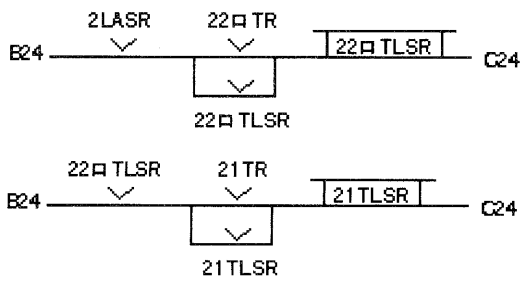


図3 進路鎖錠リレー

21TLSRは21Tの左行進路鎖錠リレーであり、22ロTLSRと同様に構成されているが、 2LASRの替わりに22ロTLSRの接点を挿入することにより、列車が22ロTを通過後さらに21Tを通過してからこの区分が解錠されるようにしている。

図３のリレー回路図から構成した有限状態機械を図４に示す。概ねリレーの自己保持接点の状態が有限状態機械の状態に、挿入され

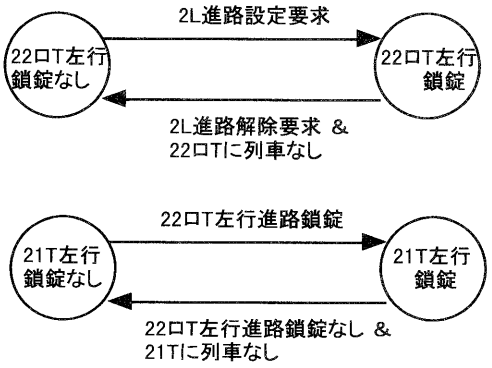


図4 進路鎖錠のモデル

たリレーの接点が状態遷移条件に対応する。（図４中の状態遷移条件は実際にはもう少し複雑になる。）連動仕様の全体は、これらの要素有限状態機械の積で表わされる。

3.3.2 現場機器のモデル化

連動仕様に加えて信号機、転轍器、軌道回路などの現場機器や制御盤上の入力装置及び列車の動作を有限状態機械でモデル化する。

転轍器の有限状態機械による記述を図５に示す。転轍器は定位・反位・転換中の３状態をとり、転轍制御リレーによってその転換方向が制御される。ここでは「転換中」の状態を転轍制御リレーの状態と関連付け、「定位→反位転換中」と「反位→定位転換中」の２つの状態に分ける。状態遷移条件は連動仕様に応じて個々の転轍器ごとに具体化される。転轍器の鎖錠については状態遷移条件が成り立たないことによって表現する。

信号機や軌道回路も転轍器と同様にモデル化する。

制御盤上の入力装置は、進路設定・解除要求を行うもの（信号てこと呼ばれる）と、転轍器の転換要求・鎖錠指令を行うもの（転轍てこと呼ばれる）がある。信号てこは、任意のタイミングでON/OFFされるスイッチの形でモデル化する。転轍てこも同様にモデル化できるが、こちらは通常の列車運行時には操作しないので、本研究では採用しない。

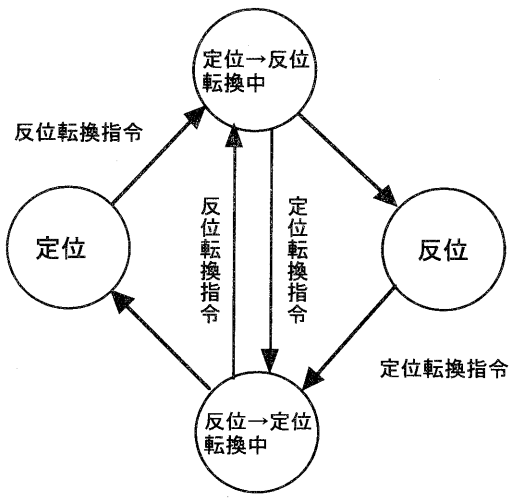


図5 転轍器のモデル

列車のモデルはその位置する進路区分を状態とする。信号機の表示に従う必要のある状態では、信号機が停止現示を出している場合はその状態に留まり（停車を表わす）、進行現示を出している場合は次の進路区分を表わす状態へ遷移可能（進行を表わす）とする。列車の速度は任意とし、進行する場合の状態遷移は非決定的に行われる。

3.3.3 検証項目

連動仕様の検証において、実際にどのような検証項目を設定すれば良いかについては議論の余地が残されている。本稿では、現時点で考えられるいくつかの例についてＣＴＬ式による検証項目の記述例を示す。

例１：進路設定

図１の連動図表で、信号機2Lが進行現示を出したとき、転轍器21及び22が定位に設定されていることを表わす検証項目は以下のように記述できる。

```
AG (s-2L.state=shinkou_genji ->
      t-21.dir=teii & t-22.dir=teii)
```

例２：列車走行中の転轍器転換禁止

列車が進路区分21Tにあるとき、転轍器21の転換が行われないことを表わす検証項目は以下のように記述できる。

```
AG ((train1.position=21T & t-21.dir=teii
      -> AX t-21.dir=teii )
   & (train1.position=21T & t-21.dir=hani
      -> AX t-21.dir=hani ))
```

例３：列車の衝突回避

連動装置は、同じ進路区分に複数の列車を同時に進入させないことにより、列車が衝突を防止している。従って、列車が衝突を起こさないことを表わす検証項目は、次のように記述できる。

AG !(train1,position=train2.position)

4．実験

前節までに述べた連動仕様のモデル化及び検証項目の記述法に基づき、 DOS/Vパソコン(PentiumⅡ 266MHz、Linux) 上で検証実験を行った。検証器はSMV Version2.5.3を使用した。実験の結果、３進路以下の連動仕様ならば１検証項目あたりの検証時間は最大数秒、メモリ消費量は２MB以下、到達可能状態数は最大１３万弱であった。また、６進路の連動仕様では、１検証項目あたりの検証時間は最大11分強、メモリ消費量は最大14MB程度、到達可能状態数は概して１０の７～８乗程度であった。

モデル検査法では問題の規模が大きくなるにつれて検証時間及びメモリ消費量が急激に増大する傾向があり、また、現場機器や列車のモデル化法についてはまだ議論の余地が残されているので、実験結果の評価には予断を許さない面がある。しかしながら、実験結果はかなり複雑の仕様を検証できることを示しており、実用規模の駅の検証へ期待が持てると考えられる。

5．おわりに

鉄道信号システムのように安全性が非常に重視される分野では、形式的手法の重要性は今後ますます増していくと考えられる。本研究ではモデル検査法を用いた連動仕様の形式的検証を試みた。今後の課題としては以下のものがあげられる。

(1) 検証できる駅の規模の限界を探り、実用規模の駅に形式的検証を適用する方法を検討する。

(2) 本稿では例としていくつかの検証項目を挙げたが、実用的にどのような検証項目が必要かを調査･検討する。

(3) 本研究では継電連動装置の標準結線に基づいた検証を行ったが、今後新規に設計されるのは電子連動装置がほとんどである。電子連動装置の連動機能は継電連動装置のものを引き継いではいるが、電子連動装置特有の機能もあるため、これらを検証の際のモデル化に反映していく必要がある。

(4) 本稿では触れなかったが、連動仕様には実時間的制約を持つ部分がある。このような仕様を検証する方法を検討する。

(5) 検証と合わせて連動図表作成やソフトウェア生成も含めたツール化を行い、連動装置の設計開発の総合的な支援を行う。

参考文献

[1] Bernardeschi,C.,Fantechi,A.,Gnesi,S.,Larosa,S.,Mongardi,G.and Romano,D.:A Formal Verification Environment for Railway Signaling System Design,Formal Method in System Design, Vol.12,pp.139-161,1998.

[2] Burch,J.R.,Clarke,E.M., McMillan,K.L. and Dill,D.L.: Sequential Circuit Verification Using Symbolic Model Checking, in Proc.of 27th Design Automation Conference pp.46-51, 1990.

[3] Clarke,E.M.,Wing,J.M. et al.:Formal Methods:state of the Art and Future Directions, ACM Computing Surveys, Vol.28, No.4, pp.626-643, 1996.

[4] 福岡、福田：ペトリネットによる連動仕様の検証、鉄道総研報告Vol.9,No.11,1995.

[5] 平尾、福田：鉄道信号におけるソフトウェア安全性技術、日本鉄道技術協会 Vol.41, No.5, 1998.

[6] 平尾、渡辺：列車保安制御システムの安全性技術指針、鉄道総研報告 Vol.10, No.11, 1996.

[7] McMillan,K.: Symbolic Model Checking, Kluwer Academic Publishers, 1993.

[8](社)信号保安協会：継電連動装置標準結線図、1976.

[9](社)日本鉄道電気技術協会編：信号入門、1988.

[10](社)日本鉄道電気技術協会編：連動装置 鉄道技術者のための電気概論 信号シリーズ５、1993.