形式的手法による鉄道保安システムの信頼性向上

○堅田　悠也（日本大学）　　［電］謝 国（日本大学）

［電］中村 英夫（日本大学）　　［電］黒田 智也（日本大学）

Reliability improvement of railway security system by formal method

○Yuya Katada, (Nihon University)　Xie Guo, (Nihon University)

Hideo Nakamura, (Nihon University)　Tomoya Kuroda, (Nihon University)

This paper describes the improvement reliability of Automatic Train Protection and Block (ATPB) railway System developed for the purpose of reproduction of a local railway. This system is a new security system which used general-purpose wireless communications. Although the reliability technology currently used there does not have progress as at before. Then, we describe the specification of the system as an abstract and strict model using VDM (Vienna Development Method) which is a kind of formal method.

キーワード：ATPB システム，VDM++
Key Words：ATPB system, VDM++

1．はじめに

沿線周辺の人口低下や、自動車との競争の影響により、地方鉄道の生存環境はますます厳しくなっている。そのため、競争力を改善し、地方鉄道を再生することを目的として、ATPB(Automatic Train Protection and Block)システムが提案されている。

このシステムの大きな特徴は汎用無線通信による列車の保守であり、わずかな軌道上設備を増設することでその後の設備の保守・点検並びに設備交換のコストを大きく抑えられるという利点がある。

本研究では ATPB システムについて正確な記述を行い、仕様の正確さおよび充足性を保証することを目的とし、そのためにまず形式的手法を用いた仕様記述を行うことで正確な仕様作成とその検証を行った。

2．ATPB システム

ATPB システムの概念図を図 1 に示す[1]。GPS による位置検知や携帯無線電話等の汎用技術が、鉄道信号に応用可能な状況となった ATPB は、これらの汎用技術、汎用インフラを利用することにより、軌道沿線設備を削減することができる。それと共に、情報技術に依拠することで機能性及び安全性に優れた列車制御システムを経済的に提供することが目的となる。

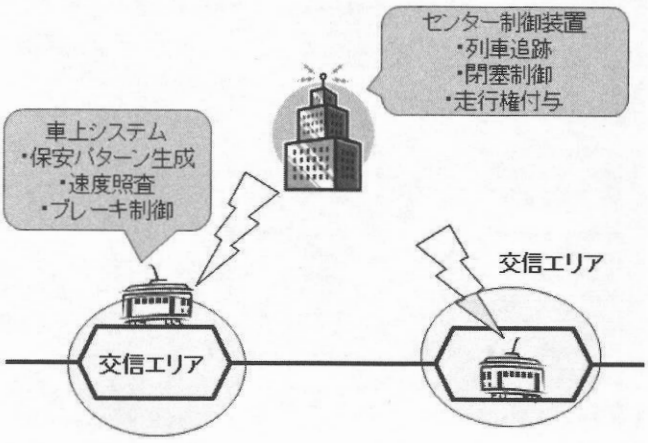

図 1　ATPB システムの概念

地方鉄道への導入を目的とした ATPB システムは、センター制御による閉塞制御と、閉塞された区間における車上での保安制御を基本とする。

車上での保安制御は、車内信号に基づき、車上に搭載した線路データから保安パターンを生成し、その下で運転するというパターン式速度照査によって行われる。

駅間運転方向の制御はセンター制御装置が行ない、また

制御装置は列車ダイヤに基づいて駅構内の進路を制御する。各駅の連動制御は、集中連動方式とし、連動装置と駅構内の制御端末との間は汎用無線電話回線を介して接続する。

車上保安装置とセンター制御装置間は汎用無線回線により、必要な箇所で接続され、車両の在線位置と車内信号に対応する信号情報を交換する。

3．形式的手法による仕様記述

3.1 形式的手法

形式的手法とはソフトウェア開発手法の一つである。この手法では、従来まで自然言語で記述していた仕様を形式仕様記述言語により記述する。形式仕様記述言語は、仕様を論理式的に記述するため、自然言語のような曖昧さが排除され、無矛盾性が保証できる [2]。

また、形式仕様記述言語で書いた仕様は、開発対象となるシステムのモデルとなるため、それを検証することで実際のシステムを作る前に仕様に内在する欠陥を見つけ出せる。これにより、システム開発段階でエラーが起こってしまうことを未然に防げるため、特に信頼性を求められるような開発などでは有効な手法である。

本研究では、形式的手法の一種である VDM(Vienna Development Method)を用いて ATPB システムの仕様を記述し、ツールによる検査を行った。

3.2 仕様記述

VDM++では、システム内の一つの機能につき一つのクラスで記述する。また、図 2 に実際に VDM++で記述した仕様の一例を示す。

```
class Speedcompaer

types
  public Speedstate = <normal>|<alarm>|<emergency>;

instance variables
  ratio : real;
  inv 0<ratio<1;
  pattern : SpeedGeneration`Pattern;

operations
  public Extractionspeedlimit: Pattern ==> Speed
  Extractionspeedlimit() == is not yet specified;

  public Seekspeedstate:Speed ==> Speedstate
  Seekspeedstate(speed,limitspeed) ==
  if speed < (1-ratio)*limitspeed
  then return <normal>
  else if speed >= (1-ratio)*limitspeed and speed < limitspeed
  then return <alarm>
  else if speed > limitspeed
  then return <emergency>;

end Speedcompaer
```

図 2　VDM++による速度照査機能の仕様

これは ATPB システムの速度照査機能について記述した仕様となっている。速度照査機能では列車の制限速度と現在の列車の走行速度を比較し、それによって normal、alert、emergency の 3 つの速度状態を決定しその値を返すものとなっている。システムではこの状態によって緊急ブレーキなどを自動で作動させる。この 3 つの状態を型定義(types)で、さらに速度の比較を行う実際の処理内容を操作定義(operations)で定義している。

さらに、インスタンス変数定義(instance variables)では 3 つの状態を分ける速度の範囲を決定するための ratio という変数が定義されているが、これには変数の値が 0 より大きく位置より小さい値は取らないという条件が課せられている。これは不変条件というもので、その条件が課せられた場合それが常に満たされるよう仕様の記述を記述することになる。この他に事前条件、事後条件というものを定義することもでき、これらの条件が満たされない場合その仕様自体に矛盾が存在することになる。そのような矛盾を検証することでも仕様の無矛盾性を保証できる [3]。

本研究で作成した仕様では、行数が 533 行、定義した事前・事後・不変条件が合計 25 個で、仕様内で明記されていない内容も追加で定義した。

3.3 ツールによる検証

作成した仕様に対して、ツールを用いた検査を行った。使用したツールは VDM++ToolboxLite、行った検査は型検査と構文検査の 2 種となっている。構文検査では、作成した仕様が VDM++の言語仕様に合致しているかをチェックする。仕様に対して構文検査を行った結果、いくつかエラーを検出した。しかし、そのほとんどが変数名や型名の誤表記、操作名の間違いなど、不注意によるミスだった。これらのエラーを適切な表記で記述しなおすことで解決した。

型検査では、操作を定義したときの入出力の型と、実際呼び出されるときに与えられるパラメータが一致するかどうかを自動的に検査する [4]。この検査を行うことで仕様内の矛盾や定義の誤りなどを見つけ出し、修正することができる。検査を行った結果、与える引数の型や、返り値の型が合致しないなどのエラーが検出された。このエラーに対して、型定義を変更する、型変換を行うといった対処を施すことで、問題を解決した。

4．まとめ

本研究では ATP 閉塞システムの仕様の記述を、形式的手法の一つである VDM++により実践した。また、VDMtools を用いて仕様の構文検査、型検査を行うことで、記述の正当性の検証を行った。結果として、曖昧性の排除、無矛盾性の保証された仕様を作成することができた。

今後は仕様の充足性について検討を行うため、仕様のモデル検査や ATPB システムのシミュレータの作成などを検討している。

参　考　文　献

1) 中村英夫：ATP 閉塞システムの検討(その 4)，pp. 1-9, 2010.

2) 佐原伸：形式手法の技術講座，ソフトリサーチセンター，pp.105-107，2008.

3) 寺田夏樹：段階的詳細化に基づく鉄道信号へのフォーマルメソッド適用法，電子情報通信学会技術研究報告，2008.

4) 張暁晶：形式仕様言語 VDM++による非接触型 IC カードの仕様記述に関する研究，九州大学工学部電気情報工学科平成 17 年度卒業論文，pp.75-81，2005.