G-20

形式的手法を用いた ATP 閉塞システムの仕様の信頼性向上

Reliability improvement of specification of the ATP confinement system using formal method

○黒田智也[1], 謝国[2], 中村英夫[3], 高橋聖[3]
*Tomoya Kuroda[1], Xie Guo[2], Hideo Nakamura[3], Sei Takahasi[3]

Abstract: The local railway is forced to the driving at the low speed under poor train control system and orbit facilities, and there are even the facilities in the situation having difficulty with maintenance more now. Then, Automatic Train Protection and Block System that doesn`t depend on ground equipment and can perform security control by radio telegraphy of Autonomous vehicles and center is proposed. but the reliability securing at the specification process is not done in this system. So we aim at the reliability improvement from the specification process of Automatic Train Protection and Block System by specification description using formal method.

1.　はじめに

現在，地方鉄道は貧弱な列車制御システムや軌道設備のもとで，低速での運転を強いられ，さらにその設備すらも維持が困難な状況にある．そこで，地方鉄道の再生と機能性に優れた新しい列車制御システムの開発を目的として ATP 閉塞システム(Automatic Train Protection and Block System)が検討されている．しかし，このシステムの仕様段階からの信頼性の検討というものはあまり行われていない．

信頼性の高い仕様の記述方式として,形式的手法というものがある．形式的手法はシステム開発において「仕様の曖昧さをなくす」,「設計のミスを防ぐ」,「実装の間違いを見つけ出す」といった利点があることから，鉄道や航空，原子力発電など重要インフラ等における制御システムの開発において高信頼性のある仕様作成に有効な技術である．

そこで，本研究ではこの ATP 閉塞システムの仕様を，VDM++を用いた形式的手法による記述・検証を行い、システムの信頼性向上について検討する．

2.　ATP 閉塞システムの基本概念

ATP 閉塞システムの概念図を Figure1 に示す．

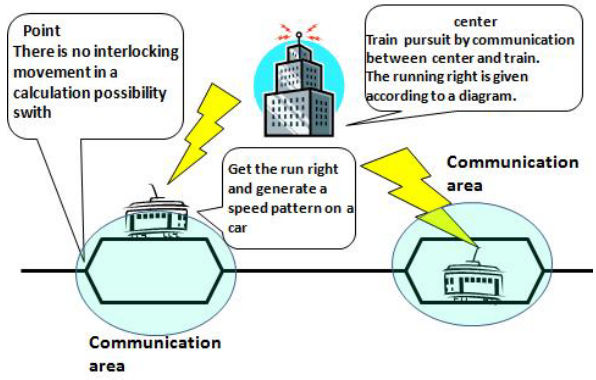

Figure1.Concept of Automatic Train Protection and Block System

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 ATP 閉塞システムは，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．

地方鉄道への導入を目的とした ATP 閉塞システムは，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，その下で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．

3.　ATP 閉塞システムの仕様記述

〈4･1〉車上位置検知機能の仕様

今回は車上位置検知機能の仕様を例に，ATP 閉塞システムの仕様記述について説明する．

ATP 閉塞システムの車上位置検知は，GPS から得られた絶対位置情報と，速度発電機のパルス数演算などから得られた相対走行距離情報を組み合わせて算出される．絶対位置情報は，2 つの GPS 受信機から位置検知検定を行う．

また，最も正しいと思われる列車位置(最尤列車位置)の先頭部と後尾部に滑走や空転による誤差を反映させる．この最尤列車位置と前後の誤差情報を車上保安制御機能とのインターフェースとする．なお，誤差情報は絶対位置取得時にリセットされる．

〈4･2〉車上位置検知機能の記述

上で述べた仕様をもとに形式的手法で記述を行った．なお，今回用いた形式仕様記述言語は VDM++と呼ばれるものである．VDM++はオブジェクト指向型に拡張された仕様記述言語となっており，システムの仕様は複数のクラスによって構成

1: 日大理工・学部・子情　2: 日大理工・院・情報　3: 日大理工・教員・子情

される．このクラスは主にひとつの機能に対してひとつ設けられ，クラス内で機能の状態や操作などが記述される．それぞれのクラスは次のような構成で記述される．

class クラス名
types 型定義
values 定数定義
instance variable インスタンス変数定義
function 関数定義
operation 操作定義
end クラス名

以下にそのソースコードを示す．なお，今回の仕様は陰仕様モデルとなっている．陰仕様モデルでは，仕様内で明確な値や操作の詳細な定義は行わず，操作や状態の条件や入出力など，機能の「満たすべき性質」を明確化させる．今回の仕様では入力と出力の定義のみを行うことでその操作に対する要求を表現し，機能がどうなっているべきかを明確にしている．

```
1   class PositionDetect
2   types
3     public Position = real;
4     public Head_Error = real
5     public Tail_Error = real;
6   instance variables
7     public position:Position;
8     public head_error:Head_Error
9     public tail_error:Tail_Error
10  operations
11  public position_detect : real* real * real ==> Position
12  position_detect(gps1,gps2,distance)== is not yet specified;
13  public head_error_detect : real ==> Head_Error
14    head_error_detect(p1) == is not yet specified
15  pre   Head_Error = 0;
16  public tail_error_detect : real ==> Tail_Error
17    tail_error_detect(p1) == is not yet specified
18  pre   Tail_Error = 0;
19  end PositionDetect
```

まず，1 行目では車上位置検知を行うクラスとして PositionDetect クラスのクラス名を定義している．2~5 行目では型の定義を行っている．型では、そのクラスを構成する要素，つまりはその機能を構成する要素を記述する．このクラスでは位置情報を Position 型として定義している．また，誤差情報を先頭誤差と後尾誤差とをそれぞれ Head_Error 型と Tail_Error 型として定義する．

6~9 行目はこのクラスが保持すべきインスタンス変数の定義を行っている．インスタンス変数はそのクラスの属性を表す変数である． position は列車の絶対位置、head_error は先頭誤差，tail_error は後尾誤差を表す変数である．

10 行目以降では操作の定義を行っている．操作定義ではその機能がどんな処理を行うのかを記述する．position_detect は GPS から得た位置情報と速度発電機等から得た積算距離から絶対位置を求める操作である． head_error_detect と tail_error_detect はそれぞれ先頭誤差と後尾誤差を求める操作となっている．

また，head_error_detect、tail_error_detect にはそれぞれ 15 行目，18 行目の pre 以降で事前条件が設定されている．事前条件とは，操作が行われる前に入力となる対象が取るべき条件である．今回の操作では，誤差情報は初期状態では 0 であるべきであり，絶対位置情報を取得したときにリセットされるという仕様であるため，処理を行う前には誤差情報が 0 であるという事前条件を設定した．この他にも，操作定義では処理が行われた後，出力が満たすべき条件である事後条件の定義も行うことができる．

4.　おわりに

今回，本稿では ATP 閉塞システムの信頼性向上のため，形式的手法の一つ VDM++ によるシステムの仕様記述について，そして ATP 閉塞システムの機能を形式的に表現する方法について述べた．また，車上位置検知機能を例に実際に記述した仕様を示した．

今回作成した仕様では，位置検知機能が処理を行う中で，どんな要素を用いて，その結果どんな要素を出力するのかということを論理的に記述することができた．さらに，誤差検知の処理では誤差情報が初期状態ではどうあるべきかということまで記述することができた．

今後は，ATP 閉塞システムを構成する他の機能についてもまず陰仕様モデルでの記述を行っていく．その後，仕様内の操作や状態について，具体的に記述すべき部分を明確化させ，実行可能なものとした陽仕様モデルの記述を行なう．そして，ツールを用いた構文検査や型検査を行ない仕様の正当性の検証を行う．

5.　参考文献

[1]　中村　英夫 :「ATP 閉塞システムの検討(その 4)」，2010

[2]　佐原　伸 :「形式手法の技術講座」,ソフトウェア・リサーチセンター ，2008

[3]　張　暁晶 :「形式仕様言語 VDM++による非接触型 IC カードの使用記述に関する研究」, 九州大学工学部電気情報工学科　平成 17 年度　卒業論文

[4]　荒木　啓二郎 :「プログラム仕様記述論」、オーム社、平成 14 年

[5]　中村　英夫 :「ATP 閉塞システムの提案」、2010