6J－2

代数仕様言語 CafeOBJ における高信頼システムの記述に関する一考察*

- 鉄道信号システムの形式仕様とその検証 -

清野 貴博† 二木 厚吉†

北陸先端科学技術大学院大学 情報科学研究科

1 はじめに

コンピュータシステムに占めるソフトウェアの役割が大きくなるにつれて、ソフトウェア開発の困難さが増大する反面、高い信頼性を備えるソフトウェアを求める声も大きくなってきている。この問題を解決するため、大規模集積回路と同様に、ソフトウェアの設計にも数学的背景を持つ形式手法が導入され、それらは信頼性の向上に貢献している。

機械を操作する上における人の動作も、広義のソフトウェアといえるが、その多くはプログラム的な手続きとして捉えることが可能であり、形式化することができると考えられる。このような観点から、本稿では、特に高い信頼性が要求されているシステムの一例として、鉄道の信号システムを取り上げる。信号システムは、単に信号機という機械だけではなく、運転士の信号見落としなどによる事故を防止するための自動列車停止装置 (ATS: Automatic Train Stop Device) や、信号機故障時の運転士の対応に関する規則など、人と機械が相互にバックアップし合うシステムである。このようなシステムを構成する人や機械の間の整合性を検証することは、鉄道の例だけに限らず、高い信頼性が必要なシステムの構築に有効であると考えられる。

2 鉄道の信号システム

鉄道の安全を守るには、列車の間の距離を常に一定以上に保つ空間間隔法と、列車を一定時間以上空けて運行する時間間隔法の二つがあるが、多くの鉄道は空間間隔法を採用している。

最も一般的な空間間隔法の実現方法は、閉そくの概念を導入することである。この概念では、線路をいくつかの閉そく区間に分割し、一つの閉そく区間には、常に高々一つの列車だけしか存在できないようにシステムを維持する。各閉そく区間が線路上の定位置にある固定閉そくが古くから使われているが、列車の移動に伴って閉そく区間が移動する移動閉そくという方法もある。現在の所、多くは固定閉そくを用いているので、以下では固定閉そくについて議論する。

閉そく区間に高々一つの列車しか存在できないようにシステムを維持するには、列車が前方の閉そく区間に他の列車が存在するのか否かを知る手段を設け、もし列車が存在するならば、その区間の手前で停止するように制御すればよい。そこで、閉そく区間の入り口に、その区間に列車がいるのかどうかを現示する信号機を設置する。これは自動信号機と呼ばれ、信号機はその防護区間に列車がいれば停止信号を、そうでなければ進行信号を現示する。ただし、閉そく区間が短い場合、停止信号を見た列車は減速が間に合わず停止できないかもしれない。そこで、次の信号が停止信号であることを予告する注意信号などを現示し、段階的に減速させる三～五位式信号機が一般的に使われている。

ATS は機械による運転士のバックアップシステムで、列車が停止信号手前に差し掛かり、なお運転士が列車を止める手配をしない時に、非常ブレーキをかけ、列車を強制停止させる装置である。

また故障等で信号機が消灯していた場合、「消灯している信号は停止信号とみなす」という規則により、運転士が信号をバックアップする。この規則は夜間であっても適用され、そのために運転士は自らが担当す

*Formal Specification in CafeOBJ of Railway Signal System and its Verification

†Takahiro Seino, Kokichi Futatsugi
Japan Advanced Institute of Science and Technology
School of Information Science

る路線の信号機の位置をすべて諳んじている。

3 CafeOBJ による記述

前節で述べた固定閉そくによる信号システムを代数仕様言語 CafeOBJ を用い、記述した。その際、CafeOBJ の隠蔽代数モデルに基づき、列車と閉そく区間をオブジェクトとして記述し、それらを合成することによって鉄道システムを表現した。記述した仕様について詳細に議論することが望ましいが、紙面の都合上、特に本稿において重視している、人と機械が相互にバックアップし合う部分の仕様を以下に示す。

閉そく区間は SectionID によって識別され、区間に列車が入った (in-train) ことと、区間から列車が出た (out-train) の二つの操作によってその状態が遷移する。オブジェクトの状態は属性 is-exist によって知ることができる。

次に、列車は TrainID によって識別され、自らが現在占有している閉そく区間の SectionID を知っている。これは属性 where によって知ることができる。

閉そく区間と列車のオブジェクトから合成したシステムでは、属性 watch によって任意の閉そくの信号機の状態を知ることができる。信号機の状態は以下の等式によって決定される。

```
pr (SECTION + TRAIN)
*[ Railway ]*
var R : Railway
var T : TrainID
var S : SectionID
bop watch  : SectionID Railway -> Signal
ceq watch S R = <R>
    if is-exist (section S R) == true .
ceq watch S R = <G>
    if is-exist (section S R) == false .
```

さらに、このシステムでは操作 move によって任意の列車を前方の閉そくへ移動させることができる。操作 move は移動元の閉そく区間に対する out-train と、移動先の閉そく区間に対する in-train に分解される。ただし、進もうとする閉そく区間の信号機は進行信号が現示されていなければならない。また、たとえ前方の閉そく区間に電車がいなくとも、信号機が消灯している場合、列車は進むことはできない。

```
bop move : TrainID Railway -> Railway
ceq move T R = out-train T
  (where (train T R)) (in-train T
  (next (where (train T R))) R)
  -- Human judgement.
  if  watch (next (...)) R == <G> .
  -- ATS judgement.
  and is-exist (next (...)) == false .
ceq move T R = R
  -- Human judgement.
  if watch (next (...)) R == <R>
  -- ATS judgement.
  or watch (next (...)) R == <X>
  or is-exist (next (...)) == true .
```

この仕様について、典型的な場合を想定し、数多くのテストを行った。期待通りの動作であることを確認した。さらにこの仕様を用い、あらゆる場合において、鉄道の安全性が保たれていることを証明することができる。

4 結論

本稿では、人と機械が相互にバックアップし合うようなシステムを形式仕様として記述し、その動作を確認した。鉄道に限らず、その全てを機械化することが困難なシステムは数限りなく存在する。そのようなシステムにおいて、特に信頼性に関わる部分だけを機械化し、人の作業と調和させる場合にも、形式手法が有効であると期待される。

今後はさらに人と機械の協調が増えていくし、滅多に壊れない機械が壊れたときに、不慣れな人力でシステムを維持しなければならないという状況も発生する。そのような時の拠り所である、人のための作業マニュアルの設計にも形式手法は役立つということも、最後に付け加えておく。

参考文献

[1] Răzvan Diaconescu, Kokichi Futatsugi, "CafeOBJ Report", World Scientific, 1998.

[2] Shusaku Iida, Michihiro Matsumoto, Răzvan Diaconescu, Kokichi Futatsugi, Dorel Lucanu, "Concurrent Object Composition in CafeOBJ", JAIST Research Report, IS-RR-98-0009S, 1998.

[3] 鉄道技術研究会 編, "信号及び線路", 第 4 版, 交友社, 1992.

[4] 曽根 悟, "信号と運転保安の考え方", 鉄道ピクトリアル, Vol.48, No. 7, July, 1998, pp.10-27.