信号保安装置向けソフトウェアの生産性向上についての研究

A Research for Improving of Productivity on Safety Related Software

東日本旅客鉄道株式会社　JR東日本研究開発センター　先端鉄道システム開発センター　上席研究員
国藤　隆

1. はじめに

信号システムは、安全・安定輸送を支える重要な基盤であり、その安全確保の考え方はフェールセーフを原則としています。従来のシステムは、単体でフェールセーフ性を有する信号リレーを用いた電気回路を主体として構成されてきました。しかしながら、その規模が大きくなると、リレーの数、配線の量が莫大となり、ヒューマンエラーを作りこみやすくなる、設計・施工に手間がかかるといった課題が存在しています。一方、1980年代半ばにコンピュータ制御システムにおけるフェールセーフ技術が確立されて以降、電子連動装置等、様々な信号システムの電子化が進展しました。これにより、複雑な電気回路がソフトウェアに置き換えられ、機能の標準化、配線の削減が実現されたことからヒューマンエラーが低減され、安全性、及び安定性の向上、さらには施工性の向上にも大きく寄与するところとなっています。

一方、電子化の進展により、保安ソフトウェアの生産性向上が新たな課題となっています。信号システムの安全性は、コンピュータのフェールセーフ性だけでなく、保安ソフトウェアの仕様に不備がないこと、バグがないことによって担保されますが、近年、保安ソフトウェアの大規模化・複雑化が進展し、その開発に莫大な工数を要するようになってきました。このことが、信号システムのコストを押し上げ、当社管内の信号システムを全面的にコンピュータ制御化するうえでの課題となりつつあることから保安ソフトウェアの生産性向上のための技術革新が急務となっています。

本稿では、信号システムの電子化の流れと、保安ソフトウェアの生産性向上のための技術開発について紹介します。

2. 信号システム電子化の流れ

2.1　電子化の目的

連動装置を例にとって、信号システム電子化の流れを図1に示します。当初、電子化の目的は、安全・安定性の向上でした。その後、ネットワーク技術の発展と高安全な伝送技術の確立により、信号システムの簡素統合化による、設計・施工性の向上が重視されるようになりました。

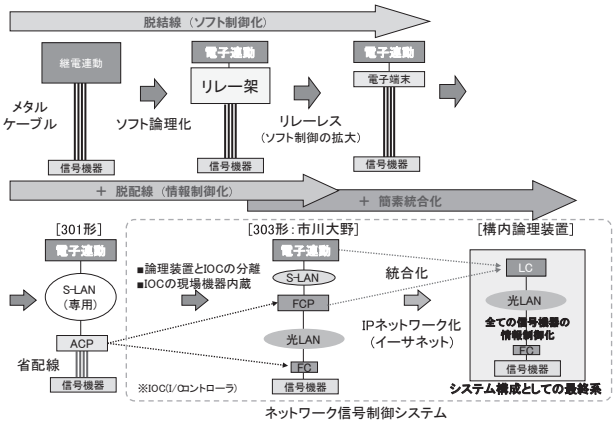

図1　連動装置発展の経緯

2.2　安全・安定性の向上

(1) 継電連動装置の課題

継電連動装置は、日本の鉄道全体でみれば、現在でもなお主流の連動装置です。その理由としては、すべての動作を結線図から読み取ることができ、その機能の安全性・妥当性を確認することが容易であること、また小駅では、ライフサイクルコストが電子連動装置とくらべて割安となることがあげられます。しかしながら、大駅では結線が大規模、かつ複雑となり、結線誤り、施工時の配線ミスなどヒューマンエラーを除去することが難しい、リレーのチャタリング、軌道回路のあおりなどの外乱に起因する誤作動の可能性があるなど、悪質な障害をゼロとすることが難しいという課題があります。また、部品点数が非常に多く、冗長構成も困難であることから、安定性の向上にも限界がありました。

(2) 電子連動化とその発展

電子連動化によって、結線図が不要となり設計段階での誤りが低減されました。また、リレー論理では不可能であった高

度な外乱除去が可能となり誤作動がほぼなくなったことによる安全性の向上、さらには冗長構成が可能となり安定性も向上しました。これらは高度なソフトウェア処理によって実現されています。このようなメリットから、信号システムの電子化は、連動装置以外にも広がっていき、現在も進化を続けています。

2.3 簡素統合化施策

(1) ネットワーク信号制御システム

信号システムの電子化の進展により、リレー結線がソフトウェアに置き換えられ、機器室内の配線作業は軽減されました。しかしながら、機器室から現場信号機器への制御回線は、依然として多芯のメタルケーブルであり、配線作業に多くの労力を必要とする状況に変わりはありませんでした。そのような状況下、2003年の中央線三鷹～立川間連続立体交差化工事において、施工誤りから大きな輸送障害を起こしたことへの対策として機器室の連動装置と現場信号機器とを2重系の光ネットワークで接続し、ケーブル敷設と現場配線の削減による施工性向上を狙った駅構内ネットワーク信号制御システム（構内ネットワーク信号）[1]の開発導入を行いました。構内ネットワーク信号は、2007年に武蔵野線市川大野駅で初号機を使用開始し、その順調な稼働実績を受けて導入の拡大が図られています。また、同様のコンセプトに基づき、駅中間信号設備のネットワーク制御化（駅中間ネットワーク信号）[2]も行われています。

(2) 駅構内論理装置（構内 LC）

信号システムは、連動、ATSなど機能別に装置化されてきたことから、機器室内には装置が乱立し、装置間のIFも多岐にわたっていました。そのため、信号システム全体での信頼性向上が困難でした。そこで、機器室内の論理装置を統合し、現場機器とはネットワークで接続することにより、システム構成の単純化による信頼性向上、システム構成の統一化、機能の統合化による設計・施工性の向上を図った駅構内論理装置が開発されました。現在、本装置は、高崎線桶川駅、及び奥羽本線大曲駅への導入工事が行われ、今後は中・大駅の連動装置の標準となる見込みです。

3. 信号システムにおける今後の研究開発の方向性

3.1 社会経済環境の変化の影響

今後の信号システム開発を方向付けるうえで、少子高齢化の影響を第一に考えると、担い手の減少の側面から、設計・施工に手間がかからないこと、習得する技術が少なく、かつ平易であることが望まれます。これには、構内LC・ネットワーク信号の導入推進が有効と考えられます。一方、収入減少の側面から、システムの老朽取替においては、工事費を現行システムより低く抑え、差額を次期システムの研究開発の原資に充てることが望まれており、開発品のコストダウンを実現するための方策を検討する必要があります。

3.2 コストダウンの考え方

システムを構成するハードウェア、ソフトウェア、それぞれのコストダウンについて、これまで、ハードウェアに関しては、汎用品の活用、装置統合による部品点数削減、連動装置の種別統一による量産化などの施策が実施されてきており、着実に開発費、及び製品価格の低減が行われてきていると考えます。一方、ソフトウェアに関しては、開発工数の適正化に着目した研究は行われてきませんでした。保安ソフトウェアには高い安全性と信頼性とが要求されるため、一般のソフトウェアよりも設計の検証、及び試験に工数がかかることは否定できません。そこで、品質を確保したまま、工数を削減する、すなわち、生産性の向上に事業者とメーカーとが一体で取り組んでいく必要があると考えます。

4. 保安ソフトウェアの生産性向上への取り組み

4.1 保安ソフトウェア開発における課題

ソフトウェア開発のライフサイクルを図2に示します。ソフトウェア開発は一般に、ユーザー要求に基づいて仕様書や設計書を作り、その後にこれらの文書に従ってプログラム作成やシステム統合を行います。このとき、設計どおりにプログラムが書かれているか、仕様どおりの機能を持っているかという評価を「検証（Verification）」と呼び、主にメーカーの工場内試験で実施されます。一方、作られたソフトウェアが大元のユーザー要求を満たしているかに関する評価を「妥当性確認（Validation）」と呼び、主に事業者の手によって、工場内での受取試験、また、現地でのモニターラン試験等によって実施されます。

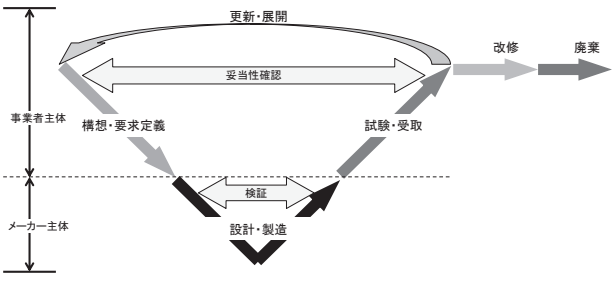

図2 ソフトウェア開発のライフサイクルモデル

ソフトウェア開発の各フェーズにおける、事業者としての課題を以下に示します。

①構想・要求定義フェーズ

このフェーズでは、事業者がシステム構想を策定し、要求仕様書等の文書でメーカーに要求事項を伝えますが、要求仕様書に記載する事柄の正確さ、細かさについては、それを作成する担当者のスキルへの依存度が高いこと、また、要求仕様書に書かれない鉄道信号に関する暗黙知が事業者とメーカーとの間で正確に共有されず、システム構想の意図するところが正確に伝わらないまま工程が進み、最終の受取試験の段階で表面化し、大きな手戻りにつながることがあります。

②試験・受取フェーズ

このフェーズで事業者が実施すべきことは、システム構想で意図したところが正しく実現されているかの確認、すなわちValidationの視点で試験を行うことですが、それには複数列車の同時運行、現場信号機器の動作遅延、あるいはリレーのチャタリング、軌道回路のあおりなどの外乱を加味した試験シナリオを作成する必要があります。これには相当の経験が必要ですが、急速に進む世代交代の中で、技術継承が十分に行われているとは言い難い状況で、ともするとメーカーの工場内試験において、仕様通りに機能するかの確認、すなわちVerificationの視点で試験された項目の追認に陥りがちです。この段階で仕様に潜在する不都合を見逃すことは、現地施工の段階、場合によっては使用開始後に重大な不具合を発生させる要因となります。

③更新フェーズ

信号システムは、制御論理の面では成熟しており、要求仕様を新規に策定するのは、今まで結線でのみ実現されていた機能をソフトウェア化する場合であったり、システム構造の変更であったりで、信号システムの機能全体から見れば、新規に作成が必要な機能の比率は、それほど大きくありません。それにもかかわらず、新しくシステム開発を行う都度、新規に要求仕様書を作成し、メーカーも一からソフトウェア制作を行うため、類似システムの開発を繰り返しても生産性の向上が見られません。

これらの課題を解決し、保安ソフトウェアの生産性向上を実現するために、ライフサイクルの各フェーズで適用可能な手法について2012年度から計画的に研究を行っています（図3）。これらの研究の概要について以下に紹介します。

4.2　構想・要求定義フェーズの改善に関する研究

本フェーズに関しては、要求仕様の精度向上に資する基礎研究、及び仕様の安全性評価技術の基礎研究を行っています。また応用研究として、仕様の安全性評価技術を構

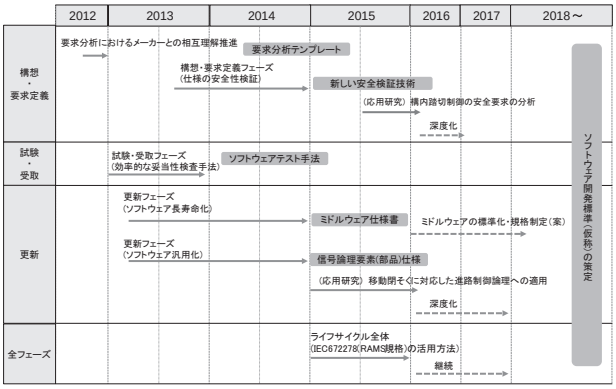

図3　保安ソフトウェア生産性向上の研究ロードマップ

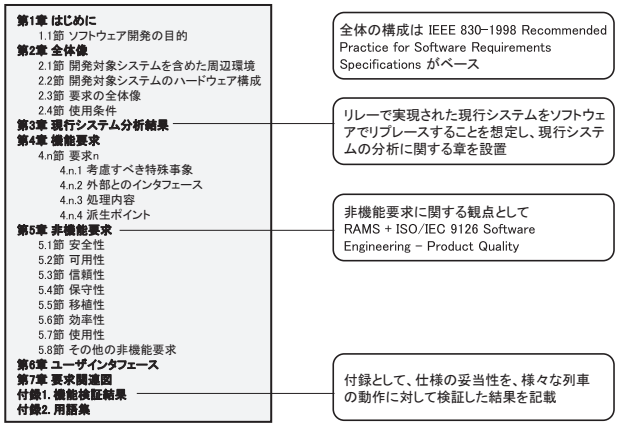

図4　要求分析テンプレートの目次

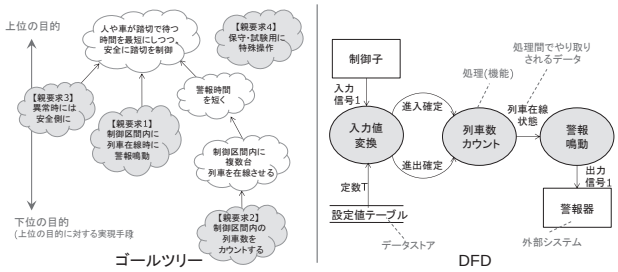

図5　要求及び仕様間の関係の明示手法

内電子踏切の安全性要件の抽出に活用することを2015年度下期から実施する予定です。ここでは要求仕様の精度向上に関する研究について紹介します。

本研究では、要求分析における課題である「仕様定義の漏れ」と「仕様の関連が不明確であること」との2点について、信号システムの特徴である、「安全性・信頼性など非機能的性能が暗黙知として要求される」、「さまざまな列車の動きを想定して仕様を定義する必要がある」こと等をふまえ、要求仕様に記載すべき内容を漏れなく抽出するためのひな型である要求分析テンプレート（図4）、及びその活用手順、また、要求と仕様、要求と要求、仕様と仕様との関連を可視化するための記法（図5）の開発を行いました。

これらツールの活用によって、要求分析作業が定型化さ

れ、業務知識や、経験の多寡によって発生しがちな、仕様の漏れ、仕様理解における担当者間での齟齬の発生を防止することが期待できます。

4.3　試験・受取フェーズの改善に関する研究

本フェーズに関しては、試験精度の向上に関する研究を行っています。信号保安システムは、オペレータの操作、現場機器の状態変化、列車の動きなどを入力として動作する、イベント駆動型のシステムです。従って、そのテストケースは、イベントの順列組合せにより機械的に生成することができますが、膨大な数となり、すべてをテストすることは不可能です。そこで、網羅性を確保しつつ、現実にテスト可能なテストケース数に絞りこむ手法について研究を行っています。現段階の研究成果では、従来の人間が作るチェックリストと比較して、網羅性はおおよそ同程度ですが、テストケース数は数倍程度です。すなわち人間のほうが数倍も効率よくテストケースを作っていると言え、今後さらなる研究が必要です。

4.4　更新フェーズに関する研究

本フェーズに関しては、ハードウェアが更新となっても、同じソフトウェアを使用可能とする「長寿命化」、及び同じソフトウェアを様々なシステムで使用可能とする「汎用化」の2つの観点から再利用の研究を行っています。

(1) 長寿命化

保安ソフトウェアは、安全性を担保するために、ハードウェアの安全機構を利用しますが、その利用手順が機種によって異なるため、機種が変更になるたびにソフトウェアの変更が必要となることが多くありました。しかしながら、安全機構の利用手順を機種によらず共通化しておけば、機種が変更になったとしても保安ソフトウェアを変更する必要はなくなります。そこで、これら安全機構を駆動する標準手順を機構ごとに定義し、それらをオペレーティングシステムからも保安ソフトウェアからも独立したソフトウェア（共通ミドルウェア）として構築する手法について研究を行っています（図6）。

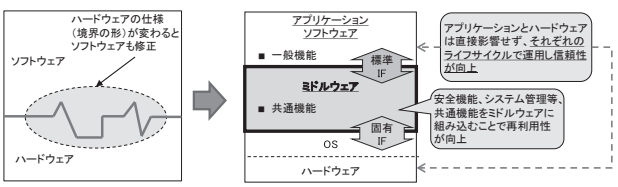

図6　共通ミドルウェアの概念

(2) 汎用化

信号システムは、システム形態が異なっても、鎖錠、信号制御など本質的に実行する機能は同じです。そこで、信号機能を要素機能に分解、部品化しておき、新しいソフトウェアを構築する際に、必要な部品だけを選択して、再利用する考え方です。

現段階では、機能仕様書レベルでの再利用が現実的と考え、要素機能への分割手法、分割された要素機能の仕様記述手法について研究を行っています。機能仕様書レベルでの再利用の場合、機能仕様書に含まれる曖昧さの排除が、再利用時の品質向上に直結するため、準形式手法であるSystems Modeling Language（SysML）※でモデル化し精度向上を図っています（図7）。

※システムエンジニアリング向けモデリング言語であり、システムの仕様記述、分析、設計、検証等が可能

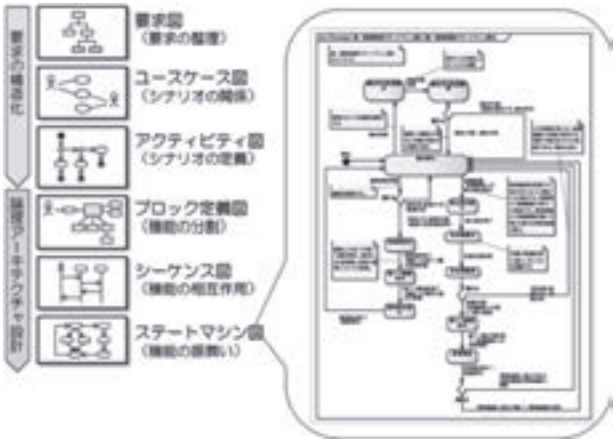

図7　準形式手法SysMLによる機能仕様記述

5. おわりに

本稿では、コンピュータ技術の発展が、信号保安システムの安全性、安定性、及び設計・施工性の向上に大きく寄与してきたことを連動装置の例で示しました。その反面、保安ソフトウェアが大規模化、複雑化し、信号システムの開発費を押し上げる要因となっており、当社管内の信号システムを全面的にコンピュータ制御化するうえでの課題となりつつあることからコストダウンの方策として、保安ソフトウェアの生産性向上への取り組み事例を紹介しました。

今後の課題としては、各手法を深度化及び、開発プロセス全体を通しての品質管理に一貫性を持たせる手法を開発し、ライフサイクルとしての生産性向上効果を最大化することがあげられます。

参考文献

1）国藤隆、樋浦昇、「ネットワーク信号制御システムの開発について」、JREA Vol.48、No.5、2005

2）石間礼次、福井聡、「駅中間ネットワーク信号制御システムの開発」JREA、Vol.51、No.8、2008