論文の内容の要旨

氏名：髙　田　哲　也
博士の専攻分野の名称：博士（工学）
論文題名：無線式列車制御システム（CBTC）用連動装置の開発と安全性評価に関する研究

安全性が要求される鉄道の列車制御は，列車を検知する軌道回路を利用して構築されてきた．軌道回路は,フェールセーフであるものの,軌道回路を単位として列車に走行の許可を与えることにより，固定閉そくと呼ばれる方式が実現されてきた．一方，近年車上から列車走行位置を取得し，前方列車の後部の一定距離まで走行を可能とする無線式列車制御システム CBTC（Communication Based Train Control）の導入が進みつつあり，移動閉そくという運転能率のよい列車制御が実現している．しかしながら，CBTC 導入線区でも駅構内は既存の連動装置による運転が行われているため，前方列車がその進路を進出しない限り続行列車が進入できない固定閉そくのままであった．このため，駅構内においても移動閉そくによる運転が可能となる CBTC 用の連動装置の開発が求められていた．本論文は，まず CBTC 用連動装置の研究成果について述べる．さらに，開発した CBTC 用連動装置の安全性評価についての研究成果を述べる．ソフトウェアを含むシステムの安全性解析・評価には，適切な手法がないことが問題となっていたが，本研究によって一つの方法論を提示することができた．

本論文は第 1 章から第 6 章からなる．以下，各章についてその要旨を述べる．

第 1 章

「序論」では本研究の目的と意義について述べている．既存の列車制御装置はフェールセーフな列車検知装置である軌道回路をベースとしている．近年 CBTC が導入され，移動閉そくによる列車制御が実現しているが，駅構内は既存の連動装置をベースとしており，効率的な運転を支障している．この状況を背景に，本研究は，CBTC 用の連動装置の開発とその安全性評価を対象としている．

また，序論では，各章の内容について簡単に説明している．

第 2 章

「鉄道信号用連動装置の機能と課題」では,軌道回路をベースとした連動装置の特徴と課題について,連動装置が内包する「各種鎖錠」論理を取り上げ，その機能と役割を分析している．また，コンピュータによって実現した既存の電子連動装置を対象に，現在行われている安全性検査の手順を紹介し，その課題について分析している．

連動装置とは，鉄道の駅構内等において分岐器を動かす転てつ機と列車の進入を指示する信号機を制御し，列車同士の衝突や列車の脱線を防止するための信号保安装置である．軌道回路をベースとした列車検知により列車制御を行ってきた固定閉そくによる ATC（Automatic Train Control：自動列車制御装置）に対して，列車の走行位置情報を基にした列車検知により列車制御を行う CBTC の運転効率の違いを最小発着時隔のシミュレーションを行い比較した.この結果,駅間では移動閉そくの実現により運転効率の向上ができているが，駅構内では軌道回路をベースとした既存の連動装置による連動処理に起因して効率的な運転ができていないことが分かった.このとから,駅構内における移動閉そくを実現する CBTC 用連動装置の開発が必要であることを明らかにしている．

第 3 章

「CBTC 用連動装置の提案」では,第 2 章の課題を克服するための手法とその仕組みを説明する．

その手法である走行路確保の考え方による移動閉そくが可能な連動機能は，既存の連動機能のように全ての条件が成り立つことで信号機により進入を許可する方式ではなく,安全に走行できる箇所(支障点）まで進入を許可する走行路の概念を導入したことで，既存の連動装置の信号結線で実現していた鎖錠条件などは以下のように整理ができた．

進路の構成要素が満たされれば，進入できなかったが，安全が確保されるところまで進入する列車に与えた占有権（閉そく）に基づき，１閉そく１列車を管理する移動閉そく論理にて進路鎖錠，進路

区分鎖錠，閉路鎖錠，てっ査鎖錠機能は満たされる．

また,接近鎖錠,保留鎖錠,時間鎖錠は,中央と列車間のクローズドループにより列車の位置情報に基づく制御を行なうため機能は満たされる．

なお，照査鎖錠は，表示制御盤を分割しなくてもよくなるので基本的に不要となり,表示鎖錠については，転てつ機制御，信号制御の現場状態と比較する処理を行うことで結線処理は不要となる．

このため，既存の連動装置で駅個別の連動結線で設定していた鎖錠論理は，不要となる．これらの検討を通じ，本研究にて提案する CBTC 用連動装置の制御方法は，駅構内においても移動閉そくを実現するのみならず，既存の連動装置の安全性が確保できることを明らかにした．

第 4 章

「既存安全性評価手法の検討」では,既存の安全性評価の現状と問題点を整理する．

まず，システムの安全性評価に使用される FMEA（Failure Mode and Effects Analysis）,FTA（Fault Tree Analysis）,STAMP(Systems-Theoretic Accident Model and Processes)にはそれぞれ特徴があることを示す.FTA においてはシステムの不具合モードから解析を深度化させていくが，解析の終端はソフトウェアのバグではなく，機能モジュールの機能不具合にとどまらざるを得ない．一方，FMEA においてもソフトウェアの故障をどう定義し，その影響を評価するか，そもそもの方法論がない．このように多くの機能がソフトウェアで実現されているにもかかわらず，既存の安全性評価手法は十分ではないことを明らかにした．

一方,構成要素間のインタフェースの齟齬に着目してシステム障害を分析する STAMP は,FTA や FMEA などの事故評価モデルでは見つけることが難しかったシステム全体の設計に起因する事故原因を特定しやすくなっていることが特徴である．このことを，鉄道信号システムの一つである踏切制御システムの解析を通して実際に起きた事故結果と比較することにより解析の網羅性と解析結果の発生確率に違いがあることを示した．しかしながら，STAMP 解析そのものの結果では,定性的な解析結果としては有効であるがその結果を定量的解析に結び付けることは難しいことがわかった．

第 5 章

「新しい安全性解析手法の提案と CBTC 用連動装置の安全性評価」では,STAMP を利用した新しい安全性解析手法を提案し,この手法に基づき，具体的に CBTC 用連動装置の安全性評価を行った．

グローバル化に伴い鉄道におけるシステム全体の安全性・信頼性の評価には，鉄道の国際規格 RAMS（IEC62278）への対応が要求される.この規格では安全性に対する評価には定量的解析が求められている.新しい安全性解析手法は，本質的な解析を行う手法として,概念図に基づく解析により結果の網羅性を示せる STAMP 解析を使用し，更に方法論を拡張して解析結果を模式化することで定量的解析に結び付けることを提案した.これにより,起こしてはいけない事象へ至る背景をシナリオとして表現する.さらに得られた結果を,FTA と同様に発生頻度の定量的評価ができるよう，原因の潜在的な危険（フォールト）を論理的にたどり，それぞれの発生確率を算出できるようにした．

また,解析結果に基づく可能な対策は,連動装置における安全性機能要求に相当するものであり,ここから連動装置に対する安全性機能要求仕様書（System Requirements Specification）を導き出すことができる．さらに,対策に対する具体的な方策はシステムアーキテクチャー仕様書（System Architecture Specification）に相当するものとして導き出すことができる．本安全性評価手法は,連動装置に起因するアクシデントをトップ事象にそこに至る要因を導き出すものである.よって,ここで導き出された要因を排除し機能を作り上げた連動装置は,アクシデントに至らない.すなわち安全であることを理論的に示すことができると考える．

継電連動の駅別信号結線に基づく既存の連動装置では，駅別データに連動機能におけるほとんどの安全性機能要求が集中することになるため，駅ごとの検査に重要度が集中することになる．これに対して，本研究で示した CBTC 用連動装置では，安全性機能要求を基本プログラムで処理することになるため，基本プログラムにおいて，一度検査が済んだ状態であれば駅ごとに安全性機能要求事項を確認する必要性がないことを示した．その上で,本方式における論理を適用した CBTC 用連動装置の評価を行い,作成した論理の妥当性の確認を行った．

第 6 章

「結論」として,各章で得られた結論を整理し，併せて今後の課題を示す.

今日の鉄道信号システムは，既に高い安全性水準に到達している.新しい安全性解析手法により,連動機能の概念を基に導き出した安全性要求事項は,この高い安全水準に達している既存連動装置の実現手法とも結びつけることができた.これにより CBTC 用連動装置の実現手法との関連性を示すことができたことも本研究の成果である.

CBTC においても既存の連動装置による駅構内の運転では課題があることを示し，その解決策として支障点の概念を用いて走行路の占有許可を与えることで,移動閉そくを実現する CBTC 用連動装置の制御方法を開発できたが，今後は，具体的なシステムへの適用を進め実用化を目指していきたい.

一方，近年主体となる制御システムはコンピュータ制御方式であり，その論理はソフトウェアによる．これに伴い，ソフトウェアの不具合による障害も多くなっている．しかしながら，ソフトウェアの故障がどのようにシステムに影響するのか,適切に解析する手法はなかった.このため本研究では,STAMP を応用した新しい安全性解析手法を開発するとともに，CBTC 用連動装置を評価し，その安全性が十分確保できることを明らかにした．なお，開発した安全性解析手法は，鉄道のみならず安全・安心を担うシステム等へ適用できるものである．今後は，より一般的に使用できるようツール化し，設計の上流段階でシステムの安全に関するリスクを把握し，ライフサイクルに亘りそのリスクを管理していくことができるようにしていくことも必要であると考えている.