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

令和元年　９月

髙　　田　　哲　　也

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

目　次

第１章　　序論

１.１　研究の背景と目的

1980 年代後半に登場した電子連動装置は目覚ましい発展を遂げてきた[1]．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. 電子連動装置は連動機能をマイクロコンピュータにて処理する連動論理部と転てつ機等の現場機器を制御する端末部で構成される. 論理部は各種マイクロコンピュータのフェールセーフ（fail-safe）構成によりシステム開発が進められた．その成功により，鉄道信号システムのコンピュータ化が進んだ．現在 IT（Information Technology），IoT（Internet of Things）の時代を迎え ATC（Automatic Train Control：自動列車制御装置）の無線化による地上装置の軽量化やシステム構成の変更が容易であるといった点から, 国内外において CBTC（Communication Based Train Control：無線式列車制御システム）の導入が進みつつある.

CBTC は，軌道回路単位でなく前方列車の位置をベースとした移動閉そくが実現できるため，列車の高密度運転が可能という利点がある．しかしながら，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ず，運転能率のネックになっていた．このため，駅構内にて移動閉そくによる運転が可能となる CBTC 用の連動装置を開発することとした．一方，ソフトウェアを含む保安装置の開発には，安全性を確保するための配慮が求められているが，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無い状況である．このため，新たな手法を提案し，CBTC 用連動装置の安全性評価を行った．本論文は，これらの研究成果について論じるものである.

１.２　本論文の構成

本論文おいて，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列車検知装置により列車制御を行ってきた固定閉そくによる ATC に対して, 列車の位置情報を基にした列車位置検知をベースとして列車制御を行う移動閉

そくによる CBTC 化の効果を説明したうえで，駅構内の連動機能実現手法の課題及び信号結線を処理する結線論理処理方式による既存の連動機能での安全性確保の手法について示す．

第 3 章「CBTC 用連動装置の提案」では，第 2 章の課題等を基にその課題を克服するための手法として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の実現方法を提案しその仕組みを説明する．

次に，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したうえで，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，新たな安全性解析手法として着目される STAMP(Systems-Theoretic Accident Model and Processes)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う．

最後に，第 6 章「結論」では，本研究の成果をまとめるとともに，各章で得られた結論を整理する．併せて，今後の課題として本方式の実用面における展開について述べる．

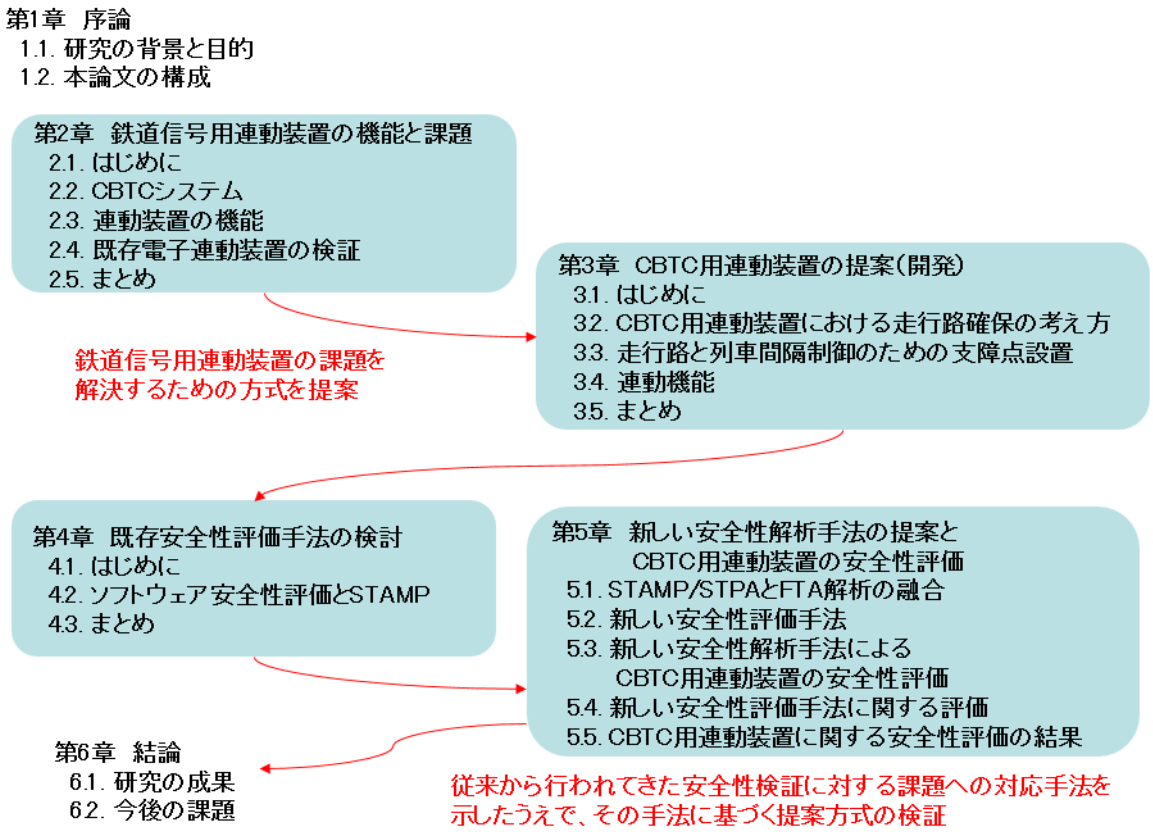


図 1-1 本論文の構成

第２章　　鉄道信号用連動装置の機能と課題

２.１　はじめに

列車運転の安全を確保するには, 走行する車両が健全であることが第一に必要であり，次に軌道が完全であり，レールに破断や落石などの障害物があってはならない. その上で, 列車衝突が起こらないように, 先行列車と次列車との間隔を制御し，また，単線区間にあっては，駅間で対向する列車間の排他制御を万全に行わなければならない. これを列車間隔制御という. また, 駅構内において分岐箇所がある場合, 所定の走行路が確保され列車や車両を運転する際に, 脱線したり別の走行路に進入してしまったりしてはならない. これを列車進路制御という．これらの制御を行う装置を総称したものが列車の信号保安装置である.

性能規定化された鉄道に関する技術上の基準を定める省令（技術基準）[2]では，信号保安装置のうち連動装置は，信号相互間を連鎖させる装置とされている．駅構内では分岐や複数の列車が存在する．列車が走行中に転てつ機（転てつ機とは列車をある線路から他の線路へ移動させるための線路部分（分岐器）を転換させる機械）が転換すれば列車は脱線する. 列車が存在する場所に列車を進入させれば列車同士が衝突する．このため，進路を構成し，その進路を解除するまで信号機をロックする．また，列車や他の進路構成が支障しているとき別の進路を構成させないようにする.また ATC は，列車を自動的に減速または停止させる装置とされている.方式としては列車検知装置で列車の在線を検知し，自動列車制御装置から送信される ATC 信号により列車の速度を制御する.

列車検知装置も，同技術基準において列車を検知する装置とされている.方式としてはレールを列車の車軸で短絡することにより検知する軌道回路と呼ばれる方式が主である．これに対して，昨今話題となっている CBTC は，列車検知の方式として車上で位置検測を行うことにより軌道回路を用いずに高精度な列車位置検出を行うシステムである.このため軌道回路をベースとした既存の鉄道信号システムに比べて列車検知装置やレール周りの設備が不要となるなど地上設備の軽量化が図れ, またシステム変更が容易であるなど事業者にとっては非常に魅力的なシステムであると考えられている.

２.２　連動装置の機能

停車場構内は，多くの線路が集中・分岐するネットワーク状に接続されるため連動装置は，列車運転に必要なすべての走行路が安全を確認しつつ構成できるように作られている．よって，線路の分岐部分や交差部分においては，走行路を構成するために必要な多くの転てつ機が設置され，また各走行路を指示するための諸信号機，合図器，標識なども多く設けられている．列車の発着，車両の入換作業なども，構内配線の許す限り同時作業を行い，高能率化を図るためには，転てつ機の転換や関係信号の取り扱いに関する制約が非常に数多く複雑となっている．このため信号機，転てつ機の間に関係をつけて扱い者が信号機または転てつ機の取り扱いを間違っても，扱うことができないようにしている.これを「鎖錠」という．さらに,これらの信号機，転てつ機のてこが互いに関連し，その取り扱いに一定の順序があり，且つ鎖錠関係のついていることを連鎖といい，連鎖関係を保って動作することを連動という．その例を図　２-１に示す．この連鎖関係を付けた装置を連動装置といい，マイクロコンピュータにより処理するものを電子連動装置という．

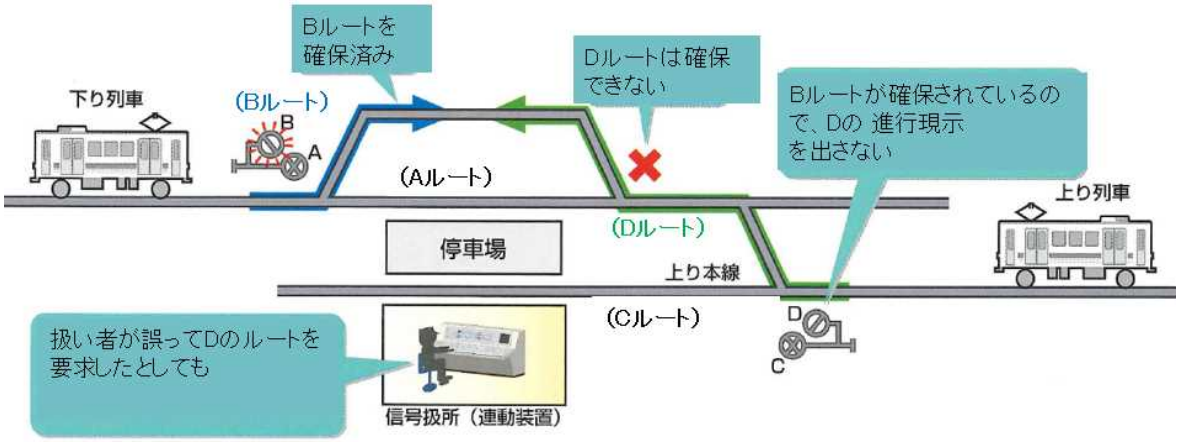


図　２-１　連動機能の例

連動装置は技術基準における信号保安装置のうちの信号相互間等を連鎖させる装置等にあたる.

信号機・転てつ機等の間に，機械的あるいは電気的な方法により，各種の鎖錠が行われ，それぞれの動作を必要に応じて制限する．このうち電気を用いて連鎖を付ける方法を電気鎖錠法という．継電連動装置では，リレーの動作によって，電気的な鎖錠を行い，高度の連鎖を行っており次に挙げる種類のものを組み合わせて安全性を確保している．

(1)　進路鎖錠

進行を指示する信号機の現示，入換標識の開通指示の表示により，列車または車両がその進路（ルート）に進入したときは，その進路を支障するほかの進路が構成できないように，列車または車両が進路内のすべての転てつ機を通過し終わるまでは関係する転てつ機を転換できないようにする鎖錠．

(2)　進路区分鎖錠

列車運転や構内作業の能率向上のため，進路鎖錠の区間を区分し，列車や車両が通過し終わった区間から順次解錠していく進路鎖錠．

(3)　閉路鎖錠

信号機の進路内の軌道回路に列車または車両が在線するとき，信号機を定位に鎖錠する信号機と軌道回路間の連鎖の一つ．

(4)　てっ査鎖錠

転てつ機を含む軌道回路内に列車または車両が存在するときに，その列車または車両自体によって当該転てつ機を転換できないようにする鎖錠．

(5)　接近鎖錠

信号機に一旦進行を指示する信号を現示させ，列車が当該信号機の接近鎖錠区間に進入したとき，または列車が接近鎖錠区間に進入しているときに，当該信号機に進行を指示する信号を現示したときは，列車が当該信号機の内方に進入するか停止信号を現示させた後，一定時分が経過するまでは列車によって進路内の転てつ機を転換できないようにする鎖錠．

(6)　保留鎖錠

信号機または入換標識などに進行を指示する信号を現示させた後，列車または車両が内方に進入するか，信号機などに停止現時を現示させてから一定時分が経過するまでは，進路内の転てつ機の直前転換や途中転換を防止するために，転てつ機を転換できないようにする鎖錠．

(7)　時間鎖錠

信号機と転てつ機のてこ相互間などで, 信号機のてこを反位から定位の状態に戻しても，なお一定時分鎖錠する連鎖.

(8)　照査鎖錠

てこ扱所が異なるてこ相互間に設けられる連鎖.

(9)　表示鎖錠

てこと現場の信号機, 転てつ機の状態が一致しているかチェックし，不一致の場合には危険な制御を防止する鎖錠.

なお，電子連動装置については, 継電連動装置のリレーロジック（信号結線）をソフトウェア処理により実現するため信号結線をシーケンス処理（信号結線をブール代数で表し定周期で順番に処理する）されるなどの違いはあるもののこの電気鎖錠法が基本となっている.

２.３　既存電子連動装置の安全性検証手順

既存の電子連動装置は，論理部と端末部で構成される. 論理部では駅別仕様に基づく信号結線を処理し, この結果に基づき端末部では現場機器を制御する．駅の規模により接続される外部機器が異なるため，駅別仕様に基づく入出力点数に従い，端末数は決定される.

駅別仕様に基づく駅別データ設計（システム設計）は鉄道の国際規格 RAMS（IEC62278）[3] 8.4 項および Table A.11 記載の安全性レベルで規定されているものと同等以上のプロセスで実施される必要があり，電子連動装置は Table A.11 に記載されている最も高い安全性達成基準である SIL4（Safety Integrity Level 4）レベルで要求されている技法の組み合わせを満たす必要がある.

日本では技術基準に規定される性能を原則として満たすことを要求事項としてシステム設計を行う.

連動装置においては技術基準七章第一節の信号保安設備の閉そくを確保する装置等や信号相互間を連鎖させる装置等が要件となる.

システム検査では各検査条件に沿って, リレー出力結果の妥当性を確認することが相当する.

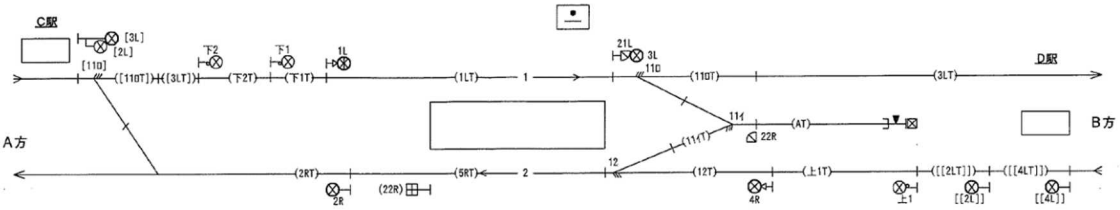
システム設計と検査は以下による.

(1)　システム設計

てこ，押し釦等に関連するリレーのダイヤグラムを作成し，信号結線図を設計する.

a)駅構内の連動関係を一括して表に表したものを連動図表といい，これに基づいて信号結線図が作られる．図 2-2に連動図表の例を示す．これを見れば駅構内の連動関係が明らかになると共に信号結線図作成の基本となるものである.

京三駅　連動図表



第1種電子連動

名称		番号	鎖錠	信号制御又はてっ査鎖錠	進路鎖錠	接近鎖錠又は保留鎖錠
場内信号機	A方 － 下り本線（警戒信号現示）	1L		1LT		[(11DT 但3L)] [3LT] 下2T 下1T ((90秒))
出発信号機	上り本線 － A方	2R		2RT		
同上	下り本線 － B方	3L	11	11DT 3LT	(11DT)	([(11DT 但11)] [3LT] 下2T 下1T 但11) 1LT ((90秒))
場内信号機	B方 － 上り本線	4R	12	12T 5RT	(12T)	[[4LT 2LT]] 上1T ((90秒))
入換信号機	下り本線 － 引上線	21L	11	11DT 11↑T AT (12T 但12)	(11DT 11↑T)	1LT ((30秒))
同上	引上線 － 上り本線	22R	11 12	11↑T 12T 5RT	(11↑T 12T)	AT ((30秒))
転てつ器	（2動）	11		11↑T 11DT (12T 但12)		
同上		12		12T		

(注意)
1．[　]はC駅の、[[　]]はD駅の所属であることを示す。

図 2-2　連動図表の例

b)連動図表で表された連動関係の一切と，場合によってはそれ以上の内容を具体的に結線で示したものを信号結線図という.

この信号結線図の中では，前述各鎖錠に関する機能を実現している．例えば，接近鎖錠リレー回路を例に説明する．接近鎖錠リレー（ASR）は，てこ（あらかじめ走行できる進路を定めこの進路にある）が定位の場合は動作しており，てこを反位にして進路が開通すると落下して進路上の転てつ機を鎖錠する．てこを定位に戻すと現場の信号機が停止信号を現示したことを条件

として，列車が接近鎖錠区間に進入していないとき，または信号機の内方に進入してしまった場合には直ちにASRが動作し接近鎖錠は解かれる．しかし列車が接近鎖錠区間に進入した後では所定時分を経過の後動作する．接近鎖錠開錠補助リレーMS１Rは時素リレーをいくつかの接近鎖錠リレーの開錠に共用しているために設けられたリレーであり，常時は落下しているが，接近鎖錠リレーを時素開錠する場合に，時素リレーが他の接近鎖錠リレーによって使用されていないことを条件として動作し，時素リレーを動作させ，一定時分を経過後，接近鎖錠リレーを動作させ，MS１Rは再び落下する．

この回路は大別して，次の３つの要素に分かれる．

・表示鎖錠の条件

・接近鎖錠をかける条件

・接近鎖錠を解く条件

なお，具体的な結線は，図　2-2の例の場合図　2-3のようになる．

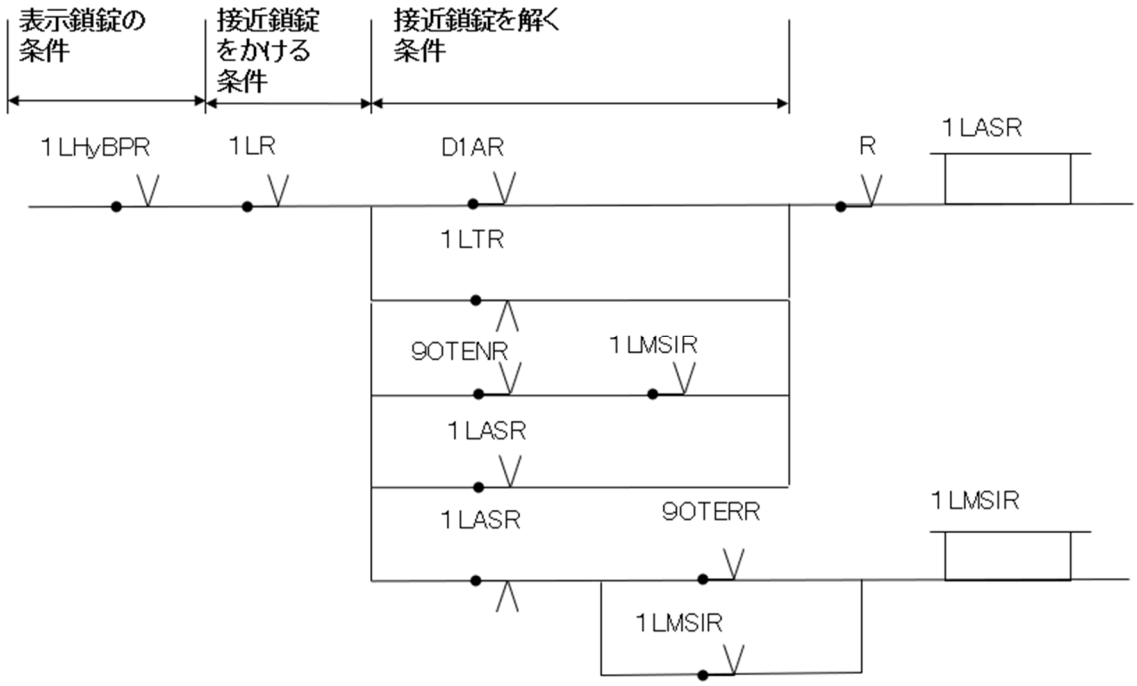


図　2-3　接近鎖錠リレー回路

(2)　検査

設計した信号結線図データの妥当性を確認する電子連動装置の連動検査は JIS E3004 継電連動機検査方法[4]で規定された継電連動装置の検査方法に準じ，実機を使用した検査機能方式で行われる．安全性の要件より検査種別を分類すると以下の 4 項目である．

a)　安全性に直接係わる連鎖条件の検査（おもて検査）

b)　上記に伴い連鎖されない条件の確認検査（裏検査）

c)　安全性に直接係わらない条件の検査で，電子化により増えた検査（新機能検査）

d)　リレー架，表示制御盤と論理部とのインタフェース検査（対照検査）

2.4　CBTC システム

CBTC とは，地上−車上間での双方向通信により列車を制御するシステムを指す．CBTC については，確立した定義はないが，米国電気電子学会の規格（IEEE Std 1474.1™-2004）[5]では ATP（Automatic Train Protection）を基にした ATO（Automatic Train Operation）,ATS (Automatic Train Supervision)を含めたシステムとして定義されている．

CBTC における ATP の定義

① 軌道回路を使わない高精度な列車位置検知

② 連続双方向の高速通信

③ 車上主体型列車制御

この定義より CBTC を考えると，先行列車の位置を逐次後続列車に伝えて，後続列車では先行列車の移動に合わせてリアルタイムに列車制御を行う
図 2-4 の b に示す「移動閉そく」が，有効である．

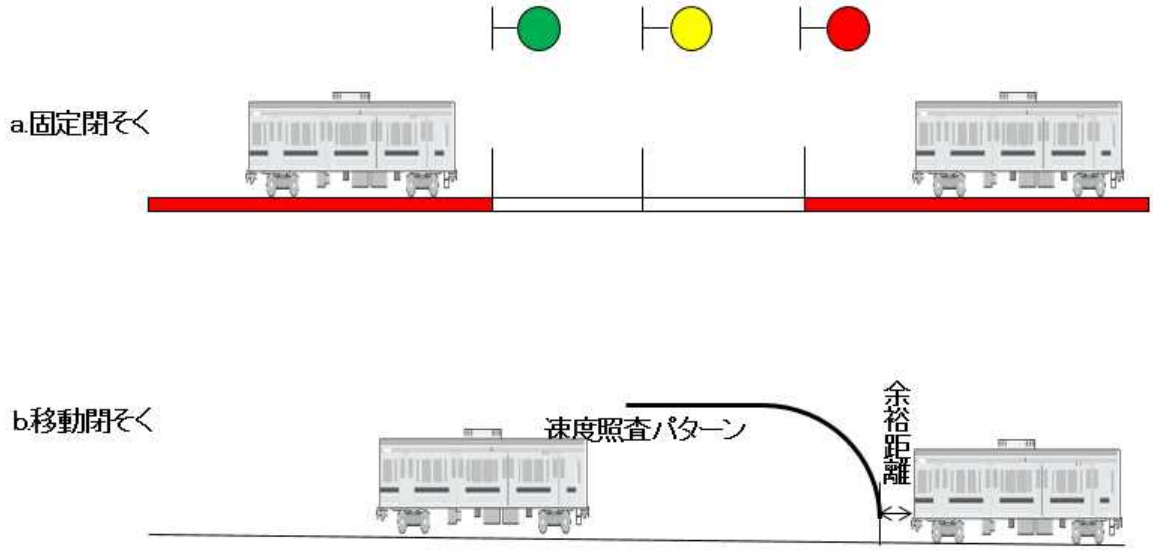


図 2-4　閉そくの違い

現在,駅間では既に列車の位置情報を基にした移動閉そくが実現されているが,駅構内では軌道回路などによる列車検知に基づく連動機能による進路制御に頼っているため,移動閉そくの特長である列車間隔が短くなり運転効率が向上する効果が得られていない.

駅構内の移動閉そくの効果については,駅において同一条件下で最小発着時隔についてシミュレーション(S-T 曲線:走行距離対走行時間曲線)を行って確認した.図 2-5 は,軌道回路(軌道回路長 60m とした場合)を用いた固定閉そく式の場合であり,図 2-6 は,移動閉そく式の場合である.結果は,軌道回路式(後方 02 信号)時隔 51.7sec(停車時間を除く発着時隔)に対し,移動閉そく式時隔 44.7sec(停車時間を除く発着時隔)であった.この結果からも駅構内を移動閉そく化することで列車間隔を短くすることができることが示されたため CBTC 用の連動装置を開発することが有効であることがわかった.

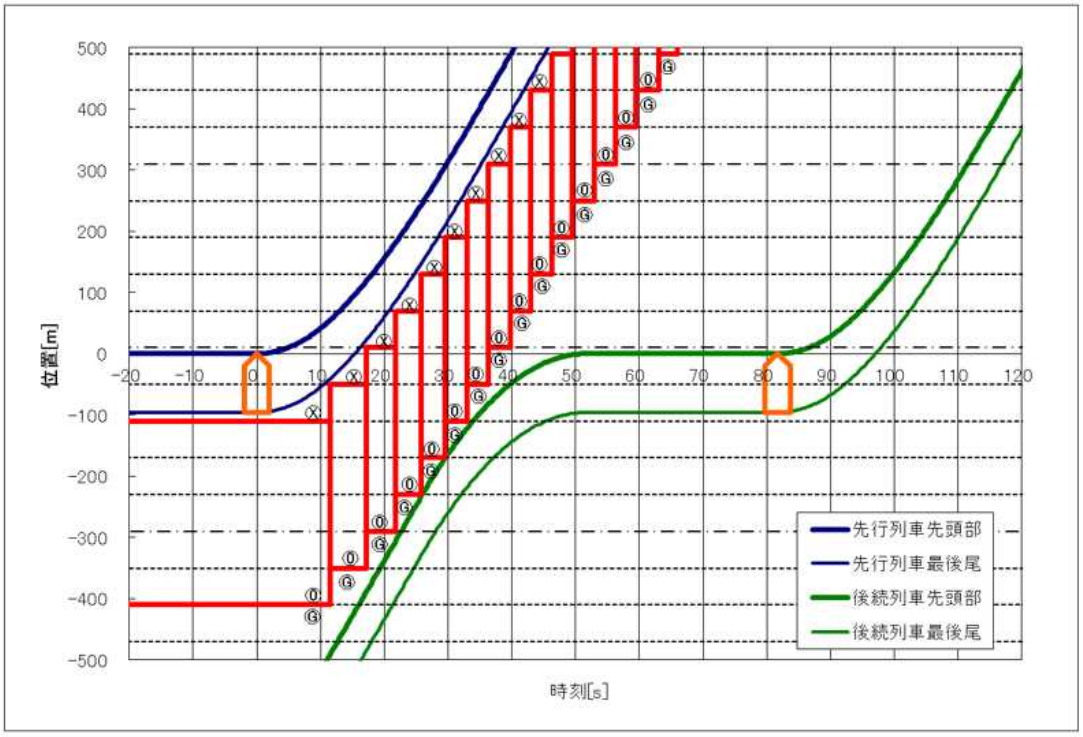


図　2-5　軌道回路式（後方 02 信号）　閉そく区間長 60m　発着時隔 51.7sec

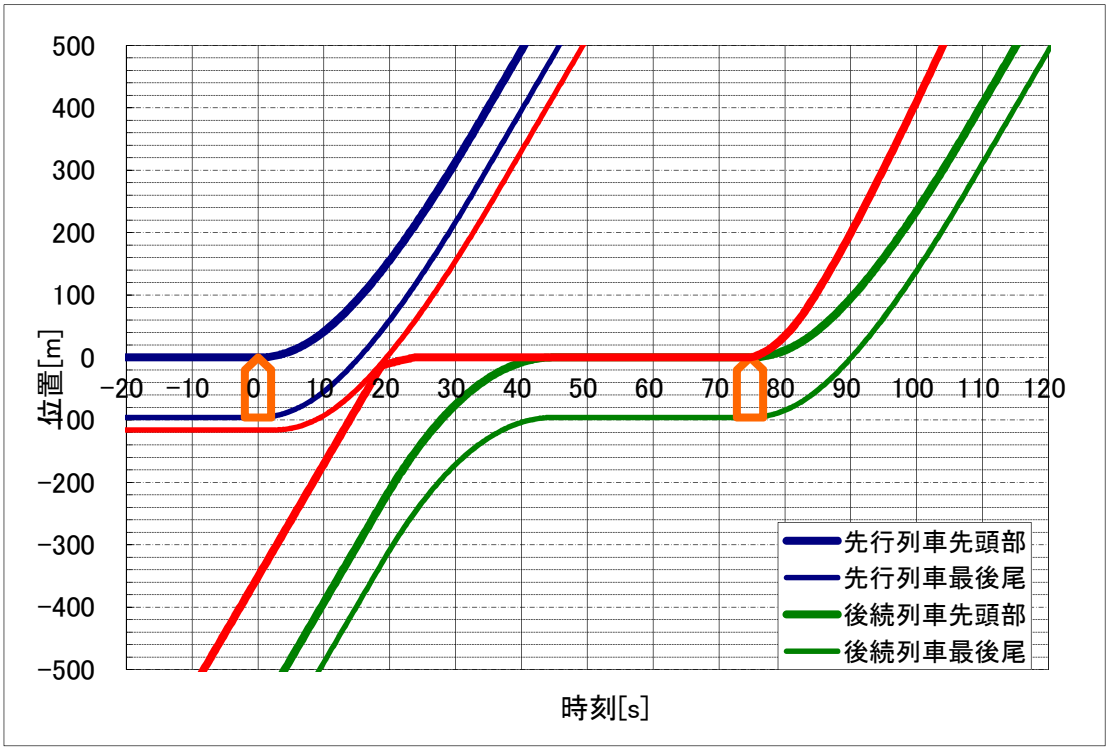


図　2-6　移動閉そく式発着時隔 44.7sec

２.５　まとめ

CBTC を実現するにあたり移動閉そくの考えを取り入れることで列車間隔が短くなり運転効率の良い列車制御が可能であり, 駅間では既に列車の位置情報を基に実現されている．しかしながら，駅構内では既存の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た進路制御に頼っているため, 移動閉そくの効果を実現できていない．また, 最小発着時隔のシミュレーションを行った結果でも軌道回路による固定閉そく式に対して移動閉そくを実現することは, 駅構内にて運転効率を向上させる効果がある．このことから，駅構内における移動閉そくを可能とするため, 新たな連動機能の実現が求められていた.

また，既存の電子連動装置は，継電連動装置によるリレーロジック（信号結線）を基にしている. この信号結線は駅別仕様に基づくためその結線自体に信号機・転てつ機等の間に，各種の鎖錠が行われるなど, それぞれの動作を必要に応じて制限する安全要求機能が含まれる構造となっている．このため，連動機能自体の安全性の確認手法は，駅ごとに確認する必要があり, 都度の検査で安全性を確認しなければならない仕組みとなっている.

第３章　　CBTC 用連動装置の提案（開発）

３.１　はじめに

現在の鉄道信号システムは，閉そく装置, ATC 装置, 連動装置, 設備監視装置などが個別に開発され導入されてきた結果, 縦割りの独立構成となっている. これらの装置にはそれぞれ処理部があり, 処理部には列車追跡など共通の機能が個別に組み込まれている. その結果, 全体の列車制御システムとしては複雑となっているほか, 各装置間のインタフェースも大きなものとなっている.

これに対し，近年では ATC の無線化による地上装置の軽量化やシステム構成の変更が容易であるといった点から, 国内外において CBTC に対する関心が高まっている.

こういったことから個別の装置で構成するシステムではなく, 効率的に機能を処理する統合したシステムの中でそれぞれの機能が相互連携をとり安全を確保するネットワークを基調とした，「システム全体で安全を確保する鉄道信号システム」化へと進んでいくと考えられる.

CBTC はこの流れの中で１つの変化点であり, 対応する上で現システムでの課題となるのが駅構内での連動機能である. 駅構内では軌道回路などによる列車検知に基づく継電連動装置による進路制御方式に頼っているため, 移動閉そくの効果を実現できていない. 最小発着時隔のシミュレーションを行った結果でも軌道回路による固定閉そく式に対して移動閉そくを実現することが必要であることが示されている. 本項では，駅構内の移動閉そくによる連動機能を実現した走行路確保の考え方について述べる.

３.２　CBTC 用連動装置における走行路確保の考え方

従来から示される, 列車を安全に運転するための条件は以下の通りである.

(1) 進路が完全に構成され, かつ確保されていること. すなわち進路上の転てつ機が進路の方向に転換され, 鎖錠されていること.
(2) この進路上に他の列車または車両が存在しないこと.

(3) この進路を支障する他の列車が運転する可能性がないこと.
(4) 列車がその進路を通過し終わるまで, 上記の状態が維持されること.

このように, あらかじめ定めておいた「進路」を列車の走行に合わせて都度構成した後, 連鎖を設けて鎖錠することにより, 関係する信号機や転てつ機が, 個々勝手に操作されないようにする. この機能を「連動」といい, 既存の連動装置はほとんどが進路式 (進路てこ式および進路選別式) であり進路てこを設けてこの進路てこを取り扱うことにより, その進路内に列車が存在しないとき, 及びその進路に関係した転てつ機を一斉に総括制御して, 全部の転てつ機が所要の方向に開通したとき, 自動的にその進路に対応した信号機に進行現示を出す仕組みである.

これに対して, 列車が進みたい終端位置までの間, 前方列車が進むことに応じてその前方列車の後端位置まで進んでもよいという考えを実現する方法として従来の「進路」に対して「走行路」と称し, 進みたい終端位置までの範囲を走行路要求範囲とし, 進んでよい範囲を走行路確保範囲として制御することすることを考えた. ただし, 駅構内には分岐器が存在するため, その状態に応じて進める範囲を制限する必要がある.

走行路確保の観点から列車を安全に運転するための条件を整理すると以下の通りとなり, これを実現するために進める範囲を指示する方法として, 進める範囲を制限する点として「支障点」を設置し, 要求走行路上に「支障点」が発生した場合は, 要求走行路に対して列車先頭位置から「支障点」までをその列車へ占有権を与え列車制御を行うという考え方が走行路確保に基づく連動装置の仕組みである.

(1) 走行路が完全に構成され, かつ確保されていること. すなわち走行路上の分岐器 (転てつ機) が走行路の方向に転換され, 鎖錠されていること.
(2) 占有した走行路上には列車または車両が存在しないこと.
(3) 占有した走行路には他の列車が運転できないこと.
(4) 列車がその走行路の通過した部分について走行路の占有権が解かれる.

これに, 走行路内に複数列車の存在を認めるための列車間隔制御条件を加える.

３.３　走行路と列車間隔制御のための支障点設置

走行路は辺の集合で定義する.その上で,その走行路上に列車走行に支障を与える点を支障点として設定する．その方式を以下に述べる.

３.３.１　　路線データベース構造

走行路の線形データは，線路網を以下の表現方法で表す位置情報で表す.

(1)線路の表現

線路網を図式化するため，線路左右のレールを１本の線とみなした，グラフで表現する．グラフは節点（図 ３-１中 v1～v13）と節点を結ぶ辺（図 ３-１中 e1～e13）から成る．節点は始点・終点・分岐点やその他線路上の設備位置付近に設定する．各辺の始端，終端および辺間の接続を定義し，辺内の相対位置を指定することで，位置を表すこととする．路線データベース上では，その他路線データベース上に必要な各設備についても，辺内の相対位置を持って表す.

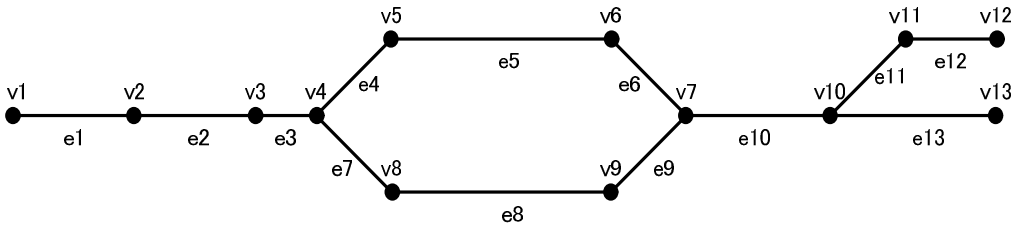


図 ３-１　線路の表現

(2)線形の表現

各辺は線路上の点の集合として管理し，点間を直線で結ぶことで図 ３-２のように線形を表現する.

点の情報は位置情報として緯度・経度・方位，そして辺の起点（節点）を０とした，辺内の相対距離で表す．その他，線路の情報として勾配・曲率半径・制限速度，表示用のキロ程情報を持つ.

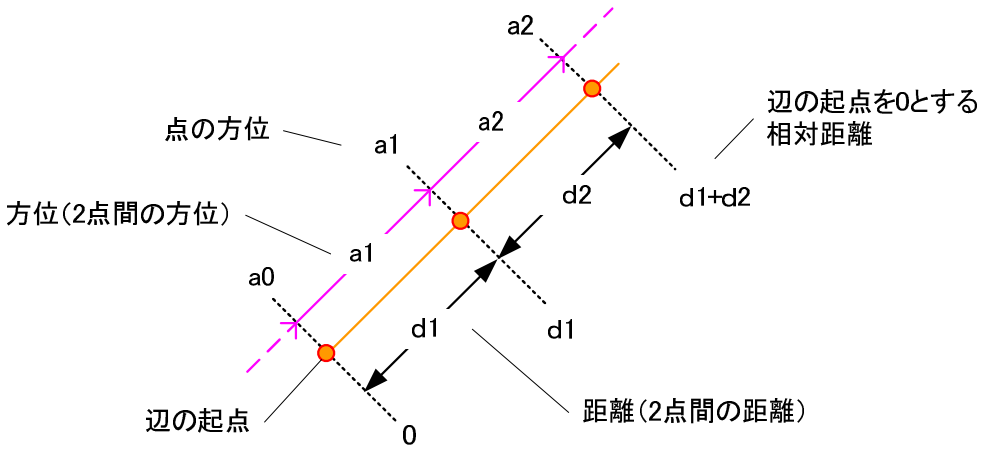


図　3-2　各点の位置情報

(3)線路形態

辺（e1～e8），転てつ機（s1～s2）が存在する図　3-3のような線区を考える．この線区の線路形態を路線データベース上で表すと，表　3-1のようになる．ある辺に対して，始端側に接続する辺，後端側に接続する辺について記載する．分岐が存在しない場合は 0 とし，接続する辺番号を定位辺番号の項目に入力する．

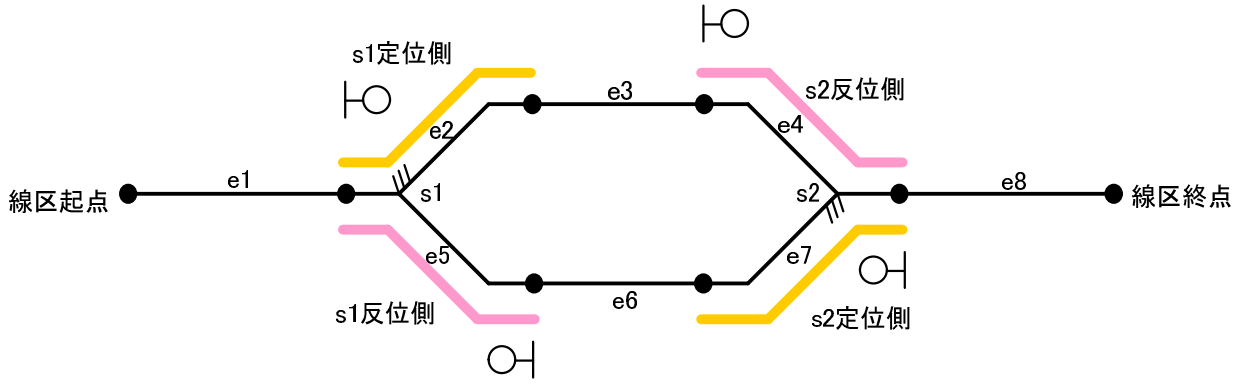


図　3-3　線路形態の例

表 3-1　線路形態データの記載例

辺番号	始端 転てつ機 番号	定位 辺番号	反位 辺番号	終端 転てつ機 番号	定位 辺番号	反位 辺番号
e1	0	0	0	s1	e2	e5
e2	s1	e1	0	0	e3	0
e3	0	e2	0	0	e4	0
e4	0	e3	0	s2	0	e8
e5	s1	0	e1	0	e6	0
e6	0	e5	0	0	e7	0
e7	0	e6	0	s2	e8	0
e8	s2	e7	e4	0	0	0

3.3.2　支障点設置

要求走行路上に支障点が発生した場合は, 要求走行路に対して列車先頭位置から支障点までをその列車へ占有権として与え列車制御を行う.

例えば, 以下のように支障点を設定する（例を図 3-4 に示す. 図中の緑▲が支障点.）.

(1) 支障点１：走行路中の前方列車後端位置

(2) 支障点２：走行路中の分岐器に関する位置

(3) 支障点３：走行路中の対向列車による確保済み走行路に関する位置

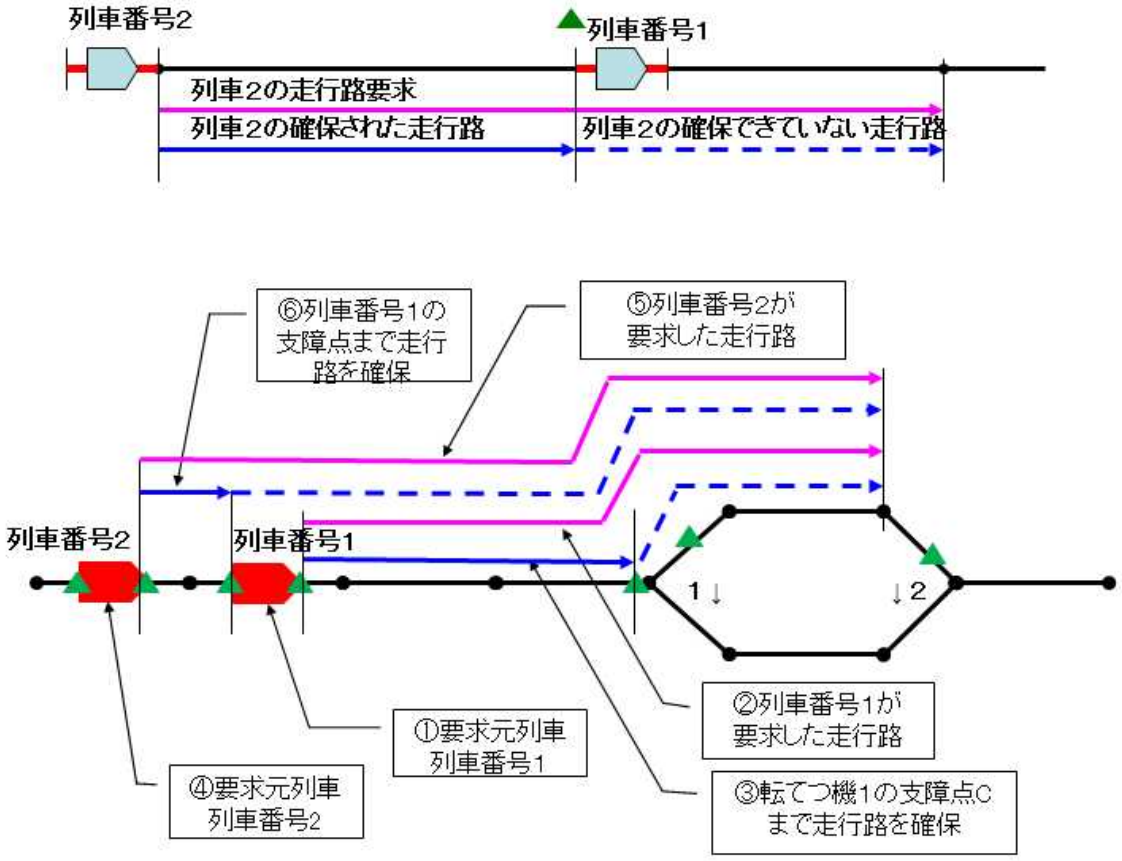


図 3-4　支障点に基づく制御

3.3.3　分岐器のための支障点設置

駅間区間においては，走行路中の前方列車の前後位置に支障点を設置することで移動閉そくは実現できるが，駅構内に入った場合は，前方列車の前後位置だけでは制御を実現できない．線路上を走行する鉄道においては，分岐器を安全に走行する必要があるためである．

そこで，分岐器のための支障点の設定位置について整理する．分岐器のための支障点は図 3-5 に示す 3 点（C，N，R）が必要となる．

設置する位置としては，支障点 C は分岐器構造上の基本レールの始点（図 3-6），支障点 N と R は，車両接触限界点の外側（図 3-7）に設定することで分岐器を安全に走行できる．

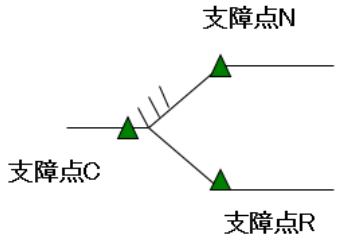


図　3-5　分岐器のための支障点

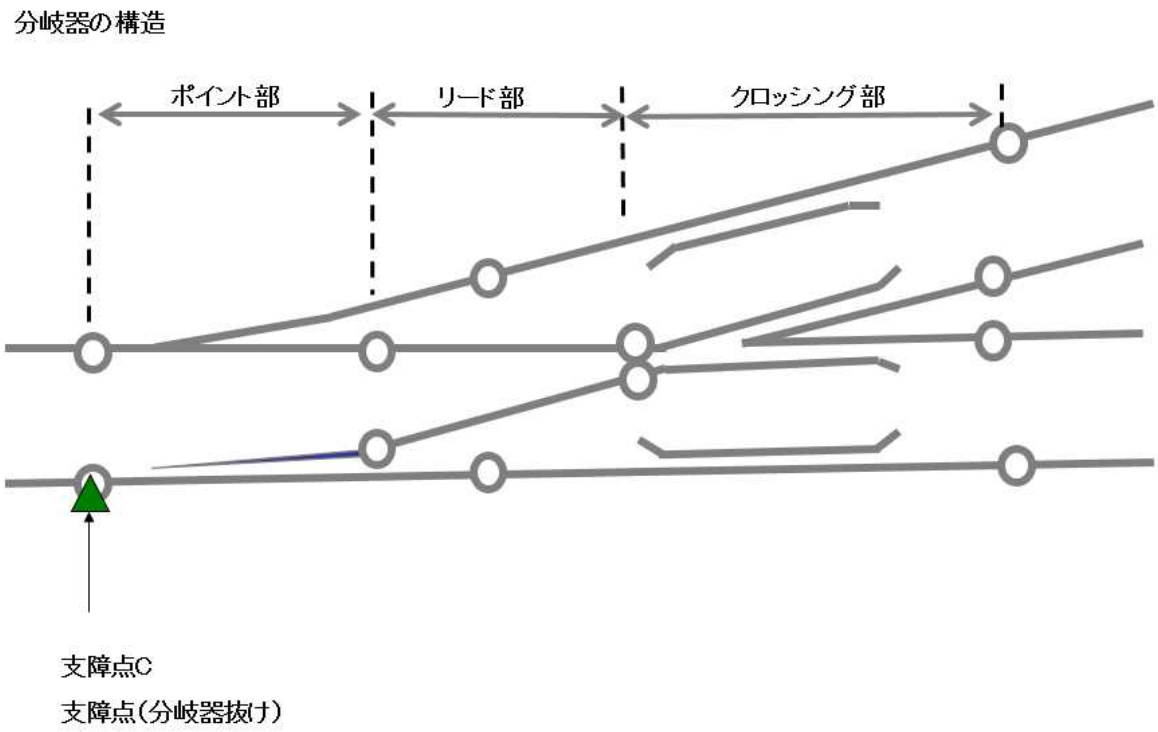


図　3-6　支障点 C

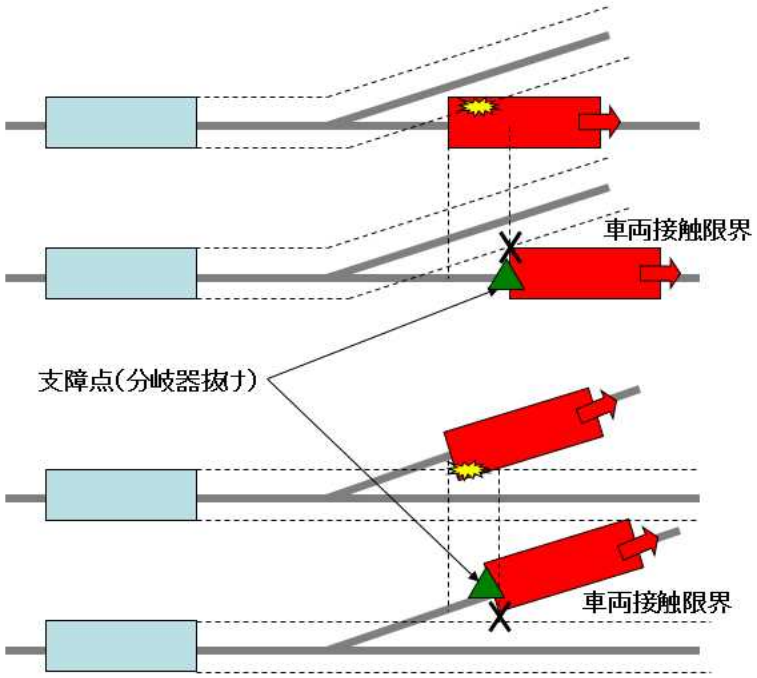


図 3-7　支障点 N,R

3.3.4　列車制御のイメージ

列車制御は，構内を含めた移動閉そくとし，列車制御のイメージは以下の(1)から(7)の通りとなる．

(1)発点から着点まで走行路が確保される条件

①列車番号 1 が点 A から点 B の走行路確保を要求する．

②転てつ機 51 が↑側に転換され，鎖錠されていること．

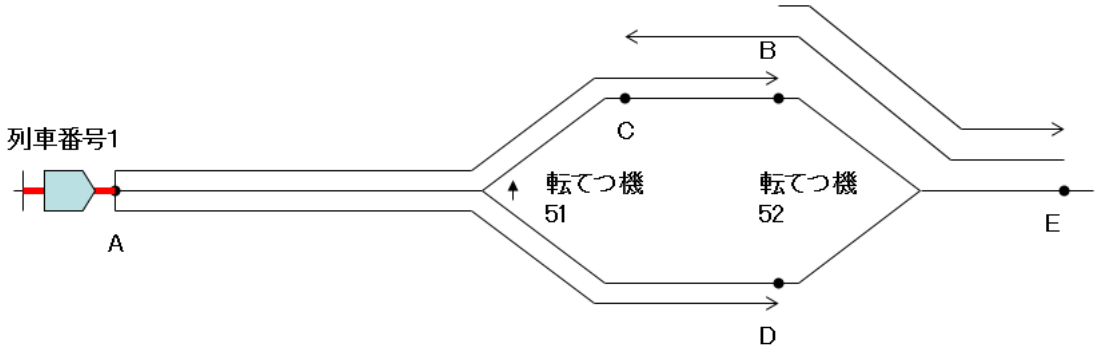


図　3-8　列車制御のイメージ

(2)列車番号 1 に点 A から点 B までの走行路の走行を許可する.

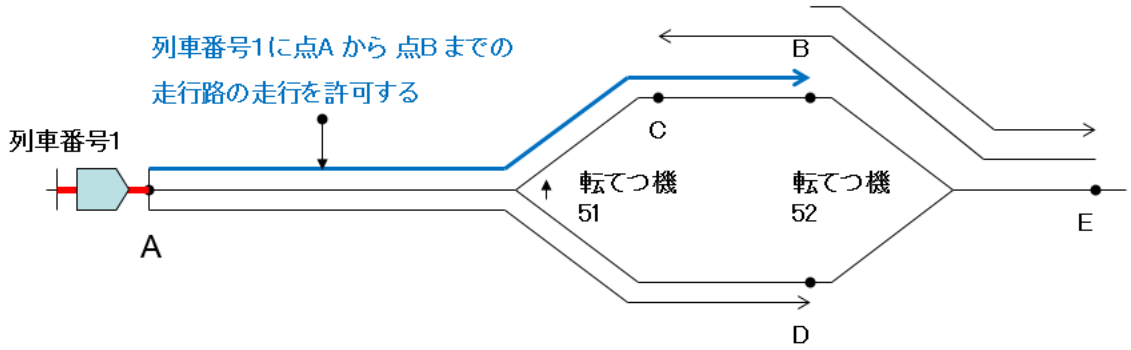


図　3-9　列車制御のイメージ２

(3)列車番号１がその走行路を通過した部分について走行路の占有権が解かれる.

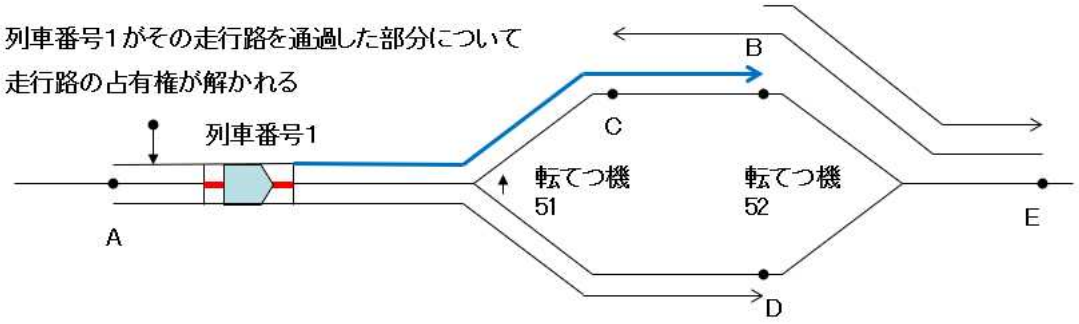


図　3-１０　列車制御のイメージ３

(4)列車番号１に続き列車番号２が点Ａから点Ｂの走行路確保を要求した場合

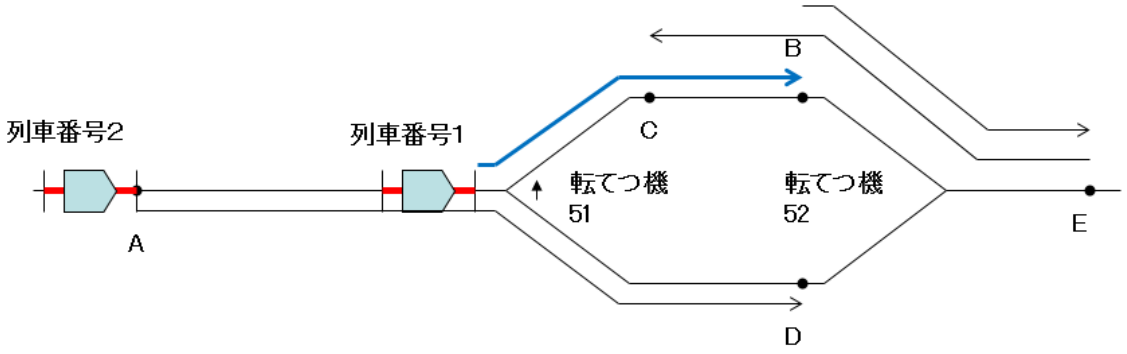


図　3-１１　列車制御のイメージ４

(5)列車番号 2 にも点 A から点 B までの走行路の走行を受け付けるが，列車番号 2 は列車番号 1 の後方までのパターン制御が行なわれる

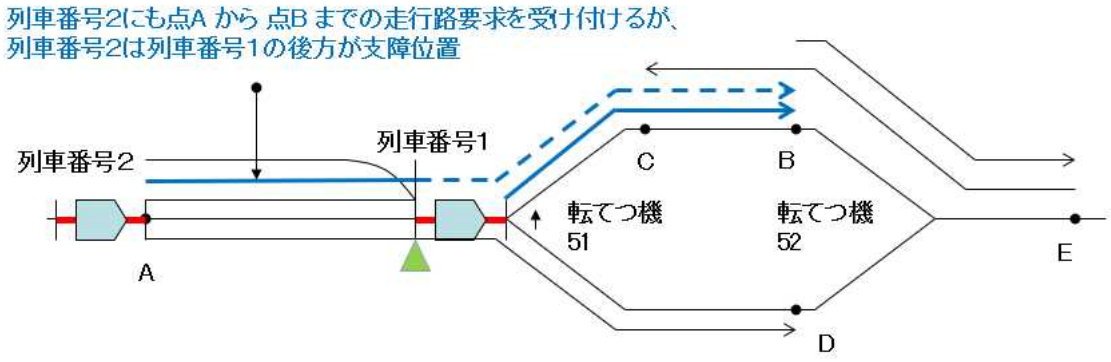


図　3-１２　列車制御のイメージ５

(6)列車番号 1 が前方走行中，列車番号 2 が点 A から点 D の走行路確保を要求した場合

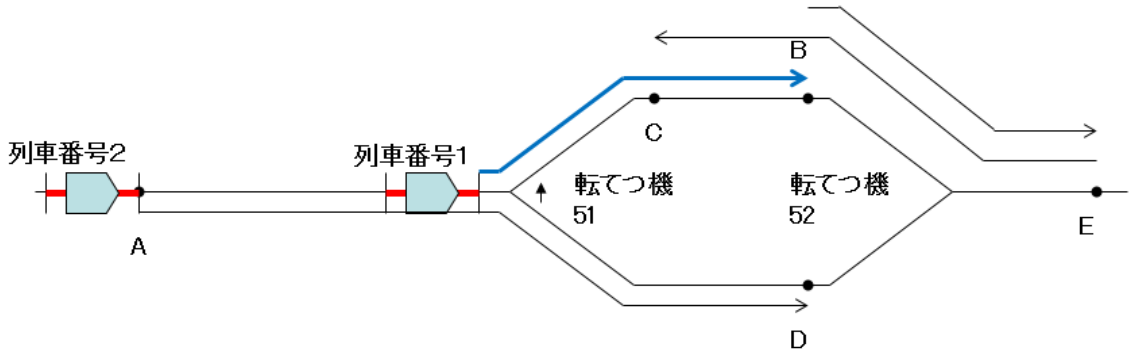


図　3-１３　列車制御のイメージ６

(7)列車番号 2 に点 A から点 D までの走行路の走行を受け付けるが, 列車番号 2 は列車番号 1 の後方までのパターン制御が行なわれる.列車番号 1 が分岐器を抜けたとしても,分岐器が転換するまでは転てつ機 51 手前の支障点となる

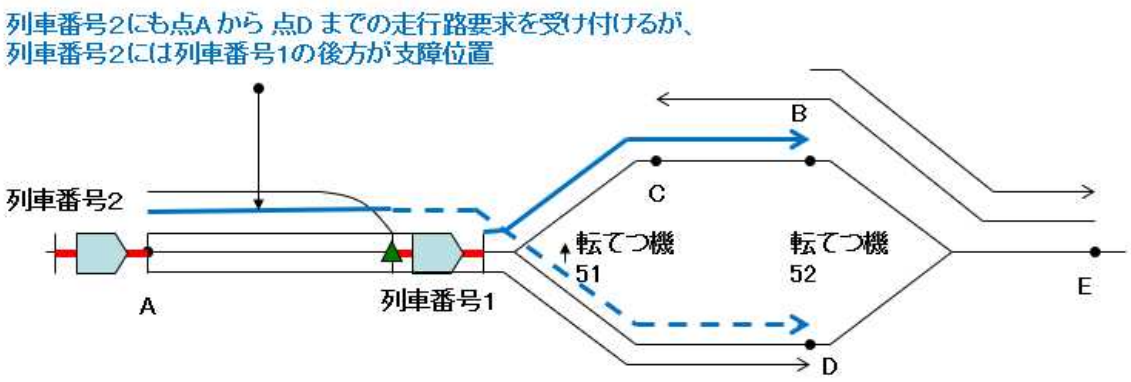


図 3-１４　列車制御のイメージ７

３.４　連動機能

走行路確保の考え方に基づく連動機能は,既存の連動装置のように,駅別連動図表に基づく信号結線論理として個別に持つのではなく,保安を確保する論理として共通プログラムとして持つ.その概念図を図　３-１５に示す.

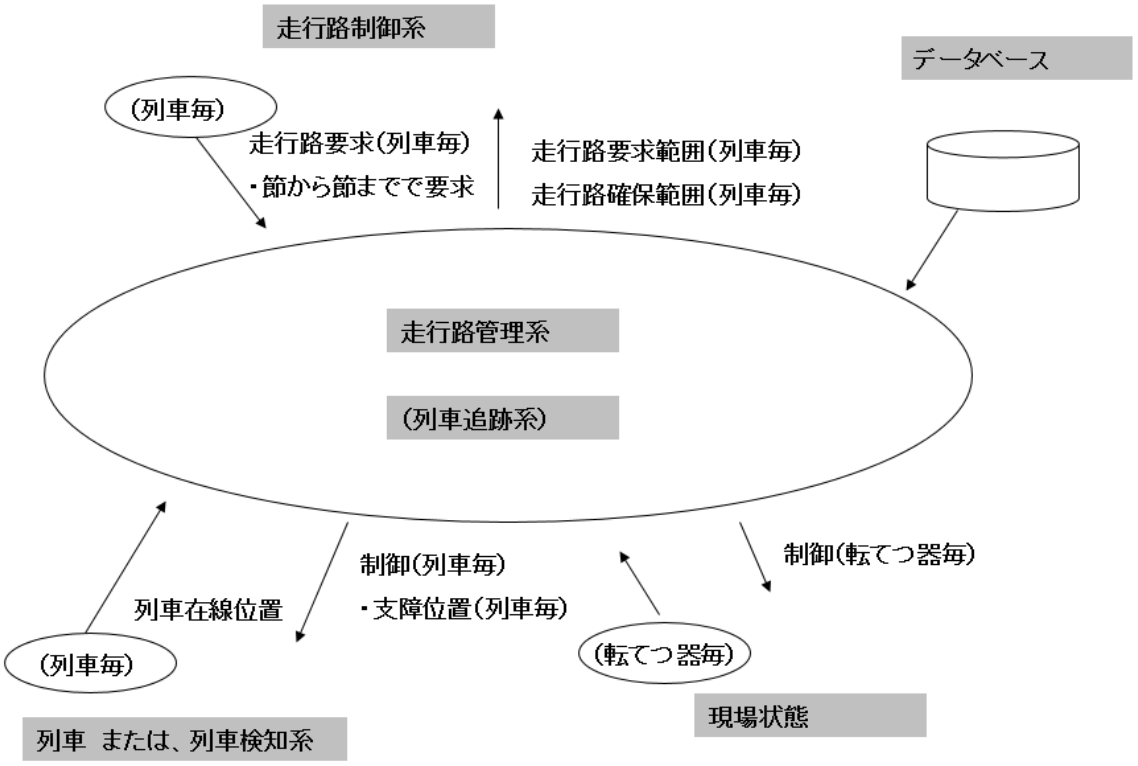


図　３-１５　保安を確保する論理

３.４.１　　処理の概要

連動装置の処理は図　３-１６に示す流れで行なわれる.

(1)走行路（走行路は発点から着点を意味する走行路名称で表現し，辺の集合として定義する）が要求される（走行路は列車単位で制御する）と該当走行路に対する走行路ステータステーブルが作成され,このテーブルを基に連動の処理が行なわれる（このテーブルは走行路要求が取り消されると消滅する）.

(2)走行路ステータステーブルには,走行路データテーブルを基に辺列が記載され,

要求に基づく列車毎の受付状態，線路形態データテーブルを基に転てつ機の制御状態を登録する．

また，支障点データテーブルと列車毎の支障点位置を基に，辺毎の走行路の許可範囲状態が登録される．

(3)転てつ機への制御は，転てつ機の制御状態に基づき転てつ機を制御し転てつ機からの表示状態を基に走行路の許可範囲が更新される．

(4)列車への制御は，許可範囲を基に直近の支障位置を列車に送ることで列車による間隔制御が行なわれる．

(5)列車進行に従い，列車の現在位置情報が更新され，列車毎の支障位置の更新に伴い，走行路ステータステーブルには，走行路の列車による支障位置の設置，走行路の解錠範囲の設定を行なう．

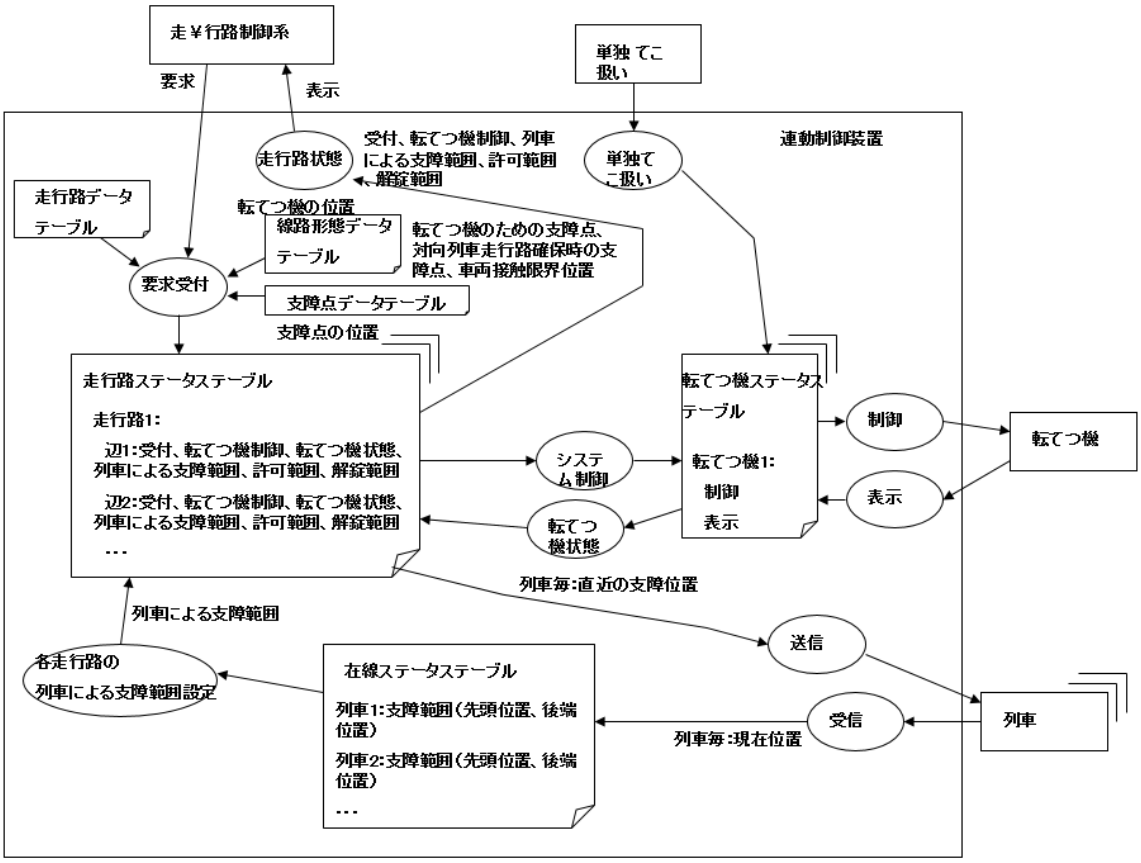


図 3-１６　連動装置の処理概念

３.４.２　　走行路要求

走行路は発点から着点までを意味する走行路名称で表現する．走行路の制御は走行路制御系からの制御（要求）により行なわれる．走行路制御系からの要求には列車 ID を伴って伝達されることとする．

(1) 走行路制御系の走行路要求は，「辺」から「辺」で定義し，要求は列車単位に行う．例えば，地点 a（始点）から地点 b（終点）までを要求する場合は，図　３-１７のように辺 A から辺 C と要求する．

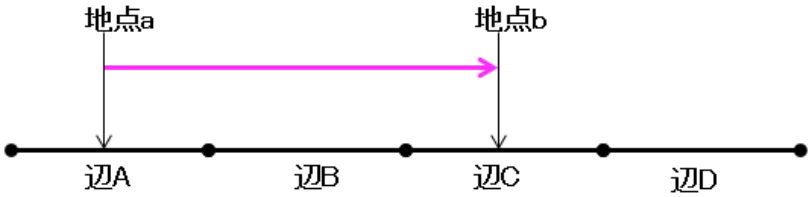


図　３-１７　走行路要求例

(2) 走行路管理系は，路線データベースを基に辺 A から辺 C の経路を検索し，途中に分岐がある場合は，分岐器の向きを指示する．ただし，要求は 1 分岐器単位とする．

(3) 走行路管理系は，要求された走行路上の支障点を確認し，直近の支障点までを該当列車に対し走行路を確保する．なお，走行路は，「該当列車の先頭から」，図　３-１８のように，既に確保されている走行路がある場合は「該当列車の確保された走行路の現在の着地点を追加で」終点の辺の節まで確保する．

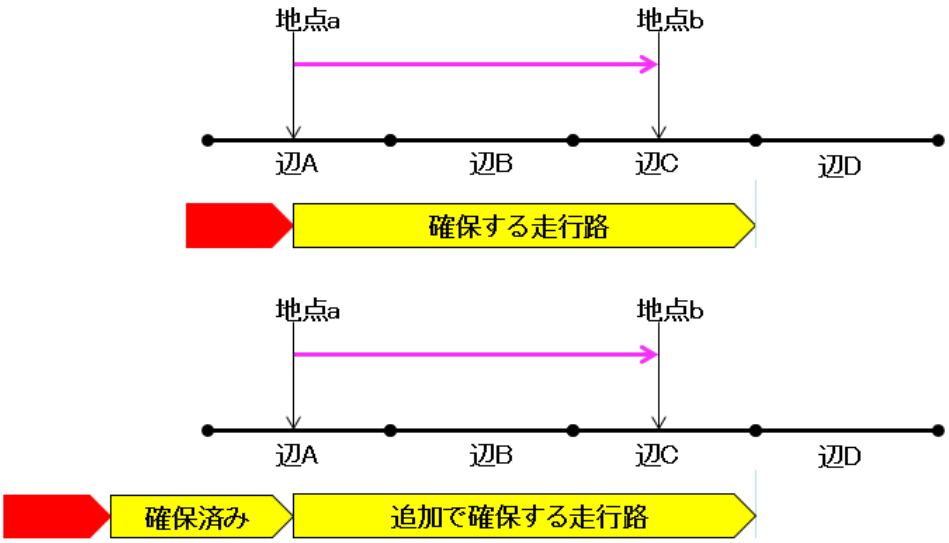


図　3-１８　走行路確保

３.４.３　　走行路検索と進入許可

走行路探索処理は表 ３-２のように，走行路テーブル，線路形態データテーブル，支障点データテーブル，在線ステータステーブルを基に行なう．走行路ステータステーブルは，現在設定中の走行路に関してのみ生成される．支障点は，前方列車の在線位置，転てつ機の状態（表示）により可変するものも含まれる．

表 ３-２　走行路要求に対する検索処理

レベル	処理内容	不合格の処理
探索０	走行路順序の適正チェック（デッドロックチェック）する．	デッドロックデータテーブル参照によるチェック
探索１	要求走行路名が走行路データテーブルにあるかないかのチェックをする．	走行路制御系に NG 返送
探索２	①走行路データテーブルから走行路ステータステーブルを作成する． ②線路形態データテーブルから走行路中の転てつ機の位置を抽出する． ③支障点データベースより分岐器のための支障点，対向列車走行路確保時の支障点，車両接触限界位置を抽出する． ④在線ステータステーブルより列車による支障範囲を抽出する．	

３.４.４　　転てつ機制御

転てつ制御は定周期で起動され，走行路に関係する転てつ機の制御が行なわれる．転てつ機の制御については，図 ３-１９のように要求走行路に基づき関連する転てつ機の制御を行う．

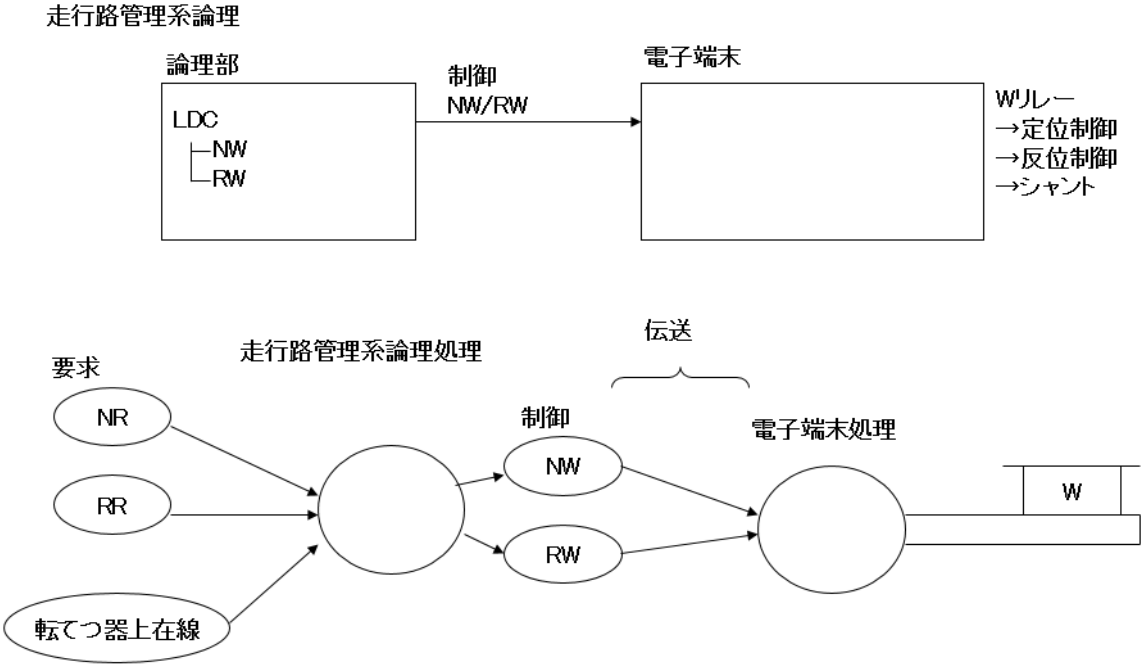


図 ３-１９　転てつ機制御シーケンス

(1)定位側に制御する場合：NR＝１，RR＝０

(2)反位側に制御する場合：RR＝１，NR＝０

(3)走行路が確保された状態では転てつ機を動かさないために，転てつ機制御リレー回路を遮断する．WLR＝０（常時 WLR＝１）

なお，転てつ機の状態は，以下の通りとする．

(1)定位側である状態：NK＝１，RK＝０

(2)反位側である状態：RK＝１，NK＝０

この状態について通常時と異常時についてタイムシーケンス図で表したものを図 3-２０，図 3-２１に示す.

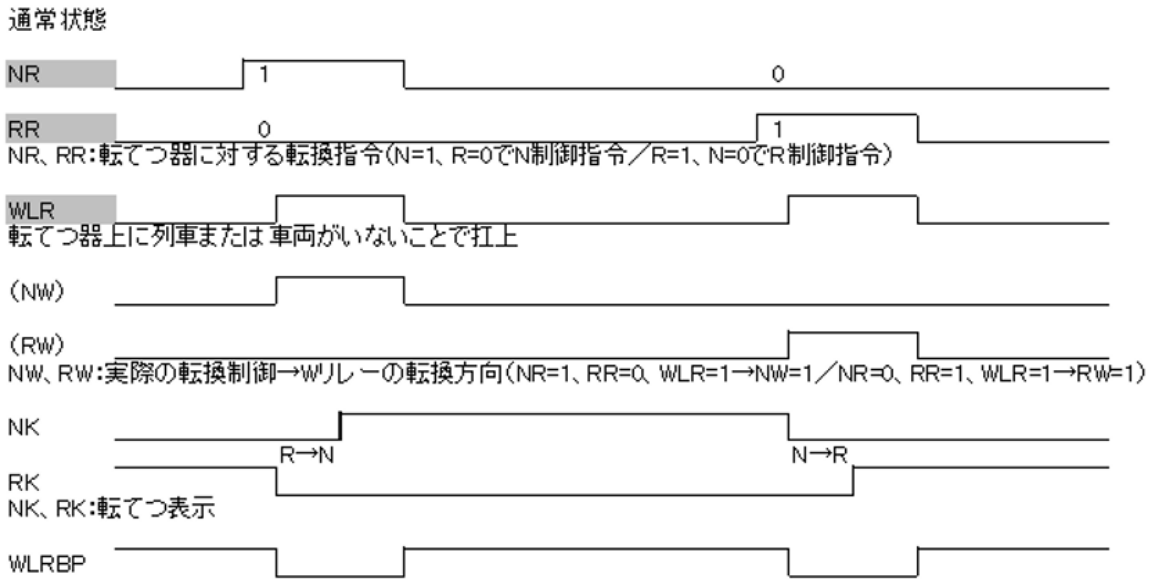


図 3-２０　転てつ機制御シーケンス（通常時）

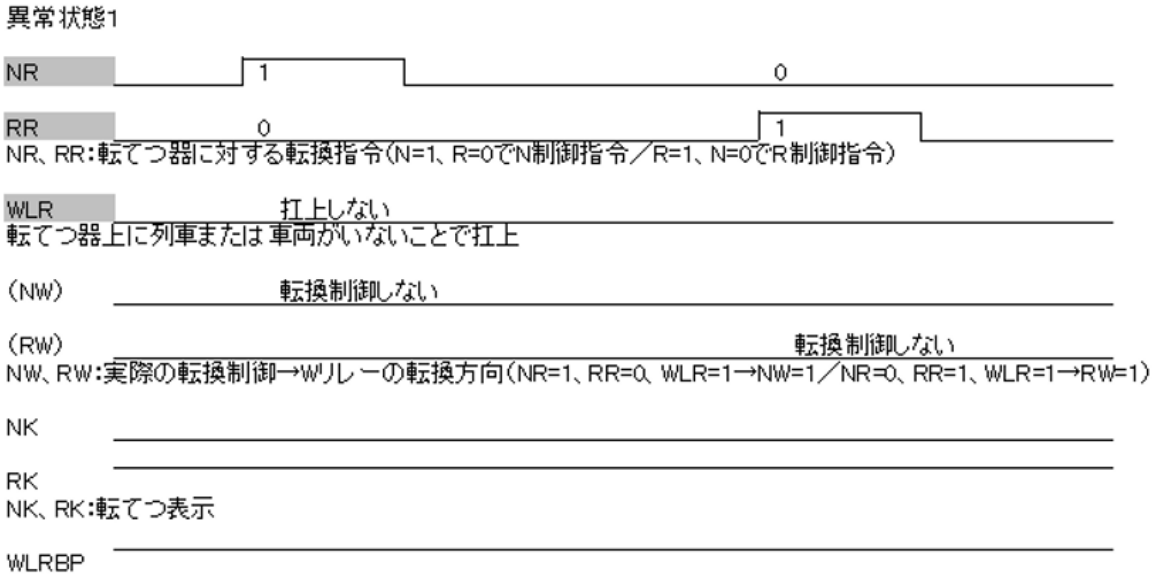


図 3-２１　転てつ機制御シーケンス（異常時）

このとき，分岐器についての支障点（前述支障点 N，C，R）は，図 3-２２及び図 3-２３，図 3-２４のように発生させることで効率的に列車制御における移動閉そくを実現できる．

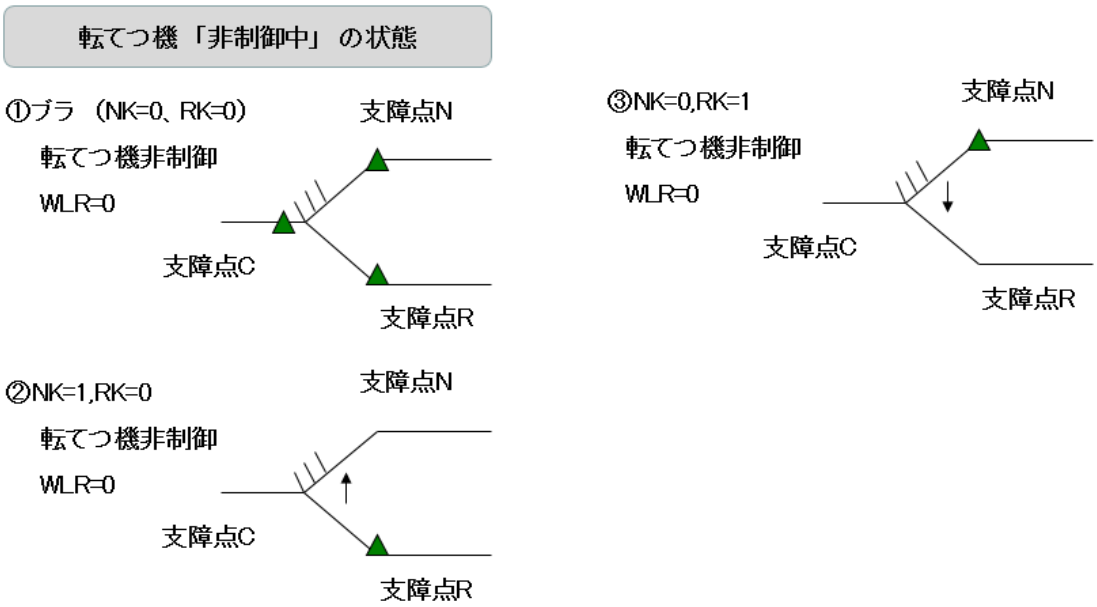


図 3-２２　分岐器による支障点発生（転てつ機非制御中）

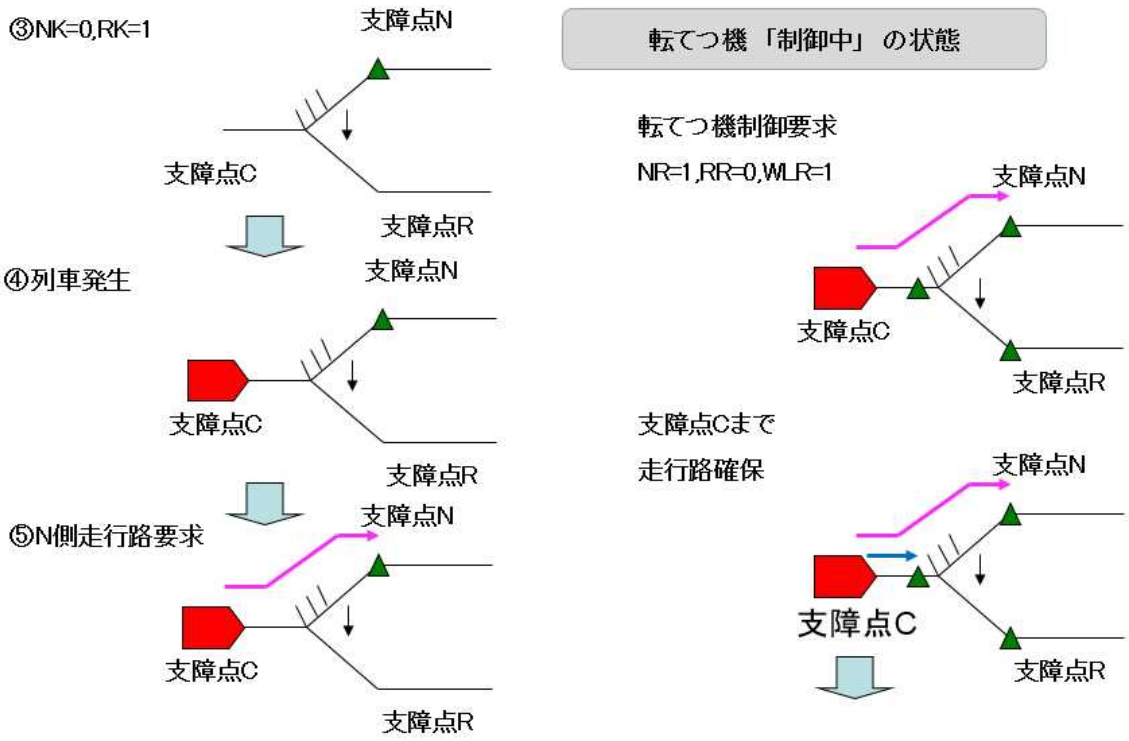


図　3-２３　分岐器による支障点発生（転てつ機制御中１）

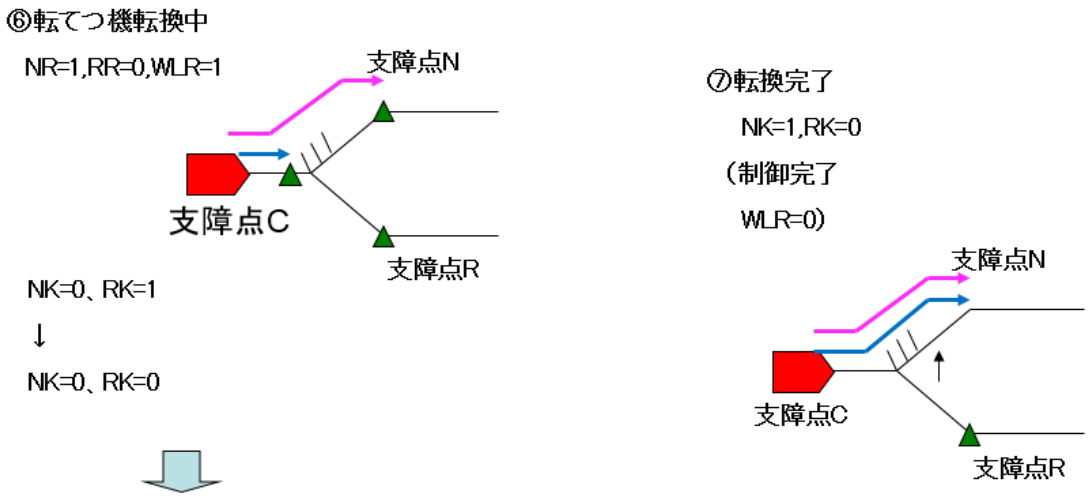


図　3-２４　分岐器による支障点発生（転てつ機制御中２）

３.４.５　　内方区間への移動

走行路は，列車毎に許可が与えられるため，該当列車の進行に伴い在線位置後方について解除を行なう．また，走行路は，列車毎に許可を行い，該当列車の在線位置を追跡する．

地上側の列車検知装置が車上装置から受信する列車位置は，列車先頭検出位置 Ph(t)のみである．位置算出処理では以下の式に従って，Ph(t)と列車長 L(t)との関係から，列車先頭補正値 Ldh(t)を加味したシステム上の列車先頭位置 Pth(t)，及び列車後端補正値 Ldr(t)を加味した，システム上の列車後端位置 Ptr(t)を算出する．図　3-２５に示す．

Pth＝xh＋Ldh＝xth

Ptr＝xh－(L＋Ldr)＝xtr

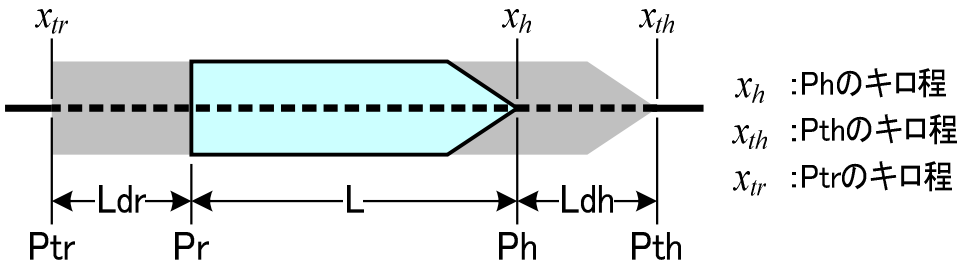


図　3-２５　Pth／Ptr の算出

列車検知の仕組みは，レール間を車軸で短絡することにより列車がその区間に在線することを検知する軌道回路方式と異なり車上の位置検知を基にする．このため，新交通で実現しているチェックイン・チェックアウト式[6]を応用した仕組みで実現する．

例えば，地上装置からの定周期ポーリング（500msec 以下）に対する車上装置が現在位置情報（列車先頭位置）を応答する伝送手順とした場合，仮に列車が

100km/h で走行した場合において，通信間隔 500msec に走行できる距離は 14m であるため，Pth／Ptr 間がこれ以上であれば実列車を追跡できるため，実質的に連続した列車の追跡ができることとなる．

この双方向の通信手順を使用して，地上装置は列車先頭位置の進入を監視することで，列車の進入を検知し，列車先頭から列車長分後ろにある列車後端位置が内方区間に移動したことを監視することにより列車の進出を検知するチェックイン・チェックアウト方式としている．

ここで考慮した点は，車軸短絡式の場合は，一旦車両が進入した区間で故障により車輪がなくなり列車検知が出来なくなることは考えられないが，チェックイン・チェックアウト方式では，車上装置の故障を考慮して一旦在線検知した列車検知リレーは，列車の確実な進出情報を当該区間への内方区間進入を検知するまで在線状態を維持する論理構成としていることである．

３.４.６　走行路復位

設定済みの走行路の復位は，原則として該当列車の走行に従い自動的に行なわれる．列車が進路に達しないうちに復位をする場合には，列車とのクローズドループが確立していることにより行なわれるものとする．

一旦確保した走行路について走行路解除要求があった場合は，走行路管理系は，列車が停止していることが確認できた場合，列車に停止指示を出した上で，解除要求のあった走行路確保を解除する．

列車が停止していることが確認できない場合，列車は急には止まれないので，急に解除してしまうと確保できている走行路を超えてしてしまう（信号冒進）ため図３-２６のように確保している走行路を解除しない．

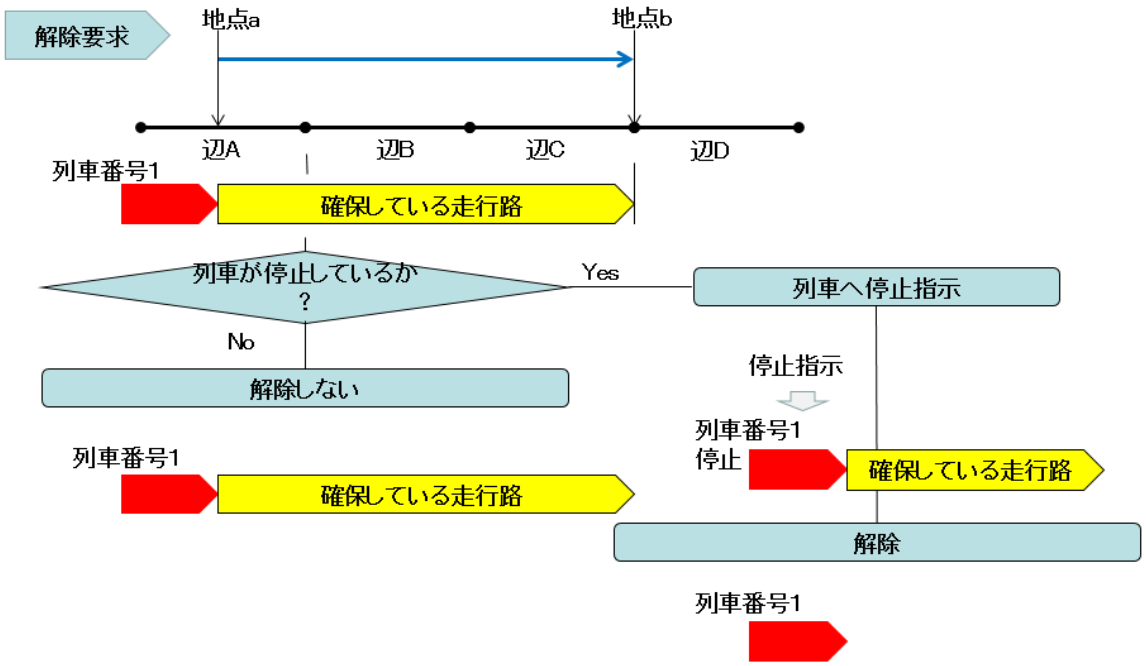


図　3-２６　要求解除

３.４.７　　その他

単独てこの扱いは，処理部で受け付けるか排除するかの処理を行う．また，デッドロックについては，走行路確保系は，走行路制御系よりデッドロックが起きない要求がくることを前提で処理を行う．ただし，走行路確保系は走行路制御系の持つデッドロックとなる条件テーブルを共有し，照査を行う機能は有する．

なお，踏切制御も走行路確保という見方をすれば走行路確保系の処理の一部となる．ただし，遮断機による道路側抑止は走行路確保という観点では不十分と考えられるため，クローズドループの考えなどを適用した踏切に関する議論は進める．（クローズドループとフラップの組み合わせなど）

ここまで，鉄道の連動機能の実現手法を述べたが，本方式は，鉄道の連動機能に留まらず，路面電車の運行制御システム等においても有効であると考えている．路面電車においては，道路交通信号機との連携が必要となるが，このような場合においては，図　3-２７に示すとおり，道路交通信号機の赤信号を支障点として設定することで同様に制御を実現できる．ただし，実現においては，直進・左折・右折でそれぞれ交通信号と支障点解除のタイミングを整理して仕様化すること，走行路を要

求後, 一度走行路が確保された後に, 旅客乗降に時間を要して出発出来なかったなどの理由により交通信号条件が変わってしまった場合, 確保した走行路を復位する条件などを整理する必要がある.

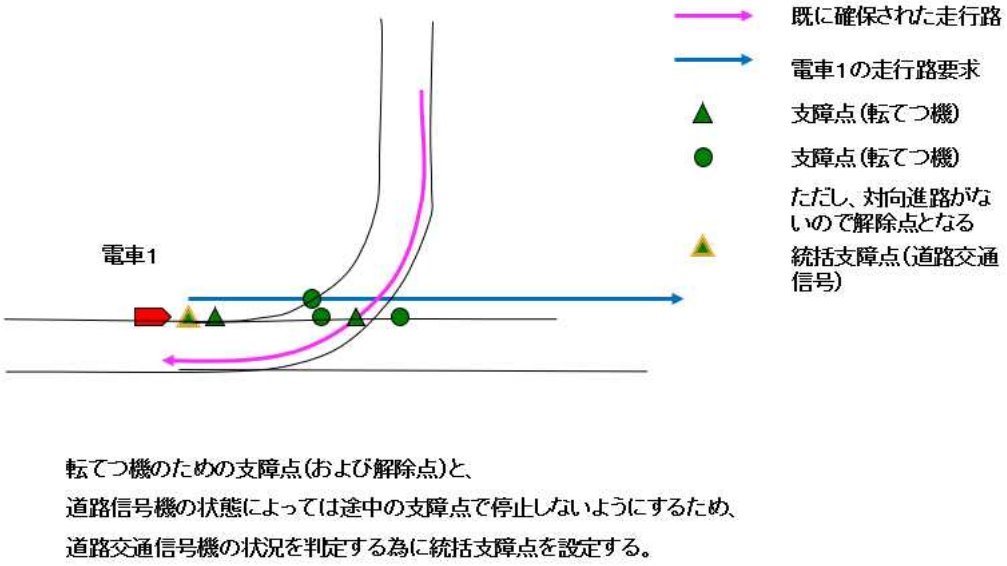


図 3-2 7　路面電車のための支障点拡張例

3.5　まとめ

本方式では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なったため, 駅構内においても運転効率の向上が可能となった.

さらに既存の連動装置で信号結線により実現していた鎖錠条件などは以下のように整理ができると考えられる.

従来，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信号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，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

４.１　はじめに

鉄道事故は 1830 年 9 月 15 日開業当日,鉄道の誕生の功労者ウィリアム・ハスキソン(William Huskisson) の代議士の人身事故から始まる.

鉄道の歴史は事故の歴史であと言われるように鉄道は多くの事故を経験しながら,安全性の向上を目標に各種装置で改善が行われ今日のシステムが形成された.

４.２　既存安全性評価の現状

今日までに形成された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ことから, 新しいシステムを評価する場合においても事故に至るシナリオが大きく変わることがない. このため, 安全性解析は基本的に完成したシステムや装置をイメージして評価が行われている. 要するにそのシステムやプロセスの構成要素に起こりうる故障モードを予測し, 考えられる原因や影響を事前に解析・評価する FMEA（Failure Mode and Effects Analysis）が重点的であり, その逆をたどる FTA（Fault Tree Analysis）は補足的に行っているのが, 一般的な状況である.

まず, FMEA による解析手法について説明する. FMEA はシステムやプロセスの構成要素に起こりうる故障モードに対し,その考えられる原因や影響を解析・評価することで設計上の問題点を摘出し, アクシデントの未然防止を図る手法であり, 「設計の不完全や潜在的な欠点を見出すために構成要素の故障モードとその上位アイテムへの影響を解析するボトムアップ解析手法である. 構成要素を単位としたシステム全体を表現する方法としてはハードウェアの構成ブロック図や, ソフトウェアの機能構成図を用いることが多い. ここでは, システムを構成する機能ブロック図を基に実施する例を示す. 図 ４-１に示すようなソフトウェアデータフロー図を作成し, その機能を対象に故障モードを設定し, その影響と防護策を明らかにする. さらにその防護策を施した上で, 当該故障が発生すると考えられる頻度・被害規模からリスク評価を行いリスクの受け入れ可否の判断を行う. このように, ブロック図に示された「機能」及び「入力・出力」のそれぞれの故障モードが起きた結果システムにどのような影響を及ぼすかの解析ができるため, 出来上がった装置

（組み立てたアルゴリズム）に対しての解析が行えるということが特徴となる.

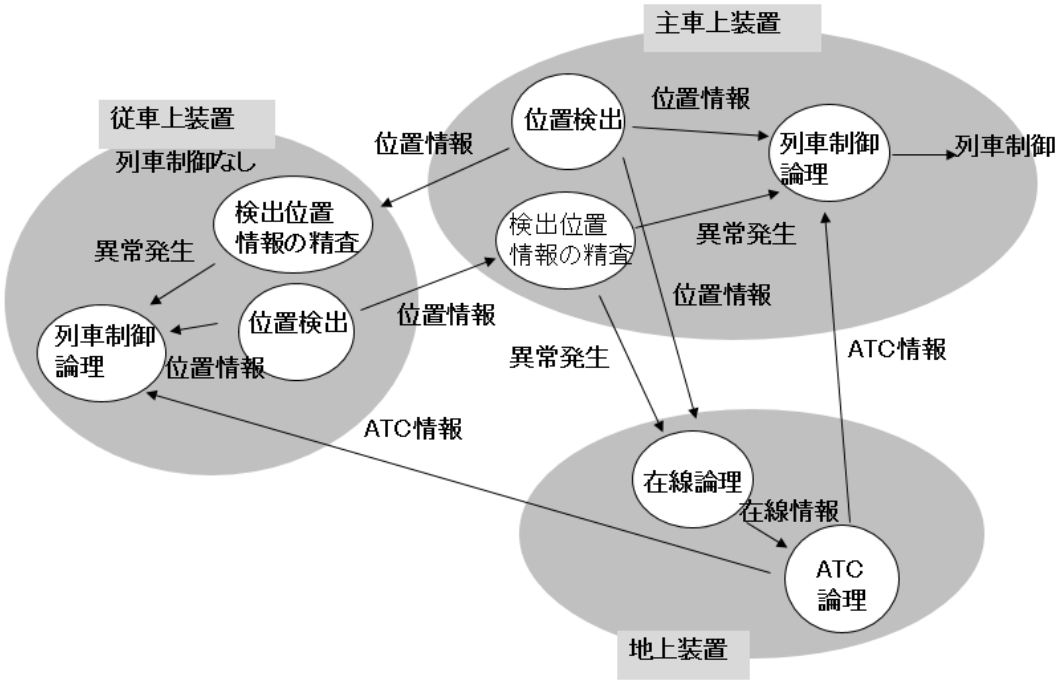


図 4-1　ソフトウェアデータフロー図

次に，FTA の解析手法について説明する．FTA は，アクシデントの発生頻度の分析のために, その原因の潜在的な機器の故障やヒューマンエラー等を論理的にたどり，それぞれの発生確率を加算し，アクシデントが起こりうる確率を算出する手法であり，望ましくない事象に対しその要因を探る，トップダウンの解析手法である．ここでは，例として既存の連動システムとして少進路型電子連動装置[7]を取り上げる. 少進路型電子連動装置とは少進路の駅向けに開発された連動装置である. 国内の連動駅のうち, 単線区間かつ 8 進路以下の駅はかなりの数を占めている．例えば, JR のある会社の場合, 連動駅の約 46%が 8 進路以下の駅であり, そのうち 83%が単線区間にあり, こういった駅に用いられる装置である.

この装置に対して錯誤現示に対する FTA 解析を行った事例を示す．図 4-2 はその FTA 図である.

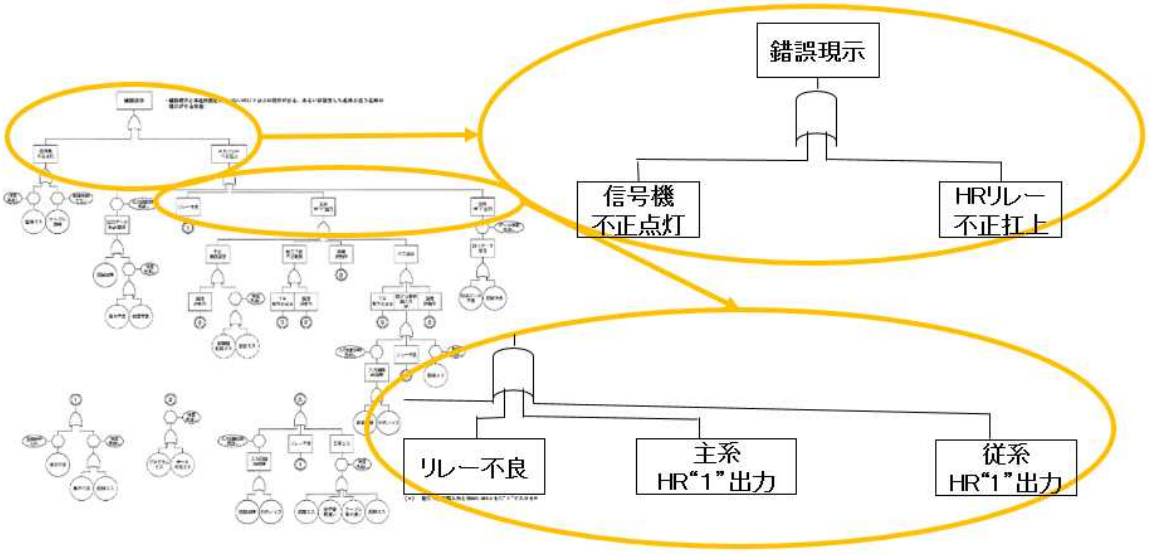


図 4-2　FTA の事例

この解析結果では，錯誤現示出力となる原因として，プログラムまたはデータの作成ミスによる論理誤動作，配線やケーブル取り違いによる工事ミス，入力回路や転てつ機の故障による転てつ表示の誤入力など，HR（Home signal Relay : 信号制御リレー）誤出力の原因となる多くの事象が抽出されている．

このように FTA 解析では，システムを設計するにあたりシステムが侵してはならない事象をトップ事象として，その要因を辿りシステムを構成する部品の故障の引き起こす経緯を示すことができることが特徴となる．

４.３　CBTC システムの FTA 解析の結果

前述の解析手法の特徴から新たに開発したシステムを解析するには, 構想設計段階ではトップダウン手法である FTA にてその思想の妥当性を確認することが,そして,具体的なシステムが完成した段階ではボトムアップ手法である FMEA にてその思想通り作られているかを確認する.

ここで新たに開発したシステムの解析事例として CBTC の事例として示す. CBTC は, 既存にないシステムであったため, 既存システムの構成を基にする解析ではなく, それを実現する本質的な概念から解析を進める必要がる. ここでは概念から FTA を描き CBTC について解析した結果を示す.

この際の解析結果の一例が図 ４-３である.

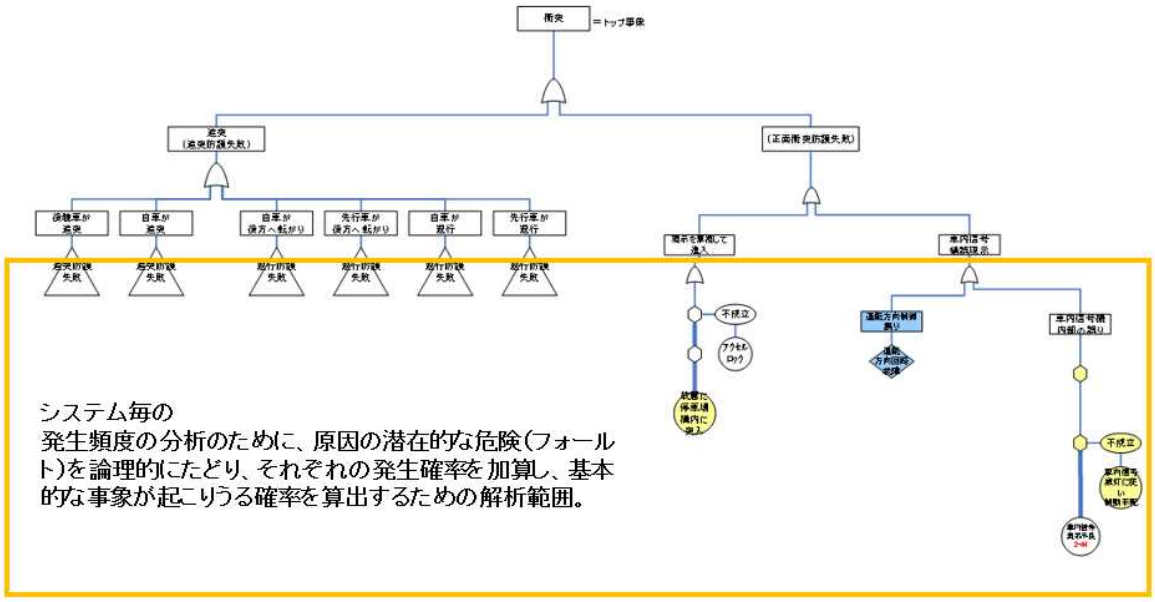


図 ４-３　CBTC の FTA 解析結果

この図の下部は, システム毎の発生頻度の分析のために, 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加算し，基本的な事象が起こりうる確率を算出するために使いやすい. この点で発生頻度の分析をするにあたり

FTA 図は整理しやすい.

前述のとおり, 既存の安全性解析は, 既に構成された装置をベースとして解析されることが多く, 外的要因やハードウェアに起因する故障や取扱いミスによる要因抽出に留まり, ソフトウェアの機能に関する要因の抽出をすることは難しい. ソフトウェアが運用段階で望ましくない状態, 特に致命的なソフトウェア故障を発生させないように, 開発プロセスのできるだけ初期段階で未然に防止対策を実施しておく必要性から同様にソフトウェアについても FTA を適用する例もあるが, ソフトウェアの安全性確保のための解析手法としては確立されていない.

これに対して, 上部は CBTC の概念に基づき, システムにおける致命的事象である「衝突」に至る原因は, 間隔制御の失敗による追突と運転方向制御失敗による正面衝突の 2 つと考え, この 2 つの事象に至る原因を細分化することで事故に至るシナリオとして分析を進めたものが図 4-4 である. この事例のように FTA で事象に至るシナリオを表現するまとめ方も可能である.

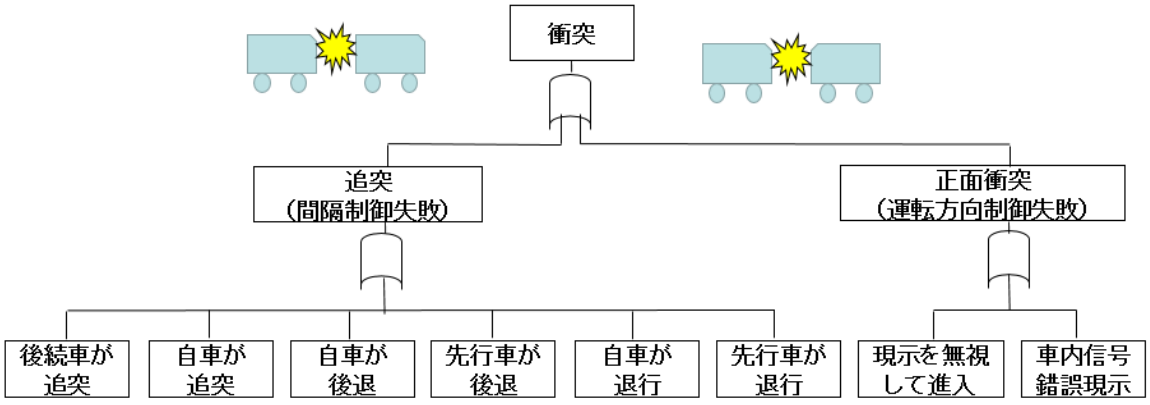


図 4-4 概念に基づく FTA 解析部分

さらに，これを，分岐部を含む列車制御における致命的事象である「列車異線進入時の衝突，脱線」をトップ事象として解析した結果が以下となる．

分岐部を含む列車制御における列車緯線進入の衝突，脱線事象は以下の４つの事象による．

(1)　停止している列車への衝突（衝突 1）

図　4－5 に示すような場面にて，前方列車に衝突する事象となる．

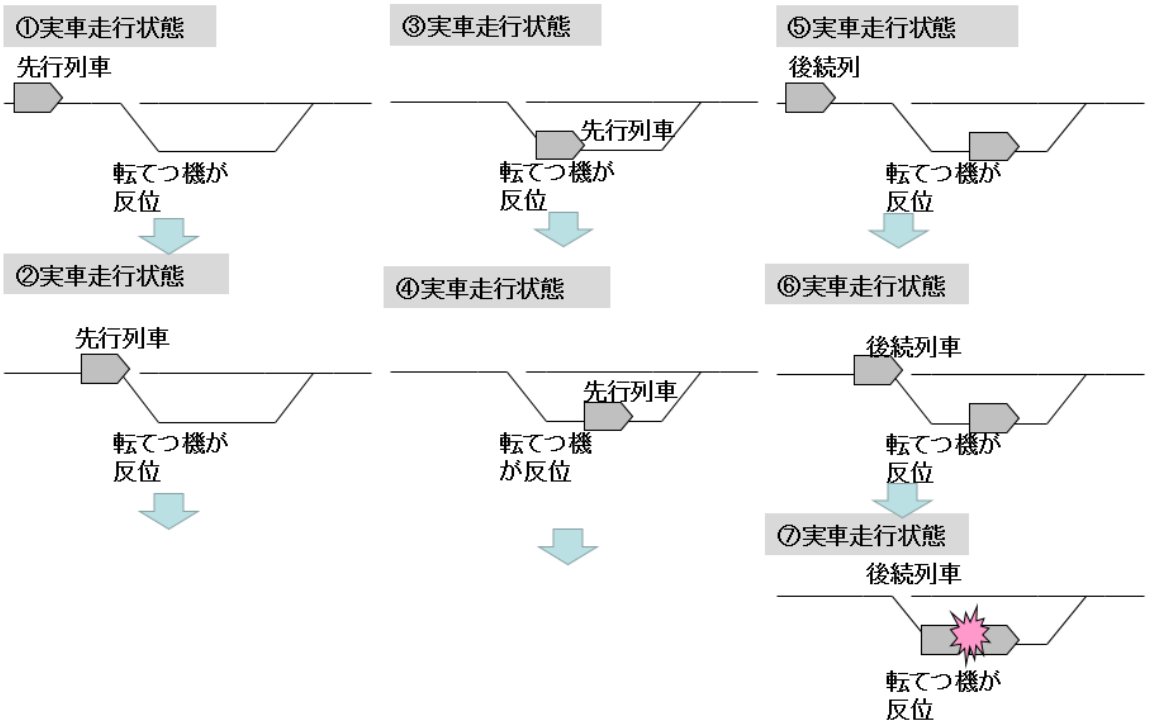


図　4-5　停止している列車への衝突

(2)　異線から出発した列車への衝突（衝突 2）

図　4-6 に示すような場面にて，位置検知誤差が蓄積しオーバーランすることにより異線から出発した列車への衝突（または，てっ査鎖錠不能による脱線）する事象となる．

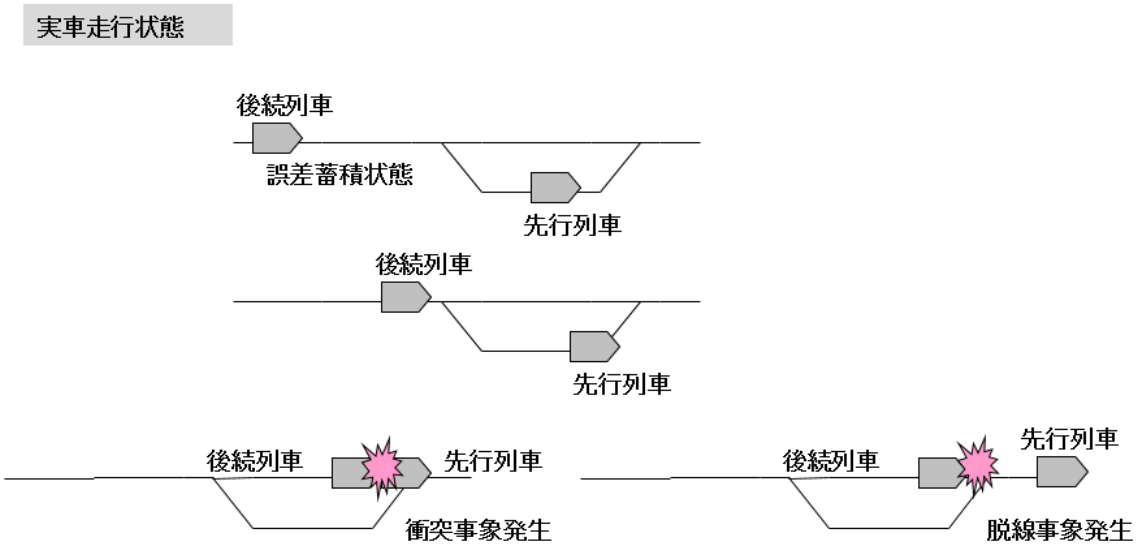


図 4-6　異線から出発した列車への衝突

(3)　転てつ機未開通方向へ進入し脱線（脱線 1）

図 4-7 に示すような場面にて，転てつ機の非開通方向へ進入し脱線する事象となる．

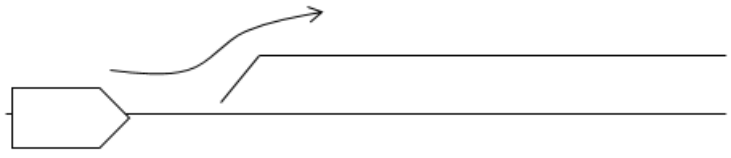


図 4-7　転てつ機未開通方向へ進入

(4)　本線と思い込み側線へ進入し脱線（脱線 2）

図 4-8 に示すような場面にて，本線進入していると思い込み副本線（制限速度がある側）へ進入し脱線する事象となる．

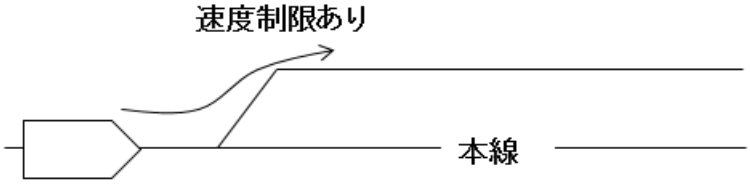


図 4-8　本線と思い込み側線へ進入

それぞれを FTA により解析した結果（衝突 1 に至る具体的事象）は図 4-9 であり，具体的には以下のような結果が得られた．

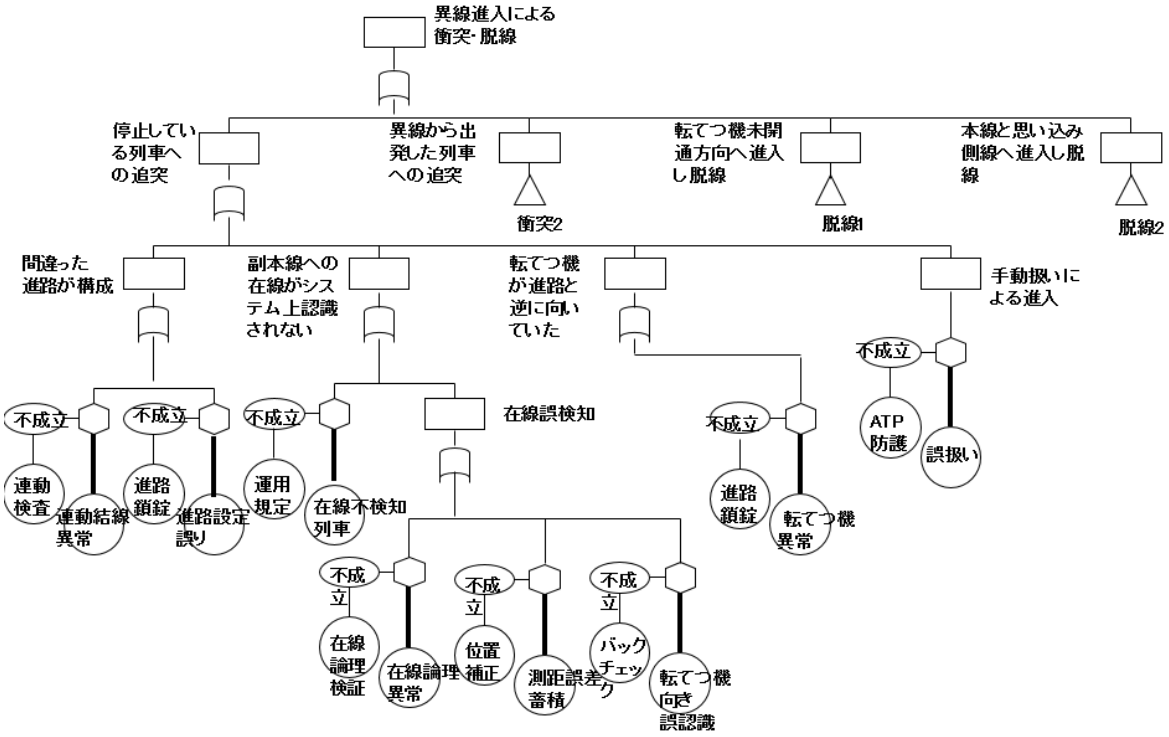


図 4-9　分岐器を含む FTA 解析（抜粋）

衝突 1 に至る具体的事象としては, 以下の 4 点が抽出されその原因事象が示された.

・間違った進路が構成された

・副本線への在線がシステム上認識されていない

・転てつ機が進路と逆に向いていた

・手動扱いにより進入した

同様に衝突 2 に至る具体的事象としては，以下の 4 点,

・間違った進路が構成された

・本線列車の在線がシステム上認識されていない

・位置検知誤差が蓄積しオーバーランした

・手動扱いにより進入した

脱線 1 に至る具体的事象としては，以下の 2 点,

・間違った進路が構成された

・手動扱いにより進入した

脱線 2 に至る具体的事象としては，以下の 2 点が示された.

・転てつ機の表示が間違っていた

・位置検知誤差が蓄積し既に副本線に進入していた

４.４　ソフトウェア安全性評価と STAMP

４.４.１　　STAMP の評価方法

ここまで，既存安全性評価の現状として，FMEA と FTA の特徴と，その特徴に基づき，構想段階の評価として CBTC システムの FTA 解析の結果を示した．鉄道は経験工学といわれるように，過去の事故やトラブルを教訓に安全性を高めてきた．しかし，それはあくまで経験であり，システムの安全性について本質的な観点から安全対策を行う必要があると考えられる．

こういった状況に対して，ソフトウェアによるシステムに対する安全性解析手法として，モジュールの相互作用とコントロールに着目したアクシデントモデル「STAMP」が Nancy. Leveson によって提唱されその有効性が注目されている[8]．

STAMP は，システムのメカニズム，テクノロジー，ヒューマンエラー，プロジェクト間の連携ミスなど，既存の FTA による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．

事故要因（ハザード）を事故が起きる前に特定するハザード分析は，STPA（System Theoretic Process Analysis）と呼ばれるハザード分析ツールをもって行われる．この STPA のハザード分析のプロセスは，以下の 4 つの段階に分かれている．

(1) 準備 1： アクシデント，ハザード，安全制約の識別

準備段階の最初のステップで，アクシデント，ハザード，安全制約の 3 つを作成する．これは，システムが回避すべき事象を事前に設定するもので，STPA Step1 で使用する．

・アクシデント（Accident）：喪失（Loss）を伴う，システムの事故.

・ハザード（Hazard）：アクシデントにつながるシステムの状態.

・安全制約（Safety Constraint）：システムが安全に保たれるために必要なルール.

⑵準備 2： 制御構造図の構築

制御構造図（Control Structure Diagram）は，システムを制御する各機能の相関関係を示した図であり，コンポーネント間でやり取りされる制御の指示やフィードバックなどを矢印で結んで表す.

⑶STPA Step1： UCA（Unsafe Control Action）の抽出

このステップは， ハザードにつながるおそれのある UCA を以下の 4 項目の観点で識別する.

・Not Provided：安全のためのコントロールアクション（Control Action）が設置されていない.
・Incorrectly Provided：ハザードにつながるおそれのある，安全ではないコントロールアクションが設置されている.
・Provided Too Early, Too Late, or Out of Sequence：コントロールアクションのタイミングが遅すぎる，早すぎる，または定められた順序に設置さていない.
・Stopped Too Soon：コントロールアクションがすぐに止まる，もしくは適用が長すぎる.

⑷STPA Step2： HCF（Hazard Causal Factor）の特定

STPA の最後の段階として，STPA Step 1 で識別した UCA の原因となる Causal factor と，予想される事故シナリオの特定を行う． 原因となる Causal factor は，コントロールループの流れにおいて予想される不備を示したもので以下の 11 項目の観点（11 個のガイドワード）で抽出する.

（Guideword No.1）上位からの指示や外部情報の誤り・欠落
（Guideword No.2）不十分なアルゴリズム（作成上の不具合，プロセス変更，不正確な修正・適応）
（Guideword No.3）プロセスモデルが不一致，不完全
（Guideword No.4）部品故障経時変化
（Guideword No.5）フィードバックの不十分・欠落・遅延
（Guideword No.6）不正確な情報，情報がない，測定の不正確さ，フィードバッ

クの遅延

(Guideword No.7)動作遅れ

(Guideword No.8) Control Action が不適切・無効・欠落

(Guideword No.9)プロセスへの入力の誤り・欠落

(Guideword No.10)意図しない，または範囲外の外乱

(Guideword No.11)プロセスからの出力の誤り

STAMP/STPA は, 既存のソフトウェアの安全性評価等に用いられる FTA や FMEA 手法と比べて，より合理的な評価が可能である．FTA はトップダウン的に致命的要因を抽出できるものの，それが，実際のソフトウェアモジュールのどのような故障によって発生するのかという問いには有効な答えが見出しえない問題があった．同様に，FMEA によるソフトウェアの評価は，作業量が膨大になるにもかかわらず, ソフトウェアの障害がどのように影響するかというシナリオの合理性についての懸念が払拭できないでいた．これらの課題について STAMP/STPA はソフトウェアモジュールの故障時のインタフェースの挙動から解析できるため, より説得力のある解析ができること，また，STAMP/STPA は定性的な安全性を評価できることが特徴である.

４.４.２　STAMP 評価方法のケーススタディ

STAMP の評価方法の有効性を検証するためにケーススタディとして鉄道信号システムの一つであり, 踏切道を通行する歩行者や自動車を列車との接触事故から守るための設備である踏切保安システムを事例に説明する.

４.４.２.１比較対象の鉄道信号システム

安全性評価の対象とする踏切制御システムの制御原理を次に紹介する.

(1)既存踏切制御システム[9]

制御が複雑な単線区間における踏切制御システムを図 ４-１０に示す. 踏切道を挟んだ遠方の両側に短小軌道回路を用いた上り列車用と下り列車用の始動点踏切制御子が配置される. いずれかの始動点に列車が進入すると，警報を開始するが，列車の進行方向（上り/下り）に応じて，踏切道を通過後に現れる反対側

の踏切制御子に対しては，その機能を抑止する必要がある．終止点踏切制御子は，踏切道の鳴動を停止し遮断桿を上げるためのものである．このほかに，遮断後に取り残された自動車などの障害物を検知する装置や，障害物検知時に運転士に伝え，いち早く停止操作を促すための踏切支障報知装置等が設置されている．

このように，既存踏切制御システムは，地上の踏切制御子で列車を検知し，処理を行い，万一危険なときには踏切支障報知装置により乗務員にその旨を伝えるもので，地上装置で処理が完結している．万一，踏切支障放置装置が障害物を検知しても，その情報に乗務員が気づかなければ衝突事故を防止することはできない．また，列車速度にかかわらず，列車が始動点に進入したときに制御を開始するため，鳴動開始から列車が到達するまでの時間に大きなばらつきを生じるといった課題もあった．

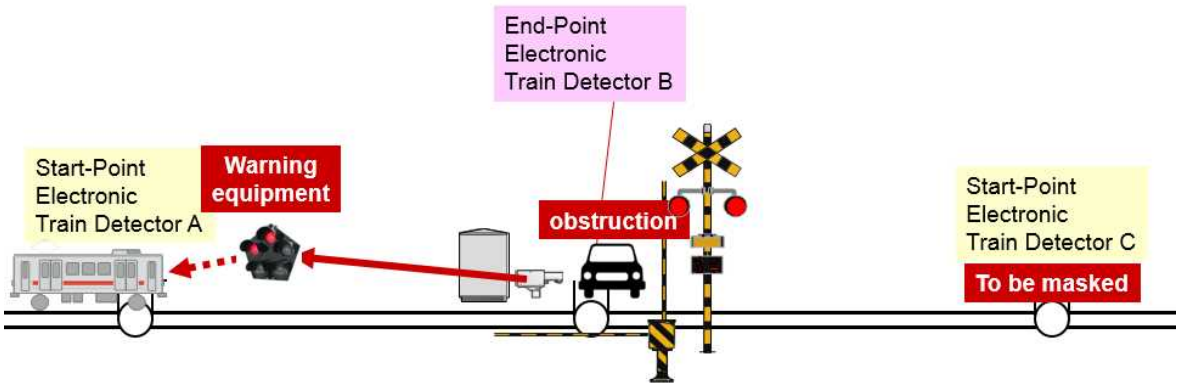


図　4-１０　既存踏切の構成

この弱点を克服し効率的な踏切制御を行うには，列車の位置だけでなく速度を含めた運転状況に応じて踏切道を制御することが有効で，車上と踏切制御部が情報交換を行いながら処理を行う，クローズドループ型の踏切制御方式が期待される．これまで，提案されたクローズドループ型踏切制御の 3 方式を紹介する．

(2) 分散制御方式

わが国最初の無線式列車制御システムとしてJR東日本の仙石線に導入された

ATACS (Advanced Train Administration and Communications System)では，分散制御方式のクローズドループ式踏切制御システムが開発され，実稼動している．順調に稼動しており，鳴動時分の短縮・均一化に効果があることが報告されている[10]．

ATACS は，沿線に配置した拠点制御装置がエリア内の列車の車上装置から走行位置と速度を受信し，車上装置に対し，走行可能地点を送信し，車上装置がその地点までの速度照査パターンを生成し，保安制御を行う．走行可能地点の終端は先行列車の後部に安全余裕をもった地点となるが，この間に踏切道がある場合には，踏切道の地点が走行可能地点とされる．列車が踏切道に接近すると，鳴動開始要求を，拠点制御装置を介して踏切制御装置に送信し，踏切制御装置から遮断完了し障害物がないことが伝達されたときに，踏切道を超えての走行を許可する．地上・車上の情報交換が失敗したときや，障害物が検出されたときには，踏切道までの停止パターンが生成されているので，踏切道の手前に停止する．

一方，沿線に処理装置を配置する分散制御方式に対し今日ではネットワーク技術，通信技術の進歩により，論理処理部をセンターに一元化する方式が可能となった．センター方式も，次に示す 2 つの方式が考えられる．

(3)集中逐次制御方式

分散制御方式の列車追跡及び，走行可能地点情報の作成及び伝達をセンターで行う方式では，踏切道の手前までを走行可能地点情報として，遮断完了かつ障害物なしの情報が得られたときに踏切道を超えて走行可能地点とすることで踏切制御を保安制御とリンクできる．集中逐次制御方式は，自列車の進行方向にある踏切道を列車走行に応じて逐次制御していくいもので，分散制御式の制御方法を，センターで一元的に実行しようとするものである．この制御方式は，分散制御方式と基本的には変わらない．ただ，全列車がセンターで管理できるため，群制御が実現でき，踏切制御の機能向上が可能になる．

(4)集中一括制御方式

集中一括制御方式は，DMV（Dual Mode Vehicle：道路とレールの両方を走行可能な新しい形態の交通機関である）の試験時に提案された方式で，図 4-1 1 に示すように，センター処理装置における列車位置情報管理に基づき踏切制御装置を制御する．

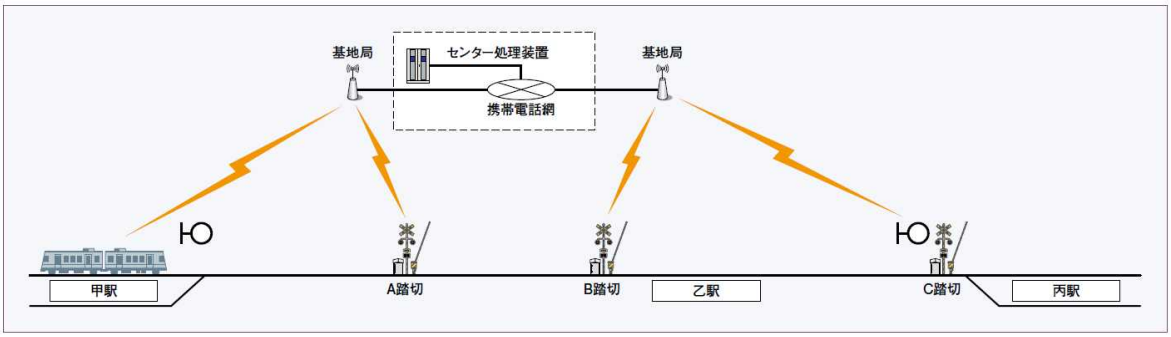


図　4-１１　集中一括制御方式による踏切制御システム

集中一括制御方式では，例えば図　4-１１に示す甲駅を出発する列車が丙駅まで運行するにあたり，駅間に存在する踏切道（A，B，C 踏切道）の踏切制御装置に対しセンター処理装置から警報開始のタイミングを指示する．なお，警報開始時刻は踏切道を列車が遮断機の無遮断状態で通過することを防ぐために列車が線区最高速度で走行した条件で算出する．列車の甲駅からの出発に際対しては，全踏切制御装置からの受信応答が確認されることが条件となる．

個々の踏切制御装置は，伝達された警報開始タイミングになったら警報開始を行う．

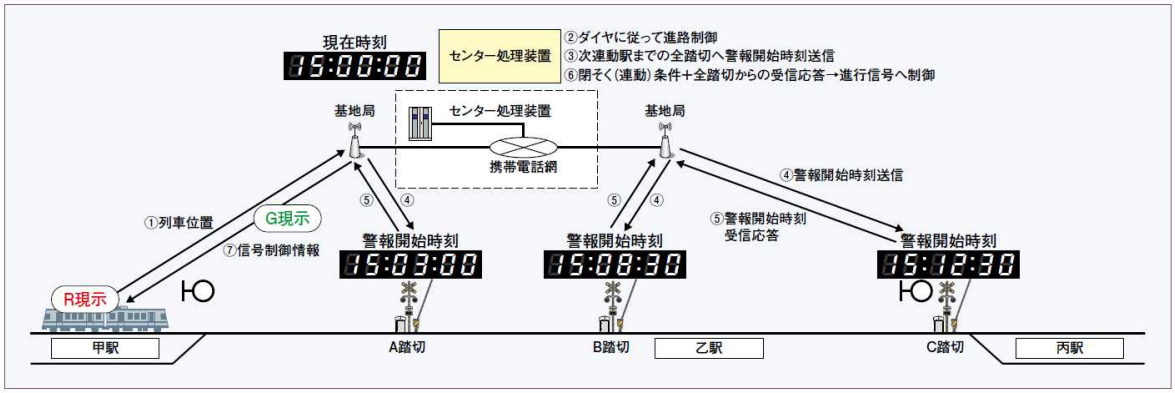


図　4-１２　警報開始時刻の設定

列車の現在位置と走行速度など走行状況により警報開始時刻も変化し得る. センター処理装置は，現在列車位置，速度情報に基づき，各踏切道に対して警報開始時刻の更新情報を送信することで, 常時最適な警報開始タイミングが与えられる．なお，踏切制御装置は，警報開始時刻のタイミングになると警報を開始し，一定時間後に踏切道を遮断, 障害物が無いことを確認するとセンター処理装置に通過 OK を送信する．この情報を受けてセンター処理装置は列車に対し，踏切道を越えた走行可能地点を探索し車上装置に送信する．この結果，集中逐次制御と同等の制御が可能となる.

なお，当該列車が踏切道を通過したことをセンター装置が知得すると，踏切制御装置に対して警報終止制御をする.

次に, これらの閉電路型踏切制御方式の安全性解析及び評価について検討する.

４.４.２.２既存踏切制御システムに対する STAMP 解析

図 ４-１０を用い，単線区間の点制御式の踏切システムについて説明する．列車検知に短小軌道回路式の踏切制御子を使用している，始動点の踏切制御子が列車の進入を検知すると，踏切道の鳴動を開始し，一定時間後に踏切遮断竿を降下させて踏切道を遮断する．列車が進入し，終止点の踏切制御子で列車を検知すると，鳴動を停止し遮断竿を上げる．なお，遮断完了後に障害物を検知したなら，特殊信号発光機により乗務員に告知して列車を停止させる．このシステムにおいては，乗務員が発光に気づくのが遅れ，衝突するといった事故がしばしば報告されている．このように既存制御システムは，地上側のセンサーと踏切制御装置の間で制御が行なわれ，万一の際には乗務員の注意力に安全性を委ねているのが特徴である．

既存制御システムについては，文献[11]に STAMP/STPA による解析事例があるが，解析は遮断までで終わっている．実際には，遮断完了時に障害物があるにもかかわらず，乗務員への伝達もしくは乗務員の認知が遅れ，事故につながるケースも多いため，本項ではこのケースも踏まえて解析を拡張した．

拡張分のケースについて登場人物を整理し，コントロールストラクチャを図 ４-１３のように定義した．

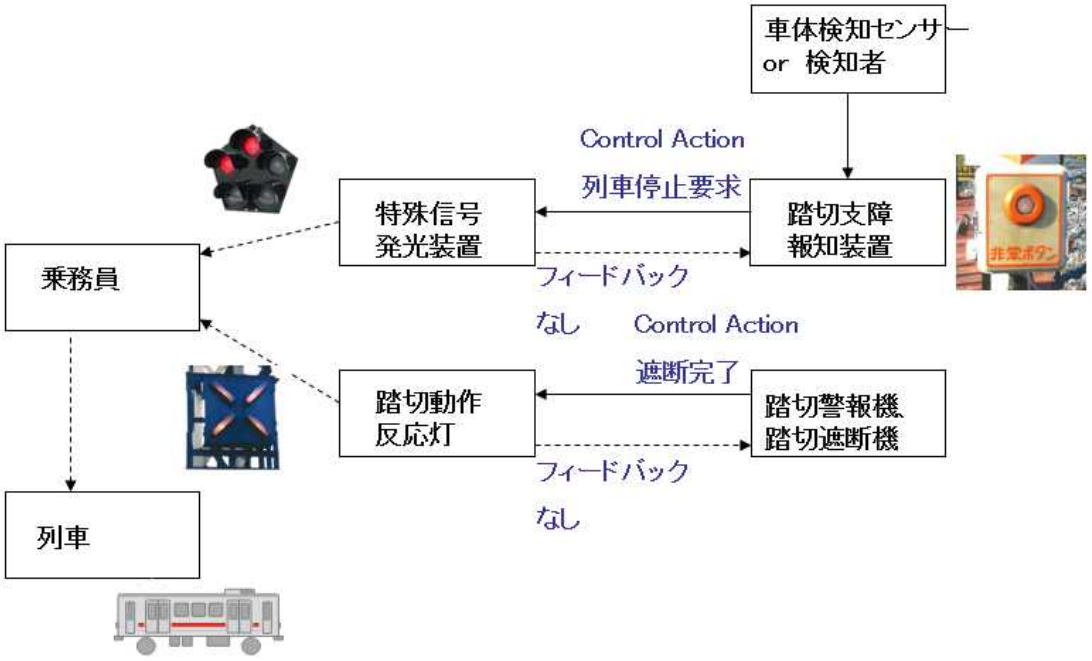


図 4-1 3　追加分のコントロールストラクチャ

この解析結果によると，文献[11]に抽出された 6 つの UCA（UCA1～6）のほかに追加分の 6 つの UCA（UCA7～12）で計 12 個の UCA が抽出された.

UCA1：警報が鳴らずに列車が踏切道を通過する．（踏切が閉まらない）

UCA2：遮断終了する前に列車が踏切道に到達する．（閉まるのが遅く，間に合わない）

UCA3：列車が踏切道を通過完了する前に鳴動停止する．（閉めた後，開くのが早すぎる）

UCA4：列車が来ないのにマスク指示し，警報鳴動しない．反対側の開始センサーにもマスク指示し，警報鳴動しない.

UCA5：開始センサーへのマスク指示が遅れ，列車の当該センサー通過に間に合わないと，マスク指示が残り，対向列車が 2 本続いたときに警報鳴動しない.

UCA6：列車が反対側の開始センサー通過後までマスク指示し続けると，対向列車が来ても鳴動しない．反対側センサーにマスク解除指示が出ず，対向列

車が来ても鳴動しない．（マスク指示後に列車が引き返す場合を含む）

UCA7：障害物があるのに発光要求が出ず特殊信号発光装置が点灯しない．

UCA8： 遮断が完了していないのに遮断完了が出て踏切動作反応灯が点灯する．

UCA9：発光要求が遅れて特殊信号発光装置の点灯が遅れる．

UCA10：発光信号認知からブレーキ操作までの時間が遅れる

UCA11： 遮断完了後に，障害物を検知し発光信号機を制御したが，タイミングが遅れブレーキ制御による制動距離を確保できない．

UCA12： 遮断完了している踏切道に列車が通過中にもかかわらず，障害物が進入した．

また，それぞれの UCA の原因となる Causal factor は文献[11]に挙げられた 17 個と追加分の 10 個を合わせ全部で 27 個挙がった．追加分の 10 個は以下の通りである．なお， UCA11，UCA12 については，踏切道横断者側の要因となるためシステム要因となる Causal factor の抽出はしなかった．

UCA7：停止要求が出ず特殊信号発光装置が点灯しない．

(Guideword No.1) 上位からの指示や外部情報の誤り・欠落

・センサーの未検知, 検知者の未扱いにより, 特殊信号発光装置が動作しない．

(Guideword No.2) 不十分な制御アルゴリズム/(Guideword No.4) 部品故障，経時変化

・停止要求処理に誤りがあり特殊信号発光装置を制御できない．

(Guideword No.9) プロセスからの入力の誤り・欠落

・特殊信号発光装置への要求誤りにより特殊信号発光装置が動作しない．

UCA8：遮断が完了していないのに遮断完了が出て踏切動作反応灯が点灯する．

(Guideword No.2) 不十分な制御アルゴリズム/(Guideword No.4) 部品故障，経時変化

・遮断完了処理に誤りがあり遮断していないのに踏切動作反応灯が点灯する．

(Guideword No.9) プロセスからの入力の誤り・欠落

・踏切動作反応灯への指示誤りにより遮断していないのに踏切動作反応灯が点灯する．

UCA9：発光要求が遅れて特殊信号発光装置の点灯が遅れる

(Guideword No.1) 上位からの指示や外部情報の誤り・欠落

・踏切支障報知機の指示遅れにより，特殊信号発光装置が遅れて点灯.

(Guideword No.2) 不十分な制御アルゴリズム/(Guideword No.4) 部品故障，経時変化

・停止要求処理に誤りがあり特殊信号発光装置を遅れて制御.

(Guideword No.7) 動作の遅れ

・踏切支障報知装置の処理遅れにより，特殊信号発光装置が遅れて点灯.

UCA10：発光信号認知からブレーキ操作までの時間が遅れる

(Guideword No.7) 動作の遅れ

・自動車の無謀横断により，設定した時間余裕が確保されない

・乗務員が他の運転操作との輻輳等により発光信号の認知が遅れ，ブレーキ操作が間に合わない.

この解析は，既存制御システムへ行ったものであり，これらの事故回避の最終的な手段は乗務員に委ねられている．このことが，遮断完了時に障害物があるにもかかわらず，乗務員への伝達もしくは乗務員による認知が遅れ，事故につながるケースが多いことに繋がっていると考えられる.

４.４.２.３クローズドループ式踏切システムの場合

(1) クローズドループ式踏切システムの評価結果

4.4.2.1 項(2)，(3)，(4) に示す各クローズドループ式踏切システムについて同様の解析を行った.

はじめに，コントロールストラクチャは，登場人物を整理し定義した．分散制御方式と集中逐次制御方式については，制御装置が沿線に分散されるか集中されるかの違いであるため，図 ４-１４のように定義した．また，集中一括制御方式は図 ４-１５のように定義した.

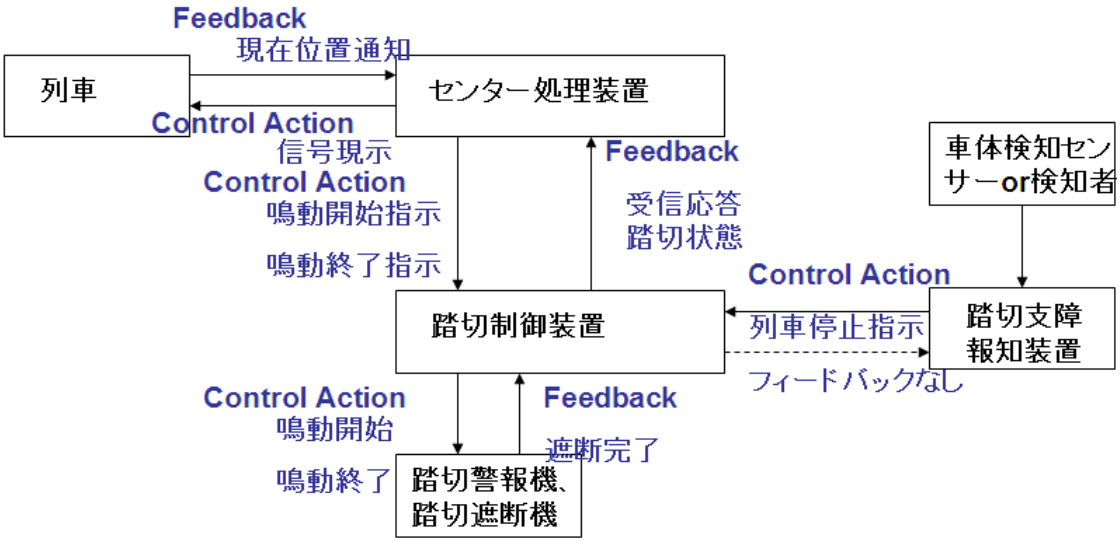


図　4-１４　分散制御方式と集中逐次制御方式

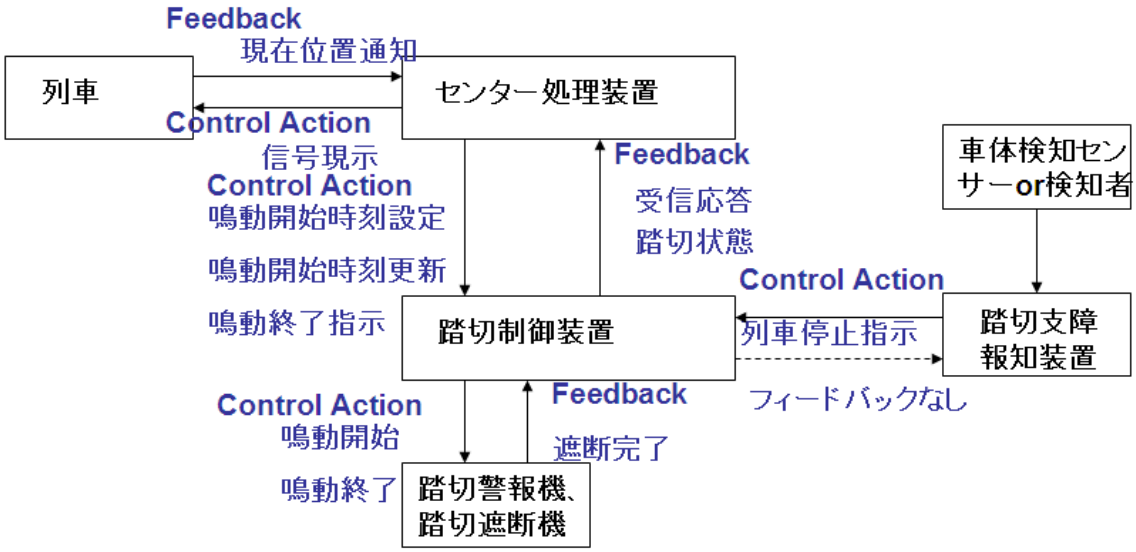


図　4-１５　集中一括制御方式

道路と線路の交差部での自動車と列車の衝突事故を防護するためのシステムで，物理的に衝突が起きるが，回避するために必要となるのが本来考えるべき道路と線路の交差部における事故回避システムである．この場合制御装置は，現在の状態に応じて列車または，自動車に対して衝突を回避する制御を行なうもので

あるため，コントロールストラクチャは図 4-16をベースに考えればよい．

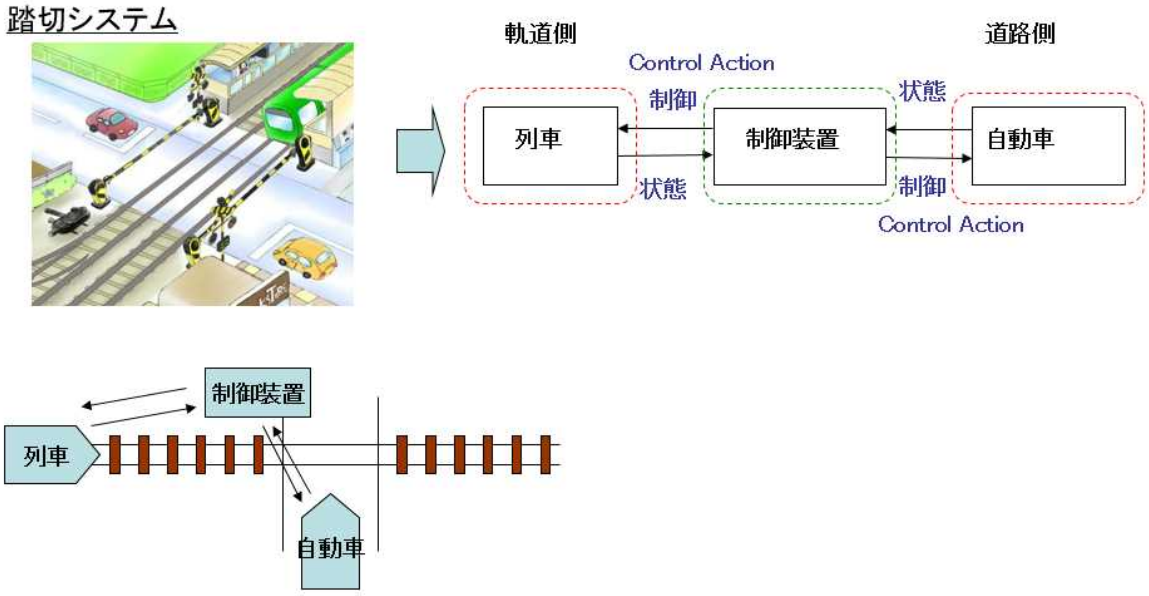


図 4-16　事故回避システムのコントロールストラクチャ

図 4-16をベースに各踏切制御システムに対して定義したコントロールストラクチャ（図 4-13，図 4-14，図 4-15）を整理すると，踏切制御システムは，自動車に対して直接的に制御を行なわず踏切遮断機，踏切障害物検知装置に事故回避対策を委ねていることが，また図 4-13を対象に整理すると既存制御システムは列車に直接的に制御できないので，列車に対する制御に対しての事故回避対策は乗務員に委ねられることになることが分かる．

次に分散制御方式・集中逐次制御方式と集中一括制御方式については，7つのUCA が抽出された．なお，抽出数には，既存制御システムと同様に制御遅れとして踏切道横断者側の要因となる2つの UCA を含んでいる．既存制御システムでは，始動点2箇所と終止点1箇所の制御子の列車検知条件を基に制御を行なうため，単線区間での上り下り列車の区別を行ない反対側の始動点の検知を無効にする仕組み(マスク処理)が必須であった．これに対し，クローズドループ式シス

テムでは列車の動きに対応してセンター処理装置が制御を行なうため，このようなマスク処理は不要となる．したがって，このマスク処理アクションに対するUCA の抽出も不要となる．

最後に，11 個のガイドワードをコントロールストラクチャにマッピングしたものが分散制御方式と集中逐次制御方式については図 4-17 で，集中一括制御方式は図 4-18 である．これを基に分析し既存制御システムと同様に事故シナリオを導出すると UCA の Causal Factor は，表 4-1 に示すとおり分散制御方式と集中逐次制御方式については 17 個，集中一括制御方式については 19 個となった．

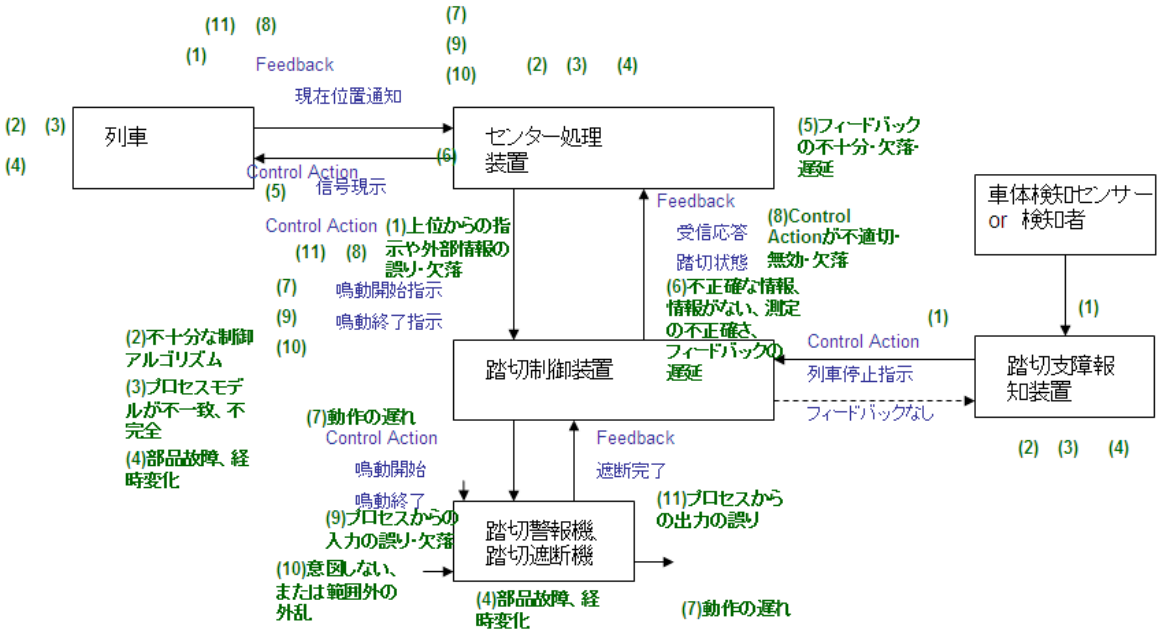


図 4-17　分散制御方式と集中逐次制御方式

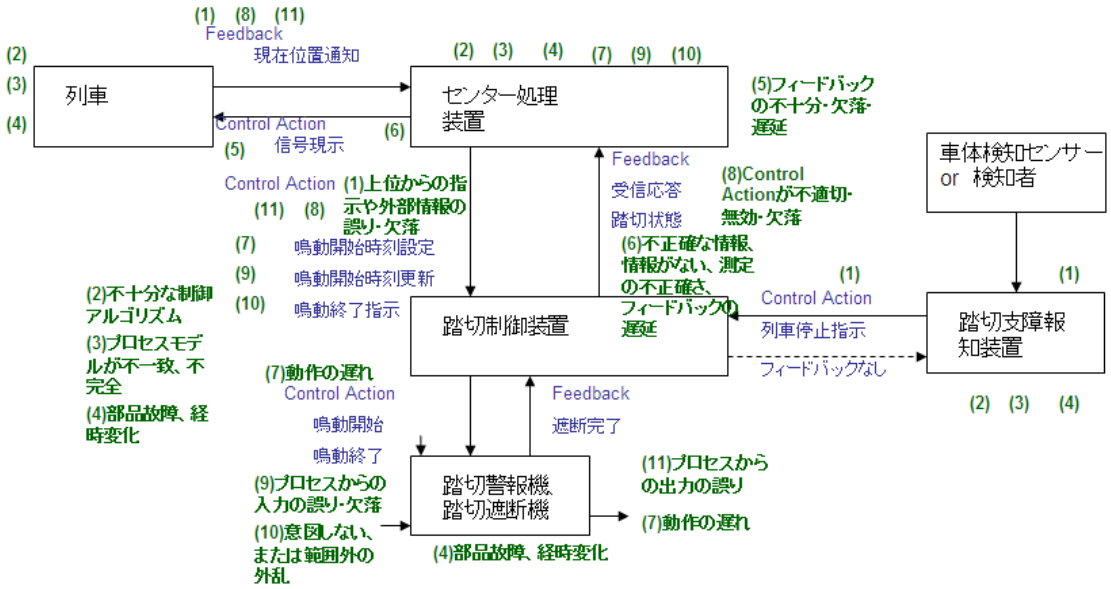


図 4-18 集中一括制御方式

表 4-1 UCA と Causal Factor

		閉電路制御式	
		分散制御方式と集中逐次制御方式	集中一括制御方式
UCA1	警報が鳴らずに列車が踏切を通過する. (踏切が閉まらない)	(1)踏切制御装置への指示誤りにより鳴動開始しない.	(1)踏切制御装置への鳴動開始時刻の設定誤りにより鳴動開始しない.
		-	(2)踏切制御装置の時間管理に誤りがあり設定時刻に制御できない.
		(4)踏切制御装置の制御部の部品故障により制御できない.	(4)踏切制御装置の時間管理部の部品故障により設定時刻に制御できない.
		-	(6)鳴動開始時刻が設定されていないのに受信応答を返したた

			め，開始時刻が設定されず，鳴動開始しない.
		(9)踏切制御装置への指示誤りにより，鳴動開始しない.	(9)踏切制御装置への時刻設定誤りにより，鳴動開始しない.
UCA2	警報鳴動開始する前に列車が踏切に到達する.（閉まるのが遅く，間に合わない）	(2)踏切制御装置の指示に誤りがあり制御できない.	(2)踏切制御装置の時間管理に誤りがあり設定時刻に制御できない.
		(4)踏切制御装置の制御部の部品故障により制御できない.	(4)踏切制御装置の時間管理部の部品故障により設定時刻に制御できない.
		(7)踏切警報機，踏切遮断機の動作遅れにより，閉まるのが間に合わない.	(7)踏切警報機，踏切遮断機の動作遅れにより，閉まるのが間に合わない.
UCA3	列車が踏切を通過完了する前に鳴動停止する.（閉めた後，開くのが早すぎる）	(1)鳴動終了の設定誤りにより，列車が通過中に鳴動停止する.	(1)鳴動終了の設定誤りにより，列車が通過中に鳴動停止する.
		(2)踏切制御装置の指示に誤りがあり誤ったタイミングに鳴動停止する.	(2)踏切制御装置の時間管理に誤りがあり誤った時刻に鳴動停止する.
		(4)踏切制御装置の制御部の部品故障により誤ったタイミングに鳴動停止.	(4)踏切制御装置の時間管理部の部品故障により誤った時刻に鳴動停止.
		(6)鳴動終了の設定がされていな	(6)鳴動終了の設定がされていな

		いのに受信応答を返したため，鳴動停止する.	いのに受信応答を返したため，鳴動停止する.
UCA4	停止指示が出ず列車に対して停止指示が出せない.	(1)センサーの未検知，検知者の未扱い.	(1)センサーの未検知，検知者の未扱い.
		(2)停止要求処理に誤りがあり制御できない.	(2)停止要求処理に誤りがあり制御できない.
		(4)停止要求処理部の部品故障により制御できない.	(4)停止要求処理部の部品故障により制御できない.
UCA5	停止指示が遅れて列車に対して停止指示が遅れる.	(1)踏切支障報知機の指示遅れにより制御が遅れる.	(1)踏切支障報知機の指示遅れにより制御が遅れる.
		(2)停止要求処理に誤りがあり遅れて制御が遅れる.	(2)停止要求処理に誤りがあり遅れて制御が遅れる.
		(4)停止要求処理部の部品故障により制御が遅れる.	(4)停止要求処理部の部品故障により制御が遅れる.
		(7)踏切支障報知装置の処理遅れにより停止制御が遅れる.	(7)踏切支障報知装置の処理遅れにより停止制御が遅れる.
UCA6	遮断完了後に，障害物を検知し発光信号機を制御したが，タイミングが遅れブレーキ制御による制動距離を確保できない.	※踏切道横断者側の要因となるためシステム要因となるCausal factorの抽出はしなかった.	

UCA7	遮断完了している踏切道に列車が通過中にもかかわらず，障害物が進入した.	

分析した結果について，ここでは対策には言及しないが，既存制御システムの場合は，各種センサ（制御子）の検知結果に基づき受動型制御を行なっているため，UCA の数が多いことにより予想される事故に至るシナリオが多岐に渡ることが分かる.

これに対して，クローズドループ式システムの場合は踏切支障報知装置を除いては，制御結果を常に監視しセンター処理装置と車上装置間で制御ループが確保される能動型制御のため，予想される事故に至るシナリオは制御実態がある踏切制御装置，踏切警報機，踏切遮断機に限定される.

このため，事故シナリオは時刻管理などの制御アルゴリズムに限定され，それ以外の不具合は列車が踏切道の前で停車する安全側への遷移となる．また，制御アルゴリズムは FS（Fail-Safe）-CPU による異常監視処理に基づくため，危険側故障確率は低く抑えられる.

クローズドループ式システムでは，踏切制御装置は遮断完了後，現場状況（踏切道内に障害物がないことなど）をセンター処理装置経由で車上装置に通知することにしている．車上装置は，安全が確認されない限り，踏切道を越えての走行を行なわない．安全性上不可欠なこの機能を前提にした上で，列車にブレーキがかからず，しかも，踏切の鳴動時分を確保する伝送タイミング等の最適化が求められる．これについて分散制御方式については，ATACS による踏切制御の実績の報告がある[10]．結果として，警報時間の短縮効果について報告されている.

またクローズドループ式システムの分析における Causal Factor 数 2 個の違いは，集中一括制御方式では，分散制御方式・集中逐次制御方式にはない時間管理部に起因する要因が挙がったことによる．逆に，集中一括制御方式では始動点通過に係らず制御上は無遮断への対応を検討する必要がほぼないが，分散制御方

式・集中逐次制御方式については，始動点通過後の無遮断対策に対する要因が挙がったことによる．

⑵STAMP/STPA による評価の有効性

運輸安全委員会が調査した踏切障害事故（2001 年 10 月から 2016 年 7 月公表分まで）としては，68 件の報告がある．このうち，障害物検知装置が設置されていた 17 件の要因別事故発生確率は以下の通りである．

・踏切道内停滞で特殊信号発光機動作しないもの：11%
・踏切道内停滞で特殊信号発光機動作したもの：23%
・直前横断（踏切道横断者側の問題）：47%
・側面衝突（踏切道横断者側の問題）：17%

この発生確率を抽出された UCA について発生確率を割り振り定量的な評価を行うと，実際にはほぼあり得ない事項と，重要な事項に UCA が分類できる（図４-１９）．

具体的には，既存制御システムにおける UCA1～UCA6 及び UCA8 は，STAMP/STPA としては抽出されるものの，現実的には無視し得る事象である．一方，UCA7 が 11%，UCA9 が 23%，UCA10,11 が 47%，UCA12 が 17%であり，注視すべき事象となる．このように，STAMP が UCA 抽出の網羅性に優れるという特長も，有効な UCA であるか，単なる方法論による抽出であり実際には無視できるものかの弁別がなされなければ意味がない．

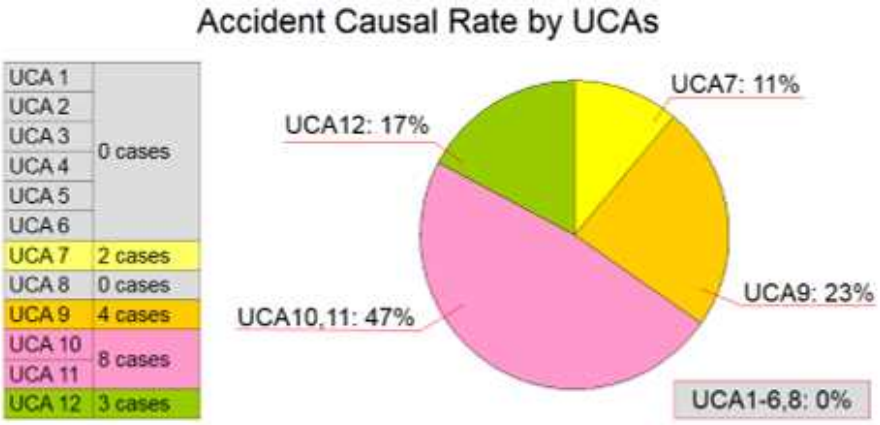


図 4-19　抽出した UCA に対する事故統計との関係

また，実際に事故に結びついた注視すべき UCA について分析すると，UCA7 については，踏切支障報知装置の検知性能によるものであるため，検知性能の向上がなされなければクローズドループ式システムでも対処できない．これに対して，UCA9 については，乗務員に安全性を委ねる既存制御システムでは限界があるものの，クローズドループ式システムでは，踏切道の通過が許容されないためシステムにより防護できると見なせる．　UCA10,11 については，UCA9 の場合と同様，クローズドループ式システムでは，障害物なしが確認できなければ停止パターンが消去されず，踏切道を越えての走行ができないため，原理的にはシステムにより防護できる．しかし，遮断竿を折ってまで無謀進入する自動車に対しては防護できない．上述の踏切障害事故の直前横断（踏切の踏切警報機が鳴動し遮断かんが降下していたにもかかわらず，自動車が列車の通過直前に踏切に進入した場合）について分類した 8 件のうち，1 件（直前横断の 12.5%）は乗務員の認知が踏切道へ進入していることの認知なので閉電路制御化で防護が出来る可能性がある．一方，残りの 7 件（直前横断の 87.5%）は，列車走行時速 70～100km/h で，踏切道からの距離が 190m 以内で障害物の進入を乗務員が認知している状況である．このタイミングで制御が行われるならクローズドループ式システムでも回避は難しいと考えられる．この対策としては，遮断完了後に横断者が踏切道へ進入できない仕組み（ロシアの一部踏切に導入されているようなフラップ等のバリアで進入防止を図るなど）の構築や，ITS（Intelligent Transport Systems：

高度道路交通システム）と連携し道路側からの進入者に対する制御の仕組みを取り入れることなどが必要となる．また，この対策を施せば，UCA12 に対しても事故防止が期待できる．

以上，クローズドループ式システムを導入するなら，17 件の事故のうち 7 件が救済可能となることが分かった．また，クローズドループ式システムでも分散制御式と集中制御式では，論理部の数が異なる．分散制御式の台数を n とすると，論理部故障に伴う誤制御は，分散制御式の場合 n 倍となるので，この点についても吟味する必要がある．ただ，クローズドループ式システムの場合には，メッセージのやり取りが成立して，順次処理フェーズが移行することと，処理の遅滞やメッセージの欠落がすべて「踏切道手前までの停止パターンが解除されない」という安全側の方向に作用する．従って，この前提下での論理部に起因する危険側事象は，条件が整わないにもかかわらず遮断 OK，障害物なしとしてパターン消去のメッセージを出すという論理部ソフトウェアの誤りによるものしか考えられない．この事象に対しては，実際には事前の入念な試験等で対処できるため，UCA1～UCA6 と同様に UCA として抽出されても，無視できるものと考えられる．

この踏切制御システムの解析により，STAMP/STPA はソフトウェアモジュールの故障時のインタフェースの挙動から解析できるため，より説得力のある解析ができるが，ケースとして詳細に列挙し，項目として抽出した UCA に対し発生確率を過去の事故統計を根拠として評価した．その結果， UCA としては抽出されたが実際にはあり得ないものと，現実に考え得る注視すべき UCA とが区別なく評価されるという STAMP/STPA 利用上の課題も認識できた．

４.５　まとめ

本章では, まず, システムの安全性評価に使用される FMEA, FTA, STAMP にはそれぞれ特徴があることを示した．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 などの自己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.

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

５.１　STAMP/STPA と FTA 解析の融合

ここまで, STAMP/STPA と FTA の解析事例を示してきた.

STAMP/STPA は, Step0 から Step2 を行うことでトップ事象からシナリオまでをつながりを持ち, 網羅的に導き出すことができるものの，解析した結果が自然言語によるシナリオ方式であるためハザードログでまとめたとしても発生頻度の分析として結果を整理することが難しい．また FTA は, 機能モジュールの機能不具合だけでなく, STAMP 同様概念から解析を行うことも可能ではあるが，STAMP/STPA のような手順が明確でないためこの網羅性の観点から劣る．このことら，トップダウンによる解析方法として STAMP/STPA か FTA かという 2 者択一するのではなく，それぞれの優位点を活用するということが重要である.

また，安全性解析を進める上で, 国際市場において製品・システムの安全性を示すためには, 国際的に広く産業界で用いられているリスクベースの設計に基づいて安全なシステムを構築することが求められる. リスクベースの設計手法においては, ハザードの抽出・リスクの評価を行い, そのリスクが受け入れ可能かどうかについて, ALARP 原理（As Low As Reasonably Practicable）に基づいて決定する. 鉄道分野でも，製品の開発段階から使用段階を経て製品寿命が尽きるまでのライフサイクルに渡って，信頼性, アベイラビリティ, 保全性，及び安全性について総合評価し，それぞれの目標とするところを達成しようとする鉄道の国際規格 RAMS の中でこの考え方が示されている．RAMS 規格では数量的評価を求められている.

このことから, STAMP/STPA にて FTA のように安全性の定量的評価ができるように拡張することを考えた．この方法論について以下に述べる.

この方法論について模式化したものが図 5-1 である. 概念図に基づく解析により結果の網羅性を示せる STAMP 解析の結果は, 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かった. これに対して, 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した結果を, FTA に引き継ぎシステム毎の発生頻度の分析のために，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加算し，起こしてはならない事象が起こりうる確率を算出することにより STAMP/STPA の結果も定量的解析ができるようにした．これにより，ALARP 原理に基づき決定されるリスク受け入れ可能性についても評価が可能とした．

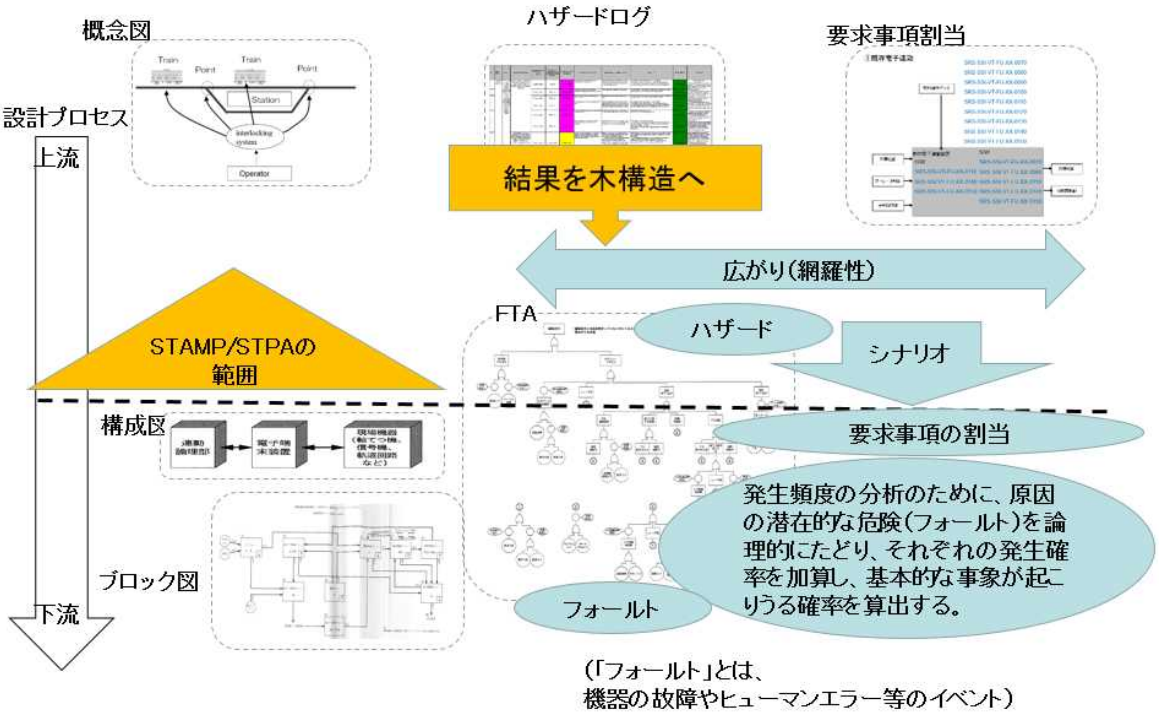


図 5-1　STAMP/STPA と FTA の融合

この方法論にて，連動装置の STAMP/STPA で解析した結果における安全性要求事項の一つ「進行許可制御を監視し，異常時は安全側に制御する」と，少進路形電子連動装置の FTA 図（錯誤現示）を繋げることで，STAMP/STPA で解析した「起こしてはいけない事象」からその背景に基づく事象が起こり得るシナリオ，そして FTA で解析した要因（機能モジュールの不具合）を一つの FTA 図に表すこともできる．これを基に発生頻度の分析を行うことを行うことで STAMP ではできなかった機能モジュールの不具合も含めた定量分析が可能となる．また，その他の要求事項（事例で示す連動装置に対する STAMP/STPA の解析結果では 10 個）についても同様に分析することで FTA では示すことが難しかった解析の網羅性（広

がり）を確保することもできることが分かった.

５.２　新しい安全性評価手法

リスク分析の流れに沿って STAMP/STPA で実施する内容を当てはめる流れを述べてきたが，鉄道の国際規格 RAMS では，リスク分析に対し，継続的なリスクマネジメントプロセスを確立することを求めている．ハザードの検出及び解析は，システムに潜在する固有のハザードやそれに誘発される事故事象または最終的な事故を引き起こすに至る要因を検出する過程で重要な部分となる．この過程は，プロジェクトの初期段階で開始され，それぞれのライフサイクルの段階で繰り返し実施され，網羅的にハザードを取り除き，潜在するリスクを軽減することである.

STAPM/STPA の解析結果は，ハザードに対して，図 5-7 のようなシナリオの形で表現されるが，ハザードと原因の関係が整理しづらい.

この課題を解決するためにハザード管理ツール（ハザードログ）として図 5-2 に示すリスク管理表を用いて結果を管理することを提案する. 管理表を整備する目的は, 全ての検出したハザードを記録すること及び追跡することである.

一方, 解析手法として取り上げた STAMP/STPA は既存の 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や構成要素間のインタフェースの齟齬に起因する事故原因をソフトウェアモジュールの故障時のインタフェースの挙動から解析できるため，より説得力のある解析ができるが，ハザードを引き起こす安全ではない制御指示としては抽出されたが実際にはあり得ないものと，現実に考え得る注視すべきものとが区別なく評価されるという STAMP/STPA 利用上の課題もある.

このことから，鉄道の国際規格 RAMS のリスク分析手法に求められるリスクベースの設計手法と STAMP/STPA による解析結果の網羅性を融合することで, 評価対象が安全なシステムを構築していることを示す証拠として有効になると考えられる.

ハザード検出過程に引き続き, この結果（No, ITEM, ハザード, 想定事象（UCA））を管理表への記入を実施する. ここでハザードによる結果の深刻さ，危険事象（想定事象）の発生頻度に基づきそのハザードのリスクレベルを算出する. 管理表は, 各ハザードのリスクの軽減過程を設計の進行と同期して更新可能で, その課程（想定

シナリオ（HCF），可能な対策，可能な対策に対する具体的な方策）での追跡性，透明性を確保し，技術の妥当性・正当性を説明する上での中心的な論拠となる． このようにこの管理表は，実際に安全性審査のためのリスク分析に使うことを想定し，ハザード管理手法の概念に基づいて整理した．

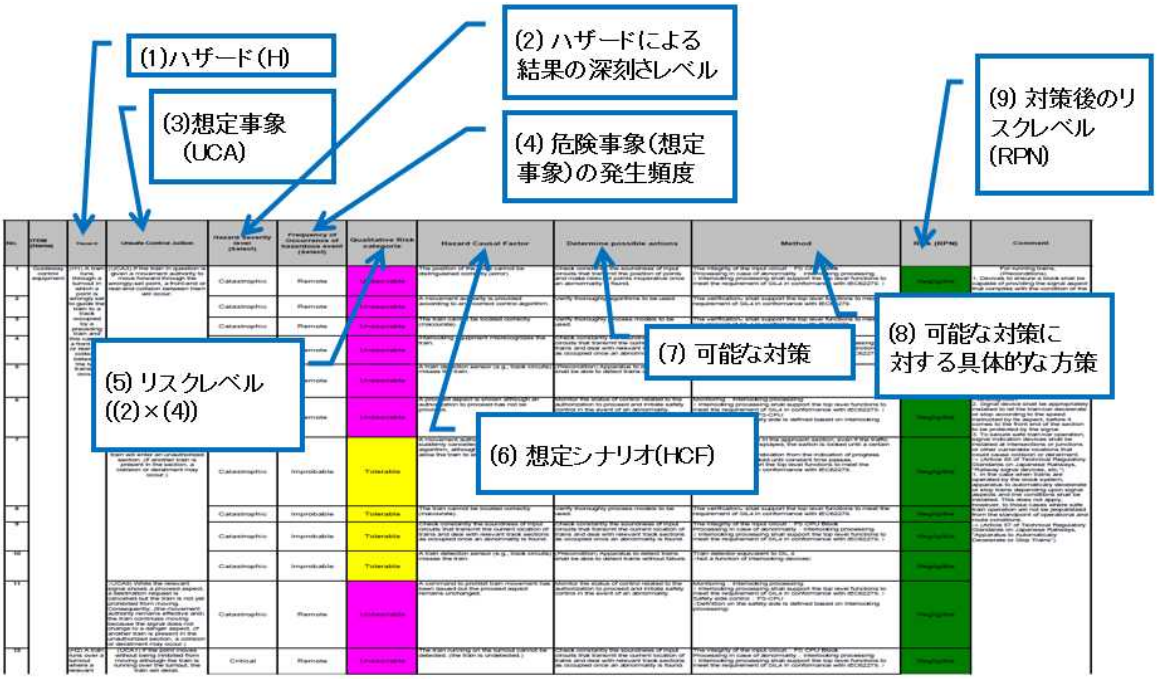


図 5-2　リスク管理表

さらに，この関係図を模式図（STAMP-FT 図とする）で表したものが図 5-3 であり，この図は FTA 図と同じようにハザードと要因を結び付けるものであり対策がその制約ゲートにあたる．また，起こり得る頻度やその事象が発生した場合の影響度を表せるためシステム毎の発生頻度の分析が可能となる．これにより，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し，起こしてはならない事象が起こりうる確率を算出することにより STAMP/STPA の結果も定量的解析ができることになる．結果として ALARP 原理に基づき決定されるリスク受け入れ可能性についても評価が可能となる．

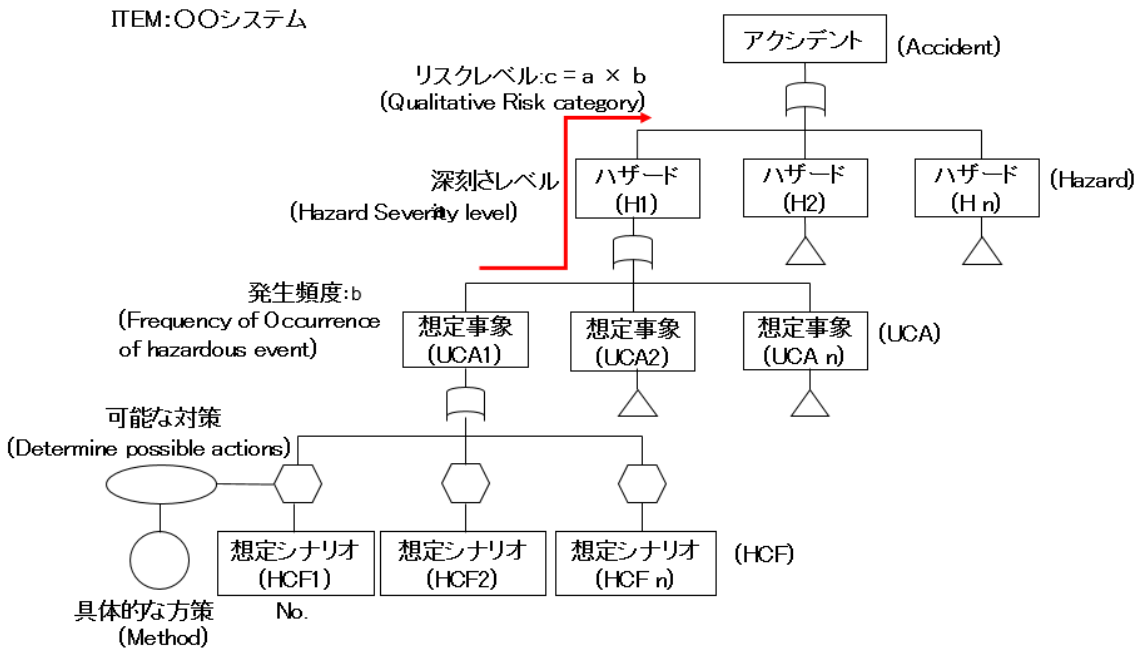


図　5-3　STAMP-FT 図

5.3　新しい安全性解析手法による CBTC 用連動装置の安全性評価

ここまで，既存安全性評価の現状と問題点，ソフトウェア安全性評価の課題について述べ，その解決策として STAMP/STPA による評価方法と鉄道信号システムの評価へ向けた拡張方法について述べた．

この結果を基に，本研究テーマである CBTC 用連動装置の安全性評価を実施する．

列車が軌道を走行するために必要な機能の一つである走行路確保の考え方に基づく連動装置を STAMP/STPA を用いて評価を実施する．

5.3.1　アクシデントの定義

前述の通り連動装置は分岐器のある停車場構内における列車の走行路を制御する装置である．

これを概念図として表したものが図　5-4 である．

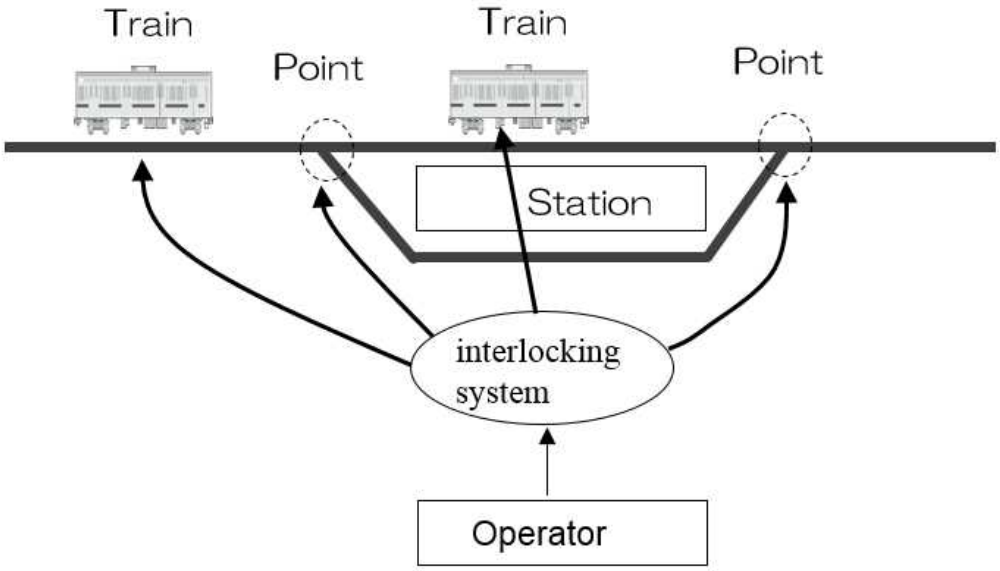


図 5-4　連動装置の概念図

この概念図に基づき走行路を制御に起因するアクシデントを定義すると以下の通りとなる.

(A1)列車同士が衝突する事態
(A2)列車が脱線する事態
(A3)列車同士が接触する事態

(1)ハザードの特定（STPA Step0 準備 1）

定義した各アクシデントに対するハザードは表 5-1の通りである.

表　5-1　ハザードの特定

アクシデント(Loss)	ハザード(Hazard)
(A1)列車と列車が衝突する。	(H1)列車の前方にいる列車と同じ側に開通した分岐器を走行し前方列車と衝突(追突)する。
(A2)列車が脱線する。	(H2)分岐器転換中に分岐器上を列車が走行し脱線する。
(A1)列車と列車が衝突する。	(H3)分岐器上で列車の走行を阻害する区間(非開通側)に他列車が存在しているために列車と接触する。

(2)制御構造図の構築（STPA Step0　準備 2）

図　5-4に基づき制御構造図を作成する．既存装置を意識せず，概念的に描くことが重要である．登場人物はオペレータ（制御盤扱い者），走行路制御（制御主体），分岐器（複数），列車（複数）とし，制御主体となる走行路を制御する装置が列車への走行を許可することと，走行路上に存在する分機器と制御することに注目して描いた構造図が図　5-5である．

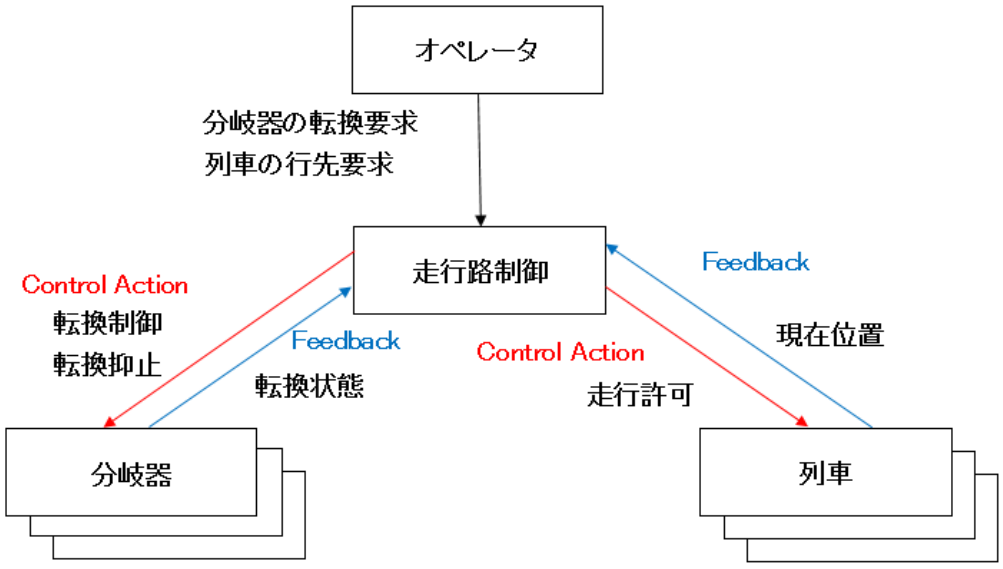


図　5-5　制御構造図

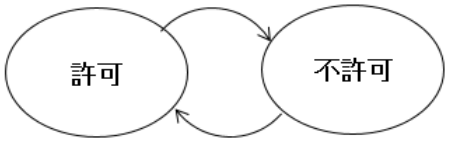
(3) UCA の識別（STPA Step1）

ここでは，ハザードを引き起こす安全ではない制御指示（UCA）の 4 項目の観点（Not Provided/Providing causes hazard/Too Early, Too Late, Wrong order causes hazard/ Stopping too soon, applying too long causes hazard）で識別する.

この際，ここで抽出したさまざまな観点で繰り返し，複数名で解析を進めることになることから，記述ルールを設定することが重要である.

例えば，図 5-6 に示すとおり, 走行制御について同じ状態遷移である「走行を許可与える」と「走行不許可を与えない」の 2 つの制御を表現してしまう問題が発生した. このため内容の記述に当たっては，相反する制御内容で記述しないよう制御（Control Action）名を合わせることとした. ここでは， 走行許可は許可すること, 同様に転換抑止はロックを与えることと, ロックを解除することを与えないことに対して, ロックすることを制御（Control Action）とした. また, 分機器上という範囲を表す場合その範囲を分岐器の構造上の名称でさまざまな観点で表現してしまい同じことを表す結果が複数抽出されるという問題が発生した. このため範囲を持つ状態を定義することで状態が「その時点特有か」,「範囲を持つものか」を明確にして遅れなどの時間的前後関係も範囲の前後として抽出結果が重複とならないようにした.

状態遷移図



タイミング図

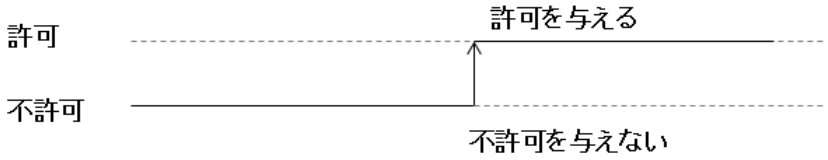


図 5-6　事例1

具体的には以下を記述ルールとした.

記述ルール：

〇〇はコントロールアクション

R1.（与えられないとハザード:Not Providing）

xx の状態で,〇〇が与えられないとハザード

R2.（与えられるとハザード:Providing causes hazard）

xx の状態で，〇〇が与えられるとハザード

R3.（早過ぎ,遅過ぎ,誤順序でハザード:Too early/too late, wrong order causes hazard）

xx の状態になる前に〇〇が与えられるとハザード

xx の状態になった後に〇〇が与えられるとハザード

コントロールアクションの順序を間違えて　〇〇を与えるとハザード

R4.（早過ぎる停止，長過ぎる適用でハザード:Stopping too soon/applying too long causes hazard）

xx の状態で〇〇が停止するとハザード

xx の状態で〇〇が継続するとハザード

この結果特定した安全ではない制御指示の結果は，(UCA1)～(UCA9)の 9 個となった．内容は以下の通りである．

(UCA1) 列車が分岐器上を走行している状態で，転換抑止が与えられないと，分岐器が動いた場合列車が脱線する．(H2)

(UCA2) 列車が分岐器上を走行している状態で，走行側と逆側に転換制御が与えられると，列車が脱線する．(H2)

(UCA3) 前方に列車がいる側に分岐器が転換された状態で，走行許可が与えられ列車が進行すると，列車が衝突（追突）する．(H1)

(UCA4) 背向で分岐器が開通していない状態で，走行許可が与えられ列車が進行すると，列車が脱線する．(H2)

(UCA5)分岐逆側を他列車が走行している状態で，背向から接触限界内に走行許可を出し列車が走行すると，前方列車に接触する．(H3)

(UCA6) 分機器が転換している状態で，走行許可を出しその分岐器上を走行すると，列車が脱線する．(H2)

(UCA7) 前方の列車が分岐器の車両接触限界点を通過完了するよりも前の状態で，走行許可が早過ぎて与えられ列車が進行すると，列車が接触する．(H3)

(UCA8) 走行許可が出て列車が走行している状態で，急に走行許可を解除すると，不許可域に進入してしまう．(不許可域に開通していない分岐器があれば脱線．)(H1,H2)

(UCA9)進行現示が出た状態で，行先要求がキャンセルされたが，走行許可が継続し停止現示にならなかったため，列車が進行する．(不許可域に列車が居れば衝突・脱線．)(H1)

UCA の識別の段階で，「走行許可が与えられ列車が進行すると，列車が衝突（追突）する．」の条件が入っているが，これは連動装置外で整理すべき内容であるため，連動装置を使う上での前提条件として定義することとした．具体的には技術基準の以下の項目に関する内容に相当する．

・技術基準第 54 条　閉そくを確保する装置等

・技術基準第 55 条　鉄道信号の現示装置等
・技術基準第 57 条　列車を自動的に減速または停止をさせる装置

(4) リスク査定

リスクベースの設計手法において, 全ての検出されたハザードは, 発生頻度及び被害の重大性の観点から分類され, 発生頻度と重大性の組み合わせにより, 当該ハザードが ALARP トライアングルのどの領域に属するのかが決定される. これによりそれぞれのハザードがランク付けされ, 定量的リスク評価アプローチにより, システムに与えられている安全目標レベルが満足されているかが確認できる. このため, STAMP/STPA で抽出された結果をこの手法に関連付けることで, 実際にはあり得ないものと, 現実に考え得る注視すべきものとが区別できるようになる. 具体的なリスク査定方法は以下による.

リスク査定を行うにあたり, 特定したハザードに対しては, 深刻さレベルの基準に基づき深刻さレベルの査定を行う. リスク査定基準は鉄道の国際規格 RAMS の 4.6.2.3 表 3 に基づき, Catastrophic/ Critical/ Marginal/ Insignificant の 4 段階に分類する.

次に抽出した UCA に対しても, 発生頻度の基準に基づき発生頻度の査定を行う. 発生頻度査定基準は鉄道の国際規格 RAMS の 4.6.2.2 表 2 に基づき, Frequent/ Probable/ Occasional/ Remote/ Improbable/ Incredible の 6 段階に分類する.

特定したハザードに対する深刻さレベルに UCA の発生頻度を掛け合わせ, リスクの査定を行う. リスク評価は鉄道の国際規格 RAMS の 4.6.2.4 表 6 に基づき, Unacceptable/ Undesirable/ Acceptable の 3 段階で評価する.

(5) HCF の特定（STPA Step2）

リスク査定の結果,「Unacceptable, Undesirable」と定義された UCA について, STAMP/STPA の最後の段階として, STPA Step 1 で識別した UCA の原因となる Causal factor と, 予想される事故シナリオの特定を行う. 原因となる Causal factor は, コントロールループの流れにおいて予想される不備を示したもので以下の 11 項目の観点(11 個のガイドワード)で抽出する.

この段階では，「分岐器上を走行している列車を把握できない」「列車を正しく認識できない」といった連動装置外で列車等を確実に検知する必要があることに起因する内容が挙がった．これは具体的には技術基準の以下の項目に関する内容に相当する内容となる．

・技術基準第 59 条　列車等を検知する装置

5.3.2　安全性評価結果

Step2 において抽出した HCF に対しては，さらに可能な対策（Determine possible actions）における具体的な方策（Method）を立て実施することにより発生要因を取り除き，リスクを低減する．具体的内容については例えば接近鎖錠に関する内容については図 5-7 のようになり，すべてを表にまとめると表 5-2 のようになる．

可能な対策を抽出した段階で挙がった以下の内容はそれぞれ既存装置の連動論理で実現している鎖錠（列車運転の安全を図るために信号機・転てつ機等の間に，電気的な方法により各種の鎖錠が行われ，それぞれの動作を必要に応じて制限する方法を電気鎖錠方法という）に関する事項が含まれることが整理できた．

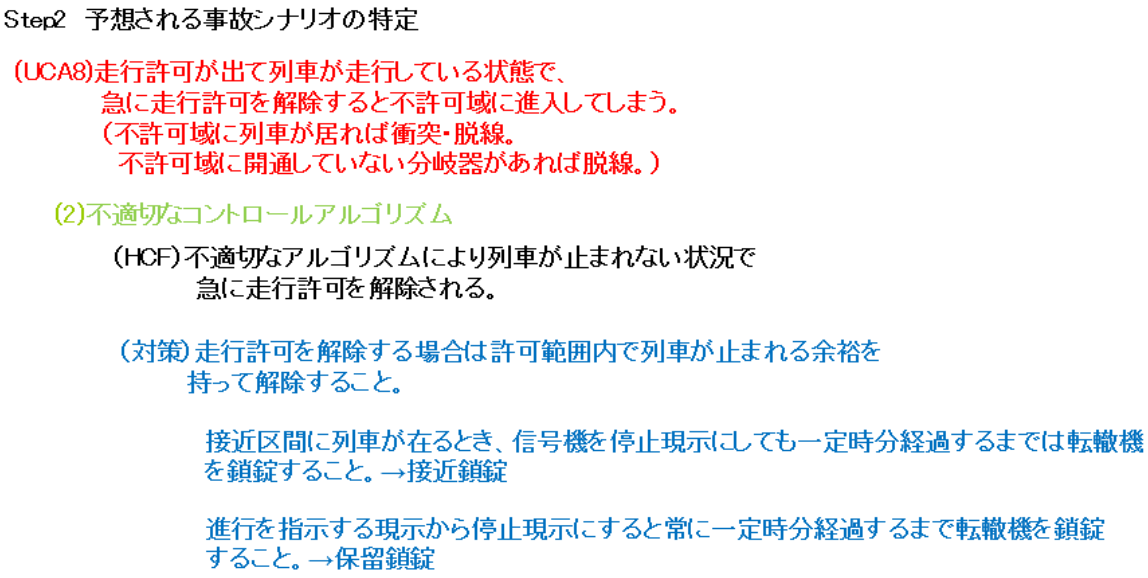


図　5-7　STAMP/STPA の解析結果例

表 5-2　具体的な解析結果

No.	Hazard	Unsafe Control Action 安全ではない制御操作	Hazard Causal Factor ハザード要因	Determine possible actions 可能な対策	Method 対策に対する具体的方策
1	（H1）列車の前方にいる列車と同じ側に開通した分岐器を走行し前方列車と衝突（追突）する.	（UCA3）前方に列車がいる側に分岐器が転換された状態で, 走行許可が与えられ列車が進行すると, 列車が衝突（追突）する.	①　転てつ機の転換方向を正しく認識できない.（誤り）	①　転てつ機の転換方向の入力回路は健全であることを常に確認し, 異常時は転換できない状態とすること.	入力回路の健全性 ： FS CPU Block 異常時処理 ： 連動処理 → 処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
2			②　不適切な制御アルゴリズムにより走行許可が出力される.	②　アルゴリズムの検証は十分に実施すること.	検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
3			③　列車の位置情報を正しく認識できない.（不完全）	③　プロセスモデルの検証は十分に実施すること.	検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
4			⑤　列車を把握できない.（欠落）	⑤　列車の現在位置情報の入力回路は健全であることを常に確認し, 異常時は列車あり側と	入力回路の健全性 ： FS CPU Block 異常時処理 ： 連動処理 → 処理は IEC62279

				すること.	に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
5			⑥ 列車を正しく認識できない. (欠如)	⑥ (前提条件) 列車等を検知する装置は, 列車等を確実に検知することができるものでなければならない.	SIL4 相当の列車等検出装置 (連動装置の機能外)
6			⑧ 進行許可を出力していないのに進行現示が出力された.	⑧ 進行許可制御を監視し, 異常時は安全側に制御すること.	監視 : 連動処理 連動処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする. 安全側制御 : FS-CPU (安全側の規定は連動処理に基づき定義する)
7		(UCA8) 走行許可が出て列車が走行している状態で, 走行許可を解除すると, 不許可域に進入してしまう. (不許可域に列車が	② 不適切なアルゴリズムにより列車が止まれない状況で急に走行許可を解除される.	② 走行許可を解除する場合は許可範囲内で列車が止まれる余裕を持って解除すること.	・接近区間に列車が在るとき, 信号機を停止現示にしても一定時分経過するまでは転轍機を鎖錠する. ・進行を指示する現示から停止現示にすると常に一定時分経過するまで転轍機を

		居れば衝突･脱線．）			鎖錠する． ・ソフトウェアは IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする．
8			③　列車の位置の状態を正しく認識できない．（不完全）	③　プロセスモデルの検証は十分に実施すること．	検証は IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする．
9			⑤　列車を把握できない．（欠落）	⑤　列車の現在位置情報の入力回路は健全であることを常に確認し，異常時は列車あり側とすること．	入力回路の健全性 ： FS CPU Block 異常時処理 ： 連動処理 → 処理は IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする．
10			⑥　列車を正しく認識できない．（欠如）	⑥　（前提条件）列車等を検知する装置は，列車等を確実に検知することができるものでなければならない．	SIL4 相当の列車等検出装置 （連動装置の機能外）

11		(UCA9) 進行現示が出た状態で, 行先要求がキャンセルされたが, 走行許可が継続し停止現示にならなかったため, 列車が進行する. (不許可域に列車が居れば衝突・脱線.)	⑧ 走行不許可を出力したが進行現示が出力したままとなった.	⑧ 進行許可制御を監視し異常時は安全側に制御すること.	監視 : 連動処理信号機が停止現示にならないときは, 鎖錠したままにすること. →表示鎖錠連動処理は IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする. 安全側制御 : FS-CPU (安全側の規定は連動処理に基づき定義する)
12	(H2) 分岐器転換中に分岐器上を列車が走行し脱線する.	(UCA1) 列車が分岐器上を走行している状態で, 転換抑止が与えられないと, 分岐器が動いた場合列車が脱線する.	①-1 分岐器上を走行している列車を把握できない. (喪失)	①-1 列車の現在位置情報の入力回路は健全であることを常に確認し, 異常時は列車あり側とすること.	入力回路の健全性 : FS CPU Block 異常時処理 : 連動処理 → 処理は IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする.
13			①-2 分岐器上を走行している列車を正しく認識できない. (誤り)	①-2 (前提条件) 列車等を検知する装置は, 列車等を確実に検知することができるものでなければならない.	SIL4 相当の列車等検出装置 (連動装置の機能外)
14			② 不適切な制御アルゴリズム	② アルゴリズムの検証は十分に実	分岐器上に列車がいる場合, その間は分岐

			により，転換抑止が出力されない.	施すること.	器を転換できないようにする.
15			④　分岐器の故障による.	④　転てつ機の状態を常に監視すること.	監視 ： 連動処理 連動処理はIEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
16			⑦　転換抑止は行われたが，転てつ機の動作遅れにより分岐器に抑止がかからない.	⑦　転てつ機の状態を常に監視すること.	監視 ： 連動処理 連動処理はIEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
17			⑧　転換抑止したが転てつ機に指示されない.	⑧　転換抑止制御を監視し異常時は安全側に制御すること.	監視 ： 連動処理 連動処理はIEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする. 安全側制御 ： FS-CPU （安全側の規定は連動処理に基づき定義する）
18			⑩　分岐部に異物が挟まり転換できない.	⑩　転てつ機の状態を常に監視すること.	監視 ： 連動処理 連動処理はIEC62279 に準拠したSIL4の要件を満た

					す最上位レベルの機能をサポートする.
19		（UCA2）列車が分岐器上を走行している状態で, 走行側と逆側に転換制御が与えられると, 列車が脱線する.	①-1　分岐器上を走行している列車を把握できない.（喪失）	①-1　列車の現在位置情報の入力回路は健全であることを常に確認し, 異常時は列車あり側とすること.	入力回路の健全性 ：FS CPU Block 異常時処理 ： 連動処理 → 処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
20			①-2　分岐器上を走行している列車を正しく認識できない.（誤り）	①-2　（前提条件）列車等を検知する装置は, 列車等を確実に検知することができるものでなければならない.	SIL4 相当の列車等検出装置 （連動装置の機能外）
21			②　不適切な制御アルゴリズムにより, 転換制御が出力される.	②　アルゴリズムの検証は十分に実施すること.	分岐器上に列車がいる場合, その間は分岐器を転換できないようにする. → 検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.

22			⑧ 転換制御したが転てつ機に指示されない.	⑧ 転換制御を監視し異常時は安全側に制御すること.	監視 : 連動処理連動処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする. 安全側制御 : FS-CPU (安全側の規定は連動処理に基づき定義する)
23		(UCA4) 背向で分岐器が開通していない状態で, 走行許可が与えられ列車が進行すると, 列車が脱線する.	① 転てつ機の転換方向を正しく認識できない. (誤り)	① 転てつ機の転換方向の入力回路は健全であることを常に確認し, 異常時は転換できていない状態とすること.	入力回路の健全性 : FS CPU Block 異常時処理 : 連動処理 → 処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
24			② 不適切な制御アルゴリズムにより, 走行許可が出力される.	② アルゴリズムの検証は十分に実施すること.	検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
25			⑧ 進行許可を出力していないのに進行現示が出力された.	⑧ 進行許可制御を監視し異常時は安全側に制御すること.	監視 : 連動処理 連動処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする. 安全側制御 : FS-

					CPU （安全側の規定は連動処理に基づき定義する）
26		（UCA6）分機器が転換している状態で，走行許可を出しその分岐器上を走行すると，列車が脱線する．	① 転てつ機の転換方向を正しく認識できない．（誤り）	① 転てつ機の転換方向の入力回路は健全であることを常に確認し，異常時は転換できていない状態とすること．	入力回路の健全性 ： FS CPU Block 異常時処理 ： 連動処理 → 処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする．
27			② 不適切な制御アルゴリズムにより，走行許可が出力される．	② アルゴリズムの検証は十分に実施すること．	検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする．
28			⑧ 進行許可を出力していないのに進行現示が出力された．	⑧ 進行許可制御を監視し異常時は安全側に制御すること．	監視 ： 連動処理 連動処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする． 安全側制御 ： FS-CPU （安全側の規定は連動処理に基づき定義する）

29		（UCA8）走行許可が出て列車が走行している状態で，急に走行許可を解除すると，不許可域に進入してしまう．（不許可域に開通していない分岐器があれば脱線．）	② 不適切なアルゴリズムにより列車が止まれない状況で急に走行許可を解除される．	② 走行許可を解除する場合は許可範囲内で列車が止まれる余裕を持って解除すること．	・接近区間に列車が在るとき，信号機を停止現示にしても一定時分経過するまでは転轍機を鎖錠する． ・進行を指示する現示から停止現示にすると常に一定時分経過するまで転轍機を鎖錠する． ・ソフトウェアは IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする．
30			③ 列車の位置の状態を正しく認識できない．（不完全）	③ プロセスモデルの検証は十分に実施すること．	検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする．
31			⑤ 列車を把握できない．（欠落）	⑤ 列車の現在位置情報の入力回路は健全であることを常に確認し，異常時は列車あり側とすること．	入力回路の健全性 ： FS CPU Block 異常時処理 ： 連動処理 → 処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする．

32			⑥ 列車を正しく認識できない．（欠如）	⑥ （前提条件）列車等を検知する装置は，列車等を確実に検知することができるものでなければならない．	SIL4 相当の列車等検出装置（連動装置の機能外）
33	（H3）分岐器上で列車の走行を阻害する地点（非開通側）に他列車が存在しているために列車と接触（衝突）する．	（UCA5）分岐逆側を他列車が走行している状態で，背向から接触限界内に走行許可を出し列車が走行すると，前方列車に接触する．	② 不適切な制御アルゴリズムにより，走行許可が出力される．	② アルゴリズムの検証は十分に実施すること．	検証は IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする．
34			③ 列車の位置情報を正しく認識できない．（不完全）	③ プロセスモデルの検証は十分に実施すること．	検証は IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする．
35			⑤ 列車を把握できない．（欠落）	⑤ 列車の現在位置情報の入力回路は健全であることを常に確認し，異常時は列車あり側とすること．	入力回路の健全性 ： FS CPU Block 異常時処理 ： 連動処理 → 処理は IEC62279 に準拠した SIL4 の要件を満たす最上位レベルの機能をサポートする．
36			⑥ 列車を正しく認識できない．（欠如）	⑥ （前提条件）列車等を検知する装置は，列車等を確実に検知することができるものでなけ	SIL4 相当の列車等検出装置 （連動装置の機能外）

				ればならない.	
37			⑧ 進行許可を出力していないのに進行現示が出力された.	⑧ 進行許可制御を監視し異常時は安全側に制御すること.	監視 : 連動処理 連動処理はIEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする. 安全側制御 : FS-CPU （安全側の規定は連動処理に基づき定義する）
38		（UCA7）前方の列車が分岐器の車両接触限界点を通過完了するよりも前の状態で, 走行許可が早過ぎて与えられ列車が進行すると, 列車が接触（追突）する.	② 不適切な制御アルゴリズムにより, 走行許可が出力される.	② アルゴリズムの検証は十分に実施すること.	検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
39			③ 列車の位置情報を正しく認識できない.（不完全）	③ プロセスモデルの検証は十分に実施すること.	検証は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする.
40			⑤ 列車を把握できない. （欠落）	⑤ 列車の現在位置情報の入力回路は健全であることを常に確認し, 異常時は列車あり側とすること.	入力回路の健全性 : FS CPU Block 異常時処理 : 連動処理 → 処理は IEC62279 に準拠したSIL4の要

					件を満たす最上位レベルの機能をサポートする.
41			⑥ 列車を正しく認識できない. （欠如）	⑥ （前提条件）列車等を検知する装置は,列車等を確実に検知することができるものでなければならない.	SIL4 相当の列車等検出装置 （連動装置の機能外）
42			⑧ 進行許可を出力していないのに進行現示が出力された.	⑧ 進行許可制御を監視し異常時は安全側に制御すること.	監視 : 連動処理 連動処理は IEC62279 に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする. 安全側制御 : FS-CPU （安全側の規定は連動処理に基づき定義する）

これは概念図を基に STAMP/STPA にて解析した抽出結果が,既存の連動装置における可能な対策を含んでいることを示している.ことから図 5-8 のように STAMP/STPA にて解析した結果は,連動装置の安全性機能要求事項について網羅性が確認できたと考えられる．具体的には以下による.

・「不適切な制御アルゴリズムにより，転換抑止が出力されない」，「不適切な制御アルゴリズムにより，転換制御が出力される」は電気鎖錠方法によるてっ査鎖錠に相当する.

・「不適切なアルゴリズムにより列車が止まれない状況で急に走行許可を解除される．」は電機鎖錠方法による接近鎖錠，保留鎖錠に相当する．

・「走行不許可を出力したが進行現示が出力したままとなった．」は電気鎖錠方法による表示鎖錠に相当する．

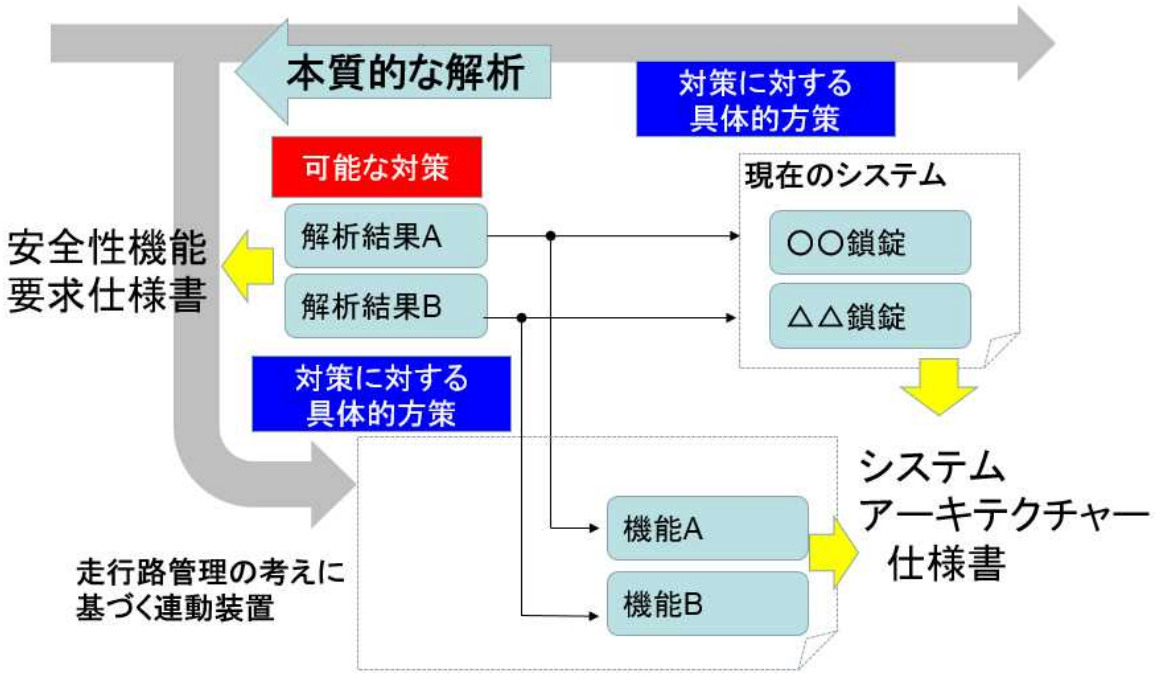


図　5-8　網羅性の確認

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列挙すると以下の通りとなる．

〈SRS-SSI-VT-FU-XX-0070〉

転てつ機の転換方向の入力回路は健全であることを常に確認し，異常時は転換でない状態とする．

（具体的解析結果の No1，No23，No26 による．）

〈SRS-SSI-VT-FU-XX-0080〉

列車の現在位置情報の入力回路は健全であることを常に確認し，異常時は列車あり側とする．

（具体的解析結果の No3，No4，No8，No9，No12，No19，No30，No31，No34，No35，No39，No40 による．）

〈SRS-SSI-VT-FU-XX-0090〉

信号機が停止現示にならないときは，鎖錠したままにする．

（具体的解析結果の No11，No27，No33 による．）

〈SRS-SSI-VT-FU-XX-0100〉

分岐器上に列車がいる場合，その間は分岐器を転換できないようにする

（具体的解析結果の No21 による．）

〈SRS-SSI-VT-FU-XX-0110〉

進行許可制御を監視し，異常時は安全側に制御する．

（具体的解析結果の No6，No2，No24，No25，No27，No28，No33，No37，No38，No42 による．）

〈SRS-SSI-VT-FU-XX-0120〉

走行許可を解除する場合は許可範囲内で列車が止まれる余裕を持って解除する．

（具体的解析結果の No7，No29 による．）

〈SRS-SSI-VT-FU-XX-0130〉

転てつ機の状態を常に監視する．

（具体的解析結果の No15，No16，No18 による．）

〈SRS-SSI-VT-FU-XX-0140〉

転換抑止制御を監視し異常時は安全側に制御する．

（具体的解析結果の No14，No17 による．）

〈SRS-SSI-VT-FU-XX-0150〉

転換制御を監視し，異常時は安全側に制御する．

（具体的解析結果の No22 による．）

この安全性機能要求を既存連動装置と本方式に対してソフトウェア（S/W），ハードウェア（H/W），設定データ（駅毎の連動データ/線形データ）のどの箇所で実現するかを当てはめると既存連動装置が図 5-9，本方式が図 5-１０となる．

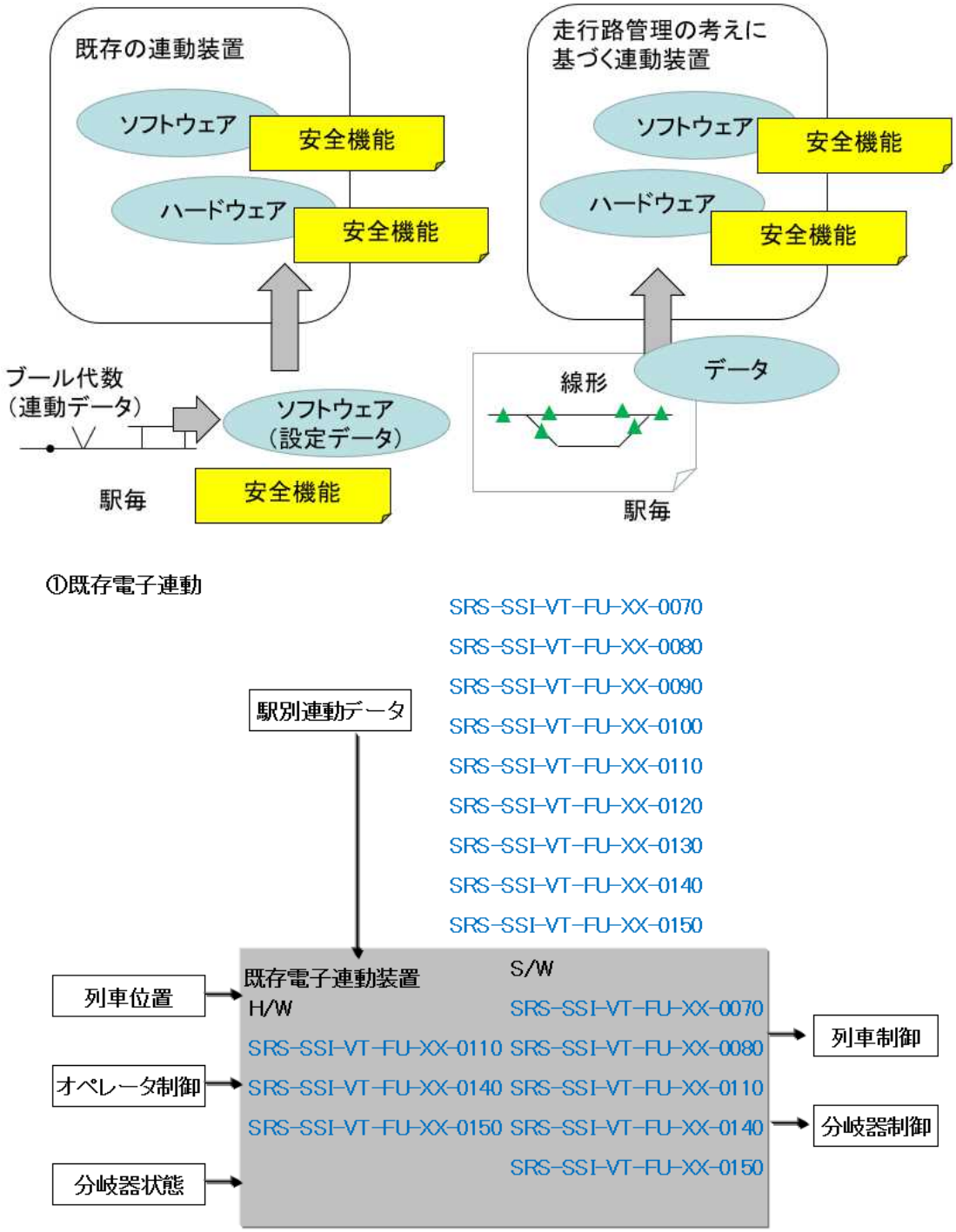


図　5-9　既存連動装置への安全性機能要求の割当

②走行路管理の考えに基づく電子連動

図　5-１０　本方式への安全性機能要求の割当

既存連動装置では安全性機能要求が信号結線図である駅別データに依存するのに対し, 本方式ではソフトウェアに依存することが明確となった. このため, 既存連動のように連動機能を駅別結線データで実現する場合に対して, 本方式では一度S/W について安全性の検証を行っておけば, 駅毎個別データについて安全性の検証を行う必要がないことが示された.

なお, 本方式のソフトウェアは図　5-１１に示す構造で実現されている.　このソフトウェアについては実績のあるソフトウェアの開発手法や社内チェック体制を踏襲し，IEC62279[12]等の国際規格を参照すれば，特に問題は無いと考えられる.

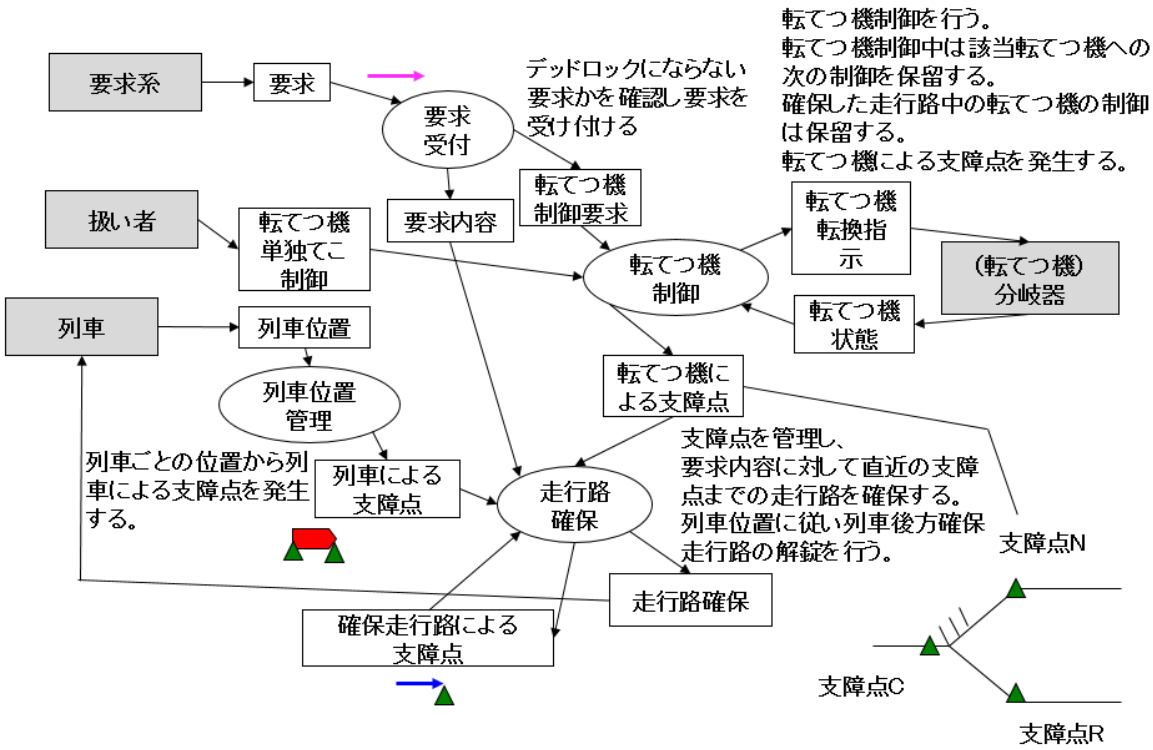


図　5-１１　本方式の制御フロー図

５.４　新しい安全性評価手法に関する評価

鉄道は経験工学といわれるように, 過去の事故やトラブルを教訓に安全性を高めてきた．しかし，それはあくまで経験であり，システムの安全性について本質的な観点から安全対策を行う必要があると考えられる．また，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 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. この規格の中では FTA,FMEA による評価が前提とされているが，ソフトウェアの故障への影響度評価の方法論がないという課題があった. そこで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, さらに方法論を拡張し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した結果を, FTA 同様にシステム毎の発生頻度の分析のために，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

るようになった. 起こしてはならない事象が起こりうる確率を算出することにより STAMP の結果も定量的解析ができることになり, ALARP 原理に基づき決定されるリスク受け入れ可能性についても評価が可能となることを示した.

この結果に基づき連動の概念図に基づき連動装置について解析を行った. その結果, 起こしてはいけない事象（ハザード）をトップ事象として, UCA に対しての HCF を特定し, その可能な対策と対策に対する具体的な方策へと解析し, 解析結果をリスク管理表（Hazard Log）としてまとめた.

なお, 図 5-1 2に示す通り, 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. さらにこの安全性機能要求を既存連動装置と CBTC 用連動装置に対して機能構造（ソフトウェア（S/W）, ハードウェア（H/W）, 設定データ（駅別連動データ/線形データ）のどの箇所）へ割り当て導き出すことができた. これは対策に対する具体的な方策でありシステムアーキテクチャー仕様書（System Architecture Specification）に相当するものを導き出すことができる.

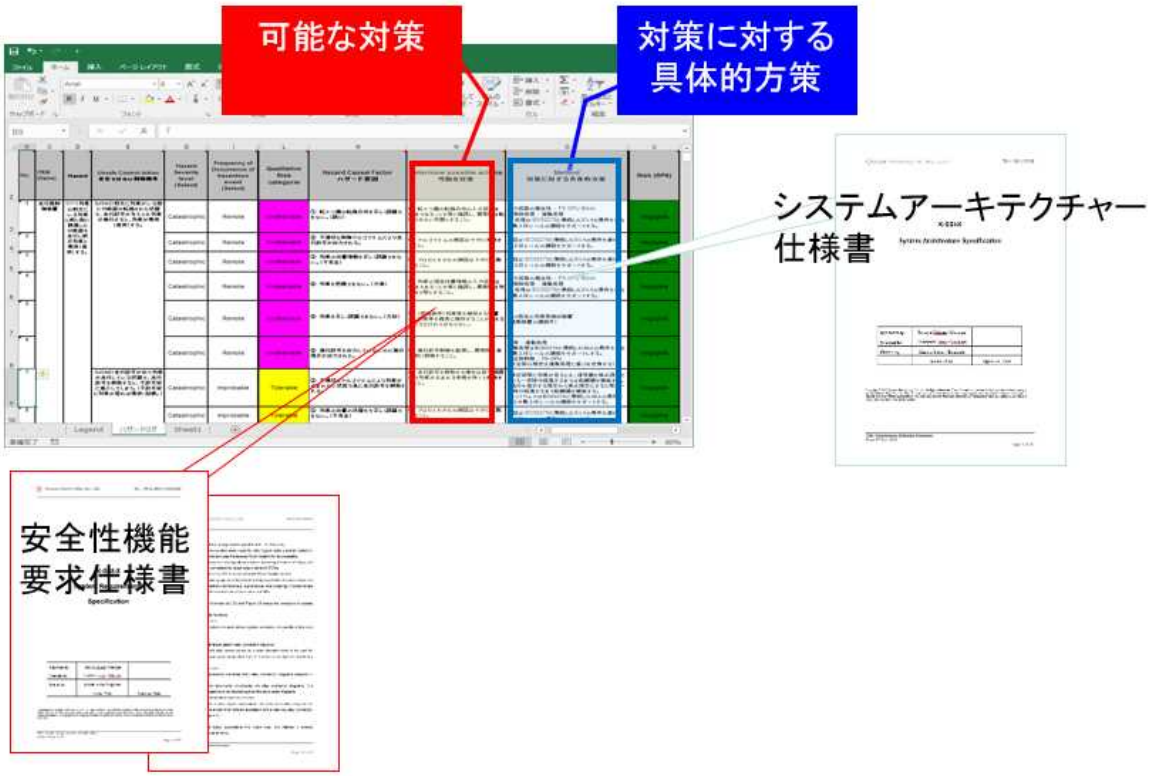


図　5-１２　仕様書への割当

本安全性解析手法は，連動装置に起因するアクシデント（衝突や脱線）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.

ここで解析した結果となる具体的な方策には，アクシデントを起こし得る要因の排除方法，それを実現するための機能に対して必要とされる異常状態の監視内容，装置外で実現する機能への要求事項が示されている.このため，ここで示された内容を全て満足するよう図　5-１１の制御フローを実現すれば連動装置は,アクシデントに至らない（安全であることが示された）ことになると考える.

５.５　CBTC 用連動装置に関する安全性評価の結果

連動装置に関する安全性評価の結果, 継電連動の駅別信号結線図に基づく既存連動装置では, 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.

また, 本方式における論理を適用した CBTC 用連動装置にて, モデル線区にて評価を行った. モデル線区は GNSS(Global Navigation Satellite System ：全球測位衛星システム)による列車位置検知に基づく CBTC 化を目指した ATP 閉そくシステムで構築しているが, この ATP 閉そくも駅構内の制御については, 列車検知は軌道回路をベースとした連動論理が使われている[13]. 今回この連動駅における連動機能を提案方式にて置き換えた上で, 連動機能について ATP 閉そく用の既存連動方式と比較を行った. モデル線区は図 ５-１３に示す通り途中 3 駅の列車交換可能な駅がありこの駅の連動機能を制御する必要がある.

モデル線区では接待したダイヤ通りに列車が動くことを想定し, 走行路制御を行った場合, 本方式では信号結線を用いることなく駅間の閉そく管理, 転てつ機の制御を既存の連動装置と同じように制御することをシミュレーションによって確認した. 6 時台から 9 時台を図 ５-１１に基づく実論理を用いてシミュレーションで確認した結果は図 ５-１３の通りである. ダイヤを変更してのシミュレーションにおいての列車の駅構内進入時に際しては, 既存方式では列車検知に軌道回路をベースとする論理を用いているため, ホームトラック（軌道回路）に列車が到着するまでは列車交換のため待機する列車の進路は出すことができなかったが, 本方式では分岐器の支障点を抜けた時点で走行路が確保できるためより効率のよい運用が可能となることが確認できた. 例えば, 既存方式では対抗列車の待ち状態で待機している列車が出発する際対抗列車がホームトラック到着まで転てつ機の制御が行われなかったが, 本方式では対抗列車が分岐器の支障点を抜けた時点で転てつ機の制御が行われる. また, 既存方式では後続列車が同一着点の走行路を要求した場合既存方式では該当進路に対するすべての条件が成り立たないと前方への進入はでき

ないが, 本方式では直近の支障点（前方の列車の後方位置）まで進入が可能となったことである.

安全性については, 継電連動装置の検査方法に準ずる連鎖条件の検査でも安全性に問題がないことが確認できた. 例えば, 接近鎖錠に関しては, 既存方式では列車が接近鎖錠区間に接近している場合はその列車が完全に停止できる所要時間を定めて制御しているが, 本方式では，列車が停止していることが確認できた場合，列車に停止指示を出した上で, 解除要求のあった走行路確保を解除するため既存方式における一定に定められた所要時間より効率的に列車運行ができるなどである. 本装置の安全性に関する評価については, 提案した解析手法により連動装置に起因するアクシデントを頂点として特定したハザードに対する対策結果については以下のとおり整理した.

（H1）列車の前方にいる列車と同じ側に開通した分岐器を走行し前方列車と衝突する事象に対しては, 転てつ機の制御の状態を監視し転てつ機に対する支障点を制御していること，不明瞭（異常な）状態ではすべての支障点を発生していることから発生しない.

（H2）分岐器転換中に分岐器場を列車が走行し脱線する事象に対しては，走行路が確保された状態で列車位置を変化させ場合において, 列車位置状態を監視してその列車位置に対して支障点を発生させ, その支障点に基づき転てつ機に対する支障点を制御していることから発生しない.

（H3）分岐器上で列車の走行を阻害する区間に他列車が存在しているために列車と接触する事象に対しては, 列車位置状態を監視してその列車位置に対して支障点を発生させ, その支障点に基づき転てつ機に対する支障点を制御していることから発生しない.

この結果は, 本方式は支障点の発生制御を, 解析により導き出したトップ事象（連動装置に起因するアクシデント : 衝突や脱線）に至る要因を排除できるつくりとしていることから, 連動装置に起因するアクシデントの発生を抑止できることを可能としていると考える.なお，本方式については基本プログラムにて安全性機能を実現しているため駅毎のデータに安全機能は存在しないが, 設定する制御ポイントである支障点の具体的位置の管理をすることが重要な観点である.

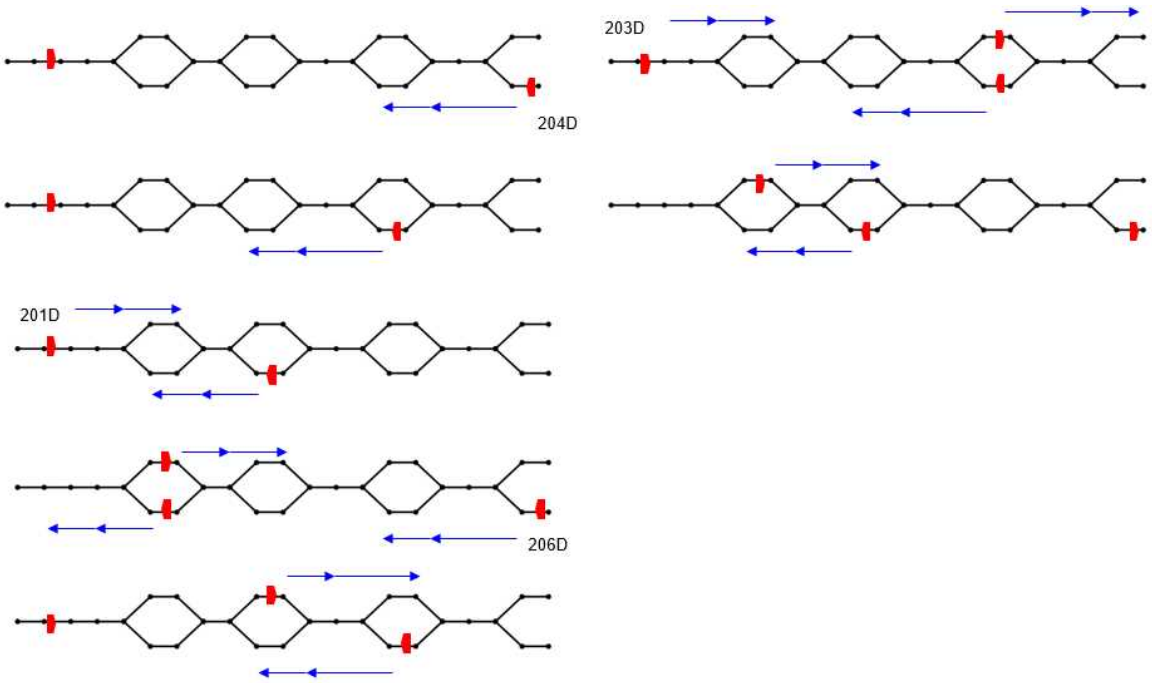


図　5-１３　シミュレーションによる動作確認結果

第６章　　結論

６.１　研究の成果

本研究では，はじめに，鉄道信号用の連動装置の機能と課題についてまとめた．CBTC の列車制御論理は，先行列車の位置を逐次後続列車に伝えて，リアルタイムに列車制御を行う「移動閉そく式」が一般的である．しかしながら，駅構内においては，軌道回路をベースとした信号結線論理に基づく連動装置による進路制御を行っていたため駅構内での移動閉そくの実現が望まれていた．そこで，これを実現するために支障点を設置し，要求走行路上に支障点が発生した場合は，要求走行路に対して列車先頭位置から支障点までをその列車へ占有権を与え列車制御を行う新しい駅構内における CBTC を実現する連動装置の仕組みを開発した．

この CBTC 用連動装置の安全性評価については，既存の解析方法を整理したうえで，解析にあたっては STAMP/STPA の概念に基づく解析と FTA の長所に着目した新たな安全性解析手法を開発した．開発した手法は FTA ではわかりづらかった結果の網羅性，STAMP では難しかった定量解析について双方を満たすことができることが特徴である．また，鉄道の国際規格 RAMS の第 3 段階リスク分析に照らし合わせ構想設計への対応方法を確立した．その方法は，STAMP/STPA は解析結果の網羅性はあるが，その解析結果は実際にはあり得ないものと，現実に考え得る注視すべきものが区別なく評価されるため，ハザードによる結果の深刻さレベルと危険事象の発生頻度を基にリスクレベルを導き出すのである．その結果をハザードログとしてまとめ，管理プロセスを構築・展開し，リスク検知手段，リスクの見える化，管理プロセスの手段を確立し，安全性解析の活動の一つとして示した．この方式に基づき，走行路確保に基づく連動機能の実現方法について評価した結果から既存連動装置との違いがどこにあるのかを示し， 開発した CBTC 用連動装置は駅個別の結線論理を持つことなく連動を実現することを示した．

新たな安全性解析手法について評価として，その要因抽出の成果については，その結果を「鉄道に関する技術基準」や「電気鎖錠方法に基づく鎖錠」と関連づけ解析の妥当性を示した．

また,開発した CBTC 用連動装置の安全性については，支障点の発生制御を，解

析により導き出したトップ事象（連動装置に起因するアクシデント：衝突や脱線）に至る要因を排除できるつくりとできていることから，連動装置に起因するアクシデントの発生を抑止できることを可能としていると考える．なお，本方式については基本プログラムにて安全性機能を実現しているため駅毎のデータに安全機能は存在しないが，設定する制御ポイントである支障点の具体的位置の管理をすることが重要な観点である．

６.２　今後の課題

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．新しい安全性評価手法により,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．これにより開発した 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，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と考えている．

謝辞

本研究を実施するにあたり，終始適切かつ熱心にご指導，ご鞭撻いただいた日本大学の中村　英夫名誉教授（現東京大学）に心から感謝いたします．各ジャーナル誌への論文投稿や国際会議等における論文発表においても懇切丁寧にご指導いただき，私にとっては大変貴重な経験となりました．また，技術的な観点からいつも適切なアドバイスをしていただいた(故)浅野　晃氏には心よりお礼申し上げます．

また，本論文をまとめるにあたり，技術的な観点からご指導をいただき，また有益なご助言をいただいた，日本大学高橋　聖教授, 吉川　浩教授, および, 泉　隆特任教授に心よりお礼申し上げます．

本研究を進めるにあたり, 適切な研究環境を整えていただきご指導をいただいた, 株式会社京三製作所の役員の方々に深く感謝いたします．また，本研究の各分析にあたり協力をいただいた堺　将人氏，山越　基玄氏に深く感謝いたします．

最後に，家庭において終始温かく支えてくれた妻美蘭や子供たち，いつも応援してくれた両親に感謝いたします．

参考文献

[1]K.Akita, K.Watanabe, H.Nakamura, I.Okumura Computerized Interlocking System for Railway Signalling Control;SMILE, IEEE Transactions on Industry application, Vol.IA-21, No.4, pp.826-834, (1985.5)

[2]国土交通省, 鉄道に関する技術上の基準を定める省令, 平成十三年国土交通省令第百五十一号

[3]IEC62278:2002. Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS).

[4]JIS E3004 継電連動機検査方法

[5]IEEE Std 1474.1TM-2004, IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements

[6]橋本文雄, 神戸新交通ポートアイランド線信号保安設備 (3)新交通における列車検知と ATC について, 京三サーキュラー, VOL.32 No.3 ,pp.6-16,(1981).

[7]水野啓介, マイクロ Ci の開発（極少進路電子連動装置）, 京三サーキュラー, Vol.52, No.2, (2001).

[8]Nancy Leveson, Engineering a Safer World, MIT press, (2012)

[9]鉄道信号, 日本鉄道電気技術協会, (2015.12)

[10]山崎勇, 内山大輔: ATACS の踏切制御機能使用開始, JREA, Vol.58, No.8, pp.22-25, (2015).

[11]独立行政法人情報処理推進機構, はじめての STAMP/STPA, 第 1 刷, 2016 年 4 月.

[12]IEC62279:2015. Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

[13]浅野晃, 神宮雅昭, 記虎正幸, 大和田厚祐, 菊池麻香, 黄怡杰(2014). 列車制御システムへの汎用技術の利用 . 京三サーキュラー,65(1),pp.6-11.

研究業績

業績論文

[1]Tetsuya TAKATA, Hideo NAKAMURA (2019). "Applicability of Methods for Safety Analysis of Railway Signaling ". Journal of the Korean Society for Railway (JKSR), Vol. 22, No. 7, pp. 538-549.

[2]Tetsuya TAKATA, Akira ASANO, Hideo NAKAMURA (2018). "Safety Assessment of Closed-Loop Level Crossing Control Systems by Means of Systems-Theoretic Accident Model and Processes (STAMP)". Journal of Traffic and Transportation Engineering, Vol. 6, No. 5, pp. 241-254.

[3]Tetsuya Takata, Akira Asano, Hideo Nakamura (2019). "Interlocking System Based on Concept of Securing a Train Travelling Path ". Proceedings of the 8th International Conference on Railway Operations Modelling and Analysis - RailNorrkoping2019, pp. 1586-1593.

[4]Tetsuya TAKATA, Akira ASANO, Hideo NAKAMURA (2019). "Interlocking System for CBTC (Communication Based Train Control) System". Journal of Traffic and Transportation Engineering, Vol. 7, No. 4, pp. 145-156.

[5]Tetsuya Takata, Akira Asano, Hideo Nakamura (2019). "A SAFETY ANALYSYS TECHNIQUE USING STAMP/STPA FOR ELECTRONIC INTERLOCKING SYSTEM ". IRSE's Aspect 2019 conference.

[6]Akira ASANO, Tetsuya TAKATA, Hideo NAKAMURA (2015). "Integrated train control system: The new direction of train control system ". The International Symposium on Seed-up and Service Technology for Railway and Maglev Systems, pp.10-12."

[7]Akira Asano, Tetsuya Takata, Hideo Nakamura (2018). "A Consideration on a Practical Use of GNSS for a Train Protection System ". Railways2018 The Fourth International Conference on Railway Technology: Research, Development and Maintenance.

その他論文等

[8]髙田哲也(1998). ″系概念を一新した新電子連動処理部 ″. 第 35 回鉄道サイバネシンポジウム.

[9]長澤弘之,髙田哲也(2000). ″無線通信進路設定システム ″. 第 37 回鉄道サイバネシンポジウム.

[10]髙田哲也(2001). ″検査期間推定による検査員配置の検討 ″. 第 17 回ファジィシステムシンポジウム.

[11]髙田哲也(2002). ″連動機能を持った電子端末装置 ″. 第 18 回ファジィシステムシンポジウム.

[12]髙田哲也(2005). ″移動式改札機という考え ″. 第 21 回ファジィシステムシンポジウム.

[13]髙田哲也(2007). ″無線式列車検知システム（K-CBTC1 形）の開発 ″. 第 44 回鉄道サイバネシンポジウム.

[14]水野 健司,木村 純司,四釜 康治,髙梨 健,板垣 朋範,髙田 哲也,大嶋 薫(2008). ″仮想閉そく方式を用いた無線式列車制御システム（K-CBTC3 形）の開発 ″. 平成 20 年電気学会産業応用部門大会.

[15]齊藤嘉久,髙田哲也,風間洋(2014). ″未來交通管理系統的新展望 ″. 2014 軌道工程建設之挑戦與創新発展研討會.

[16]髙田哲也(2015). ″致力於新世代列車控制系統開發及實踐 ″. 2015 國際鐵路工程創新發展研討會.

[17]浅野 晃 , 髙田 哲也 , 杉山 貴昭(2016). ″統合型列車制御システム ″. 第 53 回鉄道サイバネシンポジウム.

[18]髙田哲也(2016). ″STAMP 解析での定量的評価と STAMP 解析の開発プロセスにおける適用段階 ″. 第 1 回 STAMP ワークショップ.

[19]髙田哲也(2016). ″軌道維護管理運用車載感應器之大數據分析 ″. 2016 鐵路與公路工程創新發展研討會.

[20]髙田哲也(2017). ″STAMP による閉電路制御式踏切制御システムの安全性評価 ″. 第 2 回 STAMP ワークショップ.

[21]清水 雄一郎 , 浅野 晃 , 髙田 哲也 , 中村 英夫(2017). ″多情報化と状態監視可能な新 ATS 車上装置 ″. 第 54 回鉄道サイバネシンポジウム.

[22]小田嶋 舞, 林田 悠一, 森 裕貴, 高田 哲也(2017). ″地方鉄道を対象とした軌道状態監視システムの開発及び評価 ″. 日本大学生産工学部第 50 回学術講演会.

[23]小田嶋 舞, 林田 悠一, 綱島 均, 森 裕貴, 高田 哲也(2017). ″地方鉄道を対象とした軌道状態監視システムの開発と運用 ″. J-RAIL2017.

[24]清水 雄一郎 , 浅野 晃 , 髙田 哲也 , 中村 英夫(2017). ″マルチ共振式対車上伝送装置の開発 ″. J-RAIL2017.

[25]Tetsuya Takata, Takaaki Sugiyama, Yoshihisa Saito(2018). "Safety Evaluation of Level Crossing Control System using STAMP ". Transportation and Electric Railway Technical Meeting,TER-18-21.

[26]若井 翔平 , 高田 哲也 , 水間 毅 , 綱島 均 , 松本 陽 , 林田 悠一 , 廣瀬 亮太(2018). ″機械学習を用いた小型レール状態診断装置の活用方法の提案 ″. ITS 交通・電気鉄道合同研究会・ITS 交通一般, 鉄道一般電気学会研究会.

[27]若井 翔平 , 高田 哲也 , 水間 毅 , 綱島 均 , 松本 陽 , 林田 悠一 , 廣瀬 亮太(2018). ″機械学習を用いた小型レール状態診断装置の活用方法の提案 ″. 電子情報通信学会技術研究報告.

[28]髙田哲也, 堺将人(2018). ″STAMP／STPA を用いたハザードログツールの提案 ″. 第 3 回 STAMP ワークショップ.

[29]足立武士, 東濱忠良, 石川了, 岩崎照幸, 菅原健, 長谷川洋介, 植田博司, 高田哲也, 柏倉正(1994). ″営団地下鉄銀座線信号保安システム ″. 京三サーキュラー, 45(1), pp.1-19.

[30]瀬戸通夫, 荒信幸, 高田哲也, 大西雄一(1995). ″汎用フェールセーフ端末 ″. 京三サーキュラー, 46(3),pp.1-5.

[31]高田哲也, 村上洋一, 横山保(1997). ″高速 CPU と支援機能を充実した新電子連動装置 ″. 京三サーキュラー, 48(1), pp.14-23 .

[32]高田哲也, 村上洋一, 今澤利浩, 島添敏之(1998). ″高速 CPU と支援機能を充実した新電子連動装置その 2 ″. 京三サーキュラー, 49(1), pp.1-9.

[33]長澤弘之, 高田哲也(2000). ″無線による遠隔進路設定システム ″. 京三サ

ーキュラー, 51(6), pp.4-9.
[34]髙田哲也(2006). ″中国向け電子連動装置の開発 ″. 京三サーキュラー, 57(6),pp.10-13.
[35]髙田哲也(2007). ″無線利用による列車制御システム ″. 京三サーキュラー, 58(4),pp.4-9.
[36]髙田哲也(2007). ″無線利用による列車制御システム ″. 鉄道車両と技術, 137(-),pp.22-26.
[37]石川了, 本多節, 髙田哲也, 池谷崇(2007). ″ループコイルを用いた CBTC（K-CBTC2 形） ″. 京三サーキュラー,58(6),pp.6-9.
[38]大嶋薫, 髙田哲也, 板垣朋範, 高梨健, 木村純司, 水野健司, 四釜康治(2008). ″無線式列車制御システム（K-CBTC-3 形） ″. 京三サーキュラー,59(2),pp.4-9.
[39]髙田哲也(2008). ″IT-ATC″. JREA, 51(8), pp.33580-33582.
[40]横山保, 髙田哲也, 板垣朋範, 高梨健, 四釜康治, 西敏史, 中村直生(2010). ″無線式列車制御システム（IT-ATP システム） ″. 京三サーキュラー,61(6),pp.4-9.
[41]浅野晃, 髙田哲也(2015). ″統合型列車制御システム ″. 京三サーキュラー, 66(1),pp.6-9.
[42]清水雄一郎, 浅野晃, 髙田哲也, 中村英夫(2018). ″二つの共振周波数を同時受信可能な ATS 車上装置の開発 ″. 京三サーキュラー,69(2),pp.2-7.
[43]荻野誠之, 山田麻香, 髙田哲也, 浅野晃, 綱島均(2018). ″地域鉄道を対象とした軌道状態監視システムに関する研究開発 ″. 京三サーキュラー,69(6),pp.2-7.
[44]髙田哲也, 浅野晃(2019). ″鉄道信号の安全性と安全性評価の動向 ″. 日本信頼性学会誌, 41(3),pp.198-206.

[45]髙田哲也(2018). ″STAMP によるクローズドループ型踏切制御の安全性評価″. はじめての STAMP/STPA 活用編, P.4,2.1,IPA.