講演８．鉄道と自動車技術を融合した新しいモビリティと認証

鉄道認証室　　※森 崇　　交通システム研究部　山口 大助　望月 駿登

１．はじめに

鉄道は、制動距離が自動車と比べて非常に長いことから、黎明期から間隔の制御を機械的に行う装置が運行に不可分であり、また、電気車による運転が過去から行われてきている。高速鉄道では、間隔制御の高度化や電気運転が発達し、不可分な技術となっている。また鉄道においても無線による間隔制御が国内外で都市鉄道を中心に普及しつつあり、列車間隔の短縮や効率化に貢献している。

しかしながら鉄道はその設備市場が小さいことから、装置が非常にコスト高であり、高度な制御装置の普及は稠密な運行が必要な線区又は高速鉄道以外は非常に困難な状況にあり、設備投資が難しい現状がある。また、鉄道車両についても高価であり、損益分岐点が高く、多くの事業者が既存線区の在り方を検討する状況にある。ひるがえって近年、自動車の自動間隔制御や電動車が普及しつつあり、自動車にも機能安全が求められ、鉄道と自動車の技術が近づきつつある現状にある。

本稿では、鉄道の安全性と自動車の技術発展を活用した新しい保安装置をベースとしたシステムについて検討し、規格適合性を中心に考察する。

２．現状の鉄道と自動車の融合

鉄道と自動車の融合として、いくつかの類型がある。

(1) 保安装置は鉄道と同一として、車両は自動車そのものを活用する方法

この類型には 2 つの形態が存在し、既存の軌道を活用する DMV（Dual Mode Vehicle）と、新規のガイドウェイを敷設する「ガイドウェイバス」がある。前者は高知県、後者は愛知県に存在するが、鉄道と同じ間隔制御を行うことにより、安全性を確保する。

(2) 専用道を使用するが、道路交通と同一のルールで運行するもの。

これはローカル線において、災害後鉄道による復旧が困難とされている線区で活用されており、専用道を使用するためある程度の定時性が確保できるが、安全性は自動車とほぼ変わらない。

本稿においては、国際規格に準拠し、鉄道並みの保安レベルを確保しつつ、自動車の運行柔軟性を確保できる新しいモビリティについて検討する。

３．鉄道の保安の考え方

鉄道における保安の考え方は、よく知られているように、fail-safety を重視している。これは、「正常状態という確認ができない場合、安全とされる状態に遷移させる」仕組みである。例えば、車両の離隔を確保する場合、大まかには図 1 のような仕組みで実装される場合がある。車両は自車の位置及びその長さを、地上の制御装置に報告する。その位置をもとに、後続の車両に、どこまで進行してよいかの停止限界である LMA(Limit of Moving Authority)を後続の車両に送信することで、その範囲内の移動を地上の制御装置が許可する。

安全を担保するためのいくつかの技術を鉄道は使用している。一例として、制御を行う各サブシステムの安全性の確保のため、複数のデバイスの計算結果が一致しない場合は、安全側に遷移させることにより、デバイスの故障などのランダム故障の安全性を確保する。また、ソフトウェアのバグなどシステマティック故障については、重篤度に応じて管理や技術的手法の推奨事項を定めることにより、故障を防止することとしている。これらは国際規格の中にも述べられており、IEC 62425 Annex B[1]及びそこから参照されている IEC 62279[2]に考え方が示されている。これらは本質的には、安全関連系の産業機器についての考え方と同一である。

LMA の送信が連続的に行われ、許容されている時間間隔を超えて LMA の更新がない場合、またはその情報の正当性が確認できない場合はその時点で非常停止させる。これは、いずれかのサブシステムが故障した際、安全側に遷移、または通信路が途絶することにより、LMA の更新が行なえなくなるため、安全側遷移の原則により、車両を停止させる、

または確実に安全な区間のみの走行を許可することとなる。

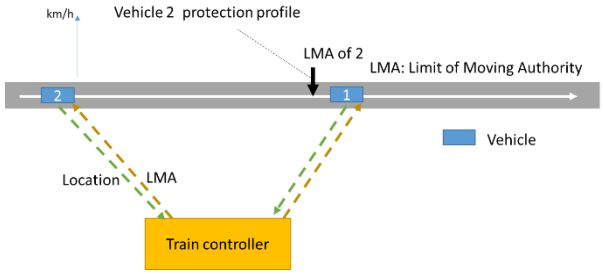

図 1　鉄道における間隔制御例

この原則により、鉄道においては、先行車両を見つけ、見つけた場合はブレーキをかけるという制御は行わない。これは、先行車両を見つけるという機能が失われた場合で、その故障が検知できなかった場合、衝突という事象が発生するため、そのような状態への遷移を防止するための思想としてそのような制御は行わないこととしている。あくまで、無難な区間においてのみ走行を許可するという思想で制御を行っている。これらの思想の具体的な要求については、IEC 62290-2[3] 5.1.4.1 Determine movement authority limit や IEEE 1474-1[4] 6.1 ATP Functions にも記載されており、鉄道の保安制御の一般的な要求事項として世界的な共通認識事項となっている。

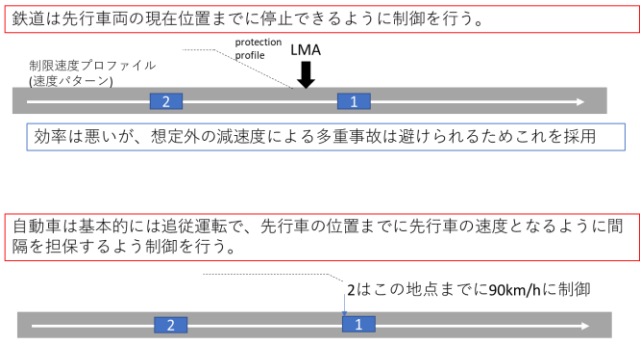

図 2　鉄道と自動車の間隔制御思想

次に鉄道と自動車の間隔制御思想の違いについて述べる。鉄道の場合は多重衝突事故の防止を非常に重視しており、前方を走行する列車との相対速度を考慮し制御するという思想は持っていない。しかしながら自動車交通においては、そのような思想について安全上は推奨されてはいるものの、実態の制御としては、相対速度をできるだけなくすように制御することが一般的であり、追従速度制御となっている。このため、鉄道の思想で運行を行う場合、どうしても時間単位当たりの輸送力は追従速度制御よりも低下することとなる。

4．モデルケースと技術課題

モデルケースとして下記のような形状の専用通路を考える。これは、一般的な鉄道複線区間の駅構造とも言え、また高速道路におけるサービスエリアの形状とも言える。このケースには、合流、分岐、間隔制御、速度制限、停車、発車を含み、一般的な鉄道のモデルを含んでいる。

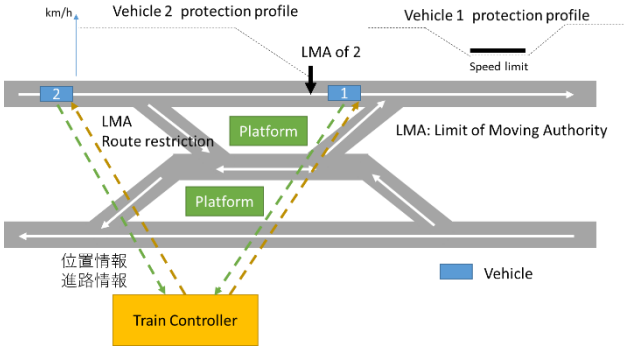

図 3　検討モデル

このモデルにおいて、必要とされる技術のうち、保安装置として代表的なものとしては、IEC 62290 によると以下のとおりである。

(1)　ensure safe separation of trains

間隔を制御するには、位置と車両長が必要。鉄軌道を使用していないため、レール短絡による位置検知は使用できず、新規の位置検知システムが必要となる。

(2)　ensure safe speed

安全な速度を担保するには、速度制限計算が必要。これには、先行列車と衝突しないための速度制限、走行路の特性による速度制限、自然条件や作業による臨時速度制限、輸送力確保のための速度制限があり、各種条件や LMA をもとにした、ブレーキ力の計算、滑走防止再粘着処理が必要。また自動運転の場合、加速計算も必要である。

(3)　authorise train movement

先行列車や合流点を基にした走行許可範囲である LMA の計算をデータが集約されている地上装置で行うことが必要。また合流する際においては、合流点までに安全な間隔を確保しつつ合流する制御が必要である。鉄道においては、線路が合流する場合、どちらか一方の車両の走行を許可し、合流点手

前で許可を受けない車両は停止させ待たせることとなるが、このような制御を行う場合、この地点がボトルネックとなり輸送力が大幅に減少することは自明である。

(4) use of data communication between wayside and onboard equipment

地上車上の通信には無線通信が必須。発達している 5G ネットワークなどを使用した場合の要件について明らかにする必要がある。

IEC 62290 規格にはないが、以下の要件も必要と考えられる。

(5) 間隔制御のボトルネックの検討

鉄道車両ではなく自動車をベースとした車両の場合、編成当たりの輸送力が減少する。ローカル線の場合はこれでも問題ない場合も多いが、ある程度の中規模線区に適用する場合は、車両間隔を適正化しないと輸送能力が大幅に低下する恐れがある。このため、鉄道の保安の思想を活用しつつ、輸送力を確保するため、何がボトルネックになるかをシミュレーションで明らかにしたのち、解決する方法を検討する。

これらはどれも重要であるが、本稿では、主に(1)と(5)について述べる。

５．位置の同定と規格

鉄輪を使用しない「鉄道」はすでに新交通システムなどで実用化しているため、技術的に位置検知は確立しているともいえる。一般的にこれらは「交差誘導線方式」[5]と言われている方法で車両を検知する。原理を図 4 に示す。車両が交番する磁束を発生し、その磁束を受けるコイルを軌道または側面に設ける。コイルはある延長ごとに交差されている仕組みとなっている。このため車両がコイルの交差点を超えると、受信機で受信された交番磁束が反転し、車両の在線位置の変化が判明する。もし車両の磁束発生装置が故障した場合やコイルが断線した場合はコイルに誘起される電流がなくなり、故障が判明することとなり、安全側に遷移できることとなる。これは、IEC 62425 Annex B における、inherent fail-safety に相当し、規格上も問題がない構成をとることができる。

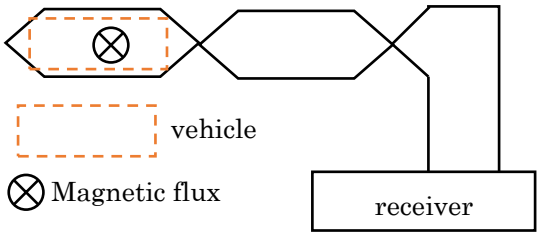

図 4　交差誘導線による検知原理

しかしながらこの方式はコイルを全線にわたり敷設する必要があり、コストの問題が過去から課題になってきた。このため、できるだけ地上システムのコストをかけず、位置検知を行う方法を検討する必要がある。

(1) GNSS を使用した方法

位置検知において、GNSS(Global Navigation Satellite System)は、各分野で普及しており、安価であるが、鉄道分野においてフェールセーフ性について明確な考え方の整理がなされている状況にはなく、電波伝搬上不可能な地域もあるため、鉄道における保安での実用化事例は乏しい。しかしながらコスト面では有利であるため検討に値すると考えている。本稿では規格上の課題と解決方針について簡単に述べる。

a) システムが正常でない場合の、安全側遷移原則の確保について

GNSS について、Preliminary Hazard Analysis を行った場合、ハザードの要因として、「衛星系の故障」、「受信機の故障」、「電波伝搬環境障害」が挙げられる。これらが発生した場合、IEC 62425 において、前述したように、故障を検知し、安全側とされる状態に遷移させることが必要であり、その失敗の頻度は、システム要求上の THR (Tolerable Hazard Rate)以下に抑える必要がある。また、規格適合性を考慮する場合は、規格が要求する、Technics and Measures を実施し検証する必要が生じる。

GNSS の衛星システムは、IEC 62425 を意識して構築されているわけではない。これは受信機においても同じである。このため、何らかの形で、故障の検知及び安全側遷移を行うため、GNSS の異常を

機器の組み合わせで故障検知及び安全側遷移をさせることを目指すとよいと考えている。

類似の事項として、fail-safety について考慮されていない集積回路を活用する場合、IEC 62425 は、C.3 b)項において、定量的な解析と悲観的に見たハザードを前提として、外部装置での故障検知及び許容時間内の安全側遷移を許容しているため、組み合わせにおける故障検知及び安全側遷移について、C.3 b)項における条件を満たす限り、許容されるものと考えている。

これらを考慮して提案する構成を以下に示す。

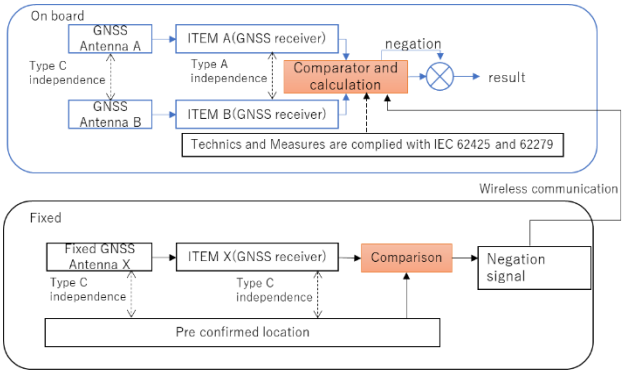

図 5　GNSS を活用した位置同定システムの案

図 5 において GNSS 受信機の故障、GNSS アンテナの故障は、IEC 62425 および IEC 62279 の規格に合致した比較器で比較し、故障検知し、異常時は安全側遷移を行う。これにより、GNSS の受信機には故障検知をはじめとするハードウェアの安全要求は行わなくとも、受信系のランダム故障検知は可能である。但し、受信機のソフトウェアの Technics and Measures は満たしていないため Pre-existing software としての要求を満たし、かつ GNSS 受信機が異なるソフトウェアを使用することによる Software Diversity を行うことにより対処を考えていく。

また、衛星系や電波伝搬の異常については、沿線数キロメートルおきに、車上と電波伝搬状態が近似となる地点に地上局を置き、地上絶対位置と測位結果を比較することにより衛星系や電波伝搬の異常を検知する。これらにより対処するシステムを提案する。

b)　路線プロファイルと位置について

GNSS で緯度経度が正確に算出できたとしても、運行は緯度経度で行われるわけではなく、走行通路のどの地点にいるかどうか、またその地点にどのような走行制約があるかどうかを正確に知る必要がある。これらの緯度経度から、路線のプロファイルに正確に置き換え、速度制限や停車位置などを守りつつ運行する必要がある。

これらのデータの正当性は、鉄道において規格上のルールがあり、IEC 62279 の 8 章に要求がまとめられている。また、そのデータを作成するツールの要件は、6.7 章に存在する。いずれにしても自動車の自動運転においてもほぼ要求されることは同一であり、これらの技術の活用を注視していきたい。

(2)　弊所の交通システム研究部により提案されている位置検知手法

前述したように、交差誘導線方式は、通路近辺にコイルを連続的に敷設する必要があることから、コストが非常にかさむ可能性があり課題となっている。そのため、弊所の交通システム研究部では、以下のようなシステムの提案と実験[6]を行っている。

図 6　ターゲットマーカ方式による位置検知

通路上に複数のターゲットマーカを敷設する。ターゲットマーカはレーザを反射する機能を有するものとする。これは反射体であるので極めて安価である。ターゲットマーカの配列に意味を持たせ、マーカの配列をスキャンすることにより車上は情報を得る。その情報をもとにデータベースと照合することにより、位置を取得できる。敷設方法を工夫することにより、Fail-safety を確保することもできる。例えば、車上からスキャンできる範囲内に必ずターゲットマーカを置き、データベースの要素と常に比較することにより、車上のスキャナとターゲットマーカの故障を連続的に検知する。故障が検知された場合は速やかに安全側遷移を行うことができ、IEC 62425 に合致した故障の検知及び安全側遷移制御ができることとなる。また、マーカの配列によっては、一部のマーカが欠損し故障した場合でも、冗長性を持たせることができ、THR を確保できる

ことが前提になるが、誤り訂正技術によって運行を継続できるとともに、故障検知も可能であり、ターゲットマーカの事後メンテナンスとするような方法も可能である。

６．新モビリティの安全性と輸送力の関係

自動車交通の場合、多くとも 50 人程度の高速バスが一単位として運行を行い、それらが相対速度で衝突を防止する追従運転制御を行っている。しかしながら、大部分の新設都市鉄道においては、前述の通り、先行の車両の後端部分から余裕距離を足した LMA の範囲内で走行を許可し、LMA までに停止できるように速度プロファイルを設定し、その速度を超過した場合はブレーキをかける方法となっている。これは、路面電車を除き、多ければ一度に 1000 人以上を輸送できる鉄道であることから 1-2km の車間距離は輸送上問題にならないことや、鉄車輪によるブレーキ力が自動車交通に比べて悪いこと、多重衝突の場合影響が甚大であることなどからそのような制御となっていると想定される。

鉄道の間隔制御方式は明らかに自動車交通よりも車間距離が広がることになる。その影響がどの程度で、現実問題として大きな影響になりうるのかをシミュレーションで検討した。

以下にシミュレーション結果を示す。前提として、LMA の計算処理時間と空走(ブレーキ処理命令を行ってから実際に減速が始まるまでの時間)を変化させた場合、また走行速度との輸送力の関係を示したものである。計算処理時間及び空走時間は、ブレーキをかけるタイミングが遅れることとなるため、その値は車両間の離隔拡大というペナルティとして現れるため、処理速度を向上させると輸送力が増大する。

この計算結果によると、輸送力は処理速度と非常に大きな因果関係があることがわかる。例えば、LMA の計算と空走の合計時間が 10 秒から 2 秒に改善した場合は、輸送力が 3 倍程度増加することがわかる。これにより処理装置の高速化がこの技術の実現の大きなカギを握ることとなる。また、速度においては 70km/h 付近に輸送力のピークがあり、自動車の速度域と合致した特性にあることがわかる。

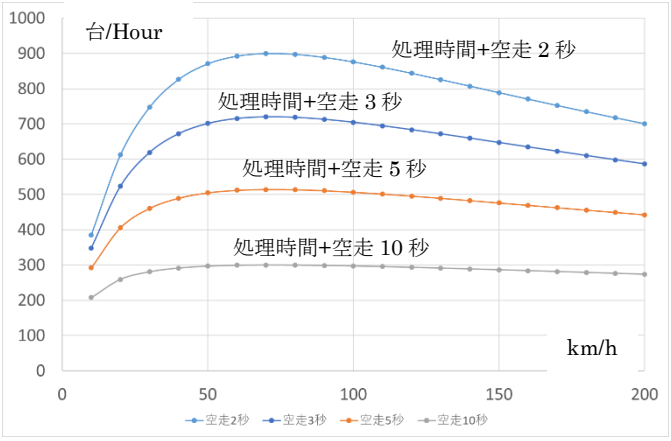

図 7　制御速度、運行速度と輸送力の関係

前提として車両長を含め最低車間 20m(速度に応じて延長され、速度が 0 のときも最低 20m は確保)、減速度 10m/s² とし、鉄道と同一の思想で保安装置を実現した場合、計算上一時間当たり 200 台から 900 台の範囲で運行することができ、これは一台当たり 10 人乗車とした場合、時間当たりの輸送力は数千人程度となる。高密度の鉄道線区には適用できないにせよ、加減速性能の高さにより、既存の新交通システムを超える程度の輸送力を処理装置の高速化で確保できる可能性がある。

７．処理高速化の戦略

現在 Fail-safety を確保するために日本国内でよく使用されている処理装置の概要を以下に示す。

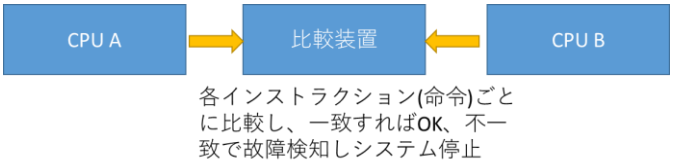

図 8　制御速度、運行速度と輸送力の関係

独立した CPU が計算を行い、インストラクションごとに比較装置で結果を比較し、一致すれば次の計算処理を許可し、不一致であればシステムを停止させる仕組みである。この比較装置の故障時の状態遷移は、安全側に遷移するように回路設計がなされている。これはインストラクションごとの比較であり、故障検知を非常に厳密に行える安全性の高い装置であるが、近年の CPU の高速化により、いろいろな課題が生じている。

- CPU の高速化により、ハードウェアの比較器の比較時間が CPU の処理時間に大きく影響を与えていること。
- CPU 黎明期のものはすべてのデータがバスに出力されており、外部の比較器により比較することも可能であったが、現在の CPU の大部分はキャッシュメモリや内蔵のメモリが存在し、必要がある場合のみバスにデータが出力されず、全てのインストラクションを比較することが困難になっていること。

上記の課題があり、鉄道信号の製作会社は、様々な取り組みをしてきたが、過去の CPU の在庫で製作することや、FPGA(Field Programmable Gate Array)に過去の CPU の IP コア(Intellectual Property Core)を導入し、互換性のあるものを作成している現状にあり、処理速度の向上を行うためには設計思想を変更する必要がある。

IEC 62425 においては、ここまでの厳密性は求められておらず、処理結果の整合性の担保のみが必要とされている。このため、故障検知と安全側遷移の目標値の確保を担保しつつ、高速処理を実現するためには、計算出力結果の比較のみを行うことで規格上は足りる。

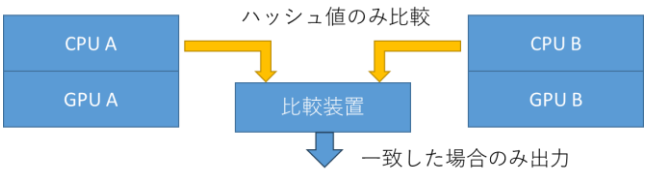

図 9　高速処理を行うための手法案

図 9 にできるだけ高速処理を行うストラクチャを示す。CPU と GPU(Graphic Processing Unit)が組み合わされている計算装置は一般的であり、入手は容易である。LMA の計算は車両ごとに行う必要があるが、どの車両においてもアルゴリズムは同一であり、GPU における並列計算になじむアルゴリズムを構築することが可能であると考えられる。それらの計算結果のハッシュ値を計算し、その結果のみを比較することにより、処理装置のランダム故障の検定を行うことを考える。これの誤りの見逃しは、ハッシュ値の系列にも依存するが、一般的に使用されている SHA-256 を活用した場合、ほぼ偏りなく均等にハッシュ値が出現するとされているため、理想的には、誤りの見逃し確率は一処理当たり 2^{-256} となり、100ms ごとに処理を行った場合の一時間当たりの誤り発生確率 p は二項定理により、

$$p = 1 - (1 - 2^{-256})^{36000} \approx 36000 \times 2^{-256}$$
$$\approx 3.1 \times 10^{-73}$$

となり、これを発生頻度に置き換えると

$$p = 1 - e^{-\lambda t} \text{から}$$
$$3.1 \times 10^{-73} = 1 - e^{-\lambda \times 1} \approx \frac{\lambda}{1!} - \frac{\lambda^2}{2!} + \cdots$$

となる。$\lambda^2/2!$以降の項は非常に小さいので無視した場合の故障発生頻度 λ は$3.1 \times 10^{-73}/h$となり一般的に許容されている THR である $10^{-9}/h$と比較しても全く問題がない値と想定される。

8．まとめ

今回検討の結果、新しいモビリティを実現していくには、保安装置単体としても、輸送計画、安全性の担保、高速処理のアーキテクチャ、位置検知技術、それに加え安全の justification など多くの技術分野の組み合わせが必要であり、総合力を生かした取り組みが必要であることを痛感させられた。総合力という観点では、自動車技術及び鉄道技術双方を兼ね備えている弊法人はそのポテンシャルを有していると考えており、今後とも多様な側面での検討を行ってまいりたい。

参考文献

1) IEC 62425 Railway applications – Communication, signalling and processing systems –Safety related electronic systems for signalling, IEC (2002)
2) IEC 62279 Ed.2 Railway applications – Communication, signalling and processing systems –Software for railway control and protection systems, IEC (2015)
3) IEC 62290-2 Ed.2 Railway applications – Urban guided transport management and command/control systems –Part 2: Functional requirements specification, IEC (2014)
4) IEEE 1474-1 IEEE Standard for Communication Based Train Control(CBTC) Performance and Functional Requirements, IEEE (2004)
5) RRR, 平栗 滋人, 鉄道総合技術研究所 (2008-12)
6) LiDAR センサを利用した衛星測位の補完手法に関する検討, 山口 大助他, 交通研フォーラム 2022