車上主体列車制御システム（無線式）開発における国際規格を活用した安全性向上の取組み

1. はじめに

ＪＲ西日本では、安全性の向上や地上設備の簡素化を目指し、列車の速度超過や列車衝突を防止するシステムである車上主体列車制御システム（無線式）（以下「本システム」という）の開発を行っています。

このシステムは東日本旅客鉄道株式会社で導入されているＡＴＡＣＳ（Ａｄｖａｎｃｅｄ Ｔｒａｉｎ Ａｄｍｉｎｉｓｔｒａｔｉｏｎ ａｎｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｙｓｔｅｍ）をベースとして、当社の列車運行形態に適用させるために様々な開発を行っています。この開発において、新たに開発した機能にシステム上の不備がないように、また新たな機能も含めてシステム全体としてより安全性の高いシステムとするべく、安全性の分析を行い、その内容について第三者に評価を受けるという取組みを行っています。

この安全性の分析および評価の進め方について、従来から社内外で蓄積してきた手法がありますが、さらに国外に目を向けると、システムの安全性などの分析および評価について体系的に整理された国際規格が存在します。

また鉄道業界全体に目を向けると、貿易の自由化の流れから鉄道に関する輸出入についてもこれまでより国際化が進み、ＪＲ西日本のような鉄道事業者としても、国際規格について理解を深める必要があると考えています。

そこで、本システムの安全性分析および評価において、国際規格の考え方を取り入れ、社外の有識者を交えたシステムの安全性分析および評価を行うこととしました。その取組みを紹介します。

2. 車上主体列車制御システム（無線式）の概要

本システムでは列車自身が列車位置を把握し、あらかじめ搭載したデータベースから線路上の制限速度などの情報を読み込みます。また、列車と地上装置は常時無線通信を行い、各列車は地上装置に列車位置を送信し、地上装置は各列車に対してルートと先行列車の状態により求められた停止限界を送信します。

これらの情報をもとに車上装置は制限速度を算出し、運転士がその速度を超えて運転を行った場合はブレーキ指令を出力し、先行列車との衝突や制限速度の超過を防止します。列車は停止限界のほか、臨時の徐行や緊急停止指令などの突発的な事象に対する情報も無線通信を介して受け取り、制御を行うことができます。

これらの制御により、突発的な事象を含めてシステムによって減速や停止を自動的に制御できるようになり、安全性が向上するとともに、従来では必要であった地上の信号機や列車の位置を検知するための設備を低減することができます。

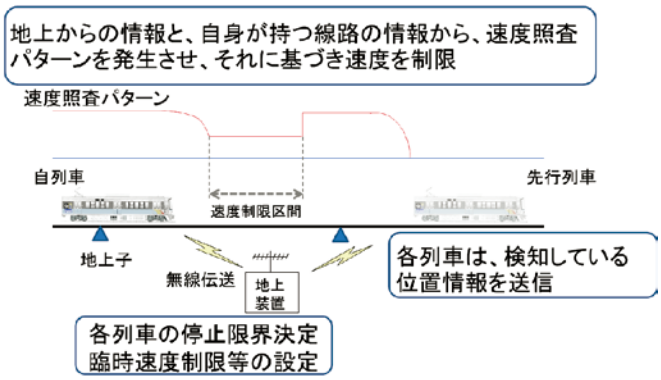

図１　：本システムの概要

3. 安全性分析および評価

本システムの安全性分析および評価は、システムの安全性などについて体系的に整理された国際規格であるRAMS規格（IEC62278）を軸に進めることとしました。

RAMSとは、Reliability：信頼性、Availability：可用性≒稼働率、Maintainability：保守性、Safety：安全性の頭文字をとったもので、システムの開発・製作から運用・廃棄に至るまでのライフサイクル全般にわたってシステムを安全・安定に稼働させるための考え方について体系的に整理されたものです。海外では、ヨーロッパを中心に広く使われています。

本システムの開発においては、安全性だけでなくRAM性（システムの信頼性、可用性、保守性）についても分析及び評価を行っていますが、ここではシステムの安全性の分析および評価について紹介します。

安全性の分析および評価においては、このRAMS規格を中心に、関連する他の規格も用いて、システムの安全性、通信の安全性・セキュリティ、運転取扱いの安全性、という大きく３つの切り口で進めることとしました。この分析及び評価は、資料の作成を行ったうえで、社外の有識者の方々に委員会形式で評価をいただく体制で進めています。

（１）システムの安全性分析および評価

システムの安全性分析および評価は、前述のRAMS規格に沿って進めています。

分析および評価を進めるに当たり、RAMS規格において求められる内容が抽象的な部分もあったため、まずは規格の内容の解釈を行い、本システムにおいて分析や評価を行うべき内容について整理しました。

そのうえでシステムの安全性についてはハザード分析（システムの制御に関係する危険な事象に対する分析）を行い、ハザードの洗い出し、リスク評価、リスク低減策の策定等をし、

それらをRAMS規格に沿ってハザードログという形でまとめました（表1）。この分析により、システムが不安全な状態になり得る事象を洗い出し、その対策をシステムの仕様に反映することができ、システムの安全性を高めることができます。

また本システムの走行試験においては、試験項目の洗い出しをRAMS規格に定められた考え方に沿って行い、本システムが想定したとおりの動作を実現できているかどうか、想定と異なる動作をしていないかを漏れなく確認できるようにしています。

（2）通信の安全性・セキュリティの分析および評価

本システムでは無線通信によって地上装置・車上装置間の通信を行うので、ノイズなどにより通信内容が誤った内容に変わり安全が阻害される事象や、無線通信の妨害や乗っ取りなどが行われるという可能性が想定できます。また地上の各装置間はネットワークにより接続することを想定しておりますが、このネットワークについても同様に安全やセキュリティに関するリスクが想定できます。

そこで、通信の安全性およびセキュリティについて、RAMS規格のほか、鉄道通信に関する国際規格（IEC62280）を用いて分析および評価を行っています。

通信のセキュリティについては脅威分析という手法を用いて分析を行い、セキュリティを向上させるための手法をシステムの仕様に反映させています。脅威分析の一例を（図2）に示します。

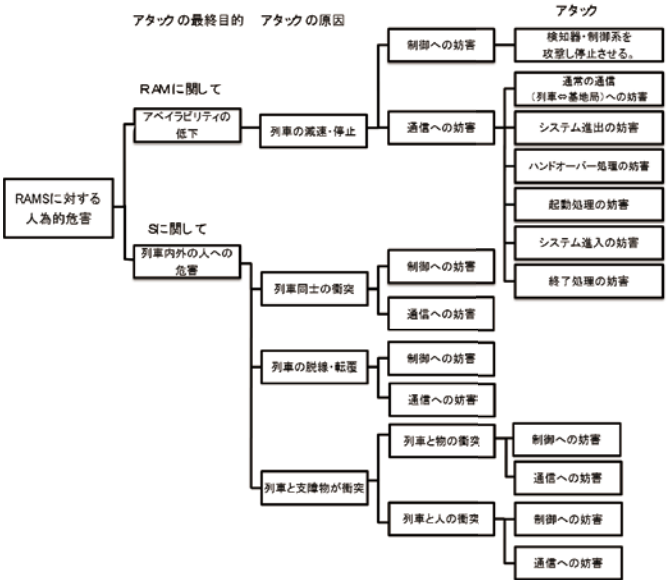

図２：脅威分析の一例

（3）運転取扱いの安全性分析および評価

本システムを使用して列車を運転する場合に、運転士や列車の運行を管理する係員などが定められたルール（このことをここでは「運転取扱い」と呼びます）を誤った場合や、またシステムが万が一故障した場合にシステムを使用せずに応急的に列車を運転しなければならなくなった場合などの場面も、安全性の分析においては想定する必要があります。そこで運転取扱いのリスクについても分析および評価を行っています。

表１：ハザードログの一例

情報		ハザードの説明						
ID	記録日	構成部品	ハザード				ハザードを導くイベント	
			ハザード	ケース①	ケース②	理由	原因-1	原因-2
1		車上装置	A-1 先行列車の在線区間に進入	A-1-1 自列車で発生する事象	A-1-1-1 本システムの要因で発生する事象	A-1-1-1-① 車上装置がシステムの制御状態から開放される	車上装置の電源が遮断	NFBのトリップ（破損を含む）
2								車両電源の遮断（破損を含む）
3								電源回路の断線（害獣等）
4								電源回路の断線・接触不良・配線ミス
5						A-1-1-1-② 自列車の位置が誤っている（または見失った）	位置補正情報の欠落	車上子の故障（破損、異物介在を含む）
6								車上子の取付け高さ調整不良
7							検知した位置情報の誤り	地上子からの受信情報のデータ化け
8								車上装置の保有する地上子データの誤り
9								乗っ取り、なりすまし

鉄道本部　技術開発部（列車制御システムＰＴ）
荒川 貴裕

この分析では、関係する運転取扱いを網羅的に洗い出したうえで、システムの安全性分析で用いる手法を応用し、運転取扱いの内容と、取扱いを誤った際のリスク評価およびリスク低減策について分析を行いました（表２）。またリスク低減策について詳細検討が必要な事象は、どのような取扱い誤りが積み重なると危険な事象に至るのか、その場合にどのようなリスク低減策が必要かを、ＥＴＡ(イベントツリー解析) という手法を活用して分析しました（図３）。

これらの分析を行うことにより、本システムを導入した区間において必要な運転取扱いの内容や、取扱いを誤った際のリスクを低減させるために必要な内容をシステムの仕様に反映させています。

4. おわりに

本システムの開発において、システム全体としてより安全性およびセキュリティの高いシステムを作るべく、国際規格を用いて分析および評価を行う取組みについて紹介しました。

この取組みを進め、安全なシステムを導入できるように開発を進めて参ります。

表２：運転取扱いリスクと対処案の一例

係員	操作内容（スイッチ等）			スイッチの機能	取扱い要件案	取扱い誤り	局所影響	最終影響	リスク評価結果	リスク低減策
運転士	（スイッチ、画面操作）	条件入力 新たに設けるスイッチ等	**非常運転スイッチの取扱い**	非常運転モード（25km/h頭打ち以外のブレーキを動作させずに走行できるモード）に遷移させる	指令員の指示を受けない限り扱わない	誤って非常運転スイッチを扱い、非常運転モードで運転する	頭打ちパターンが発生し速度が上げられない	列車遅延	安全上の影響がないため許容	–
							停止限界に対する防護が行われない	進路未構成区間に進入し脱線 他列車の進路を支障し他列車に衝突 行止りに衝突 他列車に追突	許容できない	シス評運サ１資料No.2-2-2　参照 現行より安全性が向上する
			非常運転解除スイッチの取扱い	非常運転モードを解除する	指令員の指示を受けない限り扱わない	誤って非常運転解除スイッチを扱う	影響なし（モード遷移しない）	–	安全上の影響がないため許容	–

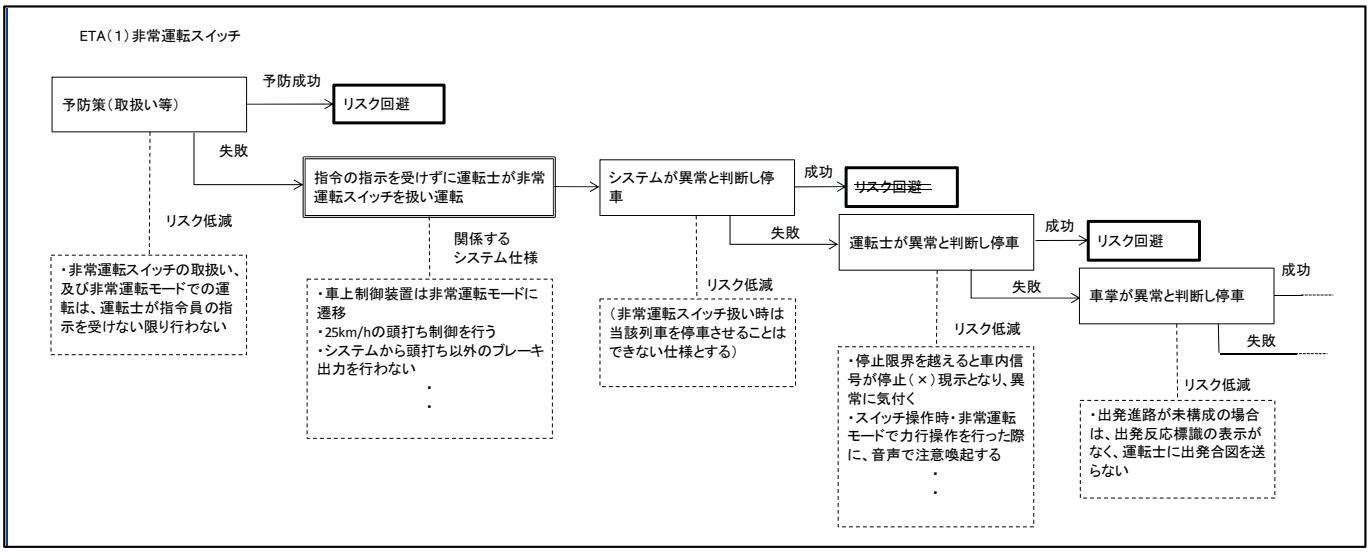

図３：ＥＴＡの一例