鉄 道 総 研 報 告

特集：信号通信技術

列車制御システム仕様書の安全性確認項目の提案

岩田　浩司*

A Proposal of Safety Requirements for Train Control Systems Specifications

Koji　IWATA

Recent train control systems tend to be larger and more complicated with the increase of the number of functions. In order to keep a very high level of safety in such a system, we are trying to prepare check items for system specifications of train control systems to be examined at the early stage in design phases to decrease the errors. In this paper, a common platform for train control systems is shown. Focused on this platform, some safety requirements defined by quantified values are shown by constraint equations. In addition, as a case study, we demonstrate an example of applying these equations to communication based train control systems with due consideration on line conditions.

キーワード：列車制御システム，安全性確認項目，システム仕様書，安全要件

1．はじめに

列車制御システムには高いレベルの安全性が要求され，システムライフサイクル全体での信頼性・安全性管理が求められる。特にシステム全体を定義するシステム仕様書は，ライフサイクルの上流に位置し，一般に鉄道事業者が作成する。この仕様書における定義漏れや記述内容の誤りは，下流の詳細設計・製造段階に大きく影響し，そこでの改修につながる可能性も高い。また，開発最終段の試験での障害分析結果では，システム仕様書に関わる誤りが 50% を占める例[1)] もある。

このような列車制御システムにおいても，信号保安装置としての高いレベルの安全性を従来同様に確保するためには，システム内の危険要因に対して対策を適切に施すことが一層必要となる。そのためには，システム仕様書への安全性確保のための要件（安全要件）の反映と，この仕様書の下流の詳細設計・製造段階への確実な反映が不可欠と考える。

下流における，システム仕様書にもとづく詳細設計・製造段階での品質向上のための管理技術は，列車制御システム以外の分野での一般産業と共通する部分も大きく，他分野での技術も参考にできる。しかしながら，高機能化に伴い，巨大化・複雑化の傾向にある列車制御システム全体を定義するシステム仕様書に安全性確保のための要件が反映されているかを確認するための機能単位での確認項目は定められていない。よって，システム開発時には，列車保安制御システムの安全性技術指針[2)] に示す基本条件をもとに適用するケース個別での確認が必要となる。また，衝突・脱線を頂上事象に FTA（故障木解析）を適用してその原因を特定し，機器を構成する要素に対して FMEA（故障モードとその影響解析）を実施してその影響を特定する。その際には，システムが複雑になるにつれて，これら解析作業は多くなり一層難しく時間を要する。

そこで，新たに作成した仕様書の誤り低減を図るため，列車制御システムを構成する機能単位での安全性確認項目を定めることとした。また，安全性の確認を容易にするため，列車制御システムの共通の基盤となる機能構成を，共通ミドルウェアとして定めた。

以下，2 章では検討対象とする列車制御システムの機能構成を述べる。3 章では，列車制御システムを構成する各機能の確認項目の設定方法を述べる。4 章では定めた安全性確認項目をもとに定式化を行い，これら確認項目間の相互の関係を制約式で定義し明確化する。また，これら項目について適用線区の条件も考慮した場合の確認項目を述べる。

2．対象機能

列車制御システムは，安全性を考慮した列車制御アプリケーションと，このアプリケーション処理を実行する処理装置で構成される。処理装置は，故障が発生した場合には安全側に遷移するフェールセーフなハードウェアが用いられる。このシステム開発においては，列車制御アプリケーションと処理装置の両方を考慮したシステム全体の動作を定義するシステム仕様書が重要である。特

＊　信号・情報技術研究部　列車制御研究室

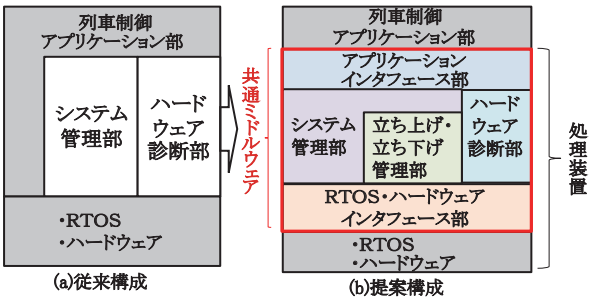

図１　提案する機能構成

に，近年のシステムは列車制御アプリケーション（ソフトウェア）で実現する機能が多く，処理装置のハードウェアに加えて，ソフトウェアで実現する機能の安全性を確認することがますます重要になりつつある。

そこで，このような高安全性が要求される列車制御システムを構成するソフトウェアで実現する機能の安全性確認を効率的に行うため，列車制御アプリケーションに関する機能と処理装置の安全性確保のための機能を明確に分けた機能構成を提案し（図 1），これら機能に対して安全性確認項目を定めた。処理装置の機能構成は，図 1 に示すように，システムを構成するソフトウェアの中から，ハードウェアに関わる共通化可能な安全関連機能（ハードウェア診断，ならびに定周期処理などのシステム管理などのハードウェア依存部分）を抽出し，共通ミドルウェアとしてモジュール化した構成としている。

共通ミドルウェアの特徴は，ソフトウェアで実現する安全関連機能のうち，ハードウェアに依存する部分を切り出してモジュール化することによって，アプリケーションから見てハードウェアの違いの影響を小さくした点である。ハードウェアの更新時にも，ソフトウェアへの影響を逐一チェックするが，共通ミドルウェア化によりソフトウェアへの影響を限定できるので，確認すべき項目数の低減が図れる。

この共通ミドルウェアを利用することで，列車制御アプリケーション特有の機能とハードウェアに関わる安全関連機能が分離可能となり，相互の影響や設計規模を低減する結果，誤りそのものの発生の低減が期待できる。

３．安全性確認項目の抽出

列車制御システムの安全性確認項目は，先に定めた共通ミドルウェアを用いた機能構成での各機能に対して定める。各機能は安全性に関わることから，これらに適用されている安全性技術を明確にする必要があるため，安全要件のフォーマット[1]（図 2）を適用する。この安全要件のフォーマットは，安全性確保の手法に着目して，制御論理・構成による「危険要因の排除」欄と，排除できない場合における診断機能の追加による「危険要因の低減」欄で構成される。

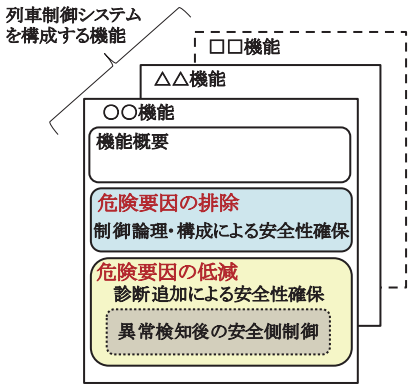

図２　安全要件のフォーマット

このように，適用する安全性技術を区分するフォーマットを適用することで，システム仕様書から排除された危険要因も明示することが可能になる。また，異常検知後の安全側制御を定義するための欄も設けてあり，仕様の定義漏れの防止を図ることが期待できる。

各機能に対する安全性確認項目は，列車保安制御システムの安全性技術指針[2]に示すソフトウェア・ハードウェアの基本条件を参考に定めた。また，従来システムで適用されている対策[3][4]なども参考にした。これら確認項目を定める際には，出力誤りを頂上事象とした FTA，また各機能の誤りの影響を確認するため FMEA も実施した。

ハードウェア診断部における安全性確認項目の一例を表 1 に示す。処理装置における「危険要因の排除」の例としては，比較対象の両系間での共通原因故障を排除するための独立性の確保があげられる。また，「危険要因の低減」の例としては，メモリチェックなどの故障診断があげられる。この故障診断で異常を検知した時には安全側制御（処理停止）させる。

また，列車制御アプリケーションの機能については，車上の位置検知結果をもとに間隔制御を行い，そのため地上・車上間の伝送に無線を用いるシステム[5][6]を対象に実施した。

４．安全性確認項目の制約式化と定量的検討

3 章で抽出したシステムを構成する機能単位での安全性確認項目の中には，定量的に明示することが可能な項目もある。これらの項目を対象に，定量化可能な要因相互の関係を制約式として定め（制約式化），安全性確認項目の明確化を図る。また，処理装置とアプリケーションを合わせたシステム全体として満たすべき安全性確認項目を定義する。さらに，これらシステムとしての確認項目と，適用線区に関わる要件とのトレードオフを検討する。

表１　処理装置（ハードウェア診断部）に関わる安全性確認項目の例

分類		危険要因の排除による安全確保	危険要因の低減による安全確保	異常検知後の安全側処理
(1) 入力	(1-1) リレー接点	・リレーは故障モードの非対称性を保証すること ・リレー接点は落下側を安全側に割り当てること ・安全側値の割り当て不可の場合は N, R 側の 2 点入力の構成とすること **・安全側の値を 0 に割り当てること** **・不安定入力に対してマスクすること** **・前回値保持の有無を明確化すること** **・入力周期，入力回路の診断周期を特定すること** **・入力状態継続時間を特定すること**	照査パルス診断による入力回路診断	**・安全側値の割当，異常時処理** ・当該入力の使用停止
	(1-2) シリアル	**・入力周期を特定すること** **・安全側の値を 0 に割り当てること** **・不安定入力に対してマスクすること** **・前回値保持の有無を明確化すること** **・伝送遅延，処理遅延時間を特定すること** **・入力状態継続時間を特定すること**	**・保安伝送としての合理性チェック（A/B 系照合対象のソフトウェアで付加する CRC 検定，等）** **・伝送断検知（伝送断許容時間，通番の大きさを定めること）** ※ IEC62280 参照。アプリケーション固有の診断はアプリケーション部で実施	**・安全側値の割当，異常時処理** ・当該入力の使用停止
(2) 処理	(2-1) CPU	・A 系と B 系の独立性を確保すること **・A 系と B 系を同期させること（照合方式に依存）** **・処理周期を特定すること** **・条件変化のとりこぼしがないことを確認すること** **・処理負荷を確認すること**	・処理結果診断（バス同期でなく，結果同期方式の場合は，A/B 系照合項目を設定すること） **・処理渋滞状態の検知** ・処理順序診断 **・CPU 電圧の診断**	・処理停止 ・安全側出力
	(2-2) メモリ	・A 系と B 系の独立性を確保すること **・処理で使用するメモリ配置を明確化すること**	**・ROM/RAM 診断（診断対象エリア，診断周期を定めること）** ・メモリプロテクションによる不正なアクセス検知	・処理停止 ・安全側出力

※**下線太字**箇所：定量的な値を用いる確認項目

これらの検討手順を図 3 に示す。以下，各 STEP の概要を述べる。

4.1　STEP 1：システム内での制約の定式化

先に述べた処理装置の各機能についての安全性確認項目のうち，時間に関わる値を割り当て可能な項目を対象に，項目間の関係を制約式で示した（表 2）。制約式は，まず機能単位での確認項目をもとにボトムアップで作成し，その後，これら相互を関連づけるため，トップダウン的にキーワードを設定し集約した。ここでのキーワードは，「処理装置のモード」，「装置の入出力」，「処理遅延」とした。また，表 2 に示す各項目相互をさらに関連づけるため，時間に関わる誤りモードに着目して，状態継続時間（制御装置における状態変化入力のとりこぼし），伝送断時間（瞬時伝送断），遅延時間（遅延）を観点に集約し，この結果を処理装置における時間に関わる安全性確認項目とした（表 3）。

以上のように定めた処理装置における時間に関わる安全性確認項目と，同様にして作成した列車制御アプリケーションでの安全性確認項目との共通項をもとに，処理装置と列車制御アプリケーションとのインタフェースとなる確認項目を定めた（図 4）。これら確認項目は「遅延時間の最大値」，「状態継続時間の最低値」，「伝送断時間の許容値」とし，さらに時間管理の基本となる「制御周期」も追加した。

特に，制御周期を変更した場合は，図 4 に示す過程で列車制御アプリケーションに影響することから，システム全体に大きな影響を与える。例えば，処理装置の制御

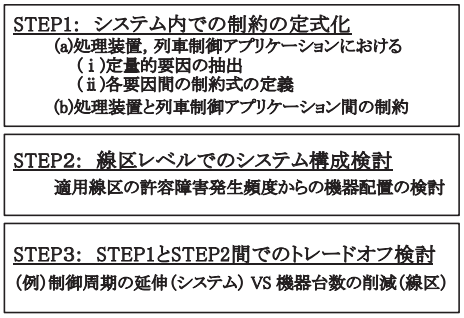

図３　システム構成の検討手順

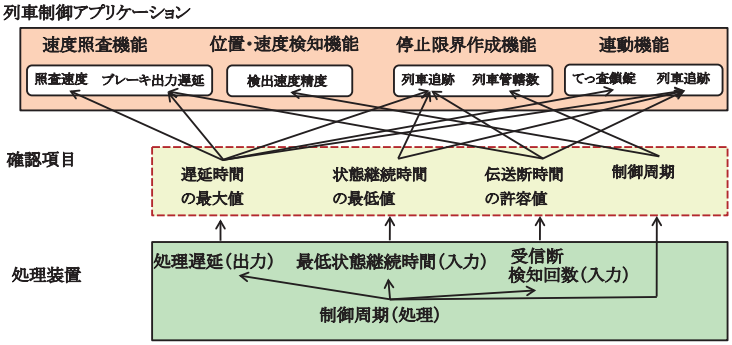

図４　処理装置と列車制御アプリケーションとのインタフェースとなる確認項目

表２　処理装置における時間に関わる安全性確認項目の制約式一覧

		制約式	ID
(1)処理装置のモード	(1–1)立ち上げ	立ち上げ所要時間 ≧ 全ハードウェア診断時間	1
		立ち上げ処理時間 ≦ WDT 監視時間	2
	(1–2)運転	状態継続時間 ≧ 制御周期×２　※状態変化と制御周期は非同期の場合	3
		状態継続時間 ≧ 制御周期　※状態変化と取込周期は同期の場合	4
		状態継続時間 ≧ 取込周期×２　※状態変化と取込周期は非同期の場合	5
		状態継続時間 ≧ 取込周期　※状態変化と取込周期は同期の場合	6
		状態継続時間 ≧ 系切替に伴う入力断（系切替時間）	7
		出力断許容値 ≧ 系切替に伴う出力断（系切替時間）	8
	(1–3)立ち下げ	WDT 監視時間 ≦ 故障発生後の立ち下げ所要時間 ≦ 安全側固定への遅延許容時間	9
	(1–4)再立ち上げ	状態継続時間 ≧ 再起動所要時間	10
		再起動所要時間 ≧ 伝送断検知時間　※一時的な伝送断もしくは出力断を許容できる場合	11
		再起動所要時間 ＜ 伝送断検知時間　※一時的な伝送断もしくは出力断を許容できない場合	12
(2)装置入出力	(2–1)リレー入出力	入力状態継続時間＞入力周期×入力一致検定回数＋不安定入力マスク時間	13
		入力状態継続時間＞入力周期×入力一致検定回数＋不安定入力マスク時間＋前回値保持時間	14
		出力状態継続時間＞出力周期×一致回数＋不安定出力マスク時間	15
		出力状態継続時間 ≧ 入力状態継続時間	16
		リレー接点入力回路の診断周期　≦　入力周期	17
	(2–2)シリアル入出力	許容伝送遅延時間 ≧ 伝送遅延時間（伝送周期）＋不安定入力のマスク時間＋処理遅延時間（制御周期）＋伝送断検知時間＋伝送断検知時の前回値保持回数×入力取込周期	18
		入力状態継続時間＞入力周期×入力一致検定回数＋不安定入力マスク時間＋伝送断検知時の前回値保持回数×（伝送周期もしくは制御周期）	19
		出力状態継続時間 ＞ 出力周期×出力一致回数＋不安定出力マスク時間 ≧ 入力状態継続時間	20
		最大伝送遅延時間 ＞ 制御周期 ≧ 最小伝送遅延時間　※この制約条件を満たす場合には受信順序の逆転となる	21
		通番の最大値×伝送周期 ＞ 伝送断検知時間	22
(3)処理遅延	(3–1)処理負荷	最大処理負荷に要する時間 ＜ 制御周期 ＜ WDT 監視時間	23
		定周期診断に要する時間 ＜ アイドル時間	24
		制御周期 × 定周期診断の分割数　≦　定周期診断時間の許容値	25
	(3–2)処理タイミング	クロック変動量 ≦　クロック診断値　≦ アプリケーションでの許容時間変動量	26
		クロック変動量　≦ 照合系間の同期ずれ許容値 ≦ 冗長系間の同期ずれ許容値	27
	(3–3)タスク切替	タスク切替時間 ≦ 出力断許容時間	28
		タスク切替時間 ≦ 入力断許容時間	29
	(3–4)排他処理	排他処理による処理遅延を含む１制御周期 ≦ 制御周期 ＜ WDT 監視時間	30
		排他処理による入力，出力断，遅延 ≦ 入力，出力断許容値，入力，出力遅延許容値	31
	(3–5)不安定入力対策	不安定入力のマスク値 ＜ 入力状態継続時間	32
		前回値保持回数×（伝送周期もしくは制御周期）＜ 入力状態継続時間	33
		前回値保持回数 ＜ 入力一致検定回数	34

表３　処理装置における時間に関わる安全性確認項目

	制約式	対応する表２の ID
(1)状態継続時間	(1-1) とりこぼし【全体】	
	状態継続時間－系切替に伴う入力断（単一系での再起動も対象の場合は再起動所要時間含む）≧ 制御周期×２ ≧ 取込周期×２ ※状態変化と制御周期が非同期系の場合	3,5,7,10
	状態継続時間－系切替に伴う入力断（単一系での再起動も対象の場合は再起動所要時間含む）≧ 制御周期 ≧ 取込周期 ※状態変化と制御周期が同期系の場合	4,6,7,10
	(1-2) とりこぼし【入力】	
	入力状態継続時間＞入力周期×入力一致検定回数＋不安定入力マスク時間＋前回値保持回数×（伝送周期もしくは制御周期もしくは入力取込周期）	13,14,19,32,33
	なお，リレー接点入力回路の診断周期　≦　入力周期。前回値保持回数 ＜ 入力一致検定回数	17,34
	(1-3) とりこぼし【出力】	
	出力状態継続時間 ＞ 出力周期×出力一致回数＋不安定出力マスク時間 ≧ 入力状態継続時間	15,16,20
(2)伝送断時間	(2-1) 瞬時伝送断	
	伝送（入力・出力）断許容値 ≧ タスク切替時間＋排他処理時間＋系切替に伴う出力断 ※単一系での再起動時は再起動所要時間の考慮も必要	8,11,12,31
	タスク切替時間＋排他処理による入力断 ≦ 入力断許容時間	29,31
	タスク切替時間＋排他処理による出力断 ≦ 出力断許容時間	28,31
	許容伝送遅延時間 ≧ 伝送遅延時間（伝送周期）＋不安定入力のマスク時間＋処理遅延時間（制御周期）＋伝送断検知時間＋伝送断時の前回値保持時間	18
	通番の最大値×伝送周期 ＞ 伝送断検知時間	22
(3)遅延時間	(3-1) 遅延【立ち上げ】	
	立ち上げ所要時間 ≧ 全ハードウェア診断時間	1
	立ち上げ処理時間 ≦ WDT 監視時間	2
	(3-2) 遅延【入力，出力】	
	最大伝送遅延時間 ＞ 制御周期 ≧ 最小伝送遅延時間　※この制約条件を満たす場合には受信順序の逆転となる	21
	排他処理による入力，出力遅延 ≦ 入力，出力遅延許容値	30
	(3-3) 遅延【定周期処理】	
	クロック変動量≦　クロック診断値　≦照合系間の同期ずれ許容値≦冗長系間の同期ずれ許容値　≦アプリケーションでの許容時間変動量	26,27
	排他処理による処理遅延＋最大処理負荷に要する時間 ＜ 制御周期 ＜ WDT 監視時間	23,30
	定周期診断に要する時間＜アイドル時間	24
	制御周期 × 定周期診断の分割数　≦　定周期診断時間の許容値	25
	(3-4) 遅延【立ち下げ】	
	WDT 監視時間 ≦ 故障発生後の立ち下げ所要時間 ≦ 安全側固定への遅延許容時間	9

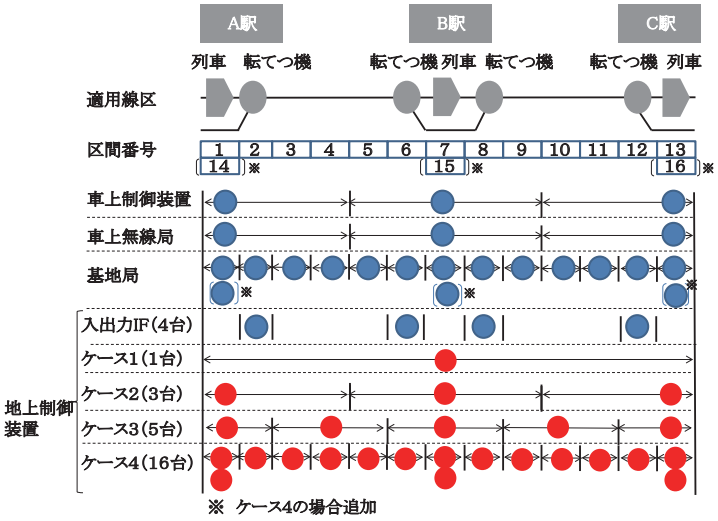

図５　機器配置

表４　１機器あたりの許容停止時間

システム構成	１システムあたりの構成機器数	１機器あたりの許容停止時間（分）
（ケース 1）集中連動相当	24	0.042
（ケース 2）各駅に設置	26	0.039
（ケース 3）駅，駅中間に設置	28	0.036
（ケース 4）各ブロックに設置	42	0.024

周期を長くした場合には，遅延時間が大きくなり，列車追跡においては実際の列車位置とシステムの認識位置のずれが大きくなる。このように，処理装置の制御周期を変更した場合には，列車制御アプリケーション機能に対する影響を確認する必要があることがわかる。これら確認項目は，システム開発時において，システム全体を定義する仕様の整合性がとれていることの確認に用いることができる。

4.2　STEP 2：線区レベルでのシステム構成検討

適用線区における機器の障害発生頻度の目標値（許容障害発生頻度）から機器配置を検討する。ここでは，一例として機器の障害に伴う線区の目標停止時間（許容停止時間）は 1 時間あたり 1 分（アベイラビリティ 98.3%）と仮定する。検討対象は図 5 に示す 3 駅 2 中間とし，地上制御装置の集中化の度合いを変えたケース 1 ～ 4 の構成である（図 5）。

線区の目標値を達成するために必要となる各箇所の 1 時間あたりの許容停止時間，ならびに機器配置を表 4 に示す。許容停止時間は，目標停止時間を機器数で除して算出した。

4.3　STEP 3：STEP 1（システム要件），STEP 2（線区要件）間のトレードオフ検討

システムに関わる要件と線区要件とのトレードオフとして，線区要件に関わる各機器の許容障害発生頻度と，システム要件に関わる列車追跡遅延を例に述べる。

各機器の許容発生頻度は，線区の許容発生頻度をもとに，システムを構成する機器数をもとに決定する。許容発生頻度は集中化してシステムを構成する機器数を減らすほど，大きくすることができる。一方，列車追跡遅延量は，システムが認識している列車位置と実際の列車位置とのずれの距離であり，制御周期を短くするほど，そのずれの量は小さくできる。

仮に，線区の要件をもとに機器を集中した場合には，1 機器あたりの処理量は増大するので，制御周期は大きく設定する必要がある。よって，線区要件の面から機器数を減らして各機器の許容障害発生頻度を大きくするべきか，それとも，システム要件の面から制御周期を短縮するべきかの比較検討（トレードオフ検討）を行う。

(1) 前提条件

制御周期は，機器の集中度に比例して伸びると仮定し，ケース 3 での 200ms を基本として最小値は 100ms，最大値は 600ms とした。

列車追跡の遅延量は，伝送断の発生回数の許容値を連続して 3 回とし，列車速度は 130km/h として算出する。

1 構成要素あたりの許容障害発生頻度は，1 機器あたりの許容停止時間を，1 障害発生後の停止時間（120 分）で除して算出する。ここでは障害発生時の暫定運転はしないものとし，停止時間は集中度によらず一律 120 分と設定した。なお，この仮定は機器集中化とこれに伴う制御周期の影響の検討に影響するものではない。

(2) 解析結果

標準的な構成と思われる「(ケース 3) 駅・駅中間に制御装置を設置する方式」と比較して，各ケースでのトレードオフを観点とした確認項目の例を示す。

①ケース 1 とケース 3 との比較

「(ケース 1) 集中連動相当の方式」は，ケース 3 と比較して機器数が少ないので 1 構成機器あたりの許容障害発生頻度を大きく設定できる。しかし，その効果は図 6 に示すように，3.0×10^{-4} 回 /h から 3.5×10^{-4} 回 /h への増加にとどまる。これは地上制御装置の集中化に対して，それ以外の構成要素の寄与の方が大きいことに起因する。その一方，地上制御装置の機器を集約することに伴い，制御周期を 200ms から 600ms まで長くなるデメリットが生じ，列車追跡遅延量は 22m から 65m まで約 3 倍増大する。

このようなことから，制御周期の増大は進路制御の遅

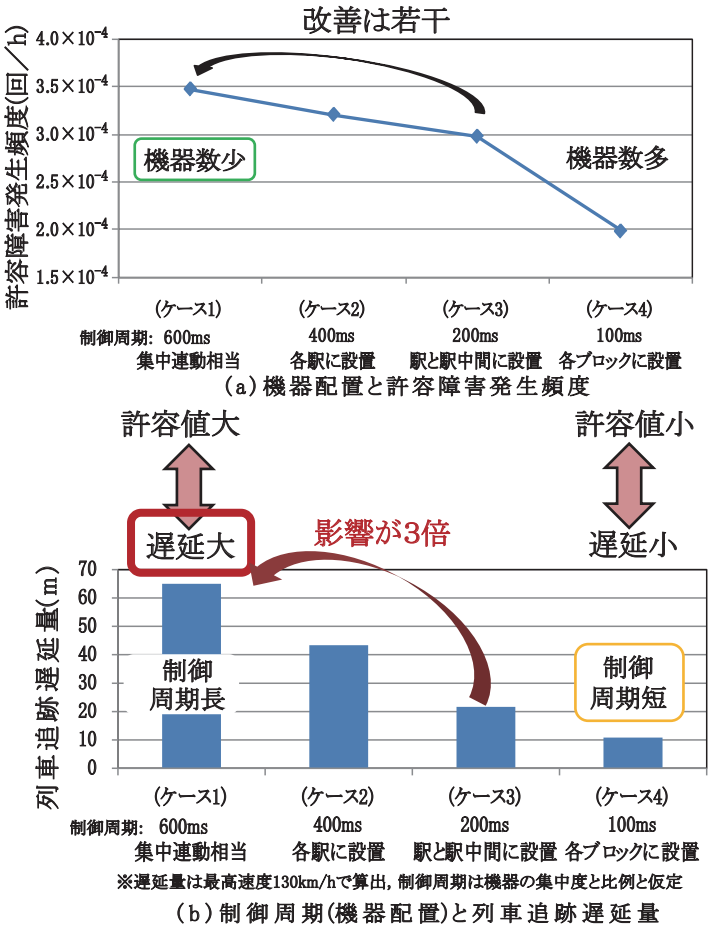

図６　許容障害発生頻度と列車追跡遅延量のトレードオフの検討例

れ，転換の遅れ，現示アップの遅れなどの装置要因に影響を与えることが想定され，影響が大きい。よって，集中化する場合はこれらの影響が許容範囲内であることの確認が必要となる。

②ケース４とケース３との比較

「(ケース４) 各区間に制御装置を設置する方式」は，区間ごとに地上制御装置を設置する構成である。制御周期は短く，列車追跡の遅延量は小さくできる。一方，各システムの構成機器に対する許容障害発生頻度に対する要求値は厳しくなり，設計が難しくなる。よって，この実現可能性についての確認が必要となる。なお，要求値の実現の際には，ここでは停止時間は一定と仮定したが，停止時間の削減の面からの検討策も有効である。

なお，現時点ではハードウェアの技術的な課題から実現できなくても，将来，処理装置の性能が向上した場合は，列車制御アプリケーションへの影響を小さくできる可能性がある。

５．おわりに

列車制御システムの高機能化に伴い，ソフトウェアは巨大化・複雑化の傾向にある。このようなシステムにおいて，信号保安装置としての安全性を確保するため，列車制御システムの共通基盤となる共通ミドルウェアを定め，システムを構成する機能単位での安全性確認項目を定めた。これら安全性確認項目のうち，定量化可能な項目については，項目相互の制約を明確にするため，地上・車上間の伝送に無線を用いた列車制御システムを一例に，システム全体として満たすべき定量的な安全性確認項目を示した。特に，処理装置の制御周期を観点に，処理装置とこれに搭載される列車制御アプリケーション間での安全性に関わるインタフェースとなる確認項目を示した。また，線区条件を考慮した場合の確認項目について示した。これらは，設計段階だけでなく改修段階においても，仕様変更に伴う労力，コスト低減に資するものであり，ライフサイクルを意識したシステムの安全性管理手法の要になると考える。

文　献

1）岩田浩司：列車制御システムの概念設計段階における安全性確認手法，鉄道総研報告，Vol.26，No.7，pp.5-10, 2012
2）鉄道総研 , 列車保安制御システムの安全性技術指針，1996
3）秋田雄志，渡辺俊勝，中村英夫 : 電子連動装置 SMILE の開発 , 鉄道技術研究報告 No.1361，1987
4）マイクロエレクトロニクス信号保安装置の安全性検討会：信号保安装置へのマイクロエレクトロニクス導入指針，鉄道技術研究所速報，No.A-83-147，1983
5）岩田浩司，西堀典幸，平尾裕司：無線による列車制御システム CARAT の事前安全性解析，鉄道総研報告，Vol.13, No.8, pp.39-44, 1999
6）無線式列車制御システム，JIS E 3801，2009