鉄 道 総 研 報 告
特集：信号通信技術

非フェールセーフ装置が混在する環境における安全関連伝送

福田　光芳*　　岩田　浩司*　　菅原　宏之*
北野　隆康*　　川﨑　邦弘**

Safety-related Communication in Transmission Systems that are Mixed with Non-safety-related Devices

Mitsuyoshi FUKUDA　　Kouji IWATA　　Hiroyuki SUGAHARA
Takayasu KITANO　　Kunihiro KAWASAKI

IEC 62280 defines requirements for safety related transmission systems in railway systems. Although the standard mentions the communication between fail-safe devices, there are many systems under which communication with non-fail-safe devices is conducted. So, it is necessary to confirm requirements for safety related transmission between devices including the non-fail-safe devices. However it is difficult to determine the behaviors of the devices, and every failure, in any transmission system, appears as the same event as threats described in IEC 62280. We analyzed the safety related transmission with non-fail-safe devices by this concept. In this paper, we describe the method of the analysis and the results.

キーワード：安全関連伝送，非フェールセーフ装置，IEC 62280，プロトコル , 安全性

1．はじめに

ネットワークで接続される構成の信号システムは今後も増えていくとみられる。安全に関連する伝送（以下，安全関連伝送）の国際規格としてIEC62280[1)]が定められている。この規格では，フェールセーフ装置（以下，FS装置）間の伝送について規定しているが，現実のシステムでは，同一ネットワーク内に接続された非フェールセーフ装置（以下，nFS装置）を含めて安全性を確保する必要がでてくる。

これまで，新しいシステムの開発の都度，FS装置とnFS装置の混在環境における安全関連伝送（以下，混在環境における安全関連伝送）に必要な安全性技術の検討や検証・評価が行われてきた。しかし，その都度，独立して検討を行う状況では，効率的な開発を阻害するだけでなく，技術・知見の共有や管理を行うことに支障をきたす恐れがある。そこで，本研究では，混在環境における安全関連伝送の安全性技術の類型化・一般化を行うこととした。なお，本研究では専用の有線伝送路で構成したネットワークを対象とし，その安全性について検討することとした。非フェールセーフ装置が混在するネットワークでは，危険側に推移する要因として装置等の異常と外部からの攻撃があり，これらを切り分けて議論する必要がある。専用の有線伝送路を対象とする場合，外部の要因に比べて装置の異常による危険側推移の可能性が高くなることから，本研究では装置の異常に着目し，外部の要因への対策であるセキュリティについては扱わないとした。

＊　信号・情報技術研究部　列車制御研究室
＊＊　信号・情報技術研究部　ネットワーク・通信研究室

2．リスク解析

2.1　伝送システムの構成の分類

必要な安全性技術は伝送システム構成（FS装置，nFS装置の機能割り当て等）により異なるので，まず，伝送システムの構成を図1の通り分類した。その中で本研究の対象となる混在環境における安全関連伝送を構成1～3と分類した。構成1, 2はnFS装置が主体となってフェールセーフ装置に問いかけ等の動作を起こす構成であり，構成3はnFS装置がフェールセーフ装置に対して従属的に動作する構成である。現状では，主に人間が介在してHMI（Human-machine interface）の処理を行う構成1が広く適用されている。nFS装置が自発的に現場機器等を制御する構成やnFS装置間で伝送を行って制御等を行う構成については，現状では信号システムに適用することが困難と考えられるので，今回の対象からは除外した。

2.2　混在環境における安全関連伝送の考え方

機能安全に関する国際規格IEC61508-2[2)]（7.4.4.1.3）において，一つ以上の構成要素の故障モードが定義でき

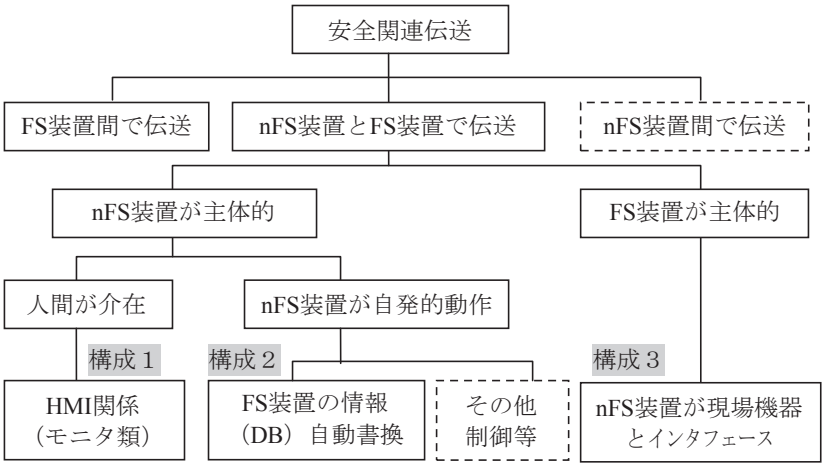

図１　伝送システムの構成の分類

ない，あるいは，故障状態における振る舞いが完全に把握できない等の性質を持つ機器を定義している。本研究で対象としている nFS 装置は，この定義に含まれると考える。規格ではこのような機器に安全関連の機能を割り当てる場合の条件を“hardware fault tolerance（HFT）”，“safe failure fraction of an element（SFF）”の 2 つの軸で示している。前者（HFT）は故障発生時に危険側の状態へ遷移する可能性の指標であり，何箇所の故障までが危険側に遷移しないかの数量を示している（0,1,2 の 3 区分が示されている）。後者（SFF）は，危険側に遷移しない確率の指標であり，故障時の状態を安全側に遷移，危険側に遷移するが検知可能，危険側に遷移して検知不可能の 3 種類に分け，安全側に遷移，または，危険側に遷移するが検知可能となる確率を示す。HFT の数量と SFF の確率により，適用可能な SIL（Safety Integrity Level）が示されている。特に HFT が 0（1 か所の故障で危険側に遷移する可能性がある）の場合は，確率だけでなく，十分な時間間隔で監視を行うことが条件に追加される。

本研究では，このような考え方を参考として検討を行った。nFS 装置と FS 装置の 2 つを合わせた構成を全体システムの中の 1 つの要素と位置づけ，nFS 装置内の 1 か所の故障で危険側へ遷移しないこと（HFT>0），あるいは，遷移させないための FS 装置側でのチェック項目を検討した。

2.3　非フェールセーフ装置とフェールセーフ装置間の伝送の解析

nFS 装置と FS 装置間の伝送について，ボトムアップ的な解析として一般的なプロトコルを仮定した網羅的な解析，トップダウン的な解析として，FTA（Fault Tree Analysis）を行った。また，検討漏れを防ぐ目的で，異常事象の発生要因に着目した解析を補足的に行った。

2.3.1　一般的なプロトコルを仮定した網羅的解析[3)]

nFS 装置と FS 装置間の伝送について，一般的なプロトコルを仮定した網羅的な解析を実施した。具体的な解析を行うにあたり，構成 1 ～ 3 に対応する検討用のプロトコルを作成し，伝送のステップ毎に 6 種類の事象（脅威）を発生させ，危険側に推移する前に検出可能であるかを調べた。基本的な考え方は次の通りである。

nFS 装置→ FS 装置，および，FS 装置→ nFS 装置の伝送に現れる異常事象は，nFS 装置や FS 装置の故障等に起因するもの，伝送システムに起因するものに分類できる。伝送システムに起因する異常は，IEC 62280 にも示される通り，重複，削除，挿入，順序誤り，破壊および遅延の 6 つの脅威に集約できる（セキュリティを対象外としているため，なりすましを除外）。また，FS 装置については，自装置に故障等が発生しても誤った出力を行わないことが求められるので，異常時には出力なし（削除に相当）になると考える。nFS 装置については，故障時の挙動が特定できないため，様々な事象を想定する必要がある。一方で，nFS 装置と FS 装置の伝送に着目すると，nFS 装置の故障等に起因する事象は，全て伝送に現れる。従って，nFS 装置の伝送に関する異常事象は，伝送システムと同様に，先述の 6 つの脅威を考えればよい。なお，nFS 装置はそれぞれの構成に応じ，FS 装置以外の機器（構成 1 の場合はユーザインタフェース用の表示や入力の機器，構成 3 の場合は制御される現場機器等）にも接続されるが，これらとの入出力も同様に先述の 6 つの脅威に集約できる。

また，次の前提条件に基づいて解析を行った。

- FS 装置が nFS 装置の異常を検出した（検出可能な）場合は，安全側制御を行う，または，プロトコルに従った再送要求等の処理を行うこととし，以降の解析を省略する。
- FS 装置が自装置の異常を検出した場合も同様に安全側制御を行うため，解析においては，FS 装置の異常を省略する。
- nFS 装置も自装置の状態や FS 装置からの電文の検定を行うが，安全性の観点からは，確実に検定できるとはいえない，nFS 装置では異常の検出を行えないという最悪条件で解析する。

なお，使用したプロトコルでは，nFS 装置と FS 装置間は論理的に 1 対 1 の伝送を行っており，プロトコルとして示した手順に従ってメッセージが発生するため，順序誤りは発生しないこととした（伝送システム上に発生した順序誤りは挿入，破壊で考慮）。構成 1 のプロトコルを図 2，構成 2，3 のプロトコルをそれぞれ図 3，図 4

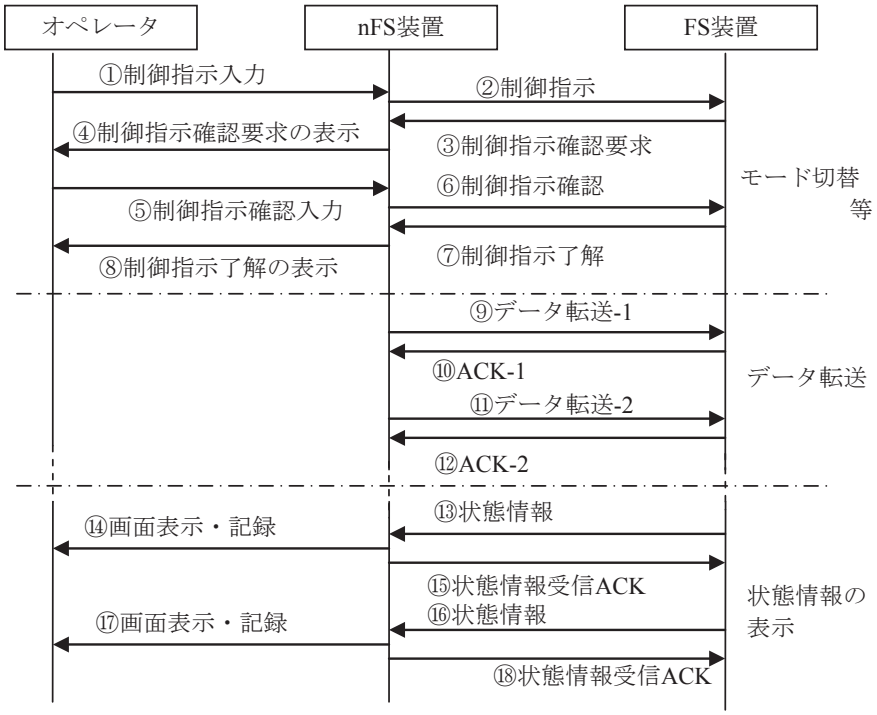

図２　解析用プロトコル（構成 1）

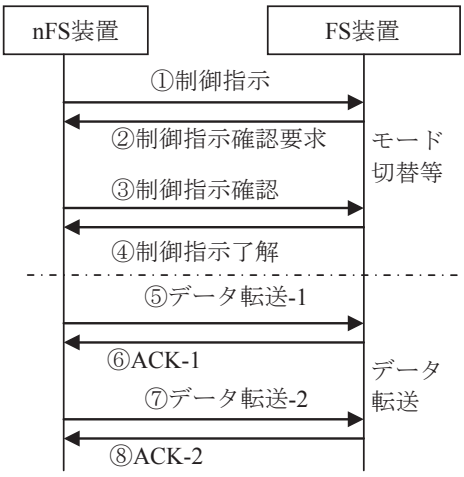

図３　解析用プロトコル（構成 2）

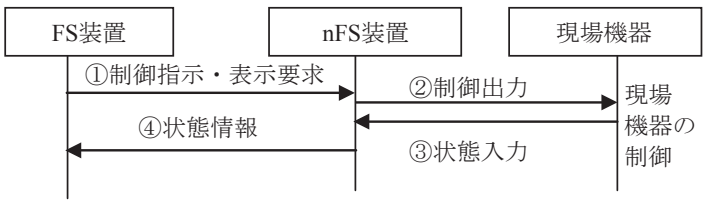

図４　解析用プロトコル（構成 3）

に示す。

構成1の解析結果の一部を抜粋したものを表1に示す。「No」の番号は，図2の矢印の番号に対応する。それぞれの電文に対して，各事象が発生した時の動作を一番右側の欄に示している。「FS 装置で検出」と書かれている場合は，FS 装置の機能により安全が確保されることを示す。ただし，網掛けとなっている箇所（意味論的チェック，タイムアウト等）は，形式的なチェックでは検出することができないので，処理内容の意味的なチェックができるようなフォーマット（意味論的チェック）やシステムの挙動の定義（タイムアウト時の挙動）を適切に行う必要がある。また，矢印と番号（→②など）が記載されている箇所は，その番号の電文に対して異常事象が発生してしまうことを示す。例えば，①に挿入が発生すると，「→②の挿入」となっているので，②の電文の挿入が発生することがわかる。①のほとんどの事象は FS 装置で検出可能であるが，挿入事象（誤って入力した，あるいは，キーボードが引っ掛かり誤入力になった等）は，FS 装置では検定できず，③，④の挿入が発生し，最終的に④をオペレータがチェックするまで検出できないことがわかる。

これらの解析より，FS 装置間の伝送で実施しているような対策に加え，次の事象への対策が必要であることがわかった。

・nFS 装置が 1 つの処理を複数回の処理として複数回送信される（構成 1，2，3）。
・nFS 装置あるいはオペレータのミスにより，不正な制御指示の電文が送信される（構成 1，2）。
・オペレータの入力なしに，nFS 装置が疑似的にオペレータの認証に相当する電文を送信する（構成 1）。
・FS 装置から nFS 装置への電文が削除された場合に，nFS 装置が適切に事象を検出できない（構成 1, 2, 3）。
・FS 装置の状態情報を nFS 装置が受信した後，画面表示やデータ記録が誤ったことを FS 装置側で検出できない（構成 1，2）。
・nFS 装置から現場機器等へ不正な出力が行われる（構成 3）。
・現場機器等からの入力を nFS が誤認識し，不正な値（状態）を FS 装置に伝送する（構成 3）。

表 1　解析結果の例

No	事象	事象が発生した時の動作
①	重複	→②の 2 回送信※
	削除	→②の削除
	挿入	→②の挿入
	順序誤り	1 対 1 で手順に従うため発生しない前提
	破壊	→②の挿入 / 破壊 / 削除
	遅延	→②の遅延
②	重複	FS 装置で検出（通番・タイムスタンプ）
	2 回送信※	FS 装置で検出（意味的チェック）
	削除	FS 装置でタイムアウト検出，または指示電文受信なしにより実行せず（この例では安全側）
	挿入	→③の挿入
	順序誤り	1 対 1 で手順に従うため発生しない前提
	破壊	FS 装置で検出（安全符号）
	遅延	FS でタイムアウトを検出（この例では安全側）

※同じ内容を別の電文として 2 回送信。電文のフォーマットとしては正しいので，通番や安全符号等ではチェックできない。

2.3.2　FTA

図 2 ～図 4 の検討用プロトコルを対象として，構成 1 ～ 3 の FTA を行った。構成 1 のトップ事象は「不正な制御」，「不正なデータ書き換え」，「不正な状態表示」であり，それぞれ，図 2 の「モード切替等」，「データ転送」，「状態情報の表示」の伝送部分の異常に対応する。構成 2 のトップ事象は「不正な制御」と「不正なデータ書き換え」であり，プロトコルへの対応は構成 1 と同様である。構成 3 のトップ事象は，「不正な制御出力」と「不正な状態認識」であり，nFS 装置から現場装置への制御出力，現場装置からの状態入力に対応する。

2.3.1 項の解析結果以外の事象（対策すべき事象）は得られなかった。抽出された事象の内容は網羅的解析と同等であったが，FTA ではその原因が明確化され，必要な対策を整理することができた。例えば，構成 1 では「nFS 装置で制御状態の変更等を認識できない」という事象が発生する可能性があり，この対策として，FS 装置から nFS 装置への電文について，FS 装置側で ACK（受信確認）やそれに相当する電文を確認する必要があることを明確化できた（図 2 のプロトコルではこの確認の処理が漏れている）。

2.3.3　事象発生要因による解析

IEC62280 の付録 A.4.3 に含まれる表 A.1 に，ハザードの原因となる事象と規格内で扱っている脅威（事象）との対応関係が示されている。このハザードの原因となる事象が発生した場合の構成 1 ～ 3 の挙動について解析を行った。まず，この表 A.1 に示されるハザードの原因の中で，nFS 装置に起因する事象に対応するものを抽出した。抽出された原因は，ハードウェア及びソフトウェアのシステム的（偶発的でない）障害，ハードウェアの偶発故障・劣化，破壊等によるハードウェアのダメージ，ハードウェアの不正な置換，不正なソフトウェア改修，人的ミス，不正な電文送信である。この中で，システム的障害，ハードウェアの偶発故障・劣化，破壊等によるハードウェアのダメージは，nFS 装置の異常時の挙動を考えた場合に同等であるため，ハードウェア及びソフトウェア（HW/SW）の故障としてまとめた。また，不正な電文送信について，nFS 装置が不正に電文送信する事象は，他の原因の結果として発生するものであると考えて検討から除外し，FS 装置あるいは伝送システムの何らかの要因で，不正な電文が送信（挿入に相当）された場合について検討した。これらの原因が発生した場合に，

表 2　原因別の考えうる発生事象

No	ハザードの原因事象	考えうる事象		
		構成 1	構成 2	構成 3
1	HW/SW の故障	不正な入力認識，不正な判断によって条件成立を誤認。不正な電文送信，制御指示等		nFS 装置と現場装置間の誤制御・誤表示等
2	HW の不正な置換	制御・表示等のコード割付の不一致等による誤制御・誤表示，あるいは不正な電文送信		
3	SW の不正な改修			
4	人的ミス	不正な宛先指定・制御指示・データ指定		不正なデータ設定
		不正な認証		
5	不正な電文送信	nFS 装置から FS 装置側への電文の異常を FS 装置で検出可能		現場装置に対して誤制御

各構成に発生すると考えられる事象を表 2 にまとめる。

構成 1，構成 2 については制御のトリガーとなる電文を不正に送信する可能性が危惧される点で，2.3.1 項の解析と一致する。また，PC 等の nFS 装置でオペレータの扱うインタフェース装置を構成する場合，HW/SW の故障と人的ミスの境界が曖昧となる。人的ミスを防ぐための工夫だけでなく，nFS 装置がオペレータの入力，特に確認・認証等の入力を模擬できないようなコード体系や仕組みが重要といえる。また，コード割付やデータ誤り等に起因する誤制御等を防止する対策として，これらのコード間に一定の符号間距離（ハミング距離）を設けることにより，ある程度の効果が得られると思われる。

3．安全性の検討・評価

3.1　安全確保手法の整理

2.3 節の解析で得られた結果（発生しうる事象）と，それぞれに対して必要な対策の要件を以下に示す①～⑫の通り整理した。対策の要件には，2.3 節の各解析の中において必要とされた技術に対応する要件を記している。システムの開発にあたっては，図 2 ～図 4 の検討用プロトコルと同等のレベルでシステムの解析を行い，下記の項目について対策が十分であるかを確認する必要がある。そのうえで，より具体的なプロトコルや電文フォーマットの適否，システム固有の事象について，具体的に検討することが必要である。

①nFS 装置や伝送路で順序誤りが発生する（構成 1, 2, 3）
・FS 装置で順序誤りを排除できるプロトコルを採用し，FS 装置で検出
②FS 装置が異常を検出すると，処理が中断する（構成 1，2，3）
・FS 装置が異常を検出した場合に安全側に制御
・FS 装置が異常を検出した後に，（制御を継続可能な場合）適切に処理再開する手順
・nFS 装置から FS 装置への制御指示等がタイムアウトしても危険側とならないような仕組み
③nFS 装置が 1 つの処理を複数回の処理として複数回送信される（構成 1，2，3）
・挿入事象への対策だけでなく，1 回の指示入力が誤って 2 回以上として処理された場合（宛先 ID，通番，安全符号等は全て正常となる）にも，FS 装置側で意味的なチェックで検出できるようなプロトコルや電文フォーマット
④nFS 装置あるいはオペレータのミスにより，不正な制御指示の電文が送信される（構成 1，2）
・nFS 装置が不正に制御指示を発生させても，FS 装置からの要求により，オペレータ等の確認（認証）を行うことにより検出
⑤オペレータが不正な認証を行う（ここでは，悪意を持った不正認証は除く）（構成 1）
・オペレータの誤解による認証を排除できるようなインタフェース
→複数回の入力による注意喚起
→単純なボタン押下等では認証できない仕組み
⑥オペレータの入力なしに，nFS 装置が疑似的にオペレータの認証に相当する電文を送信する（構成 1）
・バグ等の排除
・認証に関する nFS 装置と FS 装置間の伝送を複数回実施
・nFS 装置が認識できない情報を入力（文字等の画像を表示し，オペレータが入力等）
⑦FS 装置から nFS 装置への電文が削除された場合に，nFS 装置が適切に事象を検出できない（構成 1，2，3）
・FS 装置から nFS 装置への電文が正しく受信されたことを確認するプロトコル
⑧FS 装置の状態情報を nFS 装置が受信した後，画面表示やデータ記録が誤ったことを FS 装置側で検出できない（構成 1，2）
・画面表示等の固着を検出できる仕組み（表示方法等）
・画面表示やデータ記録の誤りが直接的に危険側とならない用途への適用
⑨nFS 装置から現場機器等へ不正な出力が行われる（構成 3）
・nFS 装置から現場機器への不正な制御出力した場合，現場機器の状態情報・制御結果を FS 装置に伝送することにより，FS 装置で誤制御を検出。検出後に安全側処理をしても時間的に問題がない用途への適用が必要。入力部の故障が潜在化するモードがある場合は，多重故障に至り，検出ができなくなる可能性があるので不可。
・現場機器への誤制御が直接危険側にならない用途への適用。
⑩現場機器等からの入力を nFS が誤認識し，不正な値（状態）を FS 装置に伝送する（構成 3）
・入力部の故障が検出できる仕組み（十分に短い間隔で入力情報が変化し，変化の妥当性等を確認できる仕組みなど）。
・現場機器からの状態情報の誤認識が直接危険側にならない用途への適用。
⑪宛先，制御指示内容，データ等の入力ミスによる異常が想定される（構成 1，2，3）
・オンラインの入力ミスを抑制するインタフェースやプロトコル
・オフラインでの入力作業でのミスを抑制，あるいは，チェックする支援機能

・オフラインでの入力結果をチェックする体制
⑫制御コマンド類のビット誤り等により異なる制御指示となる（構成 1，2，3）
・安全符号による検定
・宛先 ID，通番，安全符号等が正常であっても異常を意味的なチェックで検出可能なプロトコルや電文フォーマット
・符号間離隔を持ったコマンドやデータ体系（電文としての符号間離隔ではなく，電文内の個々のデータ等に符号間離隔を持たせる）

3.2 ネットワークシミュレータによる検証

鉄道総研で開発している無線式列車制御用ネットワークシミュレータ[4]を用いて 2.3.1 項の解析結果，3.1 節で示した対策の検証を行った。ネットワークシミュレータ上に構成 1 ～ 3 の装置をモデル化し，図 2 ～図 4 の検討用プロトコルに従った通信を実施するようにプログラムした。各装置内部には，6 つの脅威を発生させるモジュールと IEC 62280 に示されるような各種対策（通番，タイムスタンプ，タイムアウト，安全符号）を施すモジュールを組み合わせて動作できるようにし，装置間の伝送の任意のステップで脅威を発生させた場合の影響と対策の効果について確認できるようにしたものである。なお，各種対策には，その他に送受信 ID，フィードバックメッセージ，認証手続きや暗号化が IEC 62280 で述べられているが，本ネットワークシミュレータでは 1 対 1 で伝送する検討用プロトコルの性質，およびセキュリティについては扱わない関係上実装を省略した。

検討用プロトコルで各種脅威を発生させてシミュレーションした結果，FS 装置に入力される手前で脅威が発生した情報は，FS 装置自身に施した対策によって検出されることで安全側に制御できることを確認した。

なお，本検討に用いたプロトコルでは，1 対 1 で伝送を行うモデルとなっているため順序誤りについては発生しない前提となっているが，各脅威に対して有効な対策が IEC 62280 に沿っていることを確認できた。この中で，挿入に関してはオペレータや nFS 装置，現場装置でどのような情報が挿入されるかによって対策をすり抜けていくことを確認しており，有効な対策としてアプリケーションによる意味的なチェックを追加している。これは，検討用プロトコルにおいて通番やタイムスタンプなどの対策に加えて，アプリケーションのレベルで対策を施すことが必要であることを示しているものである。具体的には，入力された値の範囲をチェックすることや，以前の入力値との差分を確認することなど，情報の内容の妥当性をチェックすることが必要となる。ただし，本ネットワークシミュレータでは送受信 ID，フィードバックメッセージ，認証手続，暗号化などの対策を実装して検証していないため，これらの対策を施すことで，対応できる場合もある。

4．まとめ

これまで，新しいシステムの開発の都度，混在環境における安全関連伝送に必要な安全性技術の検討や検証・評価が行われてきた。この方法では開発の効率が悪く，さらに対策の漏れが発生することが危惧される。そこで，本研究では発生しうる事象を抽出したうえで類型化・一般化し，整理した 12 種類の事象毎に対策の要件を提示した。これらを新しいシステムの設計時や評価時に参照し，適否をチェックすることにより，対策の漏れを防ぐとともに，設計・評価作業を効率的に実施できると考える。本研究の成果を活用することにより，nFS 装置として汎用機器やより低コストな機器を導入しやすくなることが期待される。

なお，本研究では専用の有線伝送路で構成したクローズなネットワークにおける安全性を対象とし，セキュリティは対象外としている。今後，無線を用いる場合や，不正なアクセスを排除できない場合セキュリティを含めた検討を進めるとともに，伝送以外の観点からも汎用機器等を活用する場合の要件等について検討する必要がある。

謝　辞

本研究の実施にあたり，有用な助言を頂いた東日本旅客鉄道株式会社先端鉄道システム開発センター，西日本旅客鉄道株式会社技術開発部の関係各位に深く感謝いたします。

文　献

1）“Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems”，IEC 62280，2014.
2）“Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems”，IEC 61508 part 2，2010.
3）福田光芳，岩田浩司，菅原宏之，北野隆康，川﨑邦弘：非安全関連装置混在環境における安全関連伝送 , 第 22 回 鉄道技術連合シンポジウム（J-RAIL2015）予稿集，2015
4）菅原宏之，北野隆康，川﨑邦弘:無線式列車制御用通信ネットワークの性能評価システム，鉄道総研報告，Vol.28，No.11，pp.31-36，2014