鉄道の安全な運行を支える車上保安装置向け高性能プラットフォームの開発

近年，鉄道は持続可能な社会を担う移動手段として注目を浴びており，今後，世界中で鉄道システムの普及・活用が進展すると見込まれている。
こうした中，日立製作所は車上保安装置に要求される高い安全性および演算性能を実現するため，独自の安全性方式に基づいた鉄道用の車上保安装置向けプラットフォームを開発し，国内外における鉄道信号システムへの適用を進めてきた。近年では車上保安装置にさらなる高性能化・小型化が求められており，新たに車上保安装置向け高性能プラットフォームを開発した。本稿では，この新高性能プラットフォーム開発の概要について述べる。

宮路 将行 | Miyaji Masayuki
大西 康介 | Onishi Kosuke
森田 和貴 | Morita Kazuki

1. はじめに

日立製作所では独自の安全性方式に基づいた鉄道用の車上保安装置を開発し，国内外の市場における鉄道向け信号システムへの適用を進めてきた。車上保安装置に要求される高い安全性および演算性能を実現するため，日立は独自のフェールセーフCPU（FS-CPU：Fail-safe Central Processing Unit）※1)と，FS-CPUを中核としたプラットフォームを開発した。FS-CPU上に専用のOS（Operating System）を実装し，ここにATC（Automatic Train Control：自動列車制御装置）やETCS（European Train Control System：欧州における鉄道制御システム）などの信号システムに要求される動作に応じた機能を持ったアプリケーションを適用することで，プラットフォームは車上保安装置として動作する。

既存のFS-CPUの開発から10年以上が経過し，近年の信号システムで要求される無線通信方式や，列車高密度化への対応などの新たな機能の実現のため，プラットフォームにはさらなる処理性能の向上が求められている。また，既存のプラットフォームでは処理性能の制約から複数のFS-CPUを使用してシステムを構築する場合もあり，車上保安装置全体としてハードウェアが大型化し，車両艤装スペースを圧迫するという問題が挙げられている。

このため，日立は車上保安装置の高性能化，および複数装置の統合によるシステム小型化を目標とし，新たに車上保安装置向け高性能プラットフォームを開発した。本プラットフォームでは，新規開発したFS-CPUを採用することで性能向上を実現するとともに，FS-CPU上で動作するOSを開発し，単一CPU上で安全性を保証しつ

※1）二つのCPUが同一の処理を実行し，CPUの演算結果を比較器が比較・照合することで高い安全性を保証するLSI（Large-scale Integration）。

つ複数のアプリケーションの並列実行を可能とした。さらに，本プラットフォームを対象として欧州安全性規格に基づいたISA（Independent Safety Assessor：安全に関する独立査定機関）による査定を実施し，SIL4（Safety Integrity Level 4：安全度水準4）準拠の安全性認証をプラットフォームとして取得した。本稿では，新高性能プラットフォーム開発の概要について述べる。

2. 開発コンセプト

前章で述べたように，本開発では車上保安装置の高性能化，および複数装置の統合によるシステム小型化を目的とし，以下に示す実現手段によりプラットフォーム開発を実施した（**図1**参照）。

各手段の詳細は以降の節にて説明する。

(1) 新FS-CPU開発による処理性能向上

既存FS-CPUと同じ高安全性を持ち，処理性能を向上させる新FS-CPUを開発する。

(2) 複数のアプリケーションを並列実行可能なOSの開発

FS-CPUの高性能化と併せ，既存の構成において複数装置に分散された機能を単一のCPU上で並列実行可能となるよう，OSを新規開発する。

(3) 回路構成の見直しによる装置小型化

以上のFS-CPUおよびソフトウェアを実装して車上保安装置として稼働するプラットフォームを構成し，回路構成の見直しにより装置を小型化する。

2.1 新FS-CPU開発による処理性能向上

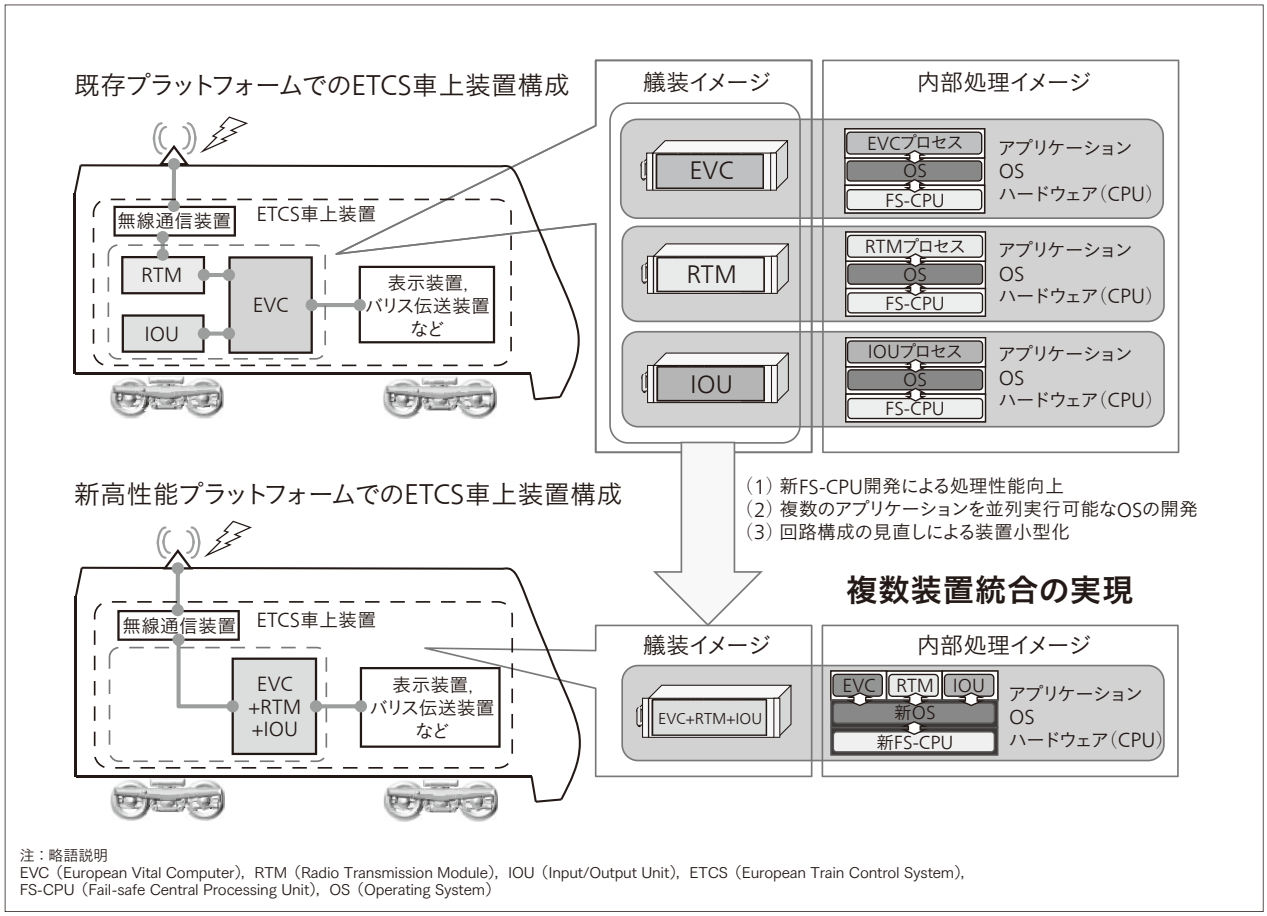
日立はプラットフォーム開発に先駆け，既存FS-CPUと同じ高安全性を有し，かつ処理性能を向上したFS-CPUを新たに開発し，採用した。

FS-CPUは二つのCPUと比較器を内蔵しており，二つのCPUが実行する演算を比較器が比較・照合し，CPUの誤動作を検出することで高い安全性を保つLSIである。

新FS-CPUは従来品と同じく二つのCPUと，二つのCPUの入出力データを比較・照合する比較器をワンチップに内蔵する構成を採用している。一方，CPUとシステムバスの動作周波数をアップすることにより，従来品と

図1｜新高性能プラットフォームの開発コンセプト

新高性能プラットフォームでは，既存プラットフォームにおいて分散して配置していた個々の機能を統合することによるシステム小型化を目的として開発を実施した。



注：略語説明
EVC（European Vital Computer），RTM（Radio Transmission Module），IOU（Input/Output Unit），ETCS（European Train Control System），FS-CPU（Fail-safe Central Processing Unit），OS（Operating System）

比較して4倍の処理性能を実現した。また，外部装置とのインタフェースとして，既存FS-CPUでは実装していなかったイーサネット※2) 通信機能を実装したほか，4チャネル分のイーサネットポートと通信バッファを内蔵し，プラットフォームへの追加LAN（Local Area Network）ボードの実装を不要としている。比較器はバスサイクルごとに診断処理を実施することで比較器自身の故障検知も可能としており，さらにチップ内レイアウト・実装設計に厳格な配置・配線ルールを適用することで，共通要因故障の潜在リスクを最小化した。さらに，大容量RAM（Random Access Memory）とキャッシュメモリにはECC（Error-correcting Code）を付加しており，車上保安装置の高安全性・高信頼性の実現に大きく寄与している。

2.2 複数装置の統合実現のための新OS開発

既存の車上保安装置のソフトウェアは，ATCやETCSなど適用する信号システムの動作に応じた機能を持ったアプリケーションと，アプリケーションからの要求に基づきハードウェアを制御するOSで構成される。本開発では既存構成において複数装置に分散されていた機能を単一のFS-CPU上で並列実行可能となるよう，OSを新規開発した。新OSでは，OSが車上保安装置のアプリケーションを管理，監視，制御する方式として，下記の三つの課題を解決することで，安全性を損なわずに複数のアプリケーションを並列実行可能とした。

(1) アプリケーション間での実行時間の侵害防止

アプリケーションは一定時間ごとに周期的に実行される。複数のアプリケーションを実行するうえで，単一のアプリケーションが規定時間内に実行完了しなかった場合，CPUが占有され後続のアプリケーションが実行できない。新OSは周期的にアプリケーションを監視・異常検知して，異常が検知されたアプリケーションのみを停止し，以降の動作の実行対象から除外することで，後続のアプリケーションの実行時間を保証し，縮退動作を行わせることができる（**図2**参照）。

(2) アプリケーション単位での機能停止

複数装置の統合において，特定のアプリケーションの異常を検知した場合，当該のアプリケーションのみを動作から切り離すようOSが制御することが要求される。新OSは各アプリケーションに独立したメモリ空間を提供することで，アプリケーション単位での機能停止を可能にし，他の正常なアプリケーションの継続動作を保証し

※2) イーサネットは，富士ゼロックス株式会社の登録商標である。

図2｜新FS-CPU上でのソフトウェア動作イメージ

新FS-CPU上で周期的に動作する新OSと複数のアプリケーションの動作状態のイメージを時系列で示す。新OSは周期的にアプリケーションを個別に監視し，異常が検知されたアプリケーションのみを停止する。図はアプリケーションAが規定時間内に未完了という異常を新OSが検知した際の動作を示しており，この場合，新OSはアプリケーションAのみを停止し，正常なアプリケーションBは継続して動作させる。

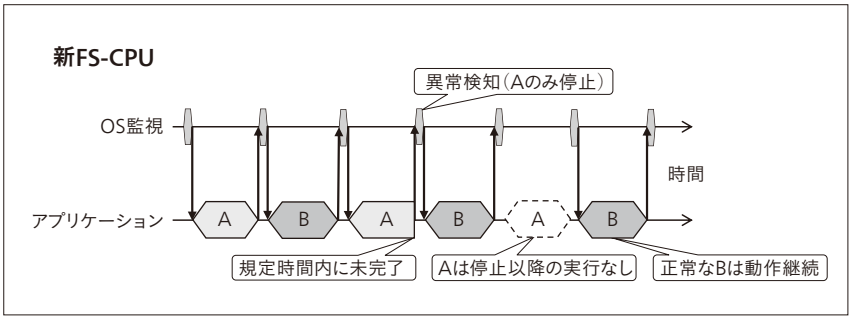
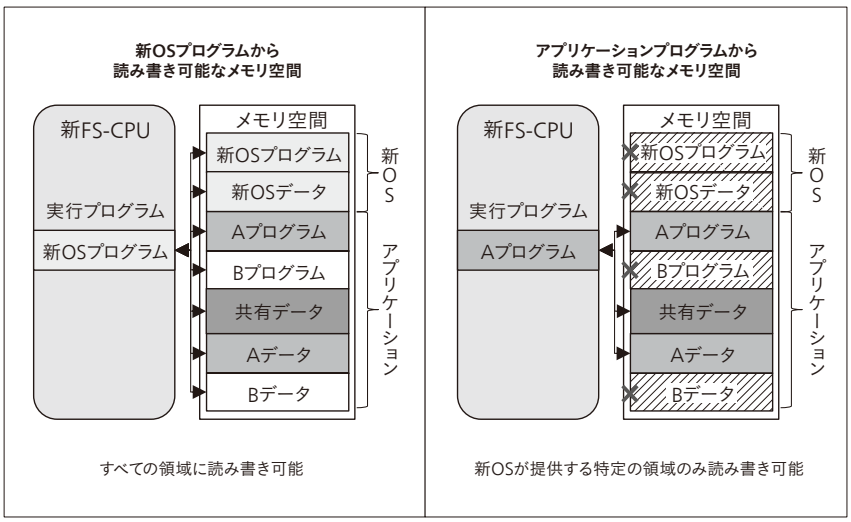


図3｜新OSとアプリケーションから読み書き可能なメモリ空間の領域

新OSは自身と複数のアプリケーションを管理，監視，制御するため，メモリ空間のすべての領域を読み書き可能である。一方で，アプリケーションは新OSが提供する特定の領域のみ読み書き可能であり，新OSや他のアプリケーションのプログラムのデータを誤って書き換えることがない構成となっている。



ている（同図参照）。

(3) アプリケーション間でのプログラムやデータの誤った書き換え防止

既存OSのメモリ空間の管理方式を用いた場合，メモリ空間が複数のアプリケーションにより共有されるため，アプリケーション間で互いのプログラムやデータを誤って書き換えてしまうというリスクがある。新OSが各アプリケーションに独立したメモリ空間を提供することで，アプリケーションは新OSが提供する特定の領域のみを読み書き可能となり，アプリケーション間でプログラムやデータが誤って書き換えられることを防止している（**図3**参照）。

2.3 プラットフォーム適用と装置小型化

新プラットフォームは，FS-CPUとOSを組み込んだ基板を中心に，鉄道車両のブレーキ回路など外部機器との入出力や通信を行うインタフェース基板により構成される。

FS-CPUはプラットフォームの中核となるCPU基板に組み込まれ，安全に関する演算を実行し，ブレーキ指令など安全性が求められる出力には二重化された専用バスを用いた出力回路を適用している。また，プラットフォーム外の装置とのインタフェース回路を基板単位で実装し，これらの基板を汎用バスで接続することで，個別システムに要求されるインタフェースに応じた基板を任意に設定・実装することが可能となっている（**図4**参照）。

これにより，汎用性と拡張性を高めると同時に，必要最小限の基板を実装することでシステムの小型化に寄与している。また，実案件適用において追加のインタフェース基板が必要な場合には，共通のバスインタフェース基板と，対象に応じたドライバを追設することで，中核となるCPU基板およびOSを変更することなく適用が可能である。

また，実装素子の小型化と，既存装置からの回路構成を見直すことにより，装置単位での小型化を実現した。前述の高性能化による装置統合と合わせ，ETCS車上装置向けEVC（European Vital Computer）装置[※3]に適用した場合，従来から50%の装置サイズの低減を可能とした。

2.4 開発プロセスと安全性認証

本開発では欧州規格EN50126[※4]，EN50128[※5]，EN50129[※6]に基づいた開発プロセスに従って設計，評価を実施し，独立安全認証機関であるISAによる査定を受け，SIL4準拠の安全性認証をプラットフォームとして取得した。

認証の段階と本開発における認証取得のスコープを**図5**に示す。既存のプラットフォームにおける認証スキームでは，製品適用が前提であり，プラットフォームとアプリケーションを包括したGA（Generic Application）[※7]，もしくはSA（Specific Application）[※8]が認証のターゲットであった。このスキームでは，プラットフォームの認

※3）速度照査，ブレーキ制御など保安装置の機能を担うETCS車上装置の制御部。
※4）RAMS（Reliability，Availability，Maintainability，Safety）プロセスについて規定した欧州規格。
※5）車上保安装置のソフトウェアについて規定した欧州規格。
※6）信号システムの安全性について規定した欧州規格。
※7）アプリケーション依存の動作など特定のアプリケーションに応じる機能を有したシステム。
※8）艤装条件なども含んだ個別アプリケーション適用のためのシステム。
※9）異なるアプリケーションに共通に適用可能なシステム。

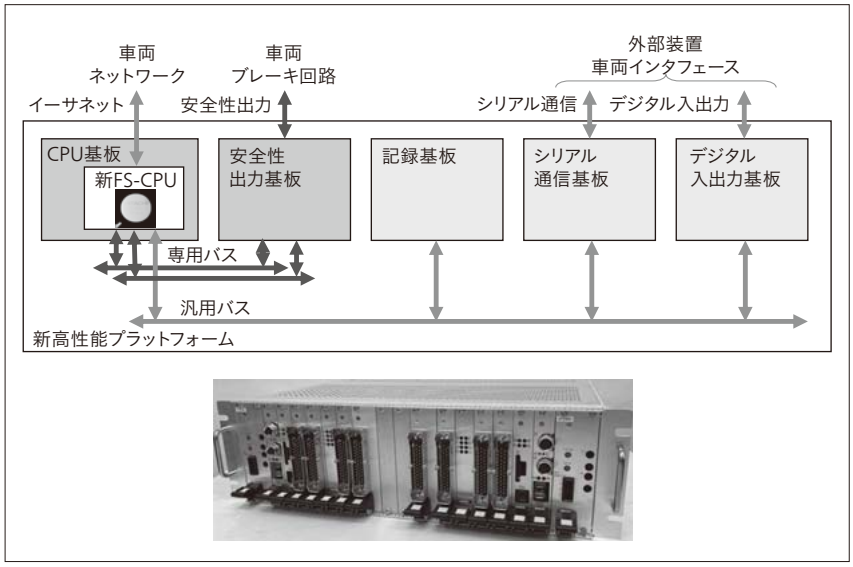
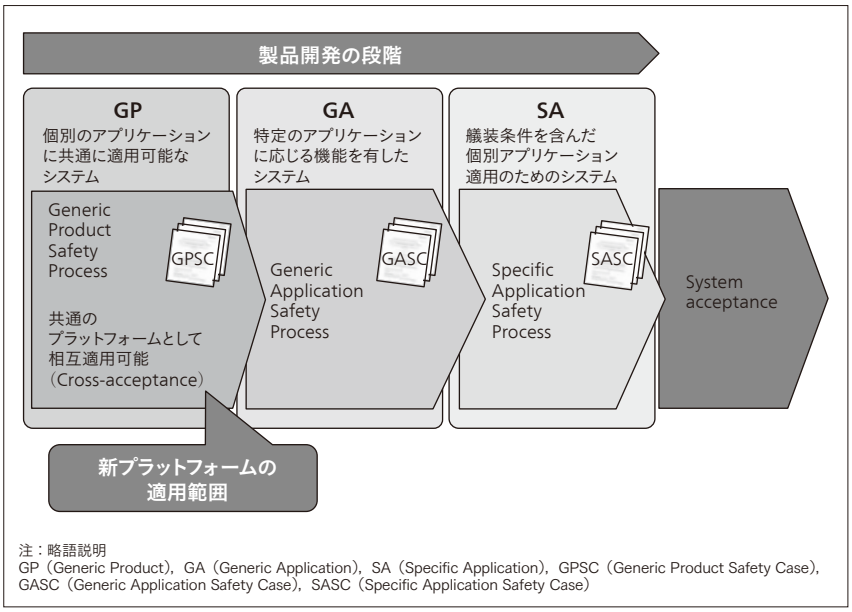


図4｜新高性能プラットフォームの外観と装置構成

新高性能プラットフォームは，新FS-CPUを搭載したCPU基板を中心に，各種インタフェース基板を機能に応じたバスにより接続することで構成される。写真はETCS車上装置向けEVC装置構成の外観を示している。

図5｜認証の段階と新プラットフォームの適用範囲

安全性認証では，システムの開発・適用段階に応じてGP，GA，SAの3段階に分けられる。新プラットフォームは以降の製品適用（GA，SA）の際，共通に適用可能なGPとしての安全性認証を取得した。



注：略語説明
GP（Generic Product），GA（Generic Application），SA（Specific Application），GPSC（Generic Product Safety Case），GASC（Generic Application Safety Case），SASC（Specific Application Safety Case）

証結果がGP（Generic Product）[※9] として共通適用ができないという問題があった。

このため，本開発ではプラットフォームをGPとし，これを安全認証取得範囲としてスキームの整理を実施した(同図参照)。本スキームでは,実案件からプラットフォームへの安全性・信頼性の要件抽出を行い，これを満足させる設計を行った。実案件適用時の安全に関する制約事項はSRAC（Safety Related Application Condition）として管理され，以降のGA，SAにおける認証活動ではSRACの条件をすべて満たすことで，本開発の安全性認証を共通に適用することが可能となる。なお，本活動の結果は，GPSC（Generic Product Safety Case）としてまとめられ，ISAによる査定が実施された。

評価においてはシステム要件に応じた機能試験に加え，EVC装置に応じたサブラックに実装したうえで温湿度，振動衝撃，EMC（Electromagnetic Compatibility）指令など欧州規格に対応した環境試験を実施し，新プラットフォームが実車両運用で要求される信頼性を備えていることを実証した。

3. おわりに

本開発では，車上保安装置向けプラットフォームの性能向上と複数装置の統合を目標とし，FS-CPUおよびOSの新規開発，車上保安装置として動作する高性能プラットフォームを開発した。また，プラットフォームとしてSIL4準拠の安全性認証を取得し，安全性に関する評価を完遂した。さらに，開発したプラットフォームを対象として，国内向け車上保安装置相当のアプリケーションを実装し，要求される機能および処理性能を満たすことを検証した。

今後は，本プラットフォームに車上保安装置に対応したアプリケーションを適用し，国内外の市場での鉄道向け信号システムへの製品展開を進める。

執筆者紹介

宮路 将行
日立製作所 鉄道ビジネスユニット
Operations Signalling & Turnkey, JPN Products development 所属
現在，車上保安装置プラットフォームの開発業務に従事

大西 康介
日立製作所 鉄道ビジネスユニット
Operations Signalling & Turnkey, JPN Products development 所属
現在，車上保安装置プラットフォームの開発業務に従事

森田 和貴
日立製作所 鉄道ビジネスユニット
Operations Signalling & Turnkey, JPN Products development 所属
現在，車上保安装置プラットフォームの開発業務に従事

日立評論

日立評論は、イノベーションを通じて社会課題に応える
日立グループの取り組みを紹介する技術情報メディアです。

日立評論Webサイトでは、日立の技術者・研究者自身の執筆による論文や、
対談やインタビューなどの企画記事、バックナンバーを掲載しています。ぜひご覧ください。

日立評論(日本語) Webサイト

https://www.hitachihyoron.com/jp/

Hitachi Review(英語) Webサイト

https://www.hitachihyoron.com/rev/

日立評論メールマガジン

Webサイトにてメールマガジンに登録いただきますと、
記事の公開をはじめ日立評論に関する最新情報をお届けします。