# 安全性を実現するアーキテクチャ

**自動車システムにおいて、スタンドアロンの安全アプリケーションを統合して、いわゆる統合安全システム (ISS) を構築する傾向が顕著になっています。これらのシステムは、乗員の安全レベルを高めるために、現在の機能を統合、拡張する安全サービスを提供します。ISS は、欧州研究プロジェクト EASIS (Electronic Architecture and System Engineering for Integrated Safety Systems) で分析と検証が行われた、先進的な電気および電子アーキテクチャを必要とします。**

- 将来の自動車安全システムのための欧州研究プロジェクト
- EASIS 検証ツールによるメインアーキテクチャ特性のプロトタイピングと妥当性の確認
- dSPACE のソフトウエアとハードウエアを使用するFlexRayアプリケーション

2001 年、欧州委員会は交通事故死亡者数を 2010 年までに 50% 削減するという意欲的な目標を自らに課しました。この目標を達成するためにとられた方策のひとつが、2004 年から 2006 年末まで運営された EASIS 研究プロジェクトでした。EASIS は、将来の安全システムを実装するための技術開発を目指して、欧州の自動車メーカー、サプライヤ、ツールメーカー、研究機関など 22 の会社と団体により共同で運営されました。

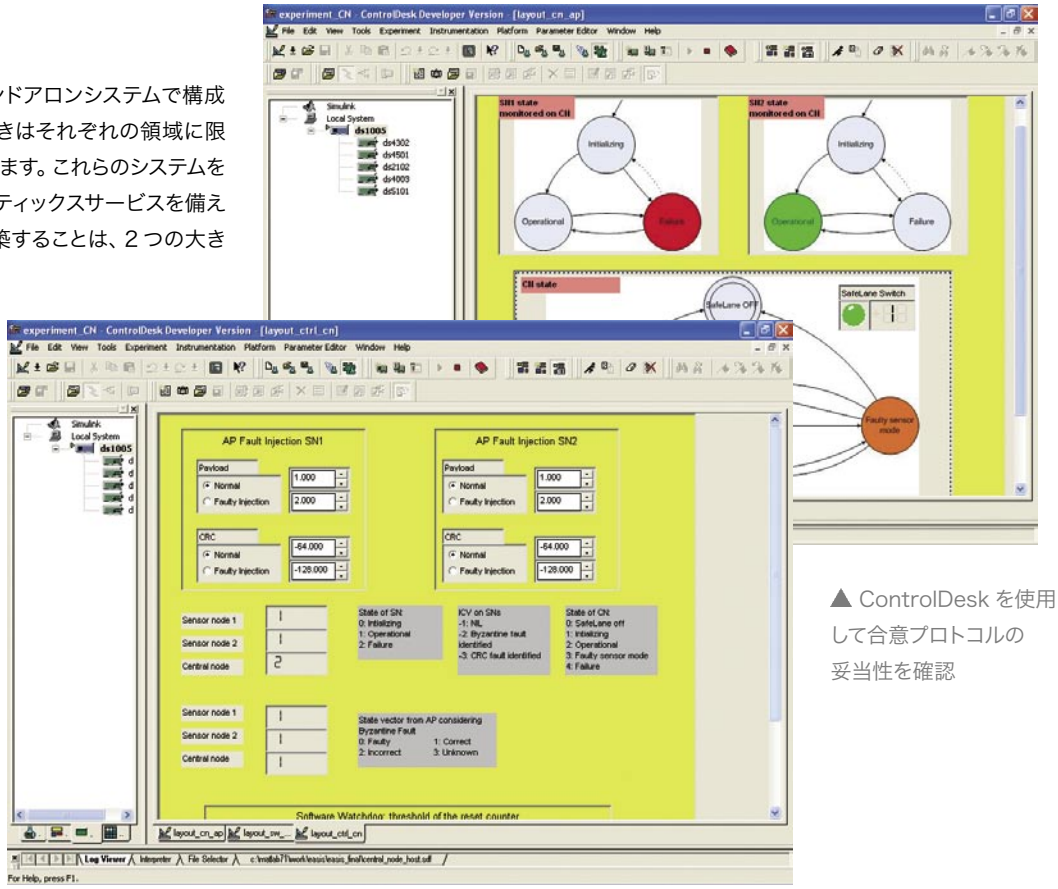
## 統合安全システム (ISS)

現在の安全システムは主にスタンドアロンシステムで構成されているため、各システムの働きはそれぞれの領域に限られ、相互依存性も限定されています。これらのシステムを組み合わせて、強化されたテレマティックスサービスを備える統合安全システム (ISS) を構築することは、2 つの大きな効果をもたらします。

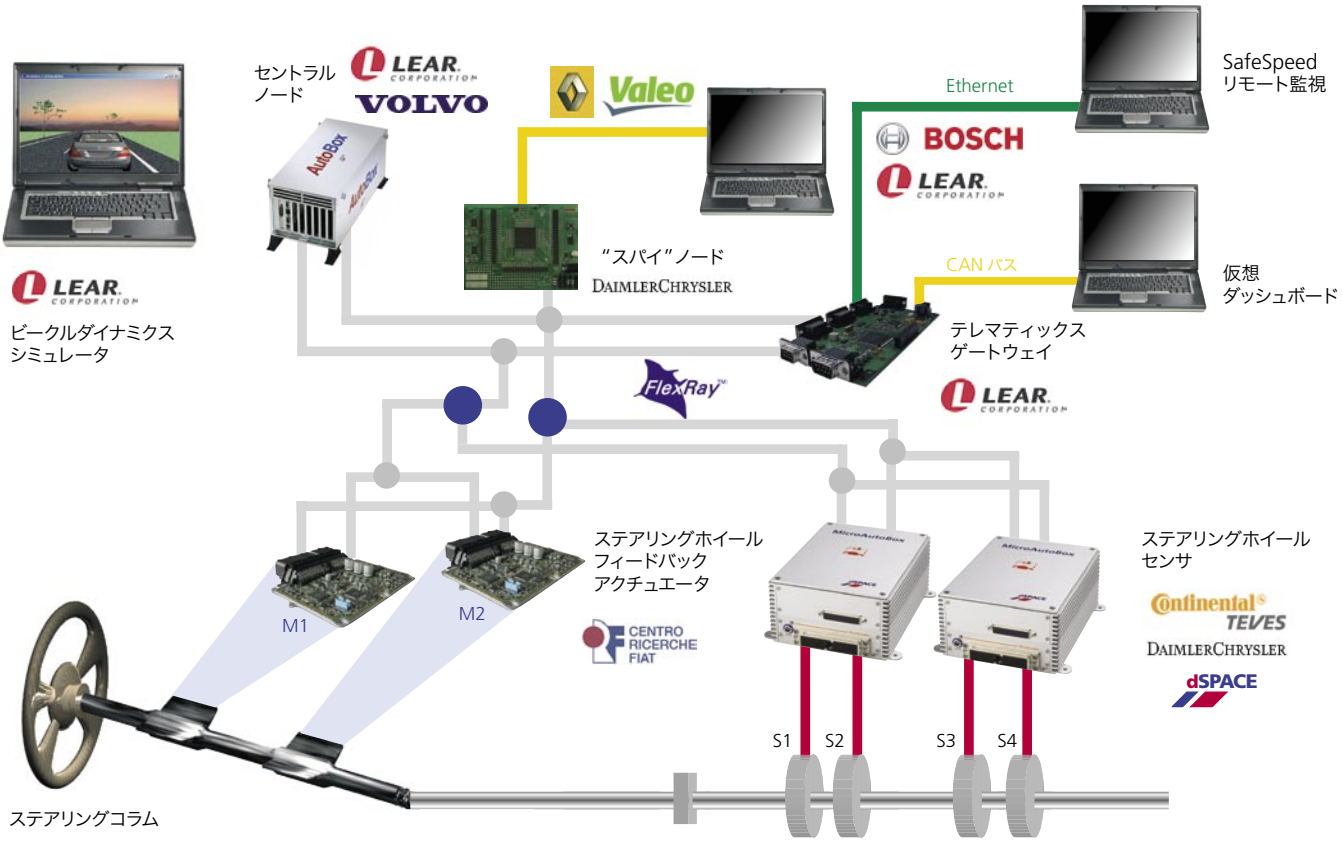
- すべての領域から提供される情報を組み合わせて、車両とその周囲の状況をより明確に把握することができ、そのおかげで安全システムが判断を下すためのより良い基礎データが提供されます。
- 異なる領域を横断して制御動作を協調させることが可能になるので、車両をより統合的に制御できるようになります。

## プラットフォームに関する要件

ISS は信頼性を保証するという観点から、基礎となるソフトウエアとハードウエアのプラットフォームに関してより高度な要件を求め、現在のシステムよりも厳格な開発プロセスを要求します。ハードウエアプラットフォームの要件を満たすため、私達 EASIS プロジェクトチームは、車載電子制御ハードウエアのインフラストラクチャを開発しました。ソフト




▲ ControlDesk を使用して合意プロトコルの妥当性を確認




▲ EASIS 検証ツールのハードウエアアーキテクチャ

ウエアプラットフォームについては、将来の ISS アプリケーション構築にも対応できるように、一連の信頼できるサービスを備えたソフトウエアアーキテクチャを選定して記述しました。将来への対応の面でも、特定の安全性に関するプロジェクトの成果は、AUTOSAR パートナーシップの活動と整合性を保っています。

## EASIS 検証ツール

私達は、ハードウエアおよびソフトウエアプラットフォームで定義された基本原理が有効かつ実行可能であることを示すため、これらの原理を EASIS 検証ツールに組み込みました。検証ツールは、テレマティックスゲートウェイ、車載センサとアクチュエータ、複数の ECU などを含む車載電子制御システムをシミュレートできます。そのシステムとは、ボルボが欧州プロジェクト PReVENT の一環として開発した車線維持補助システム（SAFELANE）に、速度制限オプション（SAFESPEED）を組み合わせた操舵システムです。ステアリングホイールセンサノードがセンサアプリケーションと合意プロトコルを実行し、フォールトトレラントの手法によりステアリングホイール角の値を生成します。セントラルノードも同様に SAFELANE アプリケーションと合意プロトコルを実行します。さらに、故障監視とテレマティックスゲートウェイのためのスパイノードが存在します。これら合計 7 個のノードは、デュアルチャンネル FlexRay 通信システムによって結合されます。

## 冗長性

システムトポロジは、車上のさまざまな領域内におけるフェールサイレント（FS）電子制御ユニット（ECU）のグループをシミュレートします。この中には、FlexRay 通信システムが領域を横断して情報交換を行うための共通バックボーンが設けられます。安全性向上のため、1 個のノードが故障しても 2 個目のノードがアプリケーションの求める操作を完全に実行できるという原理に従い、センサノードとアクチュエータノードのペアが作成されて、フェールオペレーショナル（FO）ユニットを構成します。アクチュエータノードは、EASIS プロジェクトから生み出されたハードウエア開発指針に準拠する、2 個のフェールサイレントユニット（FSU）から構成される FO ノードです。それぞれの FSU は独立したアクチュエータを駆動させ、FSU のひとつが故障してもシステムの完全な機能を保証します。私達は何種類もの欠陥を故意に発生させて、システムの正しい作動を確認するという手法により、検証ツール上でこのシナリオをテストしました。私達は dSPACE の量産コード生成ツールである TargetLink を使用して、それぞれの FSU 上でアプリケーションソフトウエアの生成と調整を行いました。

**「すべてが順調です。dSPACE のツールのファンになってきました」**

**Antoni Ferre**

### 信頼性

ソフトウエアプラットフォームにおける信頼性を確立するため、私達はそのプラットフォームが提供すべき一連のソフトウエアサービスを選定しました。これらのサービスは故障に対する許容性（fault tolerance）を備え、システムの状態と整合性に関する情報を管理し、データの完全性を確保することを目的としています。

- 合意プロトコル：プラットフォームが提供すべきサービスでは、フェールオペレーショナルな動作を保証するために、コンポーネントを分散させ、さらに一部を重複して配置し、すべてのコンポーネントで同じ入力データを使用して判断と制御が行われます。
- ソフトウエアウォッチドッグ：従来のタイムアウト割り込み機能に加え、たとえばハートビート監視、制御フローチェック、作業状態表示などによりアプリケーションの実行を監視します。
- 故障管理フレームワーク：FSU および FSU 上の個々のアプリケーションの故障の状態について、一貫性のある総合的な視点を提供します。この情報を利用することにより、分断箇所と損傷箇所の調査を行い、適切な復旧処置についての決定を下すことができます。
- テレマティックスゲートウェイ：車載の領域間通信（ルーティング）および外部との通信（データ交換、リモートアクセス）に関する EASIS サービスの窓口となります。

### 検証ツールの開発

EASIS 検証ツールの開発には、Lear Corporation 社（スペイン）、ダイムラー・クライスラー社（ドイツ）、Centro Ricerche Fiat 社（イタリア）、Valeo 社（フランス）などの複数のプロジェクトパートナーが参加しています。各パートナーは地理的に分散しており、各社のハードウエアとソフトウエアの開発スケジュールは異なっているにもかかわらず、私達は Lear Corporation 社での最終的な統合作業がスムーズに行われるようなシステムトポロジを選択しました。検証ツールの開発支援のため、dSPACE の 2 個の MicroAutoBox と 1 個のモジュール型 DS1005 システム、およびこれらに付属する FlexRay インターフェースが使用されました。これらのシステム上で実行されるソフトウエアサービス、および SAFELANE アプリケーションは、MATLAB®/Simulink®/Stateflow® モデルとして提供されました。さらにこのプロジェクトの決められた全体スケジュールに沿って、FlexRay 通信バスに接続される dSPACE の RTI FlexRay Blockset がこれらのモデルに加えられました。個々のサービスを検証するために、最初は各パートナーの社内で、さらに再び Lear Corporation 社における統合作業で、dSPACE の実験ツールとテストオートメーションツールが使われました。dSPACE の成熟した開発ソリューションを使用することで負荷が分散され、検証ツールのセットアップのリスクが最小限に抑えられました。すべての作業は予定どおりに完了し、イギリスのロンドンにおける第 13 回 World Congress and Exhibition on Intelligent Transport Systems and Services など、2006 年の秋に開催されたさまざまなイベントでその成果が発表されました。

Antoni Ferre、Lear Corporation 社、スペイン
Vera Lauer、Xi Chen、DaimlerChrysler 社、ドイツ
Fulvio Cascio、Centro Ricerche Fiat 社、イタリア
Luc Fougerousse、Valeo 社、フランス
Joachim Stroop、dSPACE、ドイツ

## 用語解説

**統合安全システム（ISS）–**
交通安全の目標を満たすべく設計され、テレマティックスおよびボディとシャシーエレクトロニクスも統合した車両機能の構成要素で、リスクを許容レベル内に抑えます。

**EASIS –**
自動車メーカー、サプライヤ、ツールメーカー、研究機関で構成される共同体（www.easis.org）

**SAFELANE –**
車両の進路が片側に大きくずれた場合、ドライバーに警告することで安全性を高める車線維持補助システム

**SAFESPEED –**
車速を外部から定義された最高速度に自動的に制限するシステム

**PReVENT –**
予防的安全のためのアプリケーションと技術を開発して実証することにより、交通安全へ寄与することを目的として、欧州委員会により共同設立された欧州自動車業界の活動（www.prevent-ip.org）