2023/4

Apposite Tech,

株式会社 理経 ビジネスイノベーション部プロダクトセールスグループ

車載イーサネットの性能をより確かなものにするための方法とは

今日の車は、動力を駆動して移動するだけの機械にとどまらず、車載インフォテインメントシステム（※1）、故障診断システム、先進運転支援システム、その他の安全システム等の機能を有し、膨大な量のデータを同時に扱う必要があります。

このデータ負荷に対応するために、新しい車両にはこれまでにない高速で信頼性の高いネットワークが必要とされており、車載イーサネットの進歩が求められています。

※1 車載インフォテインメントシステム：インフォメーションとエンターテインメントの両方を提供するシステムのこと。

車載イーサネットとは？

車載イーサネットは、車内のさまざまな機器やシステムを接続する有線ネットワークです。しかし、従来のイーサネットでは、新しい自動車技術に追いつくことができませんでした。
最新車両では BroadR-Reach（ブローダーリーチ）（※２）が車載イーサネットとして標準化されました。

これまでの LAN ケーブルを用いた接続だとノイズを拾いやすく誤動作の原因となる為、これを解決するために生まれた伝送方式です。

また、車載イーサネットのケーブルは、送受信専用線を使用する従来のイーサネットケーブルと異なり、１対で双方向の通信を可能としたツイストペアケーブルを採用しています。これにより、帯域幅と遅延のパフォーマンスが向上するだけでなく、必要なケーブルの量が減り、コストと車体重量が大幅に軽減されます。

※2 BroadR-Reach（ブローダーリーチ）：Broadcom 社が開発した車載イーサネット用データ伝送技術。

車載イーサネットはどのように使用されるのか？

多くの車には、サラウンドビューパーキングアシスタンス、衝突回避システム、車線逸脱警報など、カメラとセンサーを利用した安全機能が装備されています。
カメラとセンサーは、安全性を保証するために信頼性の高い通信が必要であり BroadR-Reach の採用により安定した通信に必要な要件を満たすことが可能となります。

車には、日々進化しているインフォテインメントシステムも装備されています。スマートフォンや、Bluetooth 機器、インタラクティブなビデオ画面まで、車にはこれまでになく多くのアプリケーションが接続されます。車載イーサネットは柔軟に設計されているため、新しいテクノロジーが発生した場合でも、ネットワークを簡単に再構成して接続を可能にします。

車の完全な自立走行の実現が近づくにつれ、車はインターネット、他の車両、さらには周辺のインフラにも同時に接続することが期待されます。このコンセプトは、Vehicle-to-Everything（V2X）と呼ばれ、すべて同じネットワークを使用して実行する必要があります。ネットワークが帯域幅と遅延の要件を満たし、娯楽よりもセーフティクリティカル（※3）な情報を優先するなど、優先順位をつけて転送するインテリジェンスを備えていることが不可欠です。

※3 セーフティクリティカル：人命や治安に関わるような高い重要度のこと

車載イーサネットのテスト要件

路上の走行において、頻繁に通信を行っている今日の車を安全に運用するには、ネットワーク自体のテスト、各デバイスのパフォーマンスの個別評価に加え、全てを統合的に検証する必要があります。車載イーサネットの適切なテストには以下の試験を含める必要があります。

- デバイスの限界点を見つけるためのデータ負荷をかけた試験
- 最悪のシナリオ上におけるネットワークの復元力の検証
- 狭帯域化、通信の途切れなどさまざまな障害条件下でのパフォーマンステスト
- D-DOS アタック（※４）などの攻撃条件下でのセキュリティ機能の検証

RFC2544

RFC 2544 テスト方法の各要素は、車載イーサネットテストに適用できます。

テスト例 ▼

スループット

スループットのテストは、大量のデータ通信に対応する十分な帯域幅があるかを判断するのに役立ちます。（負荷が大きすぎるとどうなるか、正しいアプリケーションとプロトコルが優先されているか、フェイルオーバーが正常に開始されたか、など）

レイテンシー（遅延時間）

テストにより、レイテンシーがパフォーマンスに重大な影響を及ぼし始めるポイントを特定できます。
安全機能を最適化するためには特に重要です。

フレーム損失

フレーム損失によってどの機能がより悪影響を受け、どの程度のフレーム損失で大きな問題を引き起こすか、などを理解することは車の品質を保つために非常に重要です。

新しいテクノロジー、システム、プロトコルにおいて、一定の品質と安全を確保するためには適切なテストが必要になります。

安全性

車が外部ネットワークと接続されることで、システムは他のネットワークと同じように攻撃の脅威にさらされます。実際これまでに多くの脆弱性が確認されており、ハッキングマニュアルが多数の車に存在しています。車メーカーは侵入を防ぐためのシステムを車に装備し、それらのシステムを徹底的にテストすることが不可欠です。

※4 D-DOS アタック：ネットワークを通じて大量のデータや不正なデータを送りつけて機器やネットワークなどを正常に稼働できない状態に追い込むこと。

トラフィックジェネレータを使った車載イーサネットテスト

トラフィックジェネレータは、車載イーサネットを介して大規模でさまざまなアプリケーショントラフィックを送信し、セーフティクリティカルな機能とインフォテインメントシステムの両方のパフォーマンスを評価できます。例えば、様々な組み合わせのトラフィックを生成し、ユニキャスト（※5）、マルチキャスト（※6）、ラーニングキャッシング（※7）などをテストします。
また、カメラやセンサーからの優先度の高いトラフィックがよりパフォーマンスの良いリンクにルーティングされているかを確認したりします。

他に、重いトラフィック負荷に対して、車載イーサネットを使ったすべてのコンポーネントが最適なパフォーマンスを発揮していることを確認します。悪意のある攻撃のライブラリを使用し、セキュリティと脆弱性のテストを実行することも可能です。

トラフィックジェネレータを使う事で、車載イーサネットに接続されるデバイスのテストコストと市場投入までの時間を削減し、様々な脅威から安全性を高めることが可能となります。

※5：ユニキャスト：単一のアドレスを指定して、1 対 1 で行われるデータ通信。
※6：マルチキャスト：特定のアドレスを指定して、1 対複数で行われるデータ通信。
※7：ラーニングキャッシング：通信ネットワークにおいて、同じパターンのデータを蓄積して後続の同じデータの転送を高速化するスイッチング技術。多くのネットワーク機器で使用されています。