

車載 ECU ソフトウェア更新の検討

小沼寛¹ 寺島美昭² 清原良三³

近年、自動車は先進支援システムや自動運転機能の搭載により、利便性や快適性の向上が行われている。システムの高度化に伴い通信量が増加し、従来車載ネットワークの業界標準として使用されている CAN では対応することが困難になりつつある。そこで、車載ネットワークに Ethernet の導入が検討されている。また、自動車に搭載される電子制御装置(ECU)は増加し、そのソフトウェアは大規模化している。結果、出荷後に不具合が発覚し、ソフトウェアの更新が必要となる場合がある。本論文では、今後想定される車載ネットワーク環境下での ECU ソフトウェア更新について検討を行う。

1. はじめに

自動車は先進運転支援システム(ADAS)の普及や、自動運転機能の開発などにより利便性・快適性の向上が行われている。それに伴い、自動車に搭載される Electronic Control Unit(ECU)は増加し、また、ソフトウェアの規模が増大している。その結果、出荷後に不具合が発覚する場合がある。不具合が発覚した場合、早急にソフトウェアの更新を行う必要がある。

ECU ソフトウェアの更新は車載ネットワークを介して行われる。従来、車載ネットワークは Controller Area Network(CAN)¹⁾が標準として使用されてきた。しかし、システムの高度化により通信量が増加し、CAN では対応することが困難となっている。そこで、Ethernet の導入が検討されている。Ethernet は CAN より高速な通信、柔軟なネットワークトポロジを実現できる。一方、リアルタイム性の保証がされていないため、遅延が問題となる走行に関わる部分では使用は難しい。よって、走行に関わる部分に関しては従来通り CAN が用いられることが予想される。

本論文では、今後想定される車載ネットワーク環境下での ECU ソフトウェア更新について検討する。

2. 車載ネットワーク

車載ネットワークに使用されている主なプロトコルを表 1 に示す。業界標準として使用されている CAN の最大ビットレートは 1Mbps、一度に送信可能なデータ長は 8 バイト

表 1 車載ネットワークの規格

規格	CAN	LIN	FlexRay
ビットレート	1Mbps	20kbps	10Mbps
データ長	8byte	8byte	254byte
用途	ボディ系 パワートレイン	ボディ系	パワートレイン 安全制御

1 神奈川工科大学大学院
Graduate School of Kanagawa Institute of Technology.
2 創価大学
Soka University.
3 神奈川工科大学
Kanagawa Institute of Technology.

となっている²⁾。マルチメディア系や ADAS などを使用するカメラやセンサを用いる場合、通信量が増加し CAN では帯域が不足するといった問題が生じる。そこで、Ethernet を導入する動きがある。Ethernet を導入することにより、高速なネットワークだけでなく、従来の車載ネットワークに比べワイヤハーネスを削減することができる。また、既に一般に普及している規格のため、Web サービスや様々な機器との連携が容易になることが期待される。一方、Ethernet は車載ネットワーク向けに作られていないため、走行に関わる制御系で必須となるリアルタイム性の保証や信頼性の確保がされていない問題がある。そのため、制御系には従来通り CAN や FlexRay の使用が想定される。

図 1 に今後想定される車載ネットワークの図を示す。ボディ系やパワートレインには CAN や LIN, FlexRay を使い、バックボーンやマルチメディア系、ADAS などのカメラやセンサといった通信量が多くなる部分については Ethernet が用いられると考えられる。自動車のシステムは複数の ECU が連携することで成り立っている。異なるプロトコルにある ECU 同士が連携を行う場合、ゲートウェイを通し各プロトコルの変換が必要となる。

3. ソフトウェア更新

ソフトウェア更新ではサービスの停止時間を減らすことが重要となる。ECU の更新は、自動車の所有者がディーラーに自動車を預けることで行っている。自動車をディーラーに

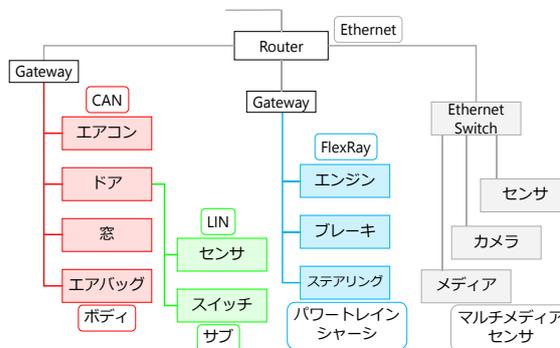


図 1 想定される車載ネットワーク図

預けるため、自動車の所有者は更新の間自動車を使用することが出来ない。そのため、更新時間を短縮し、自動車が使用できない時間を減らすことが求められる。

ソフトウェアの更新時間は更新データの転送時間と書き込み時間からなる。転送時間は更新データサイズとビットレートに依存し、書き込み時間は更新データサイズとフラッシュメモリの書き換え速度に依存する。フラッシュメモリの書き換えはイレースブロック単位で行われる。自動車に搭載されているECUのRAMやフラッシュメモリのサイズなどは様々である。更新箇所をなるべく少ないイレースブロックにまとめるようなソフトウェア構造の工夫など、各ECUの特徴を考慮することで書き込み時間を短縮できると考えられる。

4. ECU ソフトウェア更新の課題

4.1 ソフトウェア更新

自動車に搭載されるシステムの高度化により、ECUソフトウェアの更新の必要性が高まっている。また、ソフトウェアサイズの大規模化により、更新データサイズが増加し、更新時間が増えると考えられる。ボディ系のECUなどCANのような低速なネットワークを介しての更新が必要な場合、ブロードバンドに比べ転送時間が大幅にかかる。自動車内には様々なECUが混在し、他のECUの更新中にもメッセージを送信するものも存在する。そのため、ソフトウェア更新で使うことができる帯域は更に小さくなる。そこで、差分更新を用いることで更新データ量を削減し、転送時間を短縮するための研究が行われている³⁾⁴⁾。

コネクテッドカーと呼ばれるインターネットに接続した自動車や、車車間通信による情報のやりとりにもみられるように、自動車のネットワーク化が進んでいる。Over-The-Air(OTA)によるECUソフトウェア更新技術も開発されている⁵⁾。OTAにより走行中などに更新データをダウンロードしておくことで、ソフトウェア更新時のサービス停止時間を減らすことができる。また、走行中に走行に関わるECUソフトウェアの更新を行うことは危険であるが、直接走行に関わらない部分であれば更新を行うことが可能であると考えられる。表2に車両状態に応じた更新内容について示す。走行に関わる部分に関しては、停車中など、短時間自動車を使用しない間に更新を行うことでサービス停止時間を減らしつつ、ソフトウェアを早急に最新の状態に保つことが可能である。

表 2 車両状態ごとの更新内容

車両状態	更新内容
走行中	マルチメディア
停車中	パワートレイン, 安全制御
エンジン停止後	ボディ系

4.2 セキュリティ

自動車がネットワークに接続され利便性が高まる一方で、セキュリティに対する懸念も高まっている。CANはブロードキャストの配信であり、暗号化などを行っていないため、外部からCANバスに接続することができれば容易に盗聴や解析を行えてしまう。また、メッセージ認証などを行っていない場合、不正なメッセージや改ざんされたメッセージを受信してしまう恐れがある。走行に関わるECUが悪意のあるメッセージを受信してしまった場合、人命に関わるような事故が起こりかねない。ECUソフトウェア更新の際にも、更新データが正しいか認証する必要がある。

車載ソフトウェアの標準を策定するAUTOSARでは、Message Authentication Code(MAC)を用いた共通鍵暗号方式による認証方法が提案されている⁶⁾。また、MACを用いつつCANメッセージのペイロード負荷を小さくする手法も研究されている⁷⁾。これらの手法では既存のメッセージに加え、認証に用いるためのメッセージを送信しなければならないため、通信量が増加してしまう。そのため、ソフトウェア更新時の通信量も増加し、更新時間が長くなることが考えられる。

5. まとめ

本論文では、今後想定される車載ネットワークとそれに伴う課題について述べた。車載ネットワークにEthernetなど高速なネットワークの導入が検討されている一方、自動車のシステムの高度化によりソフトウェアサイズの増加や、CANを介した通信の必要性など、更新時間増加の要因となる部分も存在する。また、セキュリティの必要性が高まり、それに伴いソフトウェア更新時に必要な通信量の増加も予想される。今後、ソフトウェア更新時の更新データの認証方法や、更新時間短縮のための手法検討が必要である。

参考文献

- 1) Bosch CAN 2.0 Specification, <http://esd.cs.ucr.edu/webres/can20.pdf>
- 2) 佐藤道夫, 車載ネットワーク・システム徹底解説, CQ出版社(2005)
- 3) Yutaka Onuma, Masanao Nozawa, Yoshiaki Terashima, Ryozi Kiyohara, "Improved Software Updating for Automotive ECUs - Code Compression -," The 4th IEEE International Workshop on Consumer Devices and Systems conjunction with COMPASAC 2016
- 4) 寺岡秀敏, 中原章晴, 黒澤憲一, "車載ECU向け差分更新方式", 研究報告コンシューマ・デバイス&システム(CDS), Vol. 2016-CDS-16, No.5 (2016)
- 5) 日立, <http://www.hitachi.co.jp/New/cnews/month/2016/04/0428.html>
- 6) AUTOSAR Specification of Module Secure Onboard Communication, https://www.autosar.org/fileadmin/files/releases/4-2/software-architecture/safety-and-security/standard/AUTOSAR_SWS_SecureOnboardCommunication.pdf
- 7) 中野将志, 久保田貴也, 汐崎充, 藤野毅, "先進運転支援システムを搭載した自動車に対する制御乗っ取り攻撃の脅威分析", 研究報告組込みシステム(EMB), Vol.2016-EMB-40, No.3 (2016)