車載ソフトウェアの安全性：現状と課題

青木利晃
北陸先端科学技術大学院大学
情報科学研究科

自己紹介

- 青木 利晃（あおき としあき）
  - 北陸先端科学技術大学院大学 情報科学研究科 准教授
  - 専門分野：形式手法，ソフトウェア工学
- 研究内容・活動
  - 形式手法の産業応用（共同研究）.
    - 車載オペレーティングシステムの検証.
    - 車載システムの安全仕様の検証.
  - 実践的な形式検証手法.
  - 産業界を対象とした形式手法の普及活動.

本日の内容

- 車載ソフトウェアの概要と現状
- 車載ソフトウエアの安全性
- 車載ソフトウェアの課題

車載ソフトウェア

- 現在の自動車には多くのソフトウェアが使われている.
  - ECU (Electronic Control Unit)
- 複数のECUがネットワークで接続されている.
  - 車の制御 = ECU+ネットワーク
  - 数年前のハイエンド車でも，１００個以上のECUが使われている.

車載ソフトウェアの役割

- 自動車に占めるソフトウェアの比率は上昇している.
  - アクセサリ機能から自動車の中心的な機能，全体的な機能へ移行している.
    - 1980年(1%): アクセサリ機能.
      - カーステレオ，カーエアコン，ワイパー，etc.
    - 2005年(22%): 中心的な機能
      - 電動パワステ，ABS, ETC, カーナビ，エアバック, エンジン制御, etc.
    - 2015年(40%): 全体的な機能
      - 自動走行，衝突前検知，テレマティクス，X-by-Wire, etc.

車載ソフトウェアの規模

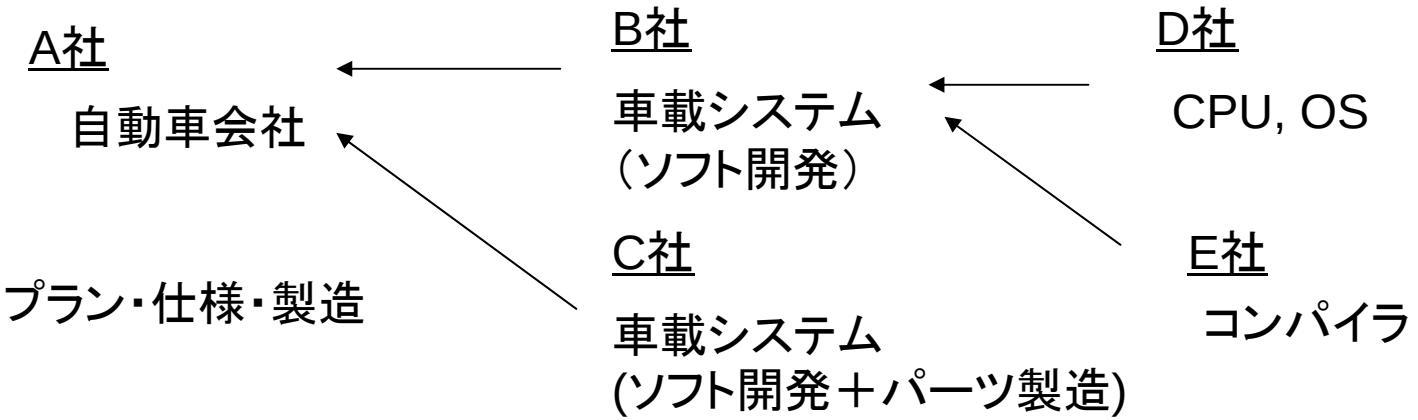
- ソフトウェア規模の変化(ROM容量).
  - 1980年代: 2KB（自動変速機の制御）
  - 1990年代: 20KB (サスペンションの制御)
  - 2003年: 200KB（駐車支援制御）
  - 2009年: 2000KB (運転支援制御)
- 現在は，車両全体のソフトウェアの規模は，約1000万行と言われている.
  - GMによると，そろそろ1億行を超えそう.
  - 10年で10倍になるという予測もある.
- 車両新機能開発工数の8割がソフトウェア開発とも言われている.

→一昔前の携帯電話と同じ状況.

  - cf) A380全体のソフトウェア規模は10億行を超える.
  - cf) Windows XPのソフトウェア規模は約4000万行.

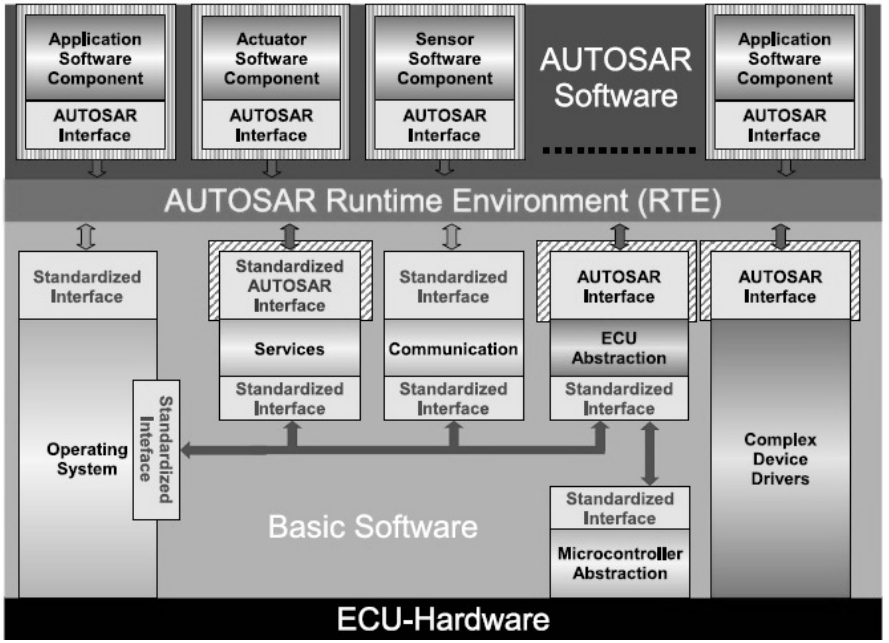
車載ソフトウェアの標準化

- 車は一社だけで作られているのではない.
- 車載ソフトウェアの部品化.
- 車載ソフトウェアの標準化.
  - AUTOSAR: the AUTomotive Open System ARchitecture



車載ソフトウエアの標準化

- AUTOSAR: 欧州が中心となって設立した組織.
  - 車載ソフトウェアの部品化，共通化することが目的.
  - 共通プラットフォームやツールなどの仕様を策定.
  - 日本の組織JASPARもあるが，世界的にはAUTOSARが主導.
    - 日本の企業もAUTOSARに加盟している.
    - AUTOSARでの活動のための調査など.



車載ソフトウェアの安全性

- 車は動いていることで危険な製品.
  - 運転者にダメージ.
  - 周囲の人にダメージ.
- 車は身近に，そして，大量に存在する.
  - 社会全体に対する危険性＝個々の製品の危険性×個数
  - 飛行機と同様の社会全体に対する危険性に抑えるためには，車の危険性をかなり抑えこむ必要がある.
    - 訓練の度合い，整備の頻度，場所などは異なるが．．．
- 車に関する安全性，信頼性の保証が重要である.
  - つまりは，車載ソフトウェアの安全性と信頼性の保証が重要.

車載ソフトウェアの安全性

- 車載ソフトウェアの安全性や信頼性に関する問題が大きな関心となりつつある.
  - 急加速問題(電子スロットル制御システムなどへの疑い）
  - ソフトウェアの不具合によるリコール
  - セキュリティ(CarShark, ハッキング)
  - 機能安全(IEC61508, ISO26262)

急加速問題

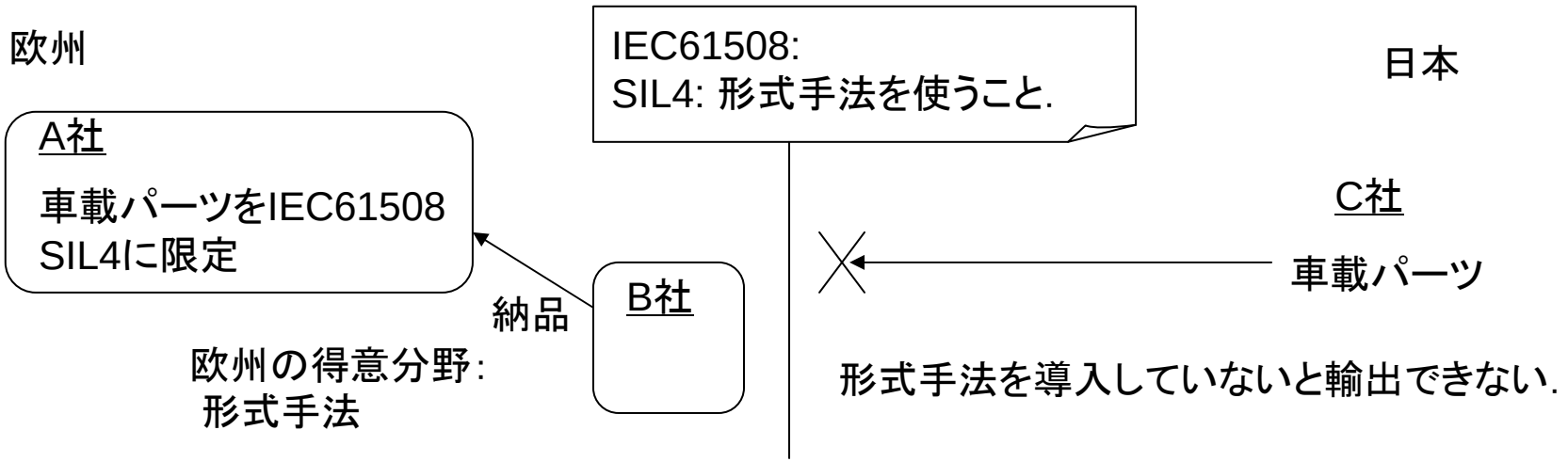
- 日本製自動車の電子スロットル制御システム(ETC, Electronic Throttle Control)の不具合の疑い.
  - 米運輸省高速道路交通安全局(NHTSA)主導での調査.
  - 米航空宇宙局への調査委託（2010/03）.
  - NHTSA報告(2011/02).
- 急加速問題を引き起こすような不具合の証拠は見つけることができなかった.
  - 急加速問題に特化した結果.
  - 急加速問題以外の問題があるかどうかの調査ではない.
- 自動車を安全に作ることは当然だが，安全であることを説明できなければならない.

リコール

- リコールは大きな損失.
  - 製品の改修にかかる費用による損失.
  - ブランドイメージの低下による損失.
- かなりの頻度でリコールは発生している.
- 車載ソフトウェアは複雑.
  - 物理世界・外部との協調動作.
  - 例外への対処.
  - 実時間性の保証.
- 色々な意味で誤りが無いソフトウェアを作ることが重要.
  - 想定や対処に漏れがない.
    - 正常処理だけでなく, 非正常処理への対処.
    - 十分な分析と対策検討.
      - 安全アセスメント, 安全設計
  - 検討結果を正しく実現するソフトウェア.

機能安全

- 機能安全（国際標準）
  - IEC61508
    - 国際電気標準会議(IEC)が制定したコンピュータ・ソフトウェアを含む電気・電子・プログラマブル電子による安全性を高めるための規格.
    - 要するに，一般的な電子機器が対象.
  - ISO26262
    - 国際標準化機構(ISO)が制定した自動車の電気/電子機器を対象とした機能安全.
    - 要するに，IEC61508を自動車分野に特化したもの.
- 安全性に関する関心の増大．．．だけ？
- 非関税障壁の恐れ.
  - 国際標準は，純粋に技術面だけではなく，政治面の意図を含んでいる.



まとめ

- 車載システムは複雑（分散システム）
- 車載ソフトウェアの規模の劇的な増大は，すでに，始まっている.
- 安全性，信頼性の低下の危惧.
- 国際競争の激化.

車載ソフトウェアの課題

- 安全性の保証.
  - 安全分析・設計の充実.
  - 分析・設計結果を正しく実装.
  - 安全であることを第三者に説明できる.
    - 第三者検証，第三者認証.
- 国際競争力をつける.
  - 内燃機関からモータへの移行に伴う，新規参入.
  - 幅広い技術力・開発力を身につける.
  - 産官学連携の推進.
    - 先進的な技術の導入と研究開発.