交通安全環境研究所フォーラム2019

ソフトウェアからみた自動車の安全性とサイバーセキュリティについて

2019年11月22日

高田 広章

名古屋大学 未来社会創造機構 モビリティ社会研究所 教授
名古屋大学 大学院情報学研究科 教授
附属組込みシステム研究センター長
APTJ株式会社 代表取締役会長・CTO
Email: hiro@ertl.jp　URL: http://www.ertl.jp/~hiro/

自己紹介

本務

- 名古屋大学 未来社会創造機構 モビリティ社会研究所 教授
- 名古屋大学 大学院情報学研究科 情報システム学専攻 教授／附属組込みシステム研究センター長

その他の役職（主なもの）

- APTJ株式会社 代表取締役会長・CTO
- TOPPERSプロジェクト 会長
- 内閣府 SIP自動走行システム 交通環境情報構築TF 主査
- 車載組込みシステムフォーラム（ASIF）会長

研究分野

- （組込みシステム向け）リアルタイムOS
- リアルタイム性解析とスケジューリング理論
- 機能安全技術，組込みシステムのサイバーセキュリティ
- 車載組込みシステムと車載ネットワーク，ダイナミックマップ

TOPPERSプロジェクト

- ITRON仕様の技術開発成果を出発点として，組込みシステム構築の基盤となる各種の高品質なオープンソースソフトウェアを開発するとともに，その利用技術を提供

組込みシステム分野において，*Linux*のように広く使われるオープンソースOSの構築を目指す!

プロジェクトの狙い

- 決定版のITRON仕様OSの開発 ← ほぼ完了
- 次世代のリアルタイムOS技術の開発
- 組込みシステム開発技術と開発支援ツールの開発
- 組込みシステム技術者の育成への貢献

プロジェクトの推進主体

- 産学官の団体と個人が参加する産学官民連携プロジェクト
- 2003年9月にNPO法人として組織化

開発成果物の主な利用事例

エスクード（スズキ）

スカイラインハイブリッド（日産）

IPSiO GX e3300（リコー）

H-IIB（JAXA）

Cell³iMager duos（SCREENホールディングス）

OSP-P300（オークマ）

SoftBank 945SH（シャープ）

UA-101（Roland）

PM-A970(エプソン)

名古屋大学 組込みシステム研究センター (NCES)

設立目的

☞ http://www.nces.is.nagoya-u.ac.jp/

- 組込みシステム分野の技術と人材に対する産業界からの要求にこたえるために，*組込みシステム技術に関する研究・教育の拠点*を，名古屋大学に形成

活動領域（スコープ）

- 大学の技術シーズを実現/実用化することを指向した研究
- プロトタイプとなるソフトウェアの開発
- 組込みシステム技術者の教育/人材育成

主な研究テーマ（プロジェクト）

- AUTOSAR Adaptive Platform（A2Pコンソーシアム）
- AUTOSARツールチェーン（APTOOLコンソーシアム）
- ダイナミックマップ（DM2.0コンソーシアム）
- 車載組込みシステムのセキュリティ強化技術

APTJ株式会社

APTJの設立背景

- AUTOSARが車載制御システム向けのSPF（広い意味でのOS）の国際標準になる流れの中で，車載制御システム向けのSPFが海外製だけになるおそれ
- 名古屋大学における研究開発だけでは不十分と判断

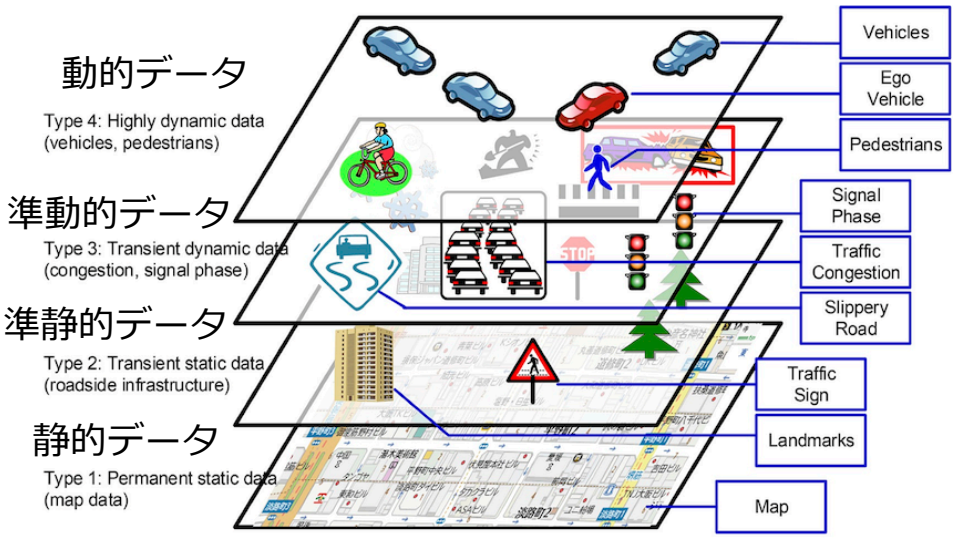
APTJの活動と位置付け

- AUTOSAR CP仕様に準拠した車載制御システム向けのSPFである Julinar SPFを開発・販売
- 名古屋大学における産学連携の研究開発成果を活用（名古屋大学発ベンチャー企業）
  - 技術的な強みは，RTOS，機能安全，サイバーセキュリティ，マルチコアプロセッサに関する要素技術と知験
- 自動車部品メーカ／自動車メーカとの共同開発
- パートナーソフトウェア企業との協力

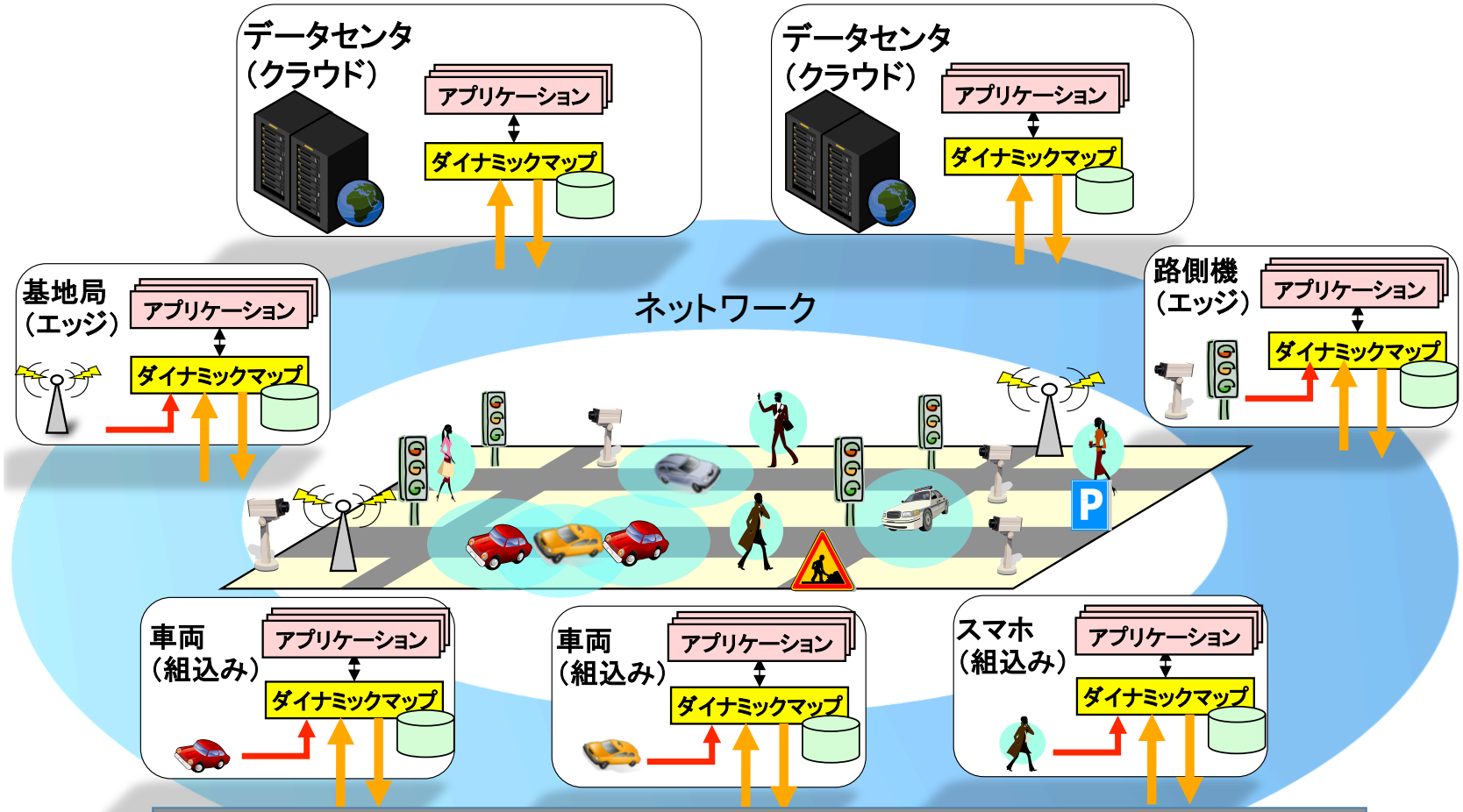
ダイナミックマップ2.0コンソーシアム

ダイナミックマップとは？

- いわゆる高精度3次元地図の上に，動的な情報を重畳させた論理的なデータの集合体（仮想的なデータベース）
- 次のような情報をリアルタイムに管理する
  - 車両や歩行者の現在位置と移動状況
  - 交通状況（信号の現示，渋滞，事故など）
- 自動運転を実現するための重要技術の1つと考えられており，国内外で研究開発が進む
  - 内閣府 SIP自動走行システムで，重点領域の1つに



ダイナミックマップ2.0の全体像



ダイナミックマップは，地図上に動的な情報を重畳させた論理的なデータの集合

- 動的な情報はローカルなセンサからだけでなく，ネットワーク経由で送受信される
- ダイナミックマップを必要とするアプリケーションは，組込み，エッジ，クラウドに存在

AGENDA

ソフトウェア化が進む自動車

自動車の安全性と機能安全 軽く説明

- 自動車の安全性と組込みシステム
- 車載システムのための機能安全規格：ISO 26262
- SOTIF（Safety Of The Intended Functionality）

サイバーセキュリティとは？ ～安全性との関係～

- セキュリティとサイバーセキュリティ
- 安全性とセキュリティの違いと関係

車載システムのセキュリティ上のリスク，分析，対策

- 自動車のサイバーセキュリティ上の脆弱性の例
- 車載システムで守るべき資産とリスク
- セキュリティ対策と安全対策の関係

車載組込みシステムのセキュリティに関する課題

ソフトウェア化が進む自動車

コンピュータ化が進む自動車（CASE以前）

例）LEXUS LS460（2006年）

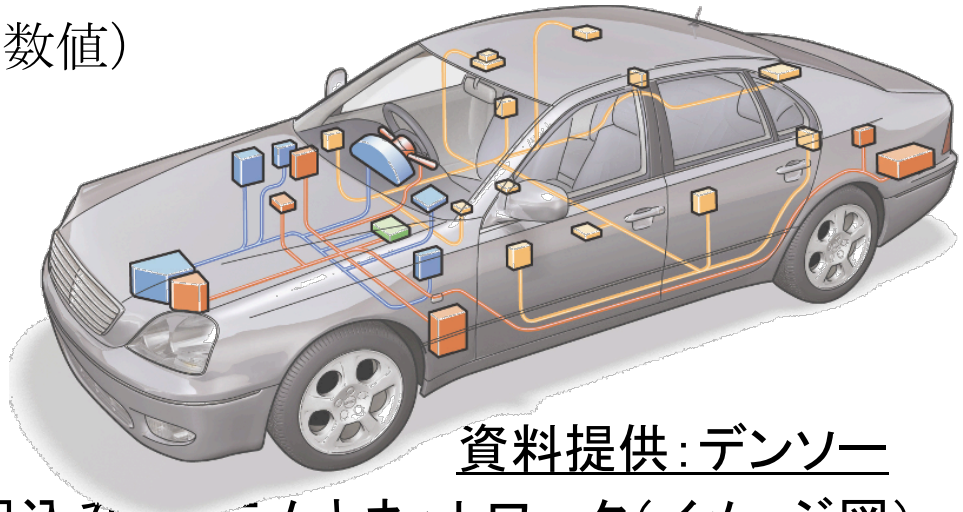
- 100個以上の車載制御コンピュータ（ECU：電子制御装置）
- 組み込まれたソフトウェアの総ライン数が7,000,000行（*A4に印刷すると10万ページに*）

（いずれも雑誌の報道による数値）

http://www.lexus.jp/

! その後の10年で，ソフトウェア規模はさらに10倍になっているとも言われている

! システムが著しく複雑化



資料提供：デンソー

車載組込みシステムとネットワーク（イメージ図）

車載組込みシステムの現状（CASE以前）

車載制御システムの高度化

- 自動車に対する新しい付加価値の多くが，電子制御/コンピュータ/ソフトウェアで実現
  - 省エネルギー，低排気ガス（エンジン制御，…）
  - 安全性の向上（ABS，エアバッグ，…）
  - 利便性の向上，娯楽性の向上（カーナビ，…）
- コンピュータを活用することで，軽量化やコストダウンが可能になる場合も

  例） 車載ネットワークによるワイヤハーネス（自動車内の配線）の軽量化
- 統合制御システム/サービス（複数のECUの協調/連携により提供するサービス）が増加

自動車に起こりつつある変化：CASE

C：Connected（つながる）

- 通信ネットワーク等により自動車の外部とデジタル情報をやりとりすることで，高度な機能やサービスを提供

A：Autonomous（自動化）

- 自動運転，無人運転

S：Shared & Services（シェアリング，サービス化）

- 自動車を個人で持つのではなく，多くの人で共有（シェア）するように？
- モノ（自動車）の所有からサービス（移動）の利用へ
  - “mobility as a service”（MaaS）

E：Electric（電動化）

- 電気自動車，ハイブリッド自動車，燃料電池自動車
- 環境問題（大気汚染，地球温暖化）への対策

CASEが車載組込みシステムに及ぼす影響

ネットワーク接続（Connected）

- 車載組込みシステムと車外のシステムの連携が拡大

自動化，知能化（Autonomous）

- 新しい技術（AIや新しいプロセッサ技術など）を取り込んで，車載組込みシステムは大きく変化
- セーフティクリティカルシステムとしては，従来になく複雑

サービス化，シェアリング（Shared & Services）

- クラウドと組込みシステムの役割分担がどうなるか？

電動化（Electric）

- HVは車載組込みシステムを複雑化．EVは単純化

共通課題

- ソフトウェアの機動的な更新（OTA）が必要に
- 車載システムのアーキテクチャが大きく変わる可能性

自動車もソフトウェア中心に？

自動車の機能・価値をソフトウェア決めるように？

- 自動車の持つ機能・価値の中で，ソフトウェアで実現されるものが増加してきた．今後，さらに増加するのは確実
- “Software-defined Vehicle”

フォルクスワーゲンが出しているメッセージ

- ハードウェアとソフトウェアを分割して調達
  - プラットフォーム（ECUのハードウェアとSPF）は，自動車メーカが用意？
- “We have to become a software company”
  - vw.OSという名称の独自のOSを開発
  - 自社内でのソフトウェア開発を増やす

自動車の安全性と機能安全

自動車の安全性と組込みシステム

安全性(など)を高める組込みシステム

- 自動車の安全性を高めるために，組込みシステムが活用されている
  - ABS(アンチロックブレーキ)，姿勢制御(例：VDIM)
  - プリクラッシュセーフティ，緊急ブレーキ
  - エアバッグ，シートベルト
- 組込みシステムは，省エネルギー・低排気ガス，利便性・娯楽性の向上のためにも活用されている

組込みシステムそのものの安全性

- 安全性(など)を高めるための組込みシステムが誤動作すると，逆に危険を引き起こす
- 組込みシステム(ソフトウェアを含む)は，十分に安全に設計・開発されなければならない → 機能安全規格

車載組込みシステムの例（1）～ ABS

ABSの機能

ABS = Anti-lock Braking System

- 車輪の回転数と車速を監視し，スリップを判定
- スリップと判定すると，ブレーキの油圧を緩めることでスリップを止める
- システムは比較的シンプル．とは言え，複雑化が進行

安全性要件とフェールセーフ設計

- ブレーキの油圧を緩め続けると，ブレーキがかからなくなる（極めて危険な事態に）
- 周期的に制御処理を行うため，1回程度の誤出力は許容される
- 何らかの異常（例えば，ECUやセンサの故障）が検知された時は，動作をやめることで，スリップは防げないが，ブレーキはかかる（フェールセーフ設計）
- 多重の自己診断機能により，異常を確実に検知する

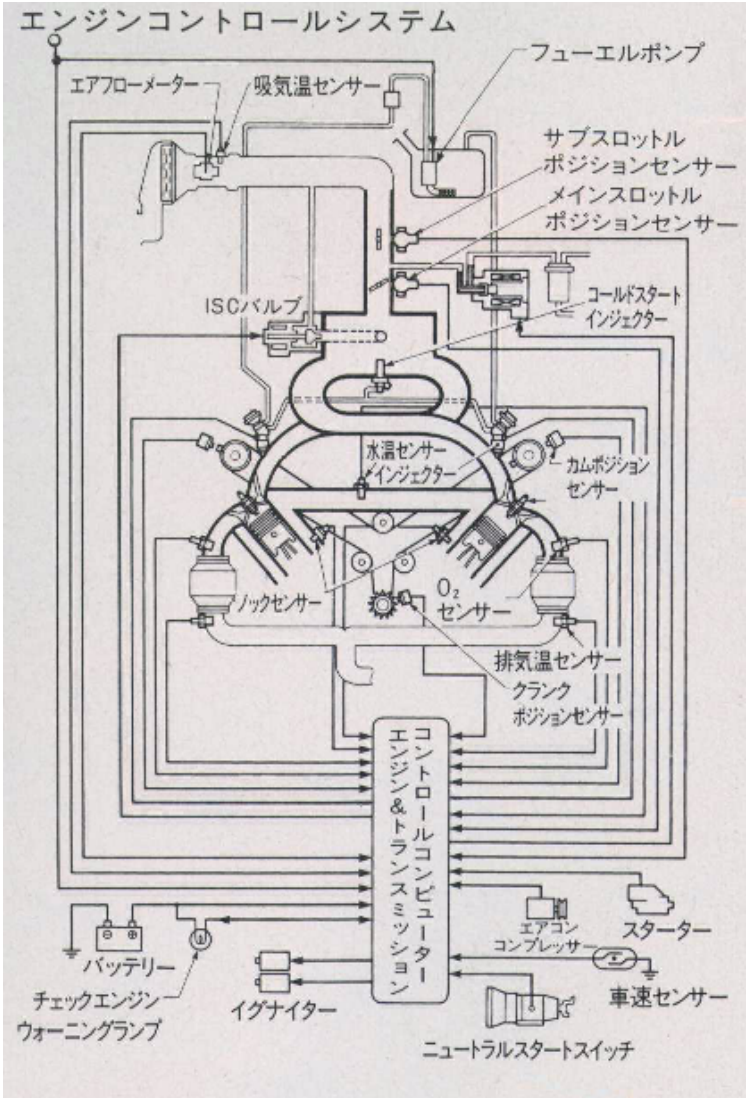
車載組込みシステムの例 (2) ～ エンジン制御

システムの構成要素

- 制御用コンピュータ
- 多数の高精度センサ
  - クランクポジションセンサ
  - エアフローメータ
  - 吸気温センサ
  - スロットルセンサ
- いくつかのアクチュエータ

システムの機能

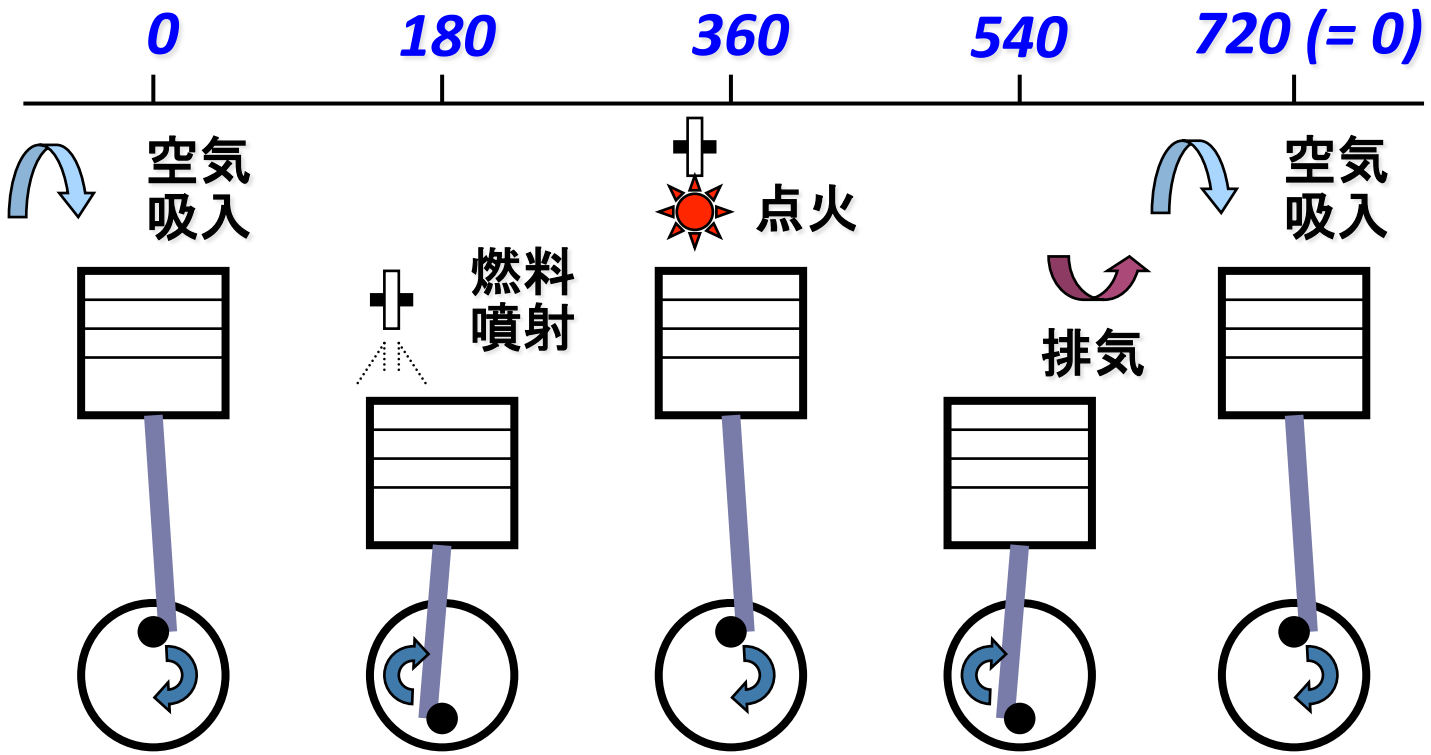
- センサからの入力をもとに，最適な燃料噴射量や点火タイミングなどを計算して，アクチュエータに出力



資料提供:トヨタ自動車

エンジン制御の基本概念

- クランク角度に同期して，1サイクル内で燃料噴射量，点火タイミングなどを制御
- 1サイクルは，6000*rpm*の時20*m*秒
- 制御タイミングの精度は，数十μ秒オーダ



エンジン制御システムの特徴

- 高速なレスポンス時間が要求される(ハードウェア:10μ秒オーダ, ソフトウェア:100μ秒オーダ)
- 時間同期処理(一定時間毎に処理)と回転同期処理(エンジンが一定角度回転する毎に処理)が混在
- 省エネルギーや低排気ガスのために複雑な制御
- 一部の処理には高い信頼性が要求される一方で, 場合によってはさぼってもよい処理がある

システムに対する安全性要件の例

- 点火をミスすると, 燃えていないガソリンが排出され, 最悪の場合は火災につながる(触媒が燃える)
- 点火プラグの制御には, 高い信頼性が要求される
- 点火プラグが故障したら, その気筒には燃料噴射してはならない. 点火プラグの故障診断が必須

安全性と機能安全

安全性（safety）

- システムが規定された条件のもとで，人の生命，健康，財産またはその環境を危険にさらす状態に移行しない期待度合い（JIS X 0134）
- 信頼性（機能単位が，要求された機能を与えられた条件のもとで，与えられた期間実行する能力（JIS X 0014））とは明確に異なる概念

機能安全（functional safety）

- 機能的な工夫（安全を確保する機能）により極力安全を確保する（NECA 技術委員会報告 第3の波「機能安全」の概要）
  - 例）踏切の警報機や遮断機
- 安全を確保するための機能を，安全機能と呼ぶ
- 本質安全と対比される考え方

機能安全と安全要求分析

機能安全と信頼性のギャップ

- 機能により，「人の生命，健康，財産またはその環境を危険にさらす状態に移行しない」ようにするのが機能安全の考え方
- まずは，安全性を確保するために必要な機能（安全機能）を定義することが必要

安全要求分析

- 安全性を確保するために取るべき手段（安全機能を含む）を抽出するための分析作業
- 危険の可能性（ハザード）の洗い出し（hazard analysis）と危険性（リスク）の評価（risk assessment）を行う
- 許容できないリスクに対して，対策を検討・追加し，再度リスクの評価を行う
- これに成功すれば，後は信頼性を確保すればよいという意味で，機能安全実現に向けての最も重要な作業

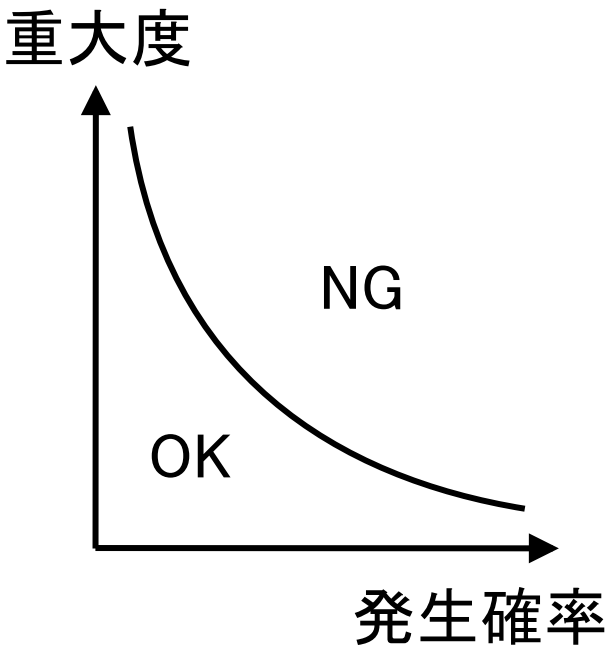
用語解説：ハザードとリスク

ハザード（潜在危険）

- 潜在的に危険の原因となりうるもの
- 自動車のハザードとしては，ブレーキがかからない，ハンドルが切れない，ハンドルが勝手に切れる，などなどが考えられる

リスク（危険性）

- ある事象生起の確からしさと，それによる負の結果の組合せ（JIS Z8115: 2000）
- 事象 ⇒ 事故
  生起の確からしさ ⇒ 発生確率
  負の結果 ⇒ 重大度（または損害）



安全要求分析の重要性

「想定外」をなくす

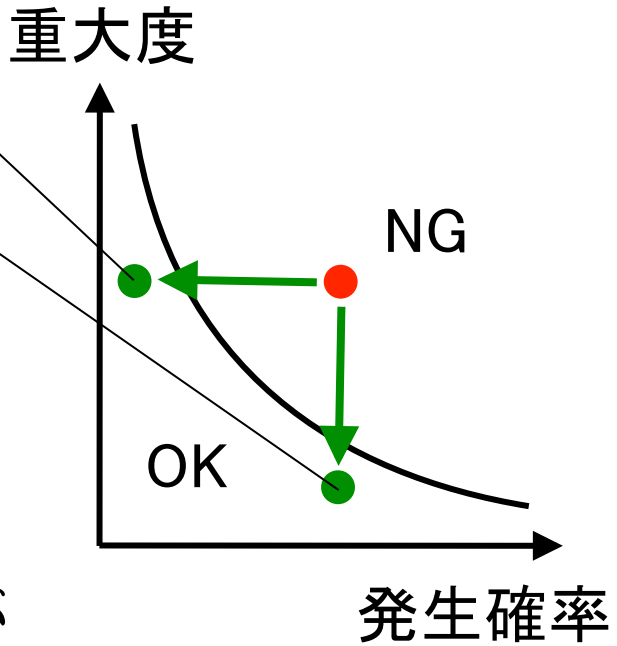
- 未知のハザードをなくす（新しいシステムで問題に）
- 正確なリスク分析は非常に難しい

安全要求の見極めによるコスト最適化

- 安全確保のために要求される特性は，システムによって大きく異なる
- システムの信頼性を高めるための技術をすべて適用すると高コストとなるため，システムに対する安全要求を見極め，最低限のコストで安全要求を満たせるようにすべき
- 信頼性と安全性が矛盾する場合があるので，両者のバランスも重要

安全システム技術

- 許容度を超えるリスクを，軽減するための技術
  - 事故の発生確率を下げる
  - 事故の重大度を下げる



高信頼システム技術

- フォールトアボイダンス
- フォールトトレランス

フェイルセーフ（fail safe）

- システムの構成要素が故障しても，システム全体が安全側（重大度が低い側）に動作するように設計する

  例）ABSの制御システムが故障したら，動作を止める
- 故障を検知する方法とそれによる検知率が問題
- 安全側の動作がないシステムには，適用できない

車載システムのための機能安全規格：ISO 26262

ISO 26262の位置付け

- “Road vehicles – Functional safety –”
- 機能安全の一般規格であるIEC 61508の自動車分野向けサブ規格
- 基本的な考え方はIEC 61508を踏襲しているが，自動車分野の状況に合致するように様々な修正/追加規定
  - 自動車向け安全度水準ASIL A～Dを規定
  - 自動車に特化したハザード分類の方法を定義
  - 大量生産品であることを考慮
  - 複数の組織で開発することを考慮
- 初版が2011年11月，第2版が2018年12月に発行
- 第2版で，適用範囲が大型車やバイクにも拡大

ISO 26262における機能安全の定義　*一般の定義より狭い*

- 電気・電子システムの誤動作を原因とするハザードによる許容できないリスクがないこと（ISO 26262-1独自訳）

規格の性格・考え方（IEC 61508と同様）

- 安全性確保のためのベストプラクティスの集大成
  - 安全性確保のための技法が数多く挙げられており，安全度水準（ASIL，A～Dの4レベル）に応じて使用すべきもの（一部，使用すべきでないもの）を定めている
- ハードウェアの信頼性は，部品の故障率から積み上げて計算する
- ソフトウェアの信頼性は，プロセスにより確保する
  - ASIL毎に規定された必須技法を使って開発されたソフトウェアは，十分な信頼性があるとみなす

ASIL（Automotive SIL）とは？

- 許容できないリスクを回避するために必要な安全方策の要求レベル
- ASIL D（もっとも厳しい）～A（もっとも厳しくない）～QM
- IEC 61508のSILと違い，確率要求/目標を含まない
  - ただし，ランダムハードウェア故障に関しては確率目標が与えられる

ASILの決定方法

- ハザードの過酷さ（severity），暴露度（exposure），制御性（controllability）から決定

過酷さ×曝露度×制御性

- 例えば，致命傷の可能性があり，頻繁に発生する状況で起こり，回避が困難なハザードは，ASIL D

SOTIF (Safety Of The Intended Functionality)

SOFITとは？

- 性能限界や誤使用など，システムの誤動作以外に起因するリスクを想定して安全なシステムを設計すること
- 本来の機能安全には含まれる

なぜ，ISO 26262の機能安全の定義は狭いのか？

- 自動車にとっての本来の機能安全は，ABS，姿勢制御，緊急ブレーキ，エアバッグといったシステムによる安全
- SOTIFは，機械技術や制御技術側の課題であった

今，SOTIFが重要視されているのはなぜ？

- レベル3以上の自動運転に必須であるため
  - これまでの安全運転支援から安全運転そのものへ
- 自動車がソフトウェア中心に変わろうとする中で，ソフトウェア技術（や電子技術）が自動車の安全性確保の前線に

国際標準規格の動向

ISO 26262 second edition – Functional safety

- 予定より遅れていたが，2018年末に正式発行
- 半導体パート（Part 11）の追加，二輪車への適用拡大（Part 12の追加），大型車・商用車への適用拡大
- ソフトウェアのパート（Part 6）の変更（ソフトウェア安全指向分析，モデルベース開発技術，A-SPICEとの整合性など）
- マネジメントのパート（Part 2）の変更（サイバーセキュリティへの言及，安全アノマリの管理など）
- フェイルオペレーショナルへの言及

ISO/PAS 21448 – Safety of the intended functionality（SOTIF）

- 性能限界と誤使用をカバー
- PAS（公開仕様書）はガイドライン（レベル2までに対応）
- 今後，自動運転に対応できるようにして国際標準化

サイバーセキュリティとは？
～安全性との関係～

セキュリティとサイバーセキュリティ

セキュリティとは？

- 単なる「セキュリティ」は意味が広い
  - 辞書で最初に書かれているのは「安全」で，セーフティと区別がつかない
  - 「安全確保」「防護」という意味もある
- 「セキュリティ」という用語は，主に，故意による攻撃からの防衛を意味している場合が多い
  - national security ＝ 安全保障
  - home security ＝ 防犯
  - 「○○セキュリティ」とは，○○に対する攻撃からの防衛を意味していることが多い
- それに対して安全技術は，主に，自然に発生する故障や，(故意でない)人為的なミスに対処することを主眼としている

情報セキュリティ（information security）

- 情報の機密性，完全性および可用性の維持（JIS X 5080）
- さらに，真正性，責任追跡性，否認防止，信頼性などの特性の維持を含める場合も（ISO/IEC 27001）

機密性（confidentiality）

- アクセスを認可された者だけが情報にアクセスできることを確実にすること

完全性（integrity）

- 情報及び処理方法が，正確であること及び完全であることを保護すること

可用性（availability）

- 認可された利用者が，必要なときに，情報及び関連する資産にアクセスできることを確実にすること

サイバーセキュリティとは？（様々な定義）

- 「サイバー攻撃に対する防御行為」（デジタル大辞泉）
  - サイバー攻撃とは，「コンピューターネットワーク上で，特定の国家，企業，団体，個人に対して行われるクラッキング行為」（デジタル大辞泉）
    - ECUに対する直接的な攻撃も考えると，「コンピュータネットワーク上で」の部分が狭いように思われる
  - 「サイバー」は，攻撃の対象ではなく，攻撃の手段を表している（他の「〇〇セキュリティ」とは用語ででき方が異なる）
- 認可されないアクセスや攻撃に対してサイバーフィジカルシステム（CPS）を守るために取られる手段（SAE J3061独自訳）
  - 「サイバー」をCPSと置き換えて，攻撃対象という解釈にしているが，無理があるように思われる

サイバーセキュリティとは？（様々な定義）– 続き

- サイバーセキュリティ基本法による定義（一部省略）

> 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること

  - 攻撃に限定されていない広い定義で，焦点がぼけている
  - 「人の知覚によっては認識することができない方式」の部分は1つの本質であろう
- 現時点で良さそうに思える定義（2案）
  - サイバー攻撃（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式による攻撃）からの防御行為
  - 電気・電子システムに対する攻撃を原因とするハザードによる許容できないリスクがないこと（ISO 26262流）

安全性とセキュリティの違いと関係

何を守るか（守るべき資産）の違い

- 安全性：人の生命，健康，財産またはその環境
- ○○セキュリティ：○○（例：情報）
- サイバーセキュリティ：限定しない

! サイバーセキュリティの方が範囲が広い（例えば，個人情報を守ることは安全性の範囲外）．ただし，「財産」を広く捉えると，違いはなくなる

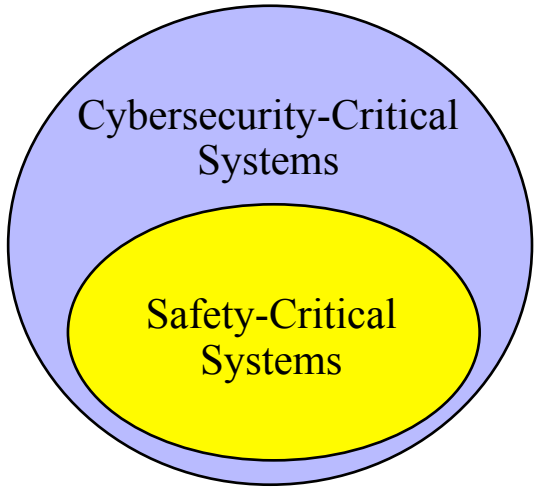
何から守るかの違い

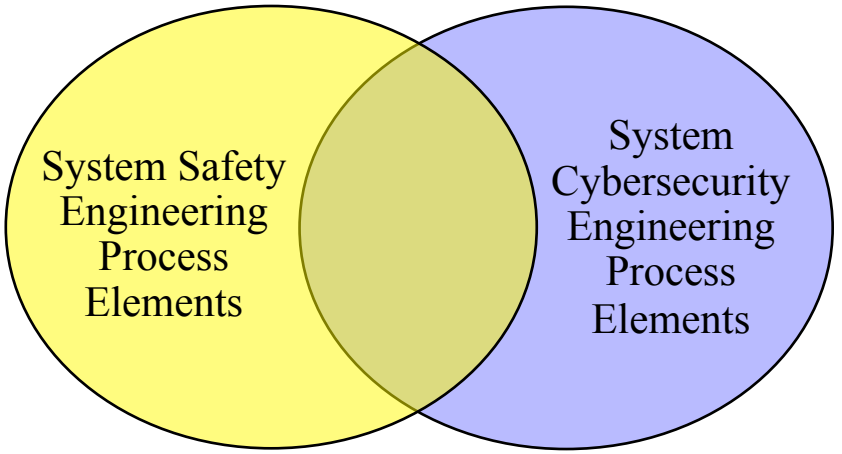
- 安全性：故障や（故意でない）人為的なミス
- セキュリティ：故意による攻撃
- サイバーセキュリティ：サイバー攻撃（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式による攻撃）

SAE J3061における安全性とサイバーセキュリティ

※ SAE J3061 : “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”

- セーフティクリティカルシステムは，すべてサイバーセキュリティクリティカルシステムである
  - 逆は成り立たない
  - 守るべき資産の違い
- セーフティエンジニアリングプロセスとサイバーセキュリティエンジニアリングプロセスには，共通部分もあるが，相違もある
  - 何から守るかの違い





車載システムのセキュリティ上のリスク，分析，対策

自動車のサイバーセキュリティ上の脆弱性の例

脆弱性を明らかにした研究報告等

- CANを通じた攻撃に対する脆弱性（2010年）
  - 市販車（米国車）に対してサイバーセキュリティ面の各種の攻撃を加えた結果，数々の脆弱性を発見
  - ECUのソフトウェアの書換えに成功
- 上と同様のことが，車外からネットワーク経由等でも可能なことが示されている（2011年）
- タイヤ圧監視システムの脆弱性（2010年）
- スマートキーシステムの脆弱性（2010年）
- イモビライザの脆弱性（2012年）
- DEF CON 21における報告（2013年）
- スマートフォンによる遠隔操作機能の脆弱性（2015年）
- テスラ Model Sの車載コンピュータの脆弱性（2016年）

脆弱性に関する最近の研究報告のトレンド

- OBD-IIポートに接続するモジュールに対する攻撃
- ADAS/自動運転のセンサに対する攻撃

サイバーセキュリティ上の事件（インシデント）

- 遠隔から100台以上の自動車を使用不能に（2010年）
- イモビライザを解除する装置（イモビカッター）の流通とそれを用いた自動車の窃盗（2010年）
- 電子機器を使って自動車を解錠し，自動車内のものを盗難（2015年に報道）

自動車のサイバーセキュリティに関する訴訟，リコール

- クラッキングされる可能性のある自動車を，それを知りながら説明せずに販売したとして，トヨタ，Ford，GMに対して集団訴訟がおこされる（米国，2015年）
- クライスラーが，車の遠隔操作問題で140万台のリコールを発表（2015年）

車載システムで守るべき資産とリスク

安全性にかかわる資産

- (主に)人の生命や健康に対するリスク

安全性には含まれない資産(境界は曖昧)

- 金銭，物品(自動車そのもの，車内に置いた物品)，エネルギー(電気自動車の電気)，環境の盗難・破壊
  - 物理的な攻撃(例:自動車の盗難)は，サイバーセキュリティの範囲外
  - これらを守る機能が情報技術で実現されていれば(例:電子キーやイモビライザ)，そこから先は範囲内
- 個人情報やその他の情報の流出・改ざん
  - 「情報セキュリティ」の範囲内

さらに「他に迷惑をかけないこと」も

- 車載システムがサイバー攻撃の踏み台に利用される

セキュリティ対策と機能安全の類似性

- 許容できないリスクに対して，セキュリティ対策を行う

セキュリティ対策は機能によって行うのが基本

- 「セキュリティ機能」によってセキュリティを確保する
- 「本質セキュリティ」もないわけではないが…

「セキュリティ機能」の決定が重要

- 機能安全においては，安全性を確保するために必要な安全機能が定義できれば，後は信頼性を確保すればよい
  - 安全性を確保するために取るべき手段（安全機能を含む）を抽出するための分析作業が，安全要求分析
- セキュリティにおいても同様
  - セキュリティ要求分析の技術が重要に
- 信頼性確保の部分は，安全性とセキュリティで大きい違いはなく，共通化が可能

セキュリティに対するリスクと評価

セキュリティに対するリスク

重大度×脆弱性×脅威

- 脆弱性（vulnerability）
  - セキュリティ上の問題を起こす可能性のあるシステムの弱点（欠陥や仕様上の問題）
  - セキュリティホール（セキュリティ上の問題を起こす可能性のあるシステムの欠陥）は脆弱性の一部
- 脅威（threat）
  - 脆弱性を利用してリスクを現実化させる手段

セキュリティリスク評価

- システムの脆弱性と脅威を特定し，発生頻度などのデータに基づき，どれだけの影響があるかを評価すること

セキュリティ分析手法

セキュリティ要求分析とは？

- セキュリティを確保するために取るべき手段（セキュリティ機能）を抽出するための分析作業
- 攻撃の可能性（attack goal）の洗い出しと危険性（リスク）の評価（risk assessment）を行う
- 許容できないリスクに対して，セキュリティ対策を検討・追加し，再度リスクの評価を行う

セキュリティ要求分析の必要性

- どのようなセキュリティ対策が必要かを明らかにするためには，セキュリティ要求分析が不可欠
  - 分析なしで対策を行うと，過剰に対策することに
- セキュリティ強化には，裏口を防ぐことが必要
  - 裏口を見つけるためには，システム全体の分析が重要

セキュリティ要求分析の要素

- 守るべき資産の特定
- 脅威分析（攻撃の可能性の網羅）
- リスク評価
- セキュリティ機能策定と要件定義

セキュリティ要求分析の困難点

- 攻撃の可能性（attack goal）の網羅方法
  - どのような攻撃がありうるかを，網羅的に数え上げるのは難しい（犯罪の手口は常に新しいものが出てくる）
- セキュリティリスクの評価
  - 特に脅威が変化するため，正確な評価が難しい

見落としがちな分析観点

- セキュリティ機能自身に脆弱性はないか？
- 鍵を無くした時の対策に脆弱性はないか？

セキュリティ対策と安全対策の関係

安全対策はセキュリティ対策としても有効な場合がある

- システムの安全性を向上させるための対策は，セキュリティを強化する上でも有効な場合がある
  - 故意による攻撃で起こることは，故障によっても起こりうるため

安全対策だけではセキュリティ対策として不十分

- 故障によって起こる確率が極めて低い（現実的には起こらない）事象も，故意による攻撃では起こりうる
  - ISO 26262では，二重故障（独立なコンポーネントが同時に故障するケース）は，基本的には想定しなくても良い
- 特に，内部の者による故意による攻撃は想定されていないことが多い

安全性とセキュリティの両立の困難性

どこまでのリスク評価を行うか？

- 機能安全規格は，厳密なリスク評価を要求する
- セキュリティリスクを厳密に評価するのは難しい

Guarantee文化とBest Effort文化の衝突？

セキュリティ分析（リスク評価を含む）の困難点

- 攻撃の可能性（attack goal）の網羅方法
  - どのような攻撃がありうるかを，網羅的に数え上げるのは難しい（犯罪の手口は常に新しいものが出てくる）
- 脅威は変化するため，セキュリティリスクを厳密に評価するのは難しい

  例）高性能な計算機ができると，暗号が破りやすくなる

  例）セキュリティホールが公表されると，攻撃が容易になる

車載組込みシステムの
セキュリティに関する課題

セキュリティ強化に向けての課題

セキュリティ対策の基準がない … *最大の課題*

- 一般に，セキュリティ対策をする（≒セキュリティ機能を追加する）ほど，コストは上がる
  - 対策をやり過ぎて，無用なコストアップになるのは避けるべきだが，何が「やり過ぎ」なのか判断が難しい
- 策定中のISO/SAE 21434で，何らかの基準（相場観）が示されることが期待されるが…
  - 策定が遅れ気味（もめているという話し）
  - CAL（Cybersecurity Assurance Level）でクラス分けという話しも聞いていたが，標準化は難しそう
- 現時点で使える基準
  - 許容されている既存リスク（特に，物理的なセキュリティリスク）との比較で考える
  - 自分がユーザになった気持ちで考える

セキュリティ要求分析技術

- Security by Design（SbD）に向けてのキーとなる技術
- Attack tree などのセキュリティ分析手法が知られているが，まだ確立された技術とは言えない

組込みシステムに向いたセキュリティ技術

- 堅いセキュリティ技術は，IT分野の技術を用いるのが妥当だが，実現コストは大きくなる
- 妥当なコスト（言い換えると，限られたリソース下）で，そこそこ堅いセキュリティを実現するには，応用ドメインの特性を活かすことが必要

V2X通信やクラウド連携を考えたセキュリティ

- 他の組込みシステムやクラウドからの情報を信じて良いか？
- 法的責任にも関連

取り組むべき技術課題

セキュリティ要求分析手法の確立と支援技術

- 中長期的には，形式手法や人工知能による分析支援が求められる

システムのアーキテクチャからの考慮

- セキュリティ確保に重要な部分と，安全性確保に重要な部分を分離したアーキテクチャとする

組込みシステムに向いたセキュリティ強化技術の開発

- 情報セキュリティ対策のための要素技術は数多く開発されており，それらの多くは組込みシステムにも使える
- 組込みシステムでは，限られたリソース下でのセキュリティ強化技術が求められる

連携セキュリティ基盤（信用フレームワーク）の構築

- 他社で開発されたシステムをどれだけ信じてよいかを判断する仕組みを，業界を超えて構築する必要

その他に取り組むべきこと

セキュリティ対策に対する相場観の醸成

- ソフトウェアの安全性の規格も相場観に過ぎず，それと同様に，セキュリティ対策に対する相場観を作ることが必要

変化する脅威に対応する仕組みの導入

- 変化する脅威に対応してシステムを更新する仕組み（制度面も含めて）を導入する（その必要性の認識を広める）

人材育成

- 情報セキュリティ技術と車載組込みシステム技術の両方に精通した技術者が必要

ユーザに対する啓蒙

- ユーザに対して，セキュリティが強い/弱いの意味を理解してもらう必要がある