Vol.2015-SLDM-170 No.50
Vol.2015-EMB-36 No.50
2015/3/7

# 自動車制御システムにおける 故障発生時の短時間機能維持による高安全化コンセプトの検討

大塚敏史[†1]　　櫻井康平[†2]

自動車の電気電子（E／E）システムは，利便性や快適性の向上と環境負荷低減を目的として大規模化を続けている．今後，予防安全技術の進化に伴いE／Eシステムの制御範囲がさらに拡大することにより，安全設計がより重要となる．本研究では，自動車制御システムの安全性確保とコスト低減の両立を目的とし，故障発生時に短時間の機能維持後ドライバに制御を引き渡す冗長性低減アーキテクチャを検討した．センサ故障により認識不能となった範囲に存在する他車の高安全な行動予測と，演算・通信機能の故障に対応する制御情報バッファリングの２つの安全機構を考案し，これらを用いた自動車制御システム向け安全コンセプトを構築した．

# A Functional Safety Concept for Highly Safe Vehicles with Keeping the Control System Alive for a Short Time

SATOSHI OTSUKA[†1]　KOHEI SAKURAI[†2]

Electric and Electronics (E/E) systems for vehicles significantly enlarge the control area to improve convenience, comfort, and environmental load reductions. Improving of driver assistance systems will accelerate the trend and require safer design than current vehicles. The purpose of this research is improving safety of vehicles and reducing the cost due to redundancy at the same time. Therefore, we focused on developing a functional safety concept which can keep the control system alive until a driver can take over the control. We designed a functional safety concept for a control system of a vehicle with two developed mechanisms: a prediction of other vehicles in unrecognized area corresponding to the failure of sensors, and a buffering of control information corresponding to the failure of communications or calculations.

## 1. はじめに

自動車の E/E （Electric and Electronics：電気電子）システムは，ドライバの安全性・快適性の向上や環境負荷低減を目的とした高度な制御を実現するために，その制御範囲を拡大している．特に，近年機能の進化が著しい先進運転支援システム（Advanced Driver Assistance Systems：ADAS）は，ドライバの制御を代替し，加減速制御や操舵（レーン走行維持）を実施し，また予防安全機能として緊急ブレーキを実現している．ADAS は，複数の E/E システム（センサ, アクチュエータ, コントロールを行う ECU （Electronic Control Unit））の連携による自動車全体の統合制御により，上記の高度な制御を実現している．

E/E システムの制御範囲拡大に伴い, E/E システムの故障に対応する安全性確保の設計が重要となる．自動車 E/E システムの故障に対しては, 機能安全規格である ISO26262[1]が 2011 年に発行されるなど，E/E システムの故障に対する安全性が広く求められている．

一方で，耐久消費財である自動車の開発においては，コストが重要な指標となる．開発コストの増加はユーザの負担になるため，不要な冗長性を削減し，必要十分な安全性を限られたコストで実現することが重要となる．

そこで本研究では，

**・ADAS の安全性向上**

**・ADAS の不要な冗長性低減によるコスト削減**

を目的とし，自動車システムの安全分析と，高度な安全性を実現する短時間機能維持という要件から安全機構（Safety Mechanism）を考案し, 安全コンセプトを構築した．

２章では，関連研究として E/E システムなどのアーキテクチャ設計評価手法および安全設計手法，３章では対象とする予防安全システムの分析内容と，分析結果に基づく安全コンセプトと安全機構の構築結果，４章では従来手法による安全コンセプトとの比較について示し，５章で結論を述べる．

## 2. 関連研究

自動車 E/E システムの安全設計･評価を行う手法として，欧州プロジェクトの SAFE[2]がある．SAFE では，アーキテクチャ記述言語の EAST-ADL[3]を用い，モデルベース開発により自動車 E/E システム全体の安全性設計・検証を実施する方法を提案している．

また，アーキテクチャを設計・評価する手法として ATAM[4]があり，安全性を含めてアーキテクチャの評価手法を提案している．また航空・自動車分野で用いられるアーキテクチャ記述言語の AADL[5]を用い，故障の伝播モデルを構築して安全分析を行う手法が提案されている[6].

制御システムの安全性・信頼性向上を目的とし，機能の

†1 (株)日立製作所 日立研究所
Hitachi Research Laboratory, Hitachi, Ltd.
†2 日立オートモティブシステムズ（株）
Hitachi Automotive Systems, Ltd.

Vol.2015-SLDM-170 No.50
Vol.2015-EMB-36 No.50
2015/3/7

一部を冗長化する Fault-Tolerant システムは，航空などの高信頼化が必要な分野で先行して研究されており[7][8]，自動車分野への適用について研究が行われている[9].

## 3. 提案方式

既存手法では，E/E システムなどの制御システムの安全性を評価する手法や，多重化により安全性・信頼性を向上する手法について述べられているが，制御システムの冗長性を効果的に低減する方法は述べられていない.

そこで本検討では，既存の安全分析手法を用いて，ADAS の安全性向上および冗長性低減のために対処すべき故障を特定し，ADAS における短時間機能維持の要件に着目して安全機構を考案し，冗長性を低減した安全コンセプトを構築した．その検討内容について以下に述べる.

### 3.1 自動車制御システム安全分析

自動車制御システム安全分析のプロセスは機能安全規格（ISO26262[1]）に倣い，アイテム定義，システムアーキテクチャの構築，ハザード分析，故障影響分析を実施した.

アイテム定義は，ADAS システムにて実現すべき機能を分析し，図 1 に示す自動車システムアーキテクチャを作成し，各機能ブロックの要件を導出した.

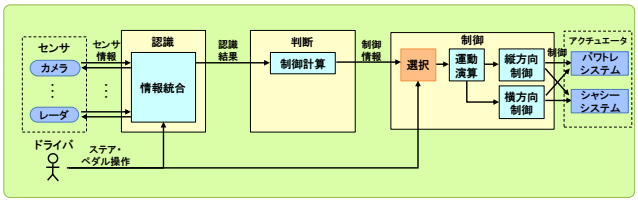



図 1　自動車システムアーキテクチャ

その後，HAZOP（Hazard and Operability Studies）[10]によるハザード分析を上記アーキテクチャの機能ブロックに対して実施し，ハザードの導出を行った.

導出したハザードを引き起こす故障モードを分析するため，システムレベルの FMEA[11]を実施することにより，対応すべき故障モードを抽出した.

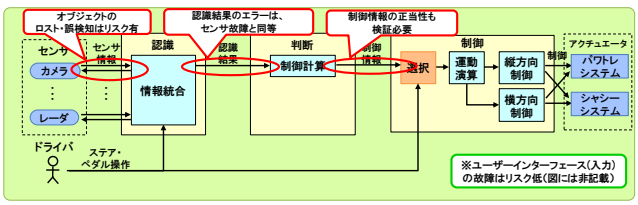



図 2　システム FMEA による故障モード抽出

図 2 に示す通り，ハザードを引き起こす故障モードは，認識，判断，制御のパスにおける誤り・機能停止であることを抽出した．これら故障モードに対応する安全コンセプトおよび安全機構を検討した.

### 3.2 安全コンセプト・安全機構

ADAS による制御実行中は，ドライバは操作の一部を制御システムに委譲している．ADAS 機能失陥時に，即座に機能を停止することに比べ，機能を一定時間継続させることによりスムーズな制御の委譲が可能になり，結果として安全性を高めることが可能となる．しかし，機能維持のために ADAS に関連する全ての構成要素を多重化することはコスト増となる.

そこで ADAS の機能を短時間維持し，ドライバに制御を引き継ぐ安全コンセプトを実現するアーキテクチャの検討を行った．アーキテクチャの概要を図 3 に示す.

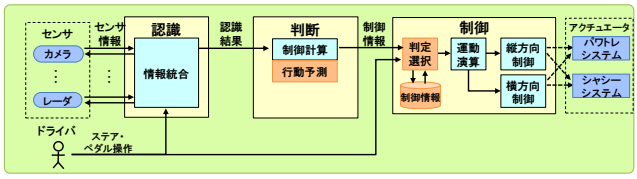



図 3　提案安全コンセプトを実現するアーキテクチャ

センサの故障に対応する障害範囲他車行動予測と，認識・判断および通信の故障に対応する制御情報バッファリングの 2 つの安全機構を用いて安全コンセプトを構築した．安全機構の詳細について以下説明する.

#### 3.2.1 障害範囲他車行動予測

センサ故障時に，短時間安全性を確保するため，センサの障害発生範囲に存在する他車の行動を高安全に予測して運動制御を行う安全機構を検討した.

センサの認識範囲を予め計算しておき，センサの故障を検出した場合には，故障したセンサの認識範囲に直前まで存在していた他車の行動について，最も自車にとって危険な行動（例：現在の運動状態で最も自車に接近可能な軌道）を想定し，自車の制御（回避行動）を実施する．これにより，認識不能な範囲の他車行動により，自車が危険な状態となることを防ぐことが可能となる．概要を図 4 に示す.

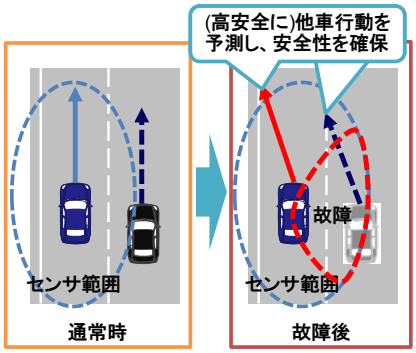



図 4　障害範囲他車行動予測

Vol.2015-SLDM-170 No.50
Vol.2015-EMB-36 No.50
2015/3/7

### 3.2.2 制御情報バッファリング

認識・判断および通信機能の故障発生時に短時間安全状態を確保するため，制御情報をバッファリングする構成を検討した．通常時に判断部が今後の制御情報を事前に演算して送信しておき，障害発生時には制御部がバッファリングした制御情報を基に制御を短時間継続する．これにより，短時間は以前の情報を基に安全な制御を実現することが可能となる．処理の概要を図 5 に示す．

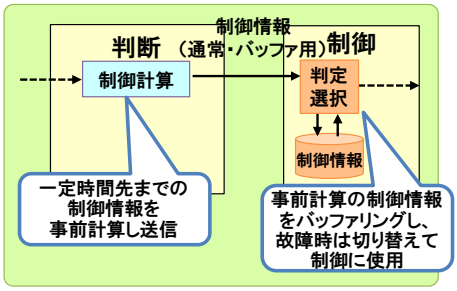


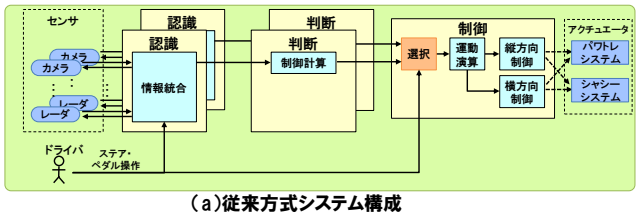

図 5　制御情報バッファリング

## 4. 評価および考察

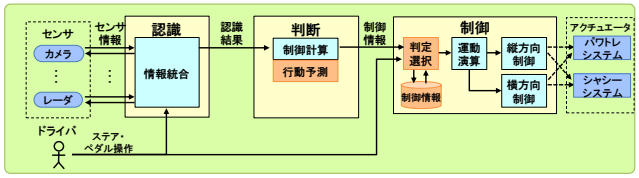
ADAS の機能における故障発生時に，制御を一定時間継続する方法として，多重化による方式と提案方式について，制御システム構成および安全性・コスト・可用性の観点から比較を行った．

前提として，どちらの方式も制御部，アクチュエータは十分な冗長性を持ち，故障時も機能を継続可能としている．

### 4.1 アーキテクチャ構成比較

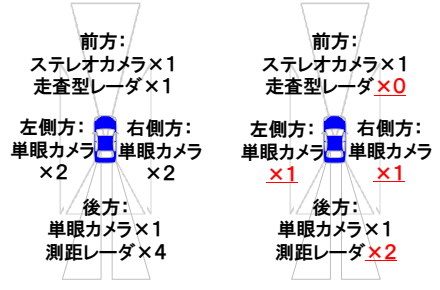



（a）従来方式システム構成




（b）提案方式システム構成

図 6　従来方式・提案方式のシステム構成




(a) 従来方式による構成　(b) 提案方式による構成

図 7　従来方式・提案方式のセンサ構成

制御システム構成の比較を図 6 に，センサ構成の比較を図 7 に示す．従来方式ではセンサ，ECU および通信経路の多重化が必要となる．特に，センサ構成は周囲いずれの方向についても認識不能を防ぐために多重化を行っている．提案方式は各方向それぞれ 1 系統のみとしている．

また ECU においても，認識および判断の演算用 ECU は従来方式では多重化が必要であり，提案方式では，ECU 多重化を不要としている．ただし，障害範囲他車行動予測および制御情報バッファリングによる演算量や通信量増加への対応は必要となる．それぞれの方式の部品点数の一覧を表 1 に示す．ここでは通信経路の冗長性や，ECU の演算性能等は考慮していない．

表 1　構成部品点数の比較

| | | 従来方式 | 提案方式 |
|---|---|---|---|
| | | 個数 | 個数 |
| センサ | ステレオカメラ | 1 | 1 |
| | 走査型レーダ | 1 | 0 |
| | 単眼カメラ | 5 | 3 |
| | 測距レーダ | 4 | 2 |
| ECU | | 4 | 2 |

各方式における故障個所への対策方針を表 2 に示す．ここでは◎は継続動作可能，○は短時間の機能維持による安全確保を示している．従来方式は，多重系によりいずれの箇所が故障しても動作継続可能であり，提案方式は短時間の機能維持による安全性確保を行う．

表 2　故障個所に対する方式ごとの対策方針

| 故障個所 | センサ | 通信 | 認識 | 判断 | 制御 |
|---|---|---|---|---|---|
| 従来方式 | ◎（多重系） | ◎（多重系） | ◎（多重系） | ◎（多重系） | ◎（多重系） |
| 提案方式 | ○（行動予測） | ○（制御情報バッファリング） | ○（制御情報バッファリング） | ○（制御情報バッファリング） | ◎（多重系） |

### 4.2 考察

従来方式と提案方式の安全性・コスト・可用性の比較を表 3 に示す．

表 3　安全性・コスト・可用性の比較

| | 安全性 | コスト | 可用性 |
|---|---|---|---|
| 提案方式 | ○ | ○ | △ |
| 従来方式 | ○ | × | ○ |

従来方式および提案方式は，どちらも安全分析にて抽出したハザードの発生を抑制可能と想定し，安全性は同様に○とした．

一方で従来方式は部品点数が多く，コストを×としている．提案方式はその点でコストを削減可能であるが，故障時は短時間のみ機能維持可能であるため，ADAS 機能の可用性は低下する．しかし，ADAS における故障発生は発生頻度が低いと想定しているため，故障発生への遭遇率が低く，故障発生時の可用性低下はユーザへの影響が少ないと想定している．

また，提案の安全機構（障害範囲他車行動予測，制御情報バッファリング）により，どの程度ハザード発生が抑制

可能であるかは，各 ADAS の機能要件や走行シチュエーションに依存するため, ADAS の機能要件を明確化した後に，走行シチュエーション分析等の実施により安全性を評価する必要がある．

## 5. おわりに

本検討では，ADAS の安全性向上とコスト削減を目的とし，短時間機能維持後ドライバに制御を引き渡す安全コンセプトを構築した．ADAS の短時間機能維持の要件を前提とし，センサの故障に対応した障害範囲他車行動予測と，認識・判断および通信機能の故障に対応する制御情報バッファリングの２つの安全機構を考案し，安全コンセプトを構築した．

今後の課題として，提案方式による安全性の検証について，ADAS 機能と走行シチュエーションに合わせた安全分析およびシミュレーションや実車環境での評価，および各安全機構の詳細検討が挙げられる．

**謝辞**　本研究を進めるにあたりご指導頂いた日立オートモティブシステムズ（株）の真野宏之主管研究長，（株）日立製作所日立研究所の成沢文雄主任研究員に感謝する．

## 参考文献

1) ISO International Standard : Road vehicles – Functional safety, ISO Standard 26262, Rev. Nov. (2011).
2) SAFE: Safe Automotive soFtware architEcture, http://www.safe-project.eu/ referenced (2014).
3) Blom, H., Lonn, H., Hagl, F., et al.: EAST-ADL: An Architecture Description Language for Automotive Software-Intensive Systems. EAST-ADL WhitePaper, Volume 1, (2013).
4) Kazman, R., Klein, M., and Clements, P.: ATAM: Method for Architecture Evaluation, Technical Report CMU/SEI-2000-TR-004, Software Engineering Institute, Carnegie–Mellon University, (2000).
5) Feiler, P. H., Gluch, D. P., and Hudak, J. J.: The Architecture Analysis and Design Language (AADL): An Introduction., Technical report, CMU/SEI-2006-TN-011, Software Engineering Institute, Carnegie–Mellon University, (2006).
6) Delange, J., Feiler, P., Gluch, D. P., and Hudak. J.: AADL Fault Modeling and Analysis within an ARP4761 Safety Assessment., Technical report, CMU/SEI-2014-TR-020, Software Engineering Institute, Carnegie–Mellon University, (2014).
7) Nelson, V.P.: Fault-tolerant computing: Fundamental concepts. IEEE Computer, 23(7):19-25, Jul (1990).
8) Armoush, A.: Design Patterns for Safety critical Embedded Systems, Ph.D. Thesis RWTH-Aachen, (2010).
9) Baleani, M., Ferrari, A., Mangeruca, L., et al.: Fault-tolerant platforms for automotive safety-critical applications, Proc. of the Intl. Conf. on Compilers, Architectures and Synthesis for Embedded Systems, pages 170–177. ACM Press, (2003).
10) Kletz, T. A.: Hazop & Hazan: Identifying and Assessing Process Industry Hazards，Taylor&Francis Group, (1999).
11) 小野寺 勝重: グローバルスタンダード時代における実践 FMEA 手法―品質管理と信頼性，保全性，安全性解析-，日科技連, (1998).