5J-05

人と協調する高度自動化システムの安全性要求分析方法の提案と先進運転支援システム(ADAS)への適用評価

松原　百映†　　青山　幹雄‡

南山大学大学院 理工学研究科 ソフトウェア工学専攻†　　南山大学 理工学部 ソフトウェア工学科‡

1.　はじめに

自動運転や自動ブレーキなどの高度自動化システム(Advanced Automated System, 以下 AAS と略記)は人と協調して高い安全性を実現することが求められている[2]．本稿では，拡張ユースケース分析とベイジアンネットワークを組み合わせた，人を含めた AAS の安全性要求の分析方法を提案し，先進運転支援システム(ADAS)へ適用してその有効性を評価する．

2.　研究課題

本稿では以下の 3 点を研究課題とする．

(1) 人と AAS が協調できるような安全性要求の適切なモデル化方法の提案
(2) (1)によるモデルを用いた安全性要求の定量的分析方法の提案
(3) 実システムを用いた提案方法の有効性の評価

3.　関連研究

(1)　ミスユースケース分析

従来のユースケース図にネガティブな要素を追加し，脅威と緩和の関係を表現する[1].

(2)　BN (Bayesian Network)

BN を応用することで複雑なシステムの障害診断や人間の行動をモデル化して予測ができる．

(3)　STPA (STAMP based Process Analysis)

システムの制御要素と被制御要素間の故障モデル STAMP(Systems-Theoretic Accident Model and Process)に基づくハザード分析方法である[3].

4.　アプローチ

人の挙動を「認知，判断，操作」から成るシステムとしてモデル化し，人間システムと呼ぶ．これと対応して，AAS の挙動は「Sensor, Controller, Actuator」でモデル化できる．この結果，人間システムと AAS との協調の構造を統一的にモデル化し，協調を含む安全性要求を分析するアプローチを取る(図 1).

5.　提案方法と例題への適用

提案する安全性要求分析プロセスは 1)拡張ユースケース分析と 2)BN による定量的評価の 2 つに分けられる(図 2)．1)では，分析対象システムについて人との協調をモデル化し，ハザードとそれに対する緩和策を特定する．緩和策の特定には安全性パターンを用いる．2)では，分析対象システムにおける事故発生までのシナリオを BN で表現し，作成された BN を用いて，分析対象システムの安全性を定量的に評価する．

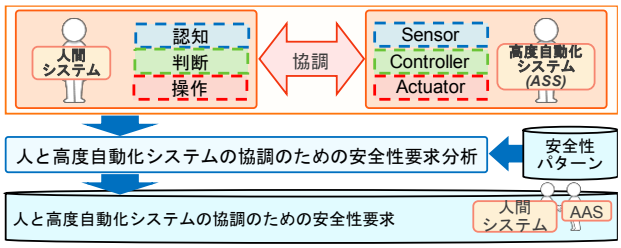

図 1 アプローチ

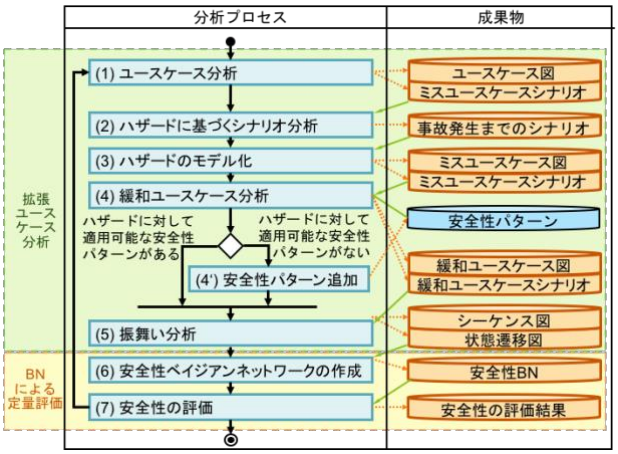

図 2 提案プロセス

6.　例題への適用

提案方法を実際の ADAS の一つである自動ブレーキシステム(Pre-Crash Safety system, 以下 PCS)[4]の仕様に適用し，そのプロセスを説明する．

(1)　ユースケース分析

人間システムと AAS に対してユースケース分析を行う．ユースケースは人間と AAS の挙動のコンテキスト(認知/Sensor, 判断/Controller, 操作/Actuator)に分割してパッケージとして表現する．

(2)　ハザードに基づくシナリオ分析

(1)で導出したユースケースを基にハザードとなるミスユースケースを特定し，それに基づき

A Safety Requirements Analysis Method for Cooperation of Human and Advanced Automation Systems and Its Evaluation with Advanced Driving Assistant Systems (ADAS)
†Moe Matsubara, Graduate School of Science and Engineering, Nanzan University.
‡ Mikio Aoyama, Department of Software Engineering, Nanzan University.

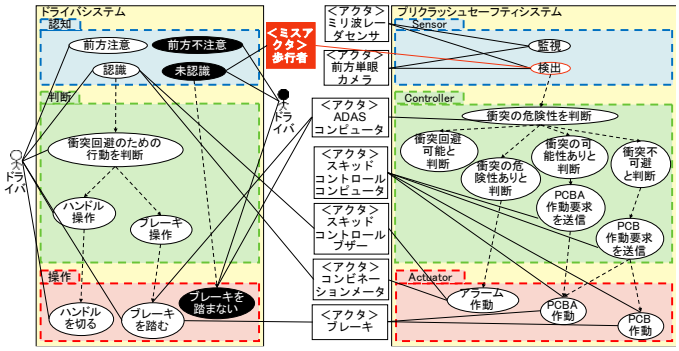

図 3 緩和ユースケース図

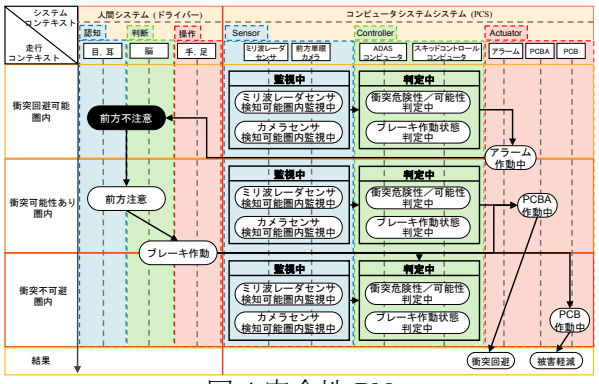

図 4 安全性 BN

事故発生までの想定シナリオを導出する(a), b)).

a) ドライバも PCS の前方単眼カメラも前方の歩行者を認識/検出せず，衝突回避支援制御も行われない.

b) ドライバは前方の歩行者を認識していないが，PCS の前方単眼カメラが歩行者を検出し，衝突回避支援制御を行う.

(3) ハザードのモデル化

(2)で導出したミスユースケースとそれにより安全性を脅かされ得るユースケースのハザード構造をモデル化する．次に，各ミスユースケースについてミスユースケースシナリオを記述し，ハザードに対する緩和ポイントを特定する(表 1).

表 1 ミスユースケース「未認識」のシナリオ

ミスユースケース名	未認識
アクタ／ミスアクタ	ドライバ，歩行者
概要	ドライバは，前方不注意により，前方に接近している歩行者を認識できない
事前条件	ドライバは前方不注意状態にある
基本シナリオ	ドライバは，歩行者が前方に接近していることを認識しない
結果	歩行者との衝突回避のために取るべき適切な操作の判断ができない
ステークホルダリスク	ドライバのリスク：歩行者と衝突 歩行者：自動車と衝突
ミスアクタ プロフィール	1) ドライバに悪意はない 2) 歩行者は接近する車両との衝突の危険性を認識していない
緩和ポイント	前方に接近していることを認識しない

(4) 緩和ユースケース分析

(3)で得られた緩和ポイントを基に，ハザードを緩和する機能としてユースケースを追加し，緩和ユースケース図(図 3)を作成する.

(5) 振舞い分析

緩和ユースケースのシナリオを基にシーケンス図を作成し，各システムの振舞いを時系列にシステムコンテキストに分割して分析する．さらに，シーケンス図からシステムの状態を特定し，システムの状態遷移図を構成する.

(6) 安全性ベイジアンネットワークの作成

状態遷移図の各状態をノードとした BN を作成する．各ノードには，人と AAS の障害発生確率に基づいて重み付き確率が付与される．安全性 BN は，横軸を人と AAS の挙動コンテキスト，縦軸を走行コンテキストとした 2 次元コンテキスト構造として表現する(図 4). 走行コンテキストは，人/AAS の障害物の認識を起点として衝突回避支援制御が終了するまでの走行に伴う安全性の推移を表す.

(7) 安全性の評価

(6)で作成した BN のノードに付与された重み付き確率を BN に沿って計算して事故発生確率を求め，人と協調する AAS の安全性を定量的に評価する.

7. 評価

人と AAS の挙動を対応づけてモデル化し，一つのシステムとして分析することで，人と AAS の協調のモデル化が可能となった．さらに，BN を用いることで，事故発生までのシナリオに沿った安全性の定量分析が可能になった.

8. 考察

本提案方法は UML を拡張して分析を行うため，先行研究の STPA[3]と比較して UML との親和性が高く，開発者にとって使用性が向上すると考えられる．また，人と AAS の挙動をモデル化したことにより，人と AAS との協調構造の統一的なモデル化が可能になった.

9. 今後の課題

今後の課題として次の 2 点を挙げる.

(1) 挙動の連続的変化に伴う安全性の定量分析

(2) リアルタイム制約の表現と分析方法の拡張

10. まとめ

本稿では，人と高度自動化システムの協調に焦点を当てて，拡張ユースケース分析と BN を組み合わせた，人を含めた高度自動化システムの安全性要求の定量的分析方法を提案した.

参考文献

[1] I. Alexander, Misuse Cases, IEEE Software, Vol. 20, No.1, Jan./Feb. 2003, pp. 58-66.
[2] 稲垣 敏之, 人と機械の共生のデザイン, 森北出版, 2010.
[3] N. G. Leveson, Engineering a Safer World, MIT Press, 2011.
[4] トヨタ自動車, プリウス電子技術マニュアル, 2016.