人と高度自動化システムの協調のため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

M2016SE006　松原　百映
指導教員　青山　幹雄

1 はじめに

高い知能性と自律性を兼ね備えた高度自動化システムの発展と普及に伴い，その安全性の保証が重要な課題となっている．自動運転や自動ブレーキなどの高度自動化システムは事故防止や運転負荷の軽減を目的としているが，事故を起こさないためには，人と高度自動化システムが協調して安全性を実現する必要がある．しかし，現状の安全性要求分析方法では高度自動化システムを対象としており，人との協調を含めた安全性要求の分析方法は体系化されていない．人と高度自動化システムとの協調を対象とする安全性要求分析方法の確立が必要である．

本稿では，人と高度自動化システムが協調して実現する安全性について，協調ユースケース分析と安全性ベイジアンネットワークによる，人を含めた高度自動化システムの安全性要求の分析方法を提案する．

2 研究課題

本稿では，人と高度自動化システムの安全性を脅かすリスクの緩和に必要な要求を安全性要求と定義し，その分析方法について以下の 4 点を研究課題とする．

(1) 人と高度自動化システムの協調構造のモデル化
(2) 協調構造モデルに基づいた安全性要求のモデル化
(3) 安全性要求の定量的分析
(4) 実システムを適用し提案方法の有効性の評価

3 関連研究

3.1 人と高度自動化システムの協調問題

高い知能と自律性を持つ機械が交通移動体の安全性，効率性，快適性に貢献している一方，人と高度自動化システムのミスマッチとも言える要因で様々な事故が起こっている．人と機械が自然な形で協調できるシステムの実現においては，人と高度自動化システムの関わり方を考慮したシステムの設計や形態が課題として挙げられている[6].

3.2 安全性／セキュリティ要求工学

セキュリティ要求工学ではシステムへの意図した攻撃に対して，安全性要求工学では合理的に予見可能なシステムの誤使用や機器の機能不全によって起こる事故に対して，リスクアセスメント，リスク対策を行う．

ここで，セキュリティ分析手法としてミスユースケース分析を，安全性要求分析手法として STAMP/STPA を挙げる．

(1) ミスユースケース分析

ミスユースケース図を用いて脅威の特定とその緩和方法を分析する．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[3].

(2) ユースケースマップ

システム規模の大粒度の振舞いパターンを説明して意味付けができる高次設計モデルである．動的な構造をユースケースマップのパスとして表現することで，システムの動的なシナリオを導出することができる[5].

(3) STAMP/STPA

STAMP(System-Theoretic Accident Model and Process)は，安全のための制御要素と被制御要素の相互作用が働かないことによって起きるアクシデントのモデルとして提唱された．このアクシデントモデルに基づくハザード要因の分析方法が STPA(STAMP based Process Analysis)である[1].

3.3 ベイジアンネットワーク (BN: Bayesian Network)

BN モデルは有向非巡回グラフで表され，各ノードは確率変数を表す．複数の確率変数間の依存関係をグラフ構造により表現し，条件付き確率により各変数間の定量的な依存関係を表す．BN は，情報量が限定されている場合の不確定状態の推定に利用でき，BN を応用することで障害診断を行うことができる[7].

4 アプローチ

人間の運転行動を「認識，判断，行動」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，高度自動化システムの振舞いは「Sensing, Control, Actuating」でモデル化できる．これにより，人間システムと高度自動化システム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)．また，高度自動化システムの安全性要求において，安全性のハザードはシステムの外部だけでなく内部にも存在することに着目して，安全性を脅かす外部要因と内部要因の両方を分析する方法を提案する．さらに，安全性を定量的に評価するために，BN を用いて事故発生確率を求めることで定量的評価を実現する[2].

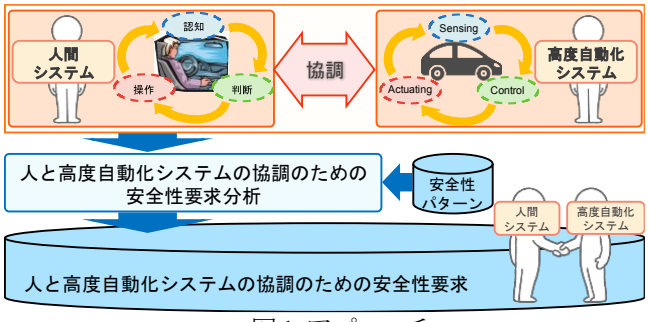

図 1 アプローチ

5 提案方法

提案する安全性要求分析プロセスは 1)協調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 2).

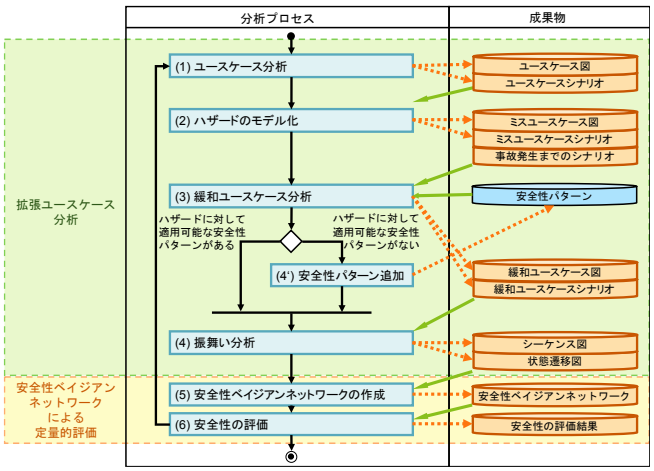

図 2 安全性要求分析プロセス

5.1 提案方法における主要な概念

5.1.1 協調構造のモデル化

本研究における協調とは，人間の運転行動を人間システムとして見なし，人間システムの「認知，判断，操作」と高度自動化システムの振舞いである「Sensing，Control，Actuating」が認知／Sensing，判断／Control，操作／Actuating として対応し，人間と高度自動化システムがそれぞれ安全性を満たすために必要な振舞いを行うことと定義する(図 3)．人間システムと高度自動化システムの協調は，協調的認識，協調的制御，協調的動作から成る(表 2).

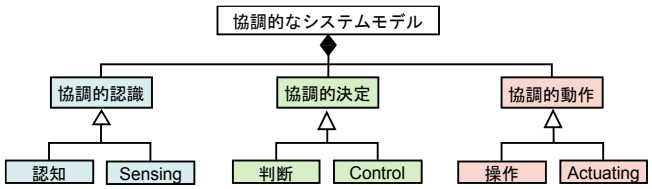

図 3 協調的なシステムモデル

表 2 協調的なシステムモデルにおける概念

概念	概要
協調的認識	認知 or Sensing により前方の障害物を認識する
協調的決定	判断 or Control により必要な振舞いを決定する
協調的動作	操作 or Actuating により決定された操作を行う

5.1.2 協調ユースケース分析

安全性に対するハザードはシステムの外部要因と内部要因の両方に着目し，従来のミスユースケース分析にシステムコンテキストとマルチアクタを導入した協調ユースケース分析を提案する．協調ユースケース分析では，人とシステムに対する安全性について外部要因と内部要因の両方からのハザードと，その緩和方法を特定する．

(1) システムコンテキストとオペレーションコンテキスト

組込みシステムアーキテクチャパターンとして SCA (Sensor-Controller-Actuator)アーキテクチャパターンが提案されている．このアーキテクチャパターンに基づき，ユースケースを認識／Sensing，判断／Control，行動／Actuating の 3 層のコンテキストに分割してパッケージとして表現する．本稿ではこれをシステムコンテキストと呼ぶ．

また，システムが稼動している間は，その稼動中の環境や時間変化によってシステムの稼働状態が変化する．したがって，システム稼働中に変化するコンテキストをオペレーションコンテキストとする．これらのコンテキストによって組込みシステムの安全性の構造的な分析を可能とする．

(2) マルチアクタ

自動車の安全性要求の特徴により，安全性のミスユースケース分析では，同一アクタが本来の役割だけでなくミスアクタの役割も果たすことがあるという特徴がある．このように，同一アクタでありながら異なる役割を持つアクタを，本稿ではマルチアクタと定義する．

(3) 緩和ユースケース

ハザードに対する緩和策として使われるユースケースを，本研究では緩和ユースケースと呼ぶ．また，これに伴い，緩和ユースケースを用いたユースケース図を緩和ユースケース図，緩和ユースケースについて記述するシナリオを緩和ユースケースシナリオと呼ぶ．

5.1.3 安全性ベイジアンネットワーク

協調ユースケース分析で導出されるシステムの状態をノードと見なし，ハザードの認識を起点とした事故発生までのシナリオに基づいた BN を作成する．

5.1.4 協調的振舞いの分析マトリクス

安全性 BN を作成するために，縦軸をシステムコンテキスト，横軸をオペレーションコンテキストとした 2 次元のコンテキスト構造上に協調的振舞を表現する．本稿では，この 2 次元コンテキスト構造を協調マトリクスと呼ぶ(図 4). 協調マトリクスを用いることにより，システムコンテキストとオペレーションコンテキストの両コンテキストの変化に対応した安全性 BN の表現が可能になる．

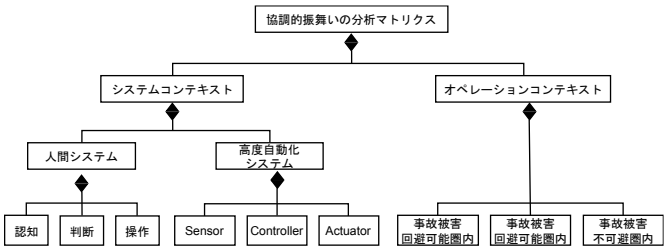

図 4 協調マトリクスのメタモデル

5.2 安全性要求メタモデル

安全性要求メタモデルを図 5 に示す．

ミスユースケースと緩和ユースケースはユースケースのサブクラスであり，緩和ユースケースはミスユースケースと関連している．安全性パターンは，システムの故障の原因や問題，対策を一般化したものであり，ミスユースケースシナリオから緩和ポイントを抽出する際に必要となる．また，安全性パターンによって，緩和ユースケースシナリオにおける緩和策を特定できる．

6 実システムへの適用

6.1 適用対象システム

本提案方法を実際の自動車の衝突防止ブレーキシステ

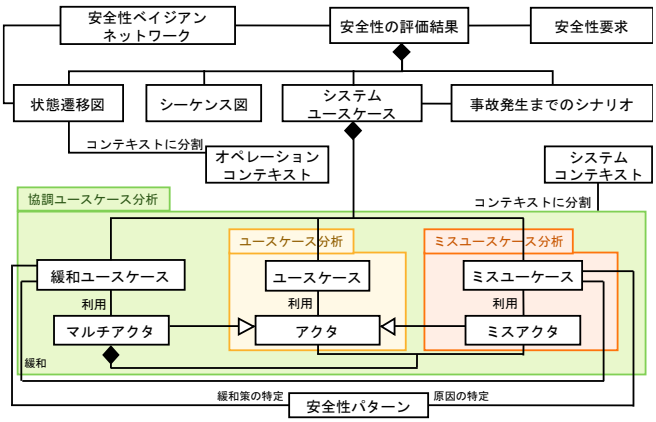

図 5 安全性要求メタモデル

ムであるプリクラッシュセーフティシステム(PCS: Pre-Crash Safety system)[9]の仕様に適用した例を用いて説明する．本システムはミリ波レーダセンサと前方監視カメラからの検知情報とドライバによるブレーキ操作状態を入力として制御を行い，衝突回避あるいは被害軽減のために必要に応じてブレーキアシストあるいは自動ブレーキを作動する．

6.1.1 PCS への適用

(1) ユースケース分析

PCS について，PCS の振舞いに影響を与え得る人として，ドライバも人間システムと見なし，ドライバも含めた分析を行った．また，ユースケースマップを用いてシステムの実行シナリオを作成した．

(2) ハザードのモデル化

PCS についてミスユースケース図を作成した．(1)と同様にユースケースマップを用いて，ミスユースケースも含めたシステムの実行シナリオを作成した．このユースケースマップを基に，例として，事故発生までの次の 2 つのシナリオを得た．

a) ドライバは，PCS のセンサが検知する前に前方の歩行者を認知し，衝突回避のために必要な操作を行う．

b) ドライバは前方の歩行者を認知していないが，PCS のミリ波センサと前方監視カメラが前方の歩行者を検出し，衝突回避支援制御を行う．

(3) 緩和ユースケース分析

(2)で得られた緩和ポイントを基に，緩和ユースケースを追加し，緩和ユースケースを基に緩和ユースケースシナリオを作成した(図 6)．例として，シナリオ a)を青色線で，シナリオ b)を朱色線のユースケースマップで示す(図 6)．

(4) 振舞い分析

(3)で作成したユースケース図を基に，システムの振舞いについてシーケンス図を作成した(図 7)．次に，特定された状態から PCS の状態遷移図を構成した(図 8)．状態遷移図はオペレーションコンテキストに分けて作成した．本稿では例題として ADAS を用いているため，オペレーションコンテキストを走行コンテキストと呼ぶ．

(5) 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 を協調マトリクス上に構成した(図 9)．

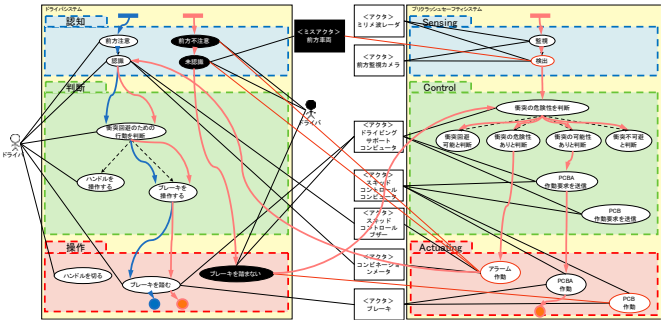

図 6 PCS の緩和ユースケース図と
シナリオ a), b)のユースケースマップ

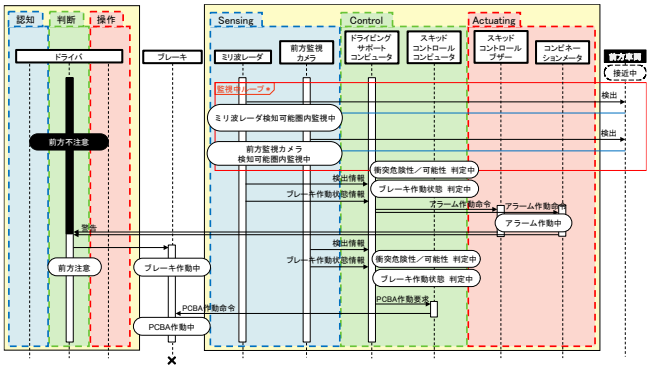

図 7 シナリオ b)のシーケンス図

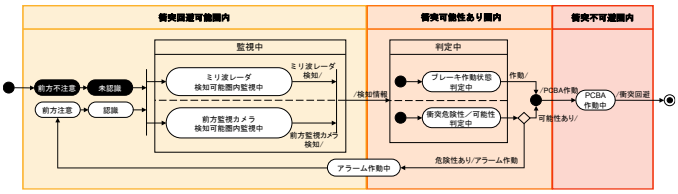

図 8 シナリオ b)の状態遷移図

(6) 安全性の定量的評価

(5)で作成した BN はコンテキストに応じで変化するので，ノードに付与される重み付き確率もそれに応じて変化する．本稿では重み付き確率の付与を行っていないため，具体的な数値を用いた評価はしていない．

7 評価

7.1 人と高度自動化システムが協調できるような安全性要求のモデル化

人の運転行動である「認知，判断，操作」と高度自動化システム「Sensor, Controller, Actuator」の振舞い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，人と高度自動化システムの協調のモデル化が可能となった．

また，協調をシステムコンテキストだけでなくオペレーションコンテキストにも対応させて表現することにより，コンテキストの変化に応じた分析が容易になった．

7.2 安全性要求モデルを用いた安全性要求の定量的分析

安全性要求の分析方法に BN を用いて事故発生までのシナリオに沿った事故発生確率を求めて安全性を定量的に評価することで，安全性要求を定量的に定義可能となった．これにより，安全性要求の定量的評価が可能になったことが示された．

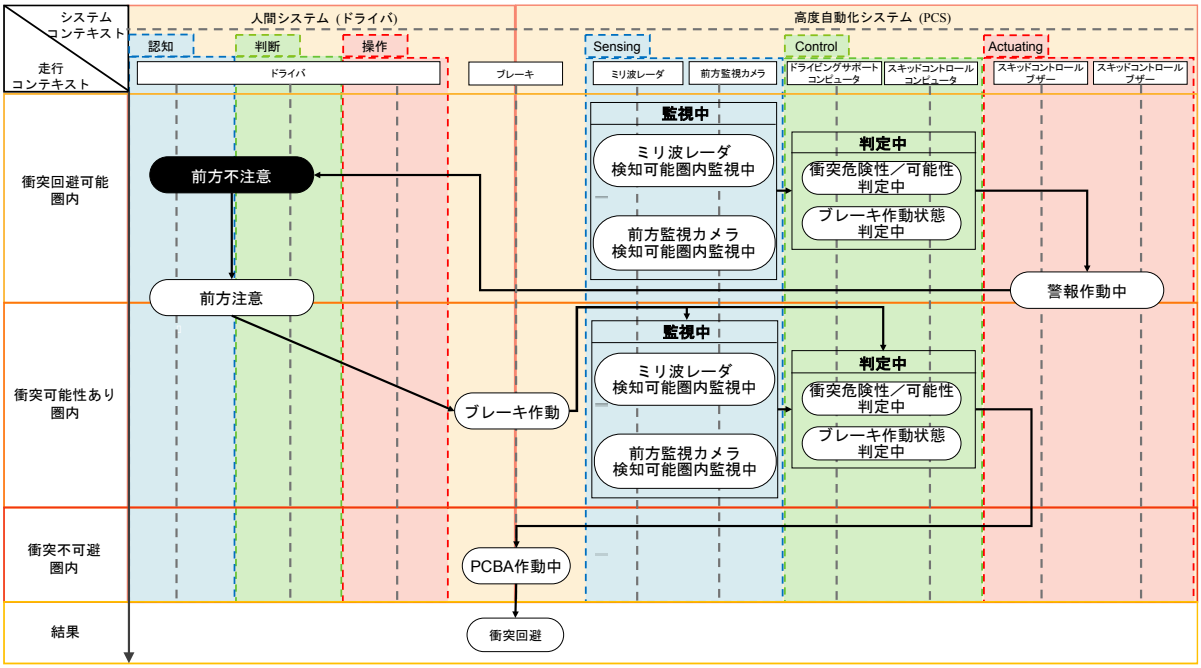

図 9 安全性ベイジアンネットワーク

7.3 実システムを用いた提案方法の有効性の評価

本提案方法を実際の ADAS の PCS に適用した．本稿では，走行コンテキストの変化に応じた PCS の安全性を定量的に評価した．提案方法では，ユースケース／ミスユースケースを要求として，それに基づき BN を生成した．BN 内のいくつかのノードはコンテキストの変化に応じて連続的に変化するので，ノードの重み付け確率もそれに応じて変化する．しかし，本研究において，連続的に変化するノードの確率の重み付け方法については議論していないため，具体的な数値を用いた評価をするまでには至っていない．

8 考察

8.1 STPA との比較

STPA では分析にあたり独自モデルを作成するため，開発者は新しくモデルを覚える必要があり学習コストが高いという問題が挙げられる．しかし，本研究では UML を用いてモデル化を行うため，開発者にとって学習が容易で，さらに，理解容易性が向上すると考えられる．

8.2 ユースケース分析の拡張の有効性

従来のミスユースケース分析にマルチアクタを導入することで，システムに対するハザードについて，外部要因と内部要因の両方によるハザードも特定可能になった．これにより，自動車の安全性の特徴に対応したミスユースケース分析を行うことが可能になった．

8.3 BN の有用性とコンテキストに依存する安全性の分析

従来のミスユースケース分析では機能の分析を行うため，定性的な要求分析であったが，BN を適用することで，安全性の向上を定量的に評価可能になった．

9 今後の課題

9.1 コンテキストの連続的変化に伴う定量的安全性分析

コンテキストの連続的変化に関わるノードの重み付き確率の評価方法あるいはコンテキストの連続的変化に対応するシナリオに沿った確率評価が必要である．

9.2 リアルタイム制約の表現と分析方法の拡張

組込みシステムの安全性要求分析では，振舞いのリアルタイム性も考慮する必要がある．本稿のモデルに対しタイミング制約を表現できる拡張とそれに基づくリアルタイム安全性分析を可能とする必要がある．

10 まとめ

本稿では，協調ユースケース分析と BN を組み合わせた，人と高度自動化システムの協調モデルに基づく，安全性要求分析方法を提案した．本提案方法を実際の ADAS に適用し，有効性を評価した．本提案方法では，人の振舞いをシステムとしてモデル化し，高度自動化システムとの協調に基づいたハザードを分析している．これにより，人の振舞いと高度自動化システムの振舞いを同じ抽象レベルで構造的に安全性を分析することが可能となった．また，提案方法は UML の拡張となっていることから，開発者にとって親和性が高く，導入と利用が容易であると言える．

参考文献

[1] A. Abdulk, et al., A Comprehensive Safety Engineering Approach for Software-Intensive Systems based on STPA, Procedia Engineering, Vol. 128, Dec. 2015, pp. 2-11.
[2] R. Adla, et al., Bayesian Network Based Collision Avoidance Systems, IEEE EIT, May 2015, pp. 605-610.
[3] I. Alexander, Misuse Cases, IEEE Software, Vol. 20, No. 1, Jan./Feb. 2003, pp. 58-66.
[4] K. Beckers, Pattern and Security Requirements, Springer, 2015.
[5] R. J. A. Buhr and R. S. Casselman, Use Case Maps for Object-Oriented Systems, Prentice Hall, 1996.
[6] 稲垣 敏之，人と機械の協調における安全と安心，日本交通科学協議会誌，Vol. 9, No. 1, 2010 年 11 月, pp. 11-20.
[7] 本村 陽一，岩崎 弘利，ベイジアンネットワーク技術，東京電機大学出版局，2006.
[8] A. Reschka, Safety Concept for Autonomous Vehicles, M. Maurer, et al.(eds.), Autonomous Driving, Springer, 2016, pp. 473-496.
[9] トヨタ自動車，CROWN MAJESTA 電子技術マニュアル，2015.
[10] W. Wachenfeld, et al., Use Case for Autonomous Driving, M. Maurer, et al.(eds.), Autonomous Driving, Springer, 2016, pp. 9-37.