Vol.2018-SE-198 No.6
2018/3/9

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[†1]　青山 幹雄[†2]

概要：自動運転や自動ブレーキなどの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．しかし，安全性を確保するためには，人と高度自動化システムの協調における安全性を保障する必要がある．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，UML のユースケース分析を拡張して，人と高度自動化システムの協調構造のモデル化とそれに基づいた安全性要求のモデル化方法を提案する．さらに，モデル化された安全性要求をベイジアンネットワーク上でシナリオごとに定量的に評価する方法を提案する．本提案方法を実際の先進運転支援システム(ADAS)へ適用し，提案方法の有効性を示す．

キーワード：安全性要求，要求分析，ユースケース分析，ベイジアンネットワーク，先進運転支援システム(ADAS)

A Safety Requirements Analysis Method Based on Cooperation Model of Human and Advanced Automation Systems and Its Evaluation with Advanced Driving Assistant Systems (ADAS)

MOE MATSUBARA[†1]　MIKIO AOYAMA[†2]

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．例えば，自動車には自動運転や自動ブレーキシステムなどの先進運転支援システム(ADAS: Advanced Driving Assistant System)が搭載されるようになった．また，産業協調ロボットや家庭用協調ロボットも普及し始めている[8, 11]．高度自動化システムは事故防止や運転負荷の軽減，効率性や快適性の向上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，高度自動化システムの導入により，2 つの問題が引き起こされる．1 つ目の問題は，高度自動化システム全体の複雑さの増大である．2 つ目の問題は，人と高度自動化システムとの間の相互作用の複雑さの増大である．特に人と高度自動化システム間の相互作用の問題は，人と高度自動化システムの間での権限移譲の問題や，高度自動化システムに対する人の信頼（過信，不信）に関わる問題など[10]，高度自動化システム側のみの要因に限らず，ヒューマンエラーや[3][10]，人と高度自動化システムとの間の協調が問題となる[10].

このことから，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，問題として挙げられる人と高度自動化システムの間の相互作用の複雑さに起因する事故を回避し高い安全性を満たすシステム設計を可能にするための安全性要求分析の体系化を目的として，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方法の提案
(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

†1 南山大学大学院 理工学研究科 ソフトウェア工学専攻
Graduate Program of Software Engineering, Nanzan University
†2 南山大学 理工学部 ソフトウェア工学科
Dep. of Software Engineering, Nanzan University

ステムの設計や形態が課題として挙げられている[10].

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とそれに関連したユースケースマップを，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[4].

(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[7].

(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アクシデントモデルとして提唱されたモデルである．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, 13].

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[2, 14].

4. アプローチ

人間の運転行動が「認知，判断，操作」で成り立っているのに対し，高度自動化システムの振舞いは，組込みシステムアーキテクチャパターンとして提案されている SCA(Sensor-Controller-Actuator)アーキテクチャパターンに基づくと，「Sensing，Control，Actuating」によって決まる[15]．このことから，人間の運転行動もひとつのシステムと見なすとすると，人間システムと高度自動化システムはそれぞれ，認知と Sensing，判断と Control，操作と Actuating で対応すると考えられる．これらに着目して，人間の運転行動を「認知，判断，操作」から成るシステムとしてモデル化した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挙動は「Sensing，Control，Actuating」でモデル化できる．この結果，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．ここで，本稿における「協調」とは，安全性を実現するために人と高度自動化システムが互いの振舞いや状態に応じて必要な動作をすることを言う(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, 16, 20].

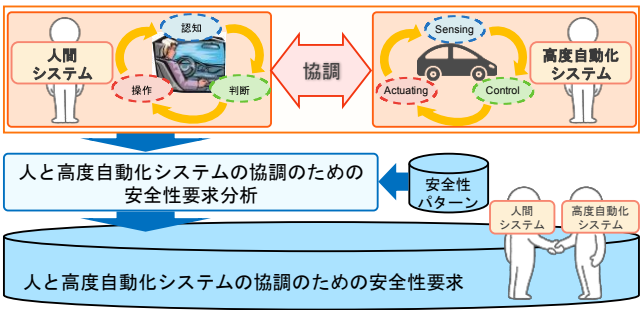

図 1 アプローチ

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)安全性 BN による定量的評価の大きく 2 つに分けられる(図 2).

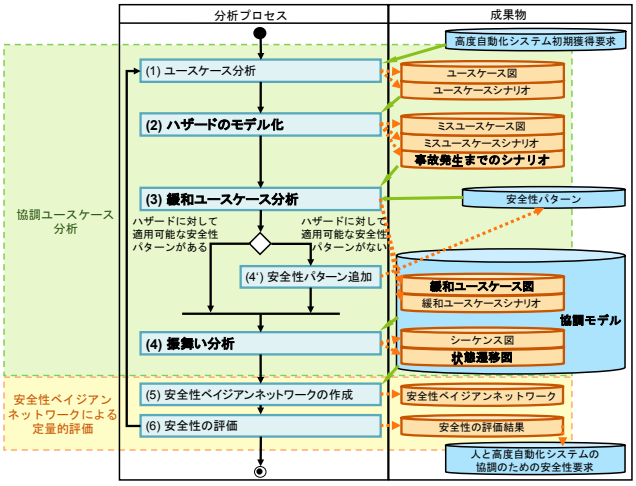

図 2 安全性要求分析プロセス

1)では，分析対象システムに対して，人間と高度自動化システムのそれぞれに必要な機能と，その機能によってどんな相互作用が起こるかを明確にするために協調ユースケース分析を行い，協調関係をモデル化する．また，ここで事故に至るまでのシナリオも導出する．

2)では，協調ユースケース分析で導出されたモデルに基づいて，事故に至るまでのシナリオごとの安全性を定量的

に求める．定量評価を行うためには，高度自動化システムと人間システムの振舞いをグラフモデル化する必要がある．ここで，人間システムすなわち人の行動は非決定的で不確実なため，不確実性を含む事象の予測をモデル化できるBN を用いて，シナリオに沿った振舞いをモデル化する．

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

人間の運転行動は「認知，判断，操作」で決まるのに対して，高度自動化システムの振舞いは「Sensing，Control，Actuating」で決まることから，人間も高度自動化システムも，「状況を認識」し，「その状況に対して必要な動作を決定」し，「決定した動作を実行」するという一連の流れが共通であることがわかる．このことから，人間の運転行動を人間システムと見なしたとき，人間システムは高度自動化システムと同様にモデル化できる．さらに，人間システムと高度自動化システムは，認知と Sensing，判断と Control，操作と Actuating がそれぞれ共通の振舞いをする協調構造であるとして統一的にモデル化できると考えられる．

そこで，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 で対応し，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)．

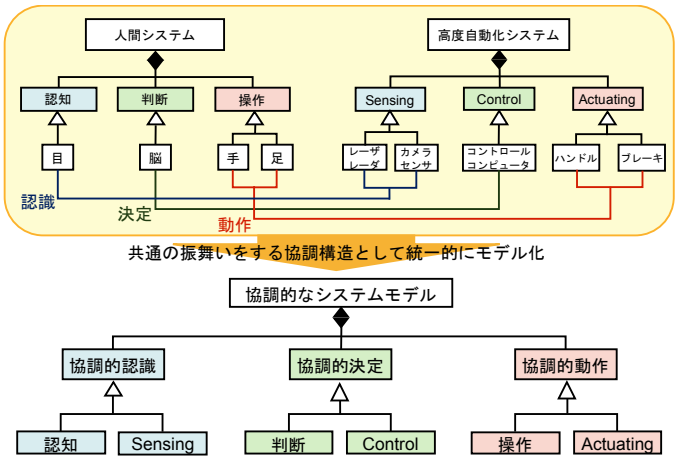

図 3 協調的なシステムモデル

表 1 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

本稿では，人間システムと高度自動システムの協調に必要なユースケースを協調ユースケースと定義し，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，安全性に対するハザードについて，システムの外部要因と内部要因の両方に着目し，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

人間システムの「認知，判断，操作」と高度自動化システムの「Sensing, Control, Actuating」それぞれをシステムコンテキストとして定義する．

システムテキストは，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．

また，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定義する．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，オペレーションコンテキストに基づいた分析を行うこと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，同一アクタでありながら異なる役割を持つアクタをマルチアクタと定義する．

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．これをマルチアクタとして表現することで，協調ユースケース分析の際に，システムに対するハザードの内部要因も表現可能になる．

(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 を作成する際，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．

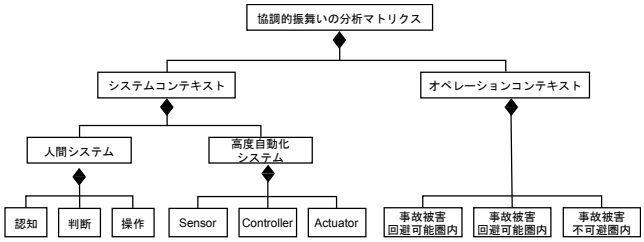

図 4 協調マトリクスのメタモデル

5.1.5 安全性パターン

(1) 安全性パターンの定義

セキュリティパターン[6]を応用し，システムに問題が起きたときを想定して，原因と対策をパターン化し，記述したものを安全性パターンとして定義する．

本稿で提案する安全性パターンは，名前，原因，問題，対策，結果の 5 項目を記述する(表 2).

表 2 安全性パターンの記述

記述項目	概要
名前	システムの不具合の名称または概要
原因	不具合が起きる原因
問題	不具合により起こる問題
対策	問題の解決方法や緩和策
結果	対策により得られる結果

(2) 安全性パターンの効果

安全性パターンを定義することによって，システムの不具合によって起こる問題やその原因と，問題に対する緩和策を対応づけて記述することができ，ミスユースケース分析で導出される緩和ポイントに対する緩和策の特定が容易となる．ただし，本研究では安全性パターンは事前に作成されている前提で分析を行う．

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.

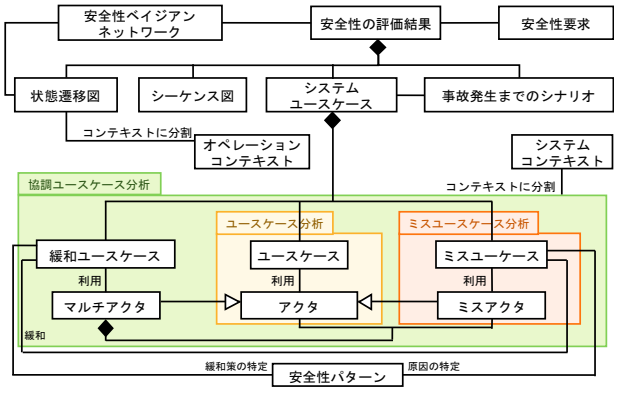

図 5 安全性要求メタモデル

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 ADAS 実用化の現状

ADAS は，自動車の安全性向上を目的とした安全運転支援システムである．例として，衝突被害軽減ブレーキ(自動ブレーキ)や車線維持支援システム，車間距離維持制御システムなどが挙げられる．

近年，ADAS は急速な発展を遂げ，現在レベル 2 まで実現されている(表 3)．これに伴って ADAS の普及率も高くなり，現在では多くの自動車に搭載されるようになった．これにより，運転における安全性や利便性が向上している一方で，ドライバのシステムへの過信や無責任な運転による事故も多発している．これは，ドライバがシステムの機能の限界や注意点を正しく理解できていないためである．現在実用化されている ADAS はあくまで「運転支援システム」であり，「完全自動運転」ではない．したがって，事故を起こさないためには，ドライバが責任を持って運転操作を行い，時にはドライバと ADAS が協調して安全を確保しなければならない[12].

情報提供型の自動車の運転制御主体がドライバのみであるのに対し，自動制御活用型の運転制御主体はドライバもしくはシステムである．特に，レベル 1 からレベル 3 はドライバとシステムの協調制御が行われる．したがって，本研究はレベル 1 からレベル 3 を研究対象とする．

表 3 安全運転支援システム・自律走行システムの定義[12]

<table>
<tr><th colspan="2">分類</th><th>概要</th><th>制御主体</th><th colspan="2">実現するシステム</th></tr>
<tr><td colspan="2">情報提供型</td><td>ドライバへの注意喚起等</td><td>ドライバのみ</td><td colspan="2" rowspan="2">安全運転支援システム</td></tr>
<tr><td rowspan="4">自動制御活用型</td><td>レベル 1
単独型
(人間中心の協調)</td><td>加速・操舵・制動のいずれかの操作をシステムが行う状態</td><td>ドライバ中心</td></tr>
<tr><td>レベル 2
システムの複合化
(人間中心の協調)</td><td>加速・操舵・制動のうち複数の操作を一度にシステムが行う状態</td><td>ドライバ中心
●監視義務およびいつでも安全運転できる状態</td><td rowspan="2">準自動走行システム</td><td rowspan="3">自動走行システム</td></tr>
<tr><td>レベル 3
システムの高度化
(システム中心の協調)</td><td>加速・操舵・制動を全てシステムが行い，システムが要請したときのみドライバが対応する状態</td><td>システム中心
(自動走行モード中)
●特定の交通環境下での自動走行(自動走行モード)
●監視業務なし(自動走行モード：システム要請前)</td></tr>
<tr><td>レベル 4
完全自動走行</td><td>加速・操舵・制動を全てシステムが行い，ドライバが全く関与しない状態</td><td>システムのみ
●全ての工程での自動走行</td><td>完全自動走行システム</td></tr>
</table>

6.2 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)[17, 18, 19]の仕様に適用した例を用いて説明する．

PCS は 1)ミリメータウェーブレーダセンサあるいはレーザレーダとフォワードレコグニションカメラからの検知情報と 2)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．

PCS に搭載されるミリメータウェーブレーダセンサ(ミリ波レーダ)，レーザレーダ(赤外線センサ)，フォワードレコグニションカメラ(単眼カメラ)は，センサによってそれぞれ性能が異なる(表 4，図 6)．

PCS は，センサが前方の障害物を検出した時点を起点として，自車と障害物との距離や自車のスピードから衝突の可能性を判断し，その可能性に応じて，次のような，衝突回避に必要な制御を行う(図 7)．

(1) 衝突の危険があると判断すると，ブザーとディスプレイでドライバに衝突の危険を警告する．
(2) 警告を受けたドライバがブレーキを踏んだ場合でも，PCS が衝突の可能性があると判断した場合は，プリクラッシュブレーキアシストが作動し，ブレーキの制動力を大きくする．
(3) 警告を受けたドライバがブレーキを踏めないなどして，PCS が衝突回避不可と判断した場合は，プリクラッシュブレーキを作動し，衝突回避もしくは衝突時の被害軽減を促す．

プリクラッシュブレーキアシストの作動時に注目すると，ドライバのブレーキ操作と PCS のプリクラッシュブレーキアシストによって衝突回避制御を行う部分に協調関係があることがわかる．これに着目しながら本提案方法による分析を行う．

表 4 ADAS／自動運転向けセンサの種類と性能[9]

	ミリ波レーダ (77GHz)	カメラ (単眼カメラ)	赤外線レーザ (レーザレーダ)
検知範囲	＜250m	＜140m	＜20m

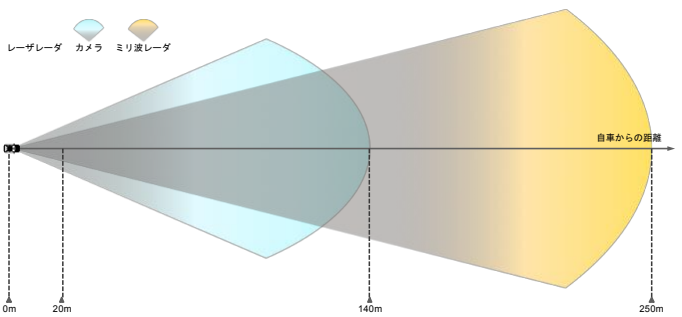

図 6 各センサの検知距離イメージ

図 7 ドライバと PCS の協調イメージ

6.3 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．本例題では，ドライバは衝突回避のための行動としてハンドル操作かブレーキ操作のいずれかを行うものとする．また，ユースケースマップを用いてシステム全体の動的シナリオを導出した．

(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．ここで，マルチアクタに着目して，システムの内部で与えられるハザード要因を特定し，モデル化した．さらに，(1)と同様にユースケースマップを用いて，ハザード要因を含む動的シナリオを導出した．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 のミリメータウェーブレーダセンサとフォワードレコグニション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．

また，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，基本シナリオに安全性パターンを対応して緩和ポイント「前方不注意」を特定した(表 5)．

表 5 「前方不注意」のミスユースケースシナリオ

＜ミスユースケースシナリオ＞	
ミスユースケース名	前方不注意
アクタ／ミスアクタ	ドライバ
概要	ドライバが前方不注意状態のため，前方に歩行者や車両が接近した場合，それらを認識できない恐れがある．
事前条件	なし
基本シナリオ	ドライバは何らかの理由により前方不注意状態にある．
結果	ドライバは，前方の歩行者もしくは車両を認識しない
ステークホルダリスク	ドライバ：歩行者もしくは車両と衝突，怪我 歩行者：車両と衝突，怪我 前方車両：後続車からの追突，前方車両への玉突き事故，怪我
ミスアクタプロフィール	ドライバの前方不注意は故意ではない

(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(表 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, 7).

表 6 緩和ユースケースシナリオ

＜緩和ユースケースシナリオ＞	
緩和ユースケース名	監視
アクタ	カメラセンサ，障害物
概要	カメラセンサは前方を監視し，障害物を検出した場合は，PSC に検出情報を送信する
事前条件	カメラセンサが正常に機能している
基本シナリオ	1) カメラセンサは車両情報を映像により監視している 2) カメラセンサは取得した映像データを PSC に送信する
結果	PSC はカメラセンサから取得した映像データを解析し，車両前方に障害物があるかどうかを判断する

(4) 振舞い分析

(3)で作成したユースケース図を基に，ドライバとシステムの振舞いについてシーケンス図を作成した(図 8, 9). これによって，ハザード要因に対する緩和ポイントとその緩和策の順序付けを明確にした．次に，特定された状態から PCS の状態遷移図を構成した(図 10, 11). 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 12, 13). 本例題では，自動車が走行中のベイジアンネットワークを作成するため，横軸のオペレーションコンテキストを「走行コンテキスト」とする.

(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

(1) 人と高度自動化システムの協調のモデル化

コンテキストに分けて表現することで，安全性の構造的な分析が可能になった．協調をモデル化したことで，どんな必要な協調の分析が容易になった．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「Sensing, Control, Actuating」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.

(2) マルチアクタの有効性

ミスユースケース分析を用いた安全性要求の分析では，同一のアクタが本来のアクタとしての役割とミスアクタとしての役割を持つという特徴があった．これをマルチアクタと定義したことにより，同一アクタの異なる役割を表現することが可能となった．また，ミスユースケース分析に加えてシーケンス図に対してもマルチアクタを導入したことで，振舞いの条件分析の表現が可能になった.

7.2 安全性要求モデルを用いた安全要求の定量的分析

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.

また，ベイジアンネットワークを協調マトリクス上に構成することにより，システムの振舞いを決めるコンテキスト(システムコンテキスト)とシステム稼働中のコンテキスト(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応じたベイジアンネットワークの構成が可能になった．これによって，コンテキストの変化に伴ってノードの重み付き確率が連続的に変化するベイジアンネットワーク表現が可能になった.

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を重み付けする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はできていない.

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手を付けにく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，開発者にとって手を付けやすく，さらに，理解容易性が向上すると考えられる.

STPA の STEP2 では, UCA に至るまでのハザードシナリオに基づいて HCF を特定する．それに対し，本提案方法では, 事故発生までのシナリオに基づいてハザードを特定し，ハザードとそれによって安全性が脅かされる機能をミスユースケース図で表現し，ハザードを緩和するための緩和ユ

ースケースを特定する．ハザードと緩和策の関係をミスユースケースで表現することにより，システムに対するハザードを特定するだけでなく，一つのハザードによって影響を受け得る機能の範囲も表現できるようになるため，構造的な安全性の分析が可能になる．また，本提案方法はシステム動作中のコンテキストに基づいた分析を行うため，システム動作中の時間変化や環境変化に対応した安全性の分析が可能になった．STPA ではコンテキストに基づいた分析は行われていないため，本提案方法におけるコンテキストに分割した協調のモデル化は，人が関わる高度自動化システムの安全性分析に有効的であると考えられる．

8.2 ユースケース分析の拡張の有効性

(1) 従来のミスユースケース分析との比較

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．

(2) セキュリティへの応用

セキュリティにおける従来のミスユースケース分析では，外部要因による脅威が分析されていたが，本提案方法を応用すると，システムのユーザによる情報漏洩などの，内部要因によるシステムのセキュリティ要求分析が可能になる．

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．自動緊急ブレーキシステムの作動は，ミリ波レーダセンサやカメラセンサのレーダの範囲に依存するため，自車と障害物との相対距離やシステムを作動させるタイミングが重要になる．ここでベイジアンネットワークを用いることにより．相対距離やタイミングのように自動車の走行に伴うコンテキストの変化に応じて変化する安全性の評価が可能となった．このように，従来のミスユースケース分析にベイジアンネットワークを組み合わせることで，定性的であった安全性要求に加え，時間や環境といったコンテキストに依存した安全性要求も定量的に分析可能となった点で，提案方法は安全性要求の新たな分析方法を提供できると言える．また，このようなコンテキストに依存する安全性の性質は，セキュリティ要求にはない新しい非機能要求の概念である．

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，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] 赤松 幹之，北崎 智之，人と自動運転システムとのインタラクションにおけるヒューマンファクタの課題，自動車技術, Vol. 69, No. 12, 2015，pp. 66-72.
[4] I. Alexander, Misuse Cases, IEEE Software, Vol. 20, No. 1, Jan./Feb. 2003, pp. 58-66.
[5] E. Ohn-Bar and M. M. Trivedi, Looking at Human in Age of Self-Driving and Highly Automated Vehicles, IEEE Trans. on Intelligent Vehicles, Vol. 1, No. 1, Mar. 2016, pp. 90-104.
[6] K. Beckers, Pattern and Security Requirements, Springer, 2015.
[7] R. J. A. Buhr and R. S. Casselman, Use Case Maps for Object-Oriented Systems, Prentice Hall, 1996.
[8] J. Guiochet, et al., Safety-Critical Advanced Robots: A Survey, Robotics and Autonomous Systems, Elsevier, Vol. 94, Aug. 2017, pp. 43-52.
[9] 池山 智也，自動運転に向けたセンサの開発動向と展望，自動車技術，Vol. 71, No. 2, Feb. 2017, pp. 13-17.
[10] 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, Nov. 2010, pp. 11-20.
[11] A. Khalid, et al., Safety Requirements in Collaborative Human Robot Cyber Physical System, M. Freitag, et al.(eds.), Dynamics in Logistics, Springer, 2017, pp. 41-51.
[12] 国土交通省自動車局，現在実用化されている「自動運転」機能は、完全な自動運転ではありません！，2017 年 4 月 14 日，http://www.mlit.go.jp/report/press/jidosha07_hh_000244.html
[13] N. G. Leveson, Engineering a Safer World, MIT Press, 2011.
[14] 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.
[15] B. Reimer, et al., Behavioral Impact of Drivers' Roles in Automated Driving, Proc. of the 8th International conference on AutomotiveUI'16, Oct. 2016.
[16] A. Reschka, Safety Concept for Autonomous Vehicles, M. Maurer, et al.(eds.), Autonomous Driving, Springer, 2016, pp. 473-496.
[17] トヨタ自動車，CROWN MAJESTA 電子技術マニュアル，2015.
[18] トヨタ自動車，PRIUS 電子技術マニュアル，2016.
[19] トヨタ自動車，AQUA 電子技術マニュアル，2017.
[20] W. Wachenfeld, et al., Use Case for Autonomous Driving, M. Maurer, et al.(eds.), Autonomous Driving, Springer, 2016, pp. 9-37.

シナリオ a) における分析プロセスの成果物

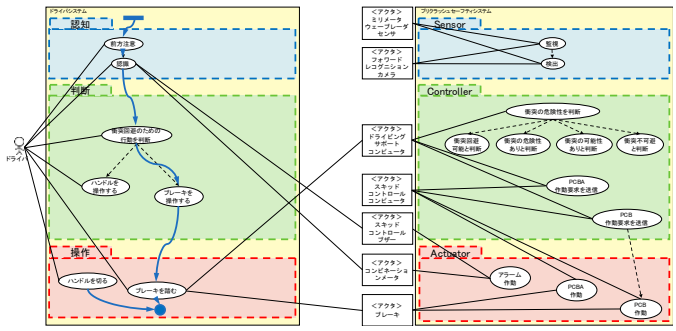

図 6 PCS の緩和ユースケース図とシナリオ a)の
ユースケースマップ

シナリオ b) における分析プロセスの成果物

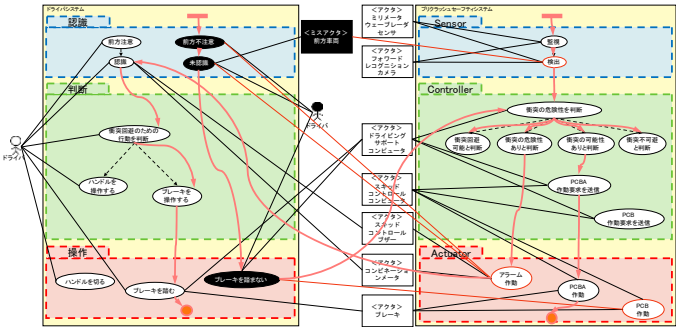

図 7 PCS の緩和ユースケース図とシナリオ b)の
ユースケースマップ

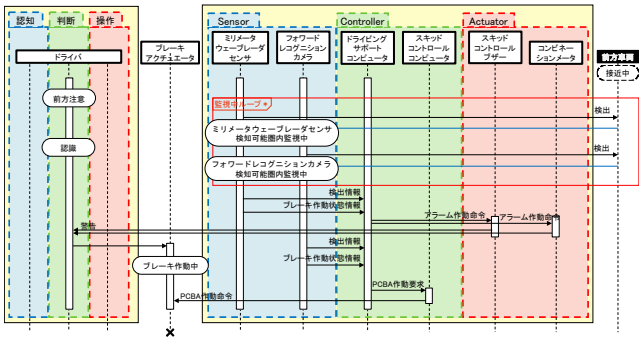

図 8 シナリオ a)のシーケンス図

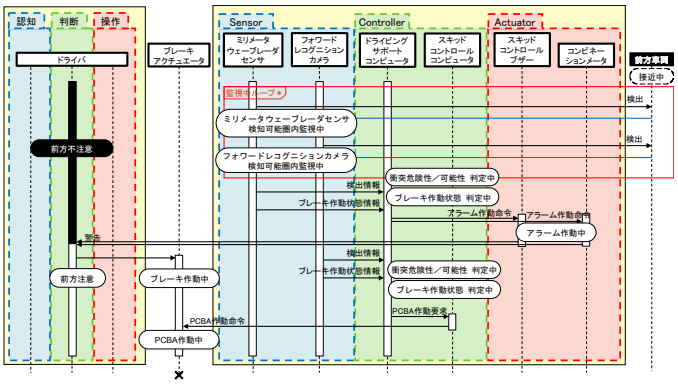

図 9 シナリオ b)のシーケンス図

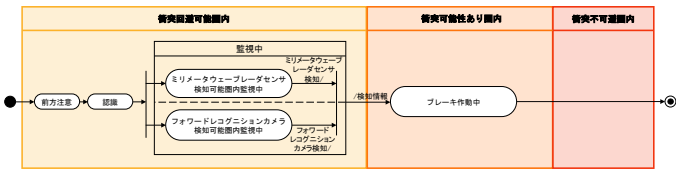

図 810 シナリオ a)の状態遷移図

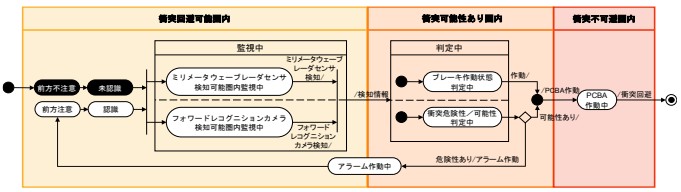

図 11 シナリオ b)の状態遷移図

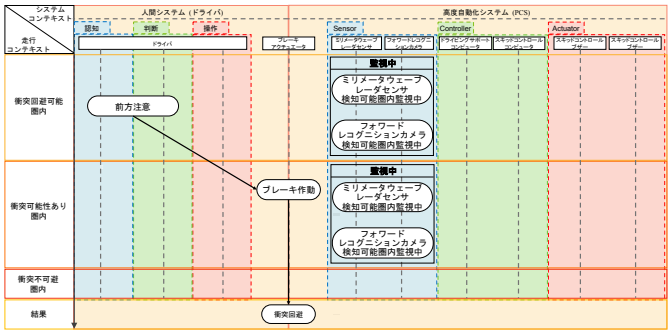

図 12 シナリオ a)の安全性ベイジアンネットワーク

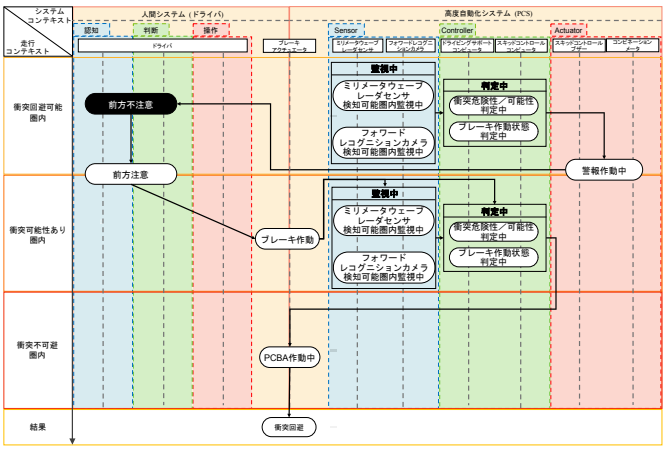

図 13 シナリオ b)の安全性ベイジアンネットワーク