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：本稿では，自動運転などの高度自動化システムと人との協調をモデル化し，協調を含む安全性要求分析方法を提案する．まず，高度自動化システムと人との協調のモデル化方法を提案する．提案モデルに対して，安全性を脅かすハザードに外部要因と内部要因があることに着目した協調の安全性モデルを提案する．次に，協調の安全性モデルにおいて，ハザードと対策をパターン化した安全性パターンを定義する．協調における安全性要求の問題として同一アクタでありながら正常とハザード要因の役割を果たすアクタをマルチアクタとして定義する．ミスユースケース分析を拡張して，マルチアクタを用いてハザードとその緩和の関係をモデル化し，安全性パターンとミスユースケースシナリオを対応することで緩和ポイントと緩和ユースケースを特定する．これを基にベイジアンネットワークを用いて安全性要求の有効性を定量的に評価する方法を提案する．本提案方法を実際の自動緊急ブレーキシステムに適用し，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)，自動緊急ブレーキ

A Safety Requirements Analysis Method based on Cooperative Model of Human and Advanced Automation System and Its Evaluation with Advanced Driving Assistant System (ADAS)

MOE MATSUBARA[†1]　MIKIO AOYAMA[†2]

1. はじめに

近年，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に伴い，高度自動化システムの安全性への注目が高まっている．例えば，自動車には先進運転支援システム(ADAS: Advanced Driving Assistant System)が，飛行機にはFBW(Fly-by-Wire)が搭載されるようになった．これらの高度自動化システムは，事故の防止や，運転あるいは操縦の負荷の軽減を目的として搭載されている．しかし，実際には事故が起きているのが現状である．この要因には，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[7]，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，人と高度自動化システムとの間の問題が挙げられる[7]．このことから，事故を起こさないためには，高度自動化システムのみで安全性を実現するのではなく，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．今後，自動運転などのより高度な自動化機能が活用される状況にあっては，人と高度自動化システムが協調して高い安全性を満たすことが求められている．

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，セキュリティ分析手法を安全性分析に応用して，安全性パターン，ミスユースケース分析，ベイジアンネットワークを組み合わせた，人を含めた高度自動化システムの安全性要求の分析方法を提案する．

本提案方法を実システムに適用し，提案方法の有効性を示す．本提案方法により，自動車の安全性要求を満たすシステムの要求定義が可能になる．

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 3 点を研究課題とする．

RQ1. 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適切なモデル化の方法とは何かを示す．

RQ2. RQ1. によるモデルを用いた安全性要求の定量的分析方法とは何かを示す．

RQ3. 実システムを用いて提案方法の有効性の評価を行う．

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

†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

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設計やシステム形態が課題として挙げられている[7]．また，人と高度自動化システムの協調モデルも未確立である．

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．

セキュリティ要求工学におけるリスク要因は主にシステムの外部にあるが，安全性要求工学におけるリスク要因はシステムの内部に存在する場合もある．

ここで，セキュリティ分析で用いられる分析手法としてミスユースケース分析とセキュリティパターンを挙げる．

(1) ミスユースケース分析

ミスユースケース分析では，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．ユースケース図に脅威を与えるミスアクタとミスユースケースを付加し，脅威と緩和の関係を表現する [2].

(2) セキュリティパターン

セキュリティパターンは，特定の状況に関した問題に対する解決法をパターン化したものである．パターンには，名前などの他に，状況，問題，解法，解法の構造や振舞い，結果などが含まれる[3]．一方，安全性のパターンに関する議論は極めて少なく，パターンカタログに関する考察はあるがパターンの具体的な提案はない．

3.3 安全性リスク分析

(1) ETA, FTA, FMEA

ETA(Event Tree Analysis)，FTA(Fault Tree Analysis)，FMEA(Failure Mode of Effect Analysis)は，いずれもリスク分析手法であり，定性的または定量的なリスク分析や評価に用いられる．これらの手法は，システムの単一故障をハザード要因として識別し，分岐条件を論理的に組むことで網羅的に分析するため深く分析できる．その反面，システムの全体的な視野での分析が難しい[6][14][20].

(2) ベイジアンネットワーク

ベイジアンネットワークは高次元確率分布を表すのに用いられる．ベイジアンネットワーク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，条件付確率により各変数間の定量的な依存関係を表す．ベイジアンネットワークは，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，ベイジアンネットワークを応用することで，障害診断を行うことができる[9].

(3) STAMP/STPA

STAMP(Systems-Theoretic Accident Model and Process)は，システムの中で安全のための制御を行う要素と制御される要素の相互作用が働かないことによって起きるという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を前提としてシステムのハザード要因を分析する手法が STPA(STAMP based Process Analysis)として提唱されている．

相互作用を行う複雑なシステムにおいて，相互作用のハザード要因を識別し，過去のアクシデント事例データに基づくガイドワークによって網羅的に分析できる．また，システム全体の振舞いを確認しながら分析することが可能である[8].

3.4 自動車の機能安全性

(1) 機能安全

機能安全とは，システムや装置に故障や異常が発生することを想定し，それらに対処を施し安全を確保するための概念である．

(2) ISO26262

ISO26262 は，自動車電子制御における機能安全規格である．ISO26262 における安全性の尺度は ASIL によって定められ，その分析方法のガイドも提示されている．しかし，ISO26262 は，システムの構成に関する安全性の基準であり，要求定義における安全性分析には適さない．

4. アプローチ

本稿のアプローチを図 1 に示す．本研究の課題は人と高度自動化システムの協調モデルに基づくシステムコンテキストを用いた安全性要求分析方法である．このとき，人もシステムとみなすと，人間システムと高度自動化システムとの間の協調のモデル化が課題として浮かび上がる(図 1).

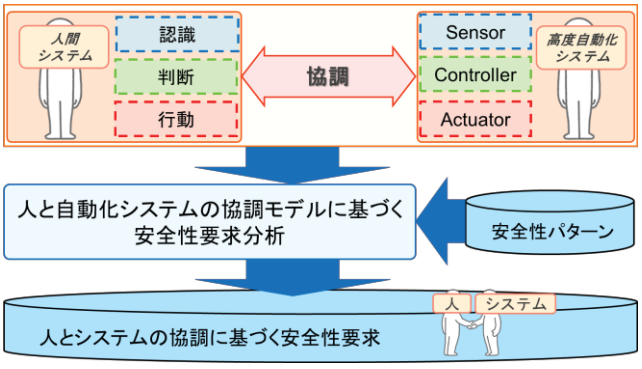

図 2 アプローチ
Fig.2 Approach

高度自動化システムにおける安全性は，システムとシステムを利用する人の協調によって実現する．よって，本稿では，人を含めた，人とシステムの協調モデルに基づいた安全性要求分析を行う．本稿では，セキュリティに対する要因を脅威と呼ぶのに対して，安全性に対する要因をハザードと呼ぶ．

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すると，システムに関与する人を含めた全てのアクタはミスアクタになり得るという特徴を持つと考えられる．したがって，安全性要求分析では，システム内部の要因も分析できるような分析方法が必要である．

また，セキュリティ分析手法の 1 つであるミスユースケース分析は，ユーザ視点で利用シーンを想定して分析を行う．安全性のハザード分析においても，人とシステムの協調によって安全性を実現することが求められている点から，ユーザ（人）視点で事故発生までのシナリオを導出，事故発生シーンを想定して分析を行えば，安全性の実現に必要な対策の分析も行うことができるのではないかと考える．

これらに着目して，外部からの脅威からシステムを守るためのセキュリティ分析を安全性分析に応用し，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，ベイジアンネットワークを用いて，事故発生確率を求めることで定量的評価を実現する[1].

5. 提案方法

本稿で提案する安全性要求分析のプロセスを図 2 に，安全性要求のメタモデルを図 3 に示す．

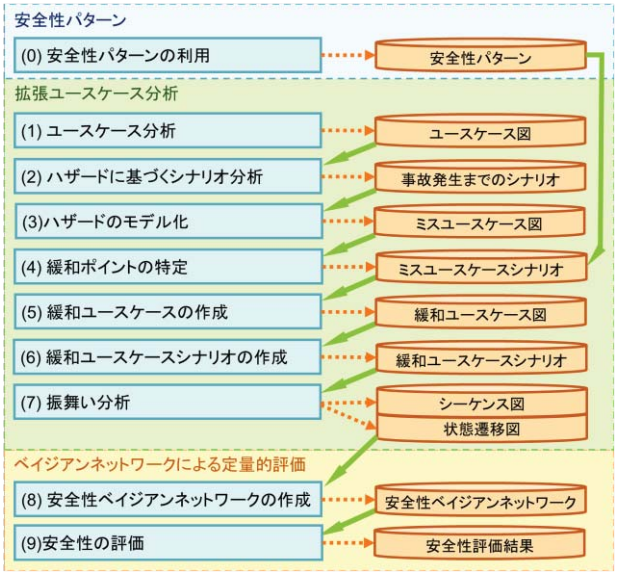

図 2 安全性要求分析方法
Fig2. Safety Requirements Analysis Method Process

本稿では，安全性システムをシーケンス図とユースケース図により表現する．ミスユースケースと緩和ユースケース図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．

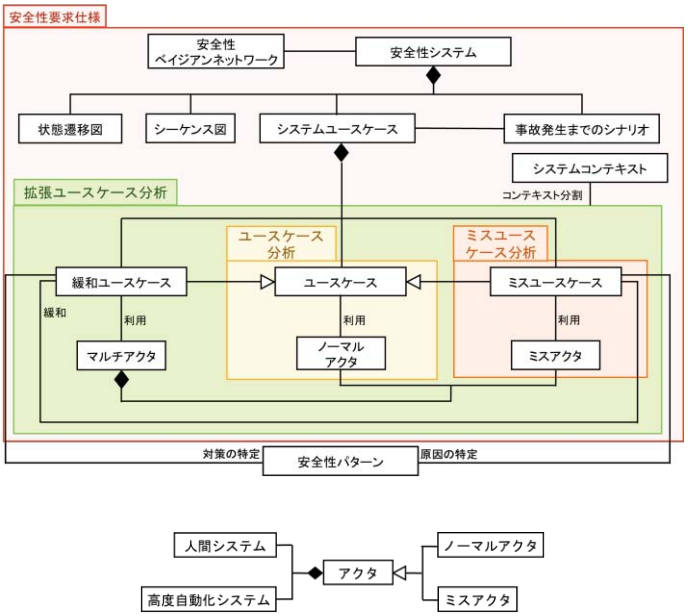

図 3 安全性要求メタモデル
Fig.3 Safety Requirements Meta Model

5.1 ユースケースモデルの拡張

本稿で用いる，ユースケースモデルを拡張したアクタとユースケースなどのモデル間の関係をメタモデルとして図 3 に示す．

安全性に対するハザードには，システムの外部要因と内部要因の両方に着目する必要がある．そこで，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拡張ユースケース分析を提案する．拡張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

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 Sensor, Controller, Actuator の 3 つのコンテキストに分割してパッケージとして表現することで，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，例えば運転者，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のことを，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，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と呼ぶことにする．

5.2 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．

(2) 安全性パターンの記述

本稿で提案する安全性パターンの記述方法を表 1 に示す．名前，原因，問題，対策，結果の 5 項目を記述する．

表 1 安全性パターンの記述
Table 1 Description of Safety Pattern

記述項目	概要
名称	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

(3) 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．

5.3 安全性ベイジアンネットワーク

拡張ユースケース分析で導出されたユースケースあるいはミスユースケースをノードと見なし，シナリオに基づいたベイジアンネットワークを作成する．

5.4 詳細プロセス

(0) 安全性パターンの作成

安全性要求分析の対象システムに対して，安全性パターンを作成する．

(1) ユースケース分析

対象システムに対してユースケース分析を行う．このとき，システムの振舞いに影響を与え得る人も含めた分析を行う．

(2) ハザードに基づくシナリオ分析

(1)で導出されたユースケースを基に，システムあるいは人の安全性を脅かし得るハザードとなるミスユースケースを特定する．さらに，ユースケースあるいはミスユースケースに基づいて，想定される事故が発生するまでのシナリオを導出する．

(3) ハザードのモデル化

システムについて，拡張ユースケース図を作成することでシステムとハザードの関係をモデル化する．拡張ユースケース図におけるユースケースやミスユースケースはシステム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，この図からマルチアクタを特定する．

(4) 緩和ポイントの特定

ミスユースケースシナリオを記述する．また，シナリオからハザードに対する緩和ポイントを特定する．

(5) 緩和ユースケースの作成

(3)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する．

(6) 緩和ユースケースシナリオの作成

緩和ユースケースをもとに，緩和ユースケースシナリオを作成する．ここでは，緩和ポイントや安全性パターンを用いることに注意する．

(7) 振舞い分析

拡張ユースケース分析で作成した拡張ユースケース図を基に，システムの振舞いの順序や時系列シーケンス図を用いて分析する．このとき，マルチアクタやユースケース，ミスユースケースを一目見てわかるように，ミスユースケースの場合は活性区間を黒塗りにし，マルチアクタはアクタの周りを太い黒枠で囲って表現する．振舞いもシステムコンテキストに分割し，シーケンス図からシステムの状態を特定する．次に，特定された状態からシステムの状態遷移図を構成する．

(8) 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ベイジアンネットワークを作成する．ここで，ベイジアンネットワークを作成する際に，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表現する．ベイジアンネットワークをこの 2 次元コンテキスト構造上に配置することで，各コンテキストの変化に応じたシナリオに沿って安全性の定量的分析が可能になる．

(9) 安全性の定量的評価

作成したベイジアンネットワークのノードに付与された重み付き確率を，ハザード緩和前とハザード緩和後についてそれぞれのベイジアンネットワークに沿って計算することにより衝突確率を求め，安全性が向上しているかどうかを評価する．ここで，「安全性が向上している」とは，ハザード緩和後の事故発生確率がハザード緩和前の事故発生確率より低下している状態とする．

6. 例題への適用

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の仕様に本提案を適用した例を用いて説明する．

6.1 適用対象システム

実際の自動車の制御システムの仕様に本提案を適用し，有効性を確認した．適用対象システムはプリクラッシュセーフティシステムである．提案方法の効果を評価するために，2004 年モデル[11]と 2009 年モデル[10]の同一の安全性システムに適用した．いずれのモデルも，ミリ波レーダセンサを入力として制御を行うが，カメラセンサが追加され

た 2009 年モデルでは安全性が向上していることを定量的に比較し，評価した．

プリクラッシュセーフティシステムの作動については，次の 4 点を前提条件とする．

(1) 自車は走行状態である．
(2) 前方に障害物がある．
(3) 対車については追突のみとする．
(4) プリクラッシュセーフティシステムの作動条件は，自車と障害物の相対速度に依存する．

6.2 適用

(0) 安全性パターンの作成

プリクラッシュセーフティシステムについて安全性パターンを作成する．安全性パターンの例として，センサ冗長構成パターンとドライバーの前方不注意に対する安全性パターンを示す(表 2).

表 2 安全性パターン
Table 2 Safety Patterns

安全性パターン 【ドライバーの前方不注意パターン】	
名前	ブレーキが作動しない
原因	ドライバーの前方不注意
問題	ドライバーは前方不注意により障害物に気付かず，適切にブレーキを作動させないため，障害物と衝突する恐れがある．
対策	アラームにより，ドライバーに警告をする
結果	アラームが作動してドライバーに注意を促すため，障害物を発見し，適切なブレーキの作動を行うことができる．よって，障害物との衝突を回避できる可能性がある．

(1) ユースケース分析

プリクラッシュセーフティシステムについてユースケース分析を行った．プリクラッシュセーフティシステムの振舞いに影響を与え得る人として，ドライバーを含めた分析を行った．

(2) ハザードに基づくシナリオ分析

(1)で行ったユースケース分析を基に，ハザードとなり得るミスユースケースを特定し，ユースケースあるいはミスユースケースに基づいて，想定されるシナリオを木構造によって導出した(図 4)．このシナリオ分析から，ハザード緩和前後のシナリオの例として次の 2 つのシナリオを抽出する．

(i) カメラセンサが搭載されず，ミリ波レーダセンサが故障した場合のシナリオ
(ii) カメラセンサが搭載され，ミリ波レーダセンサかカメラセンサの何れかが正常に作動した場合のシナリオ

(3) ハザードのモデル化

2004 年のプリクラッシュセーフティシステムの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を特定してモデル化した(図 5).

(4) 緩和ポイントの特定

ミスユースケースシナリオを記述し(表 3), 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を特定した．この結果，次の緩和ポイントを得た．

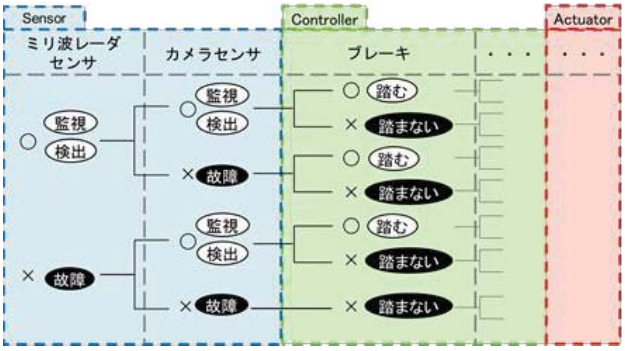

図 4 事故発生までのシナリオ
Fig.4 Scenarios until accident occurs

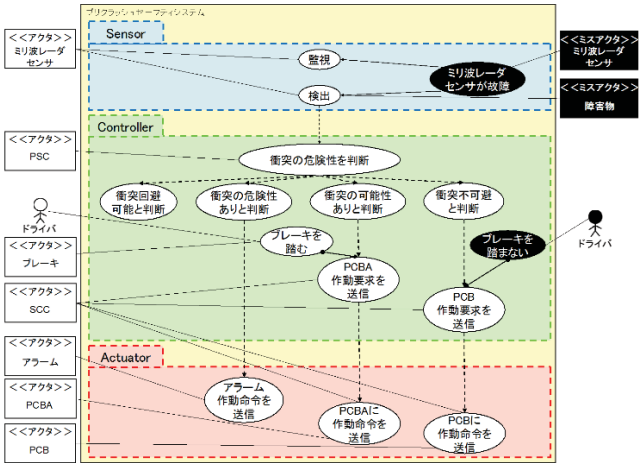

図 5 ミスユースケース図
Fig.5 Misuse Case Model

表 3 ミスユースケースシナリオ
Table 3 Misuse Case Scenario

＜ミスユースケースシナリオ＞	
ミスユースケース名	ブレーキを踏まない
アクタ／ミスアクタ	ドライバー
概要	ドライバーは前方に接近している障害物に気が付かず，ブレーキを踏まない
事前条件	障害物が接近している
基本シナリオ	ドライバーは，前方に障害物が接近していることに気が付かないまま，走行を続けようとする．
結果	ブレーキが踏まれていない
ステークホルダリスク	ドライバーのリスク ⇒ 障害物と衝突
ミスアクタ プロフィール	1) 障害物は，移動できる物でも移動できない物でもあり得る 2) ミリ波レーダセンサは機能していない
緩和ポイント	前方に障害物が接近していることに気が付かない

(5) 緩和ユースケースの作成

ミスユースケース図とミスユースケースシナリオをもとに，緩和ユースケース図を作成した(図 6). (4)で特定した緩和ポイントに着目し，ミリ波レーダセンサの故障を緩和するために「カメラセンサ」アクタを追加し，ミリ波レーダセンサと同じ「監視」と「検出」ユースケースを追加した．これにより，「ミリ波レーダセンサが故障」が「検出」に与えるハザードを緩和することが期待できる．

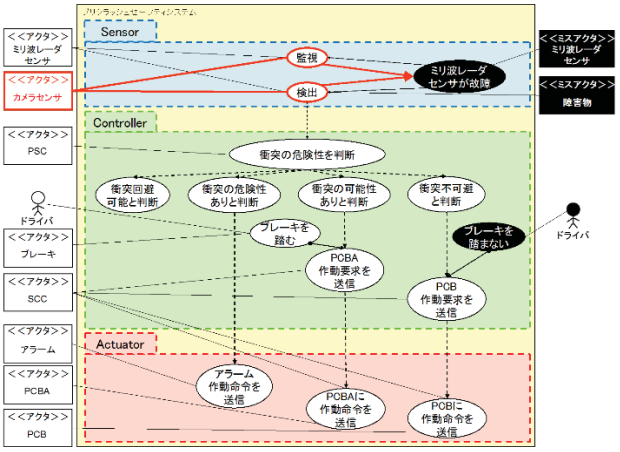

図 6 緩和ユースケース図
Fig.6 Mitigation Use Case Model

(6) 緩和ユースケースシナリオの作成

緩和ユースケースのシナリオを記述した．(4)で追加された緩和ユースケース「検出」について記述した(表 4).

表 4 緩和ユースケースシナリオ
Table 4 Mitigation Use Case Scenario

＜緩和ユースケースシナリオ＞	
緩和ユースケース名	検出
アクタ	カメラセンサ，障害物
概要	ミリ波レーダセンサとは別にカメラセンサを設置したことで，ミリ波レーダセンサが故障しても，前方の障害物を検出できるようになる
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) カメラセンサからの車両前方の映像データの解析情報をもとに，前方の障害物を検出する 2) 障害物の検出情報を PSC に送信する
結果	PCS は，アラームにアラーム作動命令を送信する

(7) 振舞い分析

緩和ユースケース図とシナリオをもとに，ハザード緩和後のプリクラッシュセーフティシステムの振舞いをシーケンス図で示した(図 7)．これによって，ハザード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．また，シナリオとシーケンス図に基づき，振舞いを状態遷移図で表現した(図 8).

(8) 安全性ベイジアンネットワークの作成

状態遷移図を基に，ベイジアンネットワークを作成した．ハザード緩和前後の事故発生確率を求めるために，ハザード緩和前後のそれぞれのベイジアンネットワークを作成した(図 9). 本例題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は「走行コンテキスト」とする．

(9) 安全性の定量的評価

(2)で導出された下記の 2 つのシナリオについて安全性の評価を行った．

(i) カメラセンサが搭載されず，ミリ波レーダセンサが故障した場合のシナリオ（ハザード緩和前のシナリオ）

(ii) カメラセンサが搭載され，ミリ波レーダセンサかカメラセンサの何れかが正常に作動した場合のシナリオ（ハザード緩和後のシナリオ）

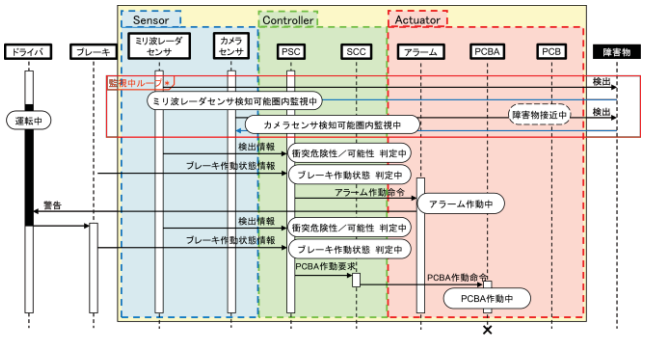

図 7 シーケンス図
Fig.7 Sequence Diagram

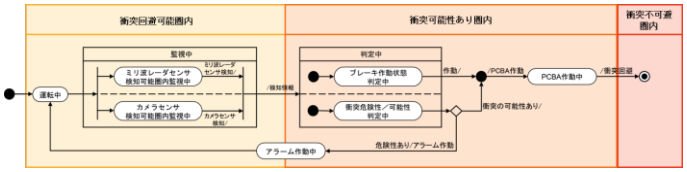

図 8 ハザード緩和後の状態遷移図
Fig.8 State Transition Diagram after Hazard Mitigation

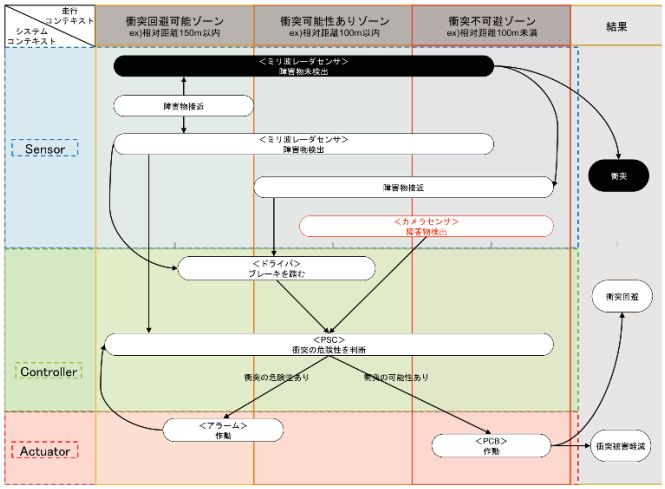

図 9 ハザード緩和後の安全性ベイジアンネットワーク
Fig.9 Safety Bayesian Networks after Hazard Mitigation

また，いずれのシナリオでも，アラーム，プリクラッシュブレーキアシスト，プリクラッシュブレーキは正常に作動するものと仮定する．

表 5 と図 10 より，次の式(1)，(2)が得られた．

(i)における衝突の確率 a

$$a = \mu_1 \tag{1}$$

(ii)における衝突回避の確率 b

$$b = \mu_0\mu_1(1-\mu_2) \tag{2}$$

このとき，a はハザードとなる確率を，b は安全性保証確率

表 5 確率表
Table 5 Probability table

機能（アクタ）	正常に作動しない確率（脅威になる確率）	正常に作動する確率（安全性を保つ確率）
ミリ波レーダセンサ	μ_1	$1-\mu_1$
カメラセンサ	μ_2	$1-\mu_2$
PSC	μ_3	$1-\mu_3$
アラーム	μ_4	$1-\mu_4$
ドライバ	μ_5	$1-\mu_5$
ブレーキ	μ_6	$1-\mu_6$
SCC	μ_7	$1-\mu_7$
プリクラッシュブレーキアシスト	μ_8	$1-\mu_8$
プリクラッシュブレーキ	μ_9	$1-\mu_9$

$(0<\mu_i<1)$

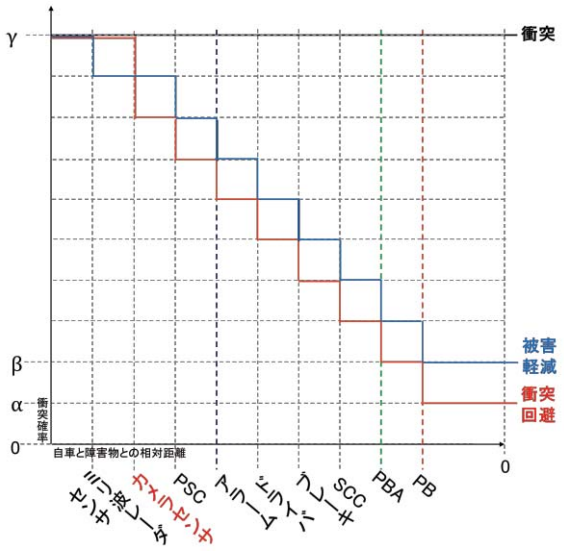

図 10 ハザード緩和前後の衝突確率
Fig.10 Collision probability before and after hazard mitigation

を表している．カメラセンサが装備されると，ミリ波レーダセンサとカメラセンサの何れか一つが正常に作動していればセンサとしての機能を果たすことから，カメラセンサが装備された場合の安全性保証確率は式(2)で表される．したがって，ハザード緩和前の事故発生確率γとハザード緩和後の事故発生確率αは次の式(3)，(4)ようになる．

$$\gamma = \mathrm{a} = \mu_1 \tag{3}$$

$$\alpha = 1 - \mathrm{b} = 1 - (\mu_0\mu_1 + \mu_0\mu_1\mu_2)$$

$$(\because \mu_0 = (1-\mu_3)(1-\mu_4)\mu_5\mu_6(1-\mu_7)(1-\mu_8)(1-\mu_9)) \tag{4}$$

式(4)と式(5)を比較して，ハザード緩和前の事故発生確率とハザード緩和後の事故発生確率の差は次の式(5)となる．

$$\gamma - \alpha = \mu_1 - \{1 - (\mu_0\mu_1 + \mu_0\mu_1\mu_2)\}$$

$$= \mu_1 + \mu_0\mu_1(1+\mu_2) - 1 > 0 \quad (\because 0 < \mu_i < 1)$$

$$\therefore \quad \gamma > \alpha \tag{5}$$

式(5)より，ハザード緩和後の事故発生確率がハザード緩和前の事故発生確率より低くなっているため，2009 年モデルでは，2004 年モデルよりさらに安全性が向上していることが定量的に評価できる．

また，2 つの各シナリオの交通事故発生確率の推移を図 12 に示す．各機能が正常に作動していれば事故発生確率は低下し，正常に作動しなければ事故発生確率は低下しないものとして，各シナリオについて事故発生確率の推移を示した．シナリオ(i)，(ii)の確率の変動をそれぞれ黒線，赤線で示す．

シナリオ(i)は，ミリ波レーダセンサが故障するとそれ以降の機能も作動しなくなるため，事故発生確率はミリ波レーダセンサが故障確率である$\mu_1=\gamma$となる．

シナリオ(ii)は，ミリ波レーダセンサかカメラセンサの何れかが正常に作動すればセンサとしての機能が保証されるため，事故発生確率はシナリオ(ii)に比べて低下し，最終的な事故発生確率はαになる．

これにより，ハザード緩和後の事故発生確率αがハザード緩和前の事故発生確率γより低下していることが確認できる．

7. 評価

7.1 RQ1: 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

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，振舞いの分岐条件の表現が可能になった．

7.2 RQ2: 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ベイジアンネットワークを用いることにより，ハザード緩和前の事故発生確率とハザード緩和後の事故発生確率を比較し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．

7.3 RQ3: 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自動車の 2004 年モデルと 2009 年モデルのプリクラッシュセーフティシステムに適用した．2004 年モデルにはミリ波レーザセンサのみ搭載されているのに対し，2009 年モデルにはミリ波レーダセンサに加えカメラセンサも搭載されていることから，2009 年モデルは 2004 年モデルより安全性が向上しているかどうかを検証した．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，ベイジアンネットワークを生成して，ハザード緩和後の事故発生確率がハザード緩和前の事故発生確率よりも低下することを定量的に定式化できるため，安全性の向上を定量的に評価可能となった．この結果は，提案方法の有効性を示すものといえる．

8. 考察

関連研究と比較して，提案方法の意義を議論する．

8.1 セキュリティパターンの応用

システムに問題が起きたときを想定して対策を示すにあたり，セキュリティパターンを応用して安全性パターンを作成することで，システムに起こる問題の原因と対策のパターン化が可能となった．これにより，システムに対するハザードとハザードの緩和ポイントを容易に特定可能となった．

8.2 ユースケース分析の拡張と有効性

(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，外部要因によるハザードだけでなく，内部要因によるハザードも明確にすることが可能になった． 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 ベイジアンネットワーク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，ベイジアンネットワークを適用することで，ハザード緩和後の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いえる．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シナリオの定量的安全性の分析

自動車の衝突防止ブレーキシステムのような組込みシステムではコンテキストの連続的変化とシステム状態の離散的変化が融合している．しかし，コンテキストの連続的変化に伴いベイジアンネットワークのノードに付与された重み付き確率も変化することが考えられる．したがって，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 システムの緩和策の優先順位付けの方法

安全性の保証には緩和策の優先順位付けも必要になる．人とシステムのハザードに対する緩和策の実行順序に加え，その優先順位付けを行う必要がある．

9.3 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，人と高度自動化システムの協調モデルに基づく，安全性パターン，拡張ユースケース分析，ベイジアンネットワークを組み合わせた，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．

本提案方法をプリクラッシュセーフティシステムに適用して，安全性が向上していることを定量的に評価した．

本提案方法の課題を解決することで，コンテキストの変化に対応した高度な制御を行うシステムの安全性を満たすシステムの設計や開発が期待できる．さらには，近年注目されているコネクテッドカーのセキュリティ面と安全性面の両面の要求分析にも応用できることが期待される．

参考文献

[1] R. Adla, et al., Bayesian Network Based Collision Avoidance Systems, IEEE EIT, May. 2015, pp. 605-610.
[2] I. Alexander, Misuse Cases, IEEE Software, Vol. 20, No.1, Jan./Feb. 2003, pp.58-66.
[3] K. Beckers, Pattern and Security Requirements, Springer, 2015.
[4] T. Bedford, and R. Cooke, Probabilistic Risk Analysis, Cambridge University Press, 2001.
[5] B. J. Czerny, et al., Effective Application of Software Safety Techniques for Automotive Embedded Control Systems, Automotive Software, SAE International, 2016, pp.95-195.
[6] C. Ebert, et al., Safety and Security Requirements Engineering, Springer, Proc. of Internationales Stuttgarter Symposium, 2016, pp. 335-346.
[7] 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，pp.11-20.
[8] IPA ソフトウェア高信頼化センター，はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～，IPA，2016.
http://www.ipa.go.jp/sec/reports/20160428.html
[9] 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.
[10] トヨタ自動車，*CROWN MAJESTA* 新型車解説書，URS206/UZS207, 2009.
[11] トヨタ自動車, *CROWN MAJESTA* 新型車解説書, UZS18#, 2004.