組込みシステム安全性要求定量的分析方法の提案

松原 百映[†1]　青山 幹雄[†2]

概要：本稿では，組込みシステム安全性要求分析のための定量的分析方法の提案とその課題を示す．拡張ユースケースでモデル化した安全性要求をベイジアンネットワークでモデル化し，ネットワーク上の確率計算によりシナリオの振舞いに沿った安全性を定量的に分析する方法を提案する．提案方法を実システムへ適用し，その課題を議論する．

A Quantitative Analysis Method for Safety Requirements of Embedded Systems

MOE MATSUBARA[†1]　MIKIO AOYAMA[†2]

1. はじめに

本稿では組込み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する．この定義に基づき，システムの安全性に対する脅威としてシステムの外部要因と内部要因の両方に着目して，安全性要求分析を行うための定量的分析方法を提案する．システムの状態遷移とその安全性の条件付き確率をベイジアンネットワークでモデル化し，シナリオの振舞いに沿った確率計算で安全性の定量的評価を可能にする．

2. 研究課題

本稿では，安全性要求の定量的分析方法について以下の 2 点を研究課題とする．
(1)安全性要求のモデル化方法を示す．
(2)安全性要求を定量的に分析するための表現方法を示す．

3. 関連研究

(1) ETA(Event Tree Analysis)[事象木解析]

ETA はリスク分析方法の1つである．システムの故障の原因事象とそれに対する対策の成否の確率を木構造でモデル化し，木構造に沿った確率計算により故障の発生確率を評価する[2].

(2) ベイジアンネットワーク

ベイジアンネットワーク(以下 BN と略記)は，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，グラフ構造に沿った条件付確率の計算により各変数間の定量的な依存関係を表す．BN を応用することで，障害診断を行うことができる[3].

4. 提案方法

本稿では，拡張ユースケース分析と BN を組み合わせた組込みシステム安全性要求分析方法を提案する．以下，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(以下 PCS と略記)の仕様に本提案を適用した例を用いて説明する[5][6].

4.1 拡張ユースケース分析

本稿では，従来のミスユースケース分析[1]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行う．拡張ユースケース分析では，システムにおける脅威と緩和の関係を特定する．

(1) システムコンテキスト

組込みシステムの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[4]．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(図 1).

(2) マルチアクタ

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可能性があるという特徴がある．このようなアクタを本稿ではマルチアクタと定義する．例えば，図 1 で示されているドライバやミリ波レーダセンサが故障することにより，マルチアクタとなる．これにより，システムの内部要因に起因する安全性の分析が可能になる

4.2 拡張ユースケース分析からベイジアンネットワークの構成

拡張ユースケース分析で作成した図 1 に示す拡張ユースケース図を基に，そのシナリオから振舞いを表すシーケンス図を作成する(図 2). 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マシン図を構成する(図 3). 最後に，状態マシン図の各状態をノードとした BN を作成する(図 4). 作成した BN のノードに付与された重み付き確率を，BN に沿って計算することにより衝突確率が求まり，安全性が定量的に評価できる．

図 4 の BN は，縦軸をシステムコンテキスト，横軸を走行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している．BN

†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
Department of Software Engineering, Nanzan University

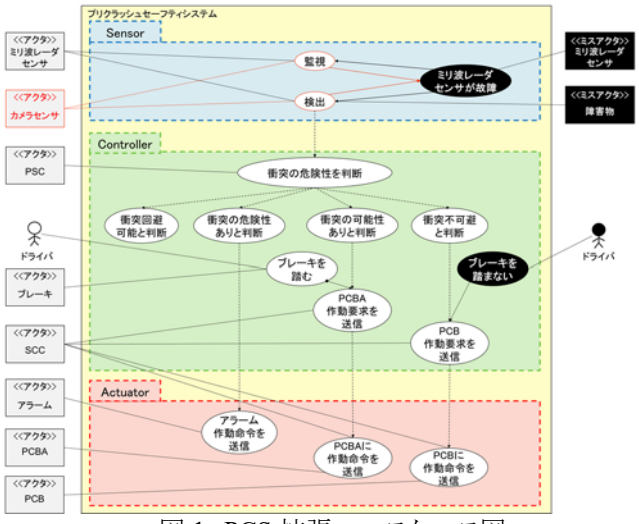

図 1　PCS 拡張ユースケース図

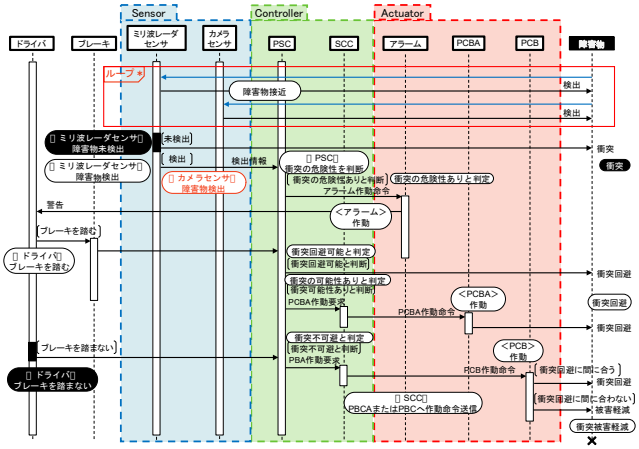

図 2　PCS シーケンス図

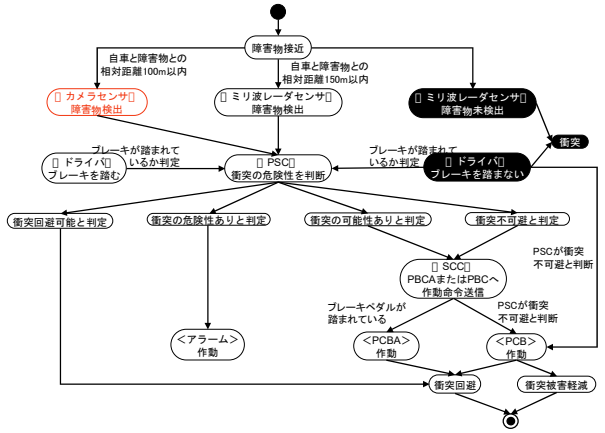

図 3　PCS 状態マシン図

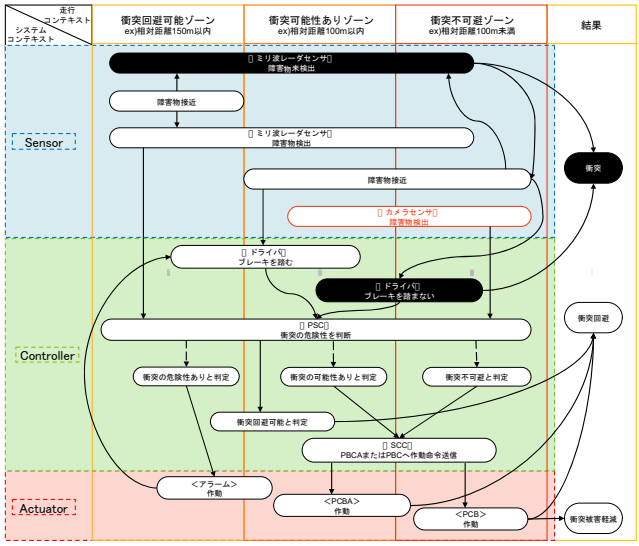

図 4　PCS ベイジアンネットワーク

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．

5.　提案分析方法の課題

(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評価方法

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 BN 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．

(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．システムの脅威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．

(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．

6.　まとめ

本稿では，拡張ユースケース分析と BN を組み合わせた組込みシステム安全性要求の定量的分析方法を提案した．さらに，提案方法の課題を明らかにした．これらの課題を解決することで，自動緊急ブレーキシステムなどのコンテキストの変化に対応した高度な制御を行う組込みシステムの安全性要求の定量的分析が可能になると考えられる．

参考文献

[1]　I. F. Alexander, and N. Maiden (eds.), Scenarios, Stories, Use Cases, John Wiley & Sons, 2004.
[2]　T. Bedford, and R. Cooke, Probabilistic Risk Analysis, Cambridge University Press, 2001.
[3]　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.
[4]　R. N. Taylor, et al., Software Architecture, John Wiley & Sons, 2010.
[5]　トヨタ自動車, TOYOTA CROWN MAJESTA 新型車解説書, 2004.
[6]　トヨタ自動車, TOYOTA CROWN MAJESTA 新型車解説書, 2009.