自動車ソフトウェアの安全性設計

2007MI195　POLZIN Ken　　2007MI200　酒向　宏誌

指導教員　青山　幹雄

1. はじめに

自動車組込みソフトウェアの課題の一つに自動車の安全性が挙げられる. ソフトウェアの規模拡大, 複雑化のため, 自動車制御システムを開発する際に信頼性, 安全性の高いシステムを作成する体系的な方法が必要である.

本研究は, 自動車ソフトウェアの安全性設計方法の提案を目的とする. 提案方法をマイクロマウスに適用することで安全性が向上することを示す.

2. 研究課題

本研究では, 自動車ソフトウェアの安全性設計を課題とする. 機能安全の考え方に基づいて, 安全性を保証できる体系的な安全性設計方法を提案する. また, 自動車のモデルとしてマイクロマウスを採用し, マイクロマウスに提案方法を適用することで, リスク低減の効果の評価をする.

3. 関連研究

(1)　機能安全

機能安全は, 機能による安全と機能の安全に分けて扱われる. 機能による安全とは, 安全を確保する機能(安全機能)を導入することによる安全性の向上である. 機能の安全とは, 特別な機能を追加して安全性を向上するわけではなく, 製品のすべての機能が正しく動作することによる安全性である. あるいは, 故障しても安全を確保できるような設計をすることによる安全性である[1, 3].

機能安全の考え方に基づいて安全性設計を行うためには, バグの発生などの機能の故障を防ぐ方法や, フェイルセーフを実現する方法, どのような安全機能を追加すべきかを検討し, リスク低減の仕組みを構築する必要がある.

(2)　リスクの状態モデル

自動車の状態を, 機能に関する状態ではなく, 安全性に関する状態に分類する[2]. 安全性に関する状態として, 安全状態, 臨界状態, 危険状態の三つを定義する. 定義の方法は定義する人に依存するが, 安全状態, 臨界状態, 危険状態の順で危害の発生確率が低いものとする. 安全状態から危険状態, 危険状態から安全状態に直接遷移することはなく, 臨界状態を介して遷移する. 臨界状態から危険状態への遷移確率を低減すること, 危険状態から臨界状態への遷移確率を向上することでリスクを低減できる.

4. アプローチ

本研究では, 機能安全と自動車の走行状態の分類を組み合わせるという視点から, ソフトウェアの安全性設計方法を提案する. まず, 自動車の走行状態を, 安全性に関する三つの状態, 安全状態, 臨界状態, 危険状態に分類する. 次に, 危険状態への遷移の原因をFTA（Fault Tree Analysis）を用いて特定し, ETA(Event Tree Analysis)を用いてイベント遷移を明確にする. そして, FT 図や ET 図を利用して, 追加すべき安全機能を特定する. 安全機能の追加前と追加後における事象の発生確率や安全機能の失敗確率を求めることで, 遷移確率の低減を評価できる. また, あらかじめ許容可能な遷移確率を決定しておき, 安全機能を組み合わせることで, 許容可能な遷移確率を下回るようにできる.

5. 安全性設計方法の提案

5.1. 安全性設計のプロセス

以下のプロセスでリスク低減することを提案する(図 1).

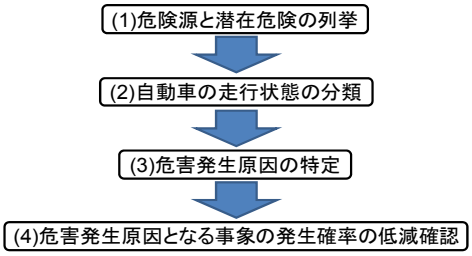

図 1 提案するリスク低減のプロセス

5.2. 危険源と潜在危険の列挙

自動車の走行システム内に存在する危険源と, その危険源が生成する潜在危険を列挙する. 危険源とは, 危害（傷害, 財産や環境の毀損）を引き起こす源泉である. 潜在危険とは, 危険源の存在によって発生する可能性のある事故の種類や, その事故によって危害に至るまでのプロセスのことである.

危険源と潜在危険を列挙することで, 発生しうる事故を特定できる. 特定した潜在危険の中からリスク低減の対象とするものを選出する.

5.3. 自動車の走行状態の分類

自動車の走行状態を, 安全状態, 臨界状態, 危険状態の三つに分類する. 選出した各潜在危険に対する危険状態

を特定し，それをもとに危険状態に遷移する直前の状態（臨界状態）を特定する．

各状態を次のように定義する．

(1) 安全状態：危害が発生せず，危険状態に遷移しない状態．

(2) 臨界状態：危害が発生せず，危険状態に遷移する可能性のある状態．

(3) 危険状態：危害が発生する可能性のある状態．例えば，衝突の危険源に暴露されている状態（走行レーンからの逸脱など）．

図 2 に，状態の分類と状態遷移の例を示す．

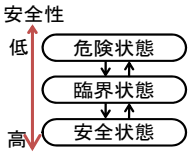

図 2 状態の分類と状態遷移の例

5.4. 危害発生原因の特定

臨界状態から危険状態へ遷移する原因を，危害発生原因とする．危害発生原因となる事象を特定し，その発生確率を低減することで，リスク低減を行う．

まず，信頼性ブロック図を作成し，自動車の走行に関するシステムを把握する．FT 図の作成において事象の原因を洗い出す際に，信頼性ブロック図のサブシステムの中に原因となり得る要素が無いかを確認することで，原因の洗い出しの漏れを防ぐことができる．

次に，危険状態への遷移を，適用するシステムにとって望ましくない事象とし，FTA を行う[4]．FTA は，結果から原因を特定する方法であり，望ましくない事象が既知である場合，有効である．本研究での設計方法では対象とする潜在危険と危険状態が特定されており，望ましくない事象は危険状態への遷移だと特定されるので，FTA は有効である．

FT 図を簡略化するため最小カットセットを求める．最小カットセットとは，FTA において，頂上事象を引き起こすために必要十分な基本事象の集合のことである．最小カットセットを求めることで，どの基本事象が頂上事象の発生に大きな影響を持っているかを知ることができる．FTA では複雑なシステムを扱う場合，FT 図が巨大になってしまい全体を見渡すのが困難になるが，最小カットセットを利用することでこの問題を解決できる．

5.5. 危害発生原因となる事象の発生確率の低減確認

機能安全に基づいて安全機能を追加することで，危険状態への遷移確率が低減されることを確認する．

(1) 許容可能リスクの決定

危険状態への遷移確率を現状からどれだけ低減するのかを決定する．

(2) 基本事象の発生確率の低減

基本事象の発生確率を低減するような安全機能を検討し，結果的に頂上事象の発生確率が低減することを，FT 図を利用して確認する．

(3) 基本事象発生時の安全確保

基本事象が発生した場合にも安全性を確保するような安全機能を検討し，結果的に頂上事象の発生確率が低減することを，FT 図を利用して確認する．

(4) ET 図の作成

危険状態への遷移のそもそもの原因である，安全状態から臨界状態への遷移を起因事象として ET 図を作成する．これにより，事象の発生や安全機能の作動といったイベントの遷移が明確にできる．ただし，イベントの発生順が一定である場合に限る．

まず，安全機能追加前の ET 図を作成することで，追加すべき安全機能の検討に利用する．

追加すべき安全機能の検討後，再度 ET 図を作成することで，安全機能の作動によってリスクが順に低減されていく仕組みを明確にする．

6. マイクロマウスへの適用と評価

自動車のモデルとしてマイクロマウスを採用し，提案方法を適用することで安全性を向上できることを示す．

6.1. マイクロマウスの概要

マイクロマウスは完全自律型のロボットであり，走行路に描かれた一本の白線をトレースしながら走行する．白線を車体前方の四つのセンサにより認識し，白線情報をもとに車輪を制御し方向転換する．

マイクロマウスの最高速度は 65.0cm/s であり，センサ値認識は 500 回/s で行われる．また，走行路内には障害物はないものとする．

6.2. マイクロマウスへの安全性設計方法の適用

(1) 危険源と潜在危険の列挙

マイクロマウスは走行路内であれば衝突の危険はないため，危険源は走行路外の障害物への衝突となり，潜在危険は衝突事故のみとなる．

(2) 自動車の走行状態の分類

状態の分類を行う際には，まず危険状態を特定する．マイクロマウスにおける潜在危険は，走行路外の障害物への衝突事故のみである．そのため，危険状態は，衝突事故の起こる可能性のある白線未認識走行状態である．実際は，白線未認識走行状態であっても走行路内であれば危害は発生しないが，マイクロマウスには走行路内と走行路外の区別がつかないため分類は不可能である．

次に，臨界状態を特定する．臨界状態は，危険状態である白線未認識走行状態に遷移する可能性のある状態である．したがって，白線を両端のセンサのみが認識している状態が臨界状態であると分類できる．

最後に，安全状態を特定する．安全状態は，危険状態でも臨界状態でもない全ての状態である．したがって，中央の二つのセンサの少なくとも一つが白線を認識している状態が安全状態である．

安全性に関する状態遷移図を図 3 に示す．

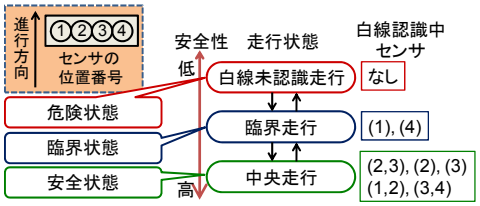

図 3 状態の分類と状態遷移

(3) 危害発生原因の特定

マイクロマウスが臨界状態である臨界走行状態から危険状態である白線未認識走行状態へ遷移する原因を，信頼性ブロック図と FTA を用いて解析する．まず，信頼性ブロック図を作成し，マイクロマウスの走行に関するシステムを把握する．作成した信頼性ブロック図を図 4 に示す．また，各サブシステムの故障モードを表 1 に示す．

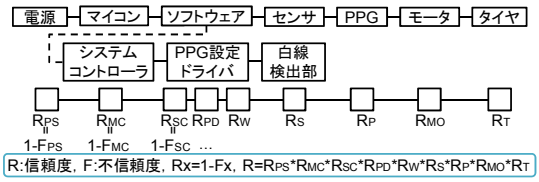

図 4 マイクロマウスの信頼性ブロック図

表 1 各サブシステムの故障モード

サブシステム	故障モード		
電源	バッテリー低下（FPS）	白線検出部	バグ（FW）
マイコン	基盤劣化（FMC）	センサ	部品劣化（FS）
システムコントローラ	バグ（FSC）	PPG	部品劣化（FP）
PPG設定ドライバ	バグ（FPD）	モータ	部品劣化（FMO）
		タイヤ	スリップ（FT）

次に，信頼性ブロック図を利用して，FT 図を作成する(図 5)．これにより，事象 A～N が特定できた．

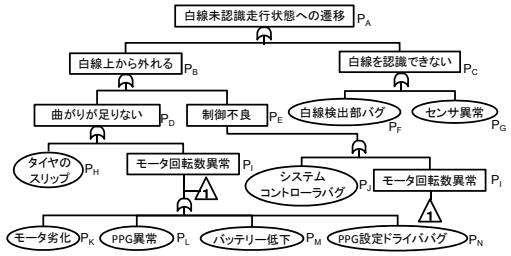

図 5 マイクロマウスの FT 図

FT 図を簡略化するため最小カットセットを求める．最小カットセットを W とすると，W は式(3)で表される．

W={H}，{K}，{L}，{M}，{N}，{J}，{F}，{G} (3)

簡略化した FT 図を図 6 に示す．

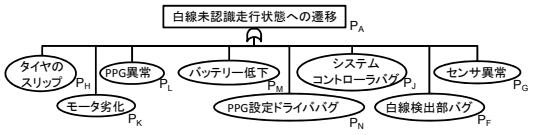

図 6 最小カットセットの FT 図

頂上事象の発生確率 P_A は式(4)で表される．

$$P_A=P_H+P_K+P_L+P_M+P_N+P_J+P_F+P_G \quad (4)$$

FT 図により，危害発生の基本事象として，タイヤのスリップ，モータ劣化，PPG(Programmable Pulse Generator)異常，バッテリー低下，システムコントローラバグ，白線検出部バグ，PPG 設定ドライババグ，センサ異常が特定できた．

ソフトウェアのイベント遷移は一定であるため，ソフトウェアの動作の関連性とイベント遷移を示す ET 図を作成する(図 7)．システムコントローラは白線検出部から現センサ情報を取得し，PPG ハンドラを起動し，PPG 設定ドライバがセンサ情報から周波数の設定を行う．そして，PPG が周波数からパルス信号を発生させモータの回転数を変更する．

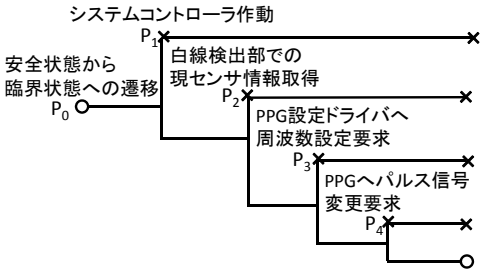

図 7 ソフトウェアの ET 図

ソフトウェアによる白線未認識走行状態への遷移確率 P は，式(5)で表される．

$$P=1-P_0*(1-P_1)*(1-P_2)*(1-P_3)*(1-P_4) \quad (5)$$

(4) 危害発生原因となる事象の発生確率の低減確認

例としてタイヤのスリップの発生確率を低減する．機能安全に基づき，安全機能を追加する．

臨界走行状態時には速度を落とすという安全機能を追加することでタイヤのスリップ確率を低減させる．

これにより，白線未認識走行状態に遷移する確率が低減できる(図 8)．

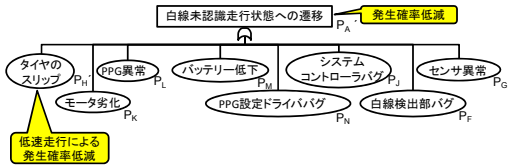

図 8 タイヤのスリップ確率低減

タイヤのスリップの発生確率を低減することにより，白線未認識走行状態へ遷移する確率を低減できた．

タイヤのスリップの発生確率 P_H が P_H' に低減されるとすると，頂上事象の発生確率 P_A も低減される．

これを P_A' とし，式(6)で表す．

$$P_A' = P_H' + P_K + P_L + P_M + P_N + P_J + P_F + P_G \quad (6)$$

また，$P_H > P_H'$ より，式(7)が成り立つ．

$$P_A - P_A' = (P_H + P_K + P_L + P_M + P_N + P_J + P_F + P_G) - (P_H' + P_K + P_L + P_M + P_N + P_J + P_F + P_G) = P_H - P_H' > 0 \quad (7)$$

式(7)より，危険状態への遷移確率が低減され，安全性が向上したと言える．

もう一つの例として，システムコントローラが白線検出部から現センサ情報を獲得するプロセスが成功しなかった場合の安全機能の追加を考える．

現センサ情報取得の動作確率を向上させるために，現センサ情報が得られなかった場合にもう一度処理を行うという機能を追加することで現センサ情報獲得の動作確率が向上する．

機能を追加した後の ET 図を図 9 に示す．

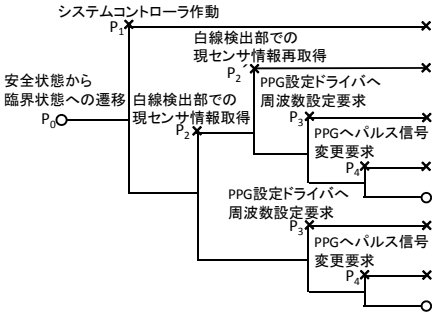

図 9 機能追加後のソフトウェアの ET 図

これにより，ソフトウェアのバグによる白線未認識走行状態へ遷移する確率を低減できる．低減された白線未認識走行状態への遷移確率 P' は式(8)で表される．

$$P' = 1 - \{P_0*(1-P_1)*P_2*(1-P_2')*(1-P_3)*(1-P_4) + P_0*(1-P_1)*(1-P_2)*(1-P_3)*(1-P_4)\} \quad (8)$$

また，式(9)が成り立つ．

$$P - P' = P_0*(1-P_1)*P_2*(1-P_2')*(1-P_3)*(1-P_4) > 0 \quad (9)$$

式(9)より，危険状態への遷移確率が低減され，安全性が向上したと言える．

7. 提案方法の評価

本研究で用いた考え方や技法の評価を以下に示す．

(1) 機能安全とリスクの状態モデル

リスク低減の方法を検討する際，機能安全の考え方に焦点を当てることで安全機能の追加という方法を導き出せた．

次に，追加すべき安全機能を特定するために，自動車走行システムにおける危険状態を特定する必要があった．そこで，リスクの状態モデルを利用した．また，危険状態へ遷移する直前の状態を臨界状態とし，臨界状態に安全機能による対策を施すことで，リスクが低減することを確認できた．

(2) FTA と ETA

危険状態への遷移確率を低減できるような安全機能を特定するために，原因となる事象を洗い出さなければならなかった．ここでは望ましくない結果が危険状態への遷移と決まっているため，FTA は有効であった．また，FTA で特定した事象の最小カットセットを求めることで，危険状態への遷移の致命的な原因となる事象が特定できた．

しかし，FTA では事象の発生や安全機能の作動の遷移を示すことはできないため，追加すべき安全機能の検討が困難となる場合がある．また，安全機能が作動すべきタイミングが明確にできない．そこで，FTA で洗い出した事象の中で遷移の順番が一定のものに関しては，ETA を利用することでその遷移を図で示した．

このように，FTA と ETA を組み合わせて利用することで，危険状態への遷移の原因となる事象とその遷移を特定し，追加した安全機能によって危険状態への遷移確率が低減できることを示した．

8. 今後の課題

提案方法をマイクロマウスにのみ適用したが，実際の自動車にも適用できることが目標である．マイクロマウスは，構造も走行環境も単純であるため，提案方法を適用できた．しかし，実際の自動車は複雑度が高いため，提案方法をそのまま適用することは困難である．

特に，第二工程では，具体的な状態分類方法を，提案方法を適用する人に依存しているため，改善の余地がある．実際の自動車の場合，交差点や歩行者，他の自動車の存在，運転手によるヒューマンエラーの可能性，道路による法定速度の違いなど，様々な要素が存在するため，より詳細な状態分類の方法を確立することが今後の課題である．

9. まとめ

本研究では，自動車ソフトウェアの安全性設計方法の提案を目的とした．機能安全と状態の分類に着眼した安全性設計方法を提案した．また，マイクロマウスに提案方法を適用することで安全性が向上することを示した．

参考文献

[1] 電気・電子・プログラマブル電子 安全関連系の機能安全−第 3 部: ソフトウェア要求事項, JIS C 0508-3:2000, 日本規格協会, 2000.

[2] 市村 尚規, 小山内 秀輔, オブジェクト指向を用いた自動車組込みソフトウェアの安全化設計, 2005 年度南山大学卒業論文, 2006.

[3] 清水 久二, 福田 隆文, 機械安全工学: 基礎理論と国際規格, 養賢堂, 2000.

[4] 鈴木 順二郎, 牧野 鉄治, 石坂 茂樹, FMEA・FTA 実施法, 日科技連出版社, 1982.