８　車載部品エレクトロニクス化における安全性向上技術の開発（第１報）
安全性を考慮した開発プロセス

倉本丈久，門藤至宏，横山詔常，後藤孝文

Improvement of safe system development process for electronic module using vehicle applications (1st Report)
Method for safe system development process

KURAMOTO Takehisa, MONDOU Munehiro, YOKOYAMA Noritsune and GOTOH Takafumi

Safety is one of the key issues of next-generation vehicle development. With the trend of increasing electronic module using vehicle applications, there are increasing risks from software failures. For that reason, development for these electrical equipments requires safe system development processes.

Hazard analysis and risk assessment are used to determine the safety objectives for the system. In this paper, we explore the fault tree analysis (FTA) and the failure mode and effect analysis (FMEA) those are one of the methods of hazard analysis and risk assessment. Furthermore, we allude to have applied these methods to the mock electric vehicle.

キーワード：開発プロセス，ハザード分析，リスクアセスメント，FTA，　FMEA

１　緒　　言

近年の自動車は，高機能化，環境性能といった付加価値の向上が求められており，これらを実現する主な手段として，自動車部品の電子化（エレクトロニクス化）が進んでいる。ハイブリッドカーや電気自動車など，次世代自動車の普及に伴い，エレクトロニクス化は今後さらに進行すると考えられ，市場も拡大する傾向にある[1)]。

一方で，車載電装品を制御するソフトウェアが原因となる自動車事故や不具合が発生するなど安全性への不安も増大していることから，安全性向上に対するメーカ，ユーザのニーズは大きい。

しかしながら，ソフトウェアを含む組込システムでは，個々の部品の信頼性を積み上げるハードウェアの手法では安全性が保証できない。そのため，これまでは主にテスト工程で改善を図ることにより一定の安全性を担保してきたが，膨大なソフトウェアを含む近年のシステムでは，テスト工程で一定の品質を作りこむ作業に莫大なコストと時間が必要となる。そのため，組込システムの安全性を設計や要件定義段階で担保できる開発プロセスの導入が求められている。

本研究では，安全性の高い組込システム開発を実現するためのプロセス整理と要素技術の開発を行う。本報では，仕様検討時に安全性を考慮する開発プロセスと，安全設計に必要となるハザード分析とリスクアセスメント手法について，実証モデルによる例示を用いて報告する。

２　安全性を考慮した開発プロセス

図１に組込システムの一般的な開発プロセスである V 字モデルを示す[2)]。安全性，信頼性を高め機能安全を実現するには，従来の開発プロセスと並行して，**図２**に示すように安全に関する要求を策定・実装し，検証する工程が必要となる[3)]。

（１）　安全目標の設定
　製品に求められる安全性や信頼性を整理し，安全目標を設定する。

（２）　システムの安全性要求定義
　安全目標に沿ってシステムに求められる安全要求を検討・定義し，システムの仕様に反映させる。

（３）　ソフトウェア／ハードウェア（SW/HW）安全性要求定義
　システムの安全性要求定義に沿って，各 SW/HW に求められる安全性要求を検討・定義し，各 SW/HW の仕様に反映させる。

（４）　SW/HW 安全設計・実装
　各 SW/HW の安全性要求定義と仕様に基づき設計・実装を行う。

（５）　安全性検証
　プロセスの各段階において，設定した安全性要求定義や仕様を満たしているかの検証を行う。

図１　V 字モデル

図２　安全性を考慮した開発プロセス

３　実証モデル

前章で述べた安全性を考慮した開発プロセスの実証モデルとして，モータで駆動する電動４輪車を製作する予定である。この電動４輪車の仕様を**表１**に，システム構成を**図３**に示す。

表１　電動４輪車の主な仕様

諸元	仕様
駆動方式	電動モータ前輪駆動
モータ	ブラシレス DC モータ２個
バッテリー	鉛蓄電池
寸法	600mm×400mm 程度
操縦方法	リモートコントロール
最高速度	10km/h 程度

４　ハザード分析とリスクアセスメント

開発プロセスに沿って安全目標の設定や安全要求定義を実施するには，対象となる製品やシステムに対して，

・どのような状況で
・どのような事象や原因により
・どのような危害が生じるか（ハザード）

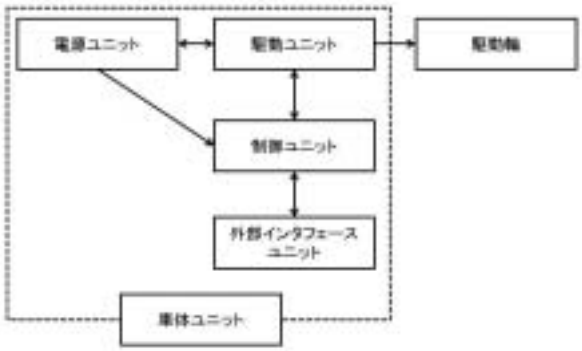

図３　システム構成図

を分析する。そしてこれらハザードの発生確率や影響などを考慮した上で，ハザードを回避するための対策やその必要性，対策によって目標とする安全性が達成できるかなどを検討する。このハザード分析の手法はこれまでに多々提案されており，主なものとしては FTA(Fault Tree Analysis)，FMEA(Failure Mode and Effect Analysis)，HAZOP(HAZard and OPerability studies)などが挙げられる [4]。今回の実証モデルの検討では，これらの手法の中から，自動車業界で用いられることの多い FTA 及び FMEA を用いた解析を行った。

4.1　FTA による解析

FTA とはシステムの特定故障（トップ事象）を想定して，その発生原因を上位レベルから下位レベルまで論理的に展開した上で，最下位レベルの事象の故障発生率からトップ事象の原因や発生確率を推定する手法である。まずトップ事象に繋がる第１次要因を列挙するとともに，事象と要因との因果関係を論理記号を用いて結びつける。続いて，第１次要因に繋がる第２次要因を列挙し因果関係を示していくといった方法を繰り返して，これ以上分解できない要因まで分析を続け，FT 図として図示する。最後に，この最下位要因の発生確率を設定することで，論理記号に従ってトップ事象の発生確率が計算できる。これにより，トップ事象の起こりやすさや各要因の影響度を評価し，リスク低減のための改善対策を検討する。実証モデルにおいて，トップ事象を「車両火災」とした場合の FT 図の例を**図４**に示す。

本研究では，この FT 図を描くためのツールとして，ちゅうごく地域組込みシステムフォーラム　平成 23 年度機能安全設計手法検討研究会にて試作された FTA 支援ツール（プロトタイプ）を用いた（**図５**）。この FTA 支援ツールは FT 図の作成のほか，記述を Prolog に変換して出力する機能を持つが，発生確率の入力や計算機能はない。そのため出力された Prolog の記述から発生確率の入力が行え，トップ事象の発生確率を計算可能なツー

ルを Visual Basic で作成した。このツールでは， FTA 支援ツールで作成した Prolog 形式のデータを一旦 Excel 形式へ変換する。この Excel 形式のデータに各事象の発生確率を入力しツールに取込むことでトップ事象の発生確率の計算を行うことが出来る（**図６**）。

図４　FTA 解析例

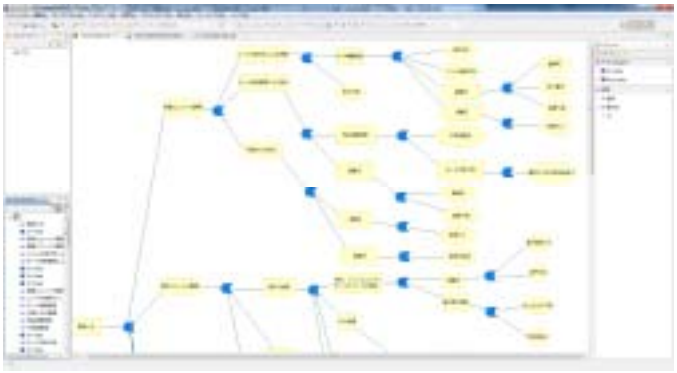

図５　FTA 支援ツール（プロトタイプ）

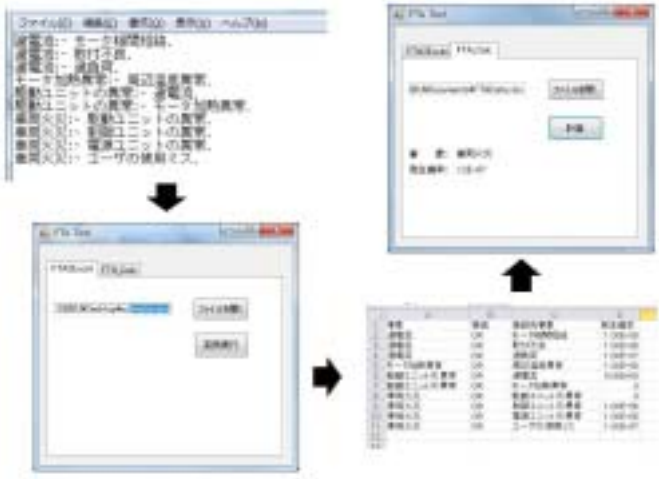

図６　FTA 発生確率計算ツール

FTA によるハザード解析では，ある事象に起こり得る要因を漏れなく列挙するとともに，それ以上分解できない要因について，その発生確率を見積もる必要がある。要因の列挙に当たっては，開発する製品に精通した担当者が加わって解析を行う必要がある。併せて，解析の結果に問題がないか検証を行うなど要因の見落としを減らす工夫が必要であるとともに，要因発生の確率をできるだけ正確に求められるよう，必要に応じてテスト等を行うことが重要である。

4.2　FMEA による解析

FMEA とは，製品及び製造プロセスについて故障モードによる影響を分析して製品やプロセスの問題の解決方法を探る手法である。まず，起こり得るすべての動作モードを考慮しながら，すべてのコンポーネントとその故障モードを識別し，リストアップする。それぞれの故障モードには，システム全体に対する影響とともに，他のシステムコンポーネントに対する影響が決定される。その

図７　FMEA 解析例

後，各故障モードにおける結果の確率と発生時の深刻度を決定し，それらを回避するための対策を検討する[5)]。**図７**に，実証モデルにおける電源ユニットの FMEA 解析例を示す。解析には，㈱構造計画研究所の FMEA-Pro を利用した。

FMEA は，ある１つのシステムや，１つの故障の分析に効果を発揮する。一方で，分析の精度向上には重要な故障モードを事前に把握しておく必要があることから，設計開発の実務担当者が分析を行うことが望ましい。

4.3　リスクの評価

前２節で行った解析を基に，ハザードのリスクが許容可能なレベルかを判断するとともに，リスクの低減が必要とされた場合は適切な対策を決定し，妥当性検討のため再度ハザード分析を行う。この作業を，すべてのハザードが許容可能なリスクレベルに到達するまで行う。今回は，**図７**に示すように，被害度，発生頻度及び検出頻度から RPN（Risk Priority Number：リスク優先度）を計算した。この数値の高いものから順にリスク低減対策を検討するとともに，得られたリスク低減対策をシステムの仕様に反映させた。また，すべての分析について，どの手法でどのように実施したかを，その結果も含めて文書で記録した。この記録は，テスト工程での検証やトレーサビリティの担保の際の重要な資料となる。

５　結　　言

安全性を考慮した開発プロセスについて，安全目標を定義するために FTA や FMEA を用いてハザード分析及びリスクアセスメントを行う手法を整理するとともに，実証モデルを用いてハザード分析及び開発プロセスの検証を実施した。今後は実証モデルを用いたハザード分析をより詳細に実施するとともに，その分析のレビューについての妥当性検証を行う。

文　　献

1）広島県：ひろしまカーエレクトロニクス戦略，2008
2）（独）情報処理推進機構ソフトウェアエンジニアリングセンター：【改訂版】 組込みソフトウェア向け開発プロセスガイド　翔泳社，2007
3）（独）情報処理推進機構ソフトウェアエンジニアリングセンター：組込みシステムの安全性向上の勧め（機能安全編）　翔泳社，2006
4）（社）組込みシステム技術協会安全性向上委員会製品安全ワーキンググループ：組込み系技術者のための安全設計入門　電波新聞社，2010
5）Nancy G. Leveson：セーフウェア　翔泳社，2009