５　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２報）
機能安全に対応した開発手法

倉本丈久，弓場憲生，横山詔常，後藤孝文，門藤至宏

Improvement of safe system development process for electronic module using vehicle applications (2nd Report)
Method of system development for functional safety

KURAMOTO Takehisa, YUBA Norio, YOKOYAMA Noritsune, GOTOU Takafumi and MONDOU Munehiro

Safety is one of the key issues in the development of next-generation vehicle. With the trend of increasing electrical equipment, risk from software failures is increasing. Therefore, development of these embedded systems requires safe development processes such as the standard ISO 26262.

ISO 26262 defines functional safety of electrical or electronic systems within road vehicle. Automobile-related enterprises will need to conform to ISO 26262. But it is difficult to correspond to this standard because this standard applies to all activities during the safety lifecycle of safety-related systems comprised of electrical or electronic and software components. This paper describes the development process according to our manual for embedded systems which include requirement definition, design, implementation and confirmation. Furthermore, we have applied the process manual to the bicycle-based electric vehicle.

キーワード：組込みシステム，機能安全，ISO26262，開発プロセス，モデルベース開発，レビュー

１　緒　　言

近年の自動車は，環境性能など様々な付加価値向上が求められている。これを実現する主な手段として，自動車部品の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，車載電装品市場も拡大傾向にある[1)]。

一方で，これらの機能を制御するソフトウェアが原因の自動車事故や不具合発生など，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ニーズは大きい。

このような背景から，自動車向けの機能安全規格 ISO26262 が策定され，2011 年に発効された。現在，各自動車メーカにおいて，この規格の準拠に向けた取り組みが進んでおり，これら自動車メーカへ車載電装品を供給するサプライヤにおいても，安全規格への対応が迫られている。

しかしながら，この規格は自動車及び車載電装品の安全に関連したコンセプト設計，開発，生産，廃棄までの広範囲にわたる内容について規定されており，規格対応を図る企業にとって高いハードルとなっている。そのため，従来からの製品開発工程に規格の内容を組み込んだツールが求められている。

本研究では，安全性の高い組込みシステム開発を実現するためのプロセスの整理と要素技術の開発を行う。本報では，組込みシステムにおけるシステム開発，ハードウェア（HW）及びソフトウェア（SW）開発の手順書を作成し，電動４輪車の開発を実証モデルとして評価したことについて報告する。

なお，手順書作成に当たっては，一般社団法人 JASPAR から公開されている機能安全テンプレート及びマニュアル[2)]を参考にした。

２　システムの安全設計

製品の安全性，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１**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)]。製品の設計段階から，その製品に求められる安全性と起こり得るハザード（危険事象）を明確にした上で，そのハザードがどのような原因でどの程度発生しうるかを分析し，目標とする安全状態を満たせるよう，危険発生原因への対策（安全要求）を決定することが求められる。このうち，ハザードの特定とリスクアセスメントの方法については前報[4)] で述べたとおりである。

ハザードの特定とリスクアセスメントの結果，問題となるハザードとその原因が特定出来たら，次にハザードの発生原因ごとに安全目標（製品が安全である状態）を定める。最後に，安全目標を満たせるよう，システムに求められる安全要求事項を定義する。その際，特定したハザードやリスクアセスメントの結果，安全目標，安全要求事項は，後日検証や修正が可能なように作成日，作

成者などの情報とともに文書（作業成果物）として残すことが重要である。この一連の手順の流れを手順書にまとめた。

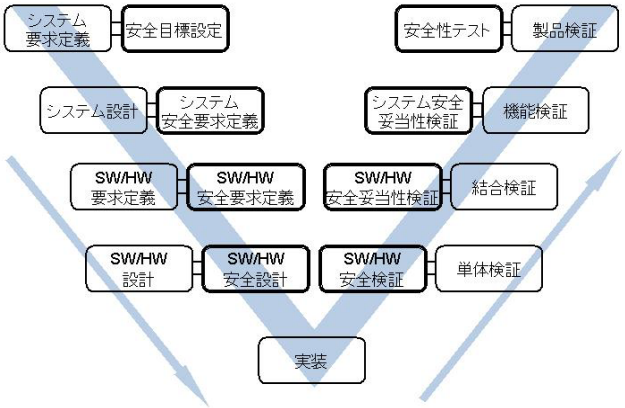

図１　安全性を考慮した開発プロセス

３　設計のレビュー

安全な製品の開発を行う上で重要となるプロセスとして，担当者が設計・開発した内容が妥当であるかどうか確認・検証（レビュー）し，必要に応じて修正を行う作業がある。レビューを行う際の手法は，**表１**に示す方法[5)]が挙げられる。

一般的に安全性を考慮した開発プロセスのレビューによく用いられるのは，インスペクションとウォークスルーである。インスペクションは，高いレベルでの安全性が求められる際のレビューには必須であり，人数をかけて厳格なレビューを行う手法である。ウォークスルーは一般的なレビューによく用いられる手法で，設計の担当者と評価者数名程度で行う手法である。

また，レビューを行うに当たり重要となるのは，設計の担当者がレビュー参加者に理解しやすい設計，記述を行うことである。そのため設計記法として UML（Unified Modeling Language）を用いるなど，設計ツールを統一しておくことが望ましい。今回作成した手順書では，これらレビュー手法の説明や実施手順，レビュー参加者の要件などのほか，設計時の記法などについて記載を行った。

表１　主なレビュー手法

手法	特徴
インスペクション	・もっとも厳格なレビュー ・参加者の役割が決まっている ・計画に基づいて実施される ・作成者が進行役や説明役になることはできない ・議事録，手順書，ガイドラインが必須 ・マイルストーンごとのレビューとして最も適している ・含まれる工程：計画，概要説明，準備，レビュー，修正，検証
チームレビュー	・参加者の役割が決まっている ・作成者が進行役や説明役になることができる ・説明者が作業成果物をチームメンバーに説明する ・マイルストーンごとのレビューに適している ・含まれる工程：計画，準備レビュー，修正
ウォークスルー	・参加者の役割は決まっていない ・手順の定義は必要ない ・作成者が作業成果物を参加者へ説明する ・設計手法やテスト手法に適する ・含まれる工程：計画，レビュー，修正
ペアレビュー	・評価者が１名で実施 ・作成者がレビューに同席しない場合もある ・手順の定義は必要ない ・コードの誤字・誤植チェックなど，低リスクの作業成果物のレビューに適している
パスアラウンド	・作成者が作業成果物をレビュー実施者に配布し，フィードバックを受ける ・対面形式レビューが困難なときに適している ・含まれる工程：レビュー，修正，検証
アドホックレビュー	・即席のレビュー ・個人レベルにおける確認で使用される ・作業成果物などに自由な意見を求めることに適している ・含まれる工程：レビュー，修正

４　ハードウェア・ソフトウェア安全設計

システム設計が終われば，次は HW, SW の設計プロセスを進め，HW, SW の設計，開発，実装を行う。システム設計において策定した安全要求仕様を基に，HW, SW に求められる HW 要求仕様，SW 要求仕様を決定し，HW, SW それぞれに安全要求仕様を定める。この HW, SW の安全要求仕様に基づいてアーキテクチャ設計，詳細設計，実装を行う。併せて，HW, SW の間のインタフェースについても安全要求仕様を考慮して仕様を決定し実装する。

これら HW, SW の設計を行う際の手法として，自動車業界ではモデルベース開発が標準的に用いられている。モデルベース開発は，機能安全に対応した開発プロセス

だけでなく，ソフトウェアを含むシステムの品質向上を図る上でも有効であることから，組込みシステム開発の際には活用を検討すべきである。作成した手順書では，これら一連のプロセスフローについてまとめたほか，モデルベース開発手法を用いる際の開発プロセスなどを記載した。

5　実証モデルによる評価

これまで述べた開発プロセスのうち，システム設計に関する内容の妥当性を評価するため，実際に開発対象として自転車をベースとした電動４輪車を選定し手順書に従って開発を行った。**表２**に電動４輪車の主な仕様を，**図２**に電動４輪車のイメージ図を示す。今回，電動４輪車を対象としたのは，昨年度の研究で電動４輪車を対象としたリスク分析，ハザード解析を行っておりその知見を生かせること[4]，自転車がベースであり機構やシステム構成が理解しやすいこと，コンセプト設計，システム設計を行った後，実際に試作して検証できることが理由である。

この電動４輪車について，今回作成した手順書に従い，次の項目を実施した。

(1) システム定義

対象を構成している個々のシステムについて，構成内

表２　電動４輪車の主な仕様

諸元	仕様
構成	自転車の後部に２輪の駆動機構部を接続した４輪車
駆動機構部構成	駆動ユニット，制御ユニット，電源ユニット，フレーム
駆動方式	ダイレクトドライブ方式
モータ	ブラシレス DC モータ
モータ制御	マイコンによる速度制御
電源	直流 24V 鉛蓄電池（自動車用 12V）利用
寸法	駆動機構部分 600㎜×400㎜ 程度
操縦方法	自転車のハンドル部にスピードコントローラを実装
最高速度	25km/h

図２　電動４輪車　イメージ図

アイテム: 2. 制御ユニット
アイテムの機能: 1. 駆動ユニットを制御する

潜在的故障モード	Max Sev	ハザード	程度	Class	潜在的な原因 / 故障のメカニズム	発生頻度	現在の設計コントロール（予防）	現在の設計コントロール（検出）	検出難度	RPN
MOSFETの損傷	9	異常加熱によるMOSFETの損傷・発火	9		過負荷による過電流	5	ヒューズ実装（３０A）	なし	4	180
		駆動ユニットが動作しない	8		ヒートシンクの取り付け不良	3	目視確認	目視確認	5	135
					石などの飛来物による破損	4	なし	なし	10	360
					MOSFETの取付不良	3	目視確認	目視確認	3	81
					配線ミス	4	目視確認	目視確認	3	108
センサ破損	8	駆動ユニットが動作しない	8		ホール素子不良	2	なし	なし	3	48
					石などの飛来物による破損	3	なし	なし	10	240
					モータとの物理的接触による破損	2	目視確認	目視確認	6	96
ヒューズ断	5	制御ユニットが動作しない	5		過負荷による過電流	5			2	50
					過負荷によらない過電流	3			2	30
					ヒューズの不良	3			2	30
マイコンの異常過熱	10	制御ユニットが動作しない	8		周辺環境温度異常	3			2	60
		駆動ユニットが動作しない	8		過電流	4	ヒューズ実装（３０A）		4	160
		速度が制御できない	10		マイコンの取付ミス	3	目視確認	目視確認	3	90
		電源のON/OFFができない	8							
		電力が回生されない	6							
マイコンの損傷	10	制御ユニットが動作しない	8		過負荷による過電流	5	ヒューズ実装（３０A）		4	200
		駆動ユニットが動作しない	8		プログラムミス	7			5	350
		速度が制御できない	10		過電圧	3	なし	なし	5	150
		電源のON/OFFができない	8		配線ミス	4	目視確認	目視確認	3	120
		電力が回生されない	6							
基板のへこみ	10	制御ユニットが動作しない	8		石などの飛来物による破損	4	なし	なし	10	400
		短絡による発火	10							
基板脱落	9	基板損傷	8		取付不良	3			3	81
		動かない　走行不能	9		固定部のゆるみ	2				
駆動ユニットからのセンサ信号入力ケーブルの損傷・断線	8	駆動ユニットが動作しない	8		駆動ユニットとの物理的接触	2	目視確認	目視確認	6	96
		短絡			石などの飛来物による破損	4	なし	なし	10	320
					過負荷による過電流	5	ヒューズ実装（３０A）		4	160

図３　FMEA によるハザード分析

容，システムの範囲，システム同士の依存関係をシステム定義書及び相関図に定義した。

(2)ハザード分析及びリスクアセスメント

システムごとに，起こり得るハザードとその発生原因を分析した。今回，分析には FMEA(Failure Mode and Effect Analysis)を用い，ツールとして IHS 社の FMEA-Pro を利用した（**図３**）。FMEA によってハザードの発生原因を特定した後，そのハザードの発生時に起こり得る危険事象と，その際のシステムの動作状況，回避可能性及び人的被害について想定を行った。この想定に基づいて動作状況，回避可能性及び人的被害のレベル分けを行うとともに，検討結果についてウォークスルーによるレビューを行い，結果に基づいて想定の追加，修正を行った。

(3)安全目標の決定

(2)で検討したハザードと動作状況，回避可能性及び人的被害のレベル分けを基に，ハザードごとに安全目標を定め，この安全目標を満たすための安全要求仕様を決定した。ここで決定した安全要求仕様としては，電源ユニット，制御ユニットそれぞれへの過電流防止ヒューズの実装や，システム異常の際に主電源を切断できるスイッチの実装などである。

これら決定した安全目標，安全要求仕様が妥当かどうかについてウォークスルーによるレビューを行うとともに，レビューで修正が必要と判断された安全要求仕様を修正した。

この一連のプロセスにより，安全性が要求されるシステム開発に求められる成果物が一通り作成可能なことが確認できた。

６ 結　　言

コンセプト設計，システム開発，HW／SW 開発のそれぞれの段階における手順書を作成し，システム設計について実証モデルによる評価を行った。今後は，作成した手順書をもとに，車載電装品を対象とした実証試験を通じて，実際の製品開発で利用可能な手順書に改善するとともに，妥当性について検証する。

文　　献

1) 広島県：ひろしまカーエレクトロニクス戦略，2008

2) Jaspar WebSite - JasPar 規格文書一覧：https://www.jaspar.jp/outcome/1307_index.html

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) 倉本他：広島県立総合技術研究所西部工業技術センター研究報告，56(2013)，8

5) ビジネスキューブ・アンド・パートナーズ：ISO26262　実践ガイドブック[入門編]　日経 BP 社，2012