１　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３報）
機能安全開発手順の実証試験

倉本丈久，弓場憲生，後藤孝文，門藤至宏

Improvement of safe system development process for electronic module using vehicle applications (3nd Report)
Validation of system development process for functional safety

KURAMOTO Takehisa, YUBA Norio, GOTOH Takafumi and MONDOU Munehiro

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

ISO 26262 defines functional safety of electrical or electronic systems within road vehicle. However, 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 proximity sensor which is similar electronic systems within road 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，本来の走行性能に加えて環境性能などに代表される付加価値向上が求められており，これらの機能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する傾向にある[1)]。

一方で，これらの機能を制御するソフトウェアに生じた不具合により自動車事故が発生するなど，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 年に発効した。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状況である。

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適用させるための方策が求められている。

そこで本研究では，安全性の高い組込みシステムを実現するために，昨年度までに機能安全規格に準拠した開発プロセス実現のための手順書を作成した[2)]。安全への要求を策定・実装し，検証するプロセスの概要図を**図１**[3)]に示す。本報では，この手順書の実証試験として行った，車載電装品を想定したコーナーセンサ（障害物との距離を検知し，障害物の接近を運転者に警告する装置）の設計，開発及びその検証について報告する。

なお，手順書作成及び実証試験に当たっては，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[4)]を参考にした。

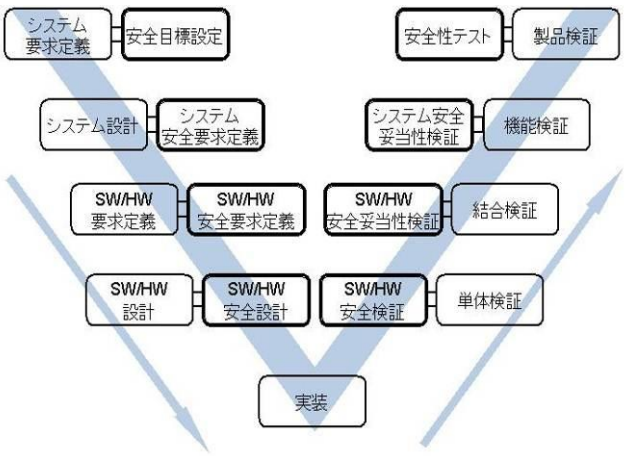

図１　安全性を考慮した開発プロセス

2　手順書の実証モデル

安全性を考慮した開発プロセス実施のための手順書の実証試験として，コーナーセンサの設計及び試作機作製を行うこととし，設計の前提条件となる機能レベルの基本設計，安全設計，安全目標，機能安全要求仕様，ランダムハードウェア故障に対する目標値をそれぞれ設定した。このコーナーセンサは，自動車を模擬した電動カートへの実装を想定し，仕様を設計した。その基本仕様とシステム図を**表１**及び**図２**に示す。障害物とセンサが一定距離以内になった場合に，LED 及びブザーで運転者に警告を発するほか，車速と障害物との距離がそれぞれ入出力される仕様である。

表１　コーナーセンサ　基本仕様

機能	仕様
障害物近接時の警報機能	車両フロント 2 箇所に取り付けたセンサ（左右）と障害物との距離を計測し，距離に応じて警報を発する。 距離 1m 以上：警報なし 距離 50cm 以上 1m 未満：LED 点滅（遅）及びブザー発報 距離 20cm 以上 50cm 未満：LED 点滅（速）及びブザー発報 距離 20cm 未満：LED 点灯及びブザー発報
システムの起動表示機能	システム ON 時に LED（PowerLED）点灯。 障害物近接時の警報機能有効時に LED(SystemONLED)点灯。
一定以上の車速でのシステム停止機能	車速が 10km/h 以上の場合，警報機能を Off に設定し，LED(SystemONLED)消灯により運転者に通知。
エラー警報機能	センサの不具合を検知した場合，LED(ErrorLED)を点灯。
センサと障害物との距離の出力機能	検知したセンサ（左右）と障害物との距離を外部へ出力。

3　開発プロセスに沿った適用

3.1　システム設計から SW/HW 要求定義まで

前節で述べたシステム開発の前提条件をもとに，手順書に従ってシステム設計，安全分析（システム FTA），技術安全要求仕様を策定した。さらに，安全機能を含むシステム設計及び技術安全要求仕様のハードウェア／ソフトウェアへの配置を行った。システム設計の過程で，システムクラス図，シーケンス図，状態遷移図など UML(Unified Modeling Language)による設計が求められるため，本研究では UML 設計ツールとして Sparx systems 社の Enterprise Architect を用いて設計した。手順書では，これら作成した内容についてのレビューを行い，結果を文書化するよう指示されている。そのため，作成した内容について一般的なレビューによく用いられる手法であるウォークスルー（設計の担当者と評価者数名程度で検証を行う手法）によるレビューを行った。その結果，警報用 LED の見落としによるハザード回避の必要が生じたため，音による警報装置を追加したほか，安全分析，シーケンス図について修正箇所が見つかったため，修正履歴を明示して成果物を修正した。

3.2　ハードウェア(HW)設計

前節で作成したシステム設計の成果物から，ハードウェア要件部分の設計を手順書に従って実施した。ここではハードウェア基本設計，ハードウェア安全分析，ハードウェア安全要求仕様，ハードウェア安全設計を行い，それぞれ文書化する工程が必要となる。ハードウェア作成に用いる部品のリストや，部品ごとの目標故障率等も規定する必要がある。これらの過程で作成したコーナー

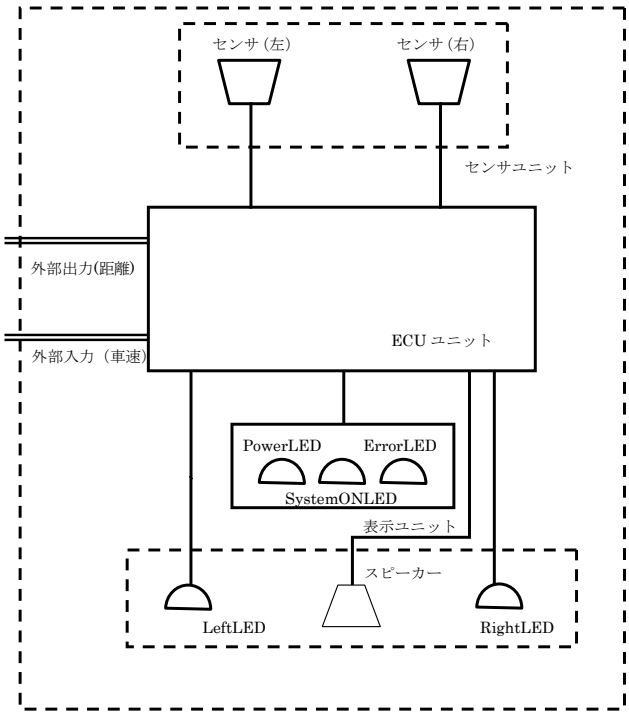

図２　コーナーセンサ　システム図

センサ用の回路図を**図３**に，ハードウェアアーキテクチャ図を**図４**に示す。また，手順書に従い設計した成果物のレビューをウォークスルーにより実施し，結果を文書化した。

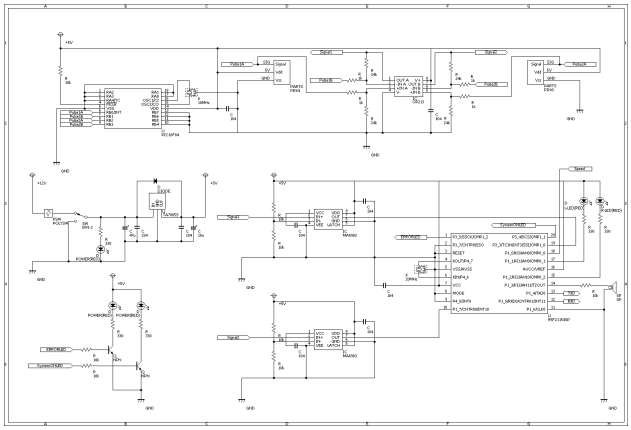

図３　コーナーセンサ用回路図

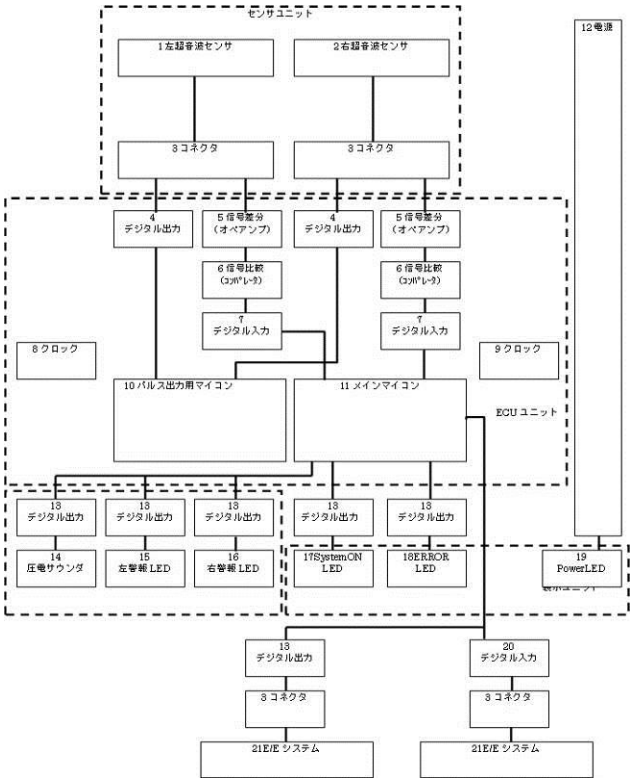

図４　ハードウェアアーキテクチャ図

3.3　ソフトウェア(SW)設計

3.1 節で作成したシステム設計の成果物から，ソフトウェア要件部分の設計を，手順書に従って実施した。ここではソフトウェア基本設計，ソフトウェア安全分析，ソフトウェア安全要求仕様，ソフトウェア安全設計を行い，それぞれ文書化する工程が必要となる。ソフトウェアで用いる定数の定義やデータ型，関数定義などもすべて規定しておく必要がある。その過程で作成したソフトウェアアーキテクチャ図を**図５**に，制御モデルを**図６**に示す。ISO26262 においてモデルベース開発が推奨されていることもあり，制御モデル作成には，モデルベース開発ツールとして自動車業界で標準的に利用されている Mathworks 社の MATLAB/Simulink を用いた。モデルベース開発を導入することにより，作成したモデルでシミュレーションを行い，挙動や動作タイミングなどを確認することが可能となる。今回の実証試験でも，ソフトウェアの検証にモデルを基にしたリアルタイムシミュレーションを活用した。

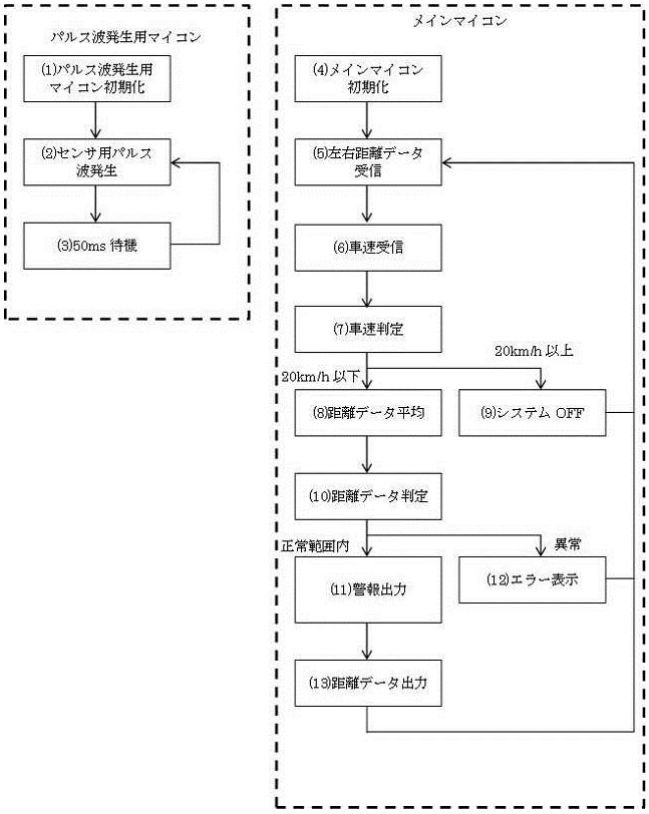

図５　ソフトウェアアーキテクチャ図

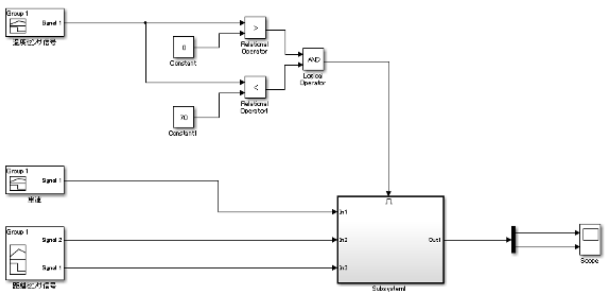

図６　制御モデル

3.4　実装及び安全性テスト

3.2節で作成したハードウェアの仕様に従ってコーナーセンサ用回路を作製した。作製した回路を**図７**に示す。また，前章で作製したソフトウェアの仕様に従って，この回路上のマイコンに実装するためのコードを作製した。これらハードウェアとソフトウェアが仕様通りに機能するかどうかについて，それぞれの仕様に対するテスト項目を作成し，テストを実施した。ここでは，手順書に従ってテストの項目や実施方法について規定するとともに，その実施内容や結果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い，文書化した。

ハードウェアとソフトウェアの作製及びテストが完了した後，システムとしてのテストを行った。テストは，実証モデルの仕様どおり，自動車を模擬した電動カートに回路を実装した状態で実施した。その様子を**図８**に示す。ここでは，テスト項目と実施方法などについて規定するとともに，安全異常が検出された場合に採る手順や，検証済みの内容について変更した際の再度の検証方法などについて規定し，文書化した。その後，規定した方法に従ってテストを行った。今回実施したテストは，システム起動テスト，動作電圧テスト，前方障害物認知テスト，側方障害物認知テストなど，システム仕様で規定した安全設計が検証できる内容について実施している。その結果，テスト項目について基本仕様の基準を満たすことが分かったため，合格と判断した。さらに，テストの項目，実施方法及び結果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い，結果を手順書に従って文書化した。

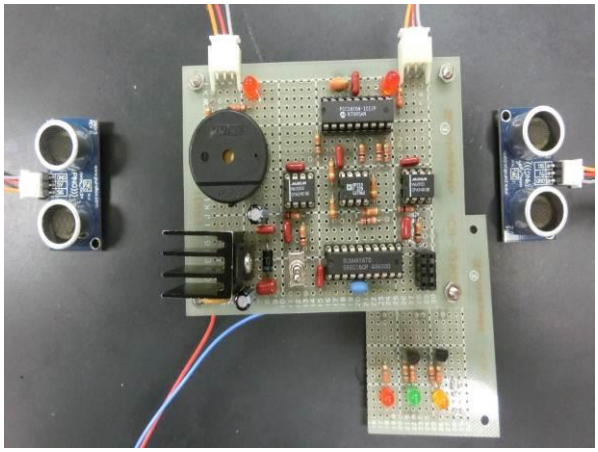

図７　試作した回路

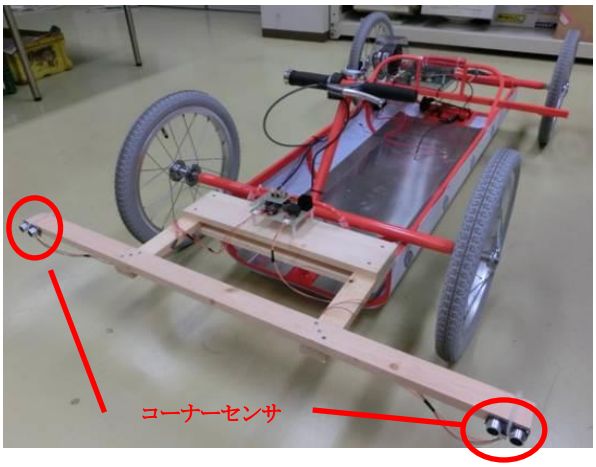

図８　電動カート実装状態

以上のことから，システム設計からシステム作成，テストまでの工程で必要な成果物を，手順書に従って作成できることが示せた。

４　結　　言

機能安全規格を考慮したシステム開発，ハードウェア開発，ソフトウェア開発及びそれらのレビューやテストについて，昨年度までに作成した手順書により実施可能であることを示した。今後は，作成した手順書について，実際の企業現場における機能安全規格準拠のためのツールとして利用できるよう改善を行うとともに，普及に努める。

文　　献

1)　広島県：ひろしまカーエレクトロニクス戦略，2008
2) 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，57(2014)，5
3) 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
4) Jaspar WebSite - JasPar 規格文書一覧：https://www.jaspar.jp/outcome/1307_index.html