

車両用エンジン制御系ソフトウェアの設計品質管理

Design Quality Management for Vehicle Engine Control Software

○戸水晴夫（正, SDI Japan, Haruo Tomizu）

1 はじめに

車両用のエンジン制御を行うソフトウェアは、ECM（Engine Control Module）と呼ばれる制御基板上に実装した数個のマイクロコンピュータに、組み込みソフトウェアとして書き込まれる。現在、8, 16, 32 ビット CPU を用いたマイクロコンピュータが主流である。それらに組み込まれているソフトウェアは、おおよそコードと称するアルゴリズムと制御データの2つから構成される。そして、センサーからの信号によって設定された条件下で制御を行う。判断する基準は、不揮発性メモリ ROM（Read Only Memory）上にある制御データであり、それらはROMパラメータまたはROM定数といわれる。パラメータ値の設計は、一般にはExcel®などのスプレッドシートに記述されて、検討される場合が多いが、実際のスプレッドシートの行数は数万行にもなることがあり、人間による間違いが多い現状である。¹⁾

本報では車両用ガソリンエンジン制御系のROM定数の量産適合作業における不具合対策に従来のSDI ToolsをカスタマイズしたEPD（Enhanced Product Development）を適用した内容を紹介する。但し、ROMパラメータ自体は自動車会社の核心的ノウハウであり、社外秘であるため、ここでは品質を検証する仕組みについてのみ紹介することとする。

2 エンジン制御系ソフトウェアの不具合

エンジン制御を行うソフトウェアで起きる不具合について、国内メーカーで発生した過去の事例を図1

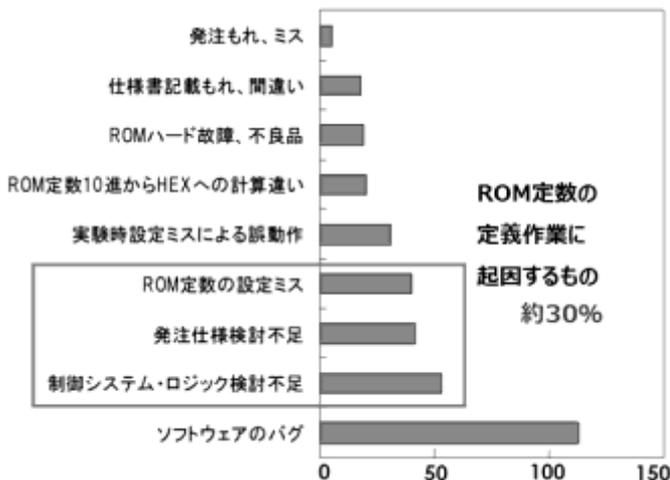


図1 制御系ソフトウェア不具合の発生例

に示した。この例の場合では、ソフトウェアのコーディングそのもののバグは35%あった。一方で、コーディング前に行うROM定数の定義作業が原因の不具合は、約30%近くになることが分かった。これは、定義が間違っていれば、コーディングの不具合がさらに多くなることが予測され、これら事前の定義作業の品質向上こそが、今後の最も重要な改善項目であると判断された。

2.1 ソフトウェア不具合の発生状況の調査

エンジン制御系のソフトウェアの品質不具合の発生状況を調査してみると、以下が挙げられた。

- (1) 制御システムが複雑・多岐にわたるため、機能の相互干渉を抽出できない。そのために起きた。
- (2) タイミング問題は、制御システム検討やロジック検討、発注仕様検討に共通しており、あらゆる組合せでの検討が不足しているために起きた。
- (3) 異常値、外乱ノイズに対する検討が十分でないために起きた。
- (4) ハードの変更時の影響が把握できていないために不整合が起きた。
- (5) 制御パラメータ適合手順を把握しきれないために起きた。

実際には、MATLAB/Simulink®などのシミュレーションツールを使用し、不具合が発生しないように適合作業を行っているが、それでも発生している。

2.2 ソフトウェア品質不具合の原因の特定

まず、機能の相互干渉を抽出できなかった理由には4つあり、ひとつは要求性能/機能を本質まで言及していなかったためであり、さらに要求機能を実現できていることを検証できなかったことによる。あるいは、最も合理的な制御であることを証明できなかったためと考えられた。それらの原因はQFDやAHPの検討が不十分であったからと分析された。また、別性能・別制御・診断への影響を見つけれなかったというのはFMEAの検討が不十分であったためとされた。2番目の場合の、あらゆる組み合わせを検討できなかった理由としては、考えるべき状態を全て抽出できていないことと、過去不具合モードに関する検討ができていなかったためと分析された。これらもFMEAの検討が不十分だったことが原因である。3番目の場合の、異常値、外乱ノイズに関する

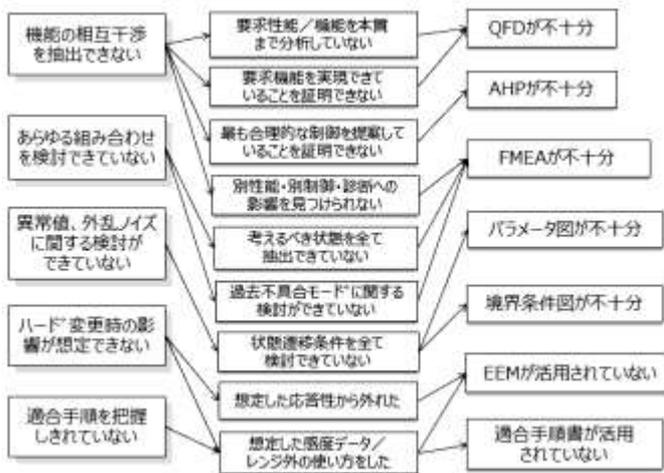


図2 制御系ソフトウェア不具合の対策例

検討ができていなかった理由は、状態遷移条件を全て検討できていなかったためと分析された。これはパラメータ図²⁾ (Parameter Diagram) と境界条件図 (Boundary Diagram) が不十分だったことが原因とされた。4番目の場合の、ハード変更時の影響が想定できなかった理由は、想定した応答性から外れたためと分析された。また、近年は車両の効率化のために極めて多数の電子コンポーネントが使われている。それらのエネルギー管理を担う電子エネルギーマネジメント³⁾ (EEM: Electronic Energy Management) が不十分だったことが原因である。5番目の場合の、適合手順を把握しきれなかった理由は、想定した感度データ/レンジ外の使い方をしたためと分析された。適合手順書が十分に活用されていないことが原因だった。結局、全ての不具合は、図2の一番右に記述した7項目に原因があったと結論された。

3 SDI Tools EPD を使用した分析プロセスの提案

ECM 開発における制御系ソフトウェア設計の場合、不具合の原因となる根源的なリスクを仕様段階

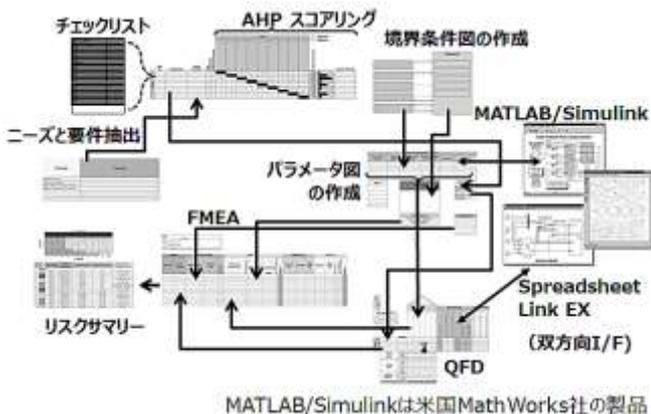


図3 SDI Tools EPD 分析プロセスの全体像

から洗い出し、排除するための機能が弊社 SDI Tools には不足していた。特に、全ての ECM に関する電子コンポーネントの境界条件図とパラメータ図を作成し、階層化ルールをもれなく記述する必要があった。また、MATLAB®のサブシステム単位に置き換えてシミュレーションによる検証ができるようなインタフェースを制作する必要もあった。そのため、ROMパラメータの相互作用をより厳密に記述できる SDI Tools EPD 製品を新たに開発することになった。

SDI Tools EPD は、設計初期段階においてパラメータを定義するプロセスを重視した分析手法を提供する。そのメソッドロジは連続的で、Stakeholder, Affinity, AHP, Boundary Diagram, Parameter Diagram, Link EX I/F, QFD, DFMEA, PFMEA, Risk Management. のツールを使用するものである (以降、ツール名に関しては英名で記述するものとする)。また、作成されたデータは Excel®のワークシート間を自動的に受け渡される。図3に SDI Tools EPD 分析プロセスの全体像を示す。その特徴は、はじめに要件抽出を行い、階層分析 AHP で要件の重要度を求める。そして、Boundary Diagram で境界条件図を作成し、それをもとに、Parameter Diagram で入出力や判断条件をパラメータ図に集約することである。また、MATLAB®を使用してシミュレーションによる検証を行う。その結果は、QFD のワークシートに転送される。最後に、QFD の項目をもとに FMEA を使って故障モード影響解析を実施する。その後、ユーザーに見やすい形のリスクサマリーシートとして結果がレポート出力される。

4 SDI Tools EPD をエンジン制御系システムの酸素濃度センサーへ適用した例

ここからは、具体例をもとに SDI Tools EPD を使用した設計品質を確保する手順についての説明をおこなう。題材はエンジン制御系システムにおいて重要な役割をはたしている酸素濃度センサーの設計とした。酸素濃度センサーは通称 O₂ センサーと呼ばれる電子部品であり、エンジン燃焼後の排気ガス中の酸素濃度を検出するセンサーである。通常は排気マニホールド後ろに設置されるものである。この O₂ センサーはエンジンの燃焼効率を測る指標である空燃比を ECM に計算させてインジェクターにおけるガソリン噴射量のフィードバック制御に使われている。

Stakeholders		Team Members
Project:	O ₂ センサー診断変更	エンジン担当、部品担当、制御SE、
Program:	低燃費PJ	ECM担当
Facilitator:	設計品質改革室	
Date:	4/25/2010	

Stakeholders	Group	Comments
顧客担当	東日本	O ₂ センサー不良で燃費が低下するクレームあり
販売ディーラー	EU	高負荷運転の割合が多く燃焼寿命低下がはやい
台上試験部門	中部	理論空燃比に改善の余地あり
工場	US	車種別の燃焼時間が異なるため標準化希望
サプライヤ	欧社	定期交換で最大15%燃費向上

図4 ステークホルダーの意見集約



図5 設計要件の重要度の数値化

4.1 ステークホルダーの意見の集約

開発プロジェクトを開始するにあたっては、現状でどのようなクレームや問題提起がステークホルダーと呼ばれる利害関係者から出ているかを調査し、まとめることが必要になる。設計部門だけではなく、多くの関係者からの意見を顧客要件として優先順位を付けて設計に反映させることが重要だからである。図4にStakeholdersワークシートを示す。

4.2 要件の重要度を階層分析で数値化

設計要件について、どれを重視して開発を進めていくかを、階層分析AHPを使用して重要度を計算し、順位付けを行う。図5に作成したAHPワークシートを示す。

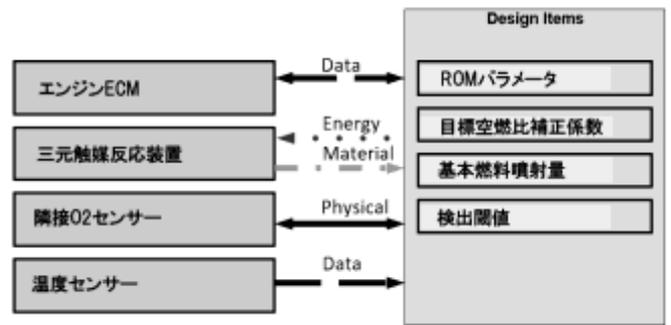


図6 境界条件図に外乱要因を定義

4.3 設計項目に影響を与える外乱要因を定義

設計項目に外部から影響を与える外乱要因を境界条件図に定義する。いま、検討すべき項目は、ROMパラメータ、目標空燃比補正係数、基本燃料噴射量、検出閾値の4項目である。これらはいずれもエンジンの燃焼をコントロールするものであるが、図6に示したように、エンジンECM、三元触媒反応装置、隣接O2センサー、温度センサーから得られる複合的なデータと相互干渉してノイズとなる場合がある。

4.4 パラメータ図にすべての関係性を定義

図7に示したパラメータ図のワークシートにすべてのパラメータの関係性を記述し、QFDとFMEAに出力する項目のエントリーを行う。そして、入出力条件を定義し、システムの境界条件を明確にし、設計項目に関するコントロール要因と外乱要因を記述する。

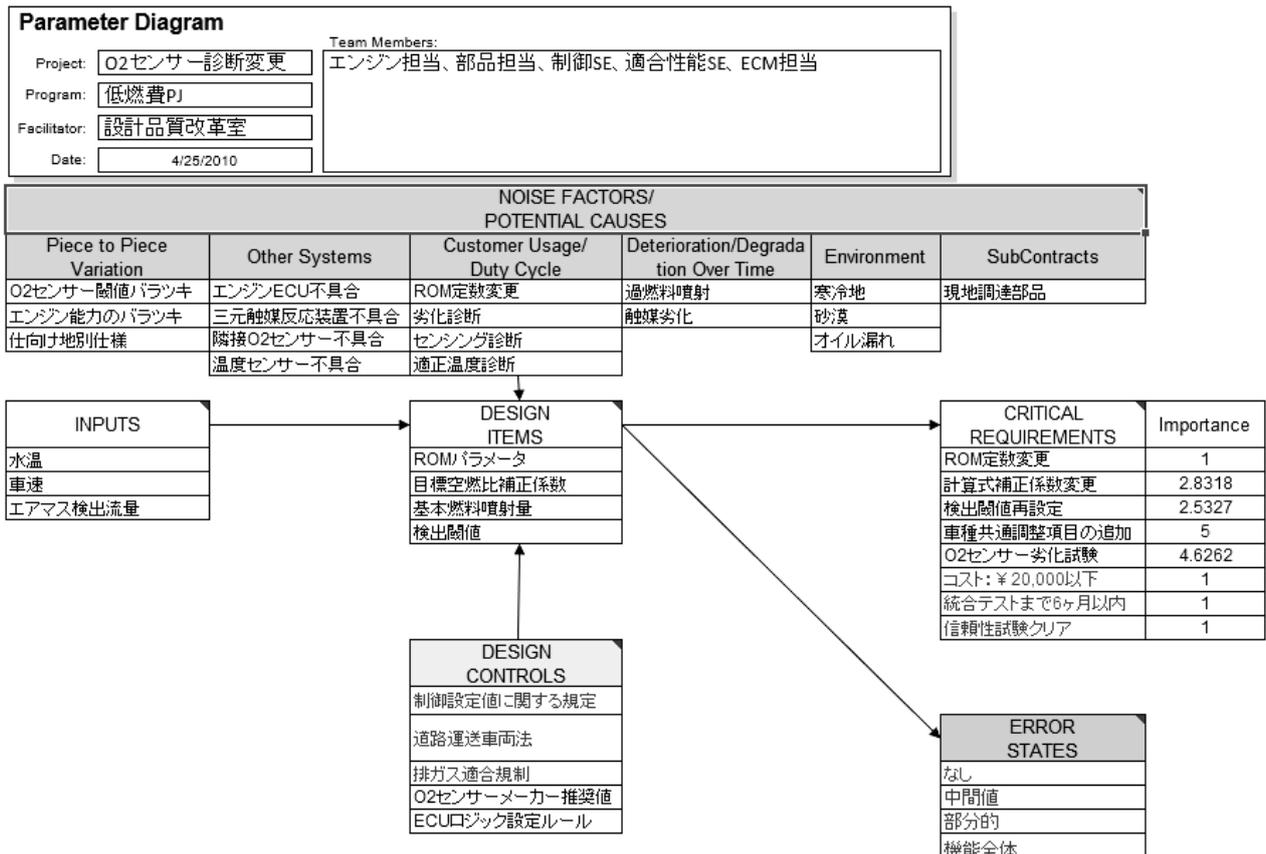


図7 パラメータ図に関係性を定義

特に、設計項目に渡されるデータとして、入力信号、外乱、設計規定があり、そこから設計要件とエラーステータスが出力される。外乱の区分としては、個別の要因によるもの、他のシステムからによるもの、検査などによる要因、劣化や経年変化の要因、環境要因、調達条件によるものなどが検討される。

4.5 品質表に要件と重要度を渡して技術項目を検討

図8に示すように品質機能展開QFDのWhat項目に、パラメータ図からCritical Requirementsの記述項目と重要度importanceの数値が自動で転記される。そして、How項目は、What項目に関するO2センサー一定数項目や診断項目をあてはめる。重要度の高いHow項目についてはMATLAB®へ渡してROMパラメータの検証シミュレーションを行う。

4.6 FMEAで故障モードの分析結果をレポート

故障モード影響解析FMEAワークシートの大項目はROM再設定とした。小項目は、ROM定数変更、計算式補正係数変更、検出閾値再設定である。ROM定数を変更しなければならない場合とは、エンジンECM、三元触媒反応装置、隣接O2センサー、温度センサーとの相互作用によって不具合がある場合であり、それぞれの故障の現象が記述される。FMEA Risk Summaryと呼ばれるレポートは、不具合を是正するアクションだけを取り出し、リスクとなる項目を優先順にレポートするので、誰にも分かりやすい報告書となっている。図9中に出力例を示す。

5 おわりに

制御系ソフトウェアの開発プロセスにSDI Tools

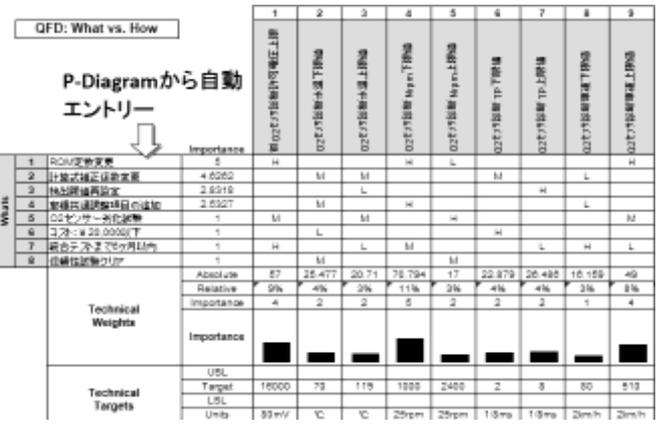


図8 要件を技術的項目にブレイクダウン

EPDを適用して、ソフトウェア特有の要件定義と外乱管理ができるようにした。特に、パラメータ図を導入したことによって、QFDとFMEAへの出力項目をすべて列挙し、リスク特定機能を強化して、潜在的な不具合要因を追及できるようにした。また、MATLAB®に対応したインタフェースを提供した。その結果、車両用エンジン制御系ソフトウェアのROM定義作業における不具合を早期設計段階で特定する手法を提供することができた。

参考文献

- 1) 菅沼賢治：自動車組み込みソフトウェアの現状、ソフトウェア工学, 134, 13, (2001), 47.
- 2) J. M. Juran, Frank M. Gryna, Jr. : Quality Planning and Analysis, TATA McGraw-Hill Publishing Co. LTD., (1982), 167.
- 3) C. Lungoci, A. Galuszkam, M. Georgescu : Energy Management in Automotive, Wydawnictwo Politechniki Śląskiej Gliwice, (2018), 41

FUNCTIONS		POTENTIAL FAILURE MODES				POTENTIAL CAUSES				
Item / Function	Sub-Item / Sub-Function	Potential Failure Mode	Potential Effects of Failure	SEVERITY	Potential Causes / Mechanisms of Failure	OCCURRENCE	Current Design Controls Prevention	DETECTABILITY	RPN	
ROM定数変更	ROM再設定	エンジンECU不具合	アイドル回転時のハンチング現象	4	トルク出力異常発生	3	アイドル燃空比変更	5	60	
		三元触媒反応装置不具合	冷燃時のガスつき、カブリつき	4	始動時水温下がり遅延	3	キャブレター設定値変更	5	60	
		隣接O2センサー不具合	検出閾値再設定	4	検出閾値再設定	3	検出閾値再設定	5	60	
		温度センサー不具合		4		3		5	60	
ROM再設定	計算式補正係数変更	No	S	O	Item / Function	Sub-Item / Sub-Function	Potential Failure Mode	Potential Effects of Failure	Potential Causes / Mechanisms of Failure	
		1	4	3	エンジンECU不具合	エンジンECU不具合	エンジンECU不具合	アイドル回転時の不制御	判定開始平均値演算回数不足	
		2	4	3	三元触媒反応装置不具合	三元触媒反応装置不具合	三元触媒反応装置不具合	アイドル回転時のハンチング現象	トルク出力異常発生	
		3	4	3	隣接O2センサー不具合	隣接O2センサー不具合	隣接O2センサー不具合	冷燃時のガスつき、カブリつき	始動時水温下がり遅延	
		4	4	3	KDUTY変化不具合	KDUTY変化不具合	KDUTY変化不具合	生ガス量多岐の燃焼ガス	失火(始動許可条件Nrpmと燃空比オーバー)	
		5	5	3	ALPHA(α)変化不具合	ALPHA(α)変化不具合	ALPHA(α)変化不具合	燃費の悪化	燃費の悪化	
		6	7	8	MNRPM変化不具合	MNRPM変化不具合	MNRPM変化不具合	シッキングの発生	燃費の悪化	
		7	2	2	TP変化不具合	TP変化不具合	TP変化不具合	アイドル回転時のハンチング現象	燃費の悪化	
		8	2	2	KBLRC(κ)変化不具合	KBLRC(κ)変化不具合	KBLRC(κ)変化不具合	シッキングの発生	燃費の悪化	
		9	9	8	O2センサー検出値不具合	O2センサー検出値不具合	O2センサー検出値不具合	シッキングの発生	燃費の悪化	
		10	5	4	O2センサー検出値不具合	O2センサー検出値不具合	O2センサー検出値不具合	シッキングの発生	燃費の悪化	
		11	5	4	前O2センサー検出値不具合	前O2センサー検出値不具合	前O2センサー検出値不具合	シッキングの発生	燃費の悪化	
12	5	5	O2センサー検出値不具合	O2センサー検出値不具合	O2センサー検出値不具合	シッキングの発生	燃費の悪化			
検出閾値再設定	検出閾値再設定	前O2センサー検出値不具合	燃費の悪化	4	燃費の悪化	4	燃費の悪化	4	4	
		O2センサー検出値不具合	燃費の悪化	4	燃費の悪化	4	燃費の悪化	4	4	
		前O2センサー検出値不具合	燃費の悪化	4	燃費の悪化	4	燃費の悪化	4	4	
		O2センサー検出値不具合	燃費の悪化	4	燃費の悪化	4	燃費の悪化	4	4	
		前O2センサー検出値不具合	燃費の悪化	4	燃費の悪化	4	燃費の悪化	4	4	
		O2センサー検出値不具合	燃費の悪化	4	燃費の悪化	4	燃費の悪化	4	4	
		S: SEVERITY								
		O: OCCURRENCE								

図9 FMEAで故障モードの分析を行った後に結果をレポート