2006－EMB－1（2）
2006／6／27

組込みシステムの動作環境の特徴に着目した仕様分析手法の提案

鷲見毅† 平山雅之† 鵜林尚靖‡
†株式会社東芝　ソフトウェア技術センター
‡九州工業大学　情報工学部　知能情報工学科

組込みシステムは様々な環境で多様な用途に利用されるため、その要求分析ではシステムの動作を網羅的に洗い出すことが重要となる。また、多様な環境で利用される組込みシステムは、利用される環境によって処理内容が異なる場合がある。その為、要求分析段階でシステム外部の環境を考慮する必要があるが、そのための手法は必ずしも十分に整備されていない。この結果、組込みシステムを対象としたシナリオでは、網羅率を上げることが極めて難しくなっている。

本稿では、組込みシステムの外部環境を考慮し、そのクラス分析を通して外部環境のシステムへの影響を洗い出す基本的な考え方を提案し、これを用いて網羅的なシナリオ作成を支援する手法を提案する。

A proposal of specification analysis technique for embedded software focusing on their operating environment

Takeshi SUMI†, Masayuki HIRAYAMA†, Naoyasu UBAYASHI‡
†TOSHIBA Corporation, Software Engineering Center
‡Department of Artificial Intelligence, Faculty of Computer Science and System Engineering, Kyushu Institute of Technology

In the development of the embedded system, it is important to clarify the system operation in the requirement analysis phase because the embedded system is used in various environments. The embedded system operates according to external environment. Therefore, it is necessary to consider the behavior feature of embedded system. However, the analysis technique focusing on that is not maintained enough.

In this text, we propose basic idea to clarify external environment of embedded system, and the influence of the environmental. And we propose the technique for making scenario by using this.

1. はじめに

近年、組込みソフトウェアを搭載した組込みシステムが様々な分野で利用されるようになってきている。我が国の組込みシステムの多くは、所謂、コンシューマプロダクトの形態をとることが多い。コンシューマプロダクトは、一般に利用するユーザが多岐に渡り、その利用シーンも様々な場面に広がることが特徴の一つである。一方で、こうしたユーザの多様性や利用シーンの多様性に対応するということは、言い換えると、システムの内部やそれを取り巻く外部の環境の組み合わせを意識した多様な機能を用意し実現するということと同義であると考えることができる。

このように多様な機能をシステムに盛り込む場合には、特に開発初期段階での組込みシステムとしての要求定義フェーズの作業精度が重要になる。特に、組込みシステムの場合、システムで実現する制御動作を介して、システムを取り巻く外界（外部環境）に様々な影響を及ぼすものが多い。一方で、システムを取り巻く外部環境は様々なバリエーションが存在する。このため、要求定義の段階で、システム外部の動作条件や状態のバリエーションをどこまで考慮し、適切かつ網羅的に分析し、それに対応するシステム機能を盛り込んでいくか

で、対象とするシステムの品質や信頼性は大きく異なってくる。

本稿では、こうしたシステムの外部環境のバリエーションを考慮して、システム動作に関する網羅的な分析を行う方法に関して検討を加える。

2 章では、組込みシステムの仕様分析における問題点を述べる。3 章では、組込みシステムの外部を考慮し、シナリオを網羅的に作成する為の考え方を示し、4 章でシステム外部の情報を用いて網羅的にシナリオを作成する手法を提案する。5 章で本提案手法の考察を行い、6 章でまとめと今後の課題について述べる。

2. 背景と問題点

一般に、制御を中心とする組込みシステムの場合、システムが主として提供する正常機能の他に、システムの動作環境・条件やユーザ操作に対応した様々な異常処理機能の充実が求められる。例えば、エレベータ制御ソフトウェアなどの場合、その 7 割近くが異常処理対応機能となっている。このような組込みシステムの要求分析では、如何に多くの外部環境やユーザ操作のバリエーションを考え、それらを網羅する形で要求を分析していくかがきわめて重要になっており、シナリオ分析などを利用することが近道である。シナリオ分析は想定するユーザ操作なども考慮し、システムがどのような振る舞いをするかを時系列も含めて分析しシステムの機能要求を分析評価するための手法である。このシナリオ分析法を組込みソフトウェアに適用しようとする場合、

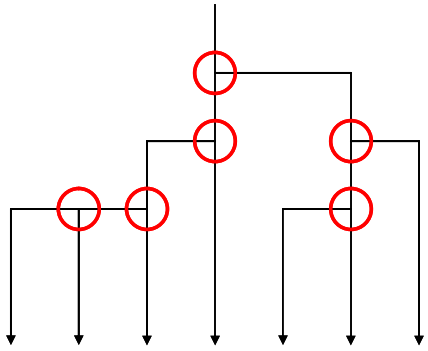
1. シナリオの網羅性に関する問題点
2. システム影響範囲の問題点

の 2 点が問題となる。

① シナリオの網羅性

通常、シナリオを用いて要求分析を行う場合には、ある特定の条件（システム内外の状態や環境、あるいはユーザ操作など）下でのある特定の一連の動作シーケンスを分析してシナリオとすることが一般的である。このため、異なる条件下では異なるシナリオとして分析されることになる。このように、一つのシナリオはシステムがおかれた特定条件下の特定の動作シーケンスを表現するものに過ぎず、言わば、システム動作のスナップショットと位置づけることが出来る。このため様々な機能や色々な異常処理動作を必要とされる組込みシステムの場合、シナリオ分析の前提とする条件の組み合わせを全て網羅する形で、様々な条件に対応するシナリオを網羅的に分析する必要がある。

またシステムの動作は図 1 に示すように、シナリオの途中においても様々な条件によって動作が分岐する場合があり、これにより別の新規シナリオを派生する場合がある。このようにシナリオ分析ではこれらの派生シナリオにも対応できる様に分析を進めていく必要がある。しかし、現状では、組込みソフトウェアの動作の背景にある様々な条件のパターンを抽出し、網羅性の高いシナリオを作成する為の具体的な手法は提案されていない。



様々な条件により複数のシナリオに分岐する

図 1：シナリオの分岐

② システム影響範囲の問題

通常、システムに対するユーザの要求は、システムの制御結果によって得られるシステム外部への影響が重視される。例えば、電気ポットを考えた場合、ユーザの要求は、ヒーターが On/Off の制御を繰り返すことによって、ポット内の液体が適切な温度に調整されるという事象が重要になる。

このため、システムの要求機能に関する動作分析の手法としてのシナリオ分析では、当該機能動作によって**「システムがその外部に対してどのような影響を及ぼすか」**、あるいは**「システム外部からどのような影響を受けるか」**を重視して分析することが求められる。

我々は、上述の 2 つの問題点を解決し、組込みシステムの要求定義フェーズでシステムの動作シナリオを効率的に分析するための手法整備を進めている。これまでの研究ではシステムの外部を分析する手法を検討し、試行評価を行ってきたが[1]、シナリオの網羅性の観点については必ずしも十分な解が得られなかった。このため、システムの外

部を分析した結果を起点として、そのとり得る条件を網羅的に組み合わせることで組込みシステムのシナリオを網羅的に作成する為の工夫が必要と判断した。

3. 手法概要

3.1 手法の狙い

組込みシステムの要求定義をより確実なものとするためには、要求段階でのシナリオ分析の網羅度を十分なレベルに引き上げることが近道である。既に述べたように、シナリオは対象システムが置かれる特定条件下での特定の動作シーケンスをスナップショット的にとらえるものである。このため本手法ではシナリオの前提となる条件を実際のシステムが置かれるであろう、様々な条件のバリエーションの数だけ設定することで、シナリオの網羅率を高めることを狙っている。

3.2 システム外部環境

本手法ではシステムを取り巻く外部環境に着目し､それらがとり得る諸条件を網羅的に抽出する。

図 3 は対象とするシステムからみた外部環境のとらえ方を示したものである。システムからみた外部環境は、制御対象、観測対象、影響要因の各クラスから構成されると考え、これらのクラスはそれぞれ複数の状態を持つことによって。結果として、外部環境の条件バリエーションが発生すると考えることができる。

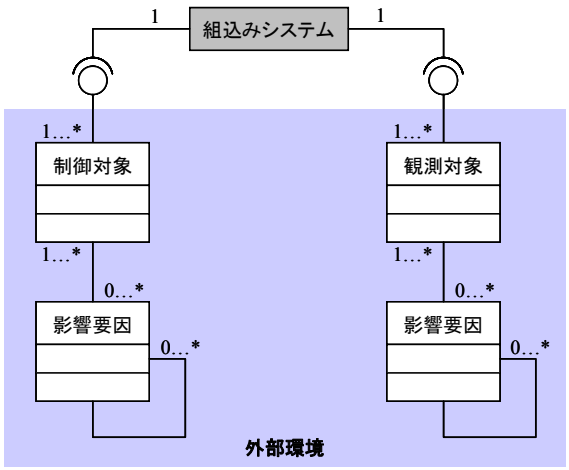


図 2：外部環境のクラス図外部環境のクラス図

制御対象：システムの要求仕様を満たす為に、システムによって制御されるデータを持つ実体

観測対象：システムが制御対象を制御する為に、センサー等の検知装置によって、積極的に収集するデータを持つ実体

影響要因：システム以外で、制御対象、観測対象が持つデータを変化させるデータを持つ実体

例えば先の電気ポットの場合、制御対象と観測対象はともにポットの水となり、具体的には水温がセンサーなどによって観測される形となる。また、この影響要因としては、水温や沸点などに影響を及ぼす気圧などを考えることができる。

3.3 外部環境の認識の差異

3.3.1 解釈系

組込みシステムの要求定義段階でのシナリオ網羅性を考えた場合、システム動作の前提となるシステムが置かれる動作環境（外部環境）の網羅性が重要な要素になる。

通常、 組込みシステムは、センサー等の検知装置によって観測対象が持つデータを観測し、そのデータから外部環境の状態を把握している。システム動作の視点でこれを考えると、**「システムはセンシングされたデータを内部で解釈することによって、システム外部がどのような状況にあるかを間接的に把握している」**と理解することができる。ここで特に重要な点は、システムはデータを解釈することで間接的に外部環境条件を把握する点である。本手法ではこうしたシステム内部におけるデータの解釈を**解釈系**と呼ぶこととする。即ち、観測されたデータを解釈する際に、場合によっては、現実世界を誤って解釈したり、正しい状況を把握しそこなったりする余地が残されている。この結果としてシナリオ分析の前提となる外部環境条件の網羅性が低くなることが考えられる。

3.3.2 解釈系に起因するシナリオ網羅の抜け

ここでは解釈系に起因するシナリオの抜けがどのようにして発生するかを例示する。

例えば、対象物の“色”が黒か白かを見分けて対応する処理を行う機能を実現するシステムを考えてみる。

方式１：システムが期待している判定結果は白黒の判別であるため直接的には対象物の“色”を直接判定するセンサーを用いる。

方式２：黒の判別を色によって行うのではなく、代替センサーとして対象物からの反射光の強度を観測し、この値によって間接的に色の白黒を判別する。

方式２の場合には、一定の反射光の強さを観測した際には色は白という解釈をシステム内部で加えることとなるが、実際には反射率の高い素材上に黄色などが塗色されている場合も、色は白と誤解釈が入る危険性を含んでおり、この場合にシステムとしての動作シナリオ検討が抜けてしまう可能性がある。

この例では、組込みシステムで観測された外部環境に起因するデータの解釈結果と、現実の外部環境の状況が、解釈系次第で必ずしも一致しないという事を示している。この為、組込みシステムの要求分析を行う場合には､現実の外部の情報を、システムが理解できている情報に変換した上で分析を行う必要があると考えられる。これは言い換えると、システムのシナリオ網羅率を上げるためには、システムの外部環境の実際の状況と、これをシステム内部でどのように捕らえているかの間の差異を極力少なくすることで、外部環境認識の差異に起因するシナリオの漏れをなくすことに他ならない。

3.4 外部環境条件の網羅（クラス図）

外部環境の正しい認識を実現するため、本手法では､対象システムに関係する外部環境を抽出し、それらをクラス図として整理する。これにより検討対象の外部環境を検討段階で見える化を進め、検討段階での抜けなどを防ぐ方式を採用している。

また､外部環境の抽出段階で先に示したように、制御対象、観測対象、影響要因といった観点を持たせることで外部環境を抽出しやすくしている。さらにこの過程でシステムに直接的な影響を及ぼさないものの、間接的に影響を及ぼす要因なども洗い出し、解釈系として分析範囲に取り込むことで外部環境の解釈系に起因するシナリオの抜けなどを極力少なくする工夫を施している。

4. Case Study

ここでは SESSAME から要求仕様が公開されている“話題沸騰ポット[2]”の「沸騰ポットの沸騰終了処理（表１参照)」を題材に、提案方式の一部を具体的に紹介する。

表 1：話題沸騰ポットの要求仕様（一部）

- 沸騰ボタンを押すと，ポット内の水を沸騰させてカルキ抜きを行う．沸騰中に押すと，沸騰を中止して保温状態になる．1回押す毎に沸騰→保温→沸騰と変わる．
- 保温設定ボタンを押すと，保温モードを高温（98℃保温），節約（90℃保温），ミルク（60℃保温）モードに設定する．1回押すごとに高温→節約→ミルク→高温とモードを変える．
- ヒーターのOn/Offによって水温を制御する．
- ヒーターは，制御周期と操作量（%）によって制御される．
- 操作量75%の時，制御周期の75%の時間だけヒーターがOn状態になる．
- 沸騰状態では，ポット内の水を加熱し，100℃に達した後も3分間加熱を続け，その後保温状態に移行する．
- 沸騰状態が終了したら，水温を98℃（節約モードでは90℃，ミルクモードでは60℃）に保つようにヒーターを制御する．
- 水温が110℃を超えた場合，ヒーター用電源をOffして30秒間ブザーを鳴らす．
- ヒーター制御中に1分毎に水温を検出し，目標温度よりも水温が5℃下がり，かつ前回検出した水温よりも今回検出した水温が低い場合，ヒーター用電源をOffして30秒間ブザーを鳴ら
- 満水センサー1つと水位センサー4つがあり，各センサーがOnの時，そのセンサー位置よりも水位が高い事になる．満水センサーOnの時は，水位が許容上限を超えている事になる．
- 第n水位センサーがOnで，かつ満水センサーがOffの場合，温度制御が可能になる．それ以外の場合には，沸騰ボタン･ヒーターは動作しない．

4.1 手法適用の流れ

提案手法は、前章で述べたように、以下のような点を特徴としている。

① 組込みシステムの外部環境抽出
② 外部環境のクラス状態の整理
③ 解釈系による外部環境認識のギャップ分析
④ 上記上を用いたシナリオ網羅性の確認

以下では、これらの特徴を踏まえて、組込みシステムの外部環境を分析、定義する事から、その情報を用いて不足するシナリオを発見する過程を紹介する。

4.2 組込みシステムの外部環境の抽出

話題沸騰ポットの沸騰終了処理に関連する動作については、表１に示した仕様を参考にすると、第一義的には制御対象、観測対象としての水（水温および沸点）を外部環境として抽出することができる。ここで､「沸点」という観測対象を考えると、水の沸点は様々な条件下で変化するという特性を持っており、例えば「気圧」といった影響要因を抽出することができる。このようにシステムが関係する外部環境をクラスとして認識し、その関係を図４のようなクラス図として表現していくことで、システムに影響を及ぼす様々な要因を比較的容易に抽出することが可能となる。

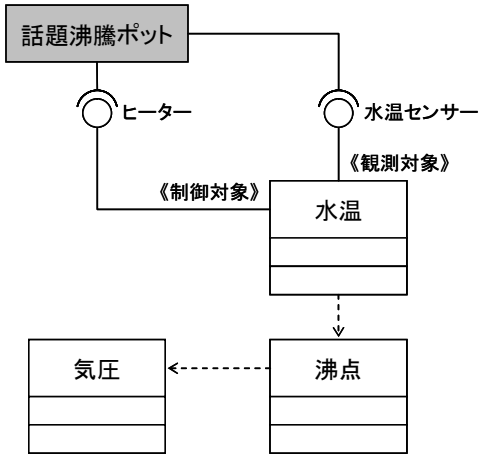


図 3：話題沸騰ポットの外部環境

4.3 外部環境のクラスの状態の整理

次に上記で作成した外部環境に関するクラス図を元に、各クラスがとりうる状態を網羅的に整理していく。例えば、「“沸点“は 100℃の場合を境にその前後を含めて３つの状態をとる」あるいは「沸点に影響を及ぼす“気圧”も１気圧を境にその前後で３つの状態をとる」といった様に、外部環境を観測し制御する対象と捉えて、その状況を計測制御可能な値として認識し整理することがここでのポイントとなる。

表 2：話題沸騰ポットの外部環境の状態

水温	沸点	気圧
水温＜沸点	沸点＞100℃	気圧＞1気圧
水温＝沸点	沸点＝100℃	気圧＝1気圧
	沸点＜100℃	気圧＜1気圧

4.4 解釈系による外部環境認識ギャップ分析

次に解釈系の概念を導入して、上記で整理された外部環境のとりうる状態とシステム視点(内部)での認識の差異を分析する。ここではシステムと《観測対象》間の I/F を経由して関連をたどり、解釈系の範囲を定義し、データの制約などを分析して、解釈系に依存する例外的な動作を更に抽出していく。

(i) 解釈系の範囲特定

この例題では、話題沸騰ポットから、I/F である水温センサー、水温、沸点、気圧と関連をたどる事ができる。結果として、「話題沸騰ポット - 水温センサー - 水温 - 沸点 - 気圧」が解釈系の範囲とすることができる。

(ii) データの変換、制約を定義する

この解釈系をトレースして関連するデータの変換ルールや制約条件などを洗い出す。例えば、水温 - 沸点の間に「水温は必ず沸点以下になる（沸点≧水温)」の様な定義がされる。

(iii) システムが観測できない要素の明確化

これらの制約条件などを考慮して、解釈系に登場するクラスの中で、システムが直接検知できないクラスを明確にしていく。この例題では、「システムは、沸点を知る術を持たない」等が定義される。

以上により、「話題沸騰ポット - 水温センサー - 水温 - 沸点 - 気圧」の解釈系は表 3 の様になる。

表 3：話題沸騰ポットの解釈系

- システムは、水温センサーの値を水温として入力する(水温センサーの値＝水温)
- 水温は必ず沸点以下になる(沸点≧水温)
- 水の沸点は、1気圧の場合に100℃になる (気圧＝1気圧 ⇔ 沸点＝100℃)
- 水の沸点は、気圧の上昇に伴って上昇する
- 水の沸点は、気圧の低下に伴って低下する
- システムは、沸点を知る術を持たない
- システムは、気圧を知る術を持たない

4.5 シナリオ網羅性の確認

本手法では 4.2～4.4 で分析した外部環境、解釈系を用いて、対象となるシステムの基本シナリオをシナリオ網羅性の視点で再評価し、不足するシナリオの洗い出しを行う。

システムの基本シナリオは、通常、システムの最も一般的な動作を代表するものであり、仕様書などを参考に作成される。話題沸騰ポットの例題では、沸騰終了の基本シナリオは以下の様になる。

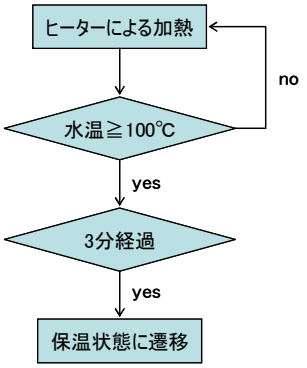


図 4：沸騰終了の基本シナリオ

作成された基本シナリオの網羅性評価および不足シナリオ抽出は以下の手順で進める。

手順 1：基本シナリオ中の分岐条件を、解釈系の定義をシステム側から適用し、変換する

- 例題では、分岐条件として“水温≧100℃”が登場する。この分岐条件を解釈系の定義に従って変換する。
- システム - 水温センサー間の定義を当てはめると、“水温センサーの値≧100℃”となる。
- 次に、水温 - 沸点間の"沸点≧水温"を当てはめ、"沸点≧水温センサーの値≧100℃"とする。
- ここから、隠れた条件として“沸点≧100℃”が抽出される。
- この条件を、沸点 - 気圧間の定義を用いて更に変換すると、“沸点≧100℃⇔気圧≧1気圧”となる。
- 従って、最初の条件は、"気圧≧1気圧⇒沸点≧水温≧100℃"と変換される。
- 変換の結果、"水温≧100℃"の条件は、"気圧≧1気圧"を前提とした条件である事が分かる。

手順 2：外部環境のクラスの状態に照し合せ、変換した条件が網羅する状態の範囲を特定する

- 例題の場合、気圧の状態は、気圧＞1気圧、気圧＝1気圧、気圧＜1気圧の3つが定義されている。
- この内、"水温≧100℃"の前提となる"気圧≧1気圧"が網羅する範囲は、3つの内2つで、"気圧＜1気圧"を網羅していない事が分かる。

手順 3：網羅していない状態が存在する場合、その状態に対応するシナリオを不足するシナリオとして分析者に示す

- 例題では、"気圧＜1気圧"に対応するシナリオが不足している事が分かる。

1.～3.の手順を繰り返す事により、不足するシナリオの存在が明確になる。不足するシナリオを補っていく事により、システムの動作を網羅したシナリオが作成される。

4.6 評価

本提案手法は、外部環境と解釈系を定義し、これらの情報を用いる事で不足しているシナリオの有無を発見する。

例題で示す様に、話題沸騰ポットの沸騰終了処理の基本シナリオに提案手法を用いる事で、"水温≧100℃"となる為には、"沸点≧100℃"でなければならないという、外部環境に起因する隠れた条件を明らかにできた。また、解釈系の定義に従って条件を変換する事で、基本シナリオが網羅する範囲を明確にし、"気圧＜1 気圧"の状態に対応するシナリオが不足している事も発見できた。

システム内部のみを分析した場合、即ち、図 3 のクラス図が無い場合、外部環境に関する情報が完全に欠落する事から、"沸点≧100℃"の条件が抽出されるかは、分析者に依存してしまう。

また、解釈系の定義が無い場合、"水温≧100℃"の条件から、"気圧＜1 気圧"の状態に対応するシナリオが不足する事を手順的に発見する事は困難と考えられる。どの様な条件に対応するシナリオが不足しているかを発見する為には、ドメイン知識が不可欠と考えられる為である。

5. まとめ

本稿では、組込みシステムにおける要求分析において、外部環境までを含めた、網羅的なシナリオの作成を支援する手法を提案した。

組込みシステムの外部を、分析者が認識する外部環境と、組込みシステムが理解できる外部環境を解釈系とで定義し、それらの情報を用いて不足している動作条件を提示する事で、より網羅的なシナリオを作成する事を可能とした。

本提案手法では組込みシステムに対する外部環境の影響に関して、外部環境の時系列的な変化は考慮せず、特に静的な条件のみを対象としたものとなっている。しかし、通常のシステム動作では、システムの動作途中に動的に外部環境が変動するといった場合もあるため、今後、動的な分析視点に対させる必要があると考えており、引き続き検討を進めていきたい。

謝辞

手法のトライアルと、そのフィードバックを行っていただいた、九州工業大学鵜林研究室の金川太俊、瀬戸敏喜、両名に心より感謝の意を表する。

参考文献

[1] 鷲見毅、平山雅之、鵜林尚靖、“組込みシステムにおける動作分析手法の提案、” SIG-SS-2005-36、pp。19-24

[2] 組込みソフトウェア管理者・技術者育成研究会 http://www。sessame。jp/ （last access:2006/05/22）