様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年　3 月 31 日現在

機関番号：１７１０４
研究種目：若手研究（B）
研究期間：２００９　～　２０１１
課題番号：２１７００００３７
研究課題名（和文）　組込みソフトウェア仕様化のための非正常系分析支援ツールの構築

研究課題名（英文）　A Study on Analysis Support Tools for Unexpected Obstacle Specification of Embedded Software

研究代表者
片峯　恵一　（KATAMINE KEIICHI）
九州工業大学・大学院情報工学研究院・助教
研究者番号：００２６４１３５

研究成果の概要（和文）：高品質な組込みソフトウェアを開発するために、非正常系と呼ばれる例外や障害などの事象に着目して、情報の流れに着目した情報フローダイアグラムによる静的要求分析手法、および状態遷移に着目した分析マトリクスによる動的な要求分析手法を統合した非正常系分析手法を研究した。また、実用性を考慮し、分析範囲を制限するための手法を導入した。

研究成果の概要（英文）：In order to improve the quality of embedded software, we studied the analysis method for extracting unexpected obstacles such as exceptions and failures. The method integrates the Embedded Systems Improving Method (ESIM) using an Analysis Matrix, and a method that uses an Information Flow Diagram (IFD). The former is a statical requirement analysis method focused on the flow of information, the latter is a dynamical analysis method focused on the state transition model. We also introduced practical techniques to decrease the analysis scope in the integrated method.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,000,000	300,000	1,300,000
2010 年度	900,000	270,000	1,170,000
2011 年度	800,000	240,000	1,040,000
年度	0	0	0
年度	0	0	0
総　計	2,700,000	810,000	3,510,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：ソフトウェア工学、ソフトウェア効率化・安定化、モデリング、非正常系、組込みソフトウェア

１．研究開始当初の背景

組込みシステム業界では、 組込みソフトウェアの多機能化や大規模化に伴う信頼性の向上と、ライフサイクル短縮に伴う生産性の向上という相反する要求が挙げられている。組込みソフトウェア産業実態調査報告書では、毎年、要求仕様の問題と品質の問題が大きく取り上げられている。

組込みソフトウェアは、 その約 8 割が例外処理機能を占めている。家電機器などの組込みシステムは、不特定多数の者が利用するため、組込みソフトウェアの開発において、利用環境や運用状態に対して通常では発生しないような状況への配慮を徹底して行う必要があるためである。 しかし、その配慮

が現実には抜け落ちやすく、品質問題の大きな原因の 1 つとなっている。そのため、要求仕様設定時に例外処理機能の抜け落ちを防止する技術が重要である。

従来、ハードウェア・デバイスの異常や障害などを分析する手法として、デバイスの特性から障害を推測するための FMEA (Failure Modes and Effects Analysis) 手法、デバイス間の流れの異常から障害を推測するための HAZOP (Hazards and Operability Study) 手法、障害から原因を推測するための FTA (Fault Tree Analysis) 手法がある。ハードウェア・デバイスを含む組込みシステムの障害分析には、これらの手法はすべて有効である。そこで、従来は個別に発展してきたこれらの手法を融合する必要がある。

一方、要求工学の分野では、障害や異常に類する例外処理について研究が行われている。例えば、Misuse Case は、悪意を持ったユースケースを UML 手法によって分析する。また、異常系をゴール指向方法論によって分析するための手法も提案されている。Abuse Frame は、セキュリティ問題のスコープを制限する方法である。これらの研究に共通しているのは重要な障害のみを分析するために、トップダウン手法を適用していることである。しかし、組込みシステムは、小さな子供を含む不特定多数の利用者が存在するため、軽微な障害の可能性も含めて分析し、対策を取る必要がある。障害は、何らかの目的を持って発生するのではなく、組込みシステムやその動作環境の構成要素の特性により、無目的に発生する。そのため、トップダウン分析だけでなくボトムアップ分析も合わせて実施する必要がある。

２．研究の目的

組込みシステムの品質を向上するためには、高品質な組込みソフトウェアが必要となる。特に、障害や異常等の例外処理を十分考慮した分析とその仕様化が重要となる。そこで、本研究では、組込みソフトウェアの正常系仕様と非正常系仕様を、以下のように定義する。

(1) 正常系仕様は、アーキテクチャ設計がはじまる前には既に決定しており、操作マニュアルに記載されている動作を規定するものである。

(2) 非正常系仕様は、障害やデバイス材料の劣化、過負荷、誤動作など、正常系から外れた動作を規定するものである。

どちらもシステム仕様書に明確に記述される。しかし、現実には仕様から抜け落ちやすいため、ソフトウェア開発プロセス全体を通して非正常系と呼び、正常系とは区別する。

著者らは、組込みシステムの非正常系分析手法として、以下の 2 つの手法を研究している。

(1) 情報フローダイアグラム(IFD)
デバイス間の情報の流れに着目して組込みシステムおよび外部環境の静的な構造を表現し、分析する。

(2) 分析マトリクスを用いた分析手法 ESIM (Embedded Systems Improving Method)
状態とイベントに着目して、組込みシステムの動的な振る舞いを分析する。

これらの分析手法は、前述したトップダウン分析およびボトムアップ分析の両方を実施する。また、障害の発生した原因から結果までを障害シナリオとして抽出し、非正常系を仕様化する。これら 2 種類の分析手法は、個別に考案されたため、それぞれ効果を挙げているが、静的な視点と動的な視点という相補的な関係にあるため、統合して利用することにより、さらなる効果が期待できる。

そこで、非正常系と呼ばれる例外や障害などの事象に注目して、情報の流れに着目した IFD による静的な要求分析手法、および状態遷移に着目した分析マトリクスによる動的な要求分析手法を統合した分析手法を研究する。

３．研究の方法

高品質な組込みソフトウェアを開発するために、IFD および分析マトリクスを用いた組込みシステムの非正常系分析を支援する方法を研究する。具体的には、統合モデルおよび分析プロセスの 2 つの視点から研究する。以下にそれぞれの概要を示す。

(1) 統合モデルの構築
IFD と分析マトリクスの統合モデルを構築する。IFD は、組込みシステムの情報伝達メカニズムを IDEF0 によるプロセス図と構成要素の関連を表すデバイス図により表現する。このため、デバイスの静的な構造とプロセスにより組込みシステムの動作を捉える。一方、分析マトリクスは、ある時点での現象を状態とイベントの観点で捉え、状態遷移により組込みシステムの動作を表現する。このように主要な概念は異なるが、各デバイスの状態に関連した情報を使用する点や

非正常系を障害のシナリオとして分析する点は同じである。さらに、静的な構造による分析と動的な振舞いによる分析という相補的な関係である。

(2) 分析プロセスの洗練

IFD は、ハードウェアの構成図を基にしているため、非正常系の分析に特別な設計スキルを要求しない。しかし分析マトリクスを用いた ESIM は、状態遷移モデルに基づく分析法であり、ハードウェアの特性や構成要素間の影響など高度な設計スキルを要求するため、効率的に非正常系を分析するためには、熟練技術者が必要となる。そこで、特に ESIM における分析プロセスを詳細化し、IFD と連携することにより、熟練技術者でなくとも実用的に分析可能にする。

４．研究成果

本研究によって得られた成果を、前述の 2 つの観点に分けて、以下に述べる。

(1) 統合モデル

IFD および分析マトリクスの概念モデル、抽象化概念の明確化、およびこれらを利用した推論方式について研究した。以下、それぞれについて述べる。

① 概念モデル

定式化では、組込みシステムの非正常系分析に必要な概念を概念モデルとして規定し、IFD の構成要素であるプロセスやデバイスを集合として定義、また、分析マトリクスの状態やイベントを関数の結合により表現した。 これらの規定により、これまで不明確であったダイアグラム間の概念の対応関係が明らかとなった。

② 抽象化概念

熟練技術者が分析時に使用している 3 種類の抽象化概念、つまり、(1)複数のデバイスを 1 つのデバイスとみなす構成要素の抽象化、(2)複合的な状態を 1 つの状態とみなす状態の抽象化、(3)複数のプロセスを 1 つのフローとみなすフロー系列の抽象化、を関数として規定することにより、概念をより明確にした。

③ 推論方式

熟練技術者の思考方法を分析し、分析過程における定性的な 4 種類の性質を抽出した。この 4 種類の性質を制約条件と性質関数として規定し、定性的に推論することにより、非正常系の分析過程において、IFD と分析マトリクスの協調作業が可能となった。

(2) 分析プロセスの洗練

IFD と分析マトリクスの役割に応じたと非正常系分析モデル、分析範囲の削減方式について研究した。以下、それぞれについて述べる。

① 非正常系分析モデル

IFD および分析マトリクスを統合した分析モデルとして、分析マトリクスを中心とした分析方法を採用した。この手法は、ESIM における分析マトリクスによる分析時に IFD を組み合わせることにより、状態遷移時の詳細情報を取得出来るようになった。これにより、設計の熟練度に合わせた非正常系分析が可能となった。

② 分析範囲の削減

実用的な非正常系分析手法とするため、分析範囲を削減する方法を研究した。具体的には、状態モデル、イベントおよび属性に関して分析範囲の削減法を導入した。

状態モデルは、複合的な要因による障害を複数の異なる関心度で分析するために、分析マトリクスの分析対象であるシステムを分割せずに全体として扱うモデルを採用した。このモデルでは、分析中のある時点で対象としている構成要素の状態に着目したシステムの全体の状態を記述することにより分析者にとって関心のある状態のみを抽出した。これにより、分析範囲を局所化し、設計者の関心事に合わせた分析を可能とした。

また、熟練技術者の考えている構成要素は、分析ごとに範囲が異なる。そこで、構成要素を各々１つの状態機械とし、各構成要素の持つ属性を内部もしくは１つの外部構成要素に影響する局所的属性と、複数の外部構成要素に影響を及ぼす大域的属性の２種類に分類した。これにより、構成要素間の関係を分析する場合、分析範囲を大域的属性のみに限定できた。

さらに、属性の分析単位を限定することにより分析範囲を制限した。たとえば、センサーは連続的に特定

の構成要素にデータを送信しているが、分析時はある閾値を超えたときの変化で判断しており、同値分割法を用いることによりイベントを限定した。ただし、非正常系となる特別な状況、たとえば、故障等により入力が変化しても出力が変化してない場合は入出力関係の矛盾という特別なイベントを発生し、非正常系として分析出来るようにした。

また、プロブレムフレームを用いて関心事の絞り込みを行うことにより、状態爆発を避ける方法を検討した。この方法は、非正常系分析に有効であるが、本課題の範囲を超えており、今後研究を進めていく予定である。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計４件）

① 三瀬敏朗、橋本正明、片峯恵一、中谷多哉子、問題フレームに基づく家電製品の非正常系シナリオの発見、電子情報通信学会技術研究報告、査読無、KBSE2011-25、2011、pp.7-12
② 三瀬敏朗、新屋敷泰史、片峯恵一、橋本正明、中谷多哉子、鵜林尚靖、非正常系現象に着目した組込みシステムの障害シナリオ分析手法、電子情報通信学会技術研究報告、査読無、KBSE2010-50、2011、pp.19-24
③ 片峯恵一、新屋敷泰史、三瀬敏朗、中谷多哉子、鵜林尚靖、橋本正明、組込みシステム非正常系分析手法の定性推論による定式化、電子情報通信学会技術研究報告、査読無、KBSE2009-27、2009、pp.57-62
④ 片峯恵一、新屋敷泰史、三瀬敏朗、橋本正明、中谷多哉子、組込みシステム非正常系分析手法の統合、ソフトウェアエンジニアリング最前線２００９情報処理学会ソフトウェアエンジニアリングシンポジウム、査読有、2009、pp.187

〔学会発表〕（計１件）

① 片峯恵一、組込みシステム非正常系分析手法、情報処理学会ソフトウェア工学研究会要求工学ワーキンググループ・ワークショップ・イン・壱岐、2010.10.21-23、長崎

６．研究組織
(1)研究代表者

片峯　恵一（KATAMINE KEIICHI）
九州工業大学・大学院情報工学研究院・助教
研究者番号：００２６４１３５