5A-5

フィードバック制御用組込みソフトウェアにおける要求仕様書記述方式と開発環境

佐藤　芳信　　高橋　弘　　西田　廣治
富士電機アドバンストテクノロジー（株）

１．はじめに

インバータに代表されるパワーエレクトロニクス製品では、電圧や電流を検出し目標に追従させるフィードバック制御を行っている。物理現象を扱っているため時間的な制約があり、定められた手順の処理を定周期で行っている。このような組込み製品においても、機器に内蔵する CPU の演算能力の増加に伴い、実装するソフトウェア機能が増えており、効率の良いソフトウェア開発方法が必要とされている。開発効率を高めるには、抜け漏れや曖昧さの無い品質の高い要求仕様書の作成による手戻り作業の削減が重要である。

そこで、本稿では、抜け漏れや曖昧さの少ない品質の高い要求仕様書の記述方式とその実現環境について述べる。

２．現状の要求仕様書作成時の課題

要求仕様書の品質を高めるためには、記述内容の抜け漏れを防ぐことと、記述内容の曖昧さを排除することが必要である。

記述内容の抜け漏れを防ぐためには、テンプレートを用いて、予め決まった項目の記述を行う方法がある。IEEE 830 では、その章項目が示されている。

また、記述内容の曖昧さを排除するためには、ISO/IEC 12207 に記述されているように、ソフトウェア要求分析のプロセスにおいて仕様書を作成し、レビューを行うことで内容を確認し、曖昧な点を明確にしていく方法がある。

これらの手法をパワーエレクトロニクス製品の開発に適用した例が紹介されている。[1]

しかし、要求仕様書を自然言語による自由記述で作成しているため、主語が無い文章が記述できるなどの要求仕様書の記述文章自体に曖昧さを残してしまう課題がある。

また、レビューを行う時にも、自由記述のため文章が統一されてなく、文や用語の解釈に時間が取られて効果的なレビューが行えないなどの課題がある。

このような自然言語による自由記述の曖昧さの課題を解決するために、形式的仕様記述言語を用いた記述方法が知られている。形式的仕様記述言語を用いることで、内容の曖昧さは無くなるが、使用する構文の理解、記述の仕方やレビューの実施を行うにあたり、ある程度の教育や訓練を行う必要がある。そのため、形式的仕様記述言語を導入して効果が出てくるまでには時間が掛かるという課題がある。

そこで、要求仕様書の作成にあたり、自然言語による自由記述の曖昧さを排除し品質の高めるため、自然言語による形式的仕様記述言語の構文記述方式および、その実現方法について検討を行った。

３．要求仕様書の記述方式

パワーエレクトロニクス製品に用いられるソフトウェアの特徴としては、物理現象の制御を行うため処理時間の制約があり、定められた処理手順を定周期で行うことが多い。そのため、処理はシングルタスクで入出力の関係が明確になっている。

これらの特徴を形式的仕様記述言語の構文で記述するために、プログラムの部分正当性の証明で使われている事前条件・事後条件の構文を適用した。事前条件と事後条件は以下のように定義されている。[2]

事前条件：入力データないし、実行前の状態が満足すべき条件
事後条件：出力結果ないし、実行後の結果が満足すべき条件

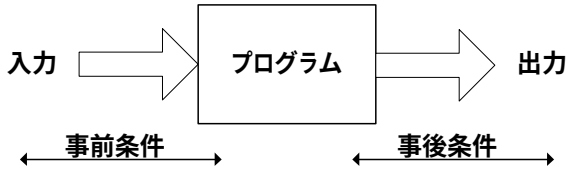

図１　プログラム入出力と事前・事後条件の関係

Description Methods and Development Tools for Software Requirements Specifications of Embedded Products with Feedback Control
Yoshinobu Sato, Hiroshi Takahashi, Hiroji Nishida
Fuji Electric Advanced Technology Co.,Ltd.

事前条件と事後条件の定義に従って処理の記述を行うにあたり、要求仕様書の段階でどのレベルまで記述すべきかなどについて、記述指針を作る必要がある。

曖昧さのある内容は検証ができないという前提に基づき、記述内容が検証可能できるかどうかで曖昧さの有無の判断を行う。検証可能な内容であるためには、以下の 2 つの条件を満たす必要がある。

条件①：試験を行うためには、入力データまたは実行前の状態が満足すべき条件設定をする

条件②：試験結果の判定を行うためには、出力結果または実行後の状態が満足すべき条件を明らかにする

この試験を行うための条件①と事前条件、試験結果の判定を行うための条件②と事後条件の内容を一致させるように要求仕様書の記述を行うことで、検証可能である曖昧さの無い要求仕様書が作成できる。

４．要求仕様書の記述環境

要求仕様書の記述指針を定めたので、自然言語による形式的仕様記述言語の構文記述環境について考える。

ドアを電気的に開閉する装置におけるドア開動作について、事前条件と事後条件を記述する入力フォームの例を図２に示す。

要求仕様書

章番号	1.1
項目定義	ドア開動作
コメント	通常のドア開動作（ドアが全閉位置から全開位置まで移動する）
事前条件（試験条件）	
条件式	条件1 and 条件2 and 条件3 ＝ TRUE
条件1	ドア開動作指令がある
条件2	ドアが全閉位置にある
条件3	ドア開時間計測タイマ値＝0
事後条件（試験の判定基準）	
条件式	条件1 and 条件2 ＝ TRUE
条件1	ドアが開位置（600mm±2mm）まで移動する
条件2	ドア開時間計測タイマ値＝1.6秒±0.2秒

図２ 要求仕様書の入力フォームの例

項目定義やコメントは自然言語による自由記述を行う。事前条件と事後条件は、箇条書きによる条件項目と、その条件項目間の関係を示す条件式で記述する。箇条書きで記述することで冗長な記述を抑制し、条件の追加と削除を容易にする。また、論理演算子を用いた条件式で記述することで各条件項目の関係が明確になり曖昧さを低減する。

検証試験を意識して事前条件と事後条件の条件項目と条件式を記述しているため、事前条件を試験条件に、事後条件を試験の判定基準に置き換えることで試験仕様書の作成が可能となる。図３に図２の内容を置き換えた試験仕様書の例を示す。

試験仕様書

章番号 項目定義	試験条件（事前条件）		出力仕様（事後条件） 判定：条件式：条件を満たすこと		試験結果	試験日	試験者
1.1 ドア開動作	条件式	条件1 and 条件2 and 条件3 ＝ TRUE	条件式	条件1 and 条件1 ＝ TRUE			
	条件1	ドア開動作指令がある	条件1	ドアが開位置（600mm±2mm）まで移動する			
	条件2	ドアが全閉位置にある					
	条件3	ドア開時間計測タイマ値＝0	条件2	ドア開時間計測タイマ値＝1.6秒±0.2秒			

図３ 試験仕様書の例

事後条件の条件項目毎に試験結果の判定ができ、条件式を満たすかどうかで機能としての合否の確認ができる。要求仕様書から試験仕様書を作成するため、機能項目と試験項目が対応し項目の抜けが無くなる。また、要求仕様書作成段階で、試験仕様書のレビューを行うことが可能となるので、条件項目の記述においても、検証しにくい定性的な表現から検証可能な定量的な表現になることが期待できる。

さらに、要求仕様書作成時に事前条件の条件項目が成立しない場合の組合せ、例えば図２において条件２のドアが全閉位置にない場合などを明示することで、非正常系の検討が容易になり要求事項の抜け漏れを低減することができる。

５．まとめ

パワーエレクトロニクス製品で用いられている定められた手順を定周期で繰り返すフィードバック制御を行う要求仕様書の記述方式について、自然言語による形式的仕様記述言語の構文（事前条件と事後条件）を検証可能な記述にすることで曖昧さを排除し品質を高めることが可能であり、また、上記構文の記述内容を用いて機能に対応した試験仕様書の作成が可能であることが分かった。

参考文献

[1]「パワーエレクトロニクス製品における要求の抽出手法の開発」高橋 弘、佐藤芳信、鈴木哲雄、城戸武志 ESS 2006

[2]「プログラム仕様記述論」荒木啓二郎、張 漢明 共著 オーム社