有限状態機械によるシステム設計の仕様記述に関する一考察

2R－5

宮崎義弘　田中誠一郎　手島文彰　井上勝博　三原幸博
株式会社　東芝
システム・ソフトウェア技術研究所

１．はじめに

われわれは、家電製品の設計仕様を有限状態機械(Finite State Machine 以下ＦＳＭとする)でモデル化し、実現された製品がその仕様を満たすか否かを、機械的に判定する動的検証システムを開発した[1][2]。このシステムは製品仕様を中間言語で与えており、必ずしも記述が容易であるとは言い難い。そこで、記述や検証の容易性と理解性の向上を目的として、階層化を導入した仕様記述言語の検討を行うことにした。ＦＳＭを用いた仕様記述言語は従来から提案されている[3][4]が、われわれがターゲットとする製品仕様を適切に記述できない。したがって、われわれは対象製品の構造や特徴を、適切に反映した家電製品向き仕様記述言語を新たに開発した。

本稿では、仕様記述の階層化に伴う問題点とその解決法について述べ、実際の製品（家庭用冷蔵庫）に適用した際の評価について報告する。なお、これはソフト開発支援システムＩＭＡＰ[5]の一環として開発している。

２．仕様記述における問題

家庭用冷蔵庫の設計仕様をＦＳＭにより記述すると、記述量が増大し、記述容易性や理解性が著しく悪化する。この一般的な解決方法としては、階層化の導入が考えられるが、ＦＳＭの設計を階層的に記述しようとすると、次のような問題が起こる。

（１）リアルタイムな処理

冷蔵庫は、例えば、冷凍ボタンが押されたら冷凍処理を行うという様に、外部入力に対しリアルタイムで処理を行う必要性のあるものが存在する。このため、製品仕様を階層化した場合、階層を越えた遷移が存在し、設計者は現在設計中以外のＦＳＭも意識しなければならず、階層化のメリットがなくなる。

（２）例外的な処理

外部入力でも、リアルタイムで処理を行わないもの、処理の一部のみをリアルタイムで行い残りを後で行うものなどがある。例えば、除霜中に冷凍ボタンが押されたらとりあえず冷凍ランプだけをつけておき、除霜処理が終了したら冷凍処理を行うという様な、処理に優先関係が存在する場合である。このような仕様は、従来のＦＳＭの枠組みでは表現することが難しい。

３．仕様記述の拡張

上記のような問題は、例えば以下に示すようなＦＳＭの拡張を行うことにより解決できる。

（ａ）内部状態

これは、例えば、トグルスイッチなどの機能を実現するために、ボタンが押された回数を示す変数を考え、その変数の値によって遷移先が変わるという様な仕様を記述できる[3]。

（ｂ）遷移規則

これは、同一階層の遷移しかできないという制約を設けてＦＳＭの設計を局所化するものである。例えば、図１に示すように、除霜装置保護ＦＳＭで上述の冷凍ボタンが押された場合、そのＦＳＭをリターンして、冷凍ＦＳＭが定義されている階層まで戻って、そこではじめて冷凍ＦＳＭに遷移する。

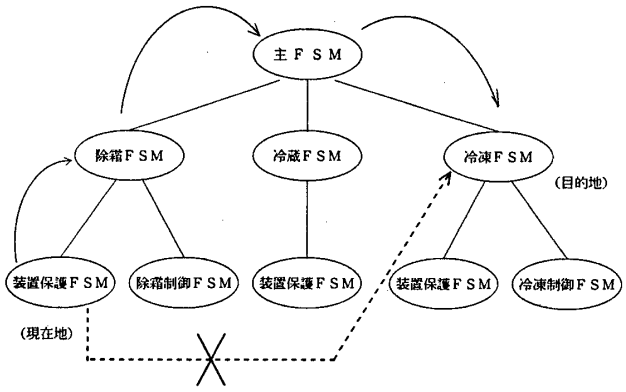

図１　階層化の概念図

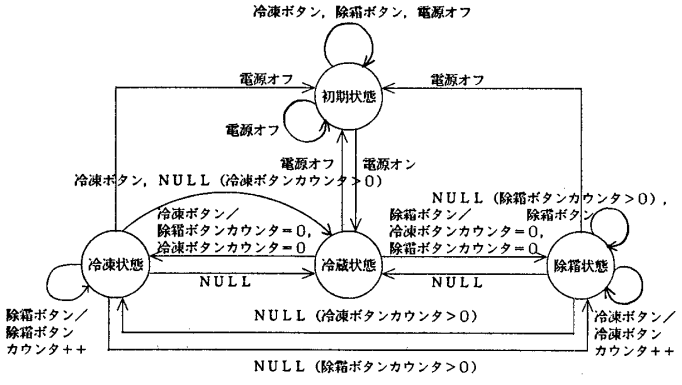

図２　仕様記述例（ボトムアップ設計）

A study of system design specification description using FSM
Yoshihiro MIYAZAKI, Seiichiro TANAKA, Fumiaki TESHIMA, Katsuhiro INOUE and Yukihiro MIHARA
TOSHIBA Corporation

図２は、単純化した冷蔵庫の機能を、ボトムアップに設計した時の主ＦＳＭを表現したものである。しかし、このような表現では、内部状態という概念を導入したことにより、仕様の独立性が失われてしまっている。また、トップダウン設計においては、論理的な設計のみを行うことができず、その実現をも意識したものとならざるを得ない。

そこで、われわれはさらに次のような拡張を行なった。

（ｃ）メッセージ通信

これは、ＦＳＭ間で情報をやりとりするためのものである。つまり、共有変数やパラメータ渡しなどの機構に基づく通信を許さないため、このようなメッセージ機能が必要となるのである。このような枠組みを設けることによって、各ＦＳＭを独立に設計することが可能になる。しかし、各ＦＳＭの局所的な変数は許している。これは、内部変数を導入することによって記述能力が大幅に向上するためである。

さらに、その他の拡張として以下のようなものがある。

（ｄ）例外処理記述

状態遷移による表現方式では、本来の機能を実現するための記述と、割り込みや例外処理などの記述が同じ形式になるため仕様の理解性を損ねている。このため、例外処理などを記述するための特別な構文を用意している。

（ｅ）簡易処理記述

ＦＳＭで仕様記述する際に、同様の遷移を全ての状態で記述することは、設計者にとって大きな負担であり、読解性という観点でも問題である。そこで、同様の状態遷移は、ＦＳＭの最初で記述すれば全ての状態で暗黙に存在することにする。

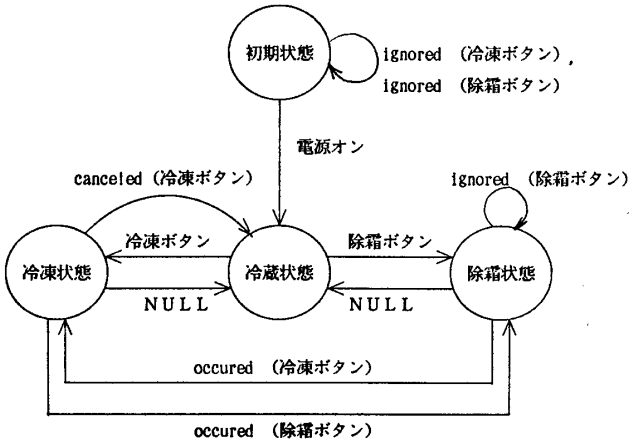

図３　仕様記述例（トップダウン設計）

図３は、図２の主ＦＳＭを（ａ）～（ｅ）を用いて表現したものである。

４．評　価

本仕様記述言語を評価するために、実際の家電製品について記述実験を行った。表１に、その仕様記述の比較結果を示す。

表１で、従来の記述方式に比べて本記述方式は記述量が約半分になることがわかる。これは、階層化の導入に加え、簡易記述を導入したことによるものと考えられる。

特に遷移数に関しては、階層化を導入することにより、大幅に削減されていることがわかる。また、状態数に関しても若干の削減が見られる。

	自然言語記述	ＦＳＭ記述	階層化ＦＳＭ記述
定義	８６（行）	４００　（行）	２３０　（行）
機能		状態２５（個）　（行） 遷移６２（個）	状態２０（個）　（行） 遷移２６（個）

表１．比較結果

仕様の理解性に関しては、図２と図３を比較してわかるように、より単純な記述となっており直感的にＦＳＭの機能を理解できるようになった。

ＦＳＭに基づく設計方法についても、階層化の導入により、概要設計から詳細設計へとトップダウン的に設計を行うことができるようになり、設計の部品化の促進や設計効率の向上につながっている。

５．まとめ

ＦＳＭにより製品仕様を記述する際の問題を整理し、それらを改善するための仕様記述言語を開発した。

本仕様記述言語では階層化や簡易記述等の概念を導入することにより、製品仕様の記述量が削減されることが分かった。また、仕様の理解性も改善されている。

今後、他の家電製品にも適用評価していく予定である。

参考文献

[1]手島他:「システム設計における仕様検証の一手法」情報処理学会ソフトウェア工学研究会 66-1 1989

[2]手島他:「システム製品テストの自動化手法の開発と適用」 日本科学技術連盟 第９回ソフトウエア生産における品質管理シンポジウム 1989

[3]白鳥他:「ＮＥＳＤＥＬ－プロトコル向き仕様記述言語とその応用」 情報処理学会論文誌 Vol.26 No.3 1985

[4]"ESTELLE - A formal description technique based on an extended state transition model", ISO/DIS 9074 1987

[5]大筆他:「ＩＭＡＰシステム（１）－（１０）」情報処理学会 第３１回全国大会予稿集 P.489-508