形式手法による組み込みソフトウェア開発

第6回 システム全体の振る舞いを検証する

藤倉 俊幸

これまで，カップラーメン・タイマの各要求項目に対する設計仕様について検証を行いつつ設計してきました．今回はそれらを統合してシステム全体の形式モデルを作成し，一つのシステムとして検証を行います．（編集部）

今回は，**図1**の手順で今まで作成した要求項目ごとの設計仕様を統合してシステム全体の振る舞いモデルを作ってみます．こうすることで要求項目間の検証が可能になります．その後，以前に従来手法で設計・実装したXMOS版の形式モデルをリバースによって作成し，システム全体の形式モデルと比較することで，XMOS版の検証と分析を行います．

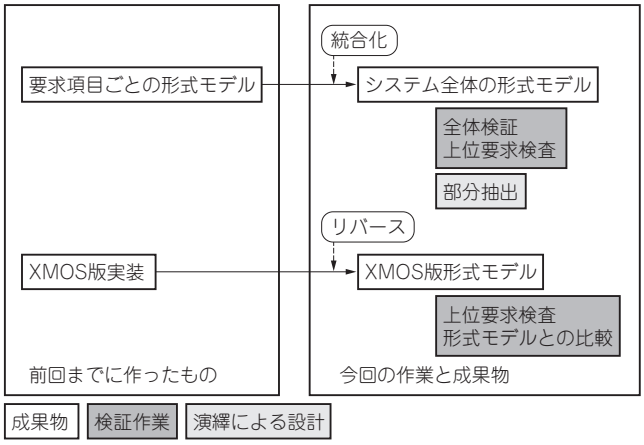

図1　今回のストーリ…ハードウェアに実装したプログラムから形式モデルを抽出して上位要求と比較する

本連載で作成した複数の形式モデルを統合して一つにまとめる．XMOS版は実装から設計を起こす．そして両者を比較する

その結果，なんと慎重に作ったはずのXMOS版には問題がありました．それは，LED4の点滅回数が多くなることです．原因はLED4コントロール・スレッドが自律的に動作してしまう設計にありました．LEDの250msの点滅が数回多くても気付かないかもしれませんが，厳密には異なる振る舞いをすることが分かりました．

1．要求項目ごとの形式モデルを統合してシステム全体のモデルを作成する

● モデル検査ツールLTSAではモデルの統合は簡単

モデルの統合といっても，モデル検査ツールLTSAの場合は並列化オペレータ（||）でモデルを合成するだけで統合できます．今までに作成した要求項目ごとのLTSAモデルの一覧を**表1**に示します．これらのモデルは独立に作ったために，アクション名（アルファベット）が重複しています．まず**表2**のように名前を変えて重複を回避します．名前を付け直したLTSAモデルで状態数の少ないSpecBを**図2**，Req02を**図3**，SP07STM2を**図4**に示します．LED4Ctrlは，状態数が多いので省略します．

```
||CupRamenTimer_ = (SpecB||Req02||
                    SP07STM2||LED4Ctrl).
```

表1　要求項目ごとの仕様とモデルの対応

先月号までにLTSAツールで仕様をもとに作成した状態遷移モデル（LTSAモデル）

ID	仕　様	LTSAモデル	状態数
Spec01	電源がONの間（プログラムが動いている間），LED1の点灯・消灯を1秒間隔で繰り返す	SpecB	10
Spec02	SW1がONになると設定時間を30秒にして，タイマを起動する	Req02	5
Spec04	タイマが動いている間にSW8がONになると，設定時間を30秒延長する		
Spec05	タイマが動いている間は，10秒間隔で，LED4を2回点滅させる．LED4の2回点滅は，点灯・消灯を0.25秒間隔で2回繰り返すことで行う	LED4Ctrl	268 （1秒間点滅では44）
Spec06	設定時間が経過すると，LED4を**15秒間点滅させた**後，消灯する．LED4の点滅は，点灯・消灯を0.25秒間隔で繰り返すことで行う		
Spec07	SW8が押されたらLED2を点灯する	SP07STM2	4