形式手法 B-Method によるデバイスドライバモデルの記述（１）
―シリアル通信デバイスドライバの記述―

苫小牧高専　○大西　孝臣、　稲川　清、　阿部　司、　吉村　斎、　北海道立総合研究機構　堀　武司

要　旨

ソフトウェアシステム構築に際して、形式手法を導入する事を通じて、従来のヒューリスティックな手法にて構築されたソフトウェアと比較して、システム開発過程の可視化・顕現化が進み、システムが起こすトラブルの低減が期待できる。

本稿では、現在、我々が行っている、リアルタイム OS に適用したシリアル通信デバイスドライバの形式手法 B-Method による記述においての要点について述べる。

１．はじめに

我々は、本稿謝辞にある研究助成において機能安全性を有する電子制御ソフトウェア基盤の開発を最終的な目標にしており、システム構築の首尾一貫性に関する証明可能性をもたらす形式手法によるソフトウェアシステムのモデル記述に取り組んでいる。

本稿では、リアルタイム OS に適用したシリアル通信デバイスドライバの記述に際しての要点について報告する。

２．記述対象のドライバについて

我々はリアルタイム OS に適用したシリアル通信デバイスドライバの記述に取り組んでいる。

当ドライバの対象の OS を AUTOSAR 仕様準拠[1]の TOPPERS/ATK2-SC1[2]とし、対象の CPU（ターゲット）をルネサスエレクトロニクス社の RX62N シリーズとする。

当ドライバのモデル記述に際しては、TOPPERS/ATK2-SC1 のユーザズマニュアルやターゲット依存部ポーティングガイド、ATK2 の外部仕様書、RX62 ハードウェアマニュアルの記述に基づくのと同時に、これらの文書において首尾一貫性に欠けている箇所、曖昧な箇所については内容を補う作業が必要となる。また、先行としてヒューリスティックな手法でポーティングされたドライバのソースプログラム[3]も参考にする（これはリバースエンジニアリングに相当する）。

図１に当ドライバの構成を示す。

当ドライバは、その仕様より、外部よりの文字単位の受信のみを担うものであり、送信の機能を有しない。

当ドライバは、ターゲット非依存部と依存部に分かれ、ターゲット依存部の中にはターゲット内のレジスタへのアクセスを指示するプリミティブインターフェースがある。

図１　シリアル通信デバイスドライバの構成

３．ドライバのモデル記述について

３－１．コンポーネント構成について

形式手法 B-Method のツールとして仏国 ClearSy 社の Aterier-B[4]採用して記述を行っている。

シリアル通信デバイスドライバモデルの主なコンポーネント構成を図２に示す。

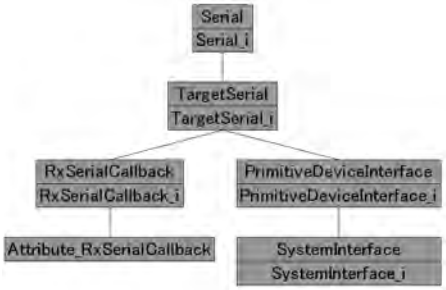

図２　ドライバモデルの主なコンポーネント構成

「Serial」および「_i」はシリアル通信デバイスドライバに対応するコンポーネント、「TargetSerial」および「_i」は当ドライバのターゲット依存部に対応するコンポーネント、「RxSerialCallback」および「_i」は当ドライバ内のコールバック受信部に対応するコンポーネント（４－１節参照）、「Attribute_RxSerialCallback」は「Serial」および「RxSerialCallback」の両コンポーネントで共有する状態変数を取扱う操作を行うコンポーネント（４－２節参照）、「PrimitiveDeviceInterface」および「_i」は当ドライバのターゲット依存部内のレジスタアクセスの指示を行うインターフェースに対応するコンポーネント、「SystemInterface」および「_i」はリアルタイム OS のターゲット依存部にあるレジスタアクセス関数に対応するコンポーネントである。

図２を構成する各ブロックは、図３に示すように、ブロックの上部は抽象機械（Abstract Machine）、下部は実装（Implementation）の各コンポーネントに対応する。

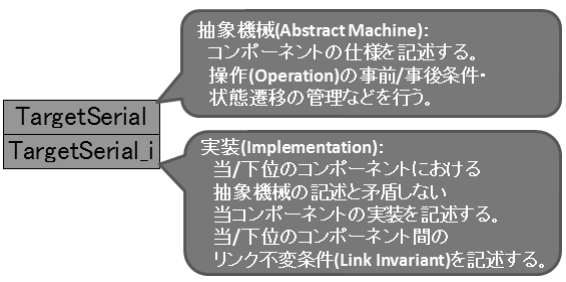

図３　抽象機械・実装の各コンポーネント

３－２．記述の進捗、論理証明について

現在、図２のシステム構成の上位よりコールバック部受信部に当たる左側下位に渡る箇所の記述について行った。

Aterier-B による論理証明の様子を図４に示す。

図４の白抜きの行が、記述を行った主な箇所である。

図２には示さなかったが、図４の下部の行にある「Utility_」の各コンポーネントには、抽象機械において扱われる状態変数が持ち得る全ての状態名を要素とする集合が格納されている。

コンポーネント	型チェック	証明責務生成	証明責務	証明済	証明未	BOチェック
Attribute_RxSerialCallback	OK	OK	0	0	0	OK
PrimitiveDeviceInterface	OK	OK	0	0	0	OK
PrimitiveDeviceInterface_i	OK	OK	19	19	0	OK
RxSerialCallback	OK	OK	0	0	0	OK
RxSerialCallback_i	OK	OK	6	6	0	OK
Serial	OK	OK	0	0	0	OK
Serial_i	OK	OK	23	23	0	OK
SystemInterface	OK	OK	0	0	0	OK
SystemInterface_i	OK	OK	0	0	0	OK
TargetSerial	OK	OK	1	1	0	OK
TargetSerial_i	OK	OK	9	9	0	OK
Utility_Interrupt	OK	OK	0	0	0	OK
Utility_SIODeviceDriver	OK	OK	0	0	0	OK
Utility_Serial	OK	OK	0	0	0	OK
Utility_SerialPort	OK	OK	0	0	0	OK

図４　Aterier-B による論理証明

４．B-Method によるモデル記述について

４－１．コールバックの記述について

図１の構成において、シリアル通信デバイスドライバのターゲット依存部よりターゲット非依存部へのコールバックが発生することが TOPPERS/ATK2-SC1 のターゲット依存部ポーティングガイドにおける仕様として示されている。

一方、B-Method の制約として、下位のコンポーネントが上位のコンポーネントの操作を呼ぶことは出来ない。

そこで便宜的措置として、図５に示すように、当ドライバのターゲット非依存部におけるコールバック受信部のみを切り離し、「RxSerialCallback」コンポーネントとして「TargetSerial」コンポーネントより下位に設けた。

ただし、当ドライバの非ターゲット依存部において、コールバック受信部とその他との間には、割込みの許可/不許可に関する状態、受信文字の有無に関する状態の共有がなされているので、状態変数の共有が必要となる（次節参照）。

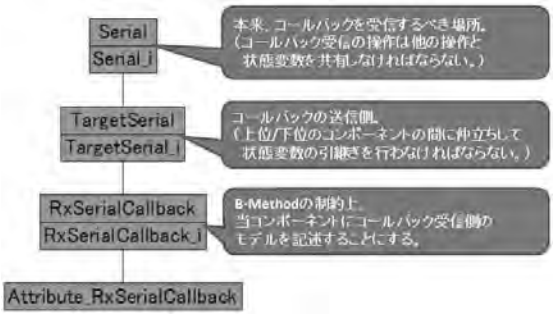

図５　コールバックのモデル記述

４－２．変数の共有について

前節のコールバックのモデルにおける状態変数の共有を記述する場合、あるいは、レジスタなどのシステム内において共有されている資源を記述する場合などの種々の事例において、異なる複数のコンポーネントより１つのコンポーネントにおける変数を共有する場合がある。

一方、B-Method においてコンポーネント間を連携させるために用いられる IMPORTS 節においては、異なる複数のコンポーネントにより連携される１つのコンポーネントを同名の別のコンポーネントして解釈されるという制約を持つ。

そこで便宜的措置として、モデルの下位のコンポーネントにおいて共有する変数とその変数を扱う操作を設けた。

図６は前節のコールバックのモデルにおける状態変数の共有の例である。

この例では、「Serial」コンポーネントと「RxSerialCallback」コンポーネントが割込みの許可/不許可に関する状態、受信文字の有無に関する状態を共有しており、それらの状態を格納する変数については「Attribute_RxSerialCallback」コンポーネントにおいて共有し、操作を受付けている。

「TargetSerial」コンポーネントと「RxSerialCallback」コンポーネントにおいては、共有する状態変数の値や状態変数の操作を下位へと引継ぐことが必要となり、本来存在しないはずの新たな状態変数が出現する形になるため、これらの新たな状態変数がこれらのコンポーネントの操作における事前/事後条件に関連し得るので、元の仕様には記されていない新たな対応が必要になる場合が生じる。

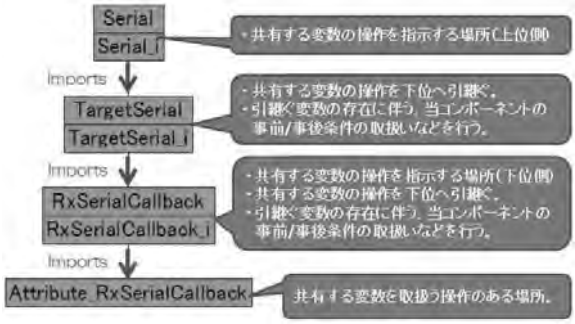

図６　記述モデルのおける変数の共有

５．おわりに

本稿では、形式手法 B-Method を用いて記述しているシリアル通信デバイスドライバについて、そのモデル記述に際して B-Method の制約に対応するために行った措置を中心に、要点の報告をした。

モデル記述を通じて、既存のマニュアル類における仕様記述の曖昧さの排除に向けて、ヒューリスティックな手法にて開発されたドライバと比較しての開発過程の可視化、顕現化に向けてのそれぞれの貢献をしているものと考える。

現在、図２のシステム構成の右側下位に当たる、ターゲットが要求するハードウェア側の仕様に合わせたモデル記述を進めている。

謝辞

本研究を進めるに当たり、平成 27 年度戦略的基盤技術高度化支援事業「農業機械のさらなる高度化と海外進出に資する次世代電子制御ソフトウェア基盤の開発」よりのご支援を頂戴しております。

参考文献および Web ページ

[1] https://www.autosar.org

[2] https://www.toppers.jp/atk2.html

[3] 水丸 和樹, 吉村 斎, 大西 孝臣, 阿部 司, 稲川 清,『RX マイコンを用いた初心者向け AUTOSAR 教材の基礎研究』, 第 15 回 複雑系マイクロシンポジウム, pp.85-86, 2016 年 3 月 5 日

[4] http://www.atelierb.eu/ja