ソフトウェア工学 96−18
（1994．1．21）

自動車用コンピュータにおける制御タイミング仕様記述方法の検討

佐野範佳* 寺嶌立太* 手嶋茂晴* 山崎知彦* 原田義久*
鈴木幹雄** 坂守**
*(株)豊田中央研究所 **アイシン精機(株)

自動車用コンピュータ（ECU）のための仕様記述方法を提案し、その記述例について述べる。近年、ECUソフトウェアの品質をより高めるための計算機支援技術が求められるようになってきた。本稿では、ECUによる自動車制御の特徴と開発スタイルを分析し、ECU仕様記述の要件を述べた後、制御タイミングおよび信号間の因果関係を図形表現する方法について提案する。本仕様記述方法では、信号変化であるイベントをノード、イベント間の因果関係をエッジで表し、因果関係のないイベント間には陽に順序を設定できるようにしている。仕様項目別にかつ段階的に分割して仕様を記述できるため、現状のECU仕様書に近い記述が可能であり、本仕様記述方法は使用者にとって馴染み易く使い易いものである。

A Graphical Form to describe Specifications about Timing and Causality for Automotive Computers

Noriyoshi SANO* Ryuta TERASHIMA* Shigeharu TESHIMA* Tomohiko YAMAZAKI*
Yoshihisa HARATA* Mikio SUZUKI** Mamoru BAN**
*Toyota Central R & D Labs.,Inc. **AISIN SEIKI Co.,Ltd.

We discuss a graphical form to describe specifications about timing and causality for automotive Electronic Control Unit (ECU), and present examples of the specifications. We analyze features of the automotive controls, ECU development style and requirements for describing the specifications of ECUs, and we propose a new graphical form of specifications of ECUs. In the graphical form, a event which means signal changing is represented by a node, a causality between events is represented by edges, and a temporal relations are defined between events without a causality. Our method describing specifications is useful for conventional users because it is possible to describe them incrementally and separately like the conventional specific documents.

1 はじめに

Electronic Control Unit (ECU)と呼ばれる自動車用コンピュータを用いた電子制御システムが自動車に多数搭載され、安全で快適、環境に適した自動車制御の実現に役立っている[1]。最近、ECUの機能が複雑になってきたため、ECUソフトウェアも大規模化、複雑化している。このECUソフトウェアの品質をより高める上で、ECUが仕様通り機能するかどうかテストするための計算機支援技術、あるいは仕様から誤りなくソースコードを自動生成する技術が必要になってきた。このため、それら計算機支援技術を実現する前提として、ECUの仕様をいかに表現するかが重要な問題となっている。しかし、ECU開発の現場では、体系的な仕様記述はまだ実施されていないのが現状である。そこで、ECUソフトウェアのテスト支援システムの構築の第一歩として、現状の開発スタイルに馴染み易くかつ体系的であることを目標に、ECU仕様記述方法を検討した。本稿では、検討したECU仕様記述方法の概要と記述例について述べる。

2 ECU仕様記述の要件

2.1 自動車制御と開発スタイル

エンジン制御ECUには、エンジン回転数、空気量などのセンサ信号から，燃料噴射量、点火時期などを計算し適切なタイミングでアクチュエータへ出力する機能がある[1]。この制御タイミングが不適切であると、十分な排出ガス浄化が行われない、燃費が悪化するなどの問題が発生する。またトランスミッション自動変速制御ECUには、アクセルの踏込み量、車速などのセンサ信号および各種スイッチから、変速時期、ロックアップ時期などを求め適切なタイミングでアクチュエータへ出力する機能がある[1]。このようにECUによる自動車制御には，適切な制御タイミングが重要である。

また、現在高精度な車両運動シミュレータは存在しないため、設計段階ですべての制御タイミングに関して仕様が決まることは少ない。試作ECUを実際に自動車へ搭載し、テスト走行を繰り返しながら最適な制御タイミング仕様を固める、という開発スタイルが一般的である。

2.2 ECU仕様記述の要件

まず、記述内容を検討する。既存のECU仕様書では、例えば以下のようなことが書かれている。

仕様項目例1：条件A1は、センサ信号1がs1以上かつセンサ信号2がs2以上のとき成立する
仕様項目例2：条件B1が成立したら、T1時間経過後、信号C1がonになる
仕様項目例3：条件D1が成立後、T2時間以内に条件D2が成立したら、そのT3時間後、信号E1がonになる
仕様項目例4：条件F1、条件F2、条件F3のすべてが順序に関係無く成立したら、T4時間後、信号G1がonになる

これらを整理するとどのようにデータを求めるか(データ依存関係)、どのような信号からどのような処理を起動するか(信号間の因果関係)および、どのような信号はどのような時間的な制約があるか(制御タイミング)、が書かれていることが分る。

よって、データ依存関係、因果関係および制御タイミングの3つを形式的に表現でき

ればよいことになる。これらの仕様のうち特に重要なのは、2.1前半でも述べたように、制御タイミングである。

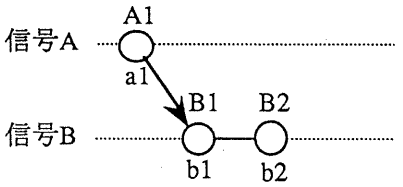
次に、記述方法を考えてみる。上記で述べたデータ依存関係および因果関係については、それぞれデータフロー図[2]、制御フロー図[2]などのグラフィカルな方法により容易に表現可能である。また制御タイミングすなわち時間関係については状態遷移図などにより表現することはできるが、ECUの仕様記述には必ずしも適していない。なぜなら、2.1後半で述べたように、制御タイミング仕様は設計段階で完全には決まらないため、ECUソフトウェア試作段階で仕様が追加／修正されることが多く、仕様全体を見通した上で記述しなければならない状態遷移図などの仕様記述方法では、手間が掛かる、誤りが入り易い、という問題があるためである。現状の開発スタイルでは、仕様項目別にかつ段階的に分割して仕様を記述できる方法が望まれる。

3 提案する仕様記述方法

自動車用コンピュータの仕様記述を対象として、制御タイミングおよび信号間の因果関係を図形表現する方法について提案する。データ依存関係はデータフロー図により別に描くものとし、提案する仕様記述方法の中では扱わない。

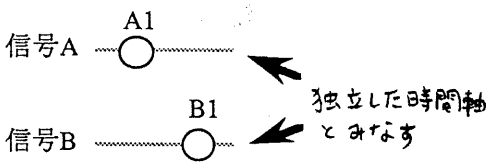
3.1 基本的な記述方法

基本的には図1に示すように、信号変化であるイベントをノード、イベント間の因果関係をエッジで表す。エッジ両端のノードにより表された（すなわち因果関係のある）イベント間には、時間に関して順序（左側は過去、右側は未来）があると解釈することにする。また後述する方法によりイベント間に陽な時間関係を設定する。ただし、同一信号のイベントを表すノードは時系列として、直線上に並べて描く。こうすると、ノードの並んだ直線は時間軸を表すことになるが、異なる時間軸には異なる時間が対応しているものとする。すなわち、図2に示すように、異なる信号のイベント間の時間関係は、特別に時間関係を設定しない限りノードの位置関係では示さないこととする。この約束により時間的に独立して発生するイベント、すなわちイベントの並行性を記述できる。またイベントを表すノードには、出力値、状態値などを属性値として設定する。



イベントA1が発生したらイベントB1が発生し、その後B2が発生する。イベントを表わすノードの下には、イベントの属性値（信号変化の内容）を置く。

図１：基本的な記述方法

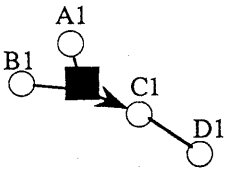


特に時間関係を設定しない限り図上の位置関係を無視して、時間的な順序を解釈する。
よってこの例では
A1 <t B1　または　B1 <t A1
または
A1 =t B1
を示している。ただしX <t Yはイベントの後にYが発生する、X =t Yはイベント X、Yが同時に発生することを表わす。

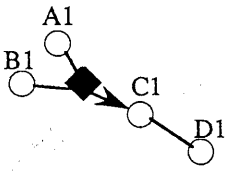
図２：イベント間の時間関係

3.2 因果関係

ECUの1つの機能に対応する因果関係は、生起条件イベント、結果イベントにグループ化し、生起条件イベントを表すノードのグループと結果イベントを表すノードのグループの間を、図3のように矢印付エッジによりつなぐことにより表す。生起条件イベント間にはAND（すべて成立）の関係であるのかOR（どれか一つ成立）の関係であるのか区別するため、図3のように矢印付エッジの前にシンボルを置く。結果イベントグループを表すノードの間には、図3のように発生時刻順にエッジによりつなぐものとする。



A1かつB1が発生したら、その後C1、D1が発生する



A1またはB1が発生したら、その後C1、D1が発生する

図３：生起条件イベントの連接

図4(a)の記述例は以下の仕様を表す。

仕様例1:イベントA1およびB1のどちらもが順序に無関係に(A1の後B1の順または、B1の後A1の順で)発生したならば、イベントC1が発生する。

図4(b)の記述例は以下の仕様を表す。

仕様例2:イベントA1が発生したならば、イベントC1、D1はこの順に発生し、イベントE1はC1とD1とは独立の順序で発生する。

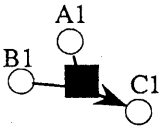


図４(a)：記述例1

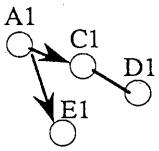


図４(b)：記述例2

図４：因果関係の記述例

順序に関していずれの例も、異なる信号のイベント間の時間関係は特別に時間関係を設定しない限りノードの位置関係では示さない、という約束により解釈されている。

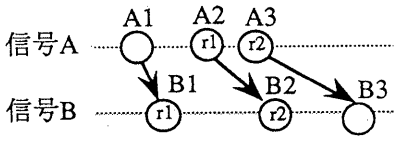
3.3 時間関係の設定

(1)因果関係による設定

3.1「基本的な記述方法」で述べたように、エッジ両端のノードにより表された（すなわち因果関係のある）イベント間には、時間に関して順序があるとみなす。

(2)陽な順序の設定

仕様によっては、異なる信号のイベント間に発生順序を明記したい場合がある。本稿で述べる仕様記述方法では、図5に示すようにノードへ共通のラベルを設定することにより、イベント間の順序をノードの位置関係により陽に表す。



ノードの中に順序関係を表わすラベルを置く。この例では

A1 <t B1 <t A2 <t A3 <t B2 <t B3

を示す。もし順序を示すラベルがすべてなければ

A1 <t A2 <t A3

B1 <t B2 <t B3

A1 <t B1

A2 <t B2

A3 <t B3

の意味となる。

図５：順序の設定

図6の記述例は以下の仕様を表す。

仕様例3:イベントA1およびB1がこの順序に発生したならば、イベントC1が発生する。

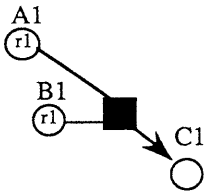


図６：記述例3

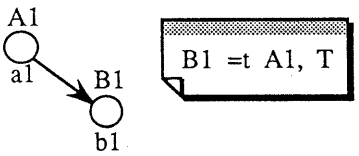
(3)時間幅の設定

例えば、あるイベントが発生して100msec後に別のイベントが発生する、という仕様すなわちイベント間の時間幅を表すために、時間幅を表す関係式をイベント間に設定する。関係式は、図７に示すように

"イベント2"　"関係記号"，"イベント1"　"時間幅"

ただし"関係記号"：＝{"=t"　|　">t"　|　">=t"}

の形式で与える。例えば関係記号に ">=t" を用いた関係式は、イベント2はイベント1から"時間幅"以後に発生する、を表す。"時間幅"は、定数またはイベントの値を引数とする関数である。



時間幅を図の右に置く。この例は

B1とA1の時間幅は、Tである

を意味する。ただしTはA1の属性値の集合から非負の実数への関数または、非負の実定数とする。

図７：時間幅の設定

3.4　イベントのキャンセル

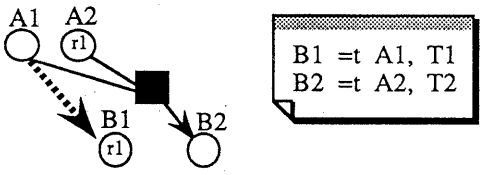
実際には発生しないけれども、他のイベントとの時間関係を設定するため、記述上必要なイベントがある。そのようなイベントは図8に示すように、破線のエッジで関係を表す。

図8の記述例は以下の仕様を示す。

仕様例4：

(1)イベントA1が発生したら、そのT1時間後、イベントB1が発生する

(2)イベントB1の発生より前にイベントA2が発生したら、イベントB1は発生せず、イベントA2が発生してからT2時間後、イベントB2が発生する



破線のエッジの右端に置かれたノードにより、実際は発生しないイベントを示す

図８：イベントのキャンセル

3.5 記述のガイドライン

同一の仕様でも利用者により記述結果が異なる、というのは問題である。そこで記述上のガイドラインを検討した。

本稿で提案する仕様記述方法では、イベントの発生順序を示す方法として、ノード間をエッジによりつなぐ方法(図9(a))と、ノード間にラベルを設定する方法(図9(b))、の2種類がある。一方、同一原因から発生する結果はできるだけまとめた方が理解し易い。そこで生起条件イベント、結果イベントは、できるだけ大きな括りで1組の因果関係としてグループ化することを、ガイドラインとする。すなわち、図9(a)のように記述する方がよい。

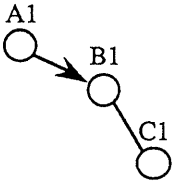


図９(a)：エッジによりつなぐ方法

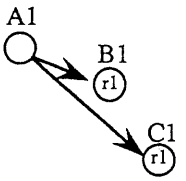


図９(b)：ラベルを置く方法

図９：記述のガイドライン

4 記述例

図10に以下の仕様を記述した例を示す。

- A1が発生したら、C1およびB1がこの順に発生する。
- C1とA1間の時間幅はT1(a1)、B1とA1間の時間幅はT2(a1)である。
- B1発生前にA2が発生したら、B1は発生せず、C2、B2、B3がこの順に発生する。
- C2とA2間の時間幅はT1(a2)、B2とA2間の時間幅はT2(a2)、B3とB2間の時間幅はT3(a2)である。

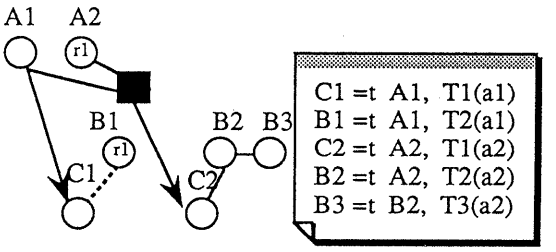


図10：記述例

5 特徴と課題

本稿で述べた仕様記述方法の特徴と課題をまとめる。

(1)並行性の記述について

異なる信号のイベント間には、特別に時間関係を設定しない限り、時間的な関係はないとみなす。このためイベントの発生順序に関する複数の仕様を一度に記述できる、という利点がある。

(2)記述し易さについて

因果関係に着目して記述するため、ECUのすべての仕様が明確になっていなくても、仕様項目別に、かつ段階的に分割して仕様を記述できる。このため現状のECU仕様書に近い記述が可能となり、馴染み易く使い易い。

(3)課題

本稿で述べた仕様記述方法をさらに使い易くするには、分割して作成された仕様項目間の矛盾チェック、仕様項目の過不足のチェックをできるようにする必要がある。これらは今後の検討課題である。

6 まとめ

自動車制御用ECUを対象に、特に制御タイミングの記述を重視した仕様記述方法について提案した。信号間の因果関係と時間関係を、分かり易く、段階的に分割して記述できるようにした点に特徴がある。

今後は、実際にECU仕様の作成を試行し、本仕様記述方法の評価を行う。また、本仕様記述方法を形式的な仕様記述言語とするための検討を進めてゆく予定である。

参考文献

[1]水谷集治監修：新カーエレクトロニクス、山海堂（1992）

[2]Derek J.Hatley：The Use of Structured Method in the Development of Large Software-based Avionics Systems、AIAA/IEEE 6th Digital Avionics Systems Conference（Dec. 1984）