

LOTOSの時間拡張に関する研究と その標準化動向について

中野 宣政、 渡辺 尚、 水野 忠則

静岡大学工学部

現行LOTOSの時間拡張として、JTC1/SC21よりこのほど発行された、ワーキングドラフトに関しその内容を紹介し、また、過去に発表のあった拡張案より、異なるポリシーに基づく主張を合わせて紹介するとともに、それに対する筆者等の見解を示す。論点としては、基本的にイベントか、プロセスか、いずれに時間属性を与えるか、その与え方が問題となること、また、時間付与に基づく必然として、平行プロセスにおけるインターリーブの可能性に関する規定をどうとるかが問題となる。いずれに関しても、本ワーキングドラフトの選択とその論理は、種々のポリシーの一つの選択の結果にすぎないと言えるが、筆者等の目指すタイムクリティカル通信に関する仕様記述に必要な特性を有していると判断する。

Survey of the Research works regarding Time enhancement for LOTOS and Introduction of its International Standardization activity

Nobumasa Nakano, Takashi Watanabe, Tadanori Mizuno

Shizuoka University

In this paper, the contents of JTC1/SC21 Working Draft for Time enhanced LOTOS is introduced relating to other papers which select and apply the different key ideas based on the different policies for Time enhancement of LOTOS, and also our opinions for these selection are described together.

The points of argument are, first, to what object(it means whether to Event, or to Process ,or to both) to endow the time characteristics, and second , the method how to endow it. And the next important argument regarding Time enhancement of LOTOS is the selection of the prescription for Interleaving of parallel process.

It is true that this Working Draft is based on the choices for those selections mentioned above and describes prescriptions and deduced definitions based on these choices of the Policy, however, in our opinion these methods and characteristics derived from this paper are adequate for the definition and description of TCCA (Time Critical Architecture) and systems especially for the systems and the architecture relating to Factory Automation arena.

1. はじめに

近来、産業界における、マルチベンダー、分散処理システム対応OS I ベースネットワークへのリアルタイム機能、性能の付与の要求が高まり、今後、それら（および一般マルチメディア通信へのサービスもふくめて）通信プロバイダーとアプリケーション間インターフェースの在り方、プロバイダーへのリアルタイム機能実現のための、メカニズムの提案、議論が始まるが、それら議論、提案に使用されるであろう形式記述技法においても性能記述を可能とすること、特に時間概念の記述を可能とすることが求められている。

過去のLOTOSの時間拡張の議論は、未だその種々の論点が集約されたとは言えないようであり、また、昨年未発行されたJTC1のLOTOS拡張に関するワーキングドラフト^[1]も、一つの立場から書かれた論文^[2]そのものが寄書となっている。従って、今後のJTC1における本LOTOS時間拡張作業に関し、その成り行きは予断を許さないが、本稿ではFA用LANのタイムクリティカル仕様記述の視点から、前記JTC1ワーキングドラフトを中心に、その他LOTOS時間拡張に関する論文から、その論点を探りその主張に関し検討する。

2. LOTOSの時間拡張に関する論点について

今まで前記SC21対応ワーキングドラフトを含め、LOTOSに関し種々の拡張案が提案されて来た。拡張の検討そのものは、従来のLOTOSシンタックス、セマンティックスへの時間の付与に関し、論理構造として考えられる多くの組み合わせから、ある特定のセットの切り出しをおこなうことを意味する。従って論理面の追求だけではなく、それを提案する側の選択ポリシーに依存するところが大きい。表 1. に、LOTOS時間拡張に関するその拡張ポリシーとその内容について典型的なものを示し、その論点を説明する。

(1) 時間データの付与の対象

基本的には、時間データをLOTOSの抽象データタイプの一つとするのであるが、イベント、プロセスの属性としてのその与えかたがポリシーにより異なる。

多数派としては、イベント、すなわちアクションプリフィックスの生起する時間を確定的に規定するもの、またはその時間領域のみを決定的に与え、実際の生起時間はその時間内で非決定的に生起させるものである。少数派として、イベントの実行時間を有限とし、その時間値を属性とするもの、または、イベントが発生してから所定のプロセス開始するまでのディレー時間を規定するもの、プロセスの処理時間を有限としその経過時間を規定するもの、がある。

これは前者（多数派）はLOTOSの基本的なイベント、プロセスに関する基本概念をできるだけ保存し、現行LOTOSの理論、環境を最大限適用しようとするのに対し、後者は、実態ベースで、イベント、プロセスの実行時間を有限とする、プラクティカルなポリシーを採用していると言える。

(2) インターリーピングに関する規定

平行プロセス間のインターリーピングに関して、イベントに時間を付与することから、現行LOTOSの非決定性が失われ、生起順に関する制限が生じるのは当然であるが、また相互の生起可能組み合わせに対する規定が必要となり、その選択をめぐる、現行のイベントの生起に関する無規定に対し生起条件を満足したら即生起を義務づけるASAP (As Soon As Possible) ルールが提唱されている。

また同じASAPルールにおいても、すべてのタイミングに関する生起可能性をみる”may” タイミングと、前後関係により、後のイベントの生起条件として、前のイベントの生起を必要条件とする”must” タイミング、の選択がある^[3]。更には、生起順の可能性に関し、外部環境の意志に

左右される外部イベントに関しては正確にインターリーピングが規定できないとし、内部イベントに関してのみ前記ASAPルールを適用するとするポリシーもある。（この場合、外部イベントの生起順の解析は、hideにより内部イベント化することによりその可能性を検討するか、または内部イベントとの組み合わせ表現により等価的にその可能性の検討をおこなう）

表 1. LOTOSの時間拡張に関するポリシーとその内容

拡張 policy	採用論文/略称	ISO/IEC JTC 1/SC 21 N 8023 (LOTOS-T) での選択
action p. への時間属性付与 deterministic non-deterministic (時間幅で生起)	拡張案の大勢である。 LOTOS-T (JTC1) 等で採用 TIC, LOTOS-T (阪大) [4] およびEXT-LOTOS等で採用	同左 同左 choiceへのguard構文で対応
(上記以外) プロセス実行時間への時間付与 action実行時間として時間付与	ET-LOTOS[5]で採用 STOC, LOTOS[7]で採用	採用せず 採用せず
discrete Time によるaction (時間の離散値としての表現) dense Timeによるaction	LOTOS/T, ET-LOTOS LOTOS-T	Time domainを利用者が任意のデータ・ソートとして選択する (descrete, dense両使用可)
ASAP action prefix (インターリーピングの規定)	"may"タイミングを主張 "must"タイミングを主張 その他 (右記など)	内部アクション対応のASAPルールを適用 action prefix のhideによる内部action置き換え分析を主張
Time dead lockの存在	ET-LOTOS (stop状態で時間停止する)	時間は永続的 (stop状態でも時間は経過) 各プロセスはIndependent Evolutionで動作
action 生起確率の指定	STOC, LOTOS (probabilistic choice) LOTOS-T(?)	JTC1のベースとなった論文ではふくまれているとしているがJTC1 版では削除されている
時間測定用プリミティブ	$t=X_0$ 等の一階述語記述 (LOTOS/T) $g@t$ (ET-LOTOS)	なし 変数choice文でその応用として対処
内部action への時間付与 禁止 付与	阪大LOTOS/T JTC1 LOTOS-T	ASAPを適用する対象として基本的である。
その他 Guard Expression での 1'st order predicate 時間記述	阪大LOTOS/T	一般的LOTOSセマンティックスの範囲で可能

3. LOTOS-T (ISO/JTC1/SC21 N8023) について

3. 1. LOTOS-Tのシンタックス、セマンティックス

以下の2つの時間に関するシンタックス、セマンティックスをスタンダードLOTOSに追加している。

表記	LOTOSにおける意味	LOTOS-Tにおける意味
a ; B	アクション" a " が起きてプロセスは" B " として振る舞う。" a " が生起する時間は不定	アクション" a " はASAP (できるだけ早く) に生起すること。" a " の生起後プロセスは" B " として振る舞う。" a " の生起を環境がブロックしても時間は経過する。
exit	プロセスの正常完了が生起する。但し、いつ生起するかは不定。	プロセスの正常完了はASAPに生起すること。
a { t } ; B	—	アクション" a " は時間 t が経過した時点でまさにその時生起する。 同時刻に環境が" a " の生起をブロックした場合は" a " は生起し得ない。但し其の場合でも時間経過はブロックされない
exit { t }	—	プロセスの正常終了が時間 t の経過時点で生起する。

3. 2. LOTOS-Tにおける時間プロパティの例 (以下に限らない)

LOTOS-Tにおいて、“ $a(0);B$ ”と、“ $a;B$ ”は異なる。前者はアクションaは即時発生する必要がある(時間ゼロで)が、後者はaが発生するまでまたされることになる。その意味ではLOTOS-Tにおける後者の意味合いはLOTOSのそれと変わらず、実質的な違いは無い。

時間の概念は、3. 1. の2つの拡張、即ちアクションプレフィックスおよび正常プロセス終了においては新たに設けたシンタックス、セマンティックスにより直接的あるが、他の遷移においては、単なる数値(または一般的な変数)として扱われることになる。例えば、下記の例において、

```
choice t: nat [] [f(t)] -> a{t};B
```

アクションaは、 $f(t)$ が真となる条件を満たすtの値で生起することになる。ここではtは単なるnatural numberとしてLOTOSシンタックス、セマンティックス上で扱われ、それ以上の時間としての意味は、アプリケーションとしてつける。以下、定量的な性能仕様記述に必要な各種プロパティをLOTOS-Tのアプリケーション上で意味を持たせた例として示す。

●D e l a y s

```
choice t: nat [] [t>5] -> a{t};B
```

アクションaは、5単位時間経過後生起し、Bとして振る舞う。上記述において、 \rightarrow の左では単なるnatとしての扱いであるが、 \rightarrow の右では値が時間としての意味を持つ。

●W a i t s (A s y n c h r o n o u s な 推 移)

```
data_req ? d: data; Data_transfer_Phase [] disc_req; Disc_Phase
```

ASAPの特性により外部環境がゲートdata_reqまたはdisc_reqのいずれかを生起させるまで待ち、ゲートdata_reqの場合はdata_transfer_phaseへ、disc_reqの場合はdisc_phaseへと移行する。

●S y n c h r o n o u s な 推 移

```
process clock [tick]: noexit :=
    tick {3}; clock [tick]
endproc
```

外部環境より供給されるtickは、process clockにより、3単位時間毎にのみ同期され生起し得る。

●T i m e o u t s

```
ack; send_next_msg [] i {5}; retransmission
```

ackが生じたらsend_next_msgへ移行する。またackが生じる前に5単位時間経過したらretransmissionへ移行する。

●A T i m e r

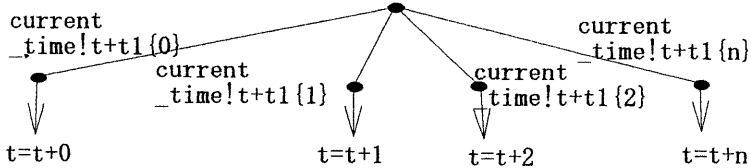
```
process timer [start, time_out]: noexit :=
    start ? t_0: nat; (time_out {t_0}; timer [start, time_out])
    [] timer [start, time_out]
```

プロセスtimerは、ゲートstartで環境より設定時間を t_0 に受け、設定時間 t_0 経過で環境よりのtime_outと同期し、次のタイマー設定に備えるか、または設定時間満了以前の再設定を受け付ける。

●時間測定

```
process global_time [current_time](t: nat): noexit :=
    choice t_1: nat [] current_time ! t + t_1 {t_1}; global_time [current_time](t + t_1)
endproc
```

choice $t_1 \sim$ により、 t_1 の値は任意の nat をとれる。即ち、 $\{t_1\}$ は、 $\{0\}, \{1\}, \{2\} \dots \{n | ne \text{ nat}\} \dots$ のいずれもある。従って、時間の経過にしたがってゲート $current_time$ は次々と開き得る。しかしながら、環境が $current_time$ を生起するまで、生起し得ず、環境が $current_time$ を生起したときまたま開いていた $\{n\}$ すなわちプロセス $global_time$ を呼んでからの計時時間に等しい値 n が t_1 の値となる。この時の t (t はプロセスがインスタシエートされたときに0にセットされている)の値と t_1 を加算し、 t に代入する。従って、 t の値はプロセスがインスタシエートされてから、 $current_time$ を環境が生起したときまでの時間となる。(次図参照)



3. 2. 時間ドメイン

LOTOS-Tでは、時間(エレメント)を自然数による指定の他、リアルタイム記述の場合いわゆる *dence domain*による指定が可能としている。数値としてはいずれの場合もLOTOS標準データタイプ・ライブラリーのNATURALS/Positive natural Numbersの定義を援用できる。

3. 3. 遷移ルール

紙面の都合により省略する。

3. 4. ASAPプロパティ

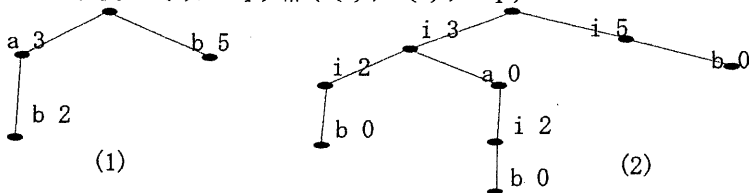
本ワーキングドラフトにおけるASAP規定とは、厳密にはシステムの遷移可能性を外部の意志によらない内部アクションに置き換えて分析することとするものである。

例えば、

$$(a\{3\}; stop) \parallel (b\{5\}; stop)$$

遷移ルール(3. 3で省略)をあてはめると次図(a)のアクション木で示される振る舞いとなる。右の枝は、時刻3で環境がイベント a を発生できず、時刻5でイベント b を発生したもの、左のアクション枝は、 a, b とも生起したものを示す。次のプロセスは、次図(b)でその挙動が示される。この時、

$$(i\{3\}; a\{0\}; stop) \parallel (i\{5\}; b\{0\}; stop)$$



i_5 が生起することにより i_3 以降が生起し得ないことになる。この場合、ASAPルールでは、時刻が短い i_3 がまず発生し、 i_5 は発生し得ない、と解釈する。したがって、 i_3 で a が生起し得れば a_0 が生起し、ついで i_2 の生起の後、 b_0 が生かされる。 i_3 で a が生起不能であれば i_2 が生起し、 b_0 が生かされる。

ASAPルールによれば、システムの遷移は、各イベントが内部アクションであった場合起り得る順序で生起する。従って、hideオペレータを仮において分析する。

$hide\ a\ in\ (a\ \{3\};\ stop)\ \parallel\ (b\ \{5\};\ stop)$
 $then,\ the\ result\ should\ be\ "i\ 3,\ b\ 2"$. or
 $hide\ a\ in\ (i\ \{3\};\ a\ \{0\};\ stop)\ \parallel\ (i\ \{5\};\ b\ \{0\};\ stop)$
 $then,\ the\ result\ should\ be\ "i\ 3,\ i\ 0,\ i\ 2,\ b\ 0"$.

3. 5. 仕様等価性の検証

強、弱 bisimulation についてのルールが規定されているが、紙面の都合で省略する。

4. TCCA記述からの評価

JTC1 拡張ワーキングドラフトの内容は、TCCA 関連仕様の記述に必要な特性を有していると思われるが、今後実際の仕様記述に適用し、その記述性、問題点の詳細の検討をおこなう。

5. 異なるポリシーについての主張検討

今までに提唱された LOTOS の時間拡張に関する主張内容を紹介し、それに対する筆者等の FA、TCCA 仕様記述の観点からの見解を表 3. に示す。

表 3. LOTOS 時間拡張に関するポリシーに関する主張と見解

ポリシー/提唱者	主張概要	TCC L 記述対応での筆者の見解
LOTOS の時間拡張に 反対 [7] BoH93, U. of Kent FORTE' 93. pp469-484	LOTOS に時間拡張を持ち込むことにより、形式仕様記述としての LOTOS の基本的抽象性質が損なわれる。 時間仕様記述に QTL を併用する。	記述対象が何であるかにより一概に言えない。但しセマンティックスが明確であればアプリケーションで記述内容を選択すればよいのではないか。
action prefix への時間 制限付与に反対 [5] LeL93, F. N. R. S. FORTE' 93. pp485-500	action prefix は、外部環境にその生起は依存しているから、時間制約を設けることは本来的でない。振るまいに時間概念を入れるべき。	仕様記述の点から言えば、外部環境を含めた振る舞いを記述しているのであって時間制約が仕様そのものであるのではないか。振る舞いに時間概念を入れると、今度は振舞同士の同期をどうするかなどの問題が生じ、プロセス間での新たなシグナルを設けたりする事になる。

6. おわりに

以上、JTC1 の LOTOS-T 時間拡張案を中心にその拡張内容について、他の主張を合わせて紹介し、また筆者等の見解を述べた。また、本ワーキングドラフトは、TCCA 関連仕様記述に必要な特性を有していると判断している。今後は TCCA 関連仕様の具体例の記述による記述性の評価と問題点の把握をおこなうとともに、そのシミュレーション実行環境の構築をおこなう所存である。

参考文献

- [1] ISO/JTC1/SC21 N 8023 Working Draft pp157-179
- [2] C. Miguel, A. Fernandez, L. Vidaller, Extending LOTOS Towards Performance Evaluation, FORTE '92 Participant's Precedings, pp115-130
- [3] J. Quemada et al, TIC: A TIMED CALCULUS FOR LOTOS FDT2, IFIP, 1990 Preceding, pp197-198
- [4] A. Nakata, T. Higashino, K. Taniguchi LOTOS enhancement to specify time constraint among non-adjacent actions using 1st-order logic, FORTE '93 Participant's Precedings, pp453-467
- [5] L. Leonard and G. Leduc An Enhanced Version of Timed LOTOS and its Application to a Case Study, FORTE'93 Preceding, pp485-500
- [6] N. Rico and G.v. Bochmann, Performance description and analysis for distributed systems using a variant of LOTOS, 11th International IFIP WG6.1 Symposium on Protocol Specification, Testing, and Verification
- [7] H. Bowman, G.S. Blair, L. Blair, A.G. Chetwynd, TIME VERSUS ABSTRACTION IN FORMAL DESCRIPTION, FORTE'93 Preceding, pp469-475