マルチメディア通信と分散処理 69－7
（１９９５．３．２）

ソフトTCCSとその開発検証システムの構築について

中野 宣政† 安藤 勉‡ 太田 賢‡ 佐藤 文明‡ 水野 忠則‡

†三菱電機（株）、‡静岡大学

既存のオープンネットワークを利用し、その上にアプリケーション機能としてTCCS (Time Critical Communication System)を構築する、いわゆるソフトTCCS 実現メカニズムの仕様記述の視点から、ISO/IECにおけるLOTOS の時間拡張仕様案を検討してきた．現在審議中の仕様案には、プロセスへのディレー時間の付与、イベントの生起時間検出機能などが追加され、さらに時間経過の効果を表現する補助演算子が提案されている。また内部アクション生起に関する新しい解釈が加えられた．我々はこれに対し、分散処理内容を容易に記述するためのローカルタイムのタイムドメインへの導入、また、仕様記述／実装において不自然な、隠蔽されたイベントへの新しい解釈（マスト・タイミング）の除去を主張する．

Soft TCCS and it's Development/Validation System

Nobumasa Nakano †, Tsutomu Ando ‡, Ken Ohta ‡, Fumiaki Sato ‡, Tadanori Mizuno ‡

† Mitsubishi Electric Co., Ltd. ‡ Shizuoka University

We have been studying on the documents that relate to the enhancement work of LOTS in ISO/IEC JTC1 as the candidates for the Formal Description Language to describe and validate TCCS (Time Critical Communication Systems) that will reside on top of any Open Networks. The current Revised Working Draft has been enriched by additional Delay operator for any Processes, Measurement property for the elapsed time in offering the event, and new auxiliary functions to describe the effectiveness of time-aging in the process. Besides, in this WD, newly defined Semanticses for internal event property have been proposed. In the consequence of our study so far, we propose to add some schemes representing local clocks to specify distributed TCCS freely, and also to restrict the scope of must timing property to internal event only but excluding hidden events.

1．はじめに

当研究会 94-DPS-66 において、形式仕様記述言語LOTOS（国際標準［ISO 8807］）の時間拡張案LOTOS-T[1]とそれを採用したTCCA(S)の仕様記述とその検証システムの構想について提案した[2].

国際標準化審議においては、ここ１年の間に３件のワーキングドラフト[3] [4] [5]が提出審議されており、仕様的にも当初[1]のイベントへの時間制限付与のみのプリミティブな提案から、任意のプロセス対応のディレー時間の付与、イベントの生起に要した時間検出機能など、仕様記述上便利な機能追加の他、さらに時間導入にまつわる本質的な問題として、時間経過の効果を表現する新たな補助演算子が提案されている．すなわち、時間仕様を内蔵したプロセスにおける一般チョイスや、一般的並列動作に関する仕様記述対応の補助演算子導入提案がなされている．また、時間概念の導入により付随的に生ずる、プロセスの実行優先度の記述／制御の必要性から、内部アクション生起への必然性の特質の付与提案がなされている．

我々は、今後の等時性を要求するデータ伝送、レート制御、あるいはマルチメディア同期など、いわゆるTCCA(S)への応用の視点から、これら提案内容の妥当性を検討中である．本稿では、以上述べた、LOTOSの時間拡張に関する国際標準化仕様提案書の内容、主張を紹介するとともに、TCCA(S)仕様記述への応用の視点から、セマンティクス仕様について現状で判明したその妥当性、問題点を述べる．

内容の変遷から見ると、最初の新作業項目提案ＮＰ(New Work Item Proposal)としてのLOTOS-T [1]は、見直され、作業原案ＷＤ第１版(Working Draft)の拡張提案Timeの付属書“F”[3]となった．また同ＷＤ‘Time’の付属書“G”として、新にET-LOTOS [4]が提案された．ＷＤ第２版(Revised Working Draft) [5]においては、この２つの付属書が一本化され、付属書“E”となっている．以下ＷＤ第２版を主体にその内容を紹介し、問題点とその解決策を検討するが、古い方の文献を参照することにより問題がはっきりする部分もあるので、その場合はそちらも参照するものとする．また２章の記述は、ワーキングドラフト仕様書[5]に基づくが、意味解釈で確認を要する箇所には、我々の解釈を（＊　～　）として記載している．

2．形式的セマンティクスと拡張LOTOSの特質

2．1．タイムドメイン

タイムドメインはデータソート（Q(time)）集合として定義される．但し、timeはLOTOSソートである．タイムドメインとしては、自然数をモデルとする離散的なものと、分解能任意の有理数をモデルとする、より稠密なもの（数え上げ可能なもの）を、設計者の当面する問題向きに任意に選択できる．

タイムソートの定義を以下に示す．

・全順序関係を“＞”で与える．

・要素0∈Q(time)とし、∀r∈Q(time):r≠0 => r>0

・要素∞∈Q(time):r≠∞=>∞>r

・計算可能な関連演算"+:Q(time),Q(time)>Q(time)

であり、

∀r,r1∈Q(time):r>r1<=>∃r'>0・(r'+r1)=r

∀r,r1∈Q(time):r>0 and r1≠∞=>r+r1>r1

∀r∈Q(time):r+0=r

∀r∈Q(time):r+∞=∞

2．2．時間拡張LOTOSの動作式構文

時間拡張LOTOSの動作式の構文は、BNF記法により以下のごとく定義される．

P:: = Q *where* $\tilde{X} = \tilde{Q}$

Q:: = *stop* | *exit* $(e_1...e_n)\{T\}$ | $gd_1,...d_n\{t\ in\ T\}$ $[SP];Q$ | $i\{t\ in\ T\};Q$ | $Wait(d);Q|Q|[]Q$ $|Q[\Gamma]Q|hide\ \Gamma\ in\ Q|Q>>accept\ x_1{:}s_1,...$ $x_n{:}s_n\ in\ Q|Q[>Q|X\ |[SP]->Q|let\ x_1{:}s_1,.$ $x_n{:}s_n\ in\ Q$ | *choice* $x_1{:}s_1,...x_n{:}s_n\ []Q$ | inf $x_1{:}s_1,...x_n{:}s_n\ |||\ Q$

2．3．表記法

P,P',Q,Q' は時間拡張LOTOS の振る舞い記述を示す．P-d->P' , d∈$D_{0\infty}$ は、プロセスPはd時間幅アイドルする（すなわちAにおいて何等アクションを起こせず）その後P'として振る舞う、ことを意味する．P-/d->, d∈$D_{0\infty}$ は、¬∃P'・P-d->P' の意で、Pはd時間幅アイドルできないことを意味する．この表記においては、P、及びP' は閉じている必要がある．すなわち、P,P' において自由変数を有しないこと、が条件とされる．

（*この条件は、推論規則を働かせる場合は、各変数は束縛されている（保護されている）か、または何らかの値が代入されていなければならないことを言っている．そうでなければ変数の値が決まらず、推論規則が働かずプロセスはブロックしてしまう）

2．4．時間を停止させるLOTOS 仕様　*ブロック*

今回のWD にて、何等の公理、推論規則を有しない　*ブロック*　と命名されたプロセスが導入されている．このプロセスはいかなるアクションも遂行せず、時間の進行をブロックする．　*ブロック*　の例としては、保護されていないプロセス仕様 P:=P なるLOTOS 仕様P があげられる．このような仕様P においては、公理、推論規則が何等見いだせないため、プロセスP において時間は停止する．

2．5．推論規則

以下の推論規則において、d∈$D_{0\infty}$, d^-, d'∈D_{∞}, d^+∈D, g∈G, およびa∈Aである．

休止

（S）　stop-d->stop

stop状態において時間は停止せず進行することを公理として定める。

可観測アクションプレフィックス

(AP1) gd1...gdn{t in d^-+d..d^++d}[SP];Pgv1,...gvn->
[ty1/y1,...tym/ym,0/t]P

(AP2) gd1...gdn{t in d^-+d..d^++d}[SP];P-d->
gd1...dn{t ind^-..d^+}[[t+d/t]SP];[t+d/t]P

(AP3) gd1...gdn{t in d^-..d^+}[SP];P-d->stop　　(d>d^+)

(AP4) gd1...gdn{t in 0..d^++d}[SP];P-d->
gd1...dn{t in 0..d^+}[[t+d/t]SP];[t+d/t]P

属性値はアクションの生起し得る期間をTの中に制約する．すなわち (AP2) では、$gd_1...d_n${t in $d_-..d_+$} [SP] ;P において、ゲートgにおけるアクションの生起は期間d^- からd^+ の間に起こる．

(AP3)において、d^+タイムユニットまでの間gにおいて何等アクションの生起がなかった場合、そのプロセスはstop となる．

属性値 {t in T} においてt はソート time の変数であり、この変数はアクションが提供され生起したとき、それをディレー値として測定するのに使用される．また変数t は SP 内で一つだけ使用できる．

(* すなわち生起した時間で t がインスタンシエートされ、その値が選択述語式 SP および P に代入されている．たとえば (AP1) では、ゲートgは即生起した状態を示しており、t のインスタンスは0 である．(AP2) では、d 単位時間経ってもgが生起しない状態で、推論結果（右辺）は、次回の推論時の前提（左辺）となる）

内部アクションプレフィックス

(I1) i{t in 0..d+};P-i->[0/t]P

(I2) i{t in d^-+d.. d^++d};P-d->i{t in d^-.. d^+};[t+d/t]P

(I3) i{t in 0.. d^++d};P-d->i{t in 0.. d^+};[t+d/t]P

i {t in d^-.. d^+} ; P　においては、d^+以上の遅延は起こり得ない．もし時間が限界まで進んで i が生起しなければ、 i が生起するまで時間は停止する．これは i の生起は強制的であると言うことを意味する．

遅延プレフィクス

(D1) P-a->P' ⊃Wait(0);P-a->P'

(D2) Wait(d'+d);P-d->Wait(d');P

(D3) P-d->P' ⊃Wait(d');P-d+d'->P'

Wait (time) ; Pは, P の実行が time だけ遅延せられる意である．

終了

(EX1) exit(e_1,...e_n){0..d^+}- δ v_1...v_n->stop
但し v_i=[t_i] e_i=t_i の場合
$v_i \in Q(s_i)$={[t]|tはソートs_iのｸﾞﾗｳﾝﾄﾞﾀｰﾑ}
d_i=any s_i の場合

(EX2) exit(e_1,...e_n){d^-+d..d^++d}
-d-> exit(e_1,...e_n){d^-..d^+}

(EX3) exit(e_1,...en){d^-..d^+}-d->stop ($d>d^+$)

(EX4) exit(e_1,...e_n){0..d^++d}-d->exit(e_1,...e_n){0..d^+}

属性値{T}はアクションプレフィックスにおける意味合いと同一である．exit{T}はδを時間インターバルT内でのみ実行可能であることを意味する．

チョイス

(Ch1) P-a->P' ⊐ P[]Q-a->P'

(Ch1') Q-a->Q ⊐ P[]Q-a->Q'

(Ch2) P-d->P',Q-d->Q' ⊐ P[]Q-d->P'[]Q'

(Ch2)は時間の一貫性を公理として示している．

汎化チョイス

チョイスのセマンティックスx_1:s_1,...x_n:s_n[]Pは、新たに提案された補助演算Achoice (d) x_1:s_1, ... x_n:s_n []Pにより定義されている．ここでd∈D_∞である．また、AchoiceはAgedChoiceを表す．

補助演算子の定義により、Choice x_1:s_1, ... x_n:s_n [] P= Achoice (0) x_1; s_1, ... x_n:s_n [] P と表される．

(GC1) Age(d', [tx_1/x_1,...tx_n/x_n]P)-a->P
⊐Achoice(d') x_1:s_1,...x_n:s_n[]P-a->P'
但し、tx_iは[tx_i]∈Q(s_i)なるｸﾞﾗｳﾝﾄﾞﾀｰﾑ

(GC2)[tx_1/x_1,...tx_n/x_n]P-d+d'->
$\forall$ <tx_1,...tx_n> ・ [tx_i]∈Q(s_i), i=1,...n
⊐Achoice(d')x_1:s_1,...x_n:s_n[]P-d->
Achoice(d+d') x_1:s_1,...x_n:s_n[]P

補助演算子は属性値として、振る舞い記述Pと時間値d∈D_∞を取り、振る舞い記述P'を返す．すなわち、P→P_1⇨P'～P_1（～は強模倣性を表す）．Age(d,P)の結果としては、もしP-/d->の場合は（たとえばPが保護されていない場合）(GC2)の前提条件（*すべてのtx_iは条件[tx_i]を満たさなければならない）でガードされ、ガードが満たされぬケースではAgeは使用されないことを保証している．　同一の理由により、Achoice(d) x_1 :s_1, ...x_n: s_n[P]のセマンティックスは、P-/d->の場合あり得ない．

(*Agedchoiceの直観的意味を考えると、時間の経過と変数の値の取りようによって、Pの時間依存の状態変化が非決定的に変化し、P'となる．従って最終状態P'は、d単位時間内のチョイスの繰り返し、すなわち、結果->前提の繰り返し推論を、少なくともn回繰り返すことになる)

平行合成

(PC1) P-a->P' ⊐ P[[Γ]]Q-a->P' [[Γ]]Q
但し(name(a)¬∈Γ ∪ {δ})

(PC1') Q-a->Q' ⊐ P[[Γ]]Q-a->P[[Γ]]Q'
但し(name(a)¬∈Γ ∪ {δ})

(PC2) P-a->P',Q-a->Q ⊐ 'P[[Γ]]Q-a->P' [[Γ]]Q'
但し(name(a)∈Γ ∪ {δ})

(PC3) P-d->P',Q-d->Q ⊐ P[[Γ]]Q-d->P' [[Γ]]Q'

無限平行合成

チョイス同様、無限x_1:s_1,...x_n:s_n|||Pのセマンティックスは、新たに提案された補助演算子により、Ainf(d) x_1:s_1,...x_n:s_n|||Pと定義されている．ここにd∈D_∞である．AinfはAgedinfを意味する．定義によりinf x_1 :s_1, ... x_n :s_n|||P =Ainf(0)x_1:s_1,...x_n:s_n |||P である．このような中間的な演算子は、もし自由変数が無いのであれば不要である．(*これは、先に定義されたLOTOSブロック　仕様、すなわち束縛（保護）されていない変数、またはプロセスがあると、推論が停止してしまうため、その救済策として、上記補助演算子を設けたのである)

(IP1) Age(d', [tx_1/x_1,...tx_n/x_n]P-a->P'
⊐Ainf(d')x_1:s_1,...x_n:s_n ||| P -a->P' |||
(Ainf(d')x_1:s_1,...x_n:s_n ||| [not(x_1=tx_1
$\wedge$...x_n=tx_n)] ->P
但しtx_iは[tx_i]∈Q(s_i)であるｸﾞﾗｳﾝﾄﾞﾀｰﾑ

(IP2) tx_1/x_1,...tx_n/x_n]P-d+d'->$\forall$[tx_i]∈Q(s_i), i=1,...n
⊐ Ainf(d')x_1:s_1,...x_n:s_n ||| P -d->
Ainf(d+d') x_1:s_1,...x_n: s_n ||| Age(d, P)

(IP3) p-a->P' ⊐ inf ||| P-a->P' ||| (inf ||| P)

(IP4) p-d->P' ⊐ inf ||| p -d-> inf ||| P'

inf x1:s1,...xn:sn|||Pは、Pの変数が取りうる範囲の

あらゆるインスタンシエーション対応のインターリービングとして記述される．規則(IP3), (IP4) は自由変数が仕様上ゼロの場合の特殊ケースに相当する．このケースにおいてはinf|||Pは同一プロセスの平行プロセスインスタンスとしての無限生成に相当する．本ET-LOTOSにおいては、そのような保護されていない動作式（たとえば　Ps:=P ||| Ps）は時間を停止させるから、再帰的プロセスとしては表現できない．

ハイド（紙面の都合上、議論にに必要もののみとし他は割愛する）

(H3) P-d->P', $\forall g \in \Gamma$ ・（P-g¬->$\wedge \forall$ P" $\forall$ d'＜d ・
（P-d'->P"⇒P"-g¬->））
⊃hide Γ in P -d->hide Γ in P'

規則 (H3) は時間拡張 LOTOS として採用した、*最大前進原理*　を表現するものである．この原理は、隠されたイベントは、必然的 (must) に生起すべきこと、を規則とする。

順次合成

(En3) P-d->P', P-δ¬->, $\forall$ P" d'< d ・
(P-d'->P"=>P"-δ ¬->)
⊃P>>accept x_1: s_1,...x_n:s_n in
Q-d->P' >>accept x_1:s_1,...x_n:s_n in Q

δの生起は、順次合成オペレータにより隠蔽される．その生起は　*最大前進原理*　により、できるだけ早く生起する．

割り込み、ガード、置換、プロセスインスタンシエーション（紙面の都合上割愛する）

2．6．補助機能

ハイドと順次合成

タイムドメインを稠密とすると、(H3), (En3)の前提が無限大となる．この問題を克服のため”Γ内ではPとして、t以前はノーアクション”を意味する補助演算子NABΓ（t, P）の導入が提案されている．但しΓはG (H3 のルールに使用）のサブセット、または｛δ｝（規則En3)として使用）の集合であるかのいずれかとし、時間と（閉じた）振る舞い記述Pを属性として持つものとする．もしPが、そのアクションプレフィックスがΓ内にあるとして、時間t以内に生起し得ないとすると、NABΓ(t, P) は真となり、それ以外では異となる．NABΓ(t, P) はP-t->においてのみ有意とする．NABΓ(t, P) により、(H3) と(En3) は以下のごとく書き換られる．

(H3') P-d->P', NABΓ(d,P)
⊃hide Γ in P -d->hide Γ in P'

(En3') P -d-> P', NAB{δ}(d,P)
⊃P>>accept x_1:s_1,...x_n:s_n in Q-d->P'
>>accept x_1:s_1,...x_n:s_n in Q

汎化チョイスと無限併列合成

(GC2)と(IP2) においても、タイムドメインが稠密であるとき前提条件が無限大となる．この問題を避けるため、”アイドリングできる”意味のC_i(t, P) なる補助関数C_iが提案されている．Ci (t, P) は属性として、時間値 t と（閉じた）動作式P を持つ．それは、P はt 時間ユニットアイドルできる、と定義される．C i 関数により、(GC2) と(IP2)規則は以下のごとく書き換えられる．

(GC2') Ci (d, Achoice(d_1) x_1:s_1,...x_n:s_n [] P)
⊃Achoice(di) x_1:s_1,....x_n:s_n [] P -d->Achoice(d+d_1)
x_1:s_1,...x_n: s_n [] P

(IP2') Ci (d, Ainf(d_1) x_1:s_1,...x_n:s_n ||| P)
⊃Ainf(d_i) x_1:s_1,....x_n:s_n ||| P -d->Ainf(d+d_1)
x_1:s_1,...x_n:s_n ||| P

3．考察

3．1．タイムドメインについて

タイムドメインの規定としては、プロセスがインスタンシエートされたとき要素０をとり、唯一無二のペース（精度も合わせ、いかなるペースかはそれは何も決っていない、実装上の問題としているのであろう）で歩進するグローバルな時間 Q(time) が規定されているのみである．形式記述の理論上からはそれで十分であろうが、仕様記述、特にネットワーク上に分散配置された、例えばソフトＴＣＣＳのごときローカル時間依存のアプリ

ケーション仕様記述には問題がある.

すなわち、タイムソートとしてはアプリケーションシステムとしての最稠密な要求時間仕様をグローバルタイムの精度として持たせ、それぞれグローバルタイムに対し任意の進み／遅れを有する、複数のローカルタイム$Q_{l1}(time),...Q_{ln}(time)$を仕様的に簡明に指定できる、マルチタイムベーススキームが有用である、と考える.

3．2．時間のブロックについて

ET-LOTOS において時間のブロックを生じるケースは、いわゆるLOTOS *ブロック　仕様*として動作仕様記述した場合と、内部アクションと生起時間の相互作用の場合である．我々は問題として後者の方が重大である、と考える．なぜならば前者の　*ブロック的仕様記述*　はほとんどあり得ないし、また避け得ると思われるのに対し、後者は可観測ゲートの隠蔽などにより、内部アクションとしての挙動は、仕様記述として不可避的に出現する可能性があるからである．（これに関してはさらに3．3．項で述べる）また、時間のブロックの波及する範囲の明確化が必要と考える。

3．3．内部イベント対応プロパティー

i {t}; P の意味は、i は時間インターバルT 内に生起　*せねばならない*．その正当化の事例として3つのケースが文献[4]に示されている．いずれの例においても、i はi {0} として、活性化されたら無条件生起する役割を担っている．我々はその場合のセマンティクスの設定、および推論規則に異論はないが、隠蔽されるイベント総てがi としての特性を有するもの、とされている点は奇異と思える．隠蔽されたからといってその制御メカニズムは不変なのだから、ここは（隠蔽されたゲートイベントに関しては）規則 (AP3) に相当する内部イベントの遷移規則を設けるべきである．また、文献[4]の正当化例において、隠蔽ゲートに i と同様の生起必然性を持たせる理由については何も示されいない．すなわちその文脈では、単にi{0}を必然的に生起するイベントであると役割づけている。

4．おわりに

以上、現在ISO/IEC において審議中の仕様記述言語 LOTOS の時間拡張仕様について、そのワーキングドラフト第2版の内容を紹介し、我々の研究対象であるソフトTCCA(S) 仕様記述への応用の視点から、仕様上の問題点および我々の考える解決策について述べた．すなわち時間ドメインに関しては、応用面からグローバル時間と複数のローカル時間の両記述スキームを言語仕様として規定して置く必要があることを主張する．内部イベントの生起必然性については、我々も時間確定的に生起するイベントを新たに設けることは、単純なタイマー機能を仕様記述する為にも不可欠であることを認めるところである．ただし、隠蔽されたゲートイベントまで必然性を付与することには反対であり、それには可観測ゲートイベント対応のいわゆるmay タイミングを適用することを主張する。

今後国際会議における本関連ワークの審議の経緯を見守るとともに、本題であるソフトTCCA(S) を実現するメカニズム記述への採用を並行して検討していく所存である。

参考文献

[1] ISO/IEC JTC1/SC21 N 8023: Initial Draft on Enhancements to LOTOS, pp157-179.

[2] 中野、太田、渡辺、水野：TCCA仕様記述対応LOTOSの時間拡張案とその実行環境について,94-DPS-66,pp43-48,1994.7

[3] ISO/IEC JTC1/SC21/WG1/Q48.6 :Revised Draft on Enhancements to LOTOS, ANNEX F: Time:LOTOS-T,March 28,1994.

[4] ISO/IEC JTC1/SC21/WG1/Q48.6 :Revised Draft on Enhancements to LOTOS, ANNEX G:Time:ET-LOTOS

[5] ISO/IEC JTC1/SC21/WG1 N 1349:Working Draft on Enhancements to LOTOS ANNEX E: Time,Octover, 1994.