A Time Fidelity Control Foundation for Hierarchical Discrete-Event Systems

Quang Ha Ngo, Student Member, IEEE, and Kiam Tian Seow, Senior Member, IEEE

Abstract—In the existing paradigm of formal languages and finite automata, the hierarchical control setup for untimed discrete-event systems (untimed DES’s) is a standard high-level command and low-level control structure, and timed DES’s (TDES’s) can be modeled by a class of automata called timed transition graphs (TTG’s) incorporated with time fidelity. In this paper, using the same hierarchical control setup, with the TDES at the low level modeled by a Moore TTG with time fidelity, supporting concepts are proposed for a timed version of the concept of output-control consistency for hierarchical control. Importantly, this new timed consistency concept also preserves the time fidelity of the resultant system model at the high level, and lays a time fidelity foundation for extending the consistency of hierarchical control in untimed DES’s to TDES’s.

Index Terms—Hierarchical control, timed discrete-event systems, formal languages and finite automata.

I. INTRODUCTION

In the general framework of formal languages and finite automata, the new concept of timed output-control consistency is developed in this paper for hierarchical control of timed discrete-event systems (TDES’s). Within the framework, a lot of hierarchical control research built upon the seminal work on supervisory control [1] for logical or untimed DES’s has been reported in the literature. In contrast, there is relatively little reported work on real-time hierarchical control, other than in [2] which extends logical hierarchical control [3], [4] to a timed version.

Our research in this paper is anchored in the basic but general two-level hierarchical control setting [3], in which the system at the high level is an abstraction of the system at the low level that drives the former via an information channel. The low-level system is modeled by a Moore automaton [5] constructed from an untimed DES (automaton) model and a hierarchical reporter map modeling the information channel. Our research work is built upon the monolithic control theory for TDES’s [6], with the low-level system similarly modeled by a Moore automaton but is constructed from a TDES (automaton) model proposed in [6] and a timed hierarchical reporter map. This TDES model is a timed transition graph and possesses sound system (event-) timing semantics. By sound system timing semantics, we refer to time fidelity of the model, characterizing time progression as unstoppable and never halting an executing activity event.

From the design perspective, the purpose of the high-level system in the hierarchical control setting is to provide significant and unambiguous information of an engineering application of interest at a suitable level of abstraction (such as, e.g., robotic object picking and placing), for clearer specification design from above for control synthesis, without the need to delve into detailed information of the low-level system (such as, e.g., robotic arm extension and contraction). This has been a compelling motivation for hierarchical control design [3]. Generalizing to real time, the high-level model abstraction, in our opinion, might aggregate time but must preserve time fidelity as with the low-level system model. Otherwise, designers would need to go beneath the abstraction level, increasing specification design complexity and effort as a result just to ensure that desired timing properties are also met.

Central to system abstraction with time fidelity for feasible timed hierarchical control is the new concept of timed output-control consistency, which is developed and discussed in this paper, extending the untimed version [3] to real time. The need for high-level time fidelity is motivated in part by real-time design challenges in cyber-physical systems (CPS’s) [7]. CPS’s are holistic integrations of computation, communication, and physical processes, and are an important source of hierarchical TDES’s. In CPS study, it has been argued that system abstractions need to correctly unify the low-level (or digital and physical) timing dynamics and the high-level (or cyber) computations in a high-level model for system control design.

On related work in timed hierarchical control [2], it is observed that the high-level time tick introduced is akin to timeout and is treated like any other high-level event. The work therefore does not guarantee high-level time fidelity, and in this aspect is fundamentally different from ours.

II. BACKGROUND

A. Languages & Automata for TDES Modeling [1]

Let \( \Sigma \) be a finite set of symbols representing events. A string is a finite sequence of events of \( \Sigma \). Let \( \Sigma^* \) be the set of finite strings with events from \( \Sigma \), including an empty string \( \varepsilon \). Let \( \Sigma^+ = \Sigma^* - \{\varepsilon\} \). A string \( s' \) is a prefix of another string \( s \), denoted by \( s' \leq s \), if \( (\exists t \in \Sigma^*) s't = s \). A string \( t \) is a suffix of \( s \) if \( (\exists s' \in \Sigma^*) s't = s \).

A formal language \( L \) over \( \Sigma \) is a subset of \( \Sigma^* \). For \( L_1, L_2 \subseteq \Sigma^* \), \( L_1 \) is said to be a sublanguage of \( L_2 \) if \( L_1 \subseteq L_2 \).

A regular language is a language that can be generated by a finite-state automaton. An automaton \( G \) is a 5-tuple \( (Q, \Sigma, \delta, q_0, Q_0) \), where \( Q \) is the finite set of states, \( \Sigma \) is the finite set of events, \( \delta : \Sigma \times Q \rightarrow Q \) is the (partial and deterministic) transition function, \( q_0 \) is the initial state, and \( Q_0 \subseteq Q \) is the subset of marked states. That an event \( \sigma \in \Sigma \) is defined at a state \( q \in Q \) is denoted by \( \delta(\sigma, q) \).

For an event subset \( \Sigma' \subseteq \Sigma \) and a state \( q \in Q \),...
let $\Sigma'(q) = \{ \sigma \in \Sigma \mid \delta(\sigma, q) \}$, which defines the subset of events in $\Sigma'$ that are defined at state $q$. The transition function $\delta$ can be extended to $\Sigma'$ as follows: $\delta(\varepsilon, q) = q$ and $(\forall \sigma \in \Sigma)(\forall s \in \Sigma')\delta(\sigma r, q) = \delta(\sigma, \delta(s, q))$, and is defined when $q' = \delta(s, q)$ and $\delta(\sigma, q')$ are both defined. A state $q \in Q$ is reachable (from the initial state $q_0$) if $(3s \in \Sigma')\delta(s, q_0) = q$.

The behavior of automaton $G$ may be described by two languages: the prefix-closed language $L(G) = \{ s \in \Sigma^* \mid \delta(s, q_0) \}$ and the marked language $L_m(G) = \{ s \in L(G) \mid \delta(s, q_0) \in \tilde{Q}_m \}$. By definition, $L_m(G) \subseteq L(G)$.

Graphically, an automaton is represented by an edge-labeled directed graph with a state represented by a node, and a transition $\delta(\sigma, q) = q'$ by a directed edge from state $q$ to $q'$ labeled with a symbol $\sigma$ of an event whose occurrence it represents. The initial state $q_0$ is represented by a node with an entering arrow, and a marked state by a darkened node or a double-concentric circle.

**B. Timed Discrete-Event System (TDES) Model [6]**

A TDES can be modeled by an automaton called activity transition graph (ATG) and the timing information associated with each system event. Combining the ATG model and timing information furnishes a timed transition graph (TTG), an automaton generating prefixed-closed and marked languages that explicitly model the timed behaviors of the TDES.

Formally, the ATG of a TDES is the automaton $G_{act} = (A, \Sigma_{act}, \delta_{act}, a_0, A_m)$, where the state set is redesignated as $A$, the finite set of activities, with each activity associated with a time duration, $\Sigma_{act}$ is the finite set of activity events, $\delta_{act} : \Sigma_{act} \times A \rightarrow A$ is the activity transition function, $a_0$ is the initial activity and $A_m \subseteq A$ is the subset of marked activities.

Let $\mathbb{N} = \{0, 1, 2, \cdots \}$, the set of natural numbers. In associating the ATG $G_{act}$ with timing information, each event $\sigma \in \Sigma_{act}$ is assigned with time bounds, namely, a lower time bound $l_\sigma \in \mathbb{N}$ and an upper time bound $u_\sigma \in \mathbb{N} \cup \{\infty\}$, where $l_\sigma \leq u_\sigma$, and specified as $\sigma[l_\sigma, u_\sigma]$. A time bound is quantified in terms of a number of ticks of the global clock. A time tick is denoted by a special event symbol $\text{tick} \notin \Sigma_{act}$, and its occurrence denotes a transition or passage of an atomic unit of time. Under these time bound assignments, $\Sigma_{act}$ is divided into two disjoint subsets $\Sigma_{ipe}$ and $\Sigma_{rem}$, i.e., $\Sigma_{act} = \Sigma_{ipe} \cup \Sigma_{rem}$ and $\Sigma_{ipe} \cap \Sigma_{rem} = \emptyset$, and this partition is denoted by $\Sigma_{act} = \Sigma_{ipe} \cup \Sigma_{rem}$. $\Sigma_{rem} = \{ \sigma \in \Sigma_{act} \mid u_\sigma = \infty \}$ is called the subset of remote events; and $\Sigma_{ipe} = \{ \sigma \in \Sigma_{act} \mid u_\sigma < \infty \}$ is called the subset of prospective events. Each event $\sigma \in \Sigma_{act}$ has a local countdown timer $t_\sigma$ with a default value $t_{\sigma 0}$ initialized as $t_{\sigma 0} = \begin{cases} u_\sigma, & \text{if } \sigma \in \Sigma_{ipe} \\ l_\sigma, & \text{if } \sigma \in \Sigma_{rem} \end{cases}$.

Intuitively, the existence of a lower time bound means that an event $\sigma$ is only eligible or ready to occur in the TDES after $l_\sigma$ ticks upon entering an activity in $G_{act}$ (1) where $\sigma$ is defined, and will never occur before that; and each tick occurrence decreases the timer $t_\sigma$ by one tick count, until $t_\sigma = 0$. If $\sigma$ is a remote event and $t_\sigma$ is or has decreased to 0, it becomes eligible but might or might not occur next. If $\sigma$ is a prospective event, it might occur during $0 \leq t_\sigma \leq u_\sigma - l_\sigma$, and must occur next when $t_\sigma = 0$ unless it is preempted by another imminent event. The timer interval or duration $D_\sigma$ is defined for $\sigma$ as follows:

$$D_\sigma = \begin{cases} [0, u_\sigma), & \text{if } \sigma \in \Sigma_{ipe} \\ [0, l_\sigma], & \text{if } \sigma \in \Sigma_{rem} \end{cases}$$

Therefore, $t_\sigma \in D_\sigma$. Being instantaneous [6], an event occurrence is modeled as abrupt with no time duration.

Let $\Sigma = \Sigma_{act} \cup \{\text{tick}\}$. Given the ATG $G_{act}$ (1) and timing information as defined above for each event $\sigma \in \Sigma_{act}$, the TTG of the TDES is the automaton $G = (Q, \Sigma, \delta, q_0, Q_m)$, with finite state set $Q = A \times \prod [D_\sigma \mid \sigma \in \Sigma_{act}]$ and marked state set $Q_m \subseteq A_m \times \prod [D_\sigma \mid \sigma \in \Sigma_{act}]$. Each state $q \in Q$ is of the form $q = (a, [t_\sigma \mid \sigma \in \Sigma_{act}])$, and $q_0 = (a_0, [t_{\sigma 0} \mid \sigma \in \Sigma_{act}])$ is the initial state.

For an activity event $\sigma \in \Sigma_{act}$ and a state $q = (a, \cdots) \in Q$, $\sigma$ is eligible at $q$ provided $\delta(\sigma, q)$! and is said to be enabled at $q$ provided $\delta(\sigma, a)!$; and $\delta(\sigma, q)!$ iff $\delta(\sigma, a)!$ and

$$t_\sigma = 0, \quad \text{if } \sigma \in \Sigma_{rem} \quad \begin{cases} 0 \leq t_\sigma \leq u_\sigma - l_\sigma, & \text{if } \sigma \in \Sigma_{ipe} \end{cases}$$

The TDES $G$ is also subjected to the following conditions: For every $q = (a, \cdots) \in Q$,

$$\text{tick}(q)! \quad \text{iff } \forall \beta \in \Sigma_{ipe}, \delta(\sigma, \beta)! \delta(\sigma, q)! > 0.$$

and

$$\forall s \in \Sigma_{act}, \delta(s, q)! \delta(s, q) \neq q.$$

Condition (4) characterizes that the time event tick is eligible at state $q$ provided no prospective event is due at the state. Condition (5) - activity-loop freeness - asserts that there is no activity loop at a state $q \in Q$ in TDES $G$. An activity loop is a cycle containing only activity events, and repeated execution of an activity loop is deemed to incur no time duration. As such loops are physically infeasible, this condition is needed to exclude such loops in TDES $G$.

In meeting Conditions (4) and (5), the persistence of time (evolution) is not violated in TDES model $G$, characterizing the fact that a TDES can never stop the clock [6]. In this paper, a TDES (automaton) model is represented by a TTG of the type (2) as reviewed above.

**C. Control-Theoretic Setting for TDES’s [6]**

The control-theoretic setting for TDES’s assumes that the subset of events controllable by an external supervisor is predetermined. In a logical DES, a controllable event is prohibitable, in that it can be prevented from occurring by (control) disablement. In a TDES, a controllable event is one that can be prevented from occurring by some means. By its timing characteristics, an event in $\Sigma_{ipe}$ is not prohibitable or uncontrollable, as it must occur next once its upper time bound is reached unless it is preempted by another imminent event, whereas an event in $\Sigma_{rem}$ may be. With
\[ \Sigma_{act} = \Sigma_{use} \cup \Sigma_{rem} \], it follows that the set of prohibitable events, denoted by \( \Sigma_{hib} \), is a subset of \( \Sigma_{rem} \); i.e., \( \Sigma_{hib} \subseteq \Sigma_{rem} \). In what follows, the uncontrollable event set is defined as \( \Sigma_u = \Sigma_{act} - \Sigma_{hib} = \Sigma_{use} \cup (\Sigma_{rem} - \Sigma_{hib}) \). Let \( \Sigma_{for} \subseteq \Sigma_{act} \) be the set of forcible events. An enforced forcible event can only preempt \( tick \), i.e., only \( tick \) will not occur next, at a state where both \( tick \) and the forcible event are eligible. The event \( tick \) is controllable by preemption through a forcible event, not by disablement as for an event in \( \Sigma_{hib} \), since nothing can stop the global clock. Accordingly, the controllable event set is defined as \( \Sigma_c = \Sigma - \Sigma_u = \Sigma_{hib} \cup \{tick\} \). Therefore, \( \Sigma = \Sigma_c \cup \Sigma_u \) and this is identical to the control-theoretic setting for logical DES’s \([1]\).

III. Time Fidelity of TDES Model

For an automaton \( G \) of the type \((2)\) modeling a TDES, the following are its qualitative temporal properties.

Property 1 (Persistence of time): Let \( q = \delta(s,q_0) \). Then \( (\Sigma_{act}(q) = \emptyset) \implies \delta(tick,q) \).

The property states that a time event \( tick \) is always eligible at a reachable state with no eligible activity events. By Property 1, the continual time elapse that persists even during the transience or absence of system activity is modeled.

Property 2 (Time invariance of event eligibility): Let \( q = \delta(s,q_0) \) and \( q' = \delta(tick,q) \). Then \( \Sigma_{act}(q) \subseteq \Sigma_{act}(q') \).

The property states that eligible activity events at a reachable state remain eligible at another following the time elapse of a tick. By Property 2, the continual execution of an activity event as time elapses is effectively modeled. Applying this property iteratively, tick occurrences represent the elapse of time until some eligible event occurs instantaneously.

Given the uncontrollable event set \( \Sigma_u \), an important system model property strengthening Property 1 may now be presented.

Property 3 (Uncontrollable persistence of time): Let \( q = \delta(s,q_0) \). Then \( (\Sigma_{act}(q) \cap \Sigma_u = \emptyset) \implies \delta(tick,q) \).

The property states that the event \( tick \) is always eligible at a reachable state with no eligible uncontrollable event. This means the evolution of time in the model \( G \) does not halt regardless of the absence of activity events or the disablement of all eligible prohibitable events at a reachable state.

Properties 1 to 3 present new supporting insights for our research. They provide a clearer understanding of the TDES model \( G \) \((2)\) \([6]\) reviewed. In fact, Properties 2 and 3 and Condition \((5)\) of TDES \( G \) together model system time fidelity, characterizing time progression as never halting an executing activity event (Property 2) and unstoppable (Property 3 and Condition \((5)\)). Equivalently, the model \( G \) is said to possess sound system (event-) timing semantics; or the time \( tick \) is said to be \( \Sigma \)-uninterrupting.

Note that, as a timed-activity event feature of an uncontrollable TDES, Property 2 need not apply to a control specification in TTG prescribing a sublanguage of the system model.

IV. TDES Hierarchy with Time Fidelity

In a two-level hierarchical setup as in \([3]\), the low-level TDES needs to be equipped with an output function that drives the high-level TDES model. To model a class of such low-level TDES’s, a Moore automaton \([5]\) is used.

A. Low-level TDES Modeling for Hierarchical Control

In general, a TDES model \( G \) \((2)\) with event set \( \Sigma \) needs to be re-structured into a Moore automaton\(^1\) - an automaton \( G_{lo} = (Q, \Sigma, \delta, q_0, Q_{lo}) \) associated with an information channel defined by a vocalization map \( V : Q \rightarrow T \cup \{\tau_o\} \), where \( T = T_{act} \cup \{t_1\} \), such that \( L(G_{lo}) = L(G) \) and \( L_{lo}(G_{lo}) = L_{lo}(G) \). \( T_{act} \) denotes the high-level (virtual) activity event set, and \( t_o \) denotes an aggregated time tick of ticks of the global clock at the low level, and the symbol \( \tau_o \) denotes a ‘silent output’. For the low-level TDES \( G_{lo} \), we henceforth replace \( tick \) by \( t_1 \) to distinguish it as a low-level atomic time tick; therefore, \( \Sigma = \Sigma_{act} \cup \{t_1\} \).

Let \( w^*_1 = \text{WWW} \cdots \) and \( w^n \) denote a string of finitely many occurrences and a string of \( n \in \mathbb{N} \) consecutive occurrences, of a string \( w \), respectively; and \( w^*_1 = \varepsilon \). Then the Moore construction \([5]\) of \( G \) for the TDES \( G \) is based on a given timed reporter map - a virtual projection \( \theta : L(G) \rightarrow T^* \), defined such that \( \theta(s) = \varepsilon \) and, for \( s \in \Sigma \) and \( s \sigma \in L(G), \theta(s\sigma) \) is either \( \theta(s) \) or \( \theta(s)\tau \) for some \( \tau \in T \). The given map \( \theta \) obeys the following time-output design laws:

1) For \( s(s's'')^n \in L(G) \), and \( s', s'' \in \Sigma \), \( \theta(s(s's'')^n) = \theta(s)(t^n t_1^n)^n \) for all \( n \geq 0 \), where \( t', t'' \in T \).

2) For \( s \in \Sigma \) and \( s \sigma \in L(G), \theta(s\sigma) = \theta(s)\tau \implies s = t \).

The constraint by Law 1 means that \( G_{lo} \) must be constructed such that whenever a state \( q = \delta(s,q_0) \) in \( G_{lo} \), has traversing through it, a loop string containing a low-level time tick \( t_1 \), i.e., \( \delta(s's'\cdots, q) = q \) for some \( s', s'' \in \Sigma \), the loop string \( s's'\cdots \) must traverse through a state in \( G_{lo} \) that outputs or vocalizes a high-level time tick \( t_1 \). In this sense, \( G_{lo} \) is \( t_1 \)-responsive. The constraint by Law 2 means that the high-level tick \( t_1 \) is a time output, in that it must be real time-driven, i.e., \( t_1 \) is always a vocalization that immediately follows the execution of a low-level tick \( t_1 \) in \( G_{lo} \). With \( \theta \) obeying the time-output design laws, the low-level TDES \( G_{lo} \) constructed is said to be time-output responsive.

For the constructed \( G_{lo} \), the vocalization map \( V \) for every \( s' \in L(G_{lo}) \) is defined by

\[
V(\delta(s',q_0)) = \begin{cases} 
\tau_o, & \text{if } s' = \varepsilon \\
\text{or } (s',q_0) \notin Q_{lo} & \forall \tau \in T, \\
\text{otherwise}.
\end{cases}
\]

where the selected subset \( Q_{lo} \subseteq Q \), called vocal state set, is defined as follows. For \( s \in \Sigma \) and \( s' = \varepsilon \),

\[
\delta(s\sigma,q_0) \begin{cases} 
\notin Q_{lo}, & \text{if } (s\sigma) \notin Q \text{ or } \theta(s) \text{ by } (s) \in Q_{lo} & \forall \tau \in T, \\
\text{if } (s\sigma) = (s) \text{ or } (s) \tau \in Q \text{ by } \theta(s) = (s) \text{ or } \theta(s) \tau \in Q \text{ by } \theta(s) = \varepsilon.
\end{cases}
\]

In the graphical representation of \( G_{lo} \), every vocal state is represented by a node containing the symbol of an event that it vocalizes.

The Moore automaton \( (G_{lo}, V) \) is simply referred to as \( G_{lo} \) when \( V \) is understood. Through the map \( V \), \( G_{lo} \) outputs

\(^1\)Although the same 3-tuple notation is used as in Section II-C, it should be clear in the context that the structure of \( G_{lo} \) is in general not the same as that of a given TDES \( G \).
events in \( T \) to drive some high-level \( \theta \)-image model \( G_{hi} \) whenever it reaches a vocal state \( q \in Q_{voc} \), and otherwise outputs the silent symbol \( \tau \not\in T \) to signal no ‘significant’ change for the high level. The high-level image of \( G_{lo} \) that results is an automaton \( G_{hi} \), such that \( L(G_{hi}) = \{ \theta(s) | s \in L(G_{lo}) \} \). \( G_{hi} \) is said to generate events of \( T \) under the \( \theta \)-map on \( L(G_{lo}) \). The pair \((G_{lo}, G_{hi})\) represents a two-level TDES hierarchy. However, note that the structure of \( G_{hi} \) is, in general, a timed transition graph that might not satisfy timing Properties 2 and 3, although the TDES \( G_{lo} \) constructed from a given TDES \( G \) (2) and reporter map \( \theta \) does.

B. System Abstraction with Time Fidelity

To lay a sound design foundation for timed hierarchical control, we postulate that high-level time fidelity must also be upheld in the design of a hierarchical abstraction for a given base or low-level TDES model.

**Example 1:** To illustrate why high-level time fidelity must be upheld, consider the example depicted in Fig. 1. Under two different timed reporter maps, the two low-level Moore TDES’s constructed for a given TDES \( G \) shown in Fig. 1(a) are System 1 and System 2, as shown in Fig. 1(b). The respective high-level systems are Abstraction 1 and Abstraction 2, as shown in Fig. 1(c). Clearly, Abstraction 2 preserves high-level time fidelity. Abstraction 1 does not because it violates Property 2. Now, consider a high-level specification \( \text{Spec} \) (in TTG) in Fig. 1(c), which asserts that a high-level activity event \( \tau \) is to be disabled if it does not occur after three high-level time ticks upon becoming eligible or ready to occur. As shown in Fig. 1(d), the sublanguage due to the specification on Abstraction 1 is represented by TTG 1, whereas that due to the same specification on Abstraction 2 is represented by TTG 2. Clearly, TTG 1 is semantically incorrect or unsound against the intended timing requirement of ‘three ticks before \( \tau \)-disability’ prescribed by Spec, as the \( \tau \)-disableness occurs after only one tick, whereas TTG 2 is.

In a TDES hierarchy \((G_{lo}, G_{hi})\), since \( G_{lo} \) is time-output responsive (due to the given map \( \theta \)) and activity-loop free (by Condition (5)), \( G_{hi} \) is also activity-loop free. This is formalized in Proposition 1.

**Proposition 1:** Given a TDES hierarchy \((G_{lo}, G_{hi})\), \( G_{hi} \) is activity-loop free.

Next, the aggregated time, as represented by the ticking of \( t_h \), is continual in the (uncontrolled) high-level TDES \( G_{hi} \), in that a tick \( t_h \) is always eligible in the absence of activity events at a state of \( G_{hi} \). This is formalized in Proposition 2.

**Proposition 2:** Given a TDES hierarchy \((G_{lo}, G_{hi})\), \( G_{hi} \) obeys Property 1.

In driving \( G_{hi} \) from below via the vocalization map \( V \), the high-level time tick evolution must not render an eligible high-level activity event ineligible, as with the respect accorded to low-level ticks and activity events by the low-level model \( G_{lo} \) (see Property 2). This requires \( G_{lo} \) to be output time-compliant (OTC), achievable by a proper design or redesign of the reporter map \( \theta \), and which is formally defined as follows: A TDES \( G_{lo} \) is said to be OTC if, for all \( ss' \in L(G_{lo}) \), where \( \delta(s, q_0) \in Q_{voc} \cup \{q_0\} \), \( \delta(s', q_0) \in Q_{voc} \) and \( \theta(s') = \theta(s)\tau \) for some \( \tau \in T_{act} \), if there exists a \( w \in L(G_{lo}) \) such that \( \delta(w, q_0) \in Q_{voc} \) and \( \theta(w) = \theta(s)t_h \), then there exists a \( w' \in L(G_{lo}) \) such that \( \delta(w', q_0) \in Q_{voc} \) and \( \theta(w') = \theta(s)t_h \). Put another way, if \( G_{lo} \) is OTC, the essence is that, as with the ticking of \( t_l \) in \( G_{lo} \), the ticking of \( t_h \) is never the cause of activity event ineligibility in \( G_{hi} \). This is formalized in Proposition 3.

**Proposition 3:** Given a TDES hierarchy \((G_{lo}, G_{hi})\) and that \( G_{lo} \) is OTC, \( G_{hi} \) obeys Property 2.

For the rest of the paper, the Moore automaton \( G_{lo} \) is assumed to be OTC.

V. TImed output-control Consistency

To admit control for a TDES hierarchy \((G_{lo}, G_{hi})\) constructed, the high-level event set \( T_{act} \) of \( G_{hi} \) is partitioned into the prohibitable event set \( T_{hi} \) and the uncontrollable
event set $T_i$, and into the forcible event set $T_{for}$ and the non-forcible event set $T_{act} - T_{for}$. However, for feasible high-level timed control, $G_{hi}$ needs to be structurally refined so that $G_{hi}$ is endowed with a natural timed control structure, i.e., every high-level event $\tau \in T_{act}$ defined and output by $G_{hi}$ is unambiguously prohibitable or uncontrollable, and unambiguously forcible or non-forcible, and the time tick $t_h \in T$ is $T$-uninterrupting. The Moore transition structure of the TDES $G_{hi}$ is defined to be timed output-control consistent (TOCC) if $G_{hi}$ possesses such a natural timed control structure.

In what follows, we present the theoretical development of the fundamental systems concept of timed output-control consistency, to lay a time fidelity foundation for feasible hierarchical control of TDES’s. We first explain the essence of the formulation: The TDES $G_{hi}$ is TOCC if it is said to be both activity output-control consistent (AOCC) and output-force consistent (OFC):

- Being AOCC means that every high-level event $\tau \in T_{act}$ (defined, and output by $G_{hi}$) is unambiguously prohibitable or uncontrollable. As stated in Proposition 4 below, for an AOCC $G_{hi}$, Property 3 holds for the resultant $G_{hi}$; and together with Condition (5) and Property 2 that also hold for $G_{hi}$ according to Propositions 1 and 3, the time tick $t_h \in T$ is $T$-uninterrupting.

- Being OFC means that every high-level event $\tau \in T_{act}$ is unambiguously forcible or non-forcible. By the standard model of event forcing [6], a high-level event is unambiguously forcible provided, when enforced, it can always preempt the time tick $t_h$.

The formulation of the two supporting structural concepts requires the following definition and terminology.

Define an arbitrary string $s \in L(G_{hi})$, denoted by

$$s = < s', \sigma_1, x_i, k, \tau >,$$

(6)

to be of the form

$s = \sigma_1 \sigma_2 \cdots \sigma_k$ or, respectively, $s = s' \sigma_1 \sigma_2 \cdots \sigma_k$

if $s', x_i, \sigma_i \in \Sigma$ ($1 \leq i \leq k$), with

- $V(\delta(\sigma_1, \sigma_2, \cdots, \sigma_i, q_0)) = \tau_0$ ($1 \leq i \leq k - 1$),
- $V(\delta(s, q_0)) = \tau$ in $T$,
- $x_0 = \delta(\varepsilon, q_0)$,
- $x_i = \delta(\sigma_1, \sigma_2, \cdots, \sigma_i, q_0)$ ($1 \leq i \leq k$),

or, respectively,

- $V(\delta(s', q_0)) \in T$,
- $V(\delta(s', \sigma_1, \sigma_2, \cdots, \sigma_i, q_0)) = \tau_0$ ($1 \leq i \leq k - 1$),
- $V(\delta(s, q_0)) = \tau$ in $T$,
- $x_0 = \delta(s', q_0)$,
- $x_i = \delta(s', \sigma_1, \sigma_2, \cdots, \sigma_i, q_0)$ ($1 \leq i \leq k$).

In every $s = < s', \sigma_1, x_i, k, \tau >$ ($6$) of $L(G_{hi})$, $s' \in L(G_{hi})$ is called the reference prefix of string $s$, and is an empty string if $x_0$ is the initial low-level system state $q_0 \in Q$. Such a string $s \in L(G_{hi})$ is called a $\tau$-string and has a suffix $\sigma_1 \sigma_2 \cdots \sigma_k$ that runs from the initial state or a vocal state, via non-vocal states of $G_{hi}$, to a vocal state outputting the high-level event $\tau \in T$. This suffix is called the co-silent string of $s$ (6).

**A. Activity Output-Control Consistency**

**Definition 1** (Activity output-control consistency): A TDES $G_{hi}$ is said to be AOCC if, for every $\tau$-string $s'$, $\sigma_1, x_i, k, \tau > \in L(G_{hi})$ with $\tau \in T_{act}$, it is the case that

- if $\tau \in T_{hib}$, then for some $i$ ($1 \leq i \leq k$), $\sigma_i \in \Sigma_{hib}$ or $(\sigma_i = t_i \& \Sigma(x_i-1) \cap \Sigma_{for} \cap \Sigma_u \neq \emptyset)$,
- if $\tau \in T_u$, then for all $i$ ($1 \leq i \leq k$), $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_i \& \Sigma(x_{i-1}) \cap \Sigma_{for} = \emptyset)$,

For an AOCC $G_{hi}$, $\tau \in T_{hib}$ only if there is a low-level event in the co-silent string, of every $\tau$-string of $L(G_{hi})$, which is prohibitable or is a tick $t_i$ at a state where an uncontrollable and forcible event is also eligible. $\tau \in T_u$ only if every low-level event in the co-silent string, of every $\tau$-string of $L(G_{hi})$, is uncontrollable or is a tick $t_i$ at a state where no forcible event is eligible.

Time, represented by tick $t_h$, is uncontrollably persistent in the high-level abstraction $G_{hi}$ of an AOCC $G_{hi}$, and this fact is formalized in Proposition 4.

**Proposition 4:** Given a TDES hierarchy $(G_{lo}, G_{hi})$ and that $G_{lo}$ is AOCC, $G_{hi}$ obeys Property 3.

Since, by Propositions 1, 3, and 4, $G_{hi}$ is activity-loop free and obeys Properties 2 and 3, it follows that $t_h$ is $T$-uninterrupting.

**B. Output-Force Consistency**

We first define and explain two supporting concepts, before defining the structure of an OFC $G_{hi}$.

**Definition 2** (Preemptability of $t_h$ by $\tau \in T_{act}$): Consider an arbitrary $\tau$-string (6) of $L(G_{hi})$ with reference prefix $s' \in L(G_{hi})$ and $\tau \in T_{act}$. Then $t_h$ is said to be unambiguously preemptable with respect to (w.r.t.) $(s', \tau)$ if, for every $t_h$-string $< w, \sigma_1, x_i, k, \tau > \in L(G_{hi})$ such that $\theta(w) = \theta(s')$ and $w \in L(G_{hi})$ is the reference prefix of some $\tau$-string (6) of $L(G_{hi})$, there exists a $\tau$-string $< w, \sigma_1, x_i, k, \tau > \in L(G_{hi})$, with $\alpha_1 \alpha_2 \cdots \alpha_p = \sigma_1 \sigma_2 \cdots \sigma_p$ for some $p$ ($0 \leq p < \min(h,k)$), and $z_0 \notin \{ x_i | 0 \leq i \leq k - 1 \}$ for all $n$ ($p < n < h$), such that

- either for some $n$ ($p < n < h$), $\alpha_n \in \Sigma_{hib}$ or $(\alpha_n = t_i \& \Sigma(z_{n-1}) \cap \Sigma_{for} \cap \Sigma_u \neq \emptyset)$,
- or $(\alpha_{p+1} = t_i \& \alpha_{p+1} \in \Sigma_{for})$.

Consider an arbitrary non-empty string $r = \alpha_{p+1} \alpha_{p+2} \cdots \alpha_h$ that leads, from a state $x_p$ lying along the transitions defining the co-silent string $\sigma_1 \sigma_2 \cdots \sigma_k$ of some $\tau$-string of $L(G_{hi})$, $\tau \in T_{act}$, that exists, to a vocal state outputting $t_h$, via subsequent non-vocal states that are not lying along the transitions defining the co-silent string. Then, in words, w.r.t the reference prefix $s'$ of a $\tau$-string of $L(G_{hi})$, $t_h$ is unambiguously preemptable if every $t_h$-string of $L(G_{hi})$ with reference prefix $w$, such that $\theta(w) = \theta(s')$ and string $w$ is also the reference prefix of some $\tau$-string of $L(G_{hi})$, has such a string $\sigma_1 \sigma_2 \cdots \sigma_p r$, $p < \min(h,k)$, as its suffix, with string $r$ either containing a prohibitable event or a $t_i$ which can be preempted by a forcible event; and this forcible event is prohibitable only if it lies along the co-silent string of the $\tau$-string that exists.
Definition 3 (Preemptability of t_h by τ-mirage, τ ∈ T_{act}): Consider an arbitrary τ-string (6) of L(G_{ih}) with reference prefix s' ∈ L(G_{ih}) and τ ∈ T_{act}. Then t_h is said to be unambiguously preemptable w.r.t the mirage of (s', τ) if, for all w ∈ L(G_{ih}), w = σ or δ(w, q_h) ∈ Q_{act}, if δ(w) = δ(s') and τ' ≠ τ for every τ'-string (6) of L(G_{ih}) with reference prefix w ∈ L(G_{ih}) and τ' ∈ T_{act}, then for every t_h-string < w, α_j, z_j, h, t_h > ∈ L(G_{ih}), there exists some j (1 ≤ j ≤ h) such that

\[ τ_j ∈ \Sigma_{hub} \text{ or } (τ_j = t_i \& Σ(z_{j-1}) ∩ Σ_{for} ∩ Σ_a ≠ ∅). \]

In words, consider an arbitrary τ-string of L(G_{ih}) with reference prefix s' and τ ∈ T_{act}. Then t_h is unambiguously preemptable w.r.t the mirage of (s', τ) if, for every other string w ∈ L(G_{ih}) that is like and has the same θ-image as string s', but is not the reference prefix of any τ-string of L(G_{ih}), every t_h-string of L(G_{ih}) with string w as its reference prefix has its co-silent string either containing a prohibitable event, or a t_l which can be preempted by a forcible event that is uncontrollable.

Definition 4 (Output-force consistency): A TDES G_{ih} is said to be OFC if, for every τ-string (6) of L(G_{ih}) with reference prefix s' ∈ L(G_{ih}) and τ ∈ T_{act}, τ ∈ T_{for} iff t_h is unambiguously preemptable w.r.t (s', τ) and its mirage.

For an OFC G_{ih}, τ ∈ T_{for} if the high-level activity event τ can unambiguously preempt the tick t_h, whenever the activity event is enforced following every low-level string that is, or is like and has the same θ-image as, the reference prefix, of every τ-string of L(G_{ih}). Otherwise, τ ∈ T_{act} ≠ T_{for}.

C. Timed Output-Control Consistency

Definition 5 (Timed output-control consistency): A TDES G_{ih} is said to be TOCC if it is both AOC and OFC.

Theorem 1: Given a TDES hierarchy (G_{ih}, G_{hi}) and that G_{ih} is TOCC, G_{hi} is a TOCC model with time fidelity.

Theorem 1 summarizes the fact that high-level time fidelity is also preserved for a TOCC TDES G_{ih}. Along with the unambiguous control properties of high-level activity events, the abstraction G_{hi} of a TOCC G_{ih} provides a decoupled, low-level independent basis, for which to specify high-level specification TGG’s for feasible hierarchical control design.

VI. An Example

Consider an example of a TDES G_{ih}, shown in Fig. 2 together with its high-level abstraction G_{hi}, with high-level event set T_{act} = \{t_i | i = 1, 2, 3, 4, 5\}, Σ_{act} = \{σ_{t_i} | i = 1, 2, 3, 4, 5, 6, 7, 8\} and the timing information associated with every event in Σ_{act} is as follows: σ_{t_1}[0, 0], σ_{t_2}[0, 0], σ_{t_3}[0, 0], σ_{t_4}[1, 0], σ_{t_5}[0, 0], σ_{t_6}[0, 0], Σ_{hub} = \{σ_{t_1} | i = 6, 7, 8\}, and the rest of Σ_{hub}, subsuming Σ_{spe} = \{σ_{t_1} | i = 1, 2, 4\}, are uncontrollable. Σ_{for} = \{σ_{t_i} | i = 7, 8\}, and the rest of Σ_{act} are non-forcible. In the figure, for ease of reference, the symbol for a prohibitable and an uncontrollable event is indicated with a superscript ‘+’ and ‘-’, respectively; and additionally with a superscript ‘#’ provided the event is forcible.

Fig. 2. An example of a TDES G_{ih} that is TOCC and its abstraction G_{hi}

- G_{ih} is AOCC and each output event of T_{act} is therefore unambiguously prohibitable or uncontrollable. Specifically, \( T_{hub} = \{t_i | i = 2, 3, 4\} \), and the rest of T_{act} are uncontrollable.
- G_{ih} is also OFC, and each output event of T_{act} is therefore unambiguously forcible or non-forceable. The preemptability of t_h can only be done by enforcing σ_{t_1}, σ_{t_4} ∈ Σ_{for} in the underlying structure of G_{ih}, inducing τ_2 as prohibitable. Therefore, T_{for} = {τ_2}, and the rest of T_{act} are non-forceable.

It follows that G_{ih} is TOCC, and as clearly depicted, the resultant G_{hi} is a TDES with time fidelity.

VII. Conclusion

The new concept of timed output-control consistency preserving high-level time fidelity is proposed and illustrated in the framework of formal languages and TGG’s. In further work, since a given low-level TDES may not be TOCC, the problem of refining the system structure so that it becomes TOCC will be investigated. The consistency concept proposed lays a time fidelity foundation for extending the consistency of hierarchical control in logical DES’s to TDES’s, which is an important subject for future research.

REFERENCES