myjournal-sample manuscript No.
(will be inserted by the editor)

A Hierarchical Consistency Framework for Real-Time Supervisory Control

Quang Ha Ngo · **Kiam Tian Seow**

Received: date / Accepted: date

Abstract The control framework of hierarchical consistency of timed discrete-event systems (TDES's) is investigated in a standard two-level hierarchy. Real-time concepts and the associated theoretical results supporting consistent TDES hierarchies are developed. Where the given low-level system model of the hierarchy possesses time fidelity, a consistency version that assures time fidelity of the high-level system model is also developed. Importantly, this version furnishes a sound real-time high-level specification design foundation for hierarchical control. An example illustrates the new time-fidelity control foundation. Given that in general, a given two-level TDES hierarchy is not hierarchically consistent between the levels, the structural existence and synthesis of the sufficiency structure for hierarchical consistency is investigated. Both the timed versions of hierarchical consistency - without and with output-time fidelity guarantee - are successively treated. The abstraction or output-system refinement procedures for the version without output-time fidelity guarantee are first developed for a class of TDES hierarchies under mild output-system design restrictions. The abstraction methods for the version with output-time fidelity are then developed for a subclass 'linearly' structured under further output-system design restrictions. A detailed example explains and illustrates the use of an overarching method developed.

Keywords Hierarchical control · timed discrete-event systems · formal languages · finite automata.

1 Introduction

Under the general framework of formal languages and finite (or finite-state) automata, the seminal concept of hierarchical consistency for logical or untimed discrete-event systems (DES's) (Zhong and Wonham, 1990) is suitably extended to timed DES's (TDES's) in this paper. In a two-level, untimed hierarchical control setup, conceptualized in (Zhong and Wonham, 1990) and algorithmically realized in (Ngo and Seow, 2014a), the system at the low level drives the system at the high level which is an abstraction of the former, via an information channel modeled by a hierarchical reporter map. Depicted in Fig. 1, this setup consists of two horizontal levels of standard feedback control which are vertically interconnected so that a manager at the high level (or high-level supervisor) can issue commands to an operator at the low level (or low-level supervisor) to control a real DES modeled by a Moore automaton (Eilenberg, 1974), in response to information of interest sent up from the low level to the high level. By hierarchical consistency between the levels (Zhong and Wonham, 1990), a low-level supervisor implementing feasible commands issued (or virtual controls) at the high level can fully realize a controllable prefix-closed specification task (Ramadge and Wonham, 1987) prescribed at the high level. The importance of hierarchical control stems from the fact that, in general, a hierarchical structure conforms better to practice and renders a given system more manageable for system specification and control in terms of large-scale system design comprehensibility and improving control computational efficiency (Ngo and Seow, 2014a).

Quang Ha Ngo
School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798, Republic of Singapore
E-mail: quang5@e.ntu.edu.sg

Kiam Tian Seow
Robot Intelligence Technology Laboratory, School of Electrical Engineering, KAIST, Daejeon 305-701, South Korea
E-mail: ktseow@rit.kaist.ac.kr

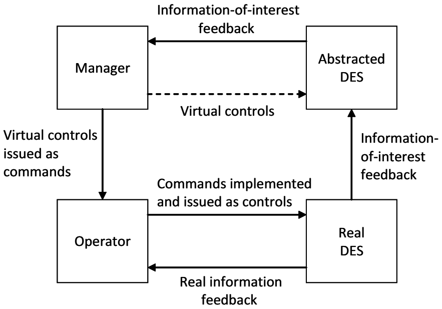

Information-of-interest feedback
Manager
Abstracted DES
Virtual controls
Virtual controls issued as commands
Information-of-interest feedback
Commands implemented and issued as controls
Operator
Real DES
Real information feedback

Fig. 1 The command & control hierarchy (Zhong and Wonham, 1990)

Based on architecturally the same two-level setup as the hierarchical control of untimed DES's (Zhong and Wonham, 1990), in this paper, a TDES hierarchy is modeled by a Moore automaton representing the low-level system driving the high-level system of the hierarchy. The Moore automaton is constructed from a given TDES (automaton) model for the low level and a new timed formulation of a hierarchical reporter map modeling the information channel, via which the high-level system is 'virtualized' and driven by the low-level system. The Moore model of the low-level system may be constructed from a TDES model proposed in (Brandin and Wonham, 1994). This TDES model is a timed transition graph, and is a formulation that possesses sound system (event-) timing semantics as implicitly founded in (Brandin and Wonham, 1994), but formally and explicitly elucidated in this paper. In this system model, time is represented by a special event denoting an atomic tick of the global clock. By sound system timing semantics, we mean the system model possesses time fidelity, characterizing time progression as unstoppable and never halting an executing activity event. In generalizing hierarchical control to real time, the high-level system abstraction may aggregate time but should respect high-level time fidelity, in tandem with the low-level system model respecting low-level time fidelity. Without high-level time or output-time fidelity, designers would often need to go beneath the abstraction level to ensure that desired timing requirements are correctly specified for the real system at the low level, and this as a result could increase complexity and effort in specification design and synthesis.

There are several real-time control approaches using different TDES models proposed in the literature. Besides 'timed transition graphs' (Brandin and Wonham, 1994), other notable TDES models include 'clock automata' (Brave and Heymann, 1988), 'timed transition (semantics) models' (Ostroff and Wonham, 1990), 'timed state automata' (Cassandras, 1993), 'timed automata' used in (Wong-Toi and Hoffman, 1988; Alur and Dill, 1994), and 'timed Petri nets' (Cofer and Garg, 1996). Timed transition graphs are a specialized class of finite automata formulated as system models for real-time supervisory control of TDES's in (Brandin and Wonham, 1994), and are able to represent a variety of timing issues for a useful range of control problems (Wonham, 2016). Despite the well-known complexity shortcomings of timed transition graphs as TDES models (Knap, 2001; Gohari and Wonham, 2003), the real-time nonblocking control theory (Brandin and Wonham, 1994) and its subsequent developments form a mathematically rigorous body of conceptually rich work based on this graph model. These developments include work on supervisor reduction (Gohari and Wonham, 2003), efficient control synthesis using binary decision diagrams (BDD's) (Saadatpoor and Wonham, 2007), control under partial observation (Lin and Wonham, 1995; Cai et al, 2014), nonblocking control with communication delay (Park and Cho, 2008), specification automaton transparency for validation (Dhananjayan and Seow, 2015) and translation (Dhananjayan and Seow, 2014) from a class of real-time temporal logic, decentralized control (Nomura and Takai, 2011, 2013; Sadid et al, 2014), modular control (Ho, 2003; Schafaschek et al, 2017), localized or distributed control (Zhang et al, 2013) and that with communication delay (Zhang et al, 2014), and hierarchical control (Wong and Wonham, 1996; Saadatpoor, 2009). In our research, we add to this intellectually promising body of real-time control research by extending the monolithic control theory for TDES's (Brandin and Wonham, 1994) to hierarchical control. The contributions include a number of new timed concepts to support hierarchical consistency with output-time fidelity, within the same elementary framework and computational foundation for formal languages and finite automata.

Central to timed system abstractions for hierarchical consistency, without and with output-time fidelity guarantee, is the strict version of the respective new system abstraction concepts called output-control consistency and timed output-control consistency, extending the untimed version (Zhong and Wonham, 1990) to real time in this paper. Of critical interest is the latter stronger concept that captures the notion of time fidelity in system abstraction. The need for physical time fidelity in system abstraction is partly motivated by challenges in real-time design of cyber-physical systems (CPS's) (Lee, 2009, 2010). Characterized as holistic integrations of computation, communication, and physical systems, CPS's are an important source of hierarchical TDES's. In CPS research, it has been put forth that system abstractions carried out need to unify the low-level (i.e., digital or physical) timing dynamics and the high-level (or cyber) computations in a high-level system model with correct time representation for control design. Generalizing logical (Zhong and Wonham, 1990) to timed hierarchical control and borrowing the CPS terminology from (Lee, 2010), the proposed system abstraction for hierarchical consistency with output-time fidelity is said to correctly 'physicalize the cyber' by aggregating the physicality of time into the cyber (virtual) system, and 'cyberize the physical' by semantically linking cyber or high-level events and their control properties, defined in the cyber system for an application of interest, to appropriate physical control behaviors in terms of timed low-level events in the real (physical) system. Importantly, with or without time fidelity, the high-level TDES model of the hierarchy resulting from the application of either abstraction concept proposed is endowed with a natural control structure, which subsumes the tick preemption concept of event forcing (Brandin and Wonham, 1994) and is a generalization of the untimed version (Zhong and Wonham, 1990).

Despite its importance as a control architecture, there is relatively little work on hierarchical control in a real-time framework. One related early effort (Wong and Wonham, 1996) extends the hierarchical control of logical DES's (Zhong and Wonham, 1990; Wonham, 2016) - a bottom-up (or detail-abstraction) design approach - to a timed version. However, unlike the timed transition graph formulation of the TDES model (Brandin and Wonham, 1994) adopted for our research, in (Wong and Wonham, 1996), the system property of time not halting an executing event is relaxed for both levels of the hierarchy. Because of this relaxation, the tick event at both levels is akin to timeout[1] in general, and may be treated like any other event. The research therefore does not consider system time fidelity, and in this aspect is fundamentally different from this paper.

Another related effort (Saadatpoor, 2009; Saadatpoor et al, 2008) extends the hierarchical control using state tree structures (Ma and Wonham, 2005) - a top-down (or detail-refinement) design approach - to a real-time version. In this approach, a given TDES model is of the type (Brandin and Wonham, 1994) possessing time fidelity, and is encoded (equivalently) into a timed state tree structure without time aggregation or abstraction for efficient BDD-based control synthesis. System time fidelity is a non-issue in this computational approach.

The rest of the paper is organized as follows. Section 2 presents a relevant background for and on the modeling and control-theoretic study of TDES's that includes unearthing the fundamental properties of system tick preemptability and time fidelity. Section 3 follows up with a Moore system formulation for two-level hierarchical control, and explains the need for system output-time fidelity. Section 4 defines the constituent concepts for the system concept of timed output-control consistency, by which the system abstraction at the high level possesses a natural timed control structure as the system at the low level. An earlier version of the work in Section 4 was published in (Ngo and Seow, 2014b); the concepts are more fully developed in this paper. Together with these constituent concepts, Section 5 adds a timed concept of partner-freeness to formulate system sufficiency structures for hierarchical consistency between the two levels, without and with output-time fidelity guarantee. Section 6 investigates the structural existence and synthesis of the sufficiency structure for hierarchical consistency, based on which in Section 7, it is shown that hierarchical consistency can be achieved for a class of TDES hierarchies under mild output-system design restrictions, and the version with output-time fidelity can be achieved for a subclass 'linearly' structured under further output-system design restrictions. Section 7 ends with a discussion on generalizing and scaling to multiple levels the consistency of a two-level hierarchy. Section 8 concludes the paper. Examples and figures are provided to help explain and illustrate the theoretical concepts and the use of the procedures developed.

2 Background

The relevant notation for and background on supervisory control of TDES's, taken mainly from (Ramadge and Wonham, 1987; Brandin and Wonham, 1994), are reviewed in this section. The fundamental properties of preemptability and fidelity of system atomic time, founded implicitly in (Brandin and Wonham, 1994), are explicitly defined or elucidated for our subsequent theoretical development.

[1] A timeout event can be used in timed models as explained in (Cassandras and Lafortune, 2008b). It is a marker that specifies the maximal duration that a system can stay in a system state, within which an activity event it is defined for at the state is expected to occur. A timeout occurrence indicates that the activity event has failed to occur within the specified duration. Because the timeout occurrence may model disablement of the activity and other events upon entering a new state, it is different from time ticks that simply model time progression.

2.1 Languages & Automata for TDES Modeling

Let Σ be a finite set of symbols representing events. A string is a finite sequence of events. Let Σ^* be the set of strings over Σ, including the empty string ε (a sequence with no events); and $\Sigma^+ = \Sigma^* - \{\varepsilon\}$. Given a string $s \in \Sigma^*$, a string s' is a prefix of s, denoted by $s' \leqslant s$, if $(\exists t \in \Sigma^*) s't = s$; a strict prefix of s, denoted by $s' < s$, if $s' \leqslant s$ and $s' \neq s$; and a suffix of s if $(\exists t \in \Sigma^*) ts' = s$.

A formal language L is defined over Σ by a subset of Σ^*. For $L_1, L_2 \subseteq \Sigma^*$, L_1 is said to be a sublanguage of L_2 if $L_1 \subseteq L_2$. The prefix closure of L, denoted by $\overline{L}$, is $\overline{L} = \{s' \mid (\exists s \in L) s' \leqslant s\}$, the set of prefix strings of strings in L. Clearly, $L \subseteq \overline{L}$, and $L \neq \emptyset$ provided $\varepsilon \in \overline{L}$. The language L is said to be prefix-closed if $L = \overline{L}$.

A regular language is a language that can be generated by a finite-state automaton (Hopcroft and Ullman, 1979). An automaton G is a 5-tuple $(Q, \Sigma, \delta, q_0, Q_m)$, where Q is the set of states, Σ is the finite set of events, $\delta : \Sigma \times Q \to Q$ is the (partial and deterministic) transition function, q_0 is the initial state, and $Q_m \subseteq Q$ is the subset of marked states. Note that the state set Q is finite unless otherwise specified. That an event $\sigma \in \Sigma$ is defined at a state $q \in Q$ is denoted by $\delta(\sigma, q)!$, and $\neg\delta(\sigma, q)!$ otherwise. For an event subset $\Sigma' \subseteq \Sigma$ and a state $q \in Q$, let $\Sigma'(q) = \{\sigma \in \Sigma' \mid \delta(\sigma, q)!\}$, the subset of events in Σ' that are defined at state q. The transition function δ can be extended to Σ^* as follows: $\delta(\varepsilon, q) = q$, and $(\forall \sigma \in \Sigma)(\forall s \in \Sigma^*) \delta(s\sigma, q) = \delta(\sigma, \delta(s, q))$, which is defined if $q' = \delta(s, q)$ and $\delta(\sigma, q')$ are both defined.

Two languages characterize the behavior of automaton G, namely, the prefix-closed language $L(G) = \{s \in \Sigma^* \mid \delta(s, q_0)!\}$ and the marked language $L_m(G) = \{s \in L(G) \mid \delta(s, q_0) \in Q_m\}$. By definition, $L_m(G) \subseteq L(G)$. We write $G = EMPTY$ (called an empty automaton) provided the state set $Q = \emptyset$; and $L(EMPTY) = L_m(EMPTY) = \emptyset$.

A state $q \in Q$ is reachable (from the initial state q_0) if $(\exists s \in \Sigma^*) \delta(s, q_0) = q$, and coreachable if $(\exists s \in \Sigma^*) \delta(s, q) \in Q_m$. Automaton G is reachable if all its states are reachable, and coreachable if all its states are coreachable and so $\overline{L_m(G)} = L(G)$. Finally, automaton G is trim if it is both reachable and coreachable.

Graphically, an automaton G is represented by an edge-labeled directed graph as follows: A graphical node denotes an automaton state. A σ-labeled edge, directed from a node denoting a state q to a node denoting a state q', represents the transition of event σ from q to q', i.e., $\delta(\sigma, q) = q'$. A node with an entering arrow denotes the initial state q_0, and a node that is darkened or is a double-concentric circle denotes a marked state.

An automaton G is usually formed by the synchronization of n component automata $G_1, G_2, \cdots, G_n$, $n \geqslant 2$, whose interactions among them may be modeled on the synchronous operator $\|$ (Cassandras and Lafortune, 2008a); and is denoted by $G = G_1 \| G_2 \| \cdots \| G_n$, called the synchronous product. This product may be constructed for $n = 2$ as detailed in (Cassandras and Lafortune, 2008b), and recursively so for $n > 2$ by the associativity of $\|$. If the n automata share the same event set, then the synchronous product G reduces to the Cartesian product (Cassandras and Lafortune, 2008a), modeled on the Cartesian operator $\sqcap$ and denoted by $G = G_1 \sqcap G_2 \sqcap \cdots \sqcap G_n$.

2.2 Timed Discrete-Event System (TDES) Model

A TDES (Brandin and Wonham, 1994) 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

$$G_{act} = (A, \Sigma_{act}, \delta_{act}, a_0, A_m), \tag{1}$$

where the state set is redesignated as A, the set of activities, and is finite, with each activity associated with a time duration, Σ_{act} is the finite set of activity events, $\delta_{act} : \Sigma_{act} \times A \to A$ 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 $l_\sigma \leqslant u_\sigma$, 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 $tick \notin \Sigma_{act}$, and its occurrence denotes a transition or passage of an atomic unit of time. Under these time bound assignments, Σ_{act} is divided into two disjoint subsets Σ_{spe} and Σ_{rem}, i.e., $\Sigma_{act} = \Sigma_{spe} \cup \Sigma_{rem}$ and $\Sigma_{spe} \cap \Sigma_{rem} = \emptyset$, and this partition is denoted by $\Sigma_{act} = \Sigma_{spe} \dot\cup \Sigma_{rem}$. The set $\Sigma_{rem} = \{\sigma \in \Sigma_{act} \mid u_\sigma = \infty\}$ is called the subset of remote events; and the set $\Sigma_{spe} = \{\sigma \in \Sigma_{act} \mid u_\sigma < \infty\}$ is called the subset of prospective events. Each event $\sigma \in \Sigma_{act}$ has a local countdown timer t_σ with a default value $t_{\sigma 0}$, initialized as u_σ if $\sigma \in \Sigma_{spe}$, and l_σ if $\sigma \in \Sigma_{rem}$. Intuitively, the existence of a lower time bound means that an event σ is only eligible or *ready to occur* in the TDES after l_σ ticks upon entering an activity in G_{act} (1) where σ is defined, and will never occur before that; and each *tick* occurrence decreases the timer t_σ by one tick count, until $t_\sigma = 0$. If σ is a remote event and t_σ is or has decreased to 0, it becomes eligible but might or might not occur next. If σ is a prospective event, it might occur during $0 \leqslant t_\sigma \leqslant u_\sigma - l_\sigma$, and must occur next when $t_\sigma = 0$ (at which it is said to be imminent) unless it is preempted by another eligible activity event. The timer interval or duration D_σ is defined for σ as $[0, u_\sigma]$ if $\sigma \in \Sigma_{spe}$, and $[0, l_\sigma]$ if $\sigma \in \Sigma_{rem}$. Therefore, $t_\sigma \in D_\sigma$. Being instantaneous (Brandin and Wonham, 1994), an event occurrence is modeled as abrupt with no time duration.

Let $\Sigma = \Sigma_{act} \dot\cup \{tick\}$. Given the ATG G_{act} (1) and timer information as defined above for each event $\sigma \in \Sigma_{act}$, the TTG of the TDES is the automaton

$$G = (Q, \Sigma, \delta, q_0, Q_m), \tag{2}$$

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 $q = (a, -) \in Q$, σ is eligible at q provided $\delta(\sigma, q)!$, and is said to be enabled at q provided $\delta_{act}(\sigma, a)!$; and $\delta(\sigma, q)!$ iff $\delta_{act}(\sigma, a)!$ and

$$\begin{cases} t_\sigma = 0, & \text{if } \sigma \in \Sigma_{rem} \\ 0 \leqslant t_\sigma \leqslant u_\sigma - l_\sigma, & \text{if } \sigma \in \Sigma_{spe}. \end{cases} \tag{3}$$

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

$$\delta(tick, q)! \text{ iff } (\forall \beta \in \Sigma_{spe}, \delta_{act}(\beta, a)!) t_\beta > 0; \tag{4}$$

$$(\forall s \in \Sigma_{act}^{+}, \delta(s, q)!) \delta(s, q) \neq q. \tag{5}$$

Condition (4) - time-progressivity (TP) - 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 (ALF) - 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 (the languages of) TDES G.

In meeting TP (4) and ALF (5), the persistence of time (evolution) is not violated in TDES model G, characterizing the fact that a TDES can never stop the clock (Brandin and Wonham, 1994).

We now briefly review TDES composition (Brandin and Wonham, 1994). A TDES G is usually a modular system of n component TDES's $G_1, G_2, \cdots, G_n$, $n \geqslant 2$, with their respective component ATG's $G_{1,act}, G_{2,act}, \cdots, G_{n,act}$; and it is herewith denoted by $G = G_1 ||| G_2 ||| \cdots ||| G_n$, where $|||$ is called the composition operator. The approach of $|||$-composing the modular TDES G based on $G_{act} = G_{1,act} \parallel G_{2,act} \parallel \cdots \parallel G_{n,act}$ - the ATG of G, is detailed in (Brandin and Wonham, 1994). Where no two arbitrary component TDES's share an activity event, $G = G_1 ||| G_2 ||| \cdots ||| G_n = G_1 \parallel G_2 \parallel \cdots \parallel G_n$ (Wonham, 2016).

2.3 Timing Properties 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 $(\Sigma_{act}(q) = \varnothing) \Longrightarrow \delta(tick, q)!$.

Proof For a state $q = (a, \{t_\beta \mid \beta \in \Sigma_{act}\})$, assume $\Sigma_{act}(q) = \varnothing$. Then, to prove that $\delta(tick, q)!$, according to TP (4), we need to show that for all $\beta \in \Sigma_{spe}$ such that $\delta_{act}(\beta, a)!$, $t_\beta > 0$. Since $\Sigma_{act}(q) = \varnothing$ iff for all $\beta \in \Sigma_{act}$, $\neg\delta(\beta, q)!$, it follows by the assumption and (3) that, for all $\beta \in \Sigma_{spe}$ such that $\delta_{act}(\beta, a)!$, $t_\beta > u_\beta - l_\beta \geqslant 0$, i.e., $t_\beta > 0$. Hence the property. □

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.

The next property strengthens Property 1.

Property 2 (Prospective persistence of time) Let $q = \delta(s, q_0)$. Then $(\Sigma_{act}(q) \cap \Sigma_{spe} = \varnothing) \Longrightarrow \delta(tick, q)!$.

Proof For a state $q = (a, \{t_\beta \mid \beta \in \Sigma_{act}\})$, assume $\Sigma_{act}(q) \cap \Sigma_{spe} = \varnothing$. Then, since $\Sigma_{act}(q) \cap \Sigma_{spe} = \varnothing$ iff $\Sigma_{act}(q) = \varnothing$ or $(\Sigma_{act}(q) \neq \varnothing \;\&\; \Sigma_{act}(q) \subseteq \Sigma_{rem})$, we need to prove two cases, as follows:

- *Case 1*: Suppose $\Sigma_{act}(q) = \emptyset$. Then, by Property 1, it follows that $\delta(tick, q)!$.
- *Case 2*: Suppose $\Sigma_{act}(q) \neq \emptyset$ & $\Sigma_{act}(q) \subseteq \Sigma_{rem}$. Then to prove that $\delta(tick, q)!$, according to TP (4), we need to show that for every event $\beta \in \Sigma_{spe}$ such that $\delta_{act}(\beta, a)!$, $t_\beta > 0$, as follows:
  Applying the fact that $\Sigma_{rem} \cap \Sigma_{spe} = \emptyset$, we have $\Sigma_{act}(q) \cap \Sigma_{spe} = \emptyset$, meaning that $\neg\delta(\beta, q)!$ for all $\beta \in \Sigma_{spe}$. Therefore, by (3), it follows that, for all $\beta \in \Sigma_{spe}$ such that $\delta_{act}(\beta, a)!$, $t_\beta > u_\beta - l_\beta \geqslant 0$, i.e., $t_\beta > 0$.

Hence the property. □

The property states that the event *tick* is always eligible at a reachable state with no eligible prospective event.

Property 3 (Time invariance of event eligibility) Let $q = \delta(s, q_0)$ and $q' = \delta(tick, q)$. Then $\Sigma_{act}(q) \subseteq \Sigma_{act}(q')$.

Proof Let $q' = \delta(tick, q)$, with $q = (a, \{t_\beta \mid \beta \in \Sigma_{act}\})$ and $q' = (a', \{t'_\beta \mid \beta \in \Sigma_{act}\})$. Since $q' = \delta(tick, q)$ and $\neg\delta_{act}(tick, a)!$, $a' = a$. Therefore, for $\beta \in \Sigma_{act}$, $\delta_{act}(\beta, a)!$ iff $\delta_{act}(\beta, a')!$. Since $\Sigma_{act} = \Sigma_{spe} \dot{\cup} \Sigma_{rem}$, to show that for $\beta \in \Sigma_{act}, \beta \in \Sigma_{act}(q) \Longrightarrow \beta \in \Sigma_{act}(q')$, we need to prove two cases, as follows:

- *Case 1*: Suppose $\beta \in \Sigma_{act}(q) \cap \Sigma_{spe}$. Then $\delta(\beta, q)!$ and by (3), $\delta_{act}(\beta, a)!$ & $0 \leqslant t_\beta \leqslant u_\beta - l_\beta$. Since $\delta(tick, q)!$, $t_\beta > 0$ by (4). Since $\delta_{act}(\beta, a)!$ & $\beta \in \Sigma_{spe}$ & $t_\beta > 0$, the occurrence of *tick* only decreases timer t_β by one unit, i.e., $t'_\beta = t_\beta - 1$. Hence, since $0 \leqslant t'_\beta \leqslant u_\beta - l_\beta$ & $\delta_{act}(\beta, a')!$, $\delta(\sigma, q')!$ by (3), and therefore $\beta \in \Sigma_{act}(q')$.
- *Case 2*: Suppose $\beta \in \Sigma_{act}(q) \cap \Sigma_{rem}$. Then $\delta(\beta, q)!$ and by (3), $\delta_{act}(\beta, a)!$ & $t_\beta = 0$. Since $\delta_{act}(\beta, a)!$ & $\beta \in \Sigma_{rem}$ & $t_\beta = 0$, the occurrence of *tick* does not decrease the timer t_β further, i.e., $t'_\beta = t_\beta = 0$. Hence, since $t'_\beta = 0$ & $\delta_{act}(\beta, a')!$, $\delta(\beta, q')!$ by (3), and therefore $\beta \in \Sigma_{act}(q')$.

Hence the property. □

The property states that eligible activity events at a reachable state remain eligible at another following the time elapse of a tick. By Property 3, 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 activity event occurs instantaneously.

2.4 Control-Theoretic Setting & System Time Fidelity

The control-theoretic setting (Brandin and Wonham, 1994) for TDES's assumes that the subset of events controllable by an external supervisor is predetermined. In a logical DES, an event is controllable if it is prohibitable, in that it can be prevented from occurring by (control) disablement. Extending to a TDES G (2), this notion of controllability is subsumed for activity events, and the event *tick* solely denoting an elapsed real time is also considered controllable wherever its system transitions can be preempted. In TDES G (2), it is further postulated that an event in Σ_{spe} is not prohibitable, or uncontrollable, and it must occur next once its upper time bound is reached unless it is preempted by another eligible activity event, whereas an event in Σ_{rem} may be. With $\Sigma_{act} = \Sigma_{spe} \dot{\cup} \Sigma_{rem}$, it follows that the set of prohibitable events, denoted by Σ_{hib}, is a subset of Σ_{rem}, i.e., $\Sigma_{hib} \subseteq \Sigma_{rem}$. In what follows, the uncontrollable event set is defined as $\Sigma_u = \Sigma_{act} - \Sigma_{hib} = \Sigma_{spe} \dot{\cup} (\Sigma_{rem} - \Sigma_{hib})$. Let $\Sigma_{for} \subseteq \Sigma_{act}$ be the set of forcible events. An event in Σ_{act} is either forcible or it is not. 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. As a forcible event can be either prohibitable or uncontrollable, various cases with regard to the preemptability of *tick* by a forcible event are distinguished in Definition 1.

Definition 1 (Tick preemptability) The event $tick \in \Sigma(q)$ with $q = \delta(s, q_0)$ for an arbitrary $s \in L(G)$ is said to be non-preemptable at q if $\Sigma(q) \cap \Sigma_{for} = \emptyset$; unambiguously preemptable at q if $\Sigma(q) \cap \Sigma_{for} \cap \Sigma_u \neq \emptyset$; and ambiguously preemptable at q if $\Sigma(q) \cap \Sigma_{for} \cap \Sigma_u = \emptyset$ & $\Sigma(q) \cap \Sigma_{for} \cap \Sigma_{hib} \neq \emptyset$.

Where the context is understood, 'at q' in Definition 1 is dropped when referring to tick preemptability.

The event *tick* is 'controllable' by preemption through a forcible event, not by disablement as for an event in Σ_{hib}, since nothing can stop the global clock. Accordingly, the controllable event set is defined as $\Sigma_c = \Sigma - \Sigma_u = \Sigma_{hib} \dot{\cup} \{tick\}$. Therefore, $\Sigma = \Sigma_c \dot{\cup} \Sigma_u$ and this is identical to the control-theoretic setting for logical DES's (Ramadge and Wonham, 1987).

Whenever it is not written as a member of the respective event subsets, a prohibitable and an uncontrollable event may be identified by a superscript '+' and '-' on its event symbol, respectively, and additionally followed by a superscript '#' provided the event is forcible.

We now define the various notions of control strings (and events) with respect to (w.r.t) the transition structure of a TDES G. Given an arbitrary nonempty string $s = \sigma_1\sigma_2 \cdots \sigma_k \in \Sigma^*$ which is a suffix of some string of $L(G)$, and where $\sigma_i \in \Sigma$ for all i $(1 \leqslant i \leqslant k)$, string s is said to be

- controllable if, for some i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_{hib}$, or $\sigma_i = tick$ and is unambiguously preemptable;
- uncontrollable if, for all i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_u$, or $\sigma_i = tick$ and is non-preemptable;
- ambiguously controllable if, for all i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_u$, or $\sigma_i = tick$ and is not unambiguously preemptable, and for some j $(1 \leqslant j \leqslant k)$, $\sigma_j = tick$ and is ambiguously preemptable;
- preemption-unambiguous if, for all i $(1 \leqslant i \leqslant k)$, either $\sigma_i \in \Sigma_{act}$, or $\sigma_i = tick$ and is not ambiguously preemptable.

Note that a string s as defined above is either controllable, uncontrollable or ambiguously controllable. Therefore, it is not controllable if it is either uncontrollable or ambiguously controllable, or equivalently, for all i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_u$, or $\sigma_i = tick$ and is not unambiguously preemptable. An ambiguously controllable event is an ambiguously preemptable *tick*. A preemption-unambiguous string does not contain ambiguously preemptable ticks, and an uncontrollable string is preemption-unambiguous.

Now, given the uncontrollable event set Σ_u in the control-theoretic setting formulated, an important system model property that strengthens Property 1 but weakens Property 2 may be presented.

Property 4 (Uncontrollable persistence of time) Let $q = \delta(s, q_0)$. Then $(\Sigma_{act}(q) \cap \Sigma_u = \varnothing) \implies \delta(tick, q)!$.

Proof By the fact that $\Sigma_{spe} \subseteq \Sigma_u$, a logical corollary, replacing Σ_{spe} in Property 2 by Σ_u, follows. Hence the property. □

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 4 present new supporting insights for our research. They provide a clearer understanding of the TDES model G (2) (Brandin and Wonham, 1994) reviewed. In fact, Properties 3 and 4 together with ALF (5) of the TDES G model system time fidelity, characterizing time progression as never halting an executing activity event (Property 3) and unstoppable (Property 4 and ALF (5)). Equivalently, the model G is said to possess sound system (event-) timing semantics; or the time *tick* is said to be Σ-uninterrupting.

In general, an arbitrary TDES model is said to possess time fidelity if it is a TTG G that obeys Properties 3 and 4, as well as ALF (5).

2.5 Supervisory Control of TDES's

For a sublanguage $L \subseteq L(G)$ (having the same event set Σ), let $\Sigma^L(q) = \{\sigma \in \Sigma \mid \delta(\sigma, q)! \text{ and } s\sigma \in \overline{L}\}$ be the set of eligible events at state q w.r.t Σ and the string $s \in \overline{L}$, such that $q = \delta(s, q_0)$. Then a (specification) language $K \subseteq \Sigma^*$ is said to be controllable w.r.t G if, for all $s \in \overline{L}$ with $\overline{L} = \overline{K} \cap L(G)$,

$$\Sigma^L(q) \supseteq \begin{cases} \Sigma(q) \cap (\Sigma_u \cup \{tick\}), & \text{if } \Sigma^L(q) \cap \Sigma_{for} = \varnothing \\ \Sigma(q) \cap \Sigma_u, & \text{if } \Sigma^L(q) \cap \Sigma_{for} \neq \varnothing. \end{cases}$$

Intuitively, it means that following an arbitrary string $s \in \overline{L}$, the TDES G does not slip out (of $\overline{L}$ and hence $\overline{K}$) on an uncontrollable event, and any *tick* that it may slip out on can be preempted without the TDES slipping out as a result. In general, K may not be controllable w.r.t G, but the supremal (or largest) controllable marked sublanguage of the TDES G that lies within K exists. This sublanguage can be generated by a trim automaton computed as $Supcon(G, K)$[2] (Brandin and Wonham, 1994; Wonham, 2016), and is exactly L provided K is controllable and $L = K \cap L_m(G)$.

$Supcon(G, K)$ is a timed supervisor automaton S with the same event set Σ, and is said to be nonblocking (for TDES G) since $\overline{L_m(S)} = L(S)$ for a trim and hence coreachable $S = Supcon(G, K)$. As a supervisor that can generate the marked language of $Supcon(G, K)$ in conjunction with TDES G, $S = Supcon(G, K)$ is said to be optimal or maximally permissive (w.r.t G under language K). To exercise supervision on G, the supervisor S can 'disable' events in $\Sigma_c = \Sigma_{hib} \dot\cup \{tick\}$, i.e., disable prohibitable activity events and preempt *tick*, where appropriate.

Let $\overline{G}$ be TDES G but with all its states marked. It follows that if $S = Supcon(\overline{G}, \overline{K})$, then $L_m(S) = L(S)$; and by definition, an arbitrary language Z for which $\overline{Z} \cap L(G) = L(S)$ is controllable w.r.t G. Such a 'safety' supervisor S obtained for Z is not guaranteed to be nonblocking for the original TDES G, unless $\overline{Z \cap L_m(G)} = L(S)$.

[2] Note that, since TDES G is a (finite-state) TTG, the language of interest for control synthesis, $K \cap L_m(G)$, is a regular language and can thus be modeled by a TTG. In the algorithmic computation (Wonham, 2016) of $Supcon(G, K)$, K can be practically expressed as a regular language by a specification TTG.

Finally, in practice, a (control) specification language, an arbitrary constraint on which a supervisor is to be synthesized to restrict (the behavior of) a TDES as specified, is prescribed by an automaton. To fix the notion of specification languages in automata, we define a specification TTG C for a TDES G as a trim automaton that shares the same event set as the TDES G. This TTG is said to prescribe the specification language $L_m(C)$ for restricting G to within the language $L_m(C \sqcap G)$. Note that the essence of the control requirements by specification TTG C is in the 'composed' specification TTG $C \sqcap G$, which prescribes intra-system restrictions. As these restrictions include prohibitions on activity events and tick preemption in general, $C \sqcap G$ need not satisfy Properties 3 and 4 of system time fidelity.

3 Towards a TDES Hierarchy with Time Fidelity

In a two-level hierarchical setup as in (Zhong and Wonham, 1990), 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 (Eilenberg, 1974) is used.

3.1 Low-level TDES Model Formulation for Hierarchical Control

In general, a TDES model G (2) with event set Σ needs to be re-structured into a Moore automaton (G_{lo}, V) - an automaton[3] $G_{lo} = (Q, \Sigma, \delta, q_0, Q_m)$ associated with an information channel defined by a vocalization map $V : Q \rightarrow T \dot\cup \{\tau_o\}$, where $T = T_{act} \dot\cup \{t_h\}$ - such that $L(G_{lo}) = L(G)$ and $L_m(G_{lo}) = L_m(G)$. T_{act} denotes the high-level (virtual) activity event set, t_h, called a high-level time or output-time tick, denotes a time aggregation of low-level ticks of the global clock in TDES G_{lo}, and the symbol τ_o denotes a 'silent output'. For the low-level TDES G_{lo}, we henceforth replace *tick* by t_l to distinguish it as a low-level atomic time tick; therefore, $\Sigma = \Sigma_{act} \dot\cup \{t_l\}$.

Let w^n denote a string of $n \in \mathbb{N}$ consecutive occurrences of string w, with $w^0 = \varepsilon$; and w^* denote strings of finitely many occurrences of string w such that we write $sw^* \in L(G_{lo})$ if, for all $n \geqslant 0$, $sw^n \in L(G_{lo})$, and is such that $\delta(w, q) = q$, where $q = \delta(s, q_0) \in Q$. Then the Moore construction (Eilenberg, 1974) of G_{lo} for the TDES G is based on a given timed reporter map - a virtual projection $\theta : L(G) \rightarrow T^*$, defined such that $\theta(\varepsilon) = \varepsilon$ and, for $\sigma \in \Sigma$ 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 θ obeys the following time-output design laws:

Law 1: For $s(s' t_l s'')^* \in L(G)$, and $s', s'' \in \Sigma^*$, $\theta(s(s' t_l s'')^n) = \theta(s)(t' t_h t'')^n$ for all $n \geqslant 0$, where $t', t'' \in T^*$.
Law 2: For $\sigma \in \Sigma$ and $s\sigma \in L(G)$, $\theta(s\sigma) = \theta(s) t_h \Longrightarrow \sigma = t_l$.

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_l, i.e., $\delta(s' t_l s'', q) = q$ for some $s', s'' \in \Sigma^*$, the loop string $s' t_l s''$ must traverse through a state in G_{lo} that outputs or vocalizes a high-level time tick t_h. In this sense, G_{lo} is t_h-responsive. The constraint by Law 2 means that the high-level tick t_h is a time output, in that it must be real time-driven, i.e., t_h is always a vocalization that immediately follows the execution of a low-level tick t_l in G_{lo}. With θ 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

$$V(\delta(s', q_0)) = \begin{cases} \tau_o, & \text{if } s' = \varepsilon \text{ or } \delta(s', q_0) \notin Q_{voc} \\ \tau \in T, \text{ otherwise,} \end{cases}$$

where the selected subset $Q_{voc} \subseteq Q$, called vocal state set, is defined as follows. For $\sigma \in \Sigma$ and $s' = s\sigma$,

$$\delta(s\sigma, q_0) \begin{cases} \notin Q_{voc}, \text{ if } \theta(s\sigma) = \theta(s) \\ \in Q_{voc}, \text{ if } \theta(s\sigma) = \theta(s)\tau. \end{cases}$$

A conceptual procedure applicable for constructing a Moore TDES (G_{lo}, V) from a given TDES G and a reporter map θ, or simply a TDES (G, θ), is prescribed in (Zhong and Wonham, 1990; Wonham, 2016). In the graphical representation of G_{lo} and any Moore automaton in general, every vocal state is represented by a node containing the symbol of an event that it vocalizes.

[3] Although the same 5-tuple notation is used as in Section 2.4, 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.

The inverse reporter map for $t \in T^*$ is now defined as follows: $\theta^{-1}(t) = \{s \in L(G_{lo}) \mid \theta(s) = t\}$. In what follows, extending θ and θ^{-1} to $\theta(K) \subseteq T^*$ for $K \subseteq L(G_{lo})$ and $\theta^{-1}(E) \subseteq L(G_{lo})$ for $E \subseteq T^*$, respectively, we have: $\theta(K) = \{\theta(s) \mid s \in K\}$, and $\theta^{-1}(E) = \bigcup_{t \in E} \theta^{-1}(t)$.

The Moore automaton (G_{lo}, V) is simply referred to as G_{lo} when V is understood. Under the map V, G_{lo} outputs events in T to drive some high-level θ-image model G_{hi} whenever it reaches a vocal state $q \in Q_{voc}$, and otherwise outputs the silent symbol $\tau_o \notin T$ to signal no 'significant' change for the high level. Formally, model G_{hi}, the high-level image of G_{lo}, is an automaton such that $L(G_{hi}) = \{\theta(s) \mid s \in L(G_{lo})\}$ and $L_m(G_{hi}) = \{\theta(s) \mid s \in L_m(G_{lo})\}$. G_{hi} is said to generate events of T under the θ-map on $L(G_{lo})$. The pair (G_{lo}, G_{hi}) represents a two-level TDES hierarchy.

The vocal language of G_{lo}, denoted by $L_{voc}(G_{lo})$, is

$$L_{voc}(G_{lo}) = \{s \in L(G_{lo}) \mid s = \varepsilon \text{ or } \delta(s, q_0) \in Q_{voc}\},$$

which is the sublanguage of $L(G_{lo})$ containing the empty string ε and all the strings of $L(G_{lo})$, called vocal strings, that end in a state of Q_{voc}. In a richer characterization, let an arbitrary vocal string $s \in L(G_{lo})$, denoted by

$$s = < s', \sigma_i, x_i, k, \tau >, \tag{6}$$

to be of the form $s = s'\sigma_1\sigma_2 \cdots \sigma_k$ with $\sigma_i \in \Sigma$ $(1 \leqslant i \leqslant k)$, such that:

- $V(\delta(s', q_0)) \in T$ if $s' \neq \varepsilon$,
- $V(\delta(s'\sigma_1\sigma_2 \cdots \sigma_i, q_0)) = \tau_o \quad (1 \leqslant i \leqslant k-1)$,
- $V(\delta(s, q_0)) = \tau \in T$,
- $x_0 = \delta(s', q_0)$,
- $x_i = \delta(s'\sigma_1\sigma_2 \cdots \sigma_i, q_0) \quad (1 \leqslant i \leqslant k)$.

In every $s = < s', \sigma_i, x_i, k, \tau >$ (6) of $L(G_{lo})$, $s' \in L(G_{lo})$ 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 $s \in L(G_{lo})$ is called a τ-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_{lo}, to a vocal state outputting the high-level event $\tau \in T$. This suffix is called the co-silent string of s (6).

A fundamental result for the Moore TDES model G_{lo} follows.

Lemma 1 $L(G_{lo}) = \overline{L_{voc}(G_{lo})}$.

Proof For a TDES model G_{lo}, that $\overline{L_{voc}(G_{lo})} \subseteq L(G_{lo})$ is straightforward. It remains to show that $L(G_{lo}) \subseteq \overline{L_{voc}(G_{lo})}$, as follows: By Property 1 and the finiteness of state set Q of the TDES G_{lo}, every $s'_p \in L(G_{lo})$ can be extended to some $s'w^* \in L(G_{lo})$, where $s'_p \leqslant s'$ and $w \in \Sigma^+$. Then since $\delta(w, q) = q$, where $q = \delta(s', q_0) \in Q$, by ALF (5) of G_{lo}, i.e., the fact that $(\forall q \in Q)(\forall s \in \Sigma^+_{act}, \delta(s, q)!)\delta(s, q) \neq q$, string $w \notin \Sigma^+_{act}$ and hence contains a tick t_l. By design Law 1 of the reporter map θ from which the time-output responsive G_{lo} is constructed, for $s'w^* \in L(G_{lo})$, it necessarily follows that $\theta(s'w) = \theta(s')t_1t_ht_2$, where $t_1, t_2 \in T^*$. Therefore, $\theta(s')t_1t_h \in L(G_{hi})$, and since $\theta(L(G_{lo})) = L(G_{hi})$, there exists a t_h-string $s'' \in L_{voc}(G_{lo})$ with $s' \leqslant s''$ such that $\theta(s'') = \theta(s')t_1t_h$. Then, since $s'_p \leqslant s'$, and therefore $s'_p \leqslant s''$, it follows that $s'_p \in \overline{L_{voc}(G_{lo})}$. Hence the lemma. □

Two propositions for a TDES hierarchy (G_{lo}, G_{hi}) may now be presented.

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

Proof Consider a TDES hierarchy (G_{lo}, G_{hi}), where $G_{hi} \overset{\text{def}}{=} (X, T, \xi, x_0, -)$. By Property 1 and the finiteness of state set Q of the TDES G_{lo}, every $s'_p \in L(G_{lo})$ can be extended to some $s'w^* \in L(G_{lo})$, where $s'_p \leqslant s'$ and $w \in \Sigma^+$. Then since $\delta(w, q) = q$, where $q = \delta(s', q_0) \in Q$, by ALF (5) of G_{lo}, i.e., the fact that $(\forall q \in Q)(\forall s \in \Sigma^+_{act}, \delta(s, q)!)\delta(s, q) \neq q$, string $w \notin \Sigma^+_{act}$ and hence contains a tick t_l. By design Law 1 of the reporter map θ from which the time-output responsive G_{lo} is constructed, it follows that, for $s'w^* \in L(G_{lo})$, $\theta(s'w^n) = \theta(s')(t_1t_ht_2)^n$ for all $n \geqslant 0$, where $t_1, t_2 \in T^*$. Since state set X of G_{hi} is finite, there exist an $n_1 \geqslant 0$ and an $n_2 \geqslant 1$ such that for all $n \geqslant 0$, $\theta(s')(t_1t_ht_2)^{n_1}t_0^n \in L(G_{hi})$, where $t_0 = (t_1t_ht_2)^{n_2}$, and is such that $\xi(t_0, x') = x'$, where $x' = \xi(\theta(s')(t_1t_ht_2)^{n_1}, x_0) \in X$ (and we can thus write $\theta(s')(t_1t_ht_2)^{n_1}t_0^* \in L(G_{hi})$). Therefore, $(\forall x \in X)(\forall t \in T^+, \xi(t, x)!)$ $((\xi(t, x) = x) \implies t \notin T^+_{act})$. By contraposition, $(\forall x \in X)(\forall t \in T^+_{act}, \xi(t, x)!)\xi(t, x) \neq x$. Hence the proposition. □

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

Proof Consider a TDES hierarchy (G_{lo}, G_{hi}), where $G_{hi} \overset{\text{def}}{=} (X, T, \xi, x_0, -)$. Then, for an arbitrary $t \in L(G_{hi})$ and hence an arbitrary state $x = \xi(t, x_0) \in X$, we need to prove that Property 1 for G_{hi}, i.e., $(T_{act}(x) = \emptyset) \Longrightarrow \xi(t_h, x)!$, holds, as follows: Since $\theta(L(G_{lo})) = L(G_{hi})$, there must exist a string $s \in L_{voc}(G_{lo})$ such that $\theta(s) = t$. By Property 1 for G_{lo}, there exists some $\sigma \in \Sigma$ such that $s\sigma \in L(G_{lo})$. Furthermore, by Lemma 1, there must also exist a string $w \in \Sigma^*$ such that $s\sigma w \in L_{voc}(G_{lo})$ and is some τ-string of $L(G_{lo})$, where $\tau \in T$ and string s is its reference prefix. With $\theta(s\sigma w) = t\tau$ and thus $\xi(\tau, \xi(t, x_0))!$, it follows that if $T_{act}(\xi(t, x_0)) = \emptyset$, then $\tau \notin T_{act}$ which means $\tau \in T - T_{act}$, i.e., $\tau = t_h$. Hence the proposition. □

In other words, the passage of aggregated time, as represented by the ticking of t_h, is continual in the (uncontrolled) high-level TDES G_{hi}, in that the tick t_h is always eligible in the absence of activity events at a state of G_{hi}.

3.2 System Abstraction: Need for Output-Time Fidelity

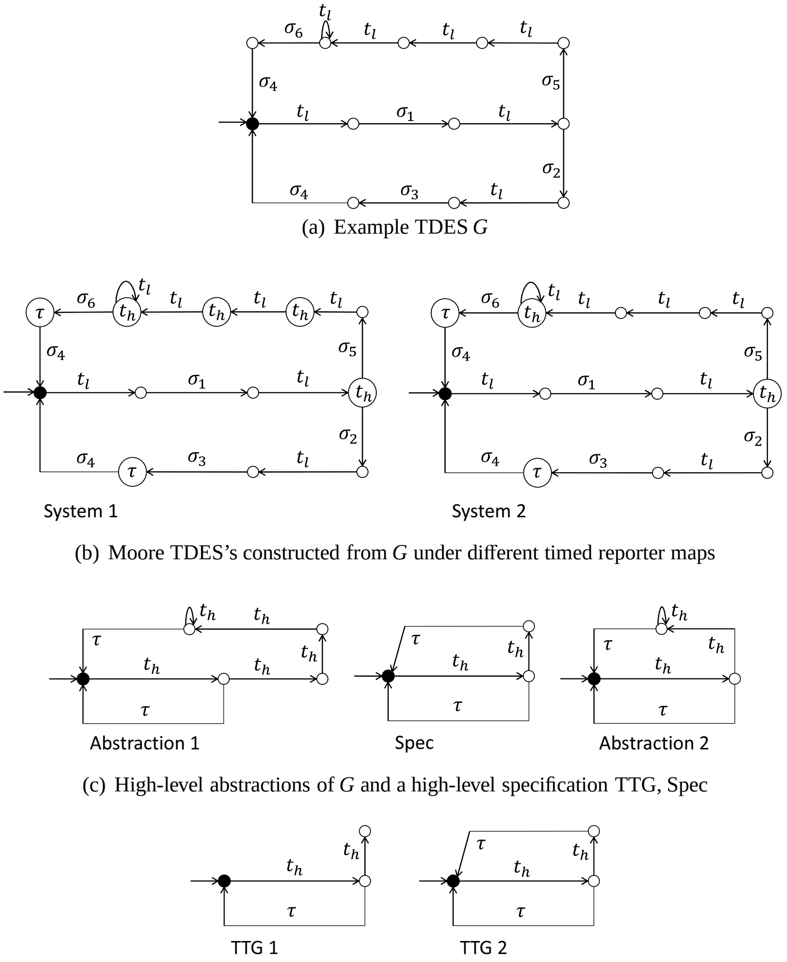
The transition of a high-level time tick $t_h \in T$ in a system model abstraction (Wong and Wonham, 1996) denotes the passage of some low-level time ticks of t_l. Time abstraction (or state vocalization of $t_h \in T$) is qualitative if it signals an amount of low-level time elapsed that is possibly irregular but deemed important by hierarchical design, in which case it is said to apply a non-periodic timescale (between the high and low level). Time abstraction is quantitative if a periodic timescale $1 : n$ reminiscent of that in (Gohari and Wonham, 2003) is applied, which is a fixed time ratio of 1 high-level tick of t_h for every n low-level ticks of t_l, where integer $n \geqslant 1$. However, be it qualitative or quantitative, to lay a sound design foundation for timed hierarchical control, we postulate that high-level time (or output-time) fidelity must also be upheld in the control design of a hierarchical abstraction for a base or low-level TDES model under the real-time control-theoretic setting (Brandin and Wonham, 1994) reviewed. This is so that the event timing feature, of *specifying a real-time requirement for control that is naturally in congruence with time fidelity of the TDES model* as laid in (Brandin and Wonham, 1994), can be extended to system abstraction. By this, we mean that a real-time specification such as ‘an activity event must complete execution within one time tick since it started’ can be prescribed in terms of $t_h \in T$ for the system abstraction, with the sublanguage generated by the high-level timed specification on the system abstraction not violating the intended high-level timing semantics of the specification. Otherwise, we would often need to go beneath the abstraction level to examine or re-examine the low-level Moore system structure, to ascertain if desired timing requirements are correctly prescribed.

Example 1 Consider an example depicted in Fig. 2. For the TDES G given in Fig. 2(a), two system abstractions are proposed, as shown in Fig 2(b). Both the abstractions possess ALF and Property 4[4]. But Abstraction 1 violates Property 3, whereas Abstraction 2 does not and hence possesses time fidelity.

Now, to illustrate the need for time fidelity in system abstraction, consider a high-level specification TTG Spec, as shown in Fig. 2(c). It asserts that a high-level activity event τ must complete execution in not more than one high-level time tick upon event eligibility or initiation. As shown in Fig. 2(d), the sublanguage due to the specification on Abstraction 1 (without time fidelity) is represented by TTG 1, whereas that due to the same specification on Abstraction 2 (with time fidelity) is represented by TTG 2. Clearly, as opposed to TTG 2, the timing semantics of TTG 1 is incorrect or unsound against the intended timing requirement of ‘at most one tick for τ-completion’ prescribed by Spec, as τ appears as disabled after a high-level tick. ■

To specify real-time high-level specifications for hierarchical control without incorrect high-level timing semantics due to the system abstraction, the problem of interest is to construct not only a system abstraction possessing time fidelity such as Abstraction 2, but also one endowed with a natural timed control structure that subsumes time fidelity, as will be elaborated in the next section. Put simply, our intent is to preserve real-time system dynamics at the abstraction or high level with conceptually the same real-time control-theoretic setting as assumed or given at the low level. Reviewed in Section 2, the assumed setting is the real-time system model and control basis under which the control synthesis method for TDES’s (Brandin and Wonham, 1994) is developed. Importantly, it is the necessary basis on which an arbitrary proper control specification for a given TDES can always be stated. A real-time specification is said to be proper if, in conjunction with a given TDES, it generates a sublanguage of sound timing semantics (against the specified high-level timings), for *real-time* and not simply *timed* control synthesis, against which the supervisor synthesized can be unambiguously understood in terms of permitting or restricting the specified real-time durations for activity events.

[4] In this example, the high-level tick t_h is eligible at every state in both the system abstractions, hence their satisfying Property 4.



(a) Example TDES G

(b) Moore TDES's constructed from G under different timed reporter maps

(c) High-level abstractions of G and a high-level specification TTG, Spec

(d) TTG's of the high-level system sublanguages generated for Spec

Fig. 2 Implications on the timing semantics of a high-level specification on system abstractions without and with high-level time fidelity: An illustration

4 Timed Control Structure

To admit control for a TDES hierarchy (G_{lo}, G_{hi}), the high-level activity event set T_{act} of G_{hi} is partitioned into the prohibitable event set T_{hib} and the uncontrollable event set T_u, and into the forcible event set T_{for} and the non-forcible event set $T_{act} - T_{for}$; with controllable event set $T_c = T_{hib} \dot{\cup} \{t_h\}$. However, the two high-level control-theoretic partitions may not be unambiguous and correct under a given control-theoretic setting and a (Moore transition) structure of G_{lo}. Even if they are, the structure of G_{hi} is a TTG that might not possess time fidelity (w.r.t t_h), although the TDES G_{lo}, constructed from a given TDES G (2) and a reporter map θ, does (w.r.t t_l).

For real-time high-level control of (G_{lo}, G_{hi}), G_{lo} in general needs to be structurally refined so that G_{hi} is endowed with a natural timed control structure (w.r.t subsets $T_{hib}, T_u, T_{for}, T_{act} - T_{for}$ and $\{t_h\}$), i.e., so that every high-level event $\tau \in T_{act}$ defined and output by G_{lo} is unambiguously prohibitable or uncontrollable if it is in T_{hib} or in T_u, respectively, and is unambiguously forcible or non-forcible if it is in T_{for} or in $T_{act} - T_{for}$, respectively, and the time tick $t_h \in T$ is T-uninterrupting. The Moore transition structure of the TDES G_{lo} is defined to be timed output-control consistent if G_{hi} possesses such a natural timed control structure.

In what follows, we present the theoretical development of the fundamental system concept of timed output-control consistency, to lay a time fidelity foundation for feasible hierarchical control of TDES's. We first formulate and explain the component concepts, namely, activity output-control consistency, output-force consistency and output time-compliance. The formulation of these concepts entails the system definition of vocal string structure (6).

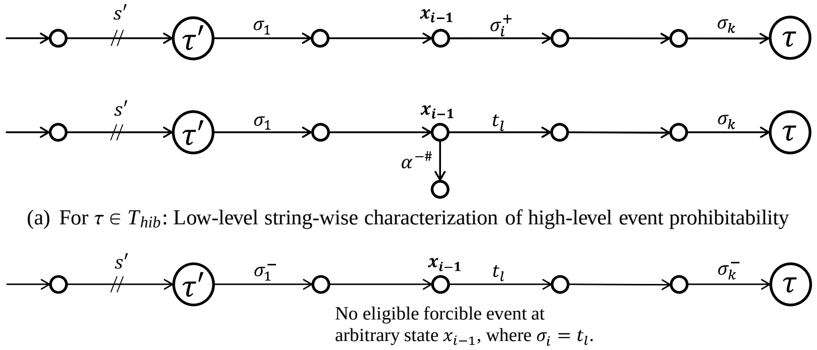
Where a graphical illustration of a concept is needed, it is concisely depicted in shorthand drawing notation, where a string traversing between two pertinent system states is graphically represented by a directed edge as for an event, and labeled by the string whose consecutive event transitions it represents unless the context is clear, without showing the intermediate states and transitions, and the edge has no double bars (//) across it only if the intermediate states that the string traverses through are all non-vocal.

4.1 Activity Output-Control Consistency

Definition 2 (Activity output-control consistency) A TDES G_{lo} is said to be activity output-control consistent (AOCC) if, for every τ-string $< s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$, it is the case that

- if $\tau \in T_{hib}$, then $\sigma_1 \cdots \sigma_k$ is controllable, i.e., for some i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_{hib}$ or $(\sigma_i = t_l \;\&\; \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_u \neq \emptyset)$,
- if $\tau \in T_u$, then $\sigma_1 \cdots \sigma_k$ is uncontrollable, i.e., for all i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \;\&\; \Sigma(x_{i-1}) \cap \Sigma_{for} = \emptyset)$.

For an AOCC G_{lo}, as depicted in Fig. 3(a), $\tau \in T_{hib}$ only if there is a low-level event in the co-silent string, of every τ-string of $L(G_{lo})$, which is prohibitable or is a tick t_l at a state where an uncontrollable and forcible event is also eligible. As depicted in Fig. 3(b), $\tau \in T_u$ only if every low-level event in the co-silent string, of every τ-string of $L(G_{lo})$, is uncontrollable or is a tick t_l at a state where no forcible event is eligible. Therefore, being AOCC means that every high-level event $\tau \in T_{act}$ (defined, and output by G_{lo}) is unambiguously prohibitable or uncontrollable.



(a) For $\tau \in T_{hib}$: Low-level string-wise characterization of high-level event prohibitability

(b) For $\tau \in T_u$: Low-level string-wise characterization of high-level event uncontrollability

Fig. 3 Activity output-control consistency

Time, represented by tick t_h, is uncontrollably persistent in the high-level abstraction G_{hi} of an AOCC G_{lo}, and this fact is formalized in Proposition 3.

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

Proof Consider a TDES hierarchy (G_{lo}, G_{hi}), where G_{lo} is AOCC and $G_{hi} \overset{\text{def}}{=} (X, T, \xi, x_0, -)$. Then, for an arbitrary string $t \in L(G_{hi})$ and hence an arbitrary state $x = \xi(t, x_0) \in X$, we need to prove Property 4 for G_{hi}, i.e., $(T_{act}(x) \cap T_u = \emptyset) \implies \xi(t_h, x)!$, holds, as follows: Since $\theta(L(G_{lo})) = L(G_{hi})$, there must exist a string $s \in L_{voc}(G_{lo})$ such that $\theta(s) = t$. By Property 1 for G_{lo}, there exists some $\sigma \in \Sigma$ such that $s\sigma \in L(G_{lo})$. Furthermore, by Lemma 1, there must also exist a string $w \in \Sigma^+$, where $\sigma \leqslant w$, such that $sw \in L_{voc}(G_{lo})$ and is some τ-string of $L(G_{lo})$, where $\tau \in T$ and string s is its reference prefix. It then follows that one such string $w = \sigma_1\sigma_2 \cdots \sigma_k$ exists that is uncontrollable or ambiguously controllable, i.e., it contains only uncontrollable activity events or t_l's that are not unambiguously preemptable, found as follows:

Let $\sigma_0 = \varepsilon$. Then for each i, $(0 \leqslant i \leqslant k-1)$, if $\Sigma(\delta(s\sigma_0\sigma_1\sigma_2 \cdots \sigma_i, q_0)) \cap \Sigma_u \neq \emptyset$, select a $\sigma_{i+1} \in \Sigma_u$ such that $\sigma_{i+1} \in \Sigma(\delta(s\sigma_0\sigma_1\sigma_2 \cdots \sigma_i, q_0))$. Otherwise, select a $\sigma_{i+1} = t_l$ that is defined by Property 4 for G_{lo}, such that $\sigma_{i+1} \in \Sigma(\delta(s\sigma_0\sigma_1\sigma_2 \cdots \sigma_i, q_0))$.

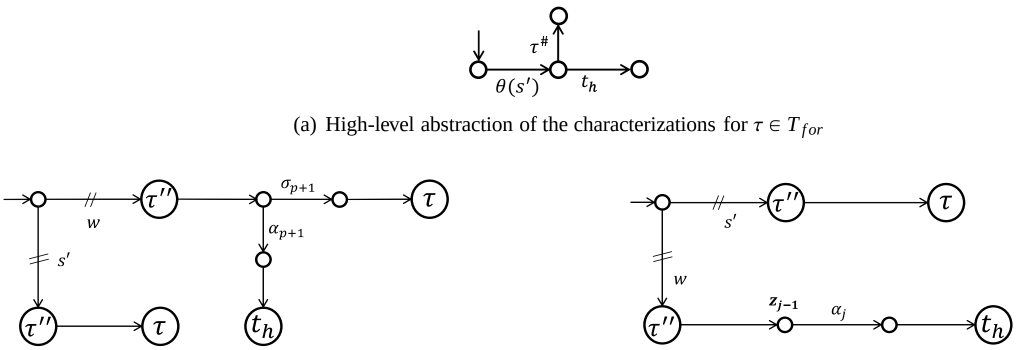
With $\theta(s\sigma_1\sigma_2 \cdots \sigma_k) = t\tau$, it is clear that $\xi(\tau, \xi(t, x_0))!$. Because G_{lo} is AOCC, by Definition 2, $\tau \notin T_{hib}$, since the co-silent string $w = \sigma_1\sigma_2 \cdots \sigma_k$ of the τ-string $sw \in L(G_{lo})$ is either uncontrollable, implying $\tau \in T_u$, or ambiguously controllable, implying $\tau = t_h$. Therefore, it can only be that $\tau \in T_u \cup \{t_h\}$. It thus follows that if $T_{act}(\xi(t, x_0)) \cap T_u = \emptyset$, then $\tau \notin T_u$, implying that $\tau = t_h$. Hence the proposition. □

4.2 Output-Force Consistency

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

Definition 3 (Preemptability of t_h by $\tau \in T_{act}$) Consider an arbitrary τ-string (6) of $L(G_{lo})$ with reference prefix $s' \in L(G_{lo})$ and $\tau \in T_{act}$. Then t_h is said to be unambiguously preemptable w.r.t (s', τ) if, for every t_h-string $< w, \alpha_j, z_j, h, t_h > \in L(G_{lo})$ such that $\theta(w) = \theta(s')$ and $w \in L(G_{lo})$ is the reference prefix of some τ-string (6) of $L(G_{lo})$, there exists a τ-string $< w, \sigma_i, x_i, k, \tau > \in L(G_{lo})$, with $\alpha_0\alpha_1 \cdots \alpha_p = \sigma_0\sigma_1 \cdots \sigma_p$ for some p $(0 \leqslant p < \min(h, k))$ where $\alpha_0 = \sigma_0 = \varepsilon$, and $z_n \notin \{x_i \mid (0 \leqslant i \leqslant k-1)\}$ for all n $(p < n < h)$, such that $\alpha_{p+1} \in \Sigma_{hib}$ or $(\alpha_{p+1} = t_l \;\&\; \sigma_{p+1} \in \Sigma_{for})$.

Consider an arbitrary nonempty string $r = \alpha_{p+1}\alpha_{p+2} \cdots \alpha_h$ that leads, from a state x_p lying along the transitions defined by the co-silent string $\sigma_1\sigma_2 \cdots \sigma_k$ of some τ-string of $L(G_{lo})$, $\tau \in T_{act}$, that exists, to a vocal state outputting t_h, via subsequent non-vocal states that are not lying along the transitions defined by the co-silent string. Then, in words, w.r.t the reference prefix s' of a τ-string of $L(G_{lo})$, t_h is unambiguously preemptable if every t_h-string of $L(G_{lo})$ with reference prefix w, such that $\theta(w) = \theta(s')$ and string w is also the reference prefix of some τ-string of $L(G_{lo})$, has such a string $\sigma_1\sigma_2 \cdots \sigma_p r$ if $0 < p < \min(h, k)$ and r if $p = 0$, as its suffix, with α_{p+1} in string r either a prohibitable event or a t_l which can be preempted by a forcible event σ_{p+1} that lies along the co-silent string of the τ-string that exists. This characterization is depicted in Fig. 4(b), and is for the high-level abstraction shown in Fig. 4(a).



(a) High-level abstraction of the characterizations for $\tau \in T_{for}$

(b) Preemptability of t_h by τ: $\theta(w) = \theta(s')$, and α_{p+1} is prohibitable, or α_{p+1} is t_l and σ_{p+1} is forcible.

(c) Preemptability of t_h by τ-mirage: $\theta(w) = \theta(s')$, and α_j is prohibitable, or α_j is t_l and there is a forcible and uncontrollable event at state z_{j-1}.

Fig. 4 Output-force consistency: Low-level string-wise characterizations of high-level event forcibility

Definition 4 (Preemptability of t_h by τ-mirage, $\tau \in T_{act}$) Consider an arbitrary τ-string (6) of $L(G_{lo})$ with reference prefix $s' \in L(G_{lo})$ and $\tau \in T_{act}$. Then t_h is said to be unambiguously preemptable w.r.t the mirage of (s', τ) if, for all $w \in L(G_{lo})$, $w = \varepsilon$ or $\delta(w, q_0) \in Q_{voc}$, if $\theta(w) = \theta(s')$ and $\tau' \neq \tau$ for every τ'-string (6) of $L(G_{lo})$ with reference prefix $w \in L(G_{lo})$ and $\tau' \in T_{act}$, then for every t_h-string $< w, \alpha_j, z_j, h, t_h > \in L(G_{lo})$, there exists some j $(1 \leqslant j \leqslant h)$ such that $\alpha_j \in \Sigma_{hib}$ or $(\alpha_j = t_l \;\&\; \Sigma(z_{j-1}) \cap \Sigma_{for} \cap \Sigma_u \neq \emptyset)$.

In words, consider an arbitrary τ-string of $L(G_{lo})$ with reference prefix s' and $\tau \in T_{act}$. Then t_h is unambiguously preemptable w.r.t the mirage of (s', τ) if, for every other string $w \in L_{voc}(G_{lo})$ that has the same θ-image as string s', but is not the reference prefix of any τ-string of $L(G_{lo})$, every t_h-string of $L(G_{lo})$ 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. This characterization is depicted in Fig. 4(c), and is for the high-level abstraction shown in Fig. 4(a).

Definition 5 (Output-force consistency) A TDES G_{lo} is said to be output-force consistent (OFC) if, for every τ-string (6) of $L(G_{lo})$ with reference prefix $s' \in L(G_{lo})$ and $\tau \in T_{act}$, for which there exists a t_h-string with reference prefix $w' \in L(G_{lo})$ such that $\theta(w') = \theta(s')$, $\tau \in T_{for}$ iff t_h is unambiguously preemptable w.r.t (s', τ) and its mirage.

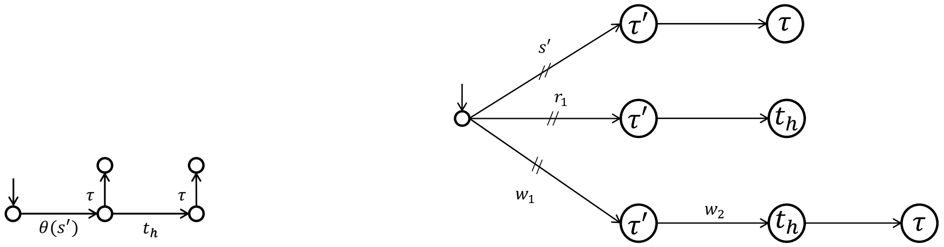
For an OFC G_{lo}, as depicted in Fig. 4, $\tau \in T_{for}$ if $\tau \in T_{act}$ can unambiguously preempt the tick t_h whenever the former is virtually enforced at a high-level state reached, where τ and t_h are eligible as depicted in Fig. 4(a). And any such high-level state is reached following an underlying vocal string that has the same θ-image as the reference prefix of an arbitrary τ-string of $L(G_{lo})$, and whose co-silent string is under the characterizations as depicted in Figs. 4(b) and 4(c). Otherwise, $\tau \in T_{act} - T_{for}$. Therefore, 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 (Brandin and Wonham, 1994), a high-level activity event is unambiguously forcible provided, when enforced, it can always preempt the time tick t_h.

4.3 Output Time-Compliance

Output time-compliance can be achieved by a proper design or redesign of the reporter map θ, and is formally defined as follows.

Definition 6 (Output time-compliance) A TDES G_{lo} is said to be output time-compliant (OTC) if, for every τ-string of $L(G_{lo})$ with reference prefix s' and $\tau \in T_{act}$, if there exists a t_h-string of $L(G_{lo})$ with reference prefix r_1 such that $\theta(s') = \theta(r_1)$, then there exists a τ-string of $L(G_{lo})$ with reference prefix r_2 such that $\theta(r_2) = \theta(r_1)t_h$.

For an OTC G_{lo}, same as the non-causal effect of the ticking of t_l on the eligibility of a low-level activity event in G_{lo}, the resultant ticking of t_h is never the cause of a high-level activity event becoming ineligible in G_{hi}. This non-causal effect is due to the defined characterization depicted in Fig. 5, and is made clear by Proposition 4.



(a) High-level abstraction of the characterization for $\tau \in T_{act}$ (b) Time-compliant $\tau \in T_{act}$: $\theta(s') = \theta(r_1)$, $r_2 = w_1w_2$, and $\theta(r_2) = \theta(r_1)t_h$.

Fig. 5 Output time-compliance: Low-level string-wise characterization for time invariance of event eligibility at the high level

Proposition 4 *Given a TDES hierarchy (G_{lo}, G_{hi}), G_{hi} obeys Property 3 iff G_{lo} is OTC.*

Proof Consider a TDES hierarchy (G_{lo}, G_{hi}), where $G_{hi} \overset{\text{def}}{=} (X, T, \xi, x_0, -)$. That G_{hi} obeys Property 3, i.e., for an arbitrary string $t \in L(G_{hi})$, and hence an arbitrary state $x = \xi(t, x_0) \in X$, if $x' = \xi(t_h, x) \in X$, then $T_{act}(x) \subseteq T_{act}(x')$, (equivalently) means that if $\tau \in T_{act}(\xi(t, x_0))$ and $t_h \in T(\xi(t, x_0))$, then $\tau \in T_{act}(\xi(tt_h, x_0))$, i.e., if $t\tau, tt_h \in L(G_{hi})$, where $\tau \in T_{act}$, then $tt_h\tau \in L(G_{hi})$. Since $\theta(L(G_{lo})) = L(G_{hi})$, there always exists an $s \in L(G_{lo})$ such that $\theta(s) = t$. Together, it means that for an arbitrary τ-string of $L(G_{lo})$ with reference prefix s', where $\theta(s') = t$, if there exists a t_h-string of $L(G_{lo})$ with reference prefix r_1 such that $\theta(r_1) = t$ and therefore $\theta(s') = \theta(r_1)$, then there exists a τ-string of $L(G_{lo})$ with reference prefix r_2 such that $\theta(r_2) = tt_h$ and therefore $\theta(r_2) = \theta(r_1)t_h$. By Definition 6, this means that G_{lo} is OTC. Hence the proposition. □

Proposition 5 *Given a TDES hierarchy (G_{lo}, G_{hi}) and that G_{lo} is AOCC and OTC, G_{hi} is a TDES model with time fidelity.*

Proof Given a TDES hierarchy (G_{lo}, G_{hi}), by Proposition 1, G_{hi} is activity-loop free. Since G_{lo} is AOCC, by Proposition 3, G_{hi} satisfies Property 4. And since G_{lo} is OTC, by Proposition 4, G_{hi} satisfies Property 3. Therefore, since G_{hi} is activity-loop free and satisfies Properties 3 and 4 of a TDES model, it is a TDES model with time fidelity. Hence the proposition. □

4.4 Timed Output-Control Consistency

Based on the concepts of activity output-control consistency, output-force consistency, and output time-compliance, the two concepts of output-control consistency may now be defined.

Definition 7 (Output-control consistency) A TDES G_{lo} is said to be output-control consistent (OCC) if it is AOCC and OFC; and timed OCC (TOCC) if it is OCC and OTC.

The foregoing theoretical development culminates in the following theorem.

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

Proof Consider a TDES hierarchy (G_{lo}, G_{hi}), where G_{lo} is TOCC. By Definition 7, a TOCC G_{lo} is necessarily AOCC and OTC. Hence the result by Proposition 5. □

Importantly, along with the unambiguous control properties of high-level activity events, the abstraction G_{hi} of a TOCC G_{lo} provides a real-time basis of generally coarser time granularity that is decoupled from the low level, for which high-level specification TTG's can be independently specified for feasible hierarchical control design.

5 Hierarchical Consistency: Theoretical Conditions

A core high-level supervisor expectation issue for timed hierarchical control design inherited from the untimed version (Zhong and Wonham, 1990) is explained, and two versions of hierarchical consistency for TDES's, without and with output-time fidelity guarantee, are then defined to address the issue. Before that, a conceptual computation tool is reviewed, and a timed concept of partner-freeness is subsequently introduced as the absence of vocal-state partners and illustrated using this tool, to complete the timed systems synthesis framework for hierarchical consistency.

5.1 Moore Reachability Tree for Conceptual Computation

Consider a Moore automaton (G_{lo}, V), where $G_{lo} = (Q, \Sigma, \delta, q_0, Q_m)$ is reachable. The (Moore) reachability tree (Wonham, 2016) generated for (G_{lo}, V) is the Moore automaton $(G_{lo,t}, V_t)$, of which:

- $G_{lo,t} = (Q_t, \Sigma, \delta_t, n_0, Q_{m,t})$, such that $L(G_{lo,t}) = L(G_{lo})$ and $L_m(G_{lo,t}) = L_m(G_{lo})$, where Q_t and $Q_{m,t}$ are called the infinite set of nodes and marked nodes, respectively, and each node is identified with a string $s \in L(G_{lo})$ by a bijection $node : L(G_{lo}) \to Q_t : s \mapsto node(s)$, such that the initial or root node $n_0 = node(\varepsilon)$, and, extended to Σ^*, $\delta_t(\varepsilon, n) = n$ where $n = node(s')$ for an $s' \in L(G_{lo})$, and $(\forall \sigma \in \Sigma)(\forall s \in \Sigma^*)\delta_t(s\sigma, n) = \delta_t(\sigma, \delta_t(s, n))$, and is defined as $node(s's\sigma)$ if $n' = \delta_t(s, n)!$ & $\delta_t(\sigma, n')!$.
- $V_t : Q_t \to T \cup \{\tau_o\}$ is the corresponding vocalization map, such that for an arbitrary $s \in L(G_{lo})$, $V_t(\delta_t(s, n_0)) = V(\delta(s, q_0))$.

Clearly, $L(G_{lo,t}) = L(G_{lo})$ and $L_m(G_{lo,t}) = L_m(G_{lo})$, and conceptually, translations between a Moore automaton and its Moore reachability tree can be made (Wonham, 2016). Corresponding with a state of G_{lo} under V, under V_t, a node of the Moore tree automaton (or simply tree) $G_{lo,t}$ is silent if it outputs τ_o, and vocal if it outputs a high-level event in T; and $Q_{voc,t} \subseteq Q_t$ denotes the vocal node set of $G_{lo,t}$. Note that every string of $L(G_{lo})$ can be uniquely identified by a node in the tree, and vice versa.

In what follows, the terminology, drawing notation and concepts formulated for states and state-transitions of G_{lo} carry over to nodes and node-transitions of the corresponding tree $G_{lo,t}$. It should be understood that, in referring to a τ-string $< s', \sigma_i, x_i, k, \tau > \in L(G_{lo,t})$, x_0 and x_i $(1 \leqslant i \leqslant k)$ are nodes defined by the transition function δ_t of $G_{lo,t}$ over the reference prefix s' and string $s'\sigma_1\sigma_2 \cdots \sigma_i$, respectively, and w.r.t the root node n_0.

5.2 Consistency for Hierarchical Control

Consider a two-level TDES hierarchy (G_{lo}, G_{hi}), where G_{lo} is OCC. Given a high-level specification $E \subseteq T^*$, the optimal high-level timed supervisor synthesized for its prefix closure $\overline{E}$ w.r.t G_{hi} is $S_{hi} = Supcon(\overline{G}_{hi}, \overline{E})$. Let $K = \theta^{-1}(L(S_{hi})) \subseteq L(G_{lo})$, the (low-level) maximal sublanguage of $L(G_{lo})$ whose projection under the timed reporter map θ is $L(S_{hi})$. In general, K is prefix-closed but not controllable w.r.t G_{lo}. Consider the low-level timed supervisor S_{lo} synthesized for K w.r.t G_{lo}, given by $S_{lo} = Supcon(\overline{G}_{lo}, K)$.Then since $L(S_{lo}) \subseteq \theta^{-1}L(S_{hi})$, it follows that in general,

$$\theta(L(S_{lo})) \subseteq L(S_{hi}). \tag{7}$$

Inclusion (7) asserts that the projection of the prefix-closed language generated by G_{lo} under the supervision of S_{lo} is a sublanguage of the prefix-closed language generated by G_{hi} under the high-level (virtual) supervision of S_{hi}. Indeed, (7) may turn out to be strict, in which case the low-level system G_{lo} under the supervision of S_{lo} cannot meet the expectation of high-level supervisor S_{hi}.

The basis for hierarchical control design for a two-level TDES hierarchy (G_{lo}, G_{hi}) requires the equality in (7), i.e., $\theta(L(S_{lo})) = L(S_{hi})$. In what follows, two concepts of hierarchical consistency are defined.

Definition 8 (Hierarchical consistency) A TDES hierarchy (G_{lo}, G_{hi}) is said to be

1. hierarchically consistent (HC) if, $(\forall E)(E \subseteq T^*)$

$$(S_{hi} = Supcon(\overline{G}_{hi}, \overline{E}))\&(S_{lo} = Supcon(\overline{G}_{lo}, \theta^{-1}(L(S_{hi})))), \theta(L(S_{lo})) = L(S_{hi});$$

2. and HC with output-time fidelity (HC-OTF) if, additionally, G_{hi} possesses high-level time fidelity.

5.3 Vocal-State Partnership & Strictness of Output-Control Consistency

That Inclusion (7) may be strict can be explained using the concept of vocal-state partnership for OCC DES's (Wonham, 2016) extended to OCC TDES's. Intuitively, if two vocal states of an OCC TDES are vocal-state partners, they output two different, eligible controllable outputs that cannot in general be independently controlled, in that, in taking a low-level control action necessary to disable or preempt one output, it is possible that this action also prevents the other output from occurring next. This partnership concept is formalized as follows.

Definition 9 (Control-dependent vocal states) For a TDES G_{lo}, let $q_1, q_2 \in Q_{voc}$, where either $V(q_1)$ or $V(q_2)$ is an event of T_{act}. Then (q_1, q_2) is said to be a pair of control-dependent vocal states over $[s', w\sigma s'', <^{s_1}_{s_2}, j]$, where $s', w, s'', s_1, s_2 \in \Sigma^*$ and $\sigma \in \Sigma$, if, for all $i \in \{1, 2\}$, there exists a $V(q_i)$-string of $L(G_{lo})$, with common reference prefix s' and co-silent string of the form $w_i = w\sigma s'' s_i$, with $q = \delta(s', q_0)$ and $q_i = \delta(w_i, q)$, such that the following three conditions hold:

CDS1) σ is not uncontrollable, i.e., $\sigma \in \Sigma_{hib}$ or $\sigma = t_l$ & $\Sigma(\delta(s'w, q_0)) \cap \Sigma_{for} \neq \emptyset$.
CDS2) $s'' \in (\Sigma_u \cup \{t_l\})^*$ and is uncontrollable, i.e., $\forall s_a \in \Sigma^*$, if $s_a t_l \leqslant s''$ then $\Sigma(\delta(s'w\sigma s_a, q_0)) \cap \Sigma_{for} = \emptyset$.
CDS3) $\exists j \in \{1, 2\}$ such that $s_j \in (\Sigma_u \cup \{t_l\})^+$ and is not controllable, i.e., $\forall s_b \in \Sigma^*$, if $s_b t_l \leqslant s_j$ then $\Sigma(\delta(s'w\sigma s'' s_b, q_0)) \cap \Sigma_{for} \cap \Sigma_u = \emptyset$.

Note that a pair (q_1, q_2) of states in G_{lo} may be control-dependent over several strings structures of the form $[s', w\sigma s'', <^{s_1}_{s_2}, j]$.

Definition 10 (Vocal-state partnership) For a TDES G_{lo}, let $q_1, q_2 \in Q_{voc}$, where either $V(q_1)$ or $V(q_2)$ is an event of T_{act}. Then (q_1, q_2) is said to be a pair of vocal-state partners if $V(q_1) \neq V(q_2)$ and (q_1, q_2) is a pair of control-dependent states.

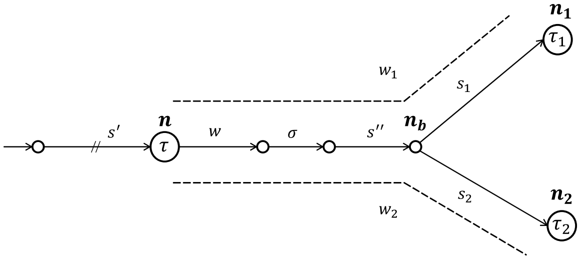


Fig. 6 Vocal-state partners q_1 and q_2 of a TDES G_{lo}: They are depicted respectively by nodes n_1 and n_2 in a subtree of the system reachability tree, with $V(q_1) = V_t(n_1) = \tau_1$ and $V(q_2) = V_t(n_2) = \tau_2$, where $\tau_1 \neq \tau_2$ and $\sigma \in \Sigma_{hib}$ or is a preemptable tick. Note that, each dotted line, for w_1 and w_2, indicates a catenation of strings between two vocal nodes.

Together with Definition 9, Definition 10 for a pair of arbitrary vocal-state partners q_1 and q_2 of a TDES (G_{lo}, V) is depicted in Fig. 6, respectively by nodes n_1 and n_2 in a subtree of the reachability tree generated for G_{lo}. As defined, this tree is also a Moore automaton, denoted by $(G_{lo,t}, V_t)$, with $G_{lo,t} \overset{\text{def}}{=} (Q_t, \Sigma, \delta_t, n_0, Q_{m,t})$ and vocal node set $Q_{voc,t} \subseteq Q_t$, except that its transition function is defined over an infinite set of elements called nodes instead of a finite set of states, with a different node representing a possibly duplicate state of G_{lo} reached by a different string of $L(G_{lo})$. As depicted, Condition CDS1 asserts that, along the string $w\sigma s''$ defining the transitions via non-vocal nodes from vocal node n of $G_{lo,t}$ corresponding to vocal state $q = \delta(s', q_0)$ of G_{lo}, the event σ is prohibitable, or is a tick t_l that is not non-preemptable. Condition CDS2 asserts that every event along the string s'' is uncontrollable, or is a non-preemptable tick. Condition CDS3 asserts that the string s_j for some $j \in \{1, 2\}$, defining the transitions from non-vocal node n_b corresponding to non-vocal state $\delta(w\sigma s'', q)$ of G_{lo}, via non-vocal nodes to the vocal node n_j that outputs $\tau_j \in T$, i.e., $V_t(n_j) = \tau_j = V(q_j)$, contains no prohibitable events and no unambiguously preemptable ticks. Therefore, along this string s_j, that τ_j cannot be prevented from occurring is definite only if no tick along the transitions defined by the string s_j is ambiguously preemptable.

For discussion's sake, let $j = 1$. Then under such vocal-state partnership of (q_1, q_2) as depicted by (n_1, n_2) in Fig. 6, if the TDES G_{lo} is OCC, then $\tau_i \in T_c$ for all $i \in \{1, 2\}$, and the low-level control action guaranteed to prevent τ_1 from occurring - by disabling or preempting an event along the transitions in G_{lo} defined by the string $w\sigma$ - will also prevent τ_2 from occurring. In other words, for an OCC G_{lo}, the control of τ_1 and τ_2 is generally not independent if the associated pair (q_1, q_2) are vocal-state partners.

It follows that, to guarantee independence of high-level control, it is sufficient for an OCC TDES G_{lo} to be free of vocal-state partners.

Definition 11 (Partner-freeness) A TDES G_{lo} is said to be partner-free (PF) if it does not contain vocal-state partners.

Two strict versions of output-control consistency follow.

Definition 12 (Strictness of output-control consistency) A TDES G_{lo} is said to be strictly OCC (SOCC) if it is OCC and PF. It is said to be strictly TOCC (STOCC) if it is SOCC and OTC, or equivalently, TOCC and PF.

5.4 Hierarchical Consistency Theorem

We are now ready to state the structural conditions for the consistency of a two-level TDES hierarchy.

Theorem 2 *A TDES hierarchy (G_{lo}, G_{hi}) is HC if G_{lo} is SOCC, and HC-OTF if G_{lo} is STOCC.*

Proof Given a TDES hierarchy (G_{lo}, G_{hi}), the proof for the two cases proceeds as follows.

Case 1: G_{lo} is SOCC. By Definition 12, G_{lo} is OCC and PF. For an arbitrary $E \subseteq T^*$, let $S_{hi} = Supcon(\overline{G}_{hi}, \overline{E})$ and $S_{lo} = Supcon(\overline{G}_{lo}, \theta^{-1}(L(S_{hi})))$. By Definition 8-1, to show that (G_{lo}, G_{hi}) is HC, we need to show that $\theta(L(S_{lo})) = L(S_{hi})$, as follows:

Suppose $L(S_{hi}) = \emptyset$. Then $L(S_{lo}) = \emptyset$ and trivially, $\theta(L(S_{lo})) = \theta(\emptyset) = \emptyset = L(S_{hi})$.

In the rest of the proof for this case, suppose $L(S_{hi}) \neq \emptyset$. Then $L(S_{lo}) \neq \emptyset$. Otherwise, $Supcon(\overline{G}_{lo}, \theta^{-1}(L(S_{hi}))) = EMPTY$. By Lemma 1 that $L(G_{lo}) = \overline{L_{voc}(G_{lo})}$ and the definition of θ^{-1}, for every $s'\sigma \in L(G_{lo})$ where $\sigma \in \Sigma$, $s' \in \theta^{-1}(L(S_{hi}))$ & $s'\sigma \notin \theta^{-1}(L(S_{hi})) \implies s'\sigma \in \overline{L}_{voc}(G_{lo})$. Therefore, that $Supcon(\overline{G}_{lo}, \theta^{-1}(L(S_{hi}))) = EMPTY$ implies $L(S_{hi}) \neq \emptyset \implies L(S_{hi}) \supset L(Supcon(\overline{G}_{hi}, L(S_{hi})))$. In turn, this means $L(S_{hi})$ is empty or not controllable, contradicting the supposition that $L(S_{hi})$ is nonempty and controllable.

By Inclusion (7), $\theta(L(S_{lo})) \subseteq L(S_{hi})$. It remains to show that $\theta(L(S_{lo})) \supseteq L(S_{hi})$. To do that, we now suppose $\theta(L(S_{lo})) \subset L(S_{hi})$ and show a contradiction of the fact that the given G_{lo} is PF, as follows:

Since $L(S_{hi}) - \theta(L(S_{lo})) \neq \emptyset$, let t be a string of $L(G_{hi})$ such that $t \in L(S_{hi}) - \theta(L(S_{lo}))$. Since $L(S_{lo}) \neq \emptyset$, $\varepsilon \in L(S_{lo})$ and hence $\varepsilon \in \theta(L(S_{lo}))$. Since $L(G_{hi})$ is prefix-closed and $\varepsilon \in \theta(L(S_{lo}))$, the longest prefix t' of t exists such that $t' < t$ and $t' \in \theta(L(S_{lo}))$. Let $s \in \theta^{-1}(t)$ and $\delta(s, q_0) \in Q_{voc} \cup \{q_0\}$. It follows that $s \notin L(S_{lo})$. Since $L(S_{lo}) \neq \emptyset$ and is prefix-closed, the longest prefix s' of s exists such that $s' \in L(S_{lo})$ and $\delta(s', q_0) \in Q_{voc} \cup \{q_0\}$. Let $t'' = \theta(s')$. Then $t'' \leqslant t'$ and therefore $t'' \in L(S_{hi})$. Let $w \in \Sigma^+$ such that $s'w \leqslant s$, $\delta(s'w, q_0) \in Q_{voc} \cup \{q_0\}$ and $\theta(s'w) = \theta(s')\tau_1$ for some $\tau_1 \in T$. Since $L(S_{lo})$ is controllable, $s' \in L(S_{lo})$ and $s'w \notin L(S_{lo})$, it follows that $(\exists w')(\exists \sigma \in \Sigma)w'\sigma \leqslant w$, $s'w' \in L(S_{lo})$ and $\sigma \in \Sigma_{hib}$ or $(\sigma = t_l)\&(\exists \gamma \in \Sigma_{for}, \delta(s'w'\gamma, q_0)!)s'w'\gamma \in L(S_{lo}))$. Otherwise, $w \in (\Sigma_u \cup t_l)^*$ and contains no unambiguously preemptable t_l, and is such that, due to the controllability of $L(S_{lo})$, every event of $\Sigma_{hib} \cap \Sigma_{for}$ that can preempt a t_l in w exits the boundary of $L(S_{lo})$, i.e., $(\forall w', w't_l \leqslant w)$ $s'w' \in L(S_{lo})$ and $(\forall \gamma \in \Sigma_{hib} \cap \Sigma_{for}, \delta(s'w'\gamma, q_0)!)s'w'\gamma \notin L(S_{lo}))$, and we have $s'w \in L(S_{lo})$, hence contradicting the maximality of s' w.r.t inclusion in $L(S_{lo})$. Thus $w \in (\Sigma^*)(\Sigma_{hib} \cup \{t_l\})(\Sigma_u \cup \{t_l\})^*$, such that the event of w in

$(\Sigma_{hib} \cup \{t_l\})$ is either prohibitable or a t_l that can be preempted by some forcible event that does not exit the boundary of $L(S_{lo})$, and every event of $\Sigma_{hib} \cap \Sigma_{for}$ that can preempt a t_l in its suffix string in $(\Sigma_u \cup \{t_l\})^*$ that contains no unambiguously preemptable t_l exits the boundary of $L(S_{lo})$. Now, let $w' \in \Sigma^*$ and $\sigma \in (\Sigma_{hib} \cup \{t_l\})$ be such that $s'w'\sigma \leqslant s'w$, $s'w' \in L(S_{lo})$ and $s'w'\sigma \notin L(S_{lo})$, i.e., σ must be disabled to stay in $L(S_{lo})$.

In what follows, there must exist a string $v \in (\Sigma_u \cup \{t_l\})^*$ that contains no unambiguously preemptable t_l, and where every event of $\Sigma_{hib} \cap \Sigma_{for}$ that can preempt a t_l in v exits the boundary of $L(S_{lo})$, such that $\delta(s'w'\sigma v, q_0) \in Q_{voc} \cup \{q_0\}$, $\theta(s'w'\sigma v) = \theta(s')\tau_2$ for some $\tau_2 \in T$ and $\theta(s'w'\sigma v) \notin L(S_{hi})$, because having no such string v contradicts the fact that $L(S_{lo})$ is the supremal controllable sublanguage of $\theta^{-1}(L(S_{hi}))$ w.r.t $\overline{G}_{lo}$.

Let $q_1 = \delta(s'w, q_0)$ and $q_2 = \delta(s'w'\sigma v, q_0)$ and. Thus $V(q_1) = \tau_1$ and $V(q_2) = \tau_2$. Since v extends from $s'w'\sigma$ and is not controllable in general, the longest common prefix string $s'w'' \in \Sigma^*$ of $s'w$ and $s'w'\sigma v$ exists such that $s'w''w_1 = s'w$ and $s'w''v_1 = s'w'\sigma v$ where $w_1, v_1 \in \Sigma^*$. It follows that $w'' = w'\sigma s_1$ for some $s_1 \in \Sigma^*$. Since v is not controllable, s_1 is not controllable. It follows that there must exist a string $s'' \in \Sigma^*$ that is the longest suffix of s_1 that is uncontrollable, i.e., $w'\sigma s_1 = w'\sigma s_2 s''$, where s_2 is not controllable (i.e., uncontrollable or ambiguously controllable). Therefore (q_1, q_2) is a pair of control-dependent vocal states over $[s', w'\sigma s_2 s'', <_{v_1}^{w_1}, -]$ since v_1 is not controllable because v is not controllable, and therefore satisfies Condition CDS3 of Definition 9; and

- if s_2 is uncontrollable, then σ satisfies Condition CDS1 and string $s_2 s''$ satisfies Condition CDS2, of Definition 9; and
- if s_2 is ambiguously controllable and thus is of the form $s_1'\sigma' s_2''$ for some $s_1', s_2'' \in (\Sigma_u \cup \{t_l\})^*$, where s_2'' is uncontrollable and $\sigma' = t_l$ is ambiguously preemptable, then event σ' satisfies Condition CDS1, and string $s_2'' s''$ satisfies Condition CDS2, of Definition 9.

Since $\theta(s'w) = t''\tau_1 \in L(S_{hi})$ and $\theta(s'w'\sigma v) = t''\tau_2 \notin L(S_{hi})$, it follows that $\tau_1 \neq \tau_2$ and therefore $V(q_1) \neq V(q_2)$. Together with the fact that (q_1, q_2) is a pair of control-dependent vocal states, (q_1, q_2) is a pair of vocal-state partners by Definition 10, contradicting the fact that the given G_{lo} is PF.

Case 2: G_{lo} is STOCC. Then, by Definition 12, it is necessary that that G_{lo} is SOCC, and therefore by the proof of Case 1 above, (G_{lo}, G_{hi}) is HC. It also necessary that G_{lo} is TOCC, and therefore by Theorem 1, G_{hi} possesses high-level time fidelity. Combining, it follows that (G_{lo}, G_{hi}) is HC-OTF by Definition 8-2.

Hence the theorem. □

5.5 Hierarchical Mission Control of a Robotic Camera System

As an illustration of the STOCC system concept for building a hierarchy that is HC-OTF, we now present an example of a simplified robotic camera system. One may think of it as a module on board a drone or an unmanned aerial vehicle, for use in a surveillance mission along a designated flying route. This module is to be organized as a hierarchy (G_{lo}, G_{hi}), constructed from a given TDES (G, θ) that is represented by a Moore ATG G_{act} and the associated event timing information as shown in Fig. 7, with $\theta : L(G) \to T^*$ and $T_{act} = \{\tau_1, \tau_2\}$, under a periodic timescale $1 : 2$. The event set $\Sigma_{act} = \{\sigma_1, \sigma_2, \sigma_3\}$ of G is partitioned with $\Sigma_{hib} = \{\sigma_1, \sigma_3\}$ and $\Sigma_{for} = \{\sigma_3\}$. The definitions of the activities and events are given in Table 1.

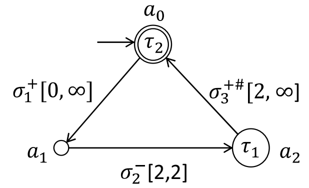


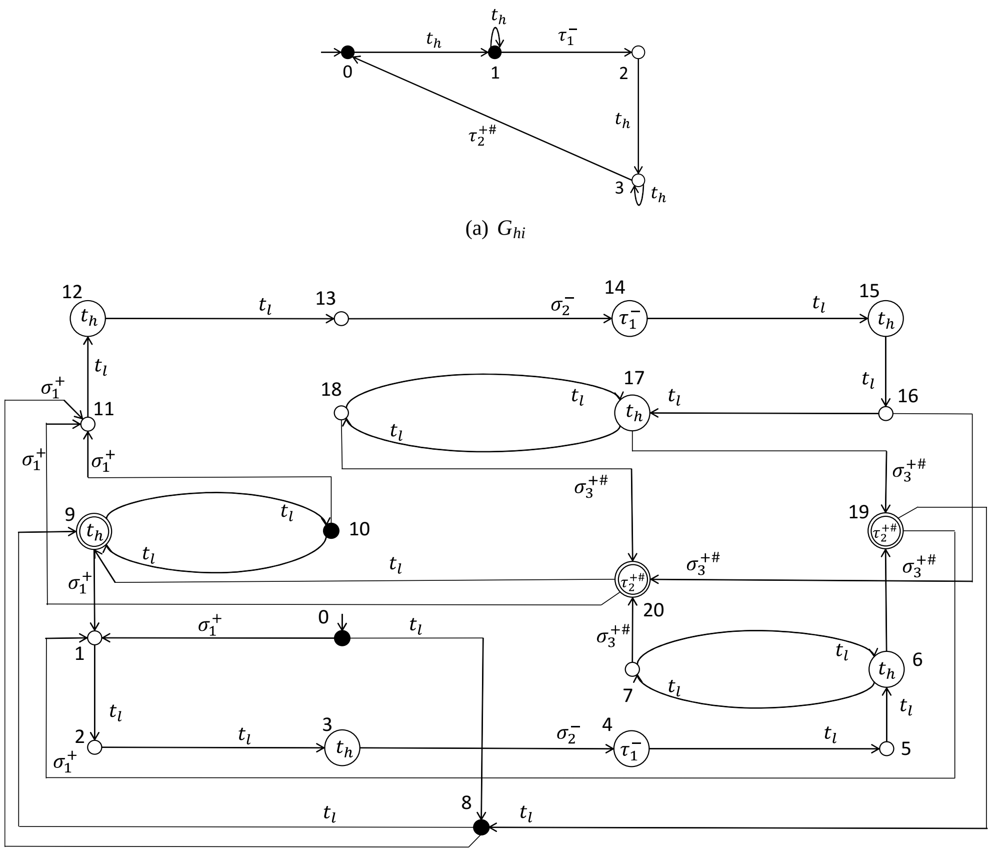
Fig. 7 Camera system: Moore ATG model and associated event timings

Following the construction as shown in Fig. 8, it can be verified that G_{lo} is:

- OCC, by setting $T_{hib} = \{\tau_2\}$ and $T_u = \{\tau_1\}$; $T_{for} = \{\tau_2\}$ and $\tau_1 \notin T_{for}$.
- PF, due to the absence of a partnership structure as depicted in Fig. 6, by determining that for all state pairs (q_1, q_2) with $V(q_1), V(q_2) \in T$, every pair of $V(q_1)$-string and $V(q_2)$-string with common reference prefix and co-silent strings with common prefix s, has either $V(q_1) = V(q_2) = t_h$ or $s = \varepsilon$.

Table 1 Symbol definitions for a robotic camera system hierarchy (G_{lo}, G_{hi})

Models	Event	Activity
G_{lo}	σ_1: Detected new object localized σ_2: Camera set σ_3: Camera clicked	a_0: Scanning and detecting new suspicious moving or stationary object of interest a_1: Setting camera shutter speed and aperture based on scene lighting a_2: Improving camera setting and zooming in on localized object
G_{hi}	τ_1: New object seen τ_2: Photo taken	



(a) G_{hi}

(b) G_{lo}

Fig. 8 Camera system: A constructed hierarchy (G_{lo}, G_{hi})

– OTC, by observing that G_{hi} obeys Property 3 and following Proposition 4.

Therefore, in the constructed hierarchy (G_{lo}, G_{hi}), G_{lo} is STOCC by Definition 12, and hence the hierarchy is HC-OTF by Theorem 2.

A system abstraction is very useful if it can abstract away unnecessary low-level language details and provide unambiguous control information of interest abstracted as languages of high-level events. As this example hierarchy shows, the abstraction G_{hi} provides a clear understanding of the application mission-level driven by the underlying real TDES G_{lo}, and allows real-time requirements to be more readily identified and specified at the high level.

As a specification example over G_{hi}, consider a controllable specification asserting that, continually, the robotic camera, upon seeing a new object, is to take a photo with no further t_h-time delay as soon as it is ready to do so (following a t_h-setup[5]). This specification may be prescribed by a TTG (say, MC) that structurally is G_{hi} (see Fig. 8(a)), but with the self-loop t_h-transition at state 3 removed. A low-level supervisor S_{lo} for the TDES G_{lo} can be synthesized for which $\theta(L(S_{lo})) = L(MC)$.

In driving home the point, a hierarchy that is HC-OTF is necessary if we need to synthesize low-level supervisor solutions that fully realize the prefix closure of controllable, high-level real-time specifications w.r.t the high-level TDES model, without violating their intended high-level timing semantics.

6 Hierarchical Consistency: Output-System Synthesis

In general, a Moore TDES (G_{lo}, V) constructed from given hierarchical system information (G, θ) is not STOCC. Refining it to be so by modifying the associated map V for G_{lo} turns out to be a challenging research problem. Herewith, we first investigate the structural existence and synthesis (or refinability) issues for SOCC systems, and point out the abstraction anomalies to be removed for obtaining STOCC systems. Along with it, the conditions under which timescale is preserved under a system refinement are also of interest. In essence, these conditions are the system structural conditions under which a refinement does not introduce a new t_h-string for the refined TDES. Details of this aspect of our investigation are found elsewhere (Ngo, 2016).

By system refinement or synthesis, we refer to redefining the map V over G_{lo}, *without removing any given high-level activity and timing information*. It can be easily deduced that a TDES G_{lo} refined as such remains time-output responsive (in the sense of not invalidating the time-output design Laws 1 and 2). Therefore, the system concepts and their constituent relationships defined for a given TDES G_{lo} are also applicable to a refined TDES, and so are the definitions and results presented in Sections 3 through 5. Where required, a refined TDES will be referred to by the same symbol, G_{lo}, to imply that it remains time-output responsive as the given TDES G_{lo}, in all the theoretical proofs of subsequent synthesis results.

For clarity of description, every system refinement (procedure or method) will be defined, and thought of, as being ‘implemented’ in terms of refinement of the Moore reachability tree introduced in Section 5.1, i.e., redefining the map V over G_{lo} is made by redefining the corresponding V_t over its tree $G_{lo,t}$. The system refinement is therefore conceptual.[6]

6.1 String-wise Control Partitions of Outputs

At this juncture, it is useful to bring in some string-wise definitions for the event-control properties of $\tau \in T$, as follows. Given an arbitrary τ-string $s = < s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$:

- $\tau \in T$ is said to be controllable w.r.t s if the co-silent string of s is controllable, i.e., for some i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_{hib}$ or $(\sigma_i = t_l \; \& \; \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_u \neq \emptyset)$.
- $\tau \in T$ is said to be uncontrollable w.r.t s if the co-silent string of s is uncontrollable, i.e., for all i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \; \& \; \Sigma(x_{i-1}) \cap \Sigma_{for} = \emptyset)$.
- $\tau \in T$ is said to be ambiguously controllable w.r.t s if the co-silent string of s is ambiguously controllable, i.e., for all i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \; \& \; \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_u = \emptyset)$, and for some i $(1 \leqslant i \leqslant k)$, $\sigma_i = t_l \; \& \; \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_{hib} \neq \emptyset$.
- $\tau \in T_{act}$ is said to be forcible w.r.t s' if t_h is unambiguously preemptable w.r.t (s', τ) and its mirage, and is not forcible w.r.t s' otherwise, in either case that there exists a t_h-string with reference prefix $s'' \in L(G_{lo})$ such that $\theta(s'') = \theta(s')$, or else it is said to be force-don’t-care w.r.t s'.

In the above, all the definitions except the last are for events in $T = T_{act} \dot\cup \{t_h\}$. A $\tau \in T_{act}$ that is force-don’t-care w.r.t the reference prefix s' of a given τ-string is said to be definable as either forcible or not forcible w.r.t s'. It follows that the definitions induce two string-wise control partitions of Moore outputs. In one partition, an arbitrary $\tau \in T$ is either controllable, uncontrollable or ambiguously controllable w.r.t to every of its τ-strings, and in the other, an arbitrary $\tau \in T_{act}$ is either forcible or non-forcible w.r.t to the reference prefix of every of its τ-strings.

[5] Examining G_{lo} for the curious reader, this high-level tick models the minimum time required by the underlying system for auto-adjusting the setting of the camera shutter speed and aperture to anticipate a clear photo finish.

[6] In principle, in place of reachability trees, more efficient and compact representations are available for practical implementation that can be stored (Wonham, 2016; Zhong and Wonham, 1989).

6.2 OCC-System Refinability & Refinement

In what follows, a TDES is said to be AOCC-, OFC-, and OCC-system refinable, if it can be refined to be AOCC, OFC, and OCC, respectively.

Theorem 3 *A TDES G_{lo} is not AOCC-system refinable iff there exists a τ-string $< s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$, such that*

- *$\sigma_1 \cdots \sigma_{k-1}$ is not controllable, i.e., for all i $(1 \leqslant i \leqslant k-1)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \ \& \ \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_u = \varnothing)$, and*
- *σ_k is ambiguously controllable, i.e., $\sigma_k = t_l$ and is ambiguously preemptable.*

Proof *(If)*: Suppose there exists a τ-string $s = < s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$, such that

- for all i $(1 \leqslant i \leqslant k-1)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \ \& \ \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_u = \varnothing)$, and
- $\sigma_k = t_l$ and is ambiguously preemptable.

Then, the τ-string $s \in L(G_{lo})$ does not satisfy any of the respective condition for $\tau \in T_{hib}$ and $\tau \in T_u$ stated in Definition 2, and it follows that G_{lo} is not AOCC. Regardless of any Moore transition redefinition along the co-silent string $\sigma_1\sigma_2 \cdots \sigma_{k-1}$ of s, that $\sigma_k = t_l$ is ambiguously preemptable remains, and hence there will always exist a τ-string of $L(G_{lo})$, with reference prefix $s'\sigma_1 \cdots \sigma_i$ for some i $(1 \leqslant i \leqslant k-1)$, for the refined G_{lo} that does not satisfy any of the respective condition for $\tau \in T_{hib}$ and $\tau \in T_u$ stated in Definition 2, implying that the refined G_{lo} is not AOCC. Hence, the given G_{lo} is not AOCC-system refinable.

(Only if): Suppose G_{lo} is not AOCC-system refinable, and is therefore not AOCC. Together, they mean that there exists a τ-string $s = < s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$, that

- does not satisfy any of the respective condition for $\tau \in T_{hib}$ and $\tau \in T_u$ stated in Definition 2 and thus
  - for all i $(1 \leqslant i \leqslant k)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \ \& \ \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_u = \varnothing)$, and
  - for some i $(1 \leqslant i \leqslant k)$, $(\sigma_i = t_l \ \& \ \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_{hib} \neq \varnothing)$,
- and no Moore transition redefinition along its co-silent string $\sigma_1\sigma_2 \cdots \sigma_{k-1}$ can be made to satisfy the condition for $\tau \in T_u$ as stated in Definition 2, implying the additional condition that $\sigma_k = t_l \ \& \ \Sigma(x_{k-1}) \cap \Sigma_{for} \cap \Sigma_{hib} \neq \varnothing$.

In other words, if G_{lo} is not AOCC-system refinable, by logical conjunction, there exists a τ-string $s = < s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$ such that

- for all i $(1 \leqslant i \leqslant k-1)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \ \& \ \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_u = \varnothing)$, and
- $\sigma_k = t_l$ and $(\Sigma(x_{k-1}) \cap \Sigma_{for} \cap \Sigma_u = \varnothing)$ & $(\Sigma(x_{k-1}) \cap \Sigma_{for} \cap \Sigma_{hib} \neq \varnothing)$, i.e., is ambiguously preemptable.

Hence the theorem. □

Noting that, by definition, $\sigma \in \Sigma$ is not ambiguously controllable if $\sigma \in \Sigma_{act}$, or $\sigma = t_l$ and is non-preemptable or unambiguously preemptable, a logically straightforward corollary of Theorem 3 follows.

Corollary 1 *A TDES G_{lo} is AOCC-system refinable iff, for every τ-string $< s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$, the following condition holds: If $\sigma_1 \cdots \sigma_{k-1}$ is not controllable, then σ_k is not ambiguously controllable.*

We now present a conceptual procedure named Procedure **OCC-SR** for a TDES (G_{lo}, V). We then show, by the proof of Theorem 4 below, that Procedure **OCC-SR** can be applied for OCC-system refinement of an AOCC-system refinable TDES (G_{lo}, V).

The procedure is defined over the reachability tree $(G_{lo,t}, V_t)$, as follows: With $T_{act} = \{\tau_n \mid 1 \leqslant n \leqslant \kappa\}$, of set cardinality $|T_{act}| = \kappa$:

Step 1) Let $\{\alpha_n \mid 1 \leqslant n \leqslant \kappa\}$, $\{\beta_n \mid 1 \leqslant n \leqslant \kappa\}$ be the sets of new high-level outputs, where $\{\alpha_n\} \cap T_{act} = \varnothing$ and $\{\beta_n\} \cap T_{act} = \varnothing$ initially, and $\{\alpha_n\} \cap \{\beta_n\} = \varnothing$. For all n $(1 \leqslant n \leqslant \kappa)$ and for every τ_n-string $s = < s', \sigma_i, x_i, k, \tau_n >$ of $L(G_{lo,t})$, if τ_n is controllable w.r.t s, redefine $V_t(\delta_t(s, n_0)) = \alpha_n$; if τ_n is uncontrollable w.r.t s, redefine $V_t(\delta_t(s, n_0)) = \beta_n$; and if τ_n is ambiguously controllable w.r.t s, for some i $(1 \leqslant i \leqslant k-1)$ such that $\sigma_i = t_l \ \& \ \Sigma(x_{i-1}) \cap \Sigma_{for} \cap \Sigma_{hib} \neq \varnothing$, and for all j $(i < j \leqslant k)$, $\sigma_j \in \Sigma_u$ or $(\sigma_j = t_l \ \& \ \Sigma(x_{j-1}) \cap \Sigma_{for} = \varnothing)$, redefine $V_t(\delta_t(s'\sigma_1 \cdots \sigma_i, n_0)) = t_h$, and redefine $V_t(\delta_t(s, n_0)) = \beta_n$. By refining $(G_{lo,t}, V_t)$ as such, each original $\tau_n \in T_{act}$ is replaced by α_n or β_n accordingly, such that the modified set $T_{act} \subseteq \{\alpha_n, \beta_n\}$.

Step 2) Let $\{\overline{\alpha_n} \mid 1 \leqslant n \leqslant \kappa\}$, $\{\overline{\beta_n} \mid 1 \leqslant n \leqslant \kappa\}$ be the sets of new high-level outputs, where $\{\overline{\alpha_n}\} \cap T_{act} = \varnothing$ and $\{\overline{\beta_n}\} \cap T_{act} = \varnothing$ initially, and $\{\overline{\alpha_n}\} \cap \{\overline{\beta_n}\} = \varnothing$, $\{\overline{\alpha_n}\} \cap \{\alpha_n\} = \varnothing$ and $\{\overline{\beta_n}\} \cap \{\beta_n\} = \varnothing$. For each $\gamma \in \{\alpha_n, \beta_n\} \cap T_{act}$ and for every γ-string of $L(G_{lo,t})$ with reference prefix s', if γ is not forcible w.r.t s', then for every γ-string s of $L(G_{lo,t})$ with reference prefix w such that $\theta(w) = \theta(s')$, redefine $V_t(\delta_t(s, n_0)) = \overline{\gamma}$; and if γ is force-don't-care w.r.t s', then for every γ-string s of $L(G_{lo,t})$ with reference prefix w such that $\theta(w) = \theta(s')$, redefine $V_t(\delta_t(s, n_0)) = \overset{x}{\gamma} \in \{\overline{\gamma}, \gamma\}$[7]. By further refining $(G_{lo,t}, V_t)$ as such, each $\alpha_n \in T_{act}$ is further replaced by either α_n or $\overline{\alpha_n}$, each $\beta_n \in T_{act}$ is further replaced by either β_n or $\overline{\beta_n}$, such that the further modified set $T_{act} \subseteq \{\alpha_n, \beta_n, \overline{\alpha_n}, \overline{\beta_n}\}$.

Following the procedure, $T_{hib} = \{\alpha_n, \overline{\alpha_n}\} \cap T_{act}$; $T_u = \{\beta_n, \overline{\beta_n}\} \cap T_{act}$; and $T_{for} = \{\alpha_n, \beta_n\} \cap T_{act}$. In the maximal case, each enumerated τ_n $(1 \leqslant n \leqslant \kappa)$ is replaced by four distinct outputs α_n, $\overline{\alpha_n}$, β_n and $\overline{\beta_n}$, and the maximal cardinality of the new T_{act} is 4κ.

Theorem 4 *A TDES G_{lo} is AOCC-system refinable iff it is OCC-system refinable.*

Proof (If): Suppose a given TDES G_{lo} is OCC-system refinable. Then G_{lo} can be refined to be OCC, and hence AOCC and OFC by Definition 7. That the TDES G_{lo} can be refined to be AOCC implies it is AOCC-system refinable.

(Only if): Suppose a given TDES G_{lo} is AOCC-system refinable. It is sufficient to show that using Procedure **OCC-SR**, it can be refined to be AOCC, and then OFC without violating the established AOCC-system property, and hence OCC by Definition 7. The necessity proof proceeds as follows:

- Show that the given TDES G_{lo} can be refined to be AOCC:
  An arbitrary $\tau_n \in T_{act}$ is, in general, either ambiguously controllable, controllable or uncontrollable w.r.t every τ_n-string of $L(G_{lo})$. By Corollary 1, for every τ-string $< s', \sigma_i, -, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$, the prefix $\sigma_i \cdots \sigma_{k-1}$ of its co-silent string is either controllable or ambiguously controllable, and its terminal event $\sigma_k \in \Sigma$ is, string-wise, either controllable or uncontrollable. Hence every τ_n-string $s = < s', \sigma_i, -, k, \tau_n >$ of $L(G_{lo})$, w.r.t which $\tau_n \in T_{act}$ is ambiguously controllable, has the longest prefix $s'\sigma_1 \cdots \sigma_p$ for some p $(1 \leqslant p \leqslant k-1)$ - at which $\sigma_p = t_l$ and is ambiguously preemptable, and beyond which the suffix $\sigma_{p+1} \cdots \sigma_k$ is uncontrollable. With the new event output notation accordingly defined, and over the reachability tree constructed for G_{lo}, Step 1 of Procedure **OCC-SR** labels such a prefix as a t_h-string and such a τ_n-string s as a β_n-string, of $L(G_{lo})$, with the new t_h-string $s'\sigma_1 \cdots \sigma_p$ as its reference prefix; and as a result, the new β_n-string s now satisfies the condition for an activity event in T_u as stated in Definition 2 (of activity output-control consistency).

  The step also relabels every other τ_n-string $s \in L(G_{lo})$, w.r.t which $\tau_n \in T_{act}$ is controllable or uncontrollable, as an α_n-string or a β_n-string, of $L(G_{lo})$, respectively, and as a result, the new α_n- or β_n-string s now satisfies the condition for an activity event in T_{hib} or T_u, respectively, as stated in Definition 2.

  It thus follows that Step 1 of Procedure **OCC-SR** refines the given TDES G_{lo} to be AOCC according to Definition 2, with the new set of high-level activity outputs $T_{act} \subseteq \{\alpha_n, \beta_n\}$ partitioned into $T_{hib} = \{\alpha_n\} \cap T_{act}$ and $T_u = \{\beta_n\} \cap T_{act}$.
- Show that the AOCC-system refined G_{lo} can be further refined to be OFC without violating the established AOCC-system property:
  With additional new event output notation accordingly defined, and over the reachability tree of the now AOCC-system G_{lo}, Step 2 of Procedure **OCC-SR** relabels α_n-strings and β_n-strings as $\overline{\alpha_n}$- and $\overline{\beta_n}$-strings, of $L(G_{lo})$, accordingly as needed, such that the refined G_{lo} becomes OFC according to Definition 5. As the step entails only output relabeling, it thus follows that every newly formed $\overline{\alpha_n}$- or $\overline{\beta_n}$-string of $L(G_{lo})$, like their α_n- or β_n-string counterpart, retains satisfying the condition for an activity event in T_{hib} or T_u, respectively, as stated in Definition 2.

  It thus follows that Step 2 of Procedure **OCC-SR** refines the TDES G_{lo} to be OFC without violating the AOCC-system property established by Step 1, and hence the refined G_{lo} is OCC according to Definition 7, with $T_{act} \subseteq \{\alpha_n, \beta_n, \overline{\alpha_n}, \overline{\beta_n}\}$ partitioned into $T_{hib} = \{\alpha_n, \overline{\alpha_n}\} \cap T_{act}$ and $T_u = \{\beta_n, \overline{\beta_n}\} \cap T_{act}$; and partitioned with $T_{for} = \{\alpha_n, \beta_n\} \cap T_{act}$.

Hence the theorem. □

In subsequent references, Steps 1 and 2 of Procedure **OCC-SR** may be separately referred to as Subprocedures **AOCC-SR** and **OFC-SR**, respectively. Henceforth, when we say a TDES is OCC-, AOCC-, and OFC-system refinable, we now mean, more specifically, that it can be refined to be OCC, AOCC and OFC, using Procedure **OCC-SR** and Subprocedures **AOCC-SR** and **OFC-SR**, respectively.

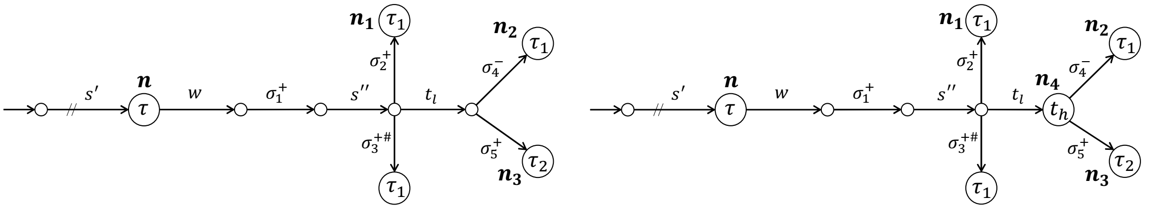
[7] An event denoted by symbol $\overset{x}{\gamma}$ is simply called a force-don't-care event, and is either $\overline{\gamma}$ or γ.

6.3 PF-System Refinement & SOCC-System Refinability

Relating as explained in Section 5.1, the terminology and concepts formulated for state pairs of G_{lo} carry over to node pairs of the corresponding tree $G_{lo,t}$.

In logical hierarchical control, a method over the system's Moore reachability tree is developed (Zhong and Wonham, 1990; Wonham, 2016) to break up vocal-node partners, by first finding them via breadth-first search of the tree. To refine a TDES (G_{lo}, V) so that it becomes free of vocal-state partners, however, it is discovered that, in finding vocal-node partners over $[s', w\sigma s'', <^{s_1}_{s_2}, j]$, similarly by breadth-first search of the tree $(G_{lo,t}, V_t)$, and breaking them up, new vocal-node partners may be introduced. This is because in breaking them up, the map V_t needs to be redefined so that the node $\delta_t(s'w\sigma, n_0)$ outputs t_h if $\sigma \in \Sigma(\delta_t(s'w, n_0))$ is an ambiguously preemptable tick, and otherwise, as in the partners-breakup method for logical hierarchical control (Zhong and Wonham, 1990; Wonham, 2016), outputs a given new activity event. The following example illustrates this issue.

Example 2 Consider a subtree of the reachability tree $(G_{lo,t}, V_t)$ for a Moore TDES G_{lo}, as depicted in Fig. 9(a) with $s' \in L_{voc}(G_{lo,t})$, $w, s'' \in \Sigma^*$, $\sigma_i \in \Sigma_{act}$ for all i $(1 \leqslant i \leqslant 5)$, and $\tau_1, \tau_2 \in T_{act}$. Suppose $\sigma_1, \sigma_2, \sigma_3$ and σ_5 are prohibitable, σ_4 is uncontrollable and σ_3 is also forcible.



(a) Partners (n_2, n_3)

(b) Partners (n_2, n_3) removed with new partners (n_1, n_4) introduced

Fig. 9 An example showing that partnership removal can introduce new partnership

The subtree, according to Definition 10, has a pair of vocal-node partners, namely, (n_2, n_3). To remove their partnership, V_t can be redefined such that the non-vocal node n_4 (reachable by string $s'w\sigma_1 s'' t_l$) becomes a vocal node outputting t_h, as depicted in Fig. 9(b). However, in so doing, a new pair of vocal-node partners is introduced, namely, (n_1, n_4), as depicted in Fig. 9(b). ■

In general, the issue is due to vocal-state partners being 'hidden' by certain pairs of control-dependent vocal states outputting the same activity event, formalized as follows.

Definition 13 (Hidden vocal-state partnership) For a TDES G_{lo}, let $q_1, q_2 \in Q_{voc}$, where either $V(q_1)$ or $V(q_2)$ is an event of T_{act}. Then (q_1, q_2) is said to be a pair of partner-hiding states if $V(q_1) = V(q_2) \in T_{act}$ and (q_1, q_2) is a pair of control-dependent states over $[s', w\sigma s'', <^{s_1}_{s_2}, j]$, for which $(\exists s_c \in \Sigma^*)(s_c t_l < s_j \;\&\; \Sigma(\delta(s'w\sigma s'' s_c, q_0)) \cap \Sigma_{for} \cap \Sigma_{hib} \neq \varnothing)$.

In words, two system vocal states q_1 and q_2 outputting the same activity event are partner-hiding if they are control dependent over $[s', w\sigma s'', <^{s_1}_{s_2}, j]$ in the system, such that an ambiguously preemptable tick exists at $q'_j = \delta(s'w\sigma s'' s_c, q_0)$ along some $s_c \in \Sigma^*$ for which $s_c t_l < s_j$, for which q_i and q'_j, $i \in \{1, 2\}$ and $i \neq j$, are vocal-state partners if q'_j were to output t_h.

To break up partners without introducing new partners, using breadth-first search strategy, conservatively, pairs of vocal-state partners and partner-hiding states need to be broken up. In what follows, a conceptual procedure for PF-system refinement, named Procedure **PF-SR**, is defined over the reachability tree $(G_{lo,t}, V_t)$ of a TDES (G_{lo}, V), as follows: For each pair (n_1, n_2) of vocal-node partners or partner-hiding nodes over $[s', w\sigma s'', <^{s_1}_{s_2}, j]$ in $G_{lo,t}$, detected with $s'w\sigma \in L(G_{lo,t})$ found by breadth-first search of the tree $G_{lo,t}$ starting from its root node, it is the case that

1. if $\sigma \in \Sigma(\delta_t(s'w, n_0))$ is ambiguously controllable, i.e., $\sigma = t_l$ and is ambiguously preemptable, then redefine $V_t(\delta_t(s'w\sigma, n_0)) = t_h$;
2. else redefine $V_t(\delta_t(s'w\sigma, n_0)) = \tau_p$, where $\tau_p \notin T$ is the given new activity event.

Definition 14 (Partner-hiding-state freeness) A TDES G_{lo} is said to be partner-hiding-state free (PHF) if it does not contain partner-hiding (vocal) states.

Therefore, by Definitions 11 and 14, Procedure **PF-SR** refines a TDES G_{lo} into a system that is not only PF, but also PHF.

Henceforth, a TDES is said to be SOCC-system refinable if it can be refined to be SOCC using the (ordered) application of Procedure **PF-SR** followed by Procedure **OCC-SR**, or either one of these two procedures.

6.4 SOCC-System Synthesis Theorems

Theorem 5 *A TDES G_{lo} is SOCC-system refinable if it is AOCC-system refinable and, over each $[s', w\sigma s'', <^{s_1}_{s_2}, j]$ of every pair (q_1, q_2) of vocal-state partners or partner-hiding states, it is the case that for $i, j, k \in \{1, 2\}$, $i \neq j$, and $s_k = s'_k\alpha_k$ where $\alpha_k \in \Sigma$,*

- *if $V(q_i) \neq t_h$ and s'_i is not controllable, then α_i is preemption-unambiguous;*
- *if $V(q_j) \neq t_h$, then α_j is uncontrollable.*

Proof Consider an AOCC-system refinable TDES G_{lo} with the structural conditions as specified. It is sufficient to show that, by applying Procedure **PF-SR** followed by Procedure **OCC-SR**, the given TDES G_{lo} can be refined to be PF without violating AOCC-system refinability and then further refined to be OCC without violating the established PF-system property, and hence SOCC by Definition 12. The proof proceeds as follows:

- Show that the given TDES G_{lo} can be refined to be PF without violating AOCC-system refinability:
  For each structure $[s', w\sigma s'', <^{s_1}_{s_2}, j]$ of every pair (q_1, q_2) of vocal-state partners (Definition 10) or partner-hiding states (Definition 13), both of which are control-dependent vocal states (Definition 9) in G_{lo}, Procedure **PF-SR**, in computing over the Moore reachability tree constructed for (G_{lo}, V), labels string $s'w\sigma$ as a τ_p-string where τ_p is a new high-level activity output, only if in the co-silent string $w\sigma$ of the new τ_p-string, either $\sigma \in \Sigma_{hib}$ or $\sigma = t_l$ and is unambiguously preemptable. Therefore, the new τ_p-string with reference prefix s' satisfies the condition for AOCC-system refinability (required by each τ-string of $L(G_{lo})$ for every high-level activity event τ), as stated in Corollary 1.

  Next, let $s_j = s'_j\alpha_j$ for $s'_j \in \Sigma^*$ and $\alpha_j \in \Sigma$, if $V(q_j) = \tau_j \in T_{act}$. Then, since s_j is not controllable by Definition 9 for control-dependent vocal states that vocal-state partners and partner-hiding states are, together with the condition that α_j is uncontrollable, it follows that the new τ_j-string with reference prefix $s'w\sigma$ and co-silent string $s''s'_j\alpha_j$ satisfies the condition for AOCC-system refinability as stated in Corollary 1.

  For $i \in \{1, 2\}, i \neq j$, let $s_i = s'_i\alpha_i$ for $s'_i \in \Sigma^*$ and $\alpha_i \in \Sigma$. It follows that if $V(q_i) = \tau_i \in T_{act}$ and s'_i is not controllable, then, that α_i is preemption-unambiguous implies α_i is either controllable or uncontrollable. Consequently, this implies that the new τ_i-string with reference prefix $s'w\sigma$ and co-silent string $s''s'_i\alpha_i$ satisfies the condition for AOCC-system refinability as stated in Corollary 1.

  Hence, by refining G_{lo} as such using Procedure **PF-SR**, the refined G_{lo} is not only PF and PHF, implying it is PF, but also remains AOCC-system refinable according to Corollary 1.
- Show that the PF-system refined G_{lo} can be further refined to be OCC without violating the established PF-system property:
  Since the refined G_{lo} is AOCC-system refinable, by Theorem 4, it is OCC-system refinable using Procedure **OCC-SR**.

  An arbitrary $\tau_n \in T_{act}$ is, in general, either ambiguously controllable, controllable or uncontrollable w.r.t every τ_n-string of $L(G_{lo})$. As defined, over the reachability tree constructed for G_{lo}, Subprocedure **AOCC-SR** of Procedure **OCC-SR** simply relabels, accordingly, τ_n-strings of $L(G_{lo})$, w.r.t which $\tau_n \in T_{act}$ is controllable or uncontrollable. Effectively, no vocal-state partners are created herewith.

  It remains to show that, in Subprocedure **AOCC-SR** relabeling τ_n-strings of $L(G_{lo})$ w.r.t which each $\tau_n \in T_{act}$ is ambiguously controllable, effectively no vocal-state partners are also created, as follows:

  We note that a τ_n-string $s = s'\sigma_1 \cdots \sigma_k \in L(G_{lo})$, where $\sigma_i \in \Sigma$ for all i $(1 \leqslant i \leqslant k)$ and s' is its reference prefix, w.r.t which $\tau_n \in T_{act}$ is ambiguously controllable, has the longest prefix $s'\sigma_1 \cdots \sigma_p$ for some p $(1 \leqslant p \leqslant k-1)$ - at which $\sigma_p = t_l$ and is ambiguously preemptable, and beyond which the suffix $\sigma_{p+1} \cdots \sigma_k$ is uncontrollable.

  Herewith, Subprocedure **AOCC-SR** labels such a prefix as a t_h-string and relabels τ_n-string s as some β_n-string accordingly, with the new t_h-string $s'\sigma_1 \cdots \sigma_p$ as its reference prefix. It then follows that, to prove by contradiction, assume that, due to the preceding refinement, q_1 is the new vocal state outputting the t_h and q_2 is some originally existent vocal state outputting an activity event such that (q_1, q_2) forms a pair of vocal-state partners over some structure $[s', w\sigma s'', <^{s_1}_{s_2}, j]$, where $q_1 = \delta(s'w\sigma s''s_1, q_0)$, $q_2 = \delta(s'w\sigma s''s_2, q_0)$ and $j \in \{1, 2\}$. Associating this structure with the form of the string s, the co-silent string of the t_h-string is $w\sigma s''s_1 = \sigma_1 \cdots \sigma_p$, which is ambiguously controllable as σ_p is, and so $\sigma_1 \cdots \sigma_{p-1}$ is either uncontrollable or ambiguously controllable. Together with Definition 9 for control-dependent vocal states that vocal-state partners are, it can only be that $\sigma = t_l$ and is ambiguously preemptable (i.e., σ is ambiguously controllable), and so the string $\sigma_1 \cdots \sigma_{p-1}$ must be ambiguously controllable. Thus, it follows that s_1 is not controllable and we may let $j = 1$.

In what follows, since state q_1 resides along the co-silent string of the initially given τ_n-string s, there exists a string $w'_1 \in (\Sigma_u \cup \{t_l\})^+$ such that $s = s'w\sigma s'' s_1 w'_1$. And since w'_1 is the co-silent string of the newly formed β_n-string s, $w'_1 = \sigma_{p+1} \cdots \sigma_k$ and is therefore uncontrollable. Since s_1 is not controllable and w'_1 is uncontrollable, it follows that the vocal state reachable by string s outputting τ_n initially and vocal state q_2 must initially be a pair of control-dependent vocal states over $[s', w\sigma s'', <_{s_2}^{s_1 w'_1}, j]$, according to Definition 9. It follows that, if they output the same activity events, they form a pair of partner-hiding states by Definition 13, or otherwise form a pair of vocal-state partners by Definition 10, contradicting the fact that the G_{lo} is PF and PHF.

Therefore, refining G_{lo} to be AOCC using Subprocedure **AOCC-SR** does not introduce new vocal-state partners, implying the AOCC-system refined G_{lo} remains PF.

Finally, as defined, over the reachability tree constructed for G_{lo}, Subprocedure **OFC-SR** of Procedure **OCC-SR** simply relabels τ_n-strings of $L(G_{lo})$ accordingly, and hence does not create new vocal states and therefore does not introduce new vocal-state partners.

All in all, the OCC-system refined G_{lo} remains PF.

Hence the theorem. □

A corollary of Theorem 5 follows.

Corollary 2 *An OCC TDES G_{lo} is SOCC-system refinable if, over each $[s', w\sigma s'', <_{s_2}^{s_1}, j]$ of every pair (q_1, q_2) of vocal-state partners or partner-hiding states, it is the case that for $i, j \in \{1, 2\}$, $i \neq j$,*

- *if $V(q_i) \neq t_h$, then s_i is preemption-unambiguous,*
- *if $V(q_j) \neq t_h$, then s_j is uncontrollable.*

Proof Consider an OCC TDES G_{lo} with the conditions as specified for each structure $[s', w\sigma s'', <_{s_2}^{s_1}, j]$ of every pair (q_1, q_2) of vocal-state partners (Definition 10) or partner-hiding states (Definition 13), both of which are control-dependent vocal states (Definition 9) in G_{lo}. Taken together, the structural conditions (and these include the given fact that G_{lo} is OCC) can be logically shown to be stronger than the sufficiency conditions stated in Theorem 5 for an SOCC-system refinable TDES. It thus follows that G_{lo} is SOCC-system refinable. Hence the corollary. □

6.5 STOCC-System Synthesis: A Discussion

Consider a hierarchy (G_{lo}, G_{hi}) built based on the proposed formulation. Suppose G_{lo} is SOCC and hence OCC. Based on the foregoing theoretical development, Property 4 and ALF (5) are satisfied for G_{hi}. Suppose we want the tick t_h for the high-level model G_{hi} to model real time, i.e., G_{hi} to possess time fidelity. What then remains to attain high-level time fidelity is that G_{hi} must also satisfy Property 3, and this is so provided G_{lo} is or can be refined to be OTC while remaining SOCC, and hence STOCC - a sufficient condition for HC-OTF. Any violation of Property 3 by G_{hi} is caused by either of two anomalies in the abstraction of the original Moore TDES[8], namely, either, upon a t_h-occurrence, an eligible high-level activity event becomes ineligible or it has one of its event-control properties modified.

W.r.t high-level time fidelity, the temporal dynamics of an SOCC G_{lo} being not OTC is deemed erroneous as the real-time soundness of all specifications w.r.t its abstraction model G_{hi} is not guaranteed. This necessitates a redesign of the reporter map θ by refining (G_{lo}, V) that removes the abstraction anomalies as well, and this general problem of existence and synthesis (by refinement) of an STOCC G_{lo} is a challenging one. In the next section, we study the SOCC-system refinability of an existent class of TDES's, and show that a 'linear' subclass formulated is STOCC-system refinable.

7 Hierarchical Consistency for NTU & NTI Systems

We consider a class of Moore TDES's, that we call next-output terminal-control unambiguous (NTU) systems. NTU systems impose some output-system design or modeling restrictions in the resultant class of TDES hierarchies. A

[8] By original, we refer to the low-level TDES prior to undergoing Procedure **OCC-SR**.

special subclass of NTU systems, called non-terminal time-control invariant (NTI) systems, is also defined. In what follows, the SOCC-system synthesis of NTU TDES's is formally proved. A further restricted linear subclass of NTI systems is also characterized, which, importantly, lends itself to STOCC-system synthesis of linear NTI systems as also formally proved, and that entails a neat strategy of arbitrarily removing the abstraction anomalies identified without violating SOCC-system refinability in obtaining STOCC systems.

Definition 15 (NTU and NTI systems) Let $s = s'\sigma_1\sigma_2\cdots\sigma_k$ be an arbitrary τ-string of $L(G_{lo})$ with reference prefix s' and $\sigma_i \in \Sigma$ for all i $(1 \leqslant i \leqslant k)$. Then the TDES G_{lo} is said to be NTU if, for each τ-string $s \in L(G_{lo})$ of every $\tau \in T_{act}$, the terminal event σ_k, if it is a tick t_l, is either non-preemptable or unambiguously preemptable. The TDES G_{lo} is said to be NTI if it is NTU and, for each τ-string $s \in L(G_{lo})$ of every $\tau \in T_{act} \cup \{t_h\}$, every (non-terminal) σ_i $(1 \leqslant i < k)$ that is a tick t_l is either non-preemptable or unambiguously preemptable.

For an NTU or NTI TDES G_{lo}, the terminal event $\sigma \in \Sigma$ in every τ-string $s\sigma \in L(G_{lo})$ of every output $\tau \in T_{act}$ is either an unambiguously preemptable or a non-preemptable tick, or an activity event (which is either prohibitable or uncontrollable). In other words, the terminal σ-control of the next activity output τ is unambiguous. For an NTI TDES G_{lo}, additionally, except the terminal tick t_l of every t_h-string of $L(G_{lo})$, the control preemptability of tick t_l elsewhere (i.e., whether t_l elsewhere can be preempted or not) is always the same under arbitrary system control dynamics. In other words, referring to t_l as a system non-terminal time tick whenever it is not the terminal event of a t_h-string of $L(G_{lo})$, the (low-level preemptive) control of non-terminal time ticks is invariant.

Remark 1 We should point out that NTU TDES's are not a limited class of hierarchical systems. It is first discussed in (Wong and Wonham, 1996) that, in general, a given TDES can be redesigned to become free of activity events, each of which is both forcible and prohibitable. A Moore TDES G_{lo} with $\Sigma_{for} \cap \Sigma_{hib} = \varnothing$ or equivalently, $\Sigma_{for} \subseteq \Sigma_u$, is clearly NTI since all its time ticks are control invariant, and hence is NTU. ■

7.1 SOCC-System Synthesis for NTU Systems

For NTU systems, an important result follows.

Theorem 6 *An NTU TDES G_{lo} is SOCC-system refinable.*

Proof Consider an NTU TDES G_{lo}. By Definition 15 of an NTU TDES and Corollary 1, G_{lo} is AOCC-system refinable. Over $[s', w\sigma s'', <^{s_1}_{s_2}, j]$ of every pair (q_1, q_2) of vocal-state partners (Definition 10) or partner-hiding states (Definition 13), both of which are control-dependent vocal states (Definition 9) in G_{lo}, and letting $s_k = s'_k\alpha_k$ where $\alpha_k \in \Sigma$, $k \in \{1, 2\}$, it is the case that, since the given G_{lo} is NTU,

if $V(q_i) \neq t_h$, then α_i is preemption-unambiguous; and if $V(q_j) \neq t_h$, then α_j is uncontrollable.

Together, it follows that the NTU TDES G_{lo} satisfies the sufficiency conditions stated in Theorem 5 for an SOCC-system refinable TDES. Hence the theorem. □

7.2 STOCC-System Synthesis for Linear NTI Systems

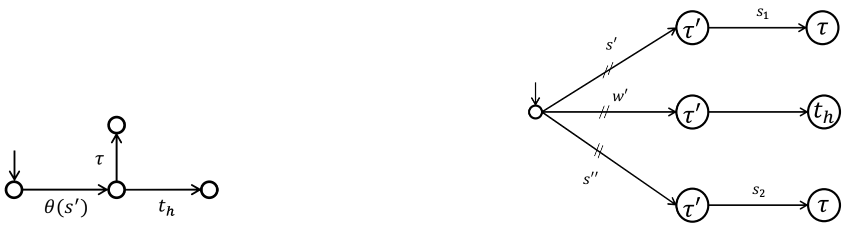
Fundamental to the linearity characterization on an NTI system is the system concept of linear time control-invariance, which requires the following definition.

Definition 16 (Timed-output-state control uniformity) A TDES G_{lo} is said to be timed-output-state control uniform (w.r.t T_{act}) if, for all $\tau \in T_{act}$, if there exists a τ-string of $L(G_{lo})$ with reference prefix s' and a t_h-string of $L(G_{lo})$ with reference prefix w' such that $\theta(w') = \theta(s')$, then for every τ-string $s \in L(G_{lo})$ with reference prefix s'' such that $\theta(s'') = \theta(s')$, τ has the same controllability property w.r.t s and the same forcibility property w.r.t s''.

The characterization of the concept is depicted in Fig. 10. The concept of linear time control-invariance follows.

Definition 17 (Linear time control-invariance) A TDES G_{lo} is linear time control-invariant (w.r.t T_{act}) if it is timed-output-state control uniform and NTI.

Thus, a TDES G_{lo} is linear time control-invariant in the sense that



(a) High-level abstraction of the characterization

(b) Low-level string-wise characterization: $\tau \in T_{act}$, $\theta(w') = \theta(s') = \theta(s'')$, the controllability property of τ w.r.t $s's_1$ is the same as that w.r.t $s''s_2$, and the forcibility property of τ w.r.t s' is the same as that w.r.t s''.

Fig. 10 Timed-output-state control uniformity

- it is timed-output-state control uniform, and thus at an arbitrary high-level state where a $\tau \in T_{act}$ and t_h are eligible, and the state is reachable from below by a string $s' \in L_{voc}(G_{lo})$, the string-wise control properties of $\tau \in T_{act}$ over every τ-string of $L(G_{lo})$ with reference prefix s'' such that $\theta(s'') = \theta(s')$ are the same; and
- it is NTI, and thus at an arbitrary low-level state, whenever a tick t_l is eligible, the control preemptability of the tick t_l under arbitrary system control dynamics is always the same if the tick t_l is not a terminal event of a t_h-string of $L(G_{lo})$.

Note that because a linear time control-invariant TDES is NTI, string-wise, no $\tau \in T_{act}$ is ambiguously controllable.

The two possible abstraction anomalies, of an eligible $\tau \in T_{act}$ becoming ineligible, and of it having one of its event-control properties modified upon a t_h-occurrence, are formalized as t_h-preemptability and t_h-property-modifiability, respectively, as follows.

Definition 18 **(t_h-preemptability of $\tau \in T_{act}$)** Consider an arbitrary τ-string of $L(G_{lo})$ with $\tau \in T_{act}$ and reference prefix s'. Then τ is said to be t_h-preemptable w.r.t s' if there exists a t_h-string $w \in L(G_{lo})$ with reference prefix w' such that $\theta(s') = \theta(w')$, but there is no τ-string of $L(G_{lo})$ with reference prefix r such that $\theta(r) = \theta(w)$.

Intuitively, t_h-preemptability of $\tau \in T_{act}$ characterizes the situation where a high-level event τ that is eligible is ‘preempted’ or becomes ineligible following an occurrence of t_h at a high-level state where τ and t_h are eligible.

A proposition relating system output time-compliance and t_h-preemptability follows.

Proposition 6 *A TDES G_{lo} is OTC iff, for every τ-string of $L(G_{lo})$ with reference prefix s', where $\tau \in T_{act}$, τ is not t_h-preemptable w.r.t s'.*

Proof For an arbitrary τ-string of $L(G_{lo})$ with reference prefix s', where $\tau \in T_{act}$, by Definition 18 of t_h-preemptability, τ is not t_h-preemptable w.r.t s'

- provided that for every t_h-string $w \in L(G_{lo})$ with reference prefix w' such that $\theta(s') = \theta(w')$, there exists a τ-string of $L(G_{lo})$ with reference prefix r such that $\theta(r) = \theta(w)$;
- provided that if there exists a $tt_h \in \theta(L(G_{lo})$ such that $\theta(s') = t$, then there exists a τ-string of $L(G_{lo})$ with reference prefix r such that $\theta(r) = \theta(w')t_h$;
- provided that, if there exists a t_h-string of $L(G_{lo})$ with reference prefix w' such that $\theta(s') = \theta(w')$, then there exists a τ-string of $L(G_{lo})$ with reference prefix r such that $\theta(r) = \theta(w')t_h$; and

provided that G_{lo} is OTC by Definition 6 of an OTC TDES. Hence the proposition. □

Next is the t_h-property-modifiability of a $\tau \in T_{act}$. Essentially, it means that, for a TDES hierarchy (G_{lo}, G_{hi}) where $G_{hi} \overset{\text{def}}{=} (X, T, \xi, x_0, -)$, there is some reachable state $x \in X$ with $\tau \in T_{act}(x)$, and a state $x' = \xi(t_h, x) \in X$, for which there is no τ-string $s_2 \in L(G_{lo})$ with reference prefix s'' such that $x' = \xi(\theta(s''), x_0)$ and $\theta(s'') = tt_h$ for some $t \in T^*$ such that $x = \xi(t, x_0)$, and for which τ has the same controllability and forcibility properties w.r.t s_2 and s'', respectively, as it respectively has w.r.t any τ-string $s_1 \in L(G_{lo})$ and s', where s' is the reference prefix of s_1 such that $\theta(s') = t$. In this paper, for a clearer exposition, it suffices to formally define this anomaly for a linear time control-invariant TDES G_{lo}.

Definition 19 **(t_h-property-modifiability of $\tau \in T_{act}$)** Consider an arbitrary τ-string $s_1 \in L(G_{lo})$ with $\tau \in T_{act}$ and reference prefix s', where TDES G_{lo} is linear time control-invariant. Then τ is said to be t_h-property-modifiable w.r.t s' if there exists a t_h-string $w \in L(G_{lo})$ with reference prefix w', where $\theta(s') = \theta(w')$, and there exists a τ-string $s_2 \in L(G_{lo})$ with reference prefix s'', where $\theta(s'') = \theta(w)$ such that, for every such $s_2 \in L(G_{lo})$,

- either, τ is controllable w.r.t s_1 iff τ is not controllable w.r.t s_2,
- or, τ is forcible w.r.t s' iff τ is not forcible w.r.t s''.

Intuitively, characterizing for a linear time control-invariant TDES G_{lo}, the t_h-property-modifiability of $\tau \in T_{act}$ refers to one ‘uniform’ string-wise event-control property (of either controllability or forcibility) of the high-level event τ changing completely, following an occurrence of t_h at a high-level state where τ and t_h are eligible.

Based on Proposition 6, we may define a stronger concept of an OTC-system.

Definition 20 (Control output time-compliance) A TDES G_{lo} is said to be control OTC if every $\tau \in T_{act}$ is neither t_h-preemptable nor t_h-property-modifiable w.r.t the reference prefix of each τ-string of $L(G_{lo})$.

We now define the relative index for the starting state of the longest suffix of the co-silent string of a t_h-string in a TDES G_{lo} that may exist, along which the TDES will never diverge from entering a state outputting t_h.

Definition 21 (Output-time attractor limit) The attractor limit for a t_h-string $< s', \sigma_i, -, k, t_h > \in L(G_{lo})$, if it exists, is the smallest index b $(1 \leqslant b < k)$ starting which the prefix $s'\sigma_1 \cdots \sigma_i$ for every i $(b \leqslant i < k)$ cannot be extended to any τ-string of $L(G_{lo})$ with reference prefix s', where $\tau \in T_{act}$.

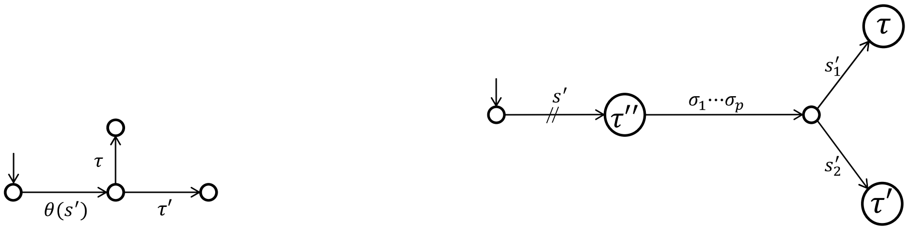
Intuitively, if no attractor limit b $(1 \leqslant b < k)$ exists for a t_h-string $< s', \sigma_i, x_i, k, t_h > \in L(G_{lo})$, it means that every prefix $s'\sigma_1 \cdots \sigma_i$ $(1 \leqslant i < k)$ can be extended to some τ-string of $L(G_{lo})$ with reference prefix s', where $\tau \in T_{act}$. If it does, then evolving from TDES state x_0, it is only after entering state x_b that the evolution towards state x_k or any other vocal state that outputs t_h is guaranteed.

Two more system concepts, for a linear time control-invariant TDES, follow.

Definition 22 *(Output-control determinism and anomalous output-time linear blockability):* Consider a linear time control-invariant TDES G_{lo}. For every τ-string $< s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$ with $\tau \in T_{act}$, and for every τ'-string $< s', \alpha_j, -, h, \tau' > \in L(G_{lo})$ with $\tau' \in T$, such that $\alpha_0\alpha_1 \cdots \alpha_p = \sigma_0\sigma_1 \cdots \sigma_p$ for some p $(0 \leqslant p < \min(h, k))$ where $\alpha_0 = \sigma_0 = \varepsilon$, the TDES G_{lo} is said to be

1. output-control deterministic, if the following condition holds: If $\tau' \neq \tau$, then $\sigma_1 \cdots \sigma_p$ is uncontrollable, i.e., for all i $(1 \leqslant i \leqslant p)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l \;\&\; \Sigma(x_{i-1}) \cap \Sigma_{for} = \emptyset)$; and
2. anomalous output-time linearly blockable, if the following condition holds: If, w.r.t s', τ is either t_h-preemptable or t_h-property-modifiable, then
   - if $\tau' = t_h$, the attractor limit b $(p + 1 \leqslant b < h)$ exists such that for some j $(b \leqslant j < h)$, $\alpha_j \in \Sigma_{act}$, and
   - for every t_h-string $< w', \beta_j, -, l, t_h > \in L(G_{lo})$, where $\theta(w') = \theta(s')$ and w' cannot be extended to a τ-string of $L(G_{lo})$ with reference prefix w', the attractor limit b' $(1 \leqslant b' < l)$ exists such that for some j $(b' \leqslant j < l)$, $\beta_j \in \Sigma_{act}$.

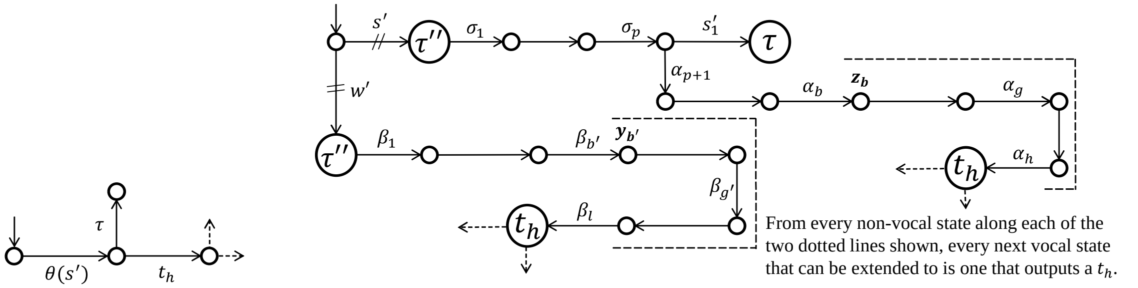
In words, for a linear time control-invariant TDES G_{lo}, it is output-control deterministic if, for every τ-string, $\tau \in T_{act}$ and for every τ'-string of $L(G_{lo})$, both with the same reference prefix s', if $\tau \neq \tau'$ and their co-silent strings share the first p low-level events, then each shared event is either uncontrollable or is a t_l that is non-preemptable. This characterization is depicted in Fig. 11. Intuitively, it ensures that every high-level prohibitable event can always be solely disabled and every preemptable t_h can always be solely preempted.



(a) High-level abstraction of the characterization

(b) Low-level string-wise characterization: $\tau \in T_{act}$, $\tau' \neq \tau$, and $\sigma_1 \cdots \sigma_p$ is uncontrollable.

Fig. 11 Output-control determinism (under linear time control-invariance)



From every non-vocal state along each of the two dotted lines shown, every next vocal state that can be extended to is one that outputs a t_h.

(a) High-level abstraction of the characterization: The t_h-occurrence either preempts τ (making it ineligible) in one anomaly, or modifies one of its control properties (making it ambiguous) in the other.

(b) Low-level string-wise characterization: $\tau \in T_{act}$, $\theta(w') = \theta(s')$, and attractor limits b, b' exist, followed by some activity events $\alpha_g, \beta_{g'}$ in the co-silent strings of the respective t_h-strings shown (representing all such t_h-strings that exist with reference prefixes w', s'). Denoted by dashed arrows are system transitions where the causes of the two abstraction anomalies lie: Either no τ-string of $L(G_{lo})$ exists with any of the t_h-strings shown as its reference prefix, or a string-wise property of controllability or forcibility for τ changes upon entering a state vocalizing a t_h.

Fig. 12 Anomalous output-time linear blockability (under linear time control-invariance)

Next, G_{lo} is anomalous output-time linearly blockable if, for every τ-string with reference prefix s', $\tau \in T_{act}$, if τ is either t_h-preemptable or t_h-property-modifiable w.r.t s', then two conditions hold. One, for every t_h-string $< s', \alpha_j, z_j, h, t_h > \in L(G_{lo})$ whose co-silent string shares its first p events with the co-silent string of the τ-string, there must exist an attractor limit b for the t_h-string such that $b > p$ and the suffix of the co-silent string of the t_h-string starting from state z_b must contain a low-level activity event α_g for some $j = g$ $(b \leqslant j < h)$. Two, for every t_h-string $< w', \beta_j, y_j, l, t_h > \in L(G_{lo})$ where its reference prefix w' has the same θ-image as the string s' and cannot be extended to a τ-string with the same reference prefix w', there exists an attractor limit b' for the t_h-string such that the suffix of the co-silent string of the t_h-string starting from state $y_{b'}$ contains a low-level activity event $\beta_{g'}$ for some $j = g'$ $(b' \leqslant j < l)$. This characterization is depicted in Fig. 12. Intuitively, anomalous output-time linearly blockability asserts that, at a high-level state where t_h and an activity event are eligible, if the occurrence of t_h preempts the activity event or changes its controllability or forcibility property, then there must exist critical low-level activity events whose occurrence discontinues or alters the nature of the on-going high-level activity w.r.t time, respectively.

We are now ready to define a linear NTI system, and present its STOCC-system synthesis result.

Definition 23 (Linear NTI system) A TDES G_{lo} is said to be linear NTI if it is linear time control-invariant, output-control deterministic and anomalous output-time linearly blockable.

A lemma follows.

Lemma 2 *A linear NTI TDES G_{lo} is PF and PHF.*

Proof For a linear NTI TDES G_{lo}, consider an arbitrary τ-string $< s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$, where $\tau \in T_{act}$ and an arbitrary τ'-string $< s', \alpha_j, -, h, \tau' > \in L(G_{lo})$, where $\tau' \in T$, such that $\alpha_0\alpha_1 \cdots \alpha_p = \sigma_0\sigma_1 \cdots \sigma_p$ for some p $(0 \leqslant p < \min(h, k))$ where $\alpha_0 = \sigma_0 = \varepsilon$, and let $q_1 = \delta(s'\sigma_1\sigma_2 \cdots \sigma_k, q_0) \in Q_{voc}$ and $q_2 = \delta(s'\alpha_1\alpha_2 \cdots \alpha_h, q_0) \in Q_{voc}$. The proof then proceeds as follows.

To prove that G_{lo} is PF: Since G_{lo} is output-control deterministic by Definition 23 of a linear NTI TDES, it follows by Definition 22-1 of output-control determinism that, if $\tau \neq \tau'$, then for all i $(1 \leqslant i \leqslant p)$, $\sigma_i \in \Sigma_u$ or $(\sigma_i = t_l$ & $\Sigma(x_{i-1}) \cap \Sigma_{for} = \varnothing)$. This implies that string $\sigma_1 \cdots \sigma_p$ is uncontrollable. Hence, (q_1, q_2) is not a pair of control-dependent states as Condition CDS1 of Definition 9 is not satisfied. Therefore (q_1, q_2) is not a pair of vocal-state partners by Definition 10. By Definition 11, since G_{lo} does not have vocal-state partners, it is PF.

To prove that G_{lo} is PHF: By Definition 23, G_{lo} is also linear time control-invariant and therefore NTI by Definition 17. This implies that if $\tau = \tau' \in T_{act}$, the co-silent strings $\sigma_1 \cdots \sigma_k$ and $\alpha_1 \cdots \alpha_h$ of the τ-string and τ'-string of $L(G_{lo})$, respectively, do not contain an ambiguously preemptable tick t_l, and hence (q_1, q_2) is not a pair of partner-hiding states by Definition 13. By Definition 14, since G_{lo} does not have partner-hiding states, it is PHF.

Hence the lemma. □

We now present a conceptual method named Method **STOCC-LNTI-SR** for a linear NTI TDES (G_{lo}, V). The method uses another conceptual method named Method **COTC-SR**, which is presented first.

Method **COTC-SR** is defined over the reachability tree $(G_{lo,t}, V_t)$ as follows: For each $\tau \in T_{act}$, and for every τ-string $s =< s', \sigma_i, -, k, \tau > \in L(G_{lo})$ for which τ is t_h-preemptable or t_h-property-modifiable w.r.t its reference prefix s':

Step 1) Add a new activity output γ to T_{act}.
Step 2) For each t_h-string $< w', \alpha_j, -, h, t_h > \in L(G_{lo})$ where $\theta(w') = \theta(s')$, find an index j such that $(b \leqslant j < h)$ and $\alpha_j \in \Sigma_{act}$, where b is the attractor limit of the t_h-string, and redefine $V_t(\delta_t(w'\alpha_1\alpha_2 \cdots \alpha_j, n_0)) = \gamma$.

Method **STOCC-LNTI-SR** for a linear NTI TDES (G_{lo}, V) is now outlined in two steps, as follows:

Step 1) Refine the TDES G_{lo} by applying Method **COTC-SR**.
Step 2) Refine the model G_{lo} further by first applying Procedure **OCC-SR**, and thereafter fixing each force-don't-care event $\overset{\mathrm{x}}{\gamma} \in \{\overline{\gamma}, \gamma\}$ in every $tt_h \overset{\mathrm{x}}{\gamma} \in \theta(L(G_{lo})$ as $\overline{\gamma}$ if $t\overline{\gamma} \in \theta(L(G_{lo}))$; and otherwise γ if $t\gamma \in \theta(L(G_{lo}))$.

Henceforth, a TDES is said to be STOCC-system refinable if it can be refined to be STOCC using Method **STOCC-LNTI-SR**.

Theorem 7 *A linear NTI TDES G_{lo} is STOCC-system refinable.*

Proof Consider a linear NTI TDES G_{lo}, which by Definition 23 is linear time control-invariant (Definition 17) [i.e., NTI (Definition 15) and timed-output-state control uniform (Definition 16)], output-control deterministic (Definition 22-1) and anomalous output-time linearly blockable (Definition 22-2).

We first show that, by applying Step 1 (i.e., Method **COTC-SR**) of Method **STOCC-LNTI-SR**, the given linear NTI TDES G_{lo} can be refined to be control OTC without violating the linear NTI-system property, as follows: Consider an arbitrary τ-string $s =< s', \sigma_i, x_i, k, \tau > \in L(G_{lo})$, where $\tau \in T_{act}$.

- Show that the given G_{lo} can be refined to be control OTC:
  If $\tau \in T_{act}$ is t_h-preemptable or t_h-property-modifiable w.r.t s', Definitions 18 and 19 together imply that there must exist a t_h-string $w =< w', \alpha_j, -, h, t_h >$ such that $\theta(w') = \theta(s')$. It follows that w' may or may not be the reference prefix of some τ-string of $L(G_{lo})$. Therefore, we have two cases to consider:
  Case 1: The string w' is the reference prefix of some τ-string.
  Then since τ is either t_h-preemptable or t_h-property-modifiable w.r.t s', τ is also t_h-preemptable or t_h-property-modifiable w.r.t w'. By Definition 22-2 of anomalous output-time linearly blockabilty, it follows that there exists an attractor limit (of Definition 21), which is an index b such that along the co-silent string $\alpha_1 \cdots \alpha_h$ of w, for some j $(b \leqslant j < h)$, $\alpha_j \in \Sigma_{act}$. Hence, in applying Method **COTC-SR**, one such index j can be found for redefining $V(\delta(w'\alpha_1\alpha_2 \cdots \alpha_j, q_0)) = \gamma$, where γ is the new activity output introduced.
  Case 2: The string w' is not the reference prefix of any τ-string.
  Then since τ is either t_h-preemptable or t_h-property-modifiable w.r.t s', by Definition 22-2 of anomalous output-time linearly blockabilty, it follows that there exists an attractor limit which is an index b', such that along the co-silent string $\alpha_1 \cdots \alpha_h$ of w, for some j $(b' \leqslant j < h)$, $\alpha_j \in \Sigma_{act}$. Hence similarly, in applying Method **COTC-SR**, one such index j can be found for redefining $V(\delta(w'\alpha_1\alpha_2 \cdots \alpha_j, q_0)) = \gamma$, where γ is the new activity output introduced.
  In (effectively) redefining the vocalization map V as such, Method **COTC-SR** refines the TDES G_{lo} such that every $\tau \in T_{act}$ for the refined G_{lo} is no longer t_h-preemptable or t_h-property-modifiable w.r.t s'. Hence the refined G_{lo} does not contain a τ-string where τ is either t_h-preemptable or t_h-property-modifiable w.r.t its reference prefix, and therefore is control OTC by Definition 20.
- Show that the refined G_{lo} remains a linear NTI system:
  To prove that G_{lo} remains NTI: As deduced from Definition 15, G_{lo} is NTI provided every event along the co-silent string of an arbitrary τ-string of $L(G_{lo})$ is not an ambiguously preemptable tick t_l, and so is every non-terminal event along the co-silent string of an arbitrary t_h-string of $L(G_{lo})$. For the given NTI G_{lo}, without relabeling or unlabeling any existing t_h-string (i.e., redefining it as a non-t_h-string or a non-vocal string, respectively), and only introducing each new γ-string as prescribed for each new γ added to T_{act}, Method **COTC-SR** clearly does not change this provision for the refined G_{lo}; and hence the refined G_{lo} remains NTI.
  To prove that G_{lo} remains timed-output-state control uniform: From the proof above showing that the given G_{lo} can be refined to be control OTC, it is clear that, for any new activity output γ, and therefore any new γ-string of $L(G_{lo})$ with reference prefix s' introduced by Method **COTC-SR**, there is no t_h-string with reference prefix w' such that $\theta(s') = \theta(w')$ in the refined G_{lo}, and the co-silent string of every τ-string in the given G_{lo} remains the same in the refined G_{lo}. Therefore, the refined G_{lo} remains timed-output-state control uniform by Definition 16.

At this juncture, we have proved that the refined G_{lo} is linear time control-invariant (Definition 17), to which Definition 22 is applicable.

To prove, by contradiction, that G_{lo} remains output-control determinstic: Suppose the refined G_{lo} is not output-control deterministic. This means that there exists a γ-string $< s', \sigma_i, x_i, k, \gamma >$ and a τ'-string $< s', \alpha_j, -, h, \tau' >$ where γ is a new activity output, $\tau' \in T$ and $\tau' \neq \gamma$, such that $\alpha_0\alpha_1 \cdots \alpha_p = \sigma_0\sigma_1 \cdots \sigma_p$ for some p $(0 \leqslant p < min(h, k))$ where $\alpha_0 = \sigma_0 = \varepsilon$, and for some i $(1 \leqslant i \leqslant p)$, $\sigma_i \notin \Sigma_u$ and $\sigma_i = t_l \Longrightarrow \Sigma(x_{i-1}) \cap \Sigma_{for} \neq \emptyset$. Then since before redefining as γ, $V(\delta(s'\sigma_1\sigma_2 \cdots \sigma_k, q_0)) = \tau_o$, it must be that in the given G_{lo}, there exists a t_h-string $< s', \sigma'_j, x'_j, k', t_h >$ such that $\sigma_1\sigma_2 \cdots \sigma_k = \sigma'_1\sigma'_2 \cdots \sigma'_k$ and $V(x'_1) = \cdots = V(x'_{k'-1}) = \tau_o$. With Method **COTC-SR** redefining similarly for every t_h-string with reference prefix w' such that $\theta(w') = \theta(s')$, it must be that $\tau' \in T_{act}$. Together, it means that in the given G_{lo}, there exists a t_h-string $< s', \sigma'_j, x'_j, k', t_h >$ and a τ'-string $< s', \alpha_j, -, h, \tau' >$ where $\tau' \neq t_h$, such that $\alpha_0\alpha_1 \cdots \alpha_p = \sigma'_0\sigma'_1 \cdots \sigma'_p$ for some p $(0 \leqslant p < min(k', h))$ and for some j $(1 \leqslant j \leqslant p)$, $\sigma_j \notin \Sigma_u$ and $\sigma_j = t_l \Longrightarrow \Sigma(x'_{j-1}) \cap \Sigma_{for} \neq \emptyset$, contradicting the fact that the given G_{lo} is output-control deterministic. Hence, the refined G_{lo} is output-control deterministic by Definition 22-1.

To prove that G_{lo} remains anomalous output-time linearly blockable: As proved above, the refined G_{lo} is control OTC (Definition 20). It follows by Definition 22-2 that it is trivially anomalous output-time linearly blockable.

Together, the refined G_{lo} that is control OTC and hence OTC by Definition 20 and Proposition 6, is a linear NTI system by Definition 23.

We then show, by applying Step 2 of Method **STOCC-LNTI-SR**, that the TDES G_{lo} can be further refined to be SOCC without violating the established OTC-system property, and hence to be STOCC by Definition 12, as follows:

Remaining linear NTI, the OTC-system refined G_{lo} is, by Lemma 2, PF and PHF, which is the same as a TDES refined using Procedure **PF-SR**. Therefore, by Theorem 6, G_{lo}, an NTI and therefore NTU TDES by Definition 15, can be further refined to be SOCC by applying the remaining Procedure **OCC-SR**. Because G_{lo} is NTI, no co-silent string of every τ-string of $L(G_{lo})$, where $\tau \in T_{act}$, is ambiguously controllable, and hence no new t_h-string is introduced by Procedure **OCC-SR** in Step 2 of Method **STOCC-LNTI-SR**. Together with the fact that the TDES G_{lo} to be further refined is control OTC, after applying Step 2 of Method **STOCC-LNTI-SR**, no (control relabeled) $\gamma \in T_{act}$ in the refined G_{lo} is t_h-preemptable or t_h-property-modifiable, string-wise. Hence the SOCC-system refined G_{lo} remains control OTC and hence OTC by Definition 20 and Proposition 6.

Hence the theorem. □

7.3 Hierarchical Control of a Photocopying System - a Linear NTI System

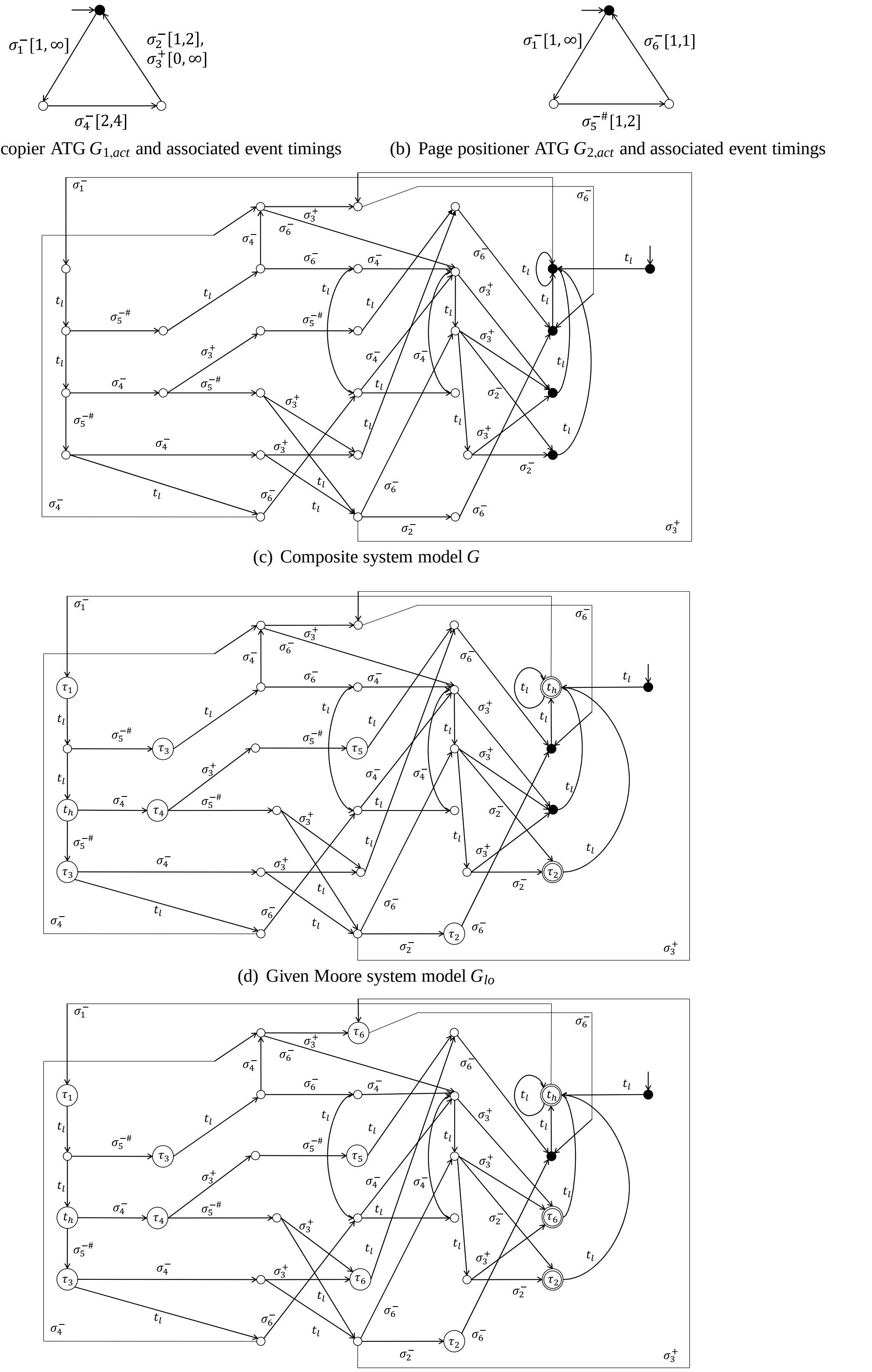
The STOCC-system synthesis for linear NTI TDES's is illustrated, with the necessity for output-time fidelity reiterated, using a simplified but non-trivial photocopying machine that takes a photo snapshot of every properly placed document page and saves it as a software image file.

7.3.1 System Description

The machine is a system composition G of two real-time component TDES's: a photocopier G_1 and a page positioner G_2. The ATG's $G_{1,act}$ and $G_{2,act}$ with their associated timing information, by which the respective components G_1 and G_2 (not shown) are constructed, are shown in Figs. 13(a) and 13(b); and the composite system $G = G_1 \| G_2$ is shown in Fig. 13(c). The event set $\Sigma_{act} = \{\sigma_i \mid 1 \leqslant i \leqslant 6\}$ is partitioned with $\Sigma_{hib} = \{\sigma_3\}$ and $\Sigma_{for} = \{\sigma_5\}$. The definitions of the system events are given in the 'Events' row of Table 2.

The dynamics of the system components are described as follows. Following a 1-tick joint initialization or re-initialization of sensors, the system components are both ready to begin the next photocopying cycle. When a document page in the input tray is detected (σ_1), the page positioner and photocopier are jointly alerted. Following, the page positioner takes 1 tick to ready itself, and up to 1 subsequent tick to pull the page from the input tray and position it in the photocopy area (σ_5). Concurrently, the photocopier takes 2 ticks to set up, and up to 2 more ticks to photocopy and save the photocopied as a software file (σ_4). Upon executing σ_4, the photocopier may clear any page in the photocopy area into the input tray (σ_3) or, following a 1 tick-delay, take up to 1 more tick to clear the page in the photocopy area into the output tray (σ_2). Upon executing σ_5 followed by a tick, the page positioner readies itself for the next document page (σ_6).

The intricate timed interleaving of the events between the system components is captured in the TDES model G.



(a) Photocopier ATG $G_{1,act}$ and associated event timings (b) Page positioner ATG $G_{2,act}$ and associated event timings

(c) Composite system model G

(d) Given Moore system model G_{lo}

(e) An output-set enlarged Moore system model G_{lo} for STOCC-system design

Fig. 13 Photocopying machine models for hierarchical control system design

7.3.2 Initial Hierarchical System Design

Suppose that in the initial hierarchical system design, we are given the set of high-level activity events, such that each is defined as an output by vocal states of a Moore version G_{lo} shown in Fig. 13(d) of the composite system G, entered following a respective low-level activity event or a string of low-level activity events (in ATG $G_{1,act} \parallel G_{2,act}$). The system outputs of interest pertain to the photocopying cycle. The definitions of these system outputs are given in the 'Outputs (given)' row of Table 2. The outputs correspond to 'next page placed for photocopying', signalled as high-level event τ_1 when σ_1 occurs; 'page processed' signalled as τ_2 when σ_2 occurs; 'page photocopy assured' signalled as τ_3 when σ_5 is the next activity event to occur after σ_1; 'page failed to be photocopied' signalled as τ_4 when σ_4 is the next activity event to occur after σ_1; and 'page left in photocopy area' signalled as τ_5 when σ_5 occurs immediately after σ_3.

7.3.3 Linear NTI System - A Verification

In the following, we verify that the given G_{lo} of Fig. 13(d) with $T_{act} = \{\tau_i \mid 1 \leqslant i \leqslant 5\}$ is linear NTI (Definition 23).

- G_{lo} is NTI (Definition 15) because no t_l in G_{lo} is ambiguously preemptable (Definition 1).
- G_{lo} is timed-output-state control uniform (Definition 16) since:
  - For each $\gamma \in T_{act} - \{\tau_2\}$ and for an arbitrary γ-string $s \in L(G_{lo})$ with reference prefix s', there does not exist a γ-string $w \in L(G_{lo})$, $w \neq s$, with reference prefix s'' such that $\theta(s'') = \theta(s')$. Therefore, each γ trivially satisfies the condition required by every $\tau \in T_{act}$ for timed-output-state control uniformity.
  - For $\tau_2 \in T_{act}$, consider an arbitrary τ_2-string of $L(G_{lo})$ with reference prefix s'. For each $s' \in R_2 = \{t_l\sigma_1 t_l t_l \sigma_4, t_l\sigma_1 t_l \sigma_5, t_l \sigma_1 t_l t_l \sigma_5\}$, there exists a t_h-string of $L(G_{lo})$ with reference prefix s'; and for every τ_2-string $s \in L(G_{lo})$ with reference prefix s'' such that $\theta(s'') = \theta(s')$ (where we note that $s'' = s'$), τ_2 stays uncontrollable w.r.t the given s and forcible w.r.t the string s''. It can be inferred from R_2 - the set of representative reference prefixes for τ_2 - and the structural regularity of (finite-state) G_{lo} that the reference prefix of every τ_2-string is the reference prefix of some t_h-string, both of $L(G_{lo})$, and for every τ_2-string $s \in L(G_{lo})$ with reference prefix s'', τ_2 is uncontrollable w.r.t s and forcible w.r.t s''. Thus, τ_2 satisfies the condition required by every $\tau \in T_{act}$ for timed-output-state control uniformity.
- G_{lo} is output-control deterministic (Definition 22-1) since:
  - For each $\gamma \in T_{act} - \{\tau_5\}$ and for every γ-string $s \in L(G_{lo})$, since its co-silent string contains only events in $\Sigma_u \cup \{t_l\}$, of which every t_l present is non-preemptable, trivially, γ satisfies the condition required by every τ-string of $L(G_{lo})$, $\tau \in T_{act}$, for output-control determinism.
  - For $\tau_5 \in T_{act}$, for the τ_5-string $s'\sigma_3\sigma_5 \in L(G_{lo})$ with reference prefix $s' = t_l\sigma_1 t_l t_l \sigma_4$ and co-silent string $\sigma_3\sigma_5$, since $s'\sigma_3$ cannot be extended, by an event or a string via intermediate non-vocal states, into states vocalizing outputs other than τ_5, this τ_5-string trivially satisfies the condition required by every τ-string of $L(G_{lo})$, $\tau \in T_{act}$, for output-control determinism. It can be inferred from the representative reference prefix $s' = t_l\sigma_1 t_l t_l \sigma_4$ for τ_5 and the structural regularity of G_{lo} that every τ_5-string of $L(G_{lo})$ satisfies the condition required by every τ-string of $L(G_{lo})$, $\tau \in T_{act}$, for output-control determinism.
- G_{lo} is anomalous output-time linearly blockable (Definition 22-2) since (string-wise), no $\tau \in T_{act}$ is t_h-property modifiable, and only $\tau_2, \tau_5 \in T_{act}$ are t_h-preemptable:

Table 2 Symbol definitions of events and outputs for the photocopying system

	Symbol:	Meaning
Events	σ_1:	next document page in input tray detected
	σ_2:	page in photocopy area cleared into output tray
	σ_3:	photocopy area cleared, moving any page there into input tray
	σ_4:	photocopy-as-software-file action executed
	σ_5:	page pulled from input tray and positioned in photocopy area
	σ_6:	ready for next photocopying cycle
Outputs (given)	τ_1:	next page placed for photocopying (vocalized after σ_1)
	τ_2:	page processed (vocalized after σ_2)
	τ_3:	page photocopy assured (vocalized after $\sigma_1\sigma_5$)
	τ_4:	page failed to be photocopied (vocalized after $\sigma_1\sigma_4$)
	τ_5:	page left in photocopy area (vocalized after $\sigma_3\sigma_5$)
Output (added)	τ_6:	page to be re-processed (vocalized after σ_3)

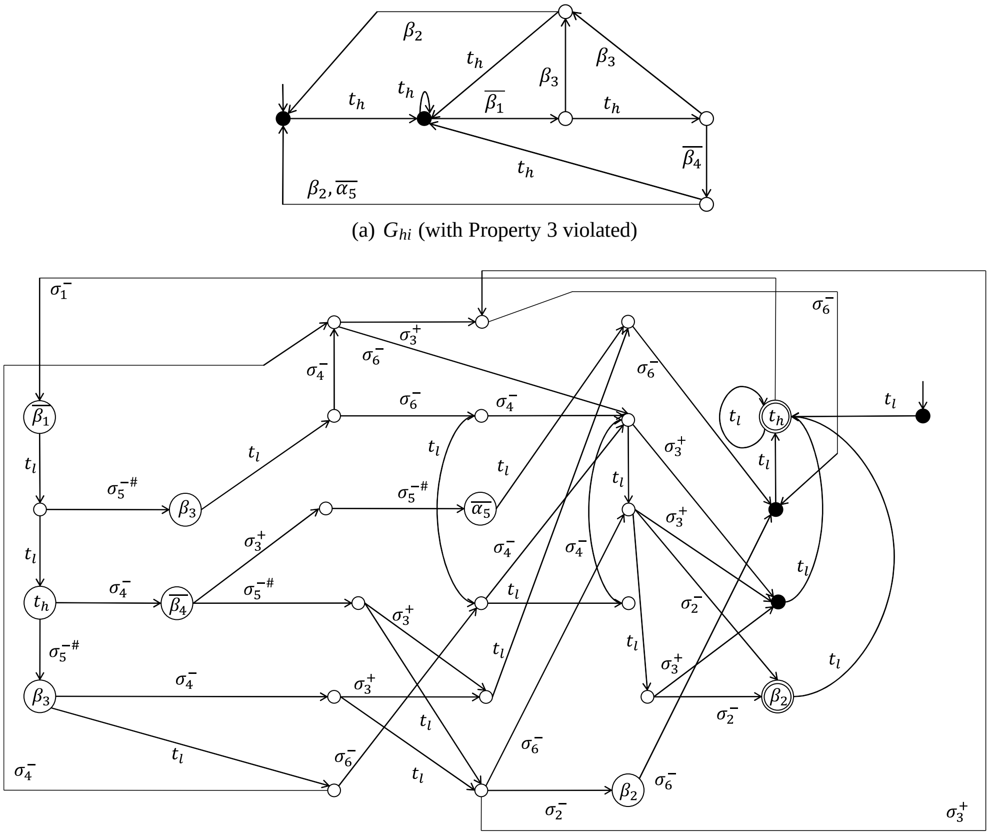
- τ_2 is t_h-preemptable w.r.t $s' \in R_2$ (with R_2 defined earlier above), τ_5 is t_h-preemptable w.r.t $t_l\sigma_1 t_l t_l \sigma_4 \in R_2$. It can be inferred from the representative reference prefix set R_2 for $\{\tau_2, \tau_5\}$ and the structural regularity of G_{lo} that $\tau_2, \tau_5 \in T_{act}$ are t_h-preemptable w.r.t every of their reference prefixes.

Along the co-silent string of every t_h-string with the same reference prefix as a τ-string of $L(G_{lo})$, where $\tau \in \{\tau_2, \tau_5\}$, there exists a non-vocal state entered via a transition of event σ_3, from which the system's reach cannot be extended, by an event or a string via intermediate non-vocal states, into a state vocalizing an activity output. Thus, for every such t_h-string, an attractor limit exists (at every state entered via a transition of σ_3).

In what follows, we explain how to refine the given TDES G_{lo} to build a consistent hierarchy, but which is one that has some design time anomalies.

7.3.4 SOCC-System Synthesis & High-Level Time Fidelity Issues

The given G_{lo} is NTI and hence NTU. By Theorem 6, it is SOCC-system refinable using Procedure **PF-SR** followed by Procedure **OCC-SR**. By Lemma 2, since the given G_{lo} is linear NTI, it is PF and PHF. To refine it into an SOCC-system, it remains to apply Procedure **OCC-SR**, to relabel accordingly and unambiguously associate every $\tau \in T_{act}$ with the event-control properties. Note that following Step 1 of Procedure **OCC-SR**, τ_4 becomes β_4; and following Step 2, string-wise, β_4 is found to be always force-don't-care, and defaulted to non-forcible with relabel $\overline{\beta_4}$. The OCC-system refined G_{lo} is also partner-free, and hence is SOCC.



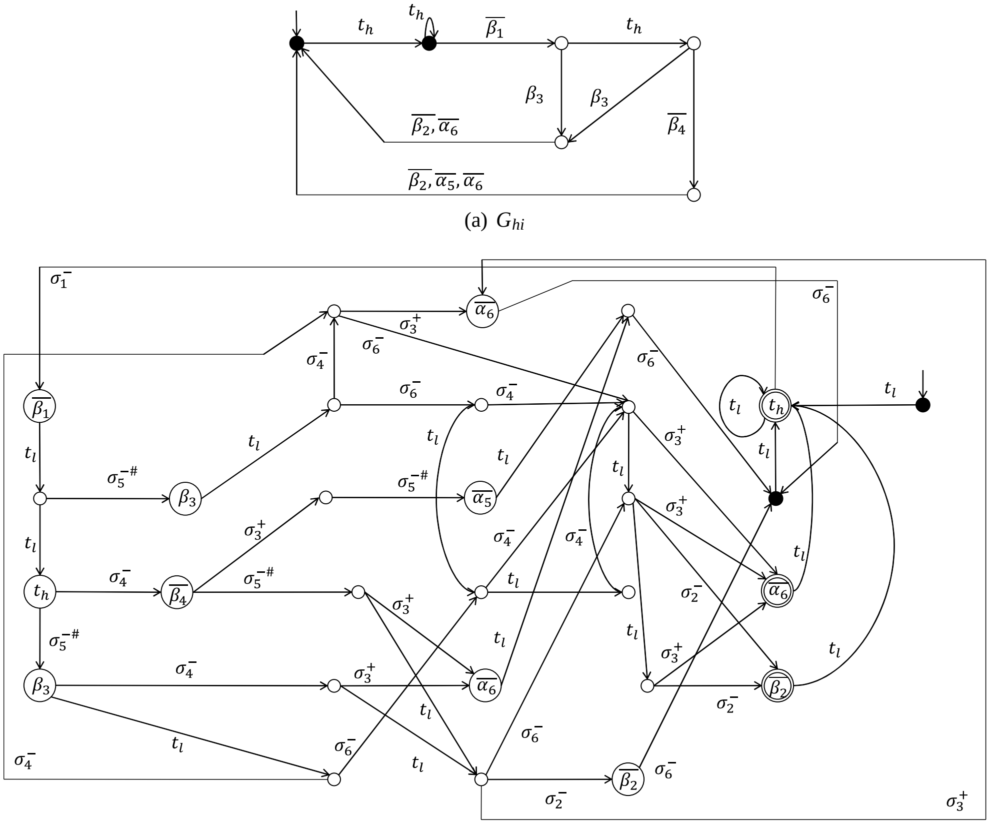
(a) G_{hi} (with Property 3 violated)

(b) SOCC G_{lo}

Fig. 14 A hierarchical photocopying system (G_{lo}, G_{hi}) that is HC

The refined hierarchy (G_{lo}, G_{hi}), where G_{lo} is SOCC, is shown in Fig. 14. By Theorem 2, it is HC.

Note that in the abstracted model G_{hi} shown in Fig. 14(a), the eligibility of giving assurance that a page can be photocopied (β_3) is invariant under high-level time tick transition. Importantly, this aspect of timing semantics captures a critical fact that any high-level tick delay in giving such assurance can result in the imminent and uncontrollable



(a) G_{hi}

(b) STOCC G_{lo}

Fig. 15 A hierarchical photocopying system (G_{lo}, G_{hi}) that is HC-OTF

possibility of page-photocopy failure $(\overline{\beta_4})$ while the assurance is still in progress. The eligibility of a page placed and ready for photocopying $(\overline{\beta_1})$ is also invariant under high-level time tick transition, and that of $\overline{\beta_4}$ is trivially so. However, high-level activity events β_2 and $\overline{\alpha_5}$ do not comply with such timed eligibility invariance, and thus G_{hi} violates Property 3, or equivalently, the SOCC G_{lo} violates the OTC-system property.

Violating Property 3 although Property 4 and ALF (5) are satisfied, model G_{hi} in Fig. 14(a) does not possess time fidelity. It follows that, as similarly illustrated in the example system depicted in Fig. 2, a high-level real-time specification such as ensuring 'at most one high-level tick for page processing (β_2) completion' has unsound timing semantics w.r.t G_{hi}. Certain high-level specifications might still have sound timing semantics, but without going underneath the abstraction to understand the low-level system dynamics of the non-OTC G_{lo}, studying the high-level model G_{hi} alone poses difficulty for a high-level control designer to identify and prescribe with confidence any correct and required high-level control specification for G_{hi}. As a matter of fact, one wonders what unabstracted low-level activity event or string of low-level events occurs along with the tick t_h, causing the system G_{hi} in Fig. 14(a) to, upon the t_h-occurrence, cancel the processing (β_2) or prevent a page from being left in the photocopy area $(\overline{\alpha_5})$.

In what follows, we explain how to refine the given TDES G_{lo} in Fig 13(d) to build a consistent hierarchy with output-time fidelity.

7.3.5 STOCC-System Synthesis

Because the given G_{lo} is linear NTI as established earlier, by Theorem 7, it is STOCC-system refinable (using Method **STOCC-LNTI-SR**). From a design perspective, the missing high-level information is the signal that a document page needs to be re-processed. So it turns out that, although technically not necessarily the only way, we may introduce a new high-level event τ_6 to represent this information, to be output by every state entered upon the occurrence of σ_3. With this event introduction, listed in the 'Output (added)' row of Table 2, the modified G_{lo}, as shown in Fig. 13(e), becomes OTC with no $\tau \in T_{act}$ that is string-wise t_h-preemptable or t_h-property-modifiable, as shown in Fig.

13(e). Applying Procedure **OCC-SR** to this modified G_{lo}, every $\tau \in T_{act}$ is relabeled accordingly and unambiguously associated with the event-control properties. Again, note that, following Step 1 of Procedure **OCC-SR**, τ_2, τ_4, τ_5 and τ_6 become β_2, β_4, α_5 and α_6, respectively; and following Step 2, string-wise, β_2, β_4, α_5 and α_6 are found to be always force-don't-care, and defaulted to non-forcible, with relabels $\overline{\beta_2}, \overline{\beta_4}$, $\overline{\alpha_5}$ and $\overline{\alpha_6}$, respectively.

The desired refined hierarchy (G_{lo}, G_{hi}), where G_{lo} is STOCC, is shown in Fig. 15. By Theorem 2, it is HC-OTF.

7.3.6 Hierarchical Control Specification

As a specification example over G_{hi} shown in Fig. 15(a), we may now assert the requirement that every document page is to be photocopied once without failure. The specification TTG for this requirement is shown in Fig. 16. A high-level supervisor (not shown) may be synthesized using standard real-time control theory (Brandin and Wonham, 1994).

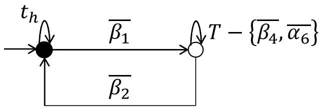


Fig. 16 A (high-level) specification TTG for the model G_{hi} in Fig. 15(a)

Note that a specialized untimed hierarchical nonblockingness result that entails the reporter map to be a system marked language observer (see (Wonham, 2016) for details) is applicable to TDES's within the same framework of formal languages and finite automata. Although hierarchical consistency, as formalized by Definition 8 and Theorem 2, does not deal with marked states, it can be shown by applying this nonblockingness result that the photocopying system hierarchy (G_{lo}, G_{hi}) in Fig. 15 admits nonblocking high-level supervisor that can be realized or implemented by a corresponding low-level supervisor generating prefix-closed sublanguages.

7.4 Framework Generalization & Scalability

Our theory development of formulating and building a consistent control hierarchy began with adopting the control-theoretic formulation of G (2) (Brandin and Wonham, 1994) as the base TDES model and our formulation of the timed reporter map θ. This puts our contribution in the context of a useful control-theoretic system model possessing time fidelity that G (2) is for real-time system and control design (Brandin and Wonham, 1994), with the added control-theoretic postulation of $\Sigma_{spe} \subseteq \Sigma_u$ being sufficient for proving Property 4 under the two partitions of Σ_{act}, namely, $\Sigma_{spe} \dot\cup \Sigma_{rem}$ and $\Sigma_{hib} \dot\cup \Sigma_u$. It should be clear that the theory part on hierarchical consistency with output-time fidelity still applies as long as a given base TDES model, a TTG, possesses time fidelity, and the part on that without output-time fidelity guarantee still applies even if the base TDES model has Property 3 relaxed, in which case we are using a TDES model where *tick* still represents time but is not always 'behaviorally' real time as it can be a timeout (see Footnote 1) - an event denoting a time elapse in simultaneity with some implied action, whose transition may disrupt the eligibility of activity events.

In concluding, we note that the hierarchical consistency for two levels may be extended to multiple levels. Once hierarchical consistency is achieved, either of the type without or with output-time fidelity guarantee as desired for, say $(G_{lo,0}, G_{hi,0})$ - the base level and initial level up - by refining accordingly, the Moore TDES $G_{lo,0}$ that is NTU or linear NTI, respectively, the constructions may be repeated by first assigning state outputs in $G_{hi,0}$ (according to the time-output design laws and respective NTU or linear NTI system modeling constraints) to obtain a Moore TDES $G_{lo,1}$ as desired, and then bringing in the next higher level, $G_{hi,1}$. Clearly, by similarly refining the TDES $G_{lo,1}$ obtained, the hierarchical consistency of the same type for $(G_{lo,1}, G_{hi,1})$ as attained for $(G_{lo,0}, G_{hi,0})$ can be achieved without disturbing the consistency of $(G_{lo,0}, G_{hi,0})$. In principle, therefore, as with the logical framework (Zhong and Wonham, 1990), our real-time framework is vertically scalable.

8 Conclusion

The concepts of output-control consistency and partner-freeness for hierarchical control are generalized, from untimed DES's (Zhong and Wonham, 1990) to TDES's (Wong and Wonham, 1996) where time fidelity need not be respected in the sense of not obeying Property 3; and the foundation is then augmented with the new concept of output time-compliance for a class of Moore TDES's that possesses time fidelity, to develop a new real-time control-theoretic framework for hierarchical control where output-time fidelity is also respected, i.e., a new framework of hierarchical consistency with output-time fidelity. In essence, developed in this paper are abstraction concepts by which to 'cyber-ize the physical TDES' at the low level and 'physicalize the cyber TDES' at the high level, when applied to building a cyber-physical system as a consistent two-level TDES hierarchy. Under this framework, supporting SOCC-system existence and synthesis results are presented, on which the results, of SOCC-system synthesis for hierarchical consistency and STOCC-system synthesis for hierarchical consistency with output-time fidelity, are proved for the mildly restrictive class of NTU systems and its subclass of linear NTI systems, respectively.

Formalized over controllable, high-level prefix-closed system sublanguages as in the logical version (Zhong and Wonham, 1990), hierarchical consistency does not ensure control nonblockingness at the high level by low-level control implementation; only the prefix-closure of high-level nonempty controllable sublanguages can be realized, unless some hierarchical observer condition holds as briefly mentioned at the end of Section 7.3. Using the key system concepts of output-control consistency developed in this paper, the logical theory of hierarchical consistency with marking (Wonham, 2016) can be extended to a timed framework, under which a high-level nonblocking supervisor can be implemented by a low-level nonblocking supervisor.

Finally, it is well understood that the problem of computational complexity in system and control synthesis for large composite TDES's is serious because of state explosion from system composition that is exacerbated by Moore TTG modeling. To graduate from theory to practice, future research will need to address and mitigate this problem in our real-time framework, by first considering more efficient and compact representations in place of (infinite node) reachability trees for the Moore system synthesis procedures conceptualized.

References

Alur R, Dill DL (1994) A theory of timed automata. Theoretical computer science 126(2):183–235

Brandin BA, Wonham WM (1994) Supervisory control of timed discrete-event systems. IEEE Transactions on Automatic Control 39(2):329–341

Brave Y, Heymann M (1988) Formulation and control of real time discrete event processes. In: Proceedings of the 27th IEEE International Conference on Decision and Control, Austin, Texas, U.S.A, pp 1131–1132

Cai K, Zhang R, Wonham WM (2014) On relative observability of timed discrete-event systems. In: Proceedings of the 12th International Workshop on Discrete-Event Systems, Cachan, France, pp 208–213

Cassandras CG (1993) Discrete Event Systems : Modeling and Performance Analysis. Richard D. Irwin, Inc., and Aksen Associates, Inc.

Cassandras CG, Lafortune S (2008a) Ch 2 : Languages and Automata. In: Introduction to Discrete Event Systems, 2nd edn, Springer-Verlag, New York, pp 53–132

Cassandras CG, Lafortune S (2008b) Introduction to Discrete Event Systems. Springer

Cofer DD, Garg VK (1996) Supervisory control of real-time discrete-event systems using lattice theory. IEEE Transactions on Automatic Control 41(2):199–209

Dhananjayan A, Seow KT (2014) A metric temporal logic specification interface for real-time discrete-event control. IEEE Transactions on Systems, Man and Cybernetics: Systems 44(9):1204–1215

Dhananjayan A, Seow KT (2015) A formal transparency framework for validation of real-time discrete-event control requirements modeled by timed transition graphs. IEEE Transactions on Human-Machine Systems 45(3):350–361

Eilenberg S (1974) Automata, Languages and Machines : Volume A. Academic Press, New York

Gohari P, Wonham WM (2003) Reduced supervisors for timed discrete-event systems. IEEE Transactions on Automatic Control 48(7):1187–1198

Ho TJ (2003) A method for the modular synthesis of controllers for timed discrete-event systems. International Journal of Control 76(5):520–535

Hopcroft JE, Ullman JD (1979) Introduction to Automata Theory, Languages and Computation. Reading, MA : Addison-Wesley

Knap SL (2001) Modelling and Control of Timed Discrete-Event Systems and its Applications to Scheduling. Doctor of Philosophy (Ph.D) Thesis, Department of Electrical and Computer Engineering, Queen's University at Kingston Kingston, Ontario, Canada

Lee EA (2009) Computing needs time. Communications of the ACM 52(5):70–79

Lee EA (2010) CPS foundations. In: Proceedings of the 47th Design Automation Conference (DAC 2010), ACM, pp 737–742

Lin F, Wonham WM (1995) Supervisory control of timed discrete-event systems under partial observation. IEEE Transactions on Automatic Control 40(3):558–562

Ma C, Wonham WM (2005) Nonblocking Supervisory Control of State Tree Structures. Lecture Notes in Control and Information Sciences, Vol 317. Springer-Verlag, New York

Ngo QH (2016) Discrete-Event System Abstractions for On-line Logical and Real-Time Hierarchical Control. Doctor of Philosophy (Ph.D) Thesis, School of Computer Science and Engineering, Nanyang Technological University, Singapore

Ngo QH, Seow KT (2014a) Command and control of discrete-event systems: Towards on-line hierarchical control based on feasible system decomposition. IEEE Transactions on Automation Science and Engineering 11(4):1218–1228

Ngo QH, Seow KT (2014b) A time fidelity control foundation for hierarchical discrete-event systems. In: Proceedings of the IEEE International Conference on Automation Science and Engineering (CASE'14), Taipei, Taiwan, pp 443–448

Nomura M, Takai S (2011) Decentralized supervisory control of timed discrete-event systems. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 94(12):2802–2809

Nomura M, Takai S (2013) A synthesis method for decentralized supervisors for timed discrete-event systems. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 96(4):835–839

Ostroff JS, Wonham WM (1990) A framework for real-time discrete event control. IEEE Transactions on Automatic Control 35(4):386–397

Park SJ, Cho KH (2008) Nonblocking supervisory control of timed discrete event systems under communication delays: The existence conditions. Automatica 44(4):1011–1019

Ramadge PJ, Wonham WM (1987) Supervisory control of a class of discrete event processes. SIAM Journal of Control and Optimization 25(1):206–230

Saadatpoor A (2009) Timed state tree structures: Supervisory control and fault diagnosis. Doctor of philosophy (ph.d) thesis, Graduate Department of Electrical and Computer Engineering, University of Toronto, Canada

Saadatpoor A, Wonham WM (2007) State based control of timed discrete event systems using binary decision diagrams. Systems & Control Letters 56(1):62–74

Saadatpoor A, Ma C, Wonham WM (2008) Supervisory control of timed state tree structures. In: Proceedings of the American Control Conference, Seattle, Washington, U.S.A, pp 477–482

Sadid WH, Hashtrudi-Zad S, Ricker SL (2014) Decentralized control of timed discrete-event systems under bounded delay communication. In: Proceedings of the IEEE Conference on Control Applications, Juan Les Antibes, France, pp 1795–1800

Schafaschek G, de Queiroz MH, Cury JER (2017) Local modular supervisory control of timed discrete-event systems. IEEE Transactions on Automatic Control 62(2):934–940

Wong KC, Wonham WM (1996) Hierarchical control of timed discrete-event systems. Discrete Event Dynamic Systems : Theory and Applications 6(3):275–306

Wong-Toi H, Hoffman G (1988) The control of dense real-time discrete event systems. In: Proceedings of the 30th IEEE International Conference on Decision and Control, Brighton, England, pp 1527–1528

Wonham WM (2016) Supervisory Control of Discrete-Event Systems. Systems Control Group, University of Toronto, Canada, http://www.control.toronto.edu/cgi-bin/dldes.cgi (Updated annually)

Zhang R, Cai K, Gan Y, Wang Z, Wonham WM (2013) Supervision localization of timed discrete-event systems. Automatica 49(9):2786–2794

Zhang R, Cai K, Wonham WM (2014) Delay-robustness in distributed control of timed discrete-event systems based on supervisor localization. In: Proceedings of the 53rd IEEE International Conference on Decision and Control, Los Angeles, CA, U.S.A, pp 6719 – 6724

Zhong H, Wonham WM (1989) Hierarchical control of discrete-event systems: Computation and examples. In: Proceedings of the 27th Annual Allerton Conference on Communication, Control, and Computing, University of Illinois, Champaign-Urbana, Illinois, U.S.A, pp 511–519

Zhong H, Wonham WM (1990) On the consistency of hierarchical supervision in discrete-event systems. IEEE Transactions on Automatic Control 35(10):1125–1134