Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005

# Synthesis of State Feedback Controllers for Parameterized Discrete Event Systems Under Partial Observation

Hans Bherer, Jules Desharnais, and Richard St-Denis

*Abstract*— **This paper considers the state feedback control of parameterized discrete event systems consisting of $N$ similar processes for the problem of maintaining a predicate on the state space of the system invariant under partial observation. The basic idea underlying the proposed approach consists in exploiting the symmetry of the system to be controlled, the symmetry of the mask, and the symmetry of the control specification, in order to avoid the exploration of the entire state space. It is shown that it suffices i) to synthesize off-line a controller for a small value ($n_0$) of the parameter $N$; and ii) to infer on-line the control for a larger system, consisting of an arbitrarily large number ($n$ with $n_0 \leq n$) of processes, from its current state and the small controller.**

## I. Introduction

In the last decade several approaches have been developed, in the context of the *Supervisory Control Theory* (SCT), to circumvent the state-space explosion problem, namely modular synthesis [1], on-line control [2], Petri nets [3], bisimulation [4], and symmetries and quotient structures [5], [6]. Recently, we have investigated a new approach in which the synthesis procedure of a state feedback control (SFBC) for a given discrete event system (DES) under complete observation relies on three main concepts introduced in the verification domain: *reduction*, *parameterization*, and *symmetry* [7]. It considers an uncontrolled parameterized discrete event system (PDES) $G^N$ —occasionally written $(G^N, x_0^N)$ to exhibit the initial state—, consisting of $N$ similar processes, and a parameterized predicate $Q^N$. A SFBC $f_A^{n_0}$ is synthesized off-line for an instance of $(G^N, Q^N)$ by using a typical synthesis algorithm, the parameter $N$ being substituted by a small value $n_0$. The SFBC $f_A^n$ for another instance of $(G^N, Q^N)$, with $n \geq n_0$, is computed on-line from $f_A^{n_0}$ and the current state of $G^n$ in the following way:

$$f_A^n(x) := \Sigma^n - \bigcup_{J \in \mathcal{J}_{n_0}^n} \theta_J^{-1}(\Sigma^{n_0} - f_A^{n_0}(\Theta_J x)), \qquad (1)$$

where $\Theta_J$ is the composition of a projection operator ($\uparrow_J$) and a substitution operator ($\theta_J$). The expression $\Sigma^{n_0} - f_A^{n_0}(\Theta_J x)$ denotes the set of disabled events in the system with $n_0$ processes, while $f_A^n(x)$ is the set of enabled events in state $x$ of the system with $n$ processes. The computational complexity for $f_A^{n_0}$ is still exponential with respect to $n_0$, but as $n_0$ is usually small this computational expense is totally acceptable. The computation of $f_A^n(\cdot)$ is tractable with worst case computational complexity in $O((n-n_0+1)^{n_0})$. As mentioned in [8], the only assumption needed is that the elapsed time-period between event occurrences be longer than the on-line computation time. These limitations are reasonable in systems whose events do not occur very frequently, or where computational resources are plentiful. The SFBC $f_A^n$ calculated in this way exhibits a form of *robustness*, because it can dynamically react to some perturbations (addition or deletion of a process) occurring in the controlled system by taking into account the number of processes that are alive. It could also be appropriate for reliable systems with many redundant components.

It is shown in [7] that this new synthesis method is *sound*, in the sense that if $f_A^{n_0}$ corresponds to the optimal (behaviorally least restrictive) SFBC for $((G^{n_0}, x_0'), Q^{n_0})$, then $f_A^n$ corresponds to the optimal SFBC for $((G^n, x_0), Q^n)$, for all $n \geq n_0$, under similarity assumptions and the condition that all events shared by all processes be controllable. However, this does not mean that the *controllability* property is preserved when the state space is expanded from dimension $n_0$ to dimension $n$. Recall that a predicate $Q$ on the state space $X$ is controllable if $Q$ is $\Sigma_u$*–invariant* and every state that satisfies $Q$ can be reached from the initial state via states satisfying $Q$ (*reachability*) [9]. Actually, the $\Sigma_u$–invariance property is preserved, but not the reachability property. This is formally expressed by the following inequalities:

$$\sup \mathcal{CP}(Q^n) \subseteq (\sup \mathcal{CP}(Q^{n_0}))^n \subseteq Q^n, \text{ where}$$

$(\sup \mathcal{CP}(Q^{n_0}))^n$ denotes the supremal controllable predicate stronger than $Q^{n_0}$ extended to the state space of dimension $n$. Nevertheless, this fact is unimportant, because each state for which $(\sup \mathcal{CP}(Q^{n_0}))^n$ holds, but $\sup \mathcal{CP}(Q^n)$ does not hold, is unreachable under the control of $f_A^n$. There are also counterexamples that show that the *nonblocking* property is not preserved.

This paper extends this approach to the case of partial observation. This particular case raises, however, new difficulties. On one hand, even though the supremal controllable and normal subpredicate always exists [10], the *normality* property is generally too restrictive for real systems. On the other hand, the notion of *strong M–controllability* [11], which is a stronger version of *M–controllability* [12] that ensures the existence of a supremal element $\sup \mathcal{SC}(Q)$, hides several pitfalls that have a significant impact on the goal of achieving optimality when the state space is expanded. First,

The research described in this paper was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Fonds québécois de la recherche sur la nature et les technologies (FQRNT).

H. Bherer and J. Desharnais are with the Département d'informatique et de génie logiciel, Université Laval, Québec, QC, Canada G1K 7P4 {Hans.Bherer, Jules.Desharnais}@ift.ulaval.ca

R. St-Denis is with the Département d'informatique, Université de Sherbrooke, Sherbrooke, QC, Canada J1K 2R1 Richard.St-Denis@USherbrooke.ca

0-7803-9568-9/05/$20.00 ©2005 IEEE

$\sup \mathcal{SC}(Q)$ can only be expressed in its simplest form as an iterative computational schema. Second, the notion of *strong M–controllability* includes a kind of reachability property, similar to the one for the notion of controllability, which cannot be preserved. Third, it also depends on the concept of *bad event set*, which merges together states that are observed in the same way, whether they satisfy the predicate $Q$ or not.

The rest of this paper is structured as follows. Section II presents an overview of the SFBC problem in the case of DESs under partial observation. Section III introduces the notation and basic definitions which are required to consider the SFBC problem in the case of PDESs under partial observation, and illustrates the synthesis procedure with the aid of a running example. Sections IV and V show that the on-line procedure is safe and maximal under some conditions, respectively. Finally, Section VI ends the paper with some concluding remarks and related work.

## II. Preliminaries

The concepts and results introduced in this section are part of the work originally developed by Ramadge and Wonham [1] and Li and Wonham [9], [13], [14], and later extended, among others, by Takai and Kodoma [11].

Let us assume that a DES is modeled by an automaton $G := (X, \Sigma, \delta, x_0, X_m)$, where $X$ is a finite set of states; $\Sigma$ is a finite set of events divided into two disjoint subsets $\Sigma_c$ and $\Sigma_u$ of controllable and uncontrollable events, respectively; $\delta : X \times \Sigma \to X$ is the partial transition function; $x_0$ is the initial state; and $X_m$ is the subset of marked states, which represents the completed tasks. It is assumed that $G$ is accessible, that is, all states are reachable from $x_0$ [11].

A SFBC for $G$ is a total function $f : X \to \Gamma$, where $\Gamma := \{\Sigma' \subseteq \Sigma \mid \Sigma' \supseteq \Sigma_u\}$. If $\sigma \in f(x)$, then $\sigma$ is *enabled* at $x$; otherwise, it is *disabled*. For $\sigma \in \Sigma$, the predicate $f_\sigma$ on $X$ is defined by $f_\sigma(x) :\Leftrightarrow \sigma \in f(x)$. Thus, $f$ may be described by a family of predicates $\{f_\sigma \mid \sigma \in \Sigma\}$.

Let $\delta(x,\sigma)!$ mean that $\delta(x,\sigma)$ is defined (for $s \in \Sigma^*$, $\delta(x,s)!$ is defined in the usual way and in particular $\delta(x,\epsilon)!$ always holds). The controller, represented by $f$, and the DES, represented by $G$, are embodied in a closed loop which is defined by $G^f := (X, \Sigma, \delta^f, x_0, X_m)$, where $\delta^f(x,\sigma) := \delta(x,\sigma)$ if $\delta(x,\sigma)!$ and $\sigma \in f(x)$, and is undefined otherwise. Let $Re(G|f)$ be the predicate that holds exactly at the reachable states in $G^f$, according to the inductive definition:

1) $Re(G|f)(x_0)$ holds;
2) $Re(G|f)(x) \wedge \sigma \in \Sigma \wedge \delta^f(x,\sigma)! \Rightarrow$ $Re(G|f)(\delta^f(x,\sigma))$;
3) no other states $x$ satisfy $Re(G|f)$.

When the states of the system are not completely observed, the state space $X$ is partitioned into a set $Y$ of equivalence classes, called observability classes [10]. The membership map $M : X \to Y$, called the *mask*, is defined as a mapping from the state space $X$ to the observation space $Y$. At the current state $x \in X$, the controller observes the value $M(x) \in Y$. In some examples presented in this paper, we denote the observability class of $x \in X$ by its representative element $x' \in X$ and simply write $M(x) = x'$.

Let $F_o$ be the set of SFBCs that satisfy the following assumption [10].

*Assumption 1:* Restriction of a SFBC to the observability classes — For any $x, x' \in X$,

$$M(x) = M(x') \Rightarrow f(x) = f(x').$$

In this context, a state feedback controller $f \in F_o$ selects a control pattern $f(x)$ based on $M(x)$.

Let $\mathrm{Pred}(X) = \{\mathsf{true}, \mathsf{false}\}^X$ be the set of all predicates on the state space $X$. A predicate $Q$ generally represents the control specification to be fulfilled. A partial order on $\mathrm{Pred}(X)$ is defined as follows[1]:

$$Q_1 \le Q_2 :\Leftrightarrow (\forall x \mid x \in X : Q_1(x) \Rightarrow Q_2(x)).$$

For a fixed $\sigma \in \Sigma$, the predicate transformer $\mathrm{wlp}_\sigma : \mathrm{Pred}(X) \to \mathrm{Pred}(X)$ is defined by

$$\mathrm{wlp}_\sigma(Q)(x) :\Leftrightarrow (\neg\delta(x,\sigma)! \vee Q(\delta(x,\sigma))).$$

The predicate transformer $\mathrm{wlp}^f_\sigma$ is defined like $\mathrm{wlp}_\sigma$, but with $\delta^f$ instead of $\delta$. The predicate transformer $\langle\cdot\rangle : \mathrm{Pred}(X) \to \mathrm{Pred}(X)$ is defined by

$$\langle Q\rangle(x) :\Leftrightarrow (\forall s \mid s \in \Sigma_u^* : \neg\delta(x,s)! \vee Q(\delta(x,s))).$$

It is worth noting that the predicate transformer $\langle\cdot\rangle$ is idempotent. Finally, for each $y \in Y$, the bad event set $\hat{A}(Q,y) \subseteq \Sigma_c$ is defined by [11]

$$\begin{aligned}\hat{A}(Q,y) \quad := \quad & \{\sigma \in \Sigma_c \mid (\exists x \mid x \in X : y = M(x) \wedge \\ & \qquad \neg\mathrm{wlp}_\sigma(Q)(x))\}.\end{aligned}$$

The function $\hat{A}$ is antimonotone with respect to its first argument, that is,

$$Q_1 \le Q_2 \Rightarrow \hat{A}(Q_2,y) \subseteq \hat{A}(Q_1,y). \tag{2}$$

In order to deal with the predicate invariant control problem formulated in the framework of SCT, the property of control-invariance has been introduced [1]. A predicate $Q \in \mathrm{Pred}(X)$ is *control-invariant* with respect to $G$ if, for some SFBC $f$, $Q \le \mathrm{wlp}^f_\sigma(Q)$ for all $\sigma \in \Sigma$. A feedback independent characterization of the control-invariance property is $\Sigma_u$-invariance. A predicate $Q \in \mathrm{Pred}(X)$ is $\Sigma_u$*-invariant* with respect to $G$ if $Q \le \mathrm{wlp}_\sigma(Q)$ for all $\sigma \in \Sigma_u$. As shown in [1], a predicate $Q$ is control-invariant if and only if $Q$ is $\Sigma_u$-invariant.

When $Q \ne \mathsf{false}$ is $\Sigma_u$-invariant, a SFBC $f$ such that $Re(G|f) \le Q$ is given by $(\forall\sigma \mid \sigma \in \Sigma_c : f_\sigma(x) \Leftrightarrow \sigma \notin \hat{A}(Q, M(x)))$. If $Q$ fails to be $\Sigma_u$-invariant, following the conventional procedure [1], $\sup \mathcal{CI}_<(Q)$ is then targeted, where

$$\begin{aligned}\mathcal{CI}_<(Q) \quad := \quad & \{Q' \in \mathrm{Pred}(X) \mid Q' \le Q \\ & \text{and } Q' \text{ is } \Sigma_u\text{-invariant}\}.\end{aligned}$$

[1] Quantifications have the form (*quantifier bound variable* | *range restriction* : *quantified expression*) (see, *e.g.*, [15]); an empty range in a quantification means that the bound variable ranges over all possible values. $(\exists x \mid P : Q)$ is read as there exists $x$ such that $P$ and $Q$. $(\forall x \mid P : Q)$ is read as for all $x$ such that $P$, $Q$ holds or as for all $x$, $P$ implies $Q$.

Based on antimonotonicity, defined by Equation 2, the behaviorally least restrictive SFBC $f^*$ is synthesized. For all $\sigma \in \Sigma_c$, $f^*_\sigma(x) :\Leftrightarrow \sigma \notin \hat{A}(\nu H, M(x))$, where $\nu H$ is the greatest fixed point of the function $H : \mathrm{Pred}(X) \to \mathrm{Pred}(X)$ defined by

$$H(T) := Q \;\wedge \bigwedge_{\sigma\in\Sigma_u} \mathrm{wlp}_\sigma(T)$$

(see [1], [16], and [17]). The following proposition shows that the greatest fixed point of $H$ is $\langle Q\rangle$.

*Proposition 1:* $\nu H = \langle Q\rangle$.

*Proof:* By a standard result of lattice theory [18], it suffices to show (i) $\langle Q\rangle \leq H(\langle Q\rangle)$ and (ii) for any $U \in \mathrm{Pred}(X)$, $U \leq H(U)$ implies $U \leq \langle Q\rangle$.

(i) Let $x \in X$ and suppose that $\langle Q\rangle(x)$ holds. Then $Q(x)$ must hold. Since $\langle\cdot\rangle$ is idempotent and $\Sigma_u \subseteq \Sigma_u^*$, $\left(\bigwedge_{\sigma\in\Sigma_u} \mathrm{wlp}_\sigma(\langle Q\rangle)\right)(x)$ also holds. This shows that $\langle Q\rangle \leq Q \wedge \bigwedge_{\sigma\in\Sigma_u} \mathrm{wlp}_\sigma(\langle Q\rangle) = H(\langle Q\rangle)$.

(ii) Suppose $U \leq H(U)$. We have to show $U \leq \langle Q\rangle$. So, assume $U(x)$. We show $\langle Q\rangle(x)$ by proving that if $\delta(x,s)!$, then $Q(\delta(x,s))$, for any $s \in \Sigma_u^*$. Because $U \leq H(U) \leq Q$, it suffices to prove that if $\delta(x,s)!$, then $U(\delta(x,s))$, for any $s \in \Sigma_u^*$.
Base case, $s = \epsilon$: This is direct by $U(x) \Leftrightarrow U(\delta(x,\epsilon))$.
Induction step: Let $s = t\sigma$, for some $t \in \Sigma_u^*$ and $\sigma \in \Sigma_u$. Assume $\delta(x,s)!$. Then, $\delta(x,t)!$, so that, by the induction hypothesis, $U(\delta(x,t))$. Because $U \leq H(U) \leq \mathrm{wlp}_\sigma(U)$, we then have $U(\delta(\delta(x,t),\sigma))$, that is, $U(\delta(x,s))$.

■

The following proposition states that if no sequence of uncontrollable events leading to a state violating $Q$ can occur in the initial state, then the same thing is true of all the states reachable under the control of $f^*$.

*Proposition 2:* If $\langle Q\rangle(x_0)$ holds then

$$Re(G|f^*) \leq \langle Q\rangle \leq Q.$$

*Proof:* See [12] for the first inequality. The second inequality follows directly from the definition of $\langle\cdot\rangle$. ■

## III. Notation and Definitions

Let us consider a PDES $G^N$, where $N$ is a parameter that denotes the number of processes, defined from the finite composition of a replicated structure

$$P_i := (X_i, \Sigma \cup \Sigma_i, \delta_i, X_{m,i}),$$

where $X_i$ is a finite set of indexed states; $\Sigma$ is a finite set of non-indexed, controllable events; $\Sigma_i$ is a finite set of indexed events, $\Sigma_i = \Sigma_{c,i} \cup \Sigma_{u,i}$; $\delta_i : X_i \times (\Sigma \cup \Sigma_i) \to X_i$ is the partial transition function; and $X_{m,i}$ is the subset of marked states. The replicated structure represents the behavior of similar processes. The parameter $N$ can be substituted by any number $n \in \mathbb{N}$. The events that belong to $\Sigma$ are shared by all processes and allow synchronization.

The concept of *replicated structure* is translated into a *process similarity assumption* [19]. Formally, let $\theta := \langle j/i\rangle$ be a substitution such that $i.\theta = j$ $(1 \leq i, j \leq N)$.

*Assumption 2:* Process Similarity Assumption (PSA) — $(\forall i, j \mid 1 \leq i, j \leq N : P_j = P_i.\theta)$, where

$$\begin{array}{rcl}
P_i.\theta & := & (X_i.\theta, \Sigma \cup \Sigma_{c,i}.\theta \cup \Sigma_{u,i}.\theta, \delta_i.\theta, X_{m,i}.\theta);\\
X_i.\theta & := & X_{i.\theta} := \{x_{i.\theta} \mid x_i \in X_i\};\\
\Sigma_{c,i}.\theta & := & \Sigma_{c,i.\theta} := \{\sigma_{i.\theta} \mid \sigma_i \in \Sigma_{c,i}\};\\
\Sigma_{u,i}.\theta & := & \Sigma_{u,i.\theta} := \{\sigma_{i.\theta} \mid \sigma_i \in \Sigma_{u,i}\};\\
\delta_i.\theta & := & \delta_{i.\theta} :=\\
 & & \{(x_{i.\theta}, \sigma, x'_{i.\theta}) \mid \sigma \in \Sigma \wedge (x_i, \sigma, x'_i) \in \delta_i\} \cup\\
 & & \{(x_{i.\theta}, \sigma_{i.\theta}, x'_{i.\theta}) \mid \sigma_i \in \Sigma_i \wedge (x_i, \sigma_i, x'_i) \in \delta_i\};\\
X_{m,i}.\theta & := & X_{m,i.\theta} := \{x_{i.\theta} \mid x_i \in X_{m,i}\}.
\end{array}$$

Therefore, a process can be derived from any other process by index substitution. A global state $x \in X^N$ is represented by a tuple of $N$ local states. Let $x[i]$ denote the $i$-th component of $x$. The transition structure $G^N$ is defined from a synchronous composition for events in $\Sigma$ and an interleaving composition for events in each $\Sigma_i$. Thus, $G^N := (X^N, \Sigma^N, \delta^N, X_m^N)$, where $\Sigma^N = \Sigma \cup \Sigma_1 \cup \cdots \cup \Sigma_N$ and $(\delta^N(x,\sigma))[i] = \delta_i(x[i], \sigma)$ if $\sigma \in \Sigma \cup \Sigma_i$ and $(\delta^N(x,\sigma))[i] = x[i]$ otherwise. An instance of a PDES, $G^N$, is denoted by $(G^n, x_0)$, where $x_0 \in X^n$ is the initial state.

*Definition 1:* Let $x := \langle x[1], x[2], \ldots, x[n]\rangle \in X^n$. Then $M^n(x) := \langle M_1(x[1]), M_2(x[2]), \ldots, M_n(x[n])\rangle$, where $M_i : X_i \to Y_i$ is the mask for process $i$.

*Example 1:* Consider a unidirectional rectangular railway with $N$ trains. The track is divided into ten different sections. The train $i$ in section $k$, $0 \leq k \leq 9$, is represented by a state $s_{k,i}$ and the passage of train $i$ from section $k$ to the adjacent section $k \oplus 1$ by the event $s_kTOs_{k\oplus 1}\_t_i$, where $k \oplus 1 = (k+1) \bmod 10$. Formally, $\delta_i(s_{k,i}, s_kTOs_{k\oplus 1}\_t_i) = s_{k\oplus 1,i}$. The events $s_kTOs_{k\oplus 1}\_t_i$, with $k$ odd, are controllable.

The mask function is derived from the fact that sections 2 and 3 are in a tunnel and sections 7 and 8 are in another tunnel.

$$M_i(s_{k,i}) = \left\{\begin{array}{lcl} s_{k,i} & : & k \in \{0,1,4,5,6,9\}\\ T_{1,i} & : & k \in \{2,3\}\\ T_{2,i} & : & k \in \{7,8\}\end{array}\right.$$

The replicated structure for train number $i$ is depicted in Fig. 1. □

*Definition 2:* Let $n_0, n \in \mathbb{N}$, where $n_0 \leq n$, $\mathcal{J}^n_{n_0} := \{J \mid (\exists j_1, \ldots, j_{n_0} \mid J = \{j_1, \ldots, j_{n_0}\} : 1 \leq j_1 < j_2 < \cdots < j_{n_0} \leq n)\}$.

*Definition 3:* Let $J \in \mathcal{J}^n_{n_0}$ (in the sequel, the expression "Let $J \in \mathcal{J}^n_{n_0}$" means "Let $J = \{j_1, \ldots, j_{n_0}\}$ and $1 \leq j_1 < \cdots < j_{n_0} \leq n$"). The projection operator $\uparrow_J$ on a global state $x \in X^n$ is a function $\uparrow_J : X^n \to X_{j_1} \times \cdots \times X_{j_{n_0}}$ that is defined as $\uparrow_J x := \langle x[j_1], \ldots, x[j_{n_0}]\rangle$.

*Definition 4:* Let $J \in \mathcal{J}^n_{n_0}$. The substitution operator $\theta_J$ on a state $x \in X_{j_1} \times \cdots \times X_{j_{n_0}}$ is a function $\theta_J : X_{j_1} \times \cdots \times X_{j_{n_0}} \to X^{n_0}$ that expresses the simultaneous replacement of process indices $j_1, \ldots, j_{n_0}$ by process indices $1, \ldots, n_0$, respectively. It is defined as $\theta_J x := \langle x[1]_{.\langle 1/j_1\rangle}, \ldots, x[n_0]_{.\langle n_0/j_{n_0}\rangle}\rangle$ (writing the substitutions as subscripts emphasizes the fact that they are to be applied to indices).

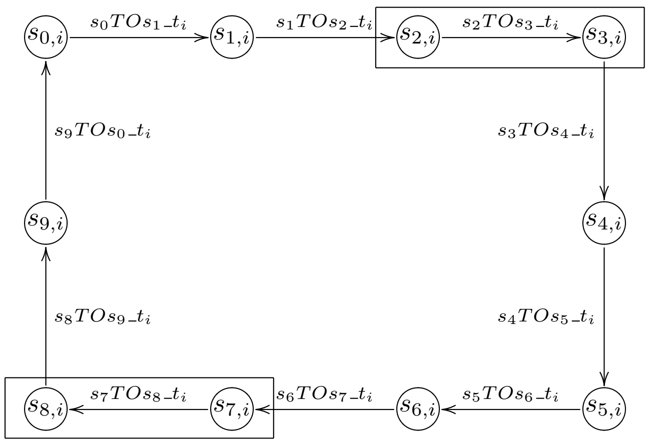

Fig. 1. Replicated structure for train number $i$

*Definition 5:* Let $J \in \mathcal{J}^n_{n_0}$. The projection operator $\uparrow_J$ on an event $\sigma \in \Sigma^n$ is a function $\uparrow_J : \Sigma^n \to \Sigma \cup \Sigma_{j_1} \cup \cdots \cup \Sigma_{j_{n_0}} \cup \{\epsilon\}$ that is defined as follows: $\uparrow_J \sigma := \sigma$, if $\sigma \in \Sigma$ or $\sigma \in \Sigma_i$ and $i \in J$; and $\uparrow_J \sigma := \epsilon$, if $\sigma \in \Sigma_i$ and $i \notin J$.

*Definition 6:* Let $J \in \mathcal{J}^n_{n_0}$. The substitution operator $\theta_J$ on an event $\sigma \in \Sigma \cup \Sigma_{j_1} \cup \cdots \cup \Sigma_{j_{n_0}} \cup \{\epsilon\}$ is a function $\theta_J : \Sigma \cup \Sigma_{j_1} \cup \cdots \cup \Sigma_{j_{n_0}} \cup \{\epsilon\} \to \Sigma^{n_0} \cup \{\epsilon\}$ that is defined as $\theta_J\sigma := \sigma$, if $\sigma \in \Sigma$; $\theta_J\sigma := \sigma_{.\langle k/j_k \rangle}$ if $\sigma \in \Sigma_{j_k}$ and $j_k \in J$; and $\theta_J\epsilon := \epsilon$.

*Definition 7:* Let $\Omega \subseteq \Sigma^n$ and $J \in \mathcal{J}^n_{n_0}$. The operator $\theta_J$ on a set of events is a function $\theta_J : 2^{\Sigma^n} \to 2^{\Sigma^{n_0} \cup \{\epsilon\}}$ defined by $\theta_J\Omega := \{\theta_J\sigma \mid \sigma \in \Omega\}$.

Let $\Theta_J := \theta_J \circ \uparrow_J$. If $x \in X^n$, $\Theta_J x$ is well defined and $\Theta_J : X^n \to X^{n_0}$. Furthermore, if $\sigma \in \Sigma^n$, $\Theta_J\sigma$ is well defined and $\Theta_J : \Sigma^n \to \Sigma^{n_0} \cup \{\epsilon\}$.

*Definition 8:* Let $J \in \mathcal{J}^n_{n_0}$. The operator $\Theta_J$ on a string of events is a function $\Theta_J : (\Sigma^n)^* \to (\Sigma^{n_0})^*$ that is recursively defined as follows: $\Theta_J\epsilon := \epsilon$ and $\Theta_J s\sigma := (\Theta_J s)(\Theta_J\sigma)$, where $\sigma \in \Sigma^n$ and $s \in (\Sigma^n)^*$.

*Example 2:* Let $n_0 = 2$, $n = 4$, and consider the train system introduced in Example 1. Let $x = \langle s_{1,1}, s_{3,2}, s_{6,3}, s_{9,4} \rangle$ and $s = s_6TOs_7\_t_3 \cdot s_3TOs_4\_t_2 \cdot s_1TOs_2\_t_1$. If $J = \{2, 4\}$, then $\Theta_J x = \langle s_{3,1}, s_{9,2} \rangle$ and $\Theta_J s = s_3TOs_4\_t_1$. □

*Remark 1:* Let $s \in (\Sigma^{n_0})^*$, $J \in \mathcal{J}^n_{n_0}$, and $\theta_J = \{1/j_1, \ldots, n_0/j_{n_0}\}$. Then $\theta_J^{-1}s$ exists, since $\theta_J^{-1} = \{j_1/1, \ldots, j_{n_0}/n_0\}$. Also, $\Theta_J(\theta_J^{-1}s) = \theta_J(\theta_J^{-1}s) = s$. It should be noted that an element of $(\Sigma^{n_0})^*$ is also an element of $(\Sigma^n)^*$.

A SFBC is synthesized from a particular instance of $G^N$, say $G^n$, and a control specification. The latter can be given in two ways: i) by a parameterized predicate $Q^N \in \mathrm{Pred}(X^N)$ or ii) by a predicate $Q^{n_0} \in \mathrm{Pred}(X^{n_0})$ with $n_0 \leq n$. In the first case, $Q^{n_0}$ and $Q^n$ are instances of $Q^N$. In the second case $Q^n$ is deduced from $Q^{n_0}$ by similarity. In both cases, $Q^{n_0}$ and $Q^n$ must satisfy the following similarity assumption.

*Assumption 3:* Specification Similarity Assumption (SSA) — Let $x \in X^n$. The assumption is

$$Q^n(x) \Leftrightarrow (\forall J \mid J \in \mathcal{J}^n_{n_0} : Q^{n_0}(\Theta_J x)).$$

Intuitively, SSA imposes the following restriction to a predicate $Q^n$: a state $x \in X^n$ of the global system satisfies $Q^n$ if and only if all the projections of $x$ on the state space of dimension $n_0$ satisfy $Q^{n_0}$.

*Example 3:* The behavior of the trains must be restrained to prevent the trains from colliding. Therefore, any two trains must be separated by at least one section to ensure that an incoming train can stop at a proper distance. This constraint is formally defined by the following predicate:

$$\begin{aligned} Q^N(x) \quad \Leftrightarrow \quad & (\forall i, j \mid 1 \leq i, j \leq N \land i \neq j : \\ & \neg(x[i] = s_{k,i} \land x[j] = s_{k,j}) \land \\ & \neg(x[i] = s_{k,i} \land x[j] = s_{k \oplus 1, j})). \end{aligned}$$

This predicate satisfies SSA, with $n_0 = 2$. □

The mask must also satisfy a similarity assumption.

*Assumption 4:* Mask Similarity Assumption (MSA) — Let $y \in Y^n$ and $x \in X^n$. The assumption is

$$y = M^n(x) \Leftrightarrow (\forall J \mid J \in \mathcal{J}^n_{n_0} : \Theta_J y = M^{n_0}(\Theta_J x)).$$

Intuitively, MSA ensures that the mask is the same for every independent process of the global system up to index substitution.

As mentioned in the introduction, the synthesis method includes two parts: an off-line synthesis and an on-line synthesis.

The off-line synthesis consists in calculating a SFBC $f^{n_0}_A$, with respect to $Q^{n_0}$, $M^{n_0}$, and $(G^{n_0}, x_0)$, where $x_0 \in X^{n_0}$, such that $Re(G^{n_0}|f^{n_0}_A) \leq \sup\mathcal{CI}_<(Q^{n_0})$. In general, this problem is undecidable, but it can be solved, by using an appropriate synthesis algorithm that mechanically constructs a correct solution and ensures that $f^{n_0}_A \in F^{n_0}_o$, for some particular forms of predicates (*e.g.*, predicates represented by a set of forbidden states, linear predicates).

*Example 4:* For the trains example, the SFBC $f^2_A$ has been synthesized. In order to present the results in a concise form, let $\overline{f}^N_A(\cdot) := \Sigma^N - f^N_A(\cdot)$ be the set of prohibited controllable events. Here are some entries for $\overline{f}^2_A$.

| | | | | | |
|---|---|---|---|---|---|
| $\langle s_{2,1}, s_{5,2} \rangle$ | : | $\{s_3TOs_4\_t_1\}$ | $\langle s_{3,1}, s_{5,2} \rangle$ | : | $\{s_3TOs_4\_t_1\}$ |
| $\langle s_{2,1}, s_{9,2} \rangle$ | : | $\{s_9TOs_0\_t_2\}$ | $\langle s_{3,1}, s_{9,2} \rangle$ | : | $\{s_9TOs_0\_t_2\}$ |
| $\langle s_{5,1}, s_{9,2} \rangle$ | : | $\{\ \}$ | $\langle s_{7,1}, s_{9,2} \rangle$ | : | $\{s_7TOs_8\_t_1\}$ |

□

From now on, we assume that the algorithm used to compute the nonprohibited events in the system with $n_0$ processes is optimal. That is, we assume $f^{n_0}_A = f^{n_0 *}$. The on-line synthesis of $f^n_A \in F^n_o$ in the context of partial observation is done by using the following equation. It is similar to Equation 1, with an additional term.

$$\begin{aligned} f^n_A(x) := \Sigma^n - & \\ & \textstyle\bigcup_{J \in \mathcal{J}^n_{n_0}} \Big( \theta_J^{-1}(\Sigma^{n_0} - f^{n_0 *}(\Theta_J x)) \cup \\ & \{\sigma \in \Sigma^n_c \mid \Theta_J\sigma = \epsilon \land (\exists x' \mid x' \in X^{n_0} : \\ & M^{n_0}(\Theta_J x) = M^{n_0}(x') \land \neg\langle Q^{n_0}\rangle(x'))\}\Big) \end{aligned} \tag{3}$$

The term $\theta_J^{-1}(\Sigma^{n_0} - f^{n_0*}(\Theta_J x))$ yields events that are prohibited because they occur in a projection $J$ for which they may lead (as determined by observing under the mask) to a state violating $\langle Q^n \rangle$, either directly or after transitions by uncontrollable events.

The other term (the one inside $\{\}$) contains events not occurring in the projection $J$ that is considered, but that must nevertheless be prohibited because the projection of the state on $J$ is in an observability class that contains a state $x'$ that is not safe (that does not satisfy $\langle Q^{n_0} \rangle$). Because the event does not occur in the projection $J$, the $J$-component of $x'$ is not changed by the transition and so does not satisfy $\langle Q^{n_0} \rangle$ after the transition.

The computational complexity is still in $O((n-n_0+1)^{n_0})$ because the additional term (with respect to Equation 1) can be calculated in a constant time for a given $J$ as far as the information required in the lower space of dimension $n_0$ is precomputed before system execution.

*Example 5:* This example shows how $\overline{f}_A^3(\langle s_{2,1}, s_{5,2}, s_{9,3} \rangle)$ is calculated.

$$\begin{array}{rcl}
\overline{f}_A^3(\langle s_{2,1}, s_{5,2}, s_{9,3} \rangle) & = & \theta_{\{1,2\}}^{-1} \overline{f}_A^{2*}(\Theta_{\{1,2\}} \langle s_{2,1}, s_{5,2}, s_{9,3} \rangle) \\
& & \cup \\
& & \theta_{\{1,3\}}^{-1} \overline{f}_A^{2*}(\Theta_{\{1,3\}} \langle s_{2,1}, s_{5,2}, s_{9,3} \rangle) \\
& & \cup \\
& & \theta_{\{2,3\}}^{-1} \overline{f}_A^{2*}(\Theta_{\{2,3\}} \langle s_{2,1}, s_{5,2}, s_{9,3} \rangle) \\
& = & \theta_{\{1,2\}}^{-1} \overline{f}_A^{2*}(\langle s_{2,1}, s_{5,2} \rangle) \cup \\
& & \theta_{\{1,3\}}^{-1} \overline{f}_A^{2*}(\langle s_{2,1}, s_{9,2} \rangle) \cup \\
& & \theta_{\{2,3\}}^{-1} \overline{f}_A^{2*}(\langle s_{5,1}, s_{9,2} \rangle) \\
& = & \theta_{\{1,2\}}^{-1} \{s_3 TO s_4\_t_1\} \cup \\
& & \theta_{\{1,3\}}^{-1} \{s_9 TO s_0\_t_2\} \cup \theta_{\{2,3\}}^{-1} \{\ \} \\
& = & \{s_3 TO s_4\_t_1\} \cup \{s_9 TO s_0\_t_3\} \\
& = & \{s_3 TO s_4\_t_1, s_9 TO s_0\_t_3\}.
\end{array}$$

In this example, because all projections of $\langle s_{2,1}, s_{5,2}, s_{9,3} \rangle$ belong to a safe observability class, no forbidden event is due to the additional term in (3). □

## IV. Soundness of the Synthesis Method

Many relationships may be established between a system of $n$ processes and a system of $n_0$ processes under the assumptions PSA, MSA, and SSA. Some of them are presented in this section, especially those required to prove the soundness of the synthesis method.

*Lemma 1:* Let $x \in X^n$ and $J \in \mathcal{J}_{n_0}^n$. Then
$$M^{n_0}(\Theta_J x) = \Theta_J M^n(x).$$

*Lemma 2:* Let $x \in X^n$, $\sigma \in \Sigma^n$, and $J \in \mathcal{J}_{n_0}^n$.
If $\delta^n(x, \sigma)!$, then $\delta^{n_0}(\Theta_J x, \Theta_J \sigma) = \Theta_J \delta^n(x, \sigma)$.

*Lemma 3:* Let $x \in X^n$, $s \in (\Sigma^n)^*$, and $J \in \mathcal{J}_{n_0}^n$.
If $\delta^n(x, s)!$, then $\delta^{n_0}(\Theta_J x, \Theta_J s) = \Theta_J \delta^n(x, s)$.

*Lemma 4:* Let $x \in X^n$ and $\sigma \in \Sigma^n$. Then
$$\delta^n(x, \sigma)! \Leftrightarrow (\forall J \mid J \in \mathcal{J}_{n_0}^n : \delta^{n_0}(\Theta_J x, \Theta_J \sigma)!).$$

*Lemma 5:* Let $x \in X^n$ and $s \in (\Sigma^n)^*$. Then
$$\delta^n(x, s)! \Leftrightarrow (\forall J \mid J \in \mathcal{J}_{n_0}^n : \delta^{n_0}(\Theta_J x, \Theta_J s)!).$$

The following proposition establishes that the predicate $\langle Q^n \rangle$ satisfies the assumption SSA [7].

*Proposition 3:* Let $x \in X^n$. Then
$$\langle Q^n \rangle(x) \Leftrightarrow (\forall J \mid J \in \mathcal{J}_{n_0}^n : \langle Q^{n_0} \rangle(\Theta_J x)).$$

*Proof:* The ($\Rightarrow$) part: The proof is by contraposition. Suppose that there exists a $J \in \mathcal{J}_{n_0}^n$ for which $\langle Q^{n_0} \rangle(\Theta_J x)$ does not hold. Then, there must exist $s \in (\Sigma_u^{n_0})^*$ and $x' := \delta^{n_0}(\Theta_J x, s)$ for which $Q^{n_0}(x')$ does not hold (definition of $\langle Q^{n_0} \rangle$). Let $x'' = \delta^n(x, \theta_J^{-1} s)$. Assumption 2 (PSA) ensures that $x''$ is well defined (note that if uncontrollable synchronous events were allowed, this would not be true; $n_0$ processes might be able to synchronize while $n$ processes might not). Since $x' = \Theta_J x''$ and $Q^{n_0}(x')$ does not hold, Assumption 3 (SSA) implies that $Q^n(x'')$ does not hold either, which in turn implies that $\langle Q^n \rangle(x)$ does not hold, because $\theta_J^{-1} s \in (\Sigma_u^n)^*$.

The ($\Leftarrow$) part:

$$\begin{array}{cl}
& (\forall J \mid J \in \mathcal{J}_{n_0}^n : \langle Q^{n_0} \rangle(\Theta_J x)) \\
= & (\forall J \mid J \in \mathcal{J}_{n_0}^n : (\forall w \mid w \in (\Sigma_u^{n_0})^* : \\
& \delta^{n_0}(\Theta_J x, w)! \Rightarrow \\
& Q^{n_0}(\delta^{n_0}(\Theta_J x, w)))) \qquad \text{(def. of } \langle\cdot\rangle\text{)} \\
= & (\forall J \mid J \in \mathcal{J}_{n_0}^n : (\forall w \mid \Theta_J(\theta_J^{-1} w) \in (\Sigma_u^{n_0})^* : \\
& \delta^{n_0}(\Theta_J x, \Theta_J(\theta_J^{-1} w))! \Rightarrow \\
& Q^{n_0}(\delta^{n_0}(\Theta_J x, \Theta_J(\theta_J^{-1} w))))) \qquad \text{(Remark 1)} \\
= & (\forall J \mid J \in \mathcal{J}_{n_0}^n : (\forall s \mid \Theta_J s \in (\Sigma_u^{n_0})^* : \\
& \delta^{n_0}(\Theta_J x, \Theta_J s)! \Rightarrow Q^{n_0}(\delta^{n_0}(\Theta_J x, \Theta_J s)))) \\
& \text{(changing dummy, } s = \theta_J^{-1} w \Leftrightarrow w = \theta_J s\text{)} \\
\Rightarrow & (\forall J \mid J \in \mathcal{J}_{n_0}^n : (\forall s \mid s \in (\Sigma_u^n)^* : \\
& \delta^{n_0}(\Theta_J x, \Theta_J s)! \Rightarrow Q^{n_0}(\delta^{n_0}(\Theta_J x, \Theta_J s)))) \\
& \text{(by Def. 8: } \Theta_J s \in (\Sigma_u^{n_0})^* \Leftrightarrow s \in (\Sigma_u^n)^*\text{)} \\
= & (\forall s \mid s \in (\Sigma_u^n)^* : (\forall J \mid J \in \mathcal{J}_{n_0}^n : \\
& \delta^{n_0}(\Theta_J x, \Theta_J s)! \Rightarrow Q^{n_0}(\delta^{n_0}(\Theta_J x, \Theta_J s)))) \\
& \text{(exchanging quantifiers)} \\
\Rightarrow & (\forall s \mid s \in (\Sigma_u^n)^* : \\
& (\forall J \mid J \in \mathcal{J}_{n_0}^n : \delta^{n_0}(\Theta_J x, \Theta_J s)!) \Rightarrow \\
& (\forall J \mid J \in \mathcal{J}_{n_0}^n : Q^{n_0}(\delta^{n_0}(\Theta_J x, \Theta_J s)))) \\
& (\forall\text{-monotonicity}) \\
= & (\forall s \mid s \in (\Sigma_u^n)^* : \delta^n(x, s)! \Rightarrow Q^n(\delta^n(x, s))) \\
& \text{(Lemmas 3, 5, and SSA)} \\
= & \langle Q^n \rangle(x) \qquad \text{(def. of } \langle\cdot\rangle\text{).}
\end{array}$$

■

The following proposition gives another expression for $f_A^n$. This is mainly for use in the proof of Theorem 1, but it also reveals something that is not apparent in the definition of $f_A^n$ (Equation 3). We consider that $f_A^n$ is (a specification of) the algorithm for computing enabled events under partial observation, but in (3), it seems that the algorithm uses the system state $x$, which it is not supposed to see. In the following proposition, the expression of $f_A^n$ clearly shows that only the observed $M^n(x)$ is needed.

*Proposition 4:* Let $x \in X^n$. Then

$$\begin{aligned}
&f_A^n(x) = \Sigma_u^n \cup \Big\{\sigma \mid \sigma \in \Sigma_c^n \wedge \\
&(\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : \Theta_J\sigma \notin \hat{A}(\langle Q^{n_0}\rangle, \Theta_J M^n(x))) \\
&\wedge (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&(\forall x' \mid x' \in X^{n_0} \wedge \Theta_J M^n(x) = M^{n_0}(x') : \langle Q^{n_0}\rangle(x')))\Big\}
\end{aligned}$$

*Proof:*

$$\begin{aligned}
&f_A^n(x) \\
&= \Sigma^n - \bigcup_{J\in\mathcal{J}_{n_0}^n} \Big(\theta_J^{-1}(\Sigma^{n_0} - f^{n_0*}(\Theta_J x)) \cup \\
&\qquad \{\sigma \in \Sigma_c^n \mid \Theta_J\sigma = \epsilon \wedge (\exists x' \mid x' \in X^{n_0} : \\
&\qquad M^{n_0}(\Theta_J x) = M^{n_0}(x') \wedge \neg\langle Q^{n_0}\rangle(x'))\}\Big) && \text{(Eq. 3)} \\
&= \Sigma^n - \bigcup_{J\in\mathcal{J}_{n_0}^n} \Big(\{\theta_J^{-1}\sigma' \mid \sigma' \in \Sigma^{n_0} \wedge \neg f_{\sigma'}^{n_0*}(\Theta_J x)\} \cup \\
&\qquad \{\sigma \in \Sigma_c^n \mid \Theta_J\sigma = \epsilon \wedge (\exists x' \mid x' \in X^{n_0} : \\
&\qquad M^{n_0}(\Theta_J x) = M^{n_0}(x') \wedge \neg\langle Q^{n_0}\rangle(x'))\}\Big) \\
&&& \text{(def. of } f_\sigma \text{ and Def. 7)} \\
&= \Sigma^n - \bigcup_{J\in\mathcal{J}_{n_0}^n} \Big(\{\sigma \mid \theta_J\sigma \in \Sigma^{n_0} \wedge \neg f_{\theta_J\sigma}^{n_0*}(\Theta_J x)\} \cup \\
&\qquad \{\sigma \in \Sigma_c^n \mid \Theta_J\sigma = \epsilon \wedge (\exists x' \mid x' \in X^{n_0} : \\
&\qquad M^{n_0}(\Theta_J x) = M^{n_0}(x') \wedge \neg\langle Q^{n_0}\rangle(x'))\}\Big) \\
&&& \text{(changing dummy, Remark 1)} \\
&= \Sigma^n - \bigcup_{J\in\mathcal{J}_{n_0}^n} \Big(\{\sigma \mid \Theta_J\sigma \neq \epsilon \wedge \neg f_{\Theta_J\sigma}^{n_0*}(\Theta_J x)\} \cup \\
&\qquad \{\sigma \mid \sigma \in \Sigma_c^n \wedge \Theta_J\sigma = \epsilon \wedge (\exists x' \mid x' \in X^{n_0} : \\
&\qquad M^{n_0}(\Theta_J x) = M^{n_0}(x') \wedge \neg\langle Q^{n_0}\rangle(x'))\}\Big) \\
&&& \text{(Def. 5 and 7, def. of } \Theta_J) \\
&= \Sigma^n - \Big\{\sigma \mid \Big((\exists J \mid J \in \mathcal{J}_{n_0}^n : \\
&\qquad \sigma \in \Sigma_c^n \wedge \Theta_J\sigma \neq \epsilon \wedge \neg f_{\Theta_J\sigma}^{n_0*}(\Theta_J x)) \vee \\
&\qquad (\exists J \mid J \in \mathcal{J}_{n_0}^n : \sigma \in \Sigma_c^n \wedge \Theta_J\sigma = \epsilon \wedge \\
&\qquad (\exists x' \mid x' \in X^{n_0} : \\
&\qquad M^{n_0}(\Theta_J x) = M^{n_0}(x') \wedge \neg\langle Q^{n_0}\rangle(x')))\Big)\Big\} \\
&&& \text{(because } \Theta_J\sigma \neq \epsilon \wedge \neg f_{\Theta_J\sigma}^{n_0*}(\Theta_J x) \Rightarrow \\
&&& \Theta_J\sigma \neq \epsilon \wedge \Theta_J\sigma \notin \Sigma_u^{n_0} \Rightarrow \sigma \in \Sigma_c^n) \\
&= \Big\{\sigma \mid \sigma \notin \Sigma_c^n \vee \\
&\qquad \Big(\neg(\exists J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : \neg f_{\Theta_J\sigma}^{n_0*}(\Theta_J x)) \wedge \\
&\qquad\quad \neg(\exists J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&\qquad\qquad (\exists x' \mid x' \in X^{n_0} \wedge M^{n_0}(\Theta_J x) = M^{n_0}(x') : \\
&\qquad\qquad\qquad \neg\langle Q^{n_0}\rangle(x')))\Big)\Big\} \\
&&& (J \text{ not free in } \sigma \in \Sigma_c^n \text{ and distributivity}) \\
&= \Sigma_u^n \cup \Big\{\sigma \mid \sigma \in \Sigma_c^n \wedge \\
&\qquad (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : f_{\Theta_J\sigma}^{n_0*}(\Theta_J x)) \wedge \\
&\qquad (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&\qquad\qquad (\forall x' \mid x' \in X^{n_0} \wedge M^{n_0}(\Theta_J x) = M^{n_0}(x') : \\
&\qquad\qquad\qquad \langle Q^{n_0}\rangle(x')))\Big\} \\
&= \Sigma_u^n \cup \Big\{\sigma \mid \sigma \in \Sigma_c^n \wedge \\
&\qquad (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : \\
&\qquad\qquad \Theta_J\sigma \notin \hat{A}(\nu H^{n_0}, M^{n_0}(\Theta_J x))) \wedge \\
&\qquad (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&\qquad\qquad (\forall x' \mid x' \in X^{n_0} \wedge M^{n_0}(\Theta_J x) = M^{n_0}(x') : \\
&\qquad\qquad\qquad \langle Q^{n_0}\rangle(x')))\Big\} && \text{(def. of } f^*) \\
&= \Sigma_u^n \cup \Big\{\sigma \mid \sigma \in \Sigma_c^n \wedge \\
&\qquad (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : \\
&\qquad\qquad \Theta_J\sigma \notin \hat{A}(\langle Q^{n_0}\rangle, \Theta_J M^n(x))) \wedge \\
&\qquad (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&\qquad\qquad (\forall x' \mid x' \in X^{n_0} \wedge \Theta_J M^n(x) = M^{n_0}(x') : \\
&\qquad\qquad\qquad \langle Q^{n_0}\rangle(x')))\Big\} && \text{(Prop. 1, Lemma 1)}
\end{aligned}$$

■

The next proposition shows that if an event $\sigma$ has to be disabled for the system with $n$ processes in a state viewed as $y$ under the mask, then either it is disabled in a system with $n_0$ processes for some projection $J$ or there is a projection $J$ of $y$ unchanged by the occurrence of $\sigma$ and such that this projection of $y$ is equivalent under the mask to an illegal state.

*Proposition 5:* Let $y \in Y^n$ and $\sigma \in \Sigma_c^n$. Then

$$\begin{aligned}
&\sigma \in \hat{A}(\langle Q^n\rangle, y) \Rightarrow \\
&\quad (\exists J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : \Theta_J\sigma \in \hat{A}(\langle Q^{n_0}\rangle, \Theta_J y)) \vee \\
&\quad (\exists J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&\qquad (\exists x' \mid x' \in X^{n_0} \wedge \Theta_J y = M^{n_0}(x') : \neg\langle Q^{n_0}\rangle(x'))).
\end{aligned}$$

The following proposition is of great importance to prove the soundness of the synthesis method. It establishes a fundamental link between the enabled events of a SFBC maintaining $\sup\mathcal{CI}_<(Q^n)$ invariant and the projections from which these events can be recovered.

*Proposition 6:* Let $x \in X^n$ and $\sigma \in \Sigma_c^n$. Then

$$\begin{aligned}
&f_\sigma^{n*}(x) \Leftarrow \\
&(\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : \Theta_J\sigma \notin \hat{A}(\langle Q^{n_0}\rangle, \Theta_J M^n(x))) \\
&\wedge (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&\quad (\forall x' \mid x' \in X^{n_0} \wedge \Theta_J M^n(x) = M^{n_0}(x') : \langle Q^{n_0}\rangle(x'))).
\end{aligned}$$

*Proof:*

$$\begin{aligned}
&f_\sigma^{n*}(x) \\
&\Leftrightarrow \sigma \notin \hat{A}(\nu H^n, M^n(x)) && \text{(def. of } f_\sigma^{n*}) \\
&\Leftrightarrow \sigma \notin \hat{A}(\langle Q^n\rangle, M^n(x)) && \text{(Prop. 1)} \\
&\Leftarrow (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma \neq \epsilon : \\
&\qquad\qquad \Theta_J\sigma \notin \hat{A}(\langle Q^{n_0}\rangle, \Theta_J M^n(x))) \wedge \\
&\qquad (\forall J \mid J \in \mathcal{J}_{n_0}^n \wedge \Theta_J\sigma = \epsilon : \\
&\qquad\qquad (\forall x' \mid x' \in X^{n_0} \wedge \Theta_J M^n(x) = M^{n_0}(x') : \\
&\qquad\qquad\qquad \langle Q^{n_0}\rangle(x'))) && \text{(Prop. 5)}
\end{aligned}$$

■

The following proposition states that, under the assumption SSA, a predicate $Q^{n_0}$ is $\Sigma_u^{n_0}$-invariant if and only if $Q^n$ is $\Sigma_u^n$-invariant.

*Proposition 7:* $(\forall \sigma \mid \sigma \in \Sigma_u^{n_0} : Q^{n_0} \leq \mathrm{wlp}_\sigma(Q^{n_0})) \Leftrightarrow$
$(\forall n \mid n \geq n_0 : (\forall \sigma \mid \sigma \in \Sigma_u^n : Q^n \leq \mathrm{wlp}_\sigma(Q^n)))$.

*Proof:* Since the ($\Leftarrow$) part is trivial, we prove the ($\Rightarrow$) part. Suppose that there exists $n > n_0$ and $\sigma \in \Sigma_u^n$ for which $Q^n \not\leq \mathrm{wlp}_\sigma(Q^n)$. By definition of $\Sigma_u^n$, $\sigma = \sigma_i \in \Sigma_{u,i}$ for some $i$ such that $1 \leq i \leq n$. Then, there exists a state $s = \langle x[1], \ldots, x[i], \ldots, x[n] \rangle$ such that $Q^n(s)$ holds, and a state $t = \langle x[1], \ldots, \delta_i(x[i], \sigma_i), \ldots, x[n] \rangle$ such that $Q^n(t)$ does not hold. Thus, there exists $J \in \mathcal{J}_{n_0}^n$, with $i \in J$, for which $Q^{n_0}(\Theta_J t)$ does not hold (SSA). If there were no such $J$, this would contradict the fact that $Q^n(s)$ holds, since the state does not change for processes other than $i$. Furthermore, $Q^{n_0}(\Theta_J s)$ holds (SSA), $\delta^{n_0}(\Theta_J s, \Theta_J \sigma) = \Theta_J t$ (Lemma 2), and $\Theta_J \sigma \in \Sigma_u^{n_0}$ (PSA). But this implies that $Q^{n_0} \not\leq \mathrm{wlp}_\sigma(Q^{n_0})$. This is a contradiction. ■

The following two theorems constitute the main result of this paper. They characterize the soundness property and establish that the synthesis method is sound in the case of partial observation.

*Theorem 1:* Let $x \in X^n$. Then $f_A^n(x) \subseteq f^{n*}(x)$.

*Proof:* This follows from Propositions 4 and 6, and the fact that $\Sigma_u^n \subseteq f^{n*}(x)$, for any $x$. ■

*Theorem 2:* If $\langle Q^n \rangle(x_0)$ holds, then $\mathit{Re}(G|f_A^n) \leq \langle Q^n \rangle$.

*Proof:* This is a direct consequence of Theorem 1 and Proposition 2. ■

The result stated in the previous theorem means that the approach is sound: the theorem shows that in the state space with $n$ components, only safe states are reached when using the algorithm computing $f_A^n$. Note that such an algorithm computes $f_A^n$ only by looking at a reduced number $n_0 \leq n$ of components (by using $f^{n_0 *}$).

## V. Maximally-Allowable Behavior

There is generally a strong interest in synthesizing the least restrictive SFBC. As mentioned in [20] and [21], it is advantageous to aim for a kind of maximality. In fact, the off-line part of the method, which synthesizes $f_A^{n_0}$ such that $\mathit{Re}(G^{n_0}|f_A^{n_0}) \leq \sup \mathcal{CI}_<(Q^{n_0})$, is precisely motivated by restricting the plant as little as possible while still satisfying the control specification. Even though Theorem 2 guarantees that $\mathit{Re}(G|f_A^n) \leq Q^n$, asserting that $\mathit{Re}(G|f_A^n) = \mathit{Re}(G|f^{n*})$ is questionable. When the last equality is met, $f_A^n$ is said to be *maximal*. In fact, even though $f_A^{n_0}$ is the least restrictive SFBC for $Q^{n_0}$, this does not imply that $f_A^n$ is maximal. The following example, which has been elaborated from the second disjunct of the consequent of proposition 8 below, shows that $f_A^n$ may be too restrictive when $\Sigma \neq \emptyset$, that is, when synchronization is allowed.

*Example 6:* Only the relevant elements of a PDES (with $n = 3$ and $n_0 = 2$) are considered. Let $\Sigma = \{r\}$. For $1 \leq i \leq 3$, let $X_i = \{a'_i, b'_i, c'_i, a_i, b_i, c_i\}$, where $M(a'_i) = M(a_i)$, $M(b'_i) = M(b_i)$, and $M(c'_i) = M(c_i)$. Suppose that $\neg\delta^3(\langle a'_1, b'_2, c'_3 \rangle, r)!$, $\delta^3(\langle a_1, b_2, c_3 \rangle, r)!$, $\langle Q^3 \rangle(\delta^3(\langle a_1, b_2, c_3 \rangle, r))$, $\delta^2(\langle a'_1, b'_2 \rangle, r)!$, $\neg\langle Q^2 \rangle(\delta^2(\langle a'_1, b'_2 \rangle, r))$, and $\mathit{Re}(G|f_A^3)(\langle a_1, b_2, c_3 \rangle)$ all hold. One can verify that such a system satisfies all the similarity assumptions. Obviously, $r \notin \hat{A}(\langle Q^3 \rangle, M^3(\langle a_1, b_2, c_3 \rangle))$, so $\mathit{Re}(G|f^{3*})(\delta^3(\langle a_1, b_2, c_3 \rangle, r))$ holds too. Since $r \notin \theta_{\{1,2\}}^{-1} f_A^2(\langle a'_1, b'_2 \rangle)$, then $r \notin f_A^3(\langle a_1, b_2, c_3 \rangle)$ and $\mathit{Re}(G|f_A^3)(\delta^3(\langle a_1, b_2, c_3 \rangle, r))$ does not hold. Hence, $f_A^3$ is not maximal. □

The following proposition characterizes three cases when $f_A^n$ prohibits a controllable event. The first disjunct is the negation of $f_\sigma^{n*}(\cdot)$. The second disjunct concerns the case where the controllable event is a synchronized event. The third disjunct represents the case in which the controllable event is erased in the lower dimension by a projection and acts as a self loop on a bad state even if the transition is not defined in the upper dimension.

*Proposition 8:* Let $x \in X^n$ and $\sigma \in \Sigma_c^n$. Then

$$\begin{aligned}
& \neg f_\sigma^{n*}(x) \vee \\
& (\sigma \in \Sigma \wedge \\
& \quad (\exists x' \mid x' \in X^n : M^n(x) = M^n(x') \wedge \neg\delta^n(x', \sigma)! \wedge \\
& \qquad (\exists J \mid J \in \mathcal{J}_{n_0}^n : \delta^{n_0}(\Theta_J x', \sigma)! \wedge \\
& \qquad\qquad \neg\langle Q^{n_0} \rangle(\delta^{n_0}(\Theta_J x', \sigma)))) \vee \\
& (\exists x' \mid x' \in X^n : M^n(x) = M^n(x') \wedge \neg\delta^n(x', \sigma)! \wedge \\
& \qquad (\exists J \mid J \in \mathcal{J}_{n_0}^n : \Theta_J \sigma = \epsilon \wedge \neg\langle Q^{n_0} \rangle(\Theta_J x'))) \\
\Leftarrow \quad & \sigma \notin f_A^n(x).
\end{aligned}$$

Proposition 8 brings the natural question as whether or not $f_A^n$ is maximal if no synchronization is allowed. Theorem 3 shows that under this restriction, $f_A^n$ is maximal.

*Theorem 3:* If $\Sigma = \emptyset$, then $\mathit{Re}(G|f_A^n) = \mathit{Re}(G|f^{n*})$.

*Proof:* First, $\mathit{Re}(G|f_A^n) \leq \mathit{Re}(G|f^{n*})$ by Theorem 1. Next, assume that $\mathit{Re}(G|f_A^n) < \mathit{Re}(G|f^{n*})$. Then there exists $x \in X^n$ and $\sigma \in \Sigma_c^n$ satisfying $\sigma \notin f_A^n(x)$ and $f_\sigma^{n*}(x)$, so that the following predicate must hold (by Proposition 8):

$$\begin{aligned}
& (\exists x' \mid x' \in X^n : M^n(x) = M^n(x') \wedge \neg\delta^n(x', \sigma)! \wedge \\
& \qquad (\exists J \mid J \in \mathcal{J}_{n_0}^n : \Theta_J \sigma = \epsilon \wedge \neg\langle Q^{n_0} \rangle(\Theta_J x'))).
\end{aligned}$$

Thus, one can choose $x' \in X^n$ and $J \in \mathcal{J}_{n_0}^n$ such that

$$M^n(x) = M^n(x') \wedge \Theta_J \sigma = \epsilon \wedge \neg\langle Q^{n_0} \rangle(\Theta_J x').$$

From $\Theta_J \sigma = \epsilon$, there exists $i \notin J$, $1 \leq i \leq n$, such that $\sigma = \sigma_i$. Now, either $\neg\delta^n(x, \sigma_i)!$ or $\delta^n(x, \sigma_i)!$. In the first case, no transition can occur whether the system is controlled by $f^{n*}$ or by $f_A^n$, thus contradicting the assumption; hence, suppose $\delta^n(x, \sigma_i)!$. Because the transition is allowed by $f^{n*}$, $\langle Q^n \rangle(\delta^n(x, \sigma_i))$ holds.

Consider the state $x'' := \langle x'[1], x'[2], \ldots, x[i], \ldots, x'[n] \rangle$. The assumption PSA ensures that $x'' \in X^n$ and $\delta^n(x'', \sigma_i)!$ and the assumption MSA ensures that $M^n(x'') = M^n(x)$; thus, $\langle Q^n \rangle(\delta^n(x'', \sigma_i))$ holds, since otherwise $f_\sigma^{n*}(x)$ would be false. But the assumption SSA implies the opposite, that $\langle Q^n \rangle(\delta^n(x'', \sigma_i))$ does not hold (because $\Theta_J x' = \Theta_J \delta^n(x'', \sigma_i)$ and $\neg\langle Q^{n_0} \rangle(\Theta_J x')$). ■

## VI. Conclusion

The synthesis method proposed in this paper was motivated by the issue of scalability arising from synthesis algorithms. It has been shown that, under some assumptions, the method ensures safety and maximality. This new result represents a fundamental step in the solution of the aforementioned issue.

The closest work to our approach is described in [19]. It exhibits a method that synthesizes a program, for a system consisting of $K$ similar interconnected sequential processes executing in parallel, from a temporal logic specification based on the calculation of a solution for a pair-system. In addition to the use of a different paradigm (SCT), our method allows to express safety properties with the aid of general predicates which are not limited to pair-systems (e.g., the mutual exclusion problem in which at most $p > 2$ processes can simultaneously use the resource). It does not only consider the case where the states of the system are completely observed, but also the case where they are partially observed. A general method, based on heuristics, has been proposed in [22], [23]. It encompasses the one described in this paper, but the problem of preserving soundness is more difficult and remains an open problem for the general case. Finally, a sound synthesis method has been recently suggested for bounded-data parameterized systems [24]. It integrates a verification technique [25] into a synthesis procedure. The verification technique is based on a heuristics for an algorithmic construction of an inductive assertion, but it is incomplete because the algorithm may fail after two trials.

Finally, this new approach raises several interesting open problems. For instance, it could be generalized to a PDES consisting of multiple classes of an arbitrarily large number of similar processes. It could also be reconsidered for the case where the control specifications are expressed by temporal logic formulas and PDES have nonterminating behaviors in order to take liveveness properties into consideration.

## References

[1] P. J. G. Ramadge and W. M. Wonham, "Modular feedback logic for discrete event systems," *SIAM Journal on Control and Optimization*, vol. 25, no. 5, pp. 1202–1218, 1987.

[2] S.-L. Chung, S. Lafortune, and F. Lin, "Limited lookahead policies in supervisory control of discrete event systems," *IEEE Transactions on Automatic Control*, vol. 37, no. 12, pp. 1921–1935, 1992.

[3] L. E. Holloway, B. H. Krogh, and A. Giua, "A survey of Petri net methods for controlled discrete event systems," *Discrete Event Dynamic Systems: Theory and Applications*, vol. 7, no. 2, pp. 151–190, 1997.

[4] G. Barrett and S. Lafortune, "Bisimulation, the supervisory control problem and strong model matching for finite state machines," *Discrete Event Dynamic Systems: Theory and Applications*, vol. 8, no. 4, pp. 337–429, 1998.

[5] M. Makungu, M. Barbeau, and R. St-Denis, "Synthesis of controllers of processes modeled as colored Petri nets," *Discrete Event Dynamic Systems: Theory and Applications*, vol. 9, no. 2, pp. 147–169, 1999.

[6] J. M. Eyzell and J. E. R. Cury, "Exploiting symmetry in the synthesis of supervisors for discrete event systems," *IEEE Transactions on Automatic Control*, vol. 46, no. 9, pp. 1500–1505, 2001.

[7] H. Bherer, J. Desharnais, M. Frappier, and R. St-Denis, "Synthesis of state feedback controllers for parameterized discrete event systems," in *Proceedings of ATVA'2004*, ser. Lecture Notes in Computer Science, F. Wang, Ed., vol. 3299. Springer, 2004, pp. 487–490.

[8] J. H. Prosser, M. Kam, and H. G. Kwatny, "Online supervisor synthesis for partially observed discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 43, no. 11, pp. 1630–1634, 1998.

[9] Y. Li and W. M. Wonham, "Controllability and observability in the state-feedback control of discrete-event systems," in *Proceedings of 27th IEEE Conference on Decision and Control*, New York, 1988, pp. 203–208.

[10] Y. Li, "Control of vector discrete-event systems," Ph.D. dissertation, University of Toronto, 1991.

[11] S. Takai and S. Kodama, "M-controllable subpredicates arising in state feedback control of discrete event systems," *International Journal of Control*, vol. 67, no. 4, pp. 553–566, 1997.

[12] S. Takai, T. Ushio, and S. Kodama, "Static-state feedback control of discrete-event systems under partial observation," *IEEE Transactions on Automatic Control*, vol. 40, no. 11, pp. 1950–1954, 1995.

[13] Y. Li and W. M. Wonham, "Controllability and observability in the state-feedback control of discrete-event systems," University of Toronto, System Control Group 8803, 1988.

[14] W. M. Wonham, "Notes on control of discrete-event systems," University of Toronto, System Control Group ECE 1636F/1637S, revised 2003.

[15] D. Gries and F. B. Schneider, *A Logical Approach to Discrete Math*. New-York: Springer-Verlag, 1993.

[16] R. Kumar and V. K. Garg, "Extremal solutions of inequations over lattices with applications to supervisory control," *Theoretical Computer Science*, vol. 148, no. 1, pp. 67–92, 1995.

[17] R. Kumar and M. A. Shayman, "Formulae relating controllability, observability, and co-observability," *Automatica*, vol. 34, no. 2, pp. 211–215, 1998.

[18] B. A. Davey and H. A. Priestley, *Introduction to Lattices and Order*. Cambridge University Press, 1990.

[19] P. C. Attie and E. A. Emerson, "Synthesis of concurrent systems with many similar processes," *ACM Transactions on Programming Languages and Systems*, vol. 20, no. 1, pp. 1–65, 1998.

[20] J. H. Prosser and M. Kam, "Supervisor synthesis for approximating maximally-allowable behaviors," in *Proceedings of the 1994 Conference on Information Science and Systems*, vol. 2, Princeton, 1994, pp. 740–746.

[21] R. D. Brandt, V. K. Garg, R. Kumar, F. Lin, S. I. Marcus, and W. M. Wonham, "Formulas for calculating supremal controllable and normal sublanguages," *Systems & Control Letters*, vol. 15, no. 2, pp. 111–117, 1990.

[22] M. Frappier and R. St-Denis, "Towards a computer-aided design of reactive systems," in *Computer Aided Systems Theory – EUROCAST 2001*, ser. Lecture Notes in Computer Science, R. Moreno-Díaz, B. Buchberger, and J.-L. Freire, Eds., vol. 2178. Springer, 2001, pp. 421–436.

[23] R. St-Denis, "Designing reactive systems: integration of abstraction techniques into a synthesis procedure," *The Journal of Systems and Software*, vol. 60, no. 2, pp. 103–112, 2002.

[24] H. Bherer, J. Desharnais, M. Frappier, and R. St-Denis, "Intégration d'une technique de vérification dans une procédure de synthèse de contrôleurs de systèmes paramétrés," in *Modélisation des systèmes réactifs (MSR 2003)*, D. Méry, N. Rezg, and X. Xie, Eds. Lavoisier, 2003, pp. 553–566.

[25] A. Pnueli, S. Ruah, and L. Zuck, "Automatic deductive verification with invisible invariants," in *Tools and Algorithms for the Construction and Analysis of Systems*, ser. Lecture Notes in Computer Science, T. Margaria and W. Yi, Eds., vol. 2031. Springer, 2001, pp. 82–97.