An Electronic Supplement for the Article
“Invariant-based Supervisory Control of Switched Discrete Event Systems with an Application to Robust Deadlock Avoidance” that is submitted to ADHS’15.

Spyros Reveliotis * Zhennan Fei **

* Georgia Institute of Technology, Atlanta, GA, 30332, USA (e-mail: spyros@isye.gatech.edu).
** Prover, Stockholm, Sweden

1. PROOF OF PROPOSITION 1

The necessity of the condition stated in Proposition 1 is obvious. The sufficiency is established by the fact that, under satisfaction of this condition, any supervisor $\Gamma$ that sets $\Gamma(x_0, s_0) = \emptyset$ is a correct supervisor.

2. PROOF OF PROPOSITION 2

It is easy to check that $\text{Reach}(\Gamma'/\mathcal{G}) \subseteq \text{Reach}(\Gamma/\mathcal{G}) \subseteq \Omega$, where the second inclusion results from the presumed correctness of supervisor $\Gamma$. Hence, the controlled DES $\Gamma'/\mathcal{G}$ satisfies the inclusion of Eq. 6 in the manuscript, and supervisor $\Gamma'$ is a correct supervisor.

3. PROOF OF PROPOSITION 3

If supervisor $\Gamma$ itself is pertinent, we can just set $\Gamma' = \Gamma$. Next, consider the case where $\Gamma$ is not a pertinent supervisor. Hence, there exists some state $(x, s) \in X \times S$ and a controllable event $\sigma \in \Sigma^c$ such that $\text{Reach}^\sigma(x, s, \sigma; \mathcal{G}) \not\subseteq \Omega$. But then, the only way that $\Gamma$ can be a correct supervisor for the considered control task is by having $(x, s) \notin \text{Reach}(\Gamma/\mathcal{G})$. Under these circumstances, we define $\Gamma_i(x, s) = \emptyset$, while setting $\Gamma_i(x', s') = \Gamma(x', s')$ for all other global states $(x', s') \neq (x, s)$. This restriction preserves correctness, while the non-reachability of the state $(x, s)$ in the original dynamics of $\text{Reach}(\Gamma/\mathcal{G})$ further implies the satisfaction of conditions (i) and (ii) in the statement of this Proposition. Repeating the above adjustment on supervisor $\Gamma_i$ for every other triplet $(x', s', \sigma') \in X \times S \times \Sigma^c$ that violates the condition of Eq. 13 in Definition 4, will eventually lead to a pertinent supervisor $\Gamma''$ that meets the conditions of this Proposition.

4. PROOF OF PROPOSITION 4

The pertinence of the supervisor $\Gamma_1 \lor \Gamma_2$ results immediately from the definitions of the disjunctive and the pertinent supervisors, and the pertinence of the constituent supervisors $\Gamma_1$ and $\Gamma_2$. Next, we prove the correctness of this supervisor.

For any state $(x, s) \in \text{Reach}(\Gamma_1 \lor \Gamma_2/\mathcal{G})$, let $\#(x, s)$ denote the minimum number of transitions that are necessary for reaching state $(x, s)$ from the initial state $(x_0, s_0)$ in the dynamics of $\Gamma_1 \lor \Gamma_2/\mathcal{G}$. We shall prove the sought result by an induction on $\#(x, s)$.

The base case of $\#(x, s) = 0$ results immediately from the presumed feasibility of the considered supervisory control problem and Proposition 1.

Next, suppose that the correctness condition holds true for every state $(x, s) \in \text{Reach}(\Gamma_1 \lor \Gamma_2/\mathcal{G})$ with $\#(x, s) \leq n$, i.e., for every such state, $s \in S_x$. We shall show that this condition also holds true for every state $(x, s)$ with $\#(x, s) = n + 1$. We prove the required result by contradiction. Hence, consider a state $(x, s)$ with $\#(x, s) = n + 1$, and suppose that $s \notin S_x$. Then, the presumed feasibility of the considered problem implies that $(x, s) \notin \text{Reach}^\sigma(x_0, s_0; \mathcal{G})$. Hence, every transition sequence leading from $(x_0, s_0)$ to $(x, s)$ must contain at least one controllable event. Consider such a transition sequence and let the triplet $(x', s', \sigma) \in X \times S \times \Sigma^c$ denote the last controllable transition on this path. Also, notice that, by the definition of this sequence, $\#(x', s') \leq n$, and thus, by the inductive hypothesis, $s' \in S_{x'}$. Finally, since the transition $(x', s', \sigma)$ is enabled by $\Gamma_1 \lor \Gamma_2$, it must be enabled by at least one of the two supervisors $\Gamma_1$ and $\Gamma_2$. On the other hand, the aforestated assumptions also imply that $(x, s) \in \text{Reach}^\sigma(x', s', \sigma; \mathcal{G})$, a fact that when combined with the working hypothesis that $s \notin S_x$, leads to the contradictory conclusion that at least one of the original supervisors $\Gamma_i$, $i = 1, 2$, is not pertinent.

5. PROOF OF THEOREM 1

The correctness of the supervisor $\Gamma^*$ defined in Eq. 15 of the considered Theorem, can be obtained from its pertinence, once the latter is established, through an argument similar to that followed in the proof of Proposition 4. Hence, to establish the results claimed by the Theorem, it suffices to establish that (i) the iteration providing $\lim \mathcal{F}^\sigma(\Omega)$ will terminate in a finite number of steps, (ii) the resultant set $\lim \mathcal{F}^\sigma(\Omega)$ will contain the initial state $(x_0, s_0)$, (iii) the supervisor $\Gamma^*$ which is subsequently constructed from this set through Eq. 15 is pertinent, and (iv) the restriction of this supervisor over the global states $(x, s) \in X \times S$ with $\text{Reach}^\sigma(x, s; \mathcal{G}) \subseteq \Omega$ is maximally permissive.
These four results can be obtained immediately from Eqs 14 and 15, the finiteness of the underlying (global) state space of DES $G$, and the following lemma:

**Lemma 1.** For every $i = 1, 2, \ldots$, a state $(x, s)$ is removed from the set $F^{(i-1)}(x, s)$ during the computation of $F^i(x, s)$ if $\text{Re} \cup_i x, s \in \Omega$ and any minimal uncontrollable transition sequence that leads from $(x, s)$ to some state $(x', s') \in X \times S \setminus \Omega$ has a length of $i$ steps.

**Proof:** The reader can easily verify that Lemma 1 holds true for $i = 1$. Next, suppose that Lemma 1 holds true for $i \leq n$. We shall show that it must also hold true for $i = n + 1$. Indeed, consider a state $(x, s)$ that is removed from $F^n(x, s)$ during the computation of $F^{(n+1)}(x, s)$. According to the logic of Eq. 14, this state is removed from $F^n(x, s)$ because there is an event $e \in \Sigma \cup E$ and a state $(x', s') \in X \times S \setminus F^n(x, s)$ such that $(x', s') \in \delta(x, s, e)$. But by the inductive hypothesis, every state $(x', s') \in X \times S \setminus F^n(x, s)$ either belongs to $X \times S \setminus \Omega$ or it has an emanating uncontrollable transition sequence leading to this set in no more than $n$ steps. Hence, state $(x, s)$ has an emanating sequence that leads to $X \times S \setminus \Omega$ in no more than $n+1$ steps. The fact that any such minimal sequence of $(x, s)$ contains exactly $n+1$ steps results from the inductive hypothesis, since otherwise this state would have been removed during the previous iterations.

6. **PROOF OF THEOREM 2**

To prove the results of this Theorem, first it is important to notice that, due to its symmetrical structure, the terminating condition of Eq. 17 is priced uniformly for every agent $A_x$, and whenever it is set to $\text{TRUE}$, all agents are in an idling mode, having set their corresponding variable $\text{DONE} x = \text{TRUE}$. Furthermore, it is easy to check, by tracing the logic of the stage “PROCESS MESSAGE QUEUE”, that once the terminating condition is set to true, it cannot be negated by the action of any agent, and therefore, all the agents $A_x$ will have to proceed from their current idling status to their termination.

On the other hand, an agent $A_x$ may exit its idling status by receiving some messages $M_{x,e}^i$ in its queue $\text{MessageQueue}_x$. But the origin and delivery of any such message $M_{x,e}^i$ by agent $A_x$ implies the reduction of the cardinality of the corresponding state set $Q_x$. Since all state sets $Q_x$, $x \in X$, are initialized to finite contents, these contents can only be reduced during the execution of the algorithm, and any single pass of the stages “COMPUTE” and “PROCESS MESSAGE QUEUE” (i.e., lines 14–39 in Fig. 2) is a finite computation, it follows that the entire algorithm will terminate in finite time.

Next, we prove the correctness of the algorithm, i.e., the validity of Eq. 18. A proof similar to that of Lemma 1 can establish that, for any value of the variable set $Q_x$, the fixed-point computation of the stage “COMPUTE” in the code of Fig. 2 will return the subset of $Q_x$ collecting all of its states that have no uncontrollable paths to $\hat{S} \setminus Q_x$. This remark together with the initial value of the sets $Q_x$, $x \in X$, further imply that the first execution of the stage “COMPUTE” by each agent $A_x$ will remove from the corresponding set $Q_x$ all states that have uncontrollable paths to states $s \in \hat{S} \setminus S_x$ (i.e., to states in $S$ that do not satisfy the predicate $P_2$). On the other hand, the messages $M_{x,e}^i$ exchanged by the agents $A_x$, and the corresponding processing of these messages that takes place in stages “PROCESS MESSAGE QUEUE” and “COMPUTE”, seek to eliminate from each state set $Q_x$ any states $s$ corresponding to global states $(x, s)$ with emanating transition sequences to some predicate-violating state $(x', s')$ that contain some event(s) $e \in E$. Hence, to establish the correctness of the claim of the considered Theorem, it remains to be shown that the considered distributed algorithm generates and processes all the messages $M_{x,e}^i$ that are necessary for the aforementioned eliminations.

To prove this last result, for any given global state $(x, s) \notin \lim F(x, s)$, let $(x, s)$ denote the minimum number of events $e \in E$ in any uncontrollable transition sequence that leads from $(x, s)$ to $X \times S \setminus \Omega$; we shall establish the sought result through an induction on this state index. The base case of $(x, s) = 0$ was already established in the previous discussion about the computation that takes place during the first visit of the stage “COMPUTE” by each agent $A_x$, $x \in X$. Next, suppose that the algorithm identifies and eliminates from the corresponding set $Q_x$ all the global states $(x, s) \notin \lim F(x, s)$ and consider a state $(x, s) \notin \lim F(x, s)$ with $(x, s) = n + 1$. By the definition of the state $(x, s)$, there is a state $(x', s')$ with $(x', s') \notin \lim F(x, s)$, and the message $(x', s')$ is reachable from $(x, s)$ through a transition sequence where $w \in \Sigma^n$ and $e \in E$. By the inductive hypothesis, state $s'$ has been eliminated from $Q_x$ by agent $A_x$, and furthermore, this elimination has been communicated to the agent $A_x$ by a message $M_{x,e}^i$ during the execution of the corresponding stage by agent $A_x$. Since agent $A_x$ was in stage “INITIALIZE” or “COMPUTE” during the composition and dispatching of the aforementioned message $M_{x,e}^i$, $\text{DONE} [x'] = \text{FALSE}$ and, according to the remarks in the opening paragraph of this proof, agent $A_x$ cannot be in its terminating stage. Furthermore, the increase of the counter $\text{COUNT}[x', s']$ by one unit upon the creation of the aforementioned message $M_{x,e}^i$ implies that the terminating condition of Eq. 17 cannot be evaluated to $\text{TRUE}$ until agent $A_x$ has processed the message $M_{x,e}^i$. Let $\hat{s}$ denote the next-to-last state visited by the aforementioned transition sequence $w$ on a path that leads from $(x, s)$ to $(x', s')$.\(^1\) State $\hat{s}$ is in $Q_{\hat{s}}$ during the processing of the considered message $M_{x,e}^i$, since, otherwise, the considered state $\hat{s}$ would have been eliminated from $Q_{\hat{s}}$ by the fixed-point iteration of stage “COMPUTE” during the elimination of the state $\hat{s}$. But then, the processing of $M_{x,e}^i$ by agent $A_x$, in stage “PROCESS MESSAGE QUEUE”, will lead to the elimination of state $\hat{s}$ from $Q_{\hat{s}}$; and this elimination subsequently will trigger the execution of the stage “COMPUTE” by the same agent; state $\hat{s}$ will be eliminated from the set $Q_{\hat{s}}$ during this stage (unless $w = \epsilon$, in which case, $\hat{s} \equiv \hat{s}$).

\(^1\) The last qualification of $\hat{s}$ is necessary since the transitions of the considered DES $G$ are nondeterministic.