Proceedings of the 12th
KACC, October 1997

Fault-Tolerant Robust Supervisor for Timed Discrete Event Systems

°Seong-Jin Park* and Jong-Tae Lim*

* Department of Electrical Engineering, Korea Advanced Institute of Science and Technology
373-1 Kusong-dong, Yusong-gu, Taejon, Korea
Tel : +82-42-869-5441 Fax : +82-42-869-3410 E-mail : sjpark@stcon1.kaist.ac.kr

Abstracts This paper presents the problem of fault-tolerant robust supervisory control of timed discrete event systems (DESs). First the concept of faults is quantitativeley defined in timed DESs and fault tolerable event sequences are presented as a desired legal language. Given a timed DES with model uncertainty, the conditions for the existence of a supervisor which always guarantees fault tolerable event sequences embedded in the system are derived.

Keywords Timed Discrete Event Systems, Fault-tolerant Control, Model Uncertainty, Robust Supervisory Control

1. INTRODUCTION

The issues of fault-tolerance and safety are important in the complex real time systems. System-theoretic methods on failure diagnosis and fault-tolerant control have been developed. In [3], the quantitative definitions of faults, failures, and fault tolerant systems are proposed in the Ramadge-Wonham framework for control of DESs [1]. However the approaches are based on untimed models which can not explain the requirement to satisfy stringent timing constraints. Also they are not valid for analysis of the systems with model uncertainty.

In this paper the problem of fault-tolerant robust supervisory control of timed DESs with model uncertainty is addressed, and the conditions to achieve fault-tolerace of the systems are derived.

2. Model Uncertainty and Faults

In [4] a system G with model uncertainty is assumed as follows. $G \in \{G_1, G_2, ..., G_m\}$. This paper follows the above assumption about model uncertainty.

This paper uses the framework of timed DESs developed in [2]. Let's review the framework. To develop the base model, we write 5 tuple $G_{act} = (A, \Sigma_{act}, \delta_{act}, a_0, A_m)$. A is the set of activities a, Σ_{act} is a finite alphabet of event, $\delta_{act} : \Sigma_{act} \times A \rightarrow A$ is the activity transition function, $a_0 \in A$ is the initial activity and $A_m \subseteq A$ is the subset of marker activities.
Let $N = \{0, 1, 2, ...\}$. In Σ_{act}, each event σ is equipped with a lower time bound (delay) $l_\sigma \in N$ and an upper time bound (deadline) $u_\sigma \in N \cup \{\infty\}$. For $j, k \in N$ let $(j, k) := \{i \in N \mid j \leq i \leq k\}$, and let $T_\sigma := (0, u_\sigma)$ if $u_\sigma < \infty$, or $T_\sigma := (0, l_\sigma)$ if $u_\sigma = \infty$. T_σ is called the timer interval for σ. The states set in timed models is $Q := A \times \sqcap\{T_\sigma \mid \sigma \in \Sigma_{act}\}$, where $\sqcap\{T_\sigma \mid \sigma \in \Sigma_{act}\}$ is cartesian product of elements in $\{T_\sigma \mid \sigma \in \Sigma_{act}\}$. Thus a state q is represented as $q = (a, \{t_\sigma \mid \sigma \in \Sigma_{act}\})$, where $a \in A$ and the t_σ(called timer of σ in q)$\in T_\sigma$. The initial state is $q_0 := (a_0, \{t_{\sigma_0} \mid \sigma \in \Sigma_{act}\})$, where the t_σ are set to their default values, $t_{\sigma_0} := u_\sigma$ if $u_\sigma < \infty$ or $t_{\sigma_0} := l_\sigma$ if $u_\sigma = \infty$. The marker state subset is $Q_m \subseteq A_m \times \sqcap\{T_\sigma \mid \sigma \in \Sigma_{act}\}$. We introduce one additional event, written *tick*, to represent "tick of the global clock", and take for our total set of events $\Sigma := \Sigma_{act} \dot{\cup} \{tick\}$. The state transition function $\delta : \Sigma \times Q \rightarrow Q$ will be defined in detail below. We can now write $G = (Q, \Sigma, \delta, q_0, Q_m)$. Then G is called a timed discrete event system (TDES).
We now provide the formal definition of δ. Write $\delta(\sigma, q) = q'$, with $q = (a, \{t_\sigma \mid \sigma \in \Sigma_{act}\})$, $q' = (a', \{t'_\tau \mid \tau \in \Sigma_{act}\})$. Then $\delta(\sigma, q)!$ (! means "is defined") if and only if (1) $\sigma = tick$ and $(\forall \tau \in \{\sigma \mid u_\sigma < \infty\})$ $t_\tau > 0$, or (2) $\sigma \in \{\sigma \mid u_\sigma < \infty\}, \delta_{act}(\sigma, a)!$, and $0 \leq t_\sigma \leq u_\sigma - l_\sigma$, or (3) $\sigma \in \{\sigma \mid u_\sigma = \infty\}, \delta_{act}(\sigma, a)!$, and $t_\sigma = 0$. The entrance state q' is defined as follows. (1) Let $\sigma = tick$. Then $a' := a$ and if $\tau \in \{\alpha \mid u_\alpha < \infty\}$, $t'_\tau := u_\tau$ if not $\delta_{act}(\tau, a)!$, or $t'_\tau := t_\tau - 1$ if $\delta_{act}(\tau, a)!$ and $t_\tau > 0$. If $\tau \in \{\alpha \mid u_\alpha = \infty\}$, $t'_\tau := l_\tau$ if not $\delta_{act}(\tau, a)!$, or $t'_\tau := t_\tau - 1$ if $\delta_{act}(\tau, a)!$ and $t_\tau > 0$, or $t'_\tau := t_\tau > 0$ if $\delta_{act}(\tau, a)!$ and $t_\tau = 0$. Recall that if $\tau \in \{\alpha \mid u_\tau < \infty\}$ and $t_\tau = 0$ then not $\delta(tick, q)!$. (2) Let $\sigma \in \Sigma_{act}$. Then $a' := \delta_{act}(\sigma, a)$ and if $\tau \neq \sigma$ and $\tau \in \{\alpha \mid u_\alpha < \infty\}$, $t'_\tau := u_\tau$ if not $\delta_{act}(\tau, a')!$, or $t'_\tau := t_\tau$ if $\delta_{act}(\tau, a')!$. If $\tau = \sigma$ and $\sigma \in \{\alpha \mid u_\alpha < \infty\}$, $t'_\tau := u_\sigma$. If $\tau \neq \sigma$ and $\tau \in \{\alpha \mid u_\alpha = \infty\}$, $t'_\tau := l_\tau$ if not $\delta_{act}(\tau, a')!$ $t'_\tau := t_\tau$ if $\delta_{act}(\tau, a')!$. If $\tau = \sigma$ and $\sigma \in \{\alpha \mid u_\alpha = \infty\}$, $t'_\tau := l_\sigma$.

In timed DES models, the forcible events, $\Sigma_{for} \subseteq \Sigma_{act}$, are defined. By forcing action of supervisor, forcible events *preempt* a *tick* of the clock. The closed behavior $L(G)$ and marked behavior $L_m(G)$ of timed DES G are $L(G) := \{s \mid s \in \Sigma^*$ and $\delta(s, q_0)!\}$ and $L_m(G) := \{s \mid s \in \Sigma^*$ and $\delta(s, q_0) \in Q_m\}$.

Let G be a TDES, and $A(q)$ be a set of events possible to occur after state q. Then *fault* and *failure* are defined as follows.

Definition 1 (fault event) : The aug-event (σ_f, q_f) is a "fault w.r.t. Q_m" and σ_f is called a "fault event" if

(1) $\sigma_f \in \Sigma_{an}$ *and*

(2) *there exists at least one event sequence* $s \in \{t \in \Sigma^* \mid \sigma_f t \in L(G)\}$ *such that* $\sigma_f s$ *leads to the marker states set* Q_m *and for each aug-event* (s_i, q_i) *of* $s = s_1 s_2 ... s_n$, *any* $\sigma \in A(q_i) - \{s_i\}$ *for all* s_i *corresponding to* q_i *is another fault event or tolerable normal event or belongs to*

$$\begin{cases} \Sigma_c & \text{if } s_i \text{ or one of tolerable normal events is forcible event} \\ \Sigma_c - \{tick\} & \text{otherwise} \end{cases}$$

Definition 2 (failure) : The aug-event (σ_f, q_f) *is a "failure w.r.t.* Q_m*" and* σ_f *is called a "failure event" if* $\sigma_f \in \Sigma_{an}$ *and* (σ_f, q_f) *is not a fault.*

Definition 3 (tolerable normal event) : The aug-event (σ, q) *is a "tolerable normal w.r.t.* Q_m*" and* σ *is called a "tolerable normal event" if*

(1) $\sigma \in (\Sigma_n \cap \Sigma_{uc}) \cup \{tick\}$ *and*

(2) *there exists at least one event sequence* $s \in \{t \in \Sigma^* \mid \sigma t \in L(G)\}$ *such that* σs *leads to the marker states set* Q_m *and for each aug-event* (s_i, q_i) *of* $s = s_1 s_2 ... s_n$, *any* $\sigma \in A(q_i) - \{s_i\}$ *for all* s_i *corresponding to* q_i *is fault event or another tolerable normal event or belongs to*

$$\begin{cases} \Sigma_c & \text{if } s_i \text{ or one of another tolerable normal events is forcible event} \\ \Sigma_c - \{tick\} & \text{otherwise} \end{cases}$$

Definition 4 (tolerable fault event sequence,TFES) : The event sequence which consists of normal events or fault events and which derives the initial state to the marker states is called a "tolerable fault event sequence(TFES)" if, for each normal event, all the possible events following the corresponding state are tolerable normal events or fault events or belongs to

$$\begin{cases} \Sigma_c & \text{if at least one event of the events (including normal events in TFES) is forcible event} \\ \Sigma_c - \{tick\} & \text{otherwise} \end{cases}$$

3. Control

Let's define the set of all TFESs in a process G_i to be $TF(G_i)$, that is, $TF(G_i) := \{t \in L(G_i) \mid t \text{ is a TFES}\}$ Let's define the set of all TFESs of all models to be $T(G)$, that is, $T(G) := \bigcup_{i=1}^{m} TF(G_i)$

Definition 5 (fault tolerant robust supervisor) : A supervisor $\mathcal{S}$ *is "fault tolerant robust supervisor" for a system* $G \in \{G_1, G_2, ..., G_m\}$ *if there exists a language* $K_i, K_i \neq \emptyset$, *for each* G_i *such that* $K_i \subseteq TF(G_i)$ *and* $L(\mathcal{S}/G_i) = \overline{K_i}$, *where* $i = 1, 2, ..., m$.

For a string s in a language L, let's define $A_L(s)$ to be $A_L(s) := \{\alpha \in \Sigma \mid s\alpha \in \overline{L}\}$, and it is called active events set after a string s.

For a string $s \in L(G_i)$, let's define $Dg_{L(G_i)}(s)$ to be $\{\alpha \in \Sigma_i \mid \alpha \in (A_{L(G_i)}(s) - A_{TF(G_i)}(s))\}$ if $s \in \overline{TF(G_i)}$, otherwise $\emptyset$. For a $s \in \bigcup_{i=1}^{m} L(G_i)$, let's define $SEL(s)$ to be $A_{T(G)}(s) - (\bigcup_{i=1}^{m} Dg_{L(G_i)}(s) - \{tick\})$. In a timed DES $G \in \{G_1, ..., G_m\}$, let's define $RISK(G)$ to be $\{s \in \overline{T(G)} \mid SEL(s) \cap A_{TF(G_i)}(s) = \emptyset$ for at least the one of G_i's satisfying $A_{TF(G_i)}(s) \neq \emptyset\} \cup \{s \in \overline{T(G)} \mid SEL(s) \cap (A_{TF(G_i)}(s) \cap \Sigma_{for,i}) = \emptyset$ for at least the one of G_i's satisfying $tick \in Dg_{L(G_i)}(s)\}$

Lemma 1 If a supervisor $\mathcal{S}$ *is a fault tolerant robust supervisor for a system* $G \in \{G_1, G_2, ...G_m\}$, *then* $L(\mathcal{S}/G) \cap RISK(G) = \emptyset$.

Proof : Suppose that $t \in L(\mathcal{S}/G)$ and t is the element of the right first set of the $RISK(G)$ definition. Then there exists at least a G_i such that $A_{TF(G_i)}(s) \neq \emptyset$ but $SEL(s) \cap A_{TF(G_i)}(s) = \emptyset$. Therefore if the controlled system is G_i, there do not exist event sequences to satisfy path-continuation of TFES in the G_i after the string s. Thus for the G_i there does not exist a $K_i, K_i \neq \emptyset$, such that $K_i \subseteq TF(G_i)$ and $L(\mathcal{S}/G_i) = \overline{K_i}$. This is contradiction.

Suppose that $t \in L(\mathcal{S}/G)$ and t is the element of the right second set of the $RISK(G)$ definition. Then there exists at least one G_i such that $tick \in Dg_{TF(G_i)}(t)$ and $SEL(t) \cap (A_{TF(G_i)}(t) \cap \Sigma_{for,i}) = \emptyset$. Then if the controlled process is G_i, there do not exist forcible events to preempt $tick$ after the string t. So the *tick becomes* an uncontrollable event, which may deviates the system,G_i, from TFES. Then for the G_i, there does not exist a K_i, $K_i \neq \emptyset$, such that $K_i \subseteq TF(G_i)$ and $L(\mathcal{S}/G_i) = \overline{K_i}$. This is contradiction. □

Theorem 1 Let $TF(G_i) \neq \emptyset$ *for all* G_i*'s and* $K \subseteq \{s \in T(G) \mid \overline{s} \cap RISK(G) = \emptyset\}$. *Then there exists a fault tolerant robust supervisor for a* $G \in \{G_1, G_2, ..., G_m\}$ *if and only if there exists a* $K, K \neq \emptyset$, *such that for all* $s \in \overline{K}$

(A1) $A_K(s) \cap A_{TF(G_i)}(s) \neq \emptyset$ *for each* G_i *such that* $A_{TF(G_i)}(s) \neq \emptyset$,

(A2) $A_K(s) \subseteq SEL(s)$,

(A3) $A_K(s) \cap (A_{TF(G_i)}(s) \cap \Sigma_{for,i}) \neq \emptyset$ *for each* G_i *satisfying* $tick \in Dg_{L(G_i)}(s)$, *and*

(A4)

$$A_K(s) \supseteq \begin{cases} A_{T(G)}(s) \cap \Sigma_{uc} & \text{if } tick \notin SEL(s) \text{ or } A_K(s) \cap (A_{TF(G_i)}(s) \cap \Sigma_{for,i}) \neq \emptyset \text{ for each } G_i \text{ satisfying } tick \in A_{TF(G_i)}(s) \\ A_{T(G)}(s) \cap (\Sigma_{uc} \cup \{tick\}) & \text{otherwise} \end{cases}$$

Proof : (If part) Consider a supervisor $\mathcal{S}$, $\mathcal{S}(t) = \{\alpha \in \Sigma \mid t\alpha \in \overline{K}\} = A_K(t)$, which means the set of the enabled or forced events after occurrence of the string t in the controlled process.

First let's consider the initial state, $t = \epsilon$. Since $TF(G_i) \neq \emptyset$ for all G_i's, $A_{TF(G_i)}(\epsilon) \neq \emptyset$ for all G_i's. Thus by $A(1)$, $\mathcal{S}(\epsilon) \cap A_{TF(G_i)}(\epsilon) \neq \emptyset$ for all G_i's. Thus

$$A_{L(\mathcal{S}/G_i)}(\epsilon) \neq \emptyset \quad \text{for all } G_i\text{'s.} \tag{1}$$

Suppose that for some G_i, $A_{L(\mathcal{S}/G_i)}(\epsilon) \supset A_{TF(G_i)}(\epsilon)$. Then there exists an event α satisfying $\alpha \in$

$A_{L(\mathcal{S}/G_i)}(\epsilon) \cap Dg_{TF(G_i)}(\epsilon)$. If α is not *tick*, it contradicts to $A(2)$. If α is *tick*, it contradicts to $A(3)$. So

$$A_{L(\mathcal{S}/G_i)}(\epsilon) \subseteq A_{TF(G_i)}(\epsilon) \qquad \text{for all } G_i\text{'s.} \tag{2}$$

Consider a case of $t \neq \epsilon$. According to the same procedure as the initial state, the following results can be proved.

$$A_{L(\mathcal{S}/G_i)}(t) \neq \emptyset \tag{3}$$

for each G_i satisfying $A_{TF(G_i)}(t) \neq \emptyset$.

$$A_{L(\mathcal{S}/G_i)}(t) \subseteq A_{TF(G_i)}(t) \tag{4}$$

for each G_i satisfying $A_{TF(G_i)}(t) \neq \emptyset$.

But there may be exist a string s such that $ts \in L(\mathcal{S}/G)$ and $ts \in RISK(G)$. For all G_i's $A(4)$ guarantees $L(\mathcal{S}/G_i) \cap RISK(G) = \emptyset$.

In summary, by (1), (2), (3), (4), it is true that for each G_i, there exists a K_i, $K_i \neq \emptyset$, such that $K_i \subseteq TF(G_i)$ and $L(\mathcal{S}/G_i) = \overline{K_i}$. Therefore $\mathcal{S}$ is a fault tolerant robust supervisor.

(Only if) Consider a supervisor $\mathcal{S}$, $\mathcal{S}(t) = \{\alpha \in \Sigma \mid t\alpha \in \overline{K}\} = A_K(t)$, which means the set of enabled or forced events after occurrence of the string t in the controlled process. And assume that $\mathcal{S}$ is a fault tolerant robust supervisor.

For each G_i satisfying $A_{TF(G_i)}(t) \neq \emptyset$, $\mathcal{S}(t) \cap A_{TF(G_i)}(t) \neq \emptyset$. This implies that $A_K(t) \cap A_{TF(G_i)}(t) \neq \emptyset$ $(A(1))$. For G_i's satisfying $tick \in Dg_{TF(G_i)}(t)$, $\mathcal{S}(t)$ has at least the one forcible event to preempt *tick*. That is, $\mathcal{S}(t) \cap (A_{TF(G_i)}(t) \cap \Sigma_{for,i}) \neq \emptyset$. This implies that $\mathcal{S}(t) \cap (A_{TF(G_i)}(t) \cap \Sigma_{for,i}) \neq \emptyset$ $(A(3))$.

Suppose that $\mathcal{S}(t) \supset SEL(t)$. Then for some G_i there exists an event α satisfying $\alpha \in \mathcal{S}(t) - SEL(t)$ and $\alpha \in Dg_{TF(G_i)}(t)$. Thus the controlled some G_i may be deviated from TFES of G_i. This contradicts to the fact that $\mathcal{S}$ is a fault tolerant robust supervisor. So $\mathcal{S}(t) \subseteq SEL(t)$, that is, $A_K(t) \subseteq SEL(t)$ $(A(2))$.

Since $\mathcal{S}$ is a fault tolerant robust supervisor, by Lemma 1 $L(\mathcal{S}/G) \cap RISK(G) = \emptyset$. Consider a case of $tick \notin SEL(t)$. Let $\alpha \in \Sigma_{uc}$ and assume that $t\alpha \in \overline{T(G)}$ but $t\alpha \notin \overline{K}$. Then there must exist a $\beta \in \Sigma^*$ such that $t\alpha\beta \in \overline{T(G)}$ and $t\alpha\beta \in RISK(G)$. So for some G_i, $t\alpha\beta \in L(\mathcal{S}/G_i)$. This contradicts to $L(\mathcal{S}/G) \cap RISK(G) = \emptyset$. Therefore $t\alpha \in \overline{K}$, that is, $A_K(t) \supseteq A_{T(G)}(t) \cap \Sigma_{uc}$.

Consider a case that for each G_i satisfying $tick \in A_{TF(G_i)}(t)$, $A_K(t) \cap (A_{TF(G_i)}(t) \cap \Sigma_{for,i}) \neq \emptyset$. Let $\alpha \in \Sigma$ and assume that $t\alpha \in \overline{T(G)}$ but $t\alpha \notin \overline{K}$. If $\alpha \in \Sigma_{uc}$, contradiction also happens by above result. If $\alpha = tick$, α can be preempted by events in $A_K(t) \cap (A_{TF(G_i)}(t) \cap \Sigma_{for,i})$. So $A_K(t) \supseteq A_T(t) \cap \Sigma_{uc}$.

Consider a case that for some G_i satisfying $tick \in A_{TF(G_i)}(t)$, $tick \in SEL(t)$ and $A_K(t) \cap (A_{TF(G_i)}(t) \cap \Sigma_{for,i}) = \emptyset$. Let $\alpha \in \Sigma$ and assume that $t\alpha \in \overline{T(G)}$ but $t\alpha \notin \overline{K}$. If $\alpha \in \Sigma_{uc}$, contradiction also happens by above result. If $\alpha = tick$, $L(\mathcal{S}/G_i) \cap RISK(G) \neq \emptyset$. It contradicts to the fact that $\mathcal{S}$ is a fault tolerant robust supervisor. So $A_K(t) \supseteq A_T(t) \cap (\Sigma_{uc} \cup \{tick\})$.

In summary, K satisfies $A(1)$, $A(2)$, $A(3)$ and $A(4)$. The proof is complete. □

4. Conclusions

The problem of supervisory control of timed DESs is developed to achieve fault-tolerant behavior of the systems with model uncetainty. When a given set of system models satisfies existence conditions developed in this paper, there always exists a fault-tolerant robust supervisor which assures fault-tolerance of the system.

References

[1] P. J. Ramadge and W. M. Wonham, "Supervisory control of a class of discrete event processes," *SIAM J. of Control and Optimization*, vol. 25, pp. 206-230, 1987.

[2] B. A. Brandin and W. M. Wonham, "Supervisory Control of Timed Discrete-Event Systems," *IEEE Trans. on Automatic Control*, vol. 39, no. 2, pp. 329-342, 1994.

[3] K.-H. Cho and J.-T. Lim, "Failure Diagnosis and Fault Tolerant Supervisory Control Systems," *IEICE Trans. Inf. and Syst.*, vol. E79-D, no. 9, pp. 1223-1231, 1996.

[4] Feng Lin, "Robust and Adaptive Supervisory Control of Discrete Event Systems," *IEEE Trans. on Automatic Control*, vol. 38, no. 12, pp. 1848-1852, 1993.