International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:10, No:9, 2016

Asynchronous Sequential Machines with Fault Detectors

Seong Woo Kwak, Jung-Min Yang

***Abstract*—**A strategy of fault diagnosis and tolerance for asynchronous sequential machines is discussed in this paper. With no synchronizing clock, it is difficult to diagnose an occurrence of permanent or stuck-in faults in the operation of asynchronous machines. In this paper, we present a fault detector comprised of a timer and a set of static functions to determine the occurrence of faults. In order to realize immediate fault tolerance, corrective control theory is applied to designing a dynamic feedback controller. Existence conditions for an appropriate controller and its construction algorithm are presented in terms of reachability of the machine and the feature of fault occurrences.

***Keywords*—**Asynchronous sequential machines, corrective control, fault diagnosis and tolerance, fault detector.

I. Introduction

CORRECTIVE control theory is a novel research approach to controlling the stable state behavior of asynchronous sequential machines. The basic configuration of corrective control is similar to that of traditional feedback control for continuous-time systems, but the way the control input is made is significantly different. As asynchronous sequential machines are classified as finite state discrete-event systems, generation of the control input and the operation of the closed-loop system must be considered in discrete mathematics and switching and finite automata theory. In the operation of asynchronous sequential machines working without no global synchronizing clock, only stable states are noticeable and practically meaningful [1]. Thus we say that a corrective controller achieves its control objective if the stable state behavior of the closed-loop system matches that of a pre-specified model.

Since first developed for general sequential machines in the mid 1990's [2], [3], corrective control theory has been mainly applied to tolerating or eliminating various deficiencies in asynchronous sequential machines. Reference [4] addresses the model matching problem for input/state asynchronous machines with critical races. Here, input/state asynchronous machines are referred to as those machines in which the current state is given as the output value. References [5], [6] extend the work of [4] to input/output asynchronous machines, where the output value is different from the machine's state. Reference [7] further generalizes the former studies by incorporating the information on the output burst. Reference [8] solves the model matching problem for input/state asynchronous machines subject to infinite cycles. References [9], [10] develop corrective controllers for diagnosing and tolerating transient faults that cause a violation of state transition characteristics of asynchronous machines. Reference [11] demonstrates that the control mechanism for transient faults can be implemented in real-world digital systems. In [12], a corrective controller is presented to realize model matching with the constraint that some external input characters are uncontrollable. A similar study with the application to error counters can be found in [13]. References [14], [15] present fault tolerant corrective control schemes for tolerating permanent faults occurring to input/output machines. Finally, [16] addresses identification and corrective control of asynchronous machines with unspecified transition parts based on an adaptive control law.

The objective of this paper is to present a scheme of fault diagnosis and tolerance for input/state asynchronous sequential machines subject to permanent state transition faults. Permanent state transition faults are defined as perpetual transformation of the feature of a transient pair to stable one caused by an occurrence of the adversarial input. Due to the absence of a global synchronizing clock, it is impossible for a corrective controller to diagnose permanent state transition faults only based on the state feedback. Hence, we propose a *fault detector* comprised of a timer and a set of static functions to determine the occurrence of faults. Note that in the case of transient faults [9]-[11], no fault detector is required since the change of the state feedback indicates an occurrence of an adversarial input. In order to realize immediate fault tolerance, corrective control theory is applied to designing a dynamic feedback controller. Existence conditions for an appropriate controller and its construction algorithm are presented in terms of reachability of the machine and the feature of fault occurrences.

The rest of this paper is organized as follows. In Section II, starting with background material on dynamics of asynchronous sequential machines, we present a model of permanent state transition faults and the basic configuration of the fault tolerant corrective controller. In Section III, we propose the structure of the fault detector and show that

The research of S. W. Kwak was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. NRF–2016R1D1A1B02012959). The research of J.-M. Yang was supported in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and future Planning (No. NRF–2015R1A2A1A15054026), in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. NRF–2015R1D1A1A01056764), and in part by the Bio & Medical Technology Development Program of the National Research Foundation (NRF) funded by the Korean government (MSIP) (No. NRF–2015M3A9A7067220).

S. W. Kwak is with the Department of Electronic Engineering, Keimyung University, Daegu, 42601, Republic of Korea (e-mail: ksw@kmu.ac.kr).

J.–M. Yang is with the School of Electronics Engineering, Kyungpook National University, Daegu, 41566, Republic of Korea (corresponding author; e-mail: jmyang@ee.knu.ac.kr).

the proposed fault detector can diagnose any occurrence of permanent state transition faults, which can be utilized to realize fault tolerant corrective controllers. Finally, Section IV summarizes the main contributions of the paper.

II. Preliminaries

A. Modeling of Asynchronous Machines

An input/state asynchronous machine Σ is modeled by the following deterministic finite-state machine.

$$\Sigma = (A, X, x_0, f)$$

where A is the input set, X is the state set, $x_0 \in X$ is the initial state, and

$$f : X \times A \to X$$

is the state transition function partially defined on $X \times A$. Owing to the lack of a synchronizing clock, a valid state–input pair $(x, v') \in X \times A$ is either stable or transient according to $f(x, v)$:

$$(x, v) = \begin{cases} \text{stable} & f(x, v) = x \\ \text{transeint} & f(x, v) \neq x \end{cases}$$

Σ stays at a stable pair (x, v') indefinitely unless the external input changes. If the input is switched to a new character v such that $f(x, v) \neq x$, then (x, v) is a transient pair and Σ initiates a chain of transient transitions, e.g.,

$$\begin{aligned} f(x, v) &= x_1, \\ f(x_1, v) &= x_2, \\ &\vdots \end{aligned}$$

while the input v remains fixed. Under the asynchronous mechanism, Σ traverses transient states $x_1, x_2, \ldots$, instantaneously. If Σ has no infinite cycle, this chain of transitions will end at a stable state x' such that $f(x', v) = x'$. x' is called the next stable state of (x, v).

It is often convenient to express the dynamics of Σ only in terms of stable states, since transient states are unnoticeable from the viewpoint of outer users. The *stable recursion function*

$$s : X \times A \to X$$

[4] is defined for this purpose. For a valid state–input pair (x, v),

$$s(x, v) := x'$$

where x' is the next stable state of (x, v). If (x, v) is a stable pair, $s(x, v) = x$. The chain of transitions from (x, v) to (x', v), represented by $s(x, v) = x'$, is termed a *stable transition*. For later usage, define two input sets $U(x), T(x) \subset A$ with respect to $x \in X$ as

$$\begin{aligned} U(x) &:= \{v \in A | s(x, v) = x\} \\ T(x) &:= \{v \in A | s(x, v) \neq x\}. \end{aligned}$$

$U(x)$ and $T(x)$ denote the set of input characters that make a stable and transient pair with x, respectively. We can extend the domain of s from input characters to strings. For $x \in X$ and $v_1 v_2 \cdots v_k \in A^+$, where A^+ is the set of all non-empty strings of characters in A,

$$s(x, v_1 v_2 \cdots v_k) := s(s(x, v_1), v_2 \cdots v_k).$$

If an input string $t \in A^+$ exists for two states x and x' such that $x' = s(x, t)$, x' is said to be *stably reachable* from x in Σ [4].

To represent the underlying transient states that are traced from a given transient pair (x, v), we define a partial function

$$\tau : X \times A \to P(X),$$

where $P(X)$ is the power set of X:

$$\tau(x, v) := \begin{cases} \{x, x_1, \ldots, x_{k-1}\} & s(x, v) \neq x \\ \varnothing & s(x, v) = x \end{cases} \quad (1)$$

$\tau(x, v)$ is the set of all transient states traversed by Σ when it goes on a chain of transitions starting from (x, v). Since a stable pair does not involve any transient state, $\tau(x, v) = \varnothing$ if $s(x, v) = x$.

In this paper, we assume that Σ suffers from permanent state transition faults, namely by an occurrence of a fault input, a transient state–input pair is transformed into a stable one. To describe permanent state transition faults, we introduce the following definition.

Definition 1: Given $\Sigma = (A, X, x_0, f)$, let

$$F := \{f_1, \ldots, f_r\}$$

be the set of permanent state transition faults, and let

$$H := \{(z_1, w_1), \ldots, (z_r, w_r)\} \subset X \times A$$

be the set of associated transient state–input pairs. f_i, the ith permanent state transition fault, alters perpetually the transition characteristics of (z_i, w_i)' from transient to stable, i.e.,

$$s(z_i, w_i) \neq z_i \xrightarrow{\text{fault } f_i} s(z_i, w_i) = z_i.$$

Each f_i is supposed to be distinctive with one another. On the other hand, z_i and z_j are not necessarily disjoint with each other. If $z_i = z_j$, however, w_i must differ from w_j; otherwise, f_i and f_j would correspond to the same state–input pair.

B. Closed-Loop System

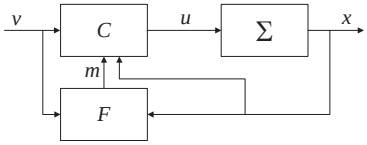

Fig. 1 Corrective control system with a fault detector

Fig. 1 shows the configuration of the proposed corrective control system for Σ. C is a corrective controller having the form of an input/output asynchronous machine. $v \in A$ is the external input, $u \in A$ is the control input provided by C, and x is the state feedback of Σ. D denotes a *fault detector* positioned in the feedback path to detect occurrences of fault inputs F. Receiving x and v, D provides C with a logical value $m \in \{0, 1\}$, called the *fault indicator signal*, that

indicates whether a permanent state transition fault occurs. Let us denote by Σ_c the closed-loop system comprised of C, D, and Σ. With no synchronizing clock, the external input v also varies asynchronously. In this study, we assume that any interval between two consecutive external inputs is greater than or equal to the *minimum interval* T_v. In other words, the external input must not change too quickly, which fits into common operations of sequential machines.

When Σ shows the normal behavior, C relays the external input v to the control input channel u without modification. When a permanent state transition fault occurs, the notification of the fault occurrence is transmitted to C via the signal $m = 1$. C generates an appropriate control input sequence so that Σ_c seems to maintain the normal operation despite the fault occurrence. In this paper, we study the single fault scenario [17] in which at most one of the fault events $f_1, \ldots, f_r$ may occur at a time.

When working with asynchronous machines, it is important to comply with the principle of fundamental mode operations [18], an operating policy that prohibits the simultaneous change of two or more system variables. This policy is intended to prevent any unpredictable outcome that attributes to asynchronous mechanisms. Adapting the results of [11], we obtain the following conditions to ensure fundamental mode operations of the closed-loop system Σ_c in Fig. 1.

Condition 1: The closed-loop system Σ_c in Fig. 1 operates in fundamental mode if and only if all the following requirements are met:

(a) Σ is at a stable state when C undergoes transitions.
(b) C is at a stable state when Σ undergoes transitions.
(c) The variables v and m change their values only when Σ and C are both at stable states, and then only one at a time.

According to Condition 1.(b), C must be designed so that it commences transitions only after verifying Σ has reached a stable pair, and must adopt a stable pair immediately prior to providing the control input u to Σ. Similarly, the fault detector D must generate the fault indicator signal m only when both Σ and C are at stable states and v does not change its value. C and D will be designed so as to satisfy all these requirements (Condition 1.(c)). The fundamental mode operation assures that all transitions of Σ_c are unambiguous and deterministic.

III. Fault Detector

A. Structure of Fault Detector

Consider a state–input pair (z_i, w_i) at which Σ may experience the permanent state transition fault f_i. Since the moment that f_i occurs to Σ is indeterminate in general, we must examine as below all the possible instances to derive detectability.

(i) First, assume that Σ has been staying at a stable pair (z_i, v) with $v \in U(z_i)$ when the fault f_i happens. The fault occurrence is not perceived at this instant because no explicit change of the system variables is observed. Suppose further that the external input changes to w_i. Were it not for the fault f_i, Σ would go through the normal stable transition from z_i to $s(z_i, w_i)$. With the incidence of f_i, however, Σ does not respond to w_i; it is stuck at z_i unless a fault-tolerant control scheme is activated. If the fault is not recovered immediately, further change of the external input would drive Σ to an incorrect next stable state, possibly leading to total breakdown of the machine.

(ii) Next, assume that for a transient pair (x, w_i) with $x \neq z_i$, z_i is an element of $\tau(x, w_i)$ where $\tau(x, w_i)$ is defined in (1). This implies that Σ passes through the transient pair (z_i, w_i) during the course of the stable transition from x to $s(x, w_i)$. Note that $s(x, w_i) = s(z_i, w_i)$ if $z_i \in \tau(x, w_i)$. If f_i has occurred before Σ begins this transition, Σ falls into z_i instead of reaching the next stable state $s(x, w_i)$. Likewise, further change of the external input would cause incorrect subsequent behaviors.

In both (i) and (ii), the result of the fault occurrence is the same: Σ does not respond to the last changed variable, either it is z_i or w_i. In case (i), for instance, if Σ has been staying at the stable state z_i, it does not carry out the innate transition from z_i to $f(z_i, w_i)$ in response to the changed input w_i after the fault occurrence. Thus we can know the occurrence of f_i by measuring the dead-lock time that lapses away from the instant that the last changed variable of (z_i, w_i) enters Σ. If the dead-lock time is greater than the prescribed threshold, we regard that f_i occurs.

The fault detector D in Fig. 1 plays the role of detecting faults using the foregoing criterion. It records the entrance time of the last changed variable among z_i and w_i, and it measures the duration during which neither the state nor input changes its value after the entrance time of the last changed variable. The fault indicator signal m is generated by the following function.

$$\nu : X \times A \times T \to \{0, 1\}$$
$$m = \nu(x, v, t) := \begin{cases} 1 & (x, v) \in H \text{ and } t \geqslant T_h \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

where t is the measured dead-lock time and T_h is the pre-determined threshold. Consider again case (i) where w_i enters Σ that has been stuck at z_i by the fault f_i. In view of Fig. 1, D records the entrance time of w_i and measures the dead-lock time t thereafter. If f_i does not occur, Σ would transfer to $f(z_i, w_i)$ instantaneously and the state feedback x would change to $f(z_i, w_i)$ right after the entrance of w_i. According to (2), we have

$$\nu(z_i, w_i, t) = 0 \quad \because t \ll T_h$$
$$\nu(f(z_i, w_i), w_i, t) = 0 \quad \because (f(z_i, w_i), w_i) \notin H.$$

Hence the fault indicator signal m remains 0. On the other hand, after the occurrence of f_i, the dead-lock time t is prolonged indefinitely. At the moment that t becomes equal to T_h, D generates the indicator signal of fault detection, namely $m = 1$. The fault detection procedure in case (ii) is analyzed in a similar manner. Recalling that T_v is the minimum interval between two consecutive external inputs, we must select T_h such that

$$T_h < T_v.$$

Otherwise, the external input might change its value before the dead-lock time accumulates to the threshold value T_h.

B. Fault Tolerant Control

We first review the existence condition and the operation of corrective controllers solving model matching problems addressed in the prior work [4]. The objective is to design a controller C so that the closed-loop system Σ_c in Fig. 1 (without D) can transfer from a state z to the desired state z' in response to an external input a. This implies that the next stable state of (z, a) is not equal to z', i.e., $s(z, a) \neq z'$, or (z, a) may not be even a valid pair of Σ. In the framework of corrective control, the necessary and sufficient condition for realizing the desired stable transition from z to z' is that z' is stably reachable from z [4], that is,

$$[\Sigma_c : z \rightarrow z'] \Leftrightarrow [\exists \alpha = u_1 \cdots u_k \in A^+ \text{ s.t. } s(z, \alpha) = z']. \quad (3)$$

C utilizes α to make a correction trajectory from z to z'. Under the principle of fundamental mode operations, Σ must stay at the stable state z when the external input changes to a (see Condition 1.(a)). In view of Fig. 1, C suppresses the incoming input a and instead generates the first input character u_1 of α. Σ then transfers to the next stable state $s(z, u_1)$. Receiving $s(z, u_1)$ as the state feedback, C undergoes its own state transition and generates the second character u_2, in response to which Σ moves to the second next stable state $s(s(z, u_1), u_2)$ and so on. The interaction between C and Σ is conducted very fast due to the lack of a synchronizing clock. Hence the closed-loop system Σ_c seems to move from z to z' instantaneously in response to a, which accomplishes the objective of model matching.

The condition (3) is equally applied to fault-tolerant control for permanent state transition faults with little modification. We can regard fault recovery as another model matching problem. When we detect an occurrence of f_i by observing that Σ is stuck at the transient state z_i longer than T_h, a control law must be activated that takes Σ_c immediately toward the desired state $s(z_i, w_i)$. The existence condition for the controller is easily derived from (3) as

$$\exists \alpha_i \in A^+ \text{ such that } s(z_i, \alpha_i) = s(z_i, w_i) \text{ and } \alpha_i \neq w_i, \ \forall w_i \in W_i. \quad (4)$$

$\alpha_i \neq w_i$ means that the correction trajectory must detour the faulty transient pair (z_i, w_i). The procedure of the correction procedure will be constructed in a similar manner to the previous results [11], [14].

IV. Summary

We have presented a corrective control scheme for asynchronous sequential machines with permanent state transition faults. Main consideration is devoted to proposing a fault detection and tolerance scheme for permanent state transition faults. Necessary and sufficient conditions for the existence of the fault detector and corrective controller are analyzed in the framework of corrective control.

References

[1] J. Sparsø and S. Furber, *Principles of Asynchronous Circuit Design — A Systems Perspective*, Kluwer Academic Publishers, 2001.
[2] J. Hammer, "On the corrective control of sequential machines," *Int. J. Control*, vol. 65, no. 2, pp. 249–276, 1996.
[3] J. Hammer, "On the control of sequential machines with disturbances," *Int. J. Control*, vol. 67, no. 3, pp. 307–331, 1997.
[4] T. E. Murphy, X. Geng, and J. Hammer, "On the control of asynchronous machines with races," *IEEE Trans. Autom. Control*, vol. 48, no. 6, pp. 1073–1081, 2003.
[5] J. Peng and J. Hammer, "Input/output control of asynchronous sequential machines with races," *Int. J. Control*, vol. 83, no. 1, pp. 125–144, 2010.
[6] X. Geng and J. Hammer, "Input/output control of asynchronous sequential machines," *IEEE Trans. Autom. Control*, vol. 50, no. 12, pp. 1956–1970, 2005.
[7] J. Peng and J. Hammer, "Bursts and output feedback control of non-deterministic asynchronous sequential machines," *European J. Control*, vol. 18, no. 3, pp. 286–300, 2012.
[8] N. Venkatraman and J. Hammer, "On the control of asynchronous sequential machines with infinite cycles," *Int. J. Control*, vol. 79, no. 7, pp. 764–785, 2006.
[9] J.–M. Yang, "Corrective control of input/output asynchronous sequential machines with adversarial inputs," *IEEE Trans. Autom. Control*, vol. 55, no. 3, pp. 755–761, 2010.
[10] J.–M. Yang and J. Hammer, "Asynchronous sequential machines with adversarial intervention: the use of bursts," *Int. J. Control,* vol. 83, no. 5, pp. 956–969, 2010.
[11] J.–M. Yang and S. W. Kwak, "Realizing fault-tolerant asynchronous sequential machines using corrective control," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 6, pp. 1457–1463, 2010.
[12] J.–M. Yang and S. W. Kwak, "Model matching for asynchronous sequential machines with uncontrollable inputs," *IEEE Trans. Autom. Control*, vol. 56, no. 9, pp. 2140–2145, 2011.
[13] J.–M. Yang and S. W. Kwak, "Corrective control of asynchronous machines with uncontrollable inputs: application to single-event-upset error counters," *IET Control Theory Appl.*, vol. 4, no. 11, pp. 2454–2462, 2010.
[14] J.–M. Yang, "Fault tolerance in asynchronous sequential machines using output feedback control," *IEEE Trans. Autom. Control*, vol. 57, no. 6, pp. 1604–1609, 2012.
[15] J.–M. Yang and S. W. Kwak, "Fault diagnosis and fault-tolerant control of input/output asynchronous sequential machines," *IET Control Theory Appl.*, vol. 6, no. 11, pp. 1682–1689, 2012.
[16] J.–M. Yang, T. Xing, and J. Hammer, "Adaptive control of asynchronous sequential machines with state feedback," *European J. Control*, vol. 18, no. 6, pp. 503–527, 2012.
[17] S. Shu and F. Lin, "Fault-tolerant control for safety of faulty discrete event systems," *IEEE Trans. Auto. Sci. Engr.*, vol. 11, no. 1, pp. 78–89, 2014.
[18] Z. Kohavi and N. K. Jha, *Switching and Finite Automata Theory*, 3rd ed. Cambridge University Press: Cambridge, UK, 2010.