'95 KACC (1995. 10. 23 ~ 25)

FAULT TOLERANT SUPERVISORY CONTROL SYSTEM AND AUTOMATED FAILURE DIAGNOSIS

°K.-H. Cho* and J.-T. 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 : ckh@stcon1.kaist.ac.kr

Abstracts We propose in this paper a systematic way for analyzing discrete event dynamic systems to classify faults and failures quantitatively and to find tolerable fault event sequences embedded in the system. An automated failure diagnosis scheme with respect to the nominal normal operating event sequences and the supervisory control problem for tolerable fault event sequences is presented. Moreover the supervisor failure diagnosis problem with respect to the tolerable fault event sequences is considered. Finally, a plasma etching system example is presented.

Keywords Discrete event dynamic system, Failure Analysis, Failure diagnosis, Supervisory control, Fault tolerant system

1. Introduction

1.1 *Overview*

As the demands on reliability and safety of modern complicated systems increase, the systematic and organizational methods for improving the supervision and monitoring are getting an increasing interest. In addition, the problem of failure diagnosis has received considerable attention and a wide variety of schemes have been proposed.

We propose a DEDS approach to the failure diagnosis problem on the work in [5], where the detection problem of the unobservable failure events on the basis of the observed events has been studied. Throughout this paper, we assume that a supervisor can record all the state transitions and events generated by the plant. In this paper, a systematic way for analyzing DEDSs is proposed to classify faults and failures quantitatively and to find tolerable fault event sequences embedded in the system. An automated failure diagnosis scheme with respect to (w.r.t.) the nominal normal operating event sequences and the supervisory control problem for tolerable fault event sequences is presented. Moreover the supervisor failure diagnosis problem w.r.t. the tolerable fault event sequences is considered. Finally, a semiconductor process — plasma etching system — example is presented.

1.2 *Notations*

- $A(x)$: The set of events possible to occur after state x.
- $B(x)$: The set of events possible to occur before state x.
- $D(a)$: The starting state of event a (domain of a).
- $R(a)$: The ending state of event a (range of a).
- aug-event : The event augmented with its originating state.
- $Ac(x)$: The set of events in the driving sequence from initial state to x.

2. Failure Analysis

In this section, the quantitative definitions of faults and failures with their classification algorithm are presented.

The unexpected changes in the system can be described as the set of abnormal events which are not expected to occur during the normal operating mode. Let Σ_{an} be the set of abnormal events and Σ_n be the set of normal events. The set Σ_{an} is a subset of Σ_{uc} and the total set of events Σ can be partitioned as $\Sigma = \Sigma_c \dot{\cup} \Sigma_{uc} = \Sigma_n \dot{\cup} \Sigma_{an}$. Assume that the set of marker states is partitioned according to the operating mode of the system, i.e., $Q_m = Q_{m_1} \dot{\cup} Q_{m_2} \dot{\cup} \cdots \dot{\cup} Q_{m_k} = \dot{\bigcup}_{i=1}^{k} Q_{m_i}$. Then Σ_{an} can be further partitioned by the set of fault and failure events defined in the following with their originating states.

Definition 1 (fault) The aug-event (σ_f, x_f) is a "fault w.r.t. Q_{m_i}" and σ_f is called a "fault event" if

(i) $\sigma_f \in \Sigma_{an}$,

(ii) there exists at least one event string $s \in L/\sigma_f := \{t \in \Sigma^* | \sigma_f t \in L\}$ such that $\sigma_f s$ leads to the marker states set Q_{m_i} and for each aug-event (s_i, x_i) of $s = s_1 s_2 \cdots s_n$, any $\sigma \in A(x_i) - \{s_i\}$ for all s_i corresponding to x_i belongs to Σ_c or is an another fault event.

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

To classify fault and failure in quantitative manner, we define a index function as follows.

Definition 3 (index function) The "index function" of each state x, $I_{m_i}(x)$, is defined according to the corresponding set of marker states Q_{m_i} as; $I_{m_i}(x) := 1$if $x \in Q_{m_i}$ or if there exists $\sigma \in A(x)$ such that $I_{m_i}(R(\sigma)) = 1$ and any $\sigma' \in A(x) - \{\sigma\}$ is in Σ_c or $I_{m_i}(R(\sigma')) = 1$, otherwise $I_{m_i}(x) := 0$.

For each state of a given DEDS, we can assign systematically the value of index function through the following algorithm.

Algorithm

Step 1. Assign $I(x_m) = 1$ *where* $x_m \in Q_m$.

Step 2. For each $x_i \in D(B(x_j))$ *where* $I(x_j) = 1$, *assign* 1 *if* $I(R(A(x_i) - B(x_j))) = 1$ *or* $A(x_i) - B(x_j) \subset \Sigma_c$.

Step 3. Assign 0*'s for all the remained states.*

For a given DEDS, we can classify faults and failures quantitatively through the following proposition.

Proposition 1 (failure analysis) The aug-event (σ, x) with $\sigma \in \Sigma_{an}$ is a fault w.r.t. Q_{m_i} if and only if $I_{m_i}(x) = 1$ and it is a failure w.r.t. Q_{m_i} if and only if $I_{m_i}(x) = 0$.

3. Failure Diagnosis and Fault Tolerant System

The nominal work procedure in the system can be represented by some normal event sequences whether an unexpected change may deviate them to certain failures or not. We can formally define such event sequences as follows.

Definition 4 (NNOES) The normal events sequence which derives the initial state to the marker one is called a "nominal normal operating events sequence (NNOES)" since it represents a nominal operating sequence when a given system is in its normal status.

During the work process along the NNOES, an unexpected change may deviate it to a certain failure. In this case, the origin of deviation is called a source failure and is defined formally as follows.

Definition 5 (source failure) For a given failure, the failure that makes the given failure event be deviated from the NNOES for the first time is called a "source failure" of the given failure.

To maintain a high level of performance for complex systems, e.g., power plants and semiconductor processes, etc., it is crucial that failures are detected promptly and diagnosed so that corrective action can be taken to reconfigure the control system. For a systematic failure diagnosis, we define a set of node functions in the following.

Definition 6 (node function) A set of "node functions" of x, $S_{J_i}(x) = \{J_i(x)\}$, w.r.t. i_{th} NNOES is defined as; $J_i(x) := (2n+1)2^m$ if x is reachable from states in i_{th} NNOES, which is again reachable from the initial state by n transitions, and there are m abnormal events in the transitions from NNOES and the first of them is abnormal, otherwise $J_i(x) := 0$.

Then we can know the source failure and the number of abnormal events occurred from NNOES for a given failure by the following proposition.

Proposition 2 (failure diagnosis) The set of source failures of (σ_f, x) w.r.t. i_{th} NNOES is $S_{f_i}(x) := \{(\sigma_{f_s}, x_s)\}$ where $J_i(x_s) = J_i(x) \bmod 2$ with $J_i(x) \neq 0$ and the number of abnormal events occurred from i_{th} NNOES is (number of abnormal events) $= \log_2 J_i(x) - \log_2 J_i(x_s)$.

When some abnormal events occurred during the work process, if we can still find an another event sequence reachable to the marker states or if we can eliminate the path to the abnormal events, then the work procedure is called fault tolerable.

Definition 7 (TFES) The events sequence which consists of normal events or fault events and which derives the initial state to the marker one is called a "tolerable fault events sequence (TFES)" if, for each normal event, all the possible events following the corresponding state belong to Σ_c or another fault events.

Once TFES is found, we can make the system evolve along the TFES through supervisor. The supervisor is designed on the basis of recognizer for L_g which is interpreted as "legal behavior' [1]. In this case, let $L_c(\mathcal{S}/G) = L_g =$ TFES $\subset L_m(G)$. Thus if we find TFES, the supervised fault tolerant system can be easily constructed.

Although we designed a fault tolerant system, a certain failure or any other aug-event not in the TFES may be reached due to the supervisor failure. In this case, a diagnosis is also required to find the source supervisor failure and to take a corrective action promptly.

Definition 8 (supervisor failure) Any aug-event which is not included in the TFES is called a "supervisor failure".

Definition 9 (source supervisor failure) For a given

supervisor failure, the aug-event (σ, x) where $\sigma \in \Sigma_c$, that makes the given failure be deviated from TFES for the first time is called a "source supervisor failure" of the given failure.

For a supervisor failure diagnosis, we define a set of modified node functions in the following.

Definition 10 (modified node function) A set of "modified node functions" of x, $S_{J_i'}(x) = \{J_i'(x)\}$, w.r.t. i_{th} TFES is defined as; $J_i'(x) := (2n+1)2^m$ if x is reachable from states in i_{th} TFES, which is again reachable from the initial state by n transitions, and there are m abnormal events in the transitions from TFES and the first of them is controllable, otherwise $J_i'(x) := 0$.

Then we can know the source supervisor failure and the number of abnormal events occurred from TFES for a given supervisor failure similarly to the failure diagnosis case by the following proposition.

Proposition 3 (supervisor failure diagnosis) The set of source supervisor failures of (σ_f, x) w.r.t. i_{th} TFES is $S_{f_i'}(x) := \{(\sigma_{fs}, x_s)\}$ where $J_i'(x_s) = J_i'(x) \bmod 2$ with $J_i'(x) \neq 0$ and $I(x_s) = 1$ and the number of abnormal events occurred from i_{th} TFES is (number of abnormal events) $= \log_2 J_i'(x) - \log_2 J_i'(x_s)$

4. Application to Plasma Etching System

Plasma etching is a critical technology for modern VLSI circuits fabrication at many steps of the manufacturing process [3] [4]. However, despite its widespread use, plasma etching remains a poorly understood operation and it is also difficult to obtain its mathematical model. Hence plasma etching system is suited to be analyzed in DEDS framework and we illustrate our approach to failure diagnosis with it. Fig. 5. illustrates a overall plasma etching system [3]. The manipulated variables are plasma species densities ($[CF_4]$, $[O_2]$, [Ar]), flow rate, RF power (E), and pressure (P) in the plasma chamber. The control objective is to maintain a constant flow rate and a constant electric field to pressure ratio in the plasma chamber.

Consider the part of B and C in Fig. 5.. Suppose that only the RF generator of the system is subject to abnormal events. Fig. 5. illustrates the component models. In Fig. 5., PW_U (PoWer_Up), PW_S (PoWer_Set), and PW_D (PoWer_Down) are normal events and, PW_US (PoWer_Up Stuck) and PW_DS (PoWer_Down Stuck) are abnormal events of RF generator. The pressure controller issues commands of W (valve Wider), S (valve Set), and N (valve Narrower). The DEM of the overall system is illustrated in Fig. 5.. The composed states and their contents are shown in Table 5.. In this case, the initial state is 1 and the marker states are 7, 8, 14, 15 if we consider only transient period. That is, the control objective of constant electric field to pressure ratio still can be satisfied by tuning the pressure controller even though RF generator malfunction may occur during the transient period. The index function values of each state are shown in the graph. From these, we can classify faults and failures according to the Proposition 1. There are 2 TFESs according to the operating mode. The 1st TFES is $1 \rightarrow 6 \rightarrow 7$ and the 2nd TFES is $1 \rightarrow 11 \rightarrow 14$. This system is fault tolerable. Hence we can construct a supervised fault tolerant system. The design procedure of supervisor is given in the next.

In this case, $\Sigma_c = \{\text{PW\_S} : c_1, \text{PW\_U} : c_2, \text{PW\_D} : c_3, \text{S} : c_4, \text{W} : c_5, \text{N} : c_6\}$ and $\Sigma_{uc} = \{\text{PW\_US}, \text{PW\_DS}\}$. Let $L_g = \text{TFES1,2}$. L_g is both controllable and $L_m(G)$-closed. Thus there exists a proper supervisor $\mathcal{S} = (S, \phi)$ [1] such that $L_c(\mathcal{S}/G) = L_g$. The state transition diagram for L_g in Fig. 5. can serve to define S; it just remains to identify the state feedback map ϕ. For each state x of S, $\phi(x)$ is a map

$$\phi(x) : \{c_1, c_2, \cdots, c_6\} \mapsto \{0, 1\},$$

i.e., a binary evaluation of each of the controls $c_1 \sim c_6$. Thus it is enough to define

$$\phi(x)(c_i) = \begin{cases} 1 & \text{if an edge corresponding to } c_i \text{ is on TFES,} \\ 0 & \text{otherwise.} \end{cases}$$

The resulting control patterns are shown in Table 5.. The supervisor $\mathcal{S} = (S, \phi)$ then certainly determines

$$L(\mathcal{S}/G) = \bar{L}_g, \quad L_m(\mathcal{S}/G) = L_g.$$

Furthermore $\mathcal{S}$ is complete w.r.t. G and there exists only a identity map for a projection π since identity map $I : x \mapsto x$ serves as a projection and the projection is unique for a complete supervisor. Thus $\mathcal{S}$ is also a quotient supervisor [1].

For supervisor failure diagnosis, the sets of modified node function values are denoted also in Fig. 5. The sets of modified node function values w.r.t. the 2nd TFES ($\{\ \}^2$) are omitted since they are symmetric with those w.r.t. the 1st TFES. If a certain supervisor failure is detected then we can find its source supervisor failure from these values according to the Proposition 3.

5. Conclusions

In this paper, we have discussed failure analysis and diagnosis issues relating to large complex systems from the point of view of DEDS. The focus of the present paper has been on analyzing DEDSs to classify faults and failures quantitatively and to find TFESs embedded in the system. An automated failure diagnosis scheme w.r.t. the NNOESs and the supervisory control problem for TFESs have been presented. Moreover the supervisor failure diagnosis problem w.r.t. the TFESs has been considered. Finally, the plasma etching system example has been presented.

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] W. M. Wonham and P. J. Ramadge, "On the supremal controllable sublanguage of a given language", *SIAM J. of Control and Optimization*, vol. 25, pp. 637–653, 1987.

[3] K. J. McLaughlin, T. F. Edgar, and I. Trachtenberg, "Real-time monitoring and control in plasma etching", *IEEE Control Systems*, pp. 3–10, April 1991.

[4] B. A. Rashop *et al.*, "Real-time control of reactive ion etching : identification and disturbance rejection", in *Proc. Conf. on Decision and Control*, pp. 3379–3385, 1993.

[5] M. Sampath *et al.*, "Failure diagnosis using discrete event models", in *Proc. Conf. on Decision and Control*, pp. 3110–3116, 1994.

Table 1. States definition of DEM in example 2

state	contents
1	PC_A, VSET, PWSET
2	PC_A, VSET, PWUP
3	PC_A, VSET, PWUSTUCK
4	PC_A, VSET, PWDOWN
5	PC_A, VSET, PWDSTUCK
6	PC_B, VWIDER, PWSET
7	PC_B, VWIDER, PWUP
8	PC_B, VWIDER, PWUSTUCK
9	PC_B, VWIDER, PWDOWN
10	PC_B, VWIDER, PWDSTUCK
11	PC_C, VNARROWER, PWSET
12	PC_C, VNARROWER, PWUP
13	PC_C, VNARROWER, PWUSTUCK
14	PC_C, VNARROWER, PWDOWN
15	PC_C, VNARROWER, PWDSTUCK

Table 2. Control data for $\mathcal{S}$

state	x_0	x_1	x_2	x_3	x_4
ϕ	000011	010000	000000	001000	000000

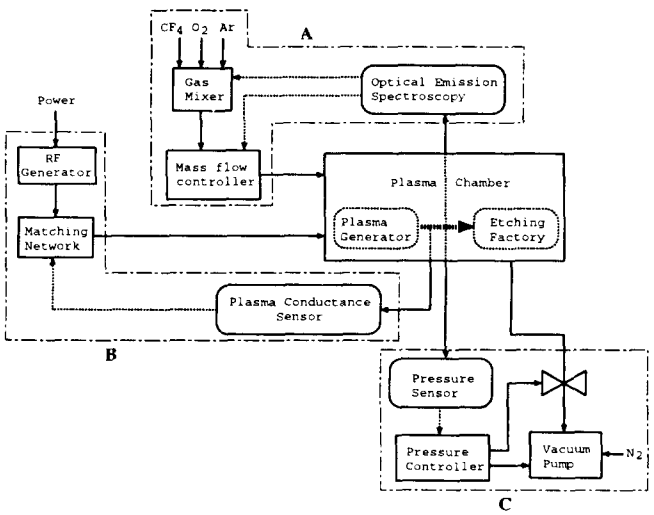

Fig. 1. Overall block diagram of plasma etching system

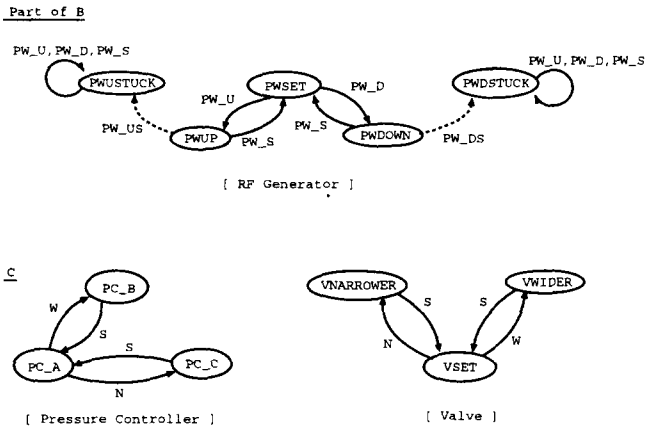

Fig. 2. DEM of components of part B and C

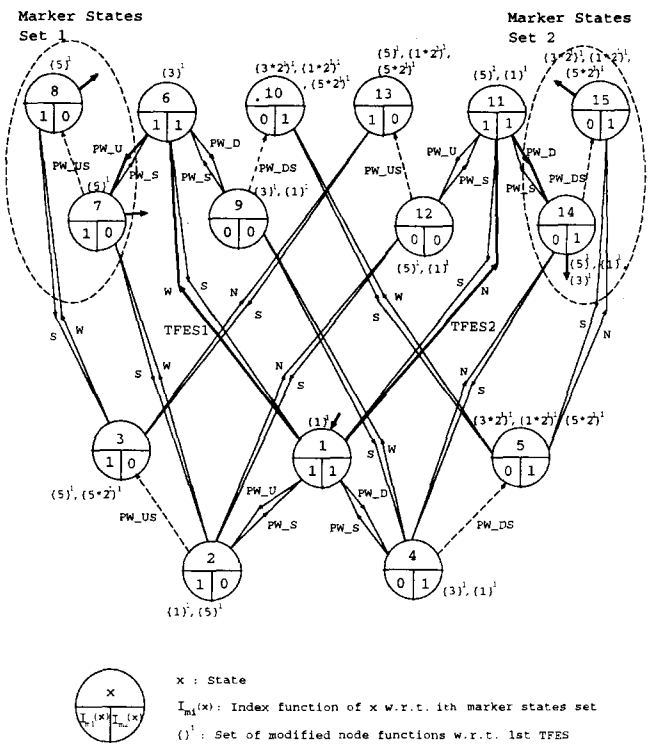

Fig. 3. Supervisor failure diagnosis : DEM of part B and C

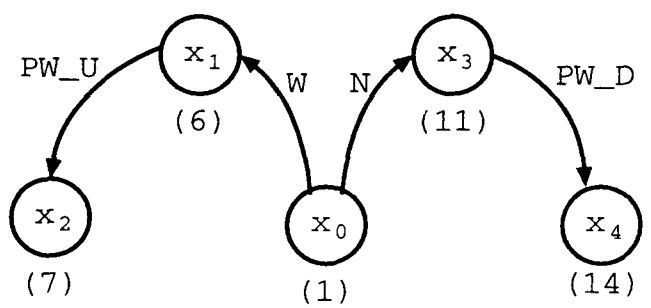

Fig. 4. Recognizer for L_g