QUALITY AND RELIABILITY ENGINEERING INTERNATIONAL
Qual. Reliab. Engng. Int. **14**: 319–330 (1998)

A PETRI NET APPROACH TO EARLY FAILURE DETECTION AND ISOLATION FOR PREVENTIVE MAINTENANCE

S. K. YANG AND T. S. LIU*

Department of Mechanical Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan, ROC

SUMMARY

To improve preventive maintenance, this study uses a hybrid Petri net modelling method coupled with parameter trend and fault tree analysis to perform early failure detection and isolation. A Petri net arrangement is proposed that facilitates alarm, early failure detection, fault isolation, event count, system state description and automatic shutdown or regulation. These functions are very useful for health monitoring and preventive maintenance of a system. A fault diagnosis system for district heating and cooling facilities is employed as an example to demonstrate the proposed method. ©1998 John Wiley & Sons, Ltd.

KEY WORDS: hybrid Petri nets; early failure detection and isolation; preventive maintenance; trend chart; threshold; fault tree analysis

INTRODUCTION

Preventive maintenance (PM) means all actions intended to keep equipment in good operating condition and to avoid failures [1]. PM should be able to indicate when a failure is about to occur, so that repair can be performed before such failure causes damage or capital investment loss. It is very important for any equipment whose failure may lead to severe consequences such as public hazard or financial loss. Such equipment includes nuclear power plants, passenger vehicles and semiconductor production lines. There are three main types of maintenance and three major divisions of PM, as illustrated in Figure 1 [1]. The most common strategy for maintenance is scheduled maintenance, i.e. maintenance is executed by time, by operation times, by material or by some other prescribed criterion. There are at least two drawbacks to this type of maintenance.

1. Criteria on which scheduled maintenance is based are statistical averages, e.g. mean time to failure. This makes the risk unavoidable that a system will fail before criteria are exceeded, i.e. a failure may occur unexpectedly.
2. The actual working lives of certain parts or modules may be longer than those averages, but such items are replaced during scheduled maintenance before they are worn out, resulting in waste.

In contrast, condition monitoring can be a better and more cost-effective type of maintenance than scheduled maintenance. However, it must be capable of detecting incipient failures prior to their occurrence.

The relationship between error, failure and fault is illustrated in Figure 2. The three terms are defined as follows [2].

1. *Error* is a discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.
2. *Failure* is an event when a required function is terminated (exceeding the acceptable limits).
3. *Fault* is the state characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions or due to lack of external resources.

Based on the above statements, an error is not a failure and a fault is hence a state resulting from a failure. An error is sometimes referred to as an incipient failure [3]. Therefore PM action is taken when the system is still in an error condition, i.e. within acceptable deviation and before failure occurs. Thus, through the technique of PM, failure can be detected early.

There have been many methods proposed for early failure detection [4–6]. This study employs the Petri net modelling method coupled with parameter trend and fault tree analysis to perform early failure detection and isolation for PM. A fault diagnosis system for district heating and cooling facilities will be employed as an example to demonstrate the proposed Petri net method.

THRESHOLD AND WARNING VALUE

A trend chart [7] is a chart that records the performance of a piece of equipment or a system by time. Methods for generating curves in a trend chart vary with different types of equipment, as depicted in Figure 3. Figure 4 shows a trend chart for a rotating machine. Trend charts are usually established by manufacturers when they run their tests in their laboratories to evaluate quality, reliability, maintainability and maintenance procedures. A threshold is a value used to judge whether an equipment failure occurs or not. It is prescribed as the measurement value that is taken just prior to or at the time of failure, i.e. the maximum allowed value in Figure 4. Life testing is one method to obtain such data, and may be performed by field engineers or users.

*Correspondence to: T. S. Liu, Department of Mechanical Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan, ROC. Email: tsliu@cc.nctu.edu.tw

CCC 0748–8017/98/050319–12$17.50

Received 30 September 1997
Revised 15 January 1998

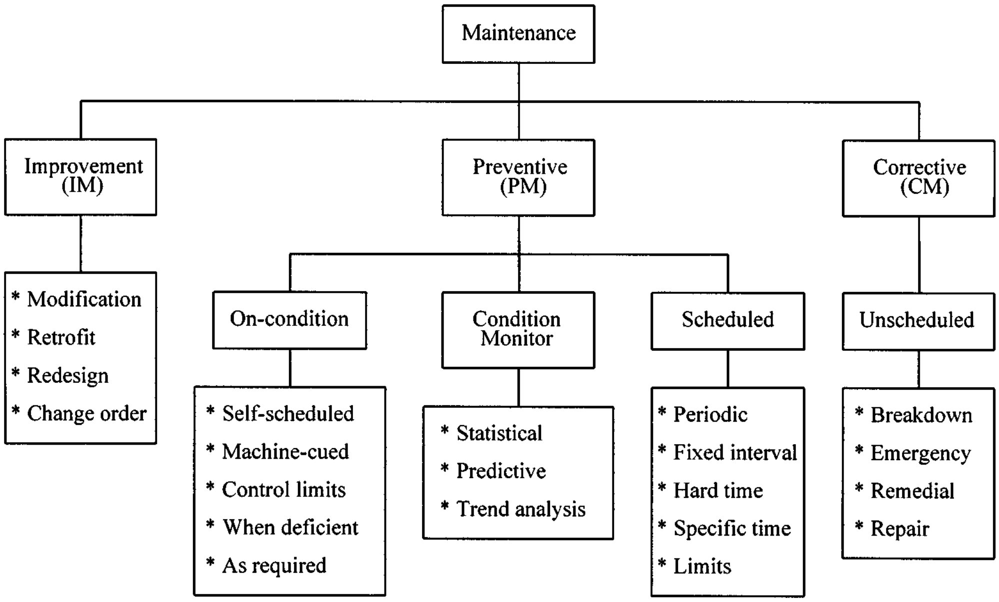


Figure 1. Classification of maintenance

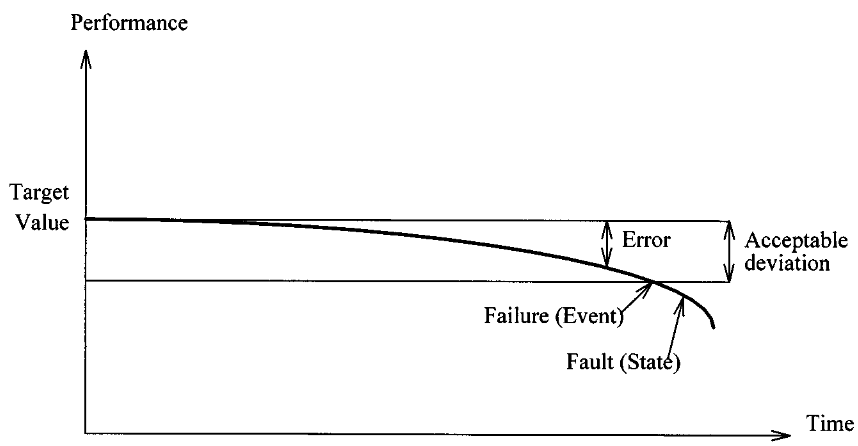


Figure 2. Error, failure and fault

Equipment	Methods
Rotating machine	* Vibration analysis * Oil analysis
Power system	* Infrared thermography
Induction motor	* Motor current signature analysis * Circuit analysis
Pipeline	* Ultrasonic thickness measurement

Figure 3. Methods for generating curves in trend charts

Once the threshold has been determined, a margin of safety should be added to account for variations in early failure detection. The warning value in Figure 4 is the edge of this margin. The safety margin can be determined by the requirement of lead time for PM or according to the physical properties and actual operating conditions of different systems. The lower the warning value is set, the greater is the assurance that PM will be done prior to failure [1], though more labour manpower and cost will have to be expended. Three standard deviations is one possible choice in prescribing a warning value [8]. On the basis of failure thresholds and warning values, a control chart [1] can be constructed to conduct limit control, as illustrated in Figure 5.

Failure detection can be carried out by comparing actual with nominal quantities, and fault isolation by comparing actual with fault quantities [9]. Consequently, an instrumentation system should be set up for the objective of PM to acquire actual quantities at measurement points. In addition to being used for comparison, acquired quantities can be stored to establish a database for modifying predetermined failure thresholds and warning values. The performance of some systems depends on external conditions. For example, the output current of a power generator varies with the load, which changes with time during a day. Hence thresholds and warning values may be varied according to a scheduled scheme that accomplishes adaptive adjustment for those values. The situation is called 'error' in this paper whenever the

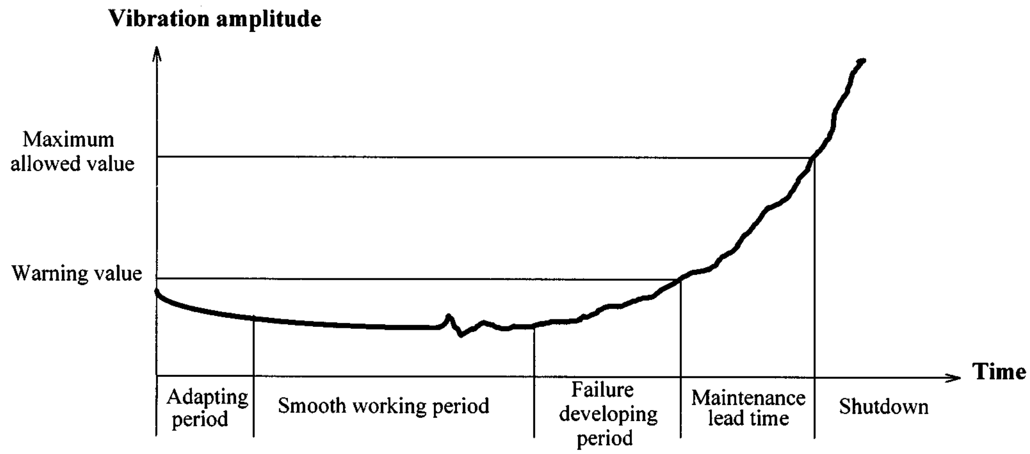


Figure 4. A trend chart for a rotating machine

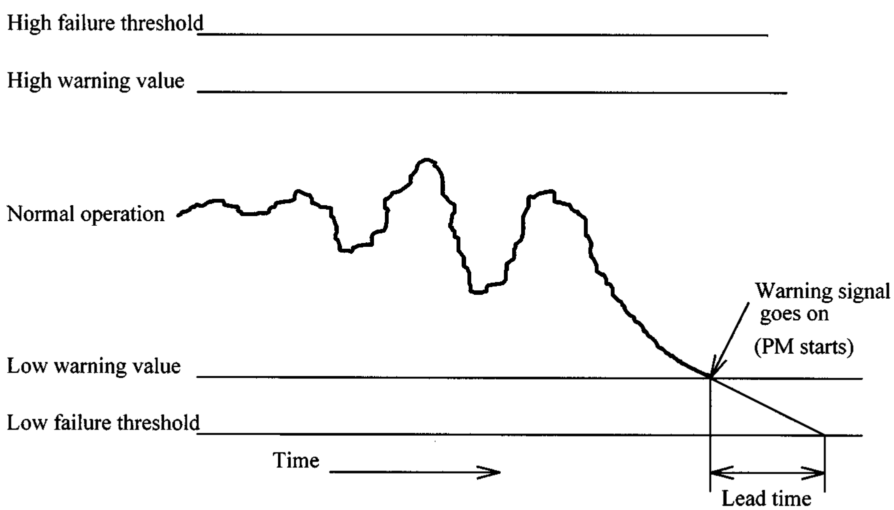


Figure 5. A control chart

acquired quantity exceeds the prescribed warning value but falls within the high and low thresholds.

A fault diagnosis system for district heating and cooling facilities has been proposed [10]. This system is employed as an example for early failure detection and isolation using the method proposed in this study. The system diagram is shown in Figure 6. The facilities are composed of two heat pumps for producing heat, four storage tanks for storing hot and chilled water, two sets of supply pumps for supplying buildings with hot and chilled water respectively, and distribution pipes. The functions of the proposed fault diagnosis system for the facilities can be divided into two parts: reduced-capability diagnosis to prevent a failure and reduced-function diagnosis after a failure. They use the threshold of symptom detection to predict the fault time and a cause–effect tree diagram to find causes of faults. A trigger signal is generated which is a fault alarm or an upper or lower limit alarm once the measured data exceed a reference value. Reference values are presented in [10]. The value for condenser pressure, for example, is 0.1–0.7 kg cm^{-2}, varying from September to December. The level of malfunction for this parameter is set at 15% up for the warning value and 20% up for the threshold. This system has been validated using real facilities.

Figure 7 depicts the fault tree of this system. Events 1–9 are measurable, whereas events 10–13 are phenomena which do not need to be measured. Since events 2-1 and 2-2 are the same event, they can be measured by the same sensor. In order to construct the Petri net dealing with system failure, nine sensors are selected to be installed at the associated test points depicted in the fault tree to acquire data. Sensor types, locations and associated sensing signals are depicted in Figure 6.

PETRI NETS

A Petri net is a general-purpose mathematical tool for describing relations existing between conditions and events [11]. The basic symbols of Petri nets include [12]:

- ○ *place*, drawn as a circle, denoting event
- — *immediate transition*, drawn as a thin bar, denoting event transfer with no delay time
- — *timed transition*, drawn as a thick bar, denoting event transfer with a period of delay time
- ↑ *arc*, drawn as an arrow, between places and transitions
- ● *token*, drawn as a dot, contained in places, denoting the data

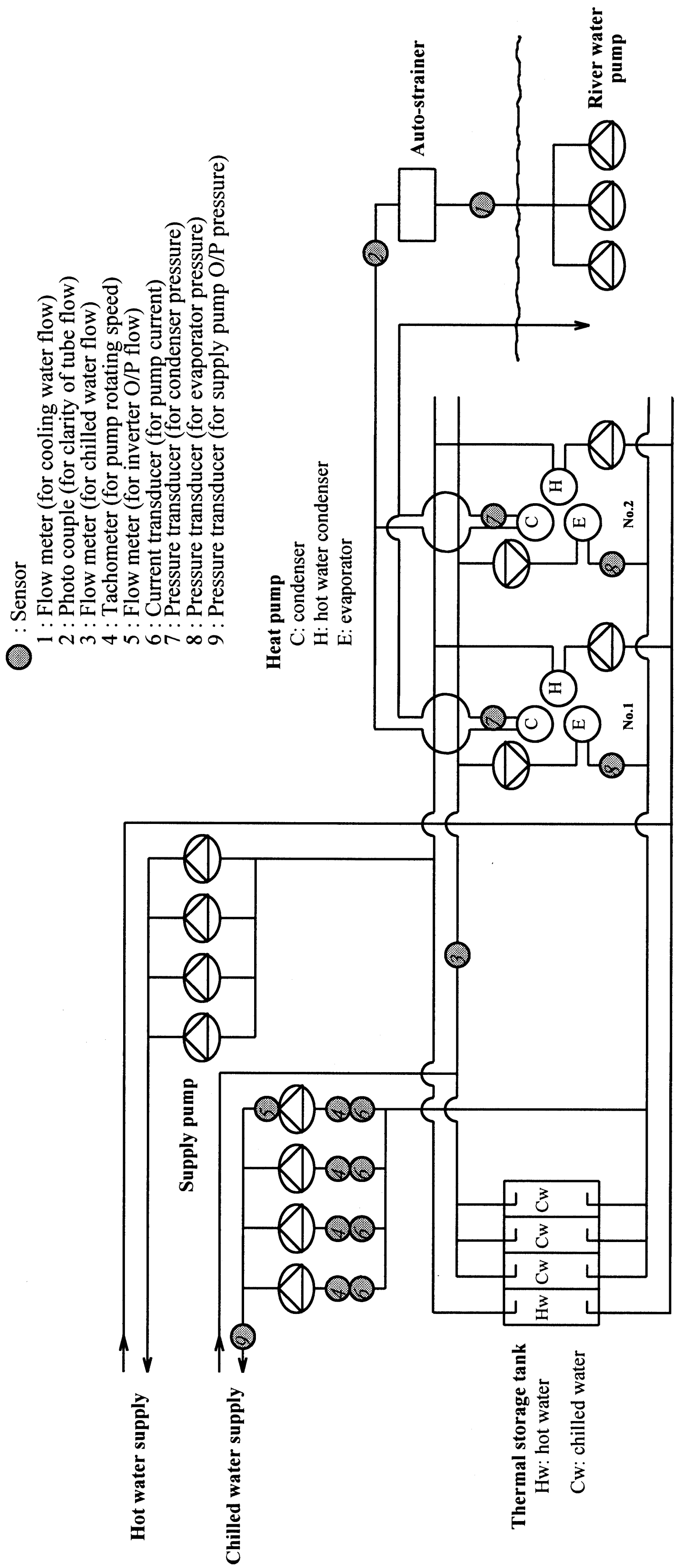


Figure 6. System diagram of heating and cooling facilities

⚲ *inhibitor arc*, drawn as a line with a circle end, between places and transitions.

A transition is said to fire if input places satisfy an enabled condition. Transition firing will remove one token from each input place and put one token into each output place [13]. The basic structures of the logic relations for Petri nets are listed in Figure 8, where there are two types of input places for transition, namely specified and conditional. The former has a single output arc, whereas the latter has multiples. Tokens in a specified-type place have only one outgoing destination; that is, if the input place(s) holds a token, then the transition fires and gives the output place(s) a token. However, tokens in a conditional-type place have more than one outgoing path, which may lead the system to different situations. For the 'TRANSFER OR' Petri net in Figure 8, whether Q or R takes over a token from P depends on conditions such as probability, extra action and self-condition of the place.

There are three types of transitions that are classified based on time [11]. Transitions with no time delay due to transition are called immediate transitions, while those that need a certain constant period of time for transition are called timed transitions. The third type is called a stochastic transition and is used for modelling a process with random time. Owing to the variety of Petri nets [11], it is a powerful tool for modelling flexible manufacturing systems [14,15], multilevel hierarchical systems [16,17], multiprocessor systems [18,19], etc. Besides, Petri nets are capable not only of simulation [20,21], reliability analysis [22] and failure monitoring [23] but also of dynamic behaviour observation [24] and activity prediction [25].

The proposed fault tree of the facilities shown in Figure 7 can be transformed into the Petri net model shown in Figure 9. Since events 2-1 and 2-2 in the fault tree depicted in Figure 7 are the same, they have been combined into P_2 in the Petri net depicted in Figure 9. As a result, each place in Figure 9 represents the associated fault event in Figure 7.

EARLY FAILURE DETECTION AND ISOLATION ARRANGEMENT

An *early failure detection and isolation arrangement* (EFDIA) is proposed in this paper. It is a hybrid Petri net [11] that includes three kinds of Petri nets: ordinary, inhibitor arc and timed. In Figure 9, each place with a monitor sensor, i.e. each of the nine measurement points in Figure 6, will be equipped with an EFDIA that facilitates alarm, early failure detection, fault isolation, event count, system state description and automatic shutdown or regulation. EFDIA is shown in Figure 10, where the symbols are defined as follows:

1. n: total number of sensing points
2. i: sequence number, $1 \le i \le n$
3. $M(P)_k$: marking of place P at state k, representing the token quantity of place P at state k, $k = 1, 2, 3, \ldots$
4. P_i: ith place of Petri net; $M(P_i) = 1$ if P_i failure occurs.
5. T_i: ith transition of Petri net, representing the time duration due to transition
6. S_i: sensing signal for ith place; S_i generates a token such that $M(S_i) = 1$ if the signal exceeds the prescribed warning value, i.e. an abnormal situation (error) occurs
7. $T_{i\mathrm{E}}$: error transition of P_i; immediate transition
8. $T_{i\mathrm{L}}$: error times log transition of P_i; immediate transition
9. $T_{i\mathrm{M}}$: maintained transition, representing the transitional time from when the PM action for P_i is taken to when P_i is maintained, timed transition
10. $T_{i\mathrm{P}}$: processing transition of P_i; immediate transition
11. $T_{i\mathrm{R}}$: reset transition of P_i; immediate transition
12. $T_{i\mathrm{S}}$: sensing transition of P_i; immediate transition
13. $T_{i\mathrm{T}}$: transfer transition of P_i; immediate transition
14. $T_{i\mathrm{U}}$: unprocessed transition of P_i, representing the transitional time from when the ith WARNING SIGNAL appears to when P_i failure occurs; timed transition
15. $T_{i\mathrm{W}}$: warning times log transition of next lower level P^{W}; immediate transition
16. P_i^{A}: PM action taken place for P_i; P_i^{A} generates a token such that $M(P_i^{\mathrm{A}}) = 1$ if the PM action for P_i is taken
17. $P_i^{\mathrm{B}j}$: jth buffer place of P_i, for tokens to stay temporarily, $j = 1, \ldots, x$; x is the number of input arcs for P_i
18. P_i^{E}: error indication place of P_i; $M(P_i^{\mathrm{E}}) = 1$ after $T_{i\mathrm{E}}$ fires if the $M(S_i) = 1$ situation is generated by P_i itself but not aroused by lower-level places (for fault isolation)
19. P_i^{F}: failure counter place of P_i; $M(P_i^{\mathrm{F}})$ represents the failure times log number of P_i; $M(P_i^{\mathrm{F}})$ increases by one when P_i failure occurs
20. P_i^{L}: error counter place of P_i; $M(P_i^{\mathrm{L}})$ represents the error times log number of P_i; $M(P_i^{\mathrm{L}})$ increases by one when P_i error occurs
21. P_i^{M}: maintenance counter place of P_i; $M(P_i^{\mathrm{M}})$ represents the maintenance times log number of P_i; $M(P_i^{\mathrm{M}})$ increases by one when the $M(S_i) = 1$ situation is maintained
22. P_i^{P}: processing place of P_i, representing P_i in the being maintained situation
23. P_i^{R}: reset counter place of P_i; $M(P_i^{\mathrm{R}})$ represents the warning times log number of P_i that are aroused by lower-level places, i.e. the reset times of the ith RESET R; $M(P_i^{\mathrm{R}})$ increases by one when the ith RESET R is triggered
24. P_i^{T}: transitional place of P_i, representing a transitional state inserted between S_i and P_i, of duration $T_{i\mathrm{S}}$ plus $T_{i\mathrm{T}}$, which is the original path from S_i to P_i without EFDIA constructed
25. P_i^{U}: unprocessed place of P_i, representing the error of P_i not corrected
26. P_i^{W}: warning counter place of P_i; $M(P_i^{\mathrm{W}})$ represents the warning times log number of P_i no matter from where warning cause arises; $M(P_i^{\mathrm{W}})$ increases by one when the ith RESET W is triggered
27. ith RESET E: reset E place of P_i, representing a reset signal for P_i^{E}; generates a token when it is triggered

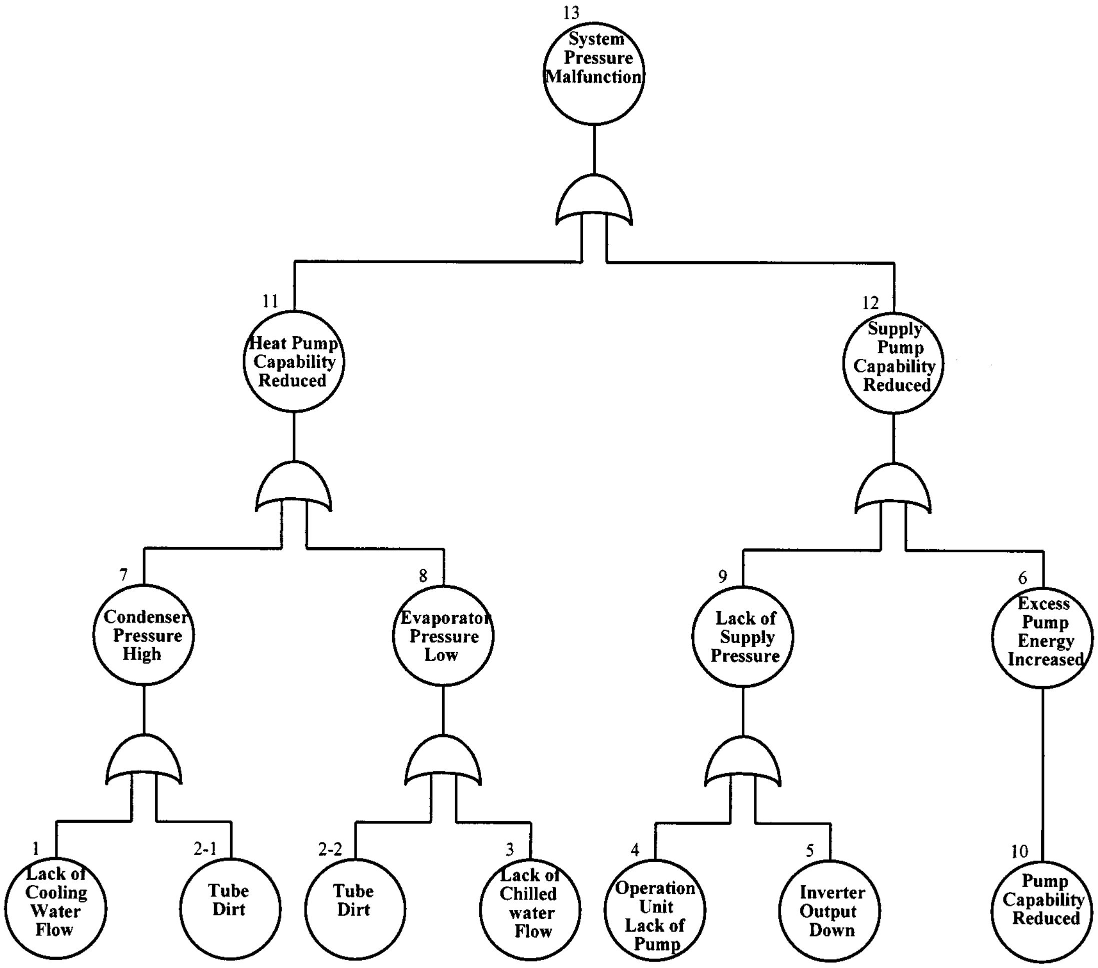


Figure 7. Fault tree of heating and cooling facilities

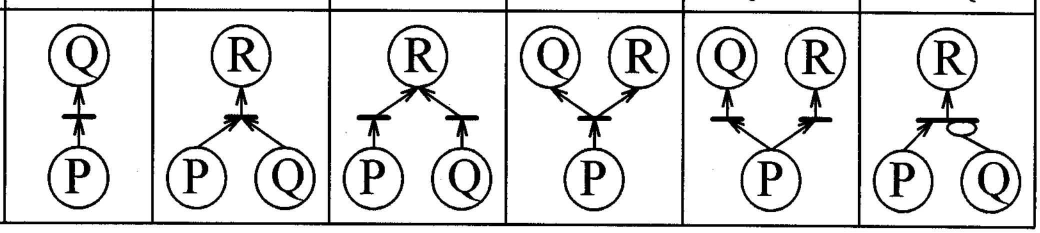
Logic relation	TRANSFER	AND	OR	TRANSFER AND	TRANSFER OR	INHIBITION
Description	If P then Q	If P AND Q then R	If P OR Q then R	If P then Q AND R	If P then Q OR R	If P AND Q' then R
Boolean function	Q=P	R=P*Q	R=P+Q	Q=R=P	Q+R=P	R=P*Q'
Petri nets						

Figure 8. Basic structures of logic relations for Petri nets

28. ith RESET R: reset R place of P_i, representing a reset signal for P_i^{R}; generates a token when it is triggered
29. ith RESET W: reset W place of P_i, representing a reset signal for P_i^{B}; generates a token when it is triggered; the number of the ith RESET W should equal number of inhibitor arcs of transition $T_{i\mathrm{E}}$
30. ASFM: automatic shutdown or feedback mechanism; for instance, an air-conditioning or ventilation system is a feedback mechanism for an over temperature module
31. ith WARNING SIGNAL: warning signal place for P_i
32. CLOCK: a clock is embedded to record the time of event occurrence

The operational steps for EFDIA are described as follows.

1. Transition $T_{i\mathrm{S}}$ fires if S_i exceeds the prescribed warning value. Subsequently, each of P_i^{B1}, ith WARNING SIGNAL, P_i^{T} and next higher P^{B2} obtains a token. As defined in the previous paragraph, $M(P)$ is the marking of place P. Thus $M(P_i^{\mathrm{T}}) = 1$ represents this S_i monitored subsystem (module) at a transitional state. Similarly, $M(i$th WARNING SIGNAL$) = 1$ represents that the ith

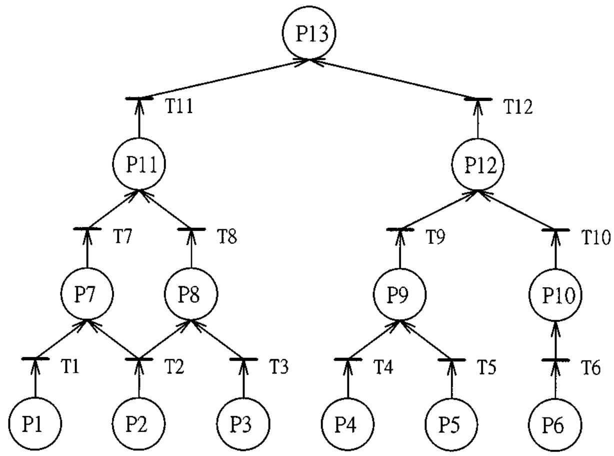


Figure 9. Petri net of Figure 7

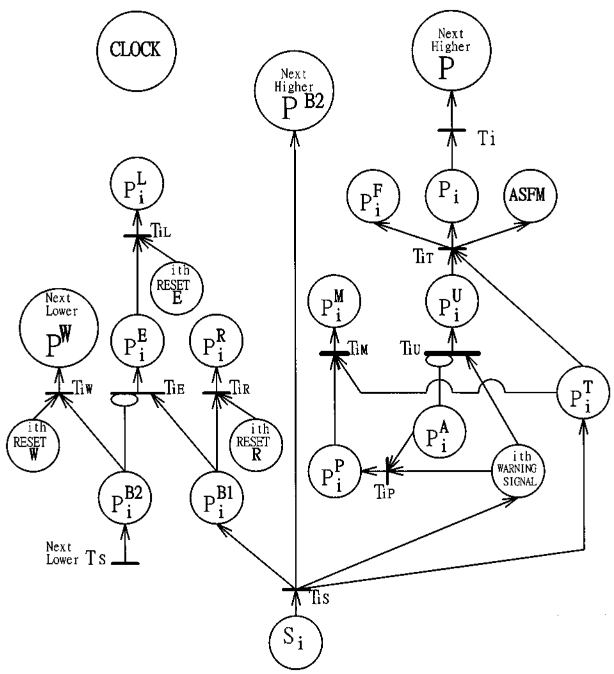


Figure 10. Early failure detection and isolation arrangement (EFDIA)

WARNING SIGNAL goes on, which may be a light, a beep or some other form, to indicate that S_i exceeds the prescribed warning value.

2. There are two paths to follow.
   (a) $T_{i\mathrm{P}}$ fires if P_i^{A} generates a token, i.e. PM action is taken. The tokens in P_i^{A} and the ith WARNING SIGNAL move to P_i^{P}, i.e. the subsystem (module) is being maintained. Otherwise, $T_{i\mathrm{U}}$ fires if P_i^{A} does not generate a token during the transition time of $T_{i\mathrm{U}}$, such that P_i^{U} acquires a token.
   (b) $T_{i\mathrm{E}}$ fires if P_i^{B2} has no token, i.e. this error is not caused by the next lower subsystem (module) but by the ith-level subsystem (module) itself, such that P_i^{E} obtains a token. On the other hand, if P_i^{B2} holds a token, i.e. this error results from the next lower subsystem (module), then $T_{i\mathrm{E}}$ does not fire, such that the token from S_i will be held in P_i^{B1}. The error is hence isolated.

3. There are again two paths to follow.
   (a) $T_{i\mathrm{M}}$ fires if the PM action is finished, such that the tokens in P_i^{P} and in P_i^{T} move to P_i^{M}, i.e. this error has been corrected. Otherwise, $T_{i\mathrm{T}}$ fires if P_i^{U} obtains a token resulting from the firing of $T_{i\mathrm{U}}$, i.e. PM action was not taken in time, such that tokens in P_i^{U} and P_i^{T} move to P_i, i.e. P_i failure occurs. As a consequence, both P_i^{F} and ASFM also obtain a token. Accordingly, the failure times log number increases by one and the ASFM is triggered. This mechanism can be optional for different systems.
   (b) $T_{i\mathrm{L}}$ fires if P_i^{E} holds a token and the ith RESET E is triggered, such that P_i^{L} obtains a token, i.e. the error times log number of P_i increases by one. Otherwise, the token in buffer place P_i^{B1} will move to P_i^{R} when $T_{i\mathrm{R}}$ fires by triggering the ith RESET R, i.e. this error is not caused by P_i and the reset times log number of P_i increases

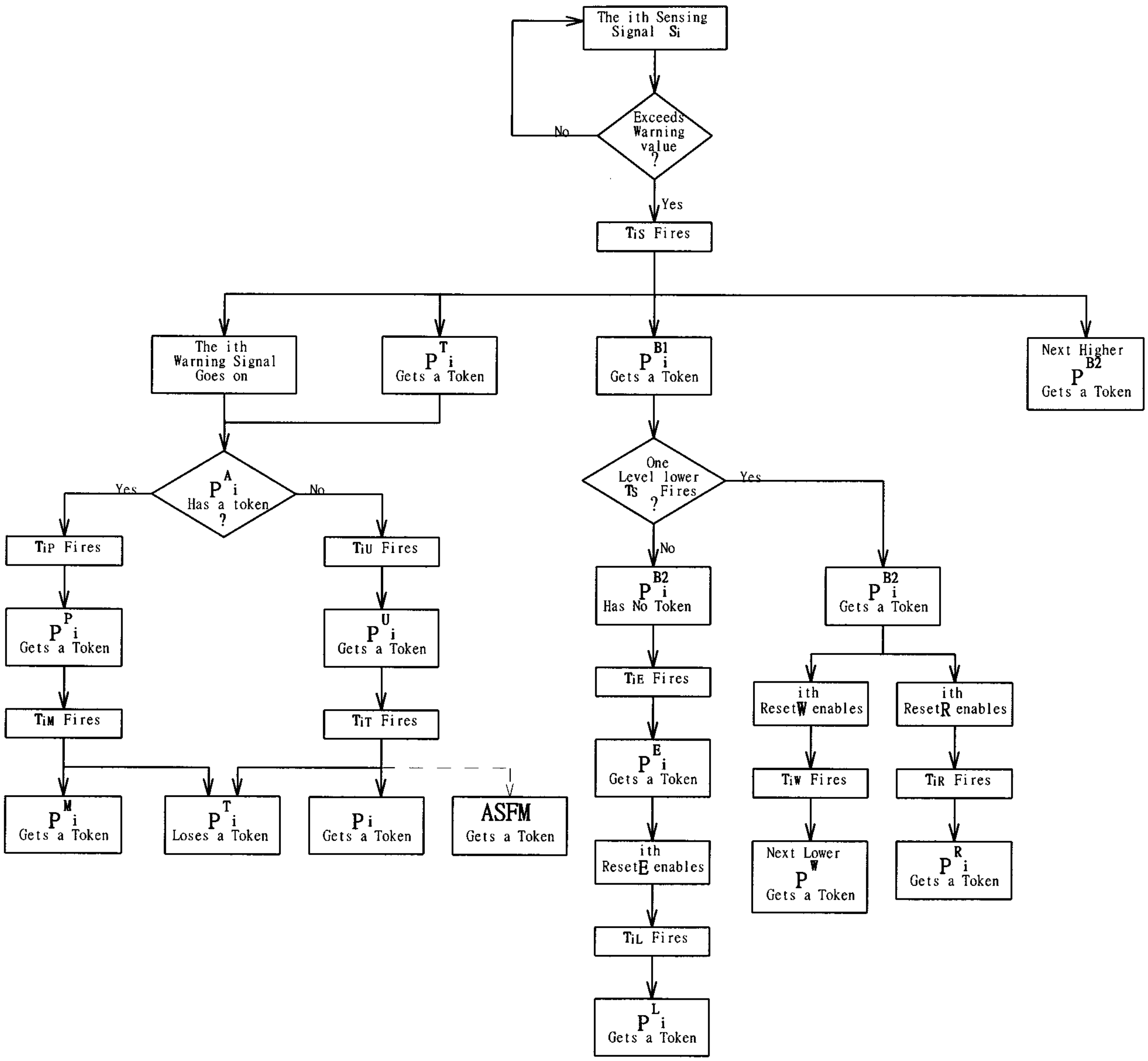


Figure 11. Flow chart of EFDIA

by one. Similarly, the ith RESET W triggers to fire T_{iW} such that the token in the other buffer place, P_i^{B2}, moves to the next lower P^W, i.e. the warning times log number of the next lower P^W increases by one.

Conventionally, a flow chart is an easier representation for understanding the operational steps. Therefore the above descriptions are summarized into a flowchart for clarity, as shown in Figure 11.

EFDIA is composed of several small arrangements, each of which has a specific function.

1. *Reset*. The ith RESET E and P_i^E together with T_{iL} form a logic AND relation. The ith RESET E generates a token whenever this reset button has been triggered, so as to fire T_{iL} and remove a token from P_i^E to P_i^L whenever P_i^E holds a token and needs to be reset. In a similar manner, the ith RESET R and ith RESET W are designed to reset P_i^{B1} and P_i^{B2} respectively.
2. *Inhibition*. Both T_{iE} and T_{iU} are transitions with an inhibitor arc. This arrangement is designed to inhibit the firing of T_{iE} and T_{iU} whenever the place where the inhibitor arc is connected, i.e. P_i^{B2} and P_i^A respectively, holds a token.
3. *Conditional place*. Any place that has more than one outgoing arc is called a conditional place. Tokens contained in a conditional place will move to an output place through the transition which is firstly enabled among all the output transitions of the transitional places. A conditional place models a conditional state of a system or process. In EFDIA, P_i^A, P_i^{B1}, P_i^{B2}, P_i^T and the ith WARNING SIGNAL are conditional places.
4. *Counter*. P_i^F, P_i^L, P_i^M, P_i^R and P_i^W perform as counters to accumulate occurrence times of associated events.
5. *Event flag*. Several places are designed as event flags. Each of them represents an associated event once the marking of the place becomes unity.
   (a) P_i denotes the failure of the ith place.

(b) P_i^{E} denotes the error located at the ith place.
(c) P_i^{T} denotes the ith place at a transitional state.
(d) The ith WARNING SIGNAL denotes the ith monitored signal exceeding the warning value.
(e) ASFM means the automatic shutdown function or feedback mechanism is triggered.

PROPERTIES OF EFDIA

This section presents the capabilities of EFDIA and the invariants derived from EFDIA.

Capabilities

1. *Alarm.* EFDIA provides alarm capability whenever an over-warning-value situation occurs, by triggering the ith WARNING SIGNAL for the associated place.
2. *Early failure detection.* EFDIA is capable of early failure detection, since the alarm function operates whenever the acquired signal exceeds a prescribed warning value but not the failure threshold. This means that the abnormal situation is detected before failure occurs. As shown in Figure 5, the lead time of early detection can be obtained by extrapolating the curve in a control chart with a line slope that is constructed by the last two sampled points on the curve [10]. The lead time is the period between the time point where the warning value is exceeded and the intersection of the extended line and time axis.
3. *Fault isolation*. The cause(s) of malfunction of a system can be located anywhere within the system. However, since malfunction causes are constrained by the logic relations of the fault tree, they can be isolated by the inhibit transition $T_{i\mathrm{E}}$ via the indication of the event flag P_i^{E}. The error is located at the ith place if $M(P_i^{\mathrm{E}}) = 1$. Otherwise, the error of the ith place arises from the lower-level place(s) even if the ith WARNING SIGNAL appears.
4. *Event count.* All the counters designated in EFDIA record the associated occurrence times of events. By incorporating a time clock, the associated rates can be obtained at the same time. The following items can be derived from EFDIA:
   (a) failure rate of the ith place: $M(P_i^{\mathrm{F}})/t$
   (b) error rate of the ith place: $M(P_i^{\mathrm{L}})/t$
   (c) maintenance rate of the ith place: $M(P_i^{\mathrm{M}})/t$
   (d) alarm rate of the ith place: $M(P_i^{\mathrm{W}})/t$.
   From these rates, two advantages can be obtained.
   (a) If the ith subsystem is maintained whenever an error is detected, the failure rate of the ith place can be minimized such that the system reliability is promoted.
   (b) All the rates can be recorded as historical data so as to perform statistical prediction for system failure (by failure rate and error rate), and the time needed for maintenance (by maintenance rate) of each subsystem can be derived.
5. *System state description*. The system state is clearly visible by the indication of every place in EFDIA. The following parameters are defined to account for the system state:
   (a) $\mathbf{M}_k$: marking of the Petri net at state k, $\mathbf{M}_k = [M(P_1), M(P_2), \ldots, M(P_n)]^{\mathrm{T}}$
   (b) $\mathbf{S}_k$: sensing signal matrix at state k, $\mathbf{S}_k = [M(S_1), M(S_2), \ldots, M(S_n)]^{\mathrm{T}}$
   (c) $\mathbf{L}_k$: maintenance log matrix at state k, $\mathbf{L}_k = [M(P_1^{\mathrm{M}}), M(P_2^{\mathrm{M}}), \ldots, M(P_n^{\mathrm{M}})]^{\mathrm{T}}$
   (d) $\mathbf{F}_k$: failure times log matrix at state k, $\mathbf{F}_k = [M(P_1^{\mathrm{F}}), M(P_2^{\mathrm{F}}), \ldots, M(P_n^{\mathrm{F}})]^{\mathrm{T}}$
   (e) $\mathbf{E}_k$: error indication matrix at state k, $\mathbf{E}_k = [M(P_1^{\mathrm{E}}), M(P_2^{\mathrm{E}}), \ldots, M(P_n^{\mathrm{E}})]^{\mathrm{T}}$; the ith entry indicates that the error is located at the ith place if the ith entry value is unity.
6. *Auto shutdown or regulation*. Automatic shutdown or regulation capability can be provided by EFDIA through triggering the ASFM place.
7. *Time recording*. The time at which each event occurs can be recorded by the embedded CLOCK. This is required for failure analysis.

Invariants

According to the properties of EFDIA, the following invariants can be derived:

1. $M(P_i^{\mathrm{L}})k + M(P_i^{\mathrm{R}})k = M(P_i^{\mathrm{W}})k$. The number of warning signals for the ith place at state k is equal to the summation of the error times log number and the reset times log number at state k for the ith place.
2. $M(P_i^{\mathrm{F}})k + M(P_i^{\mathrm{M}})k = M(P_i^{\mathrm{W}})k$. For the ith place at state k, failure times plus maintenance times equal the warning times log number.
3. At basic places, $M(P^{\mathrm{R}})k = 0$ and $M(P^{\mathrm{L}})k = M(P^{\mathrm{W}})k$. Since there is no place lower than basic places, the error times log number and the warning times log number are equal at basic places.
4. $M(P_i^{\mathrm{P}})k + M(P_i^{\mathrm{U}})k = 1$. Since the conditions that an error place is maintained and not maintained are mutually exclusive, at state k either the marking for P_i^{P} or that for P_i^{U} is unity.

EXAMPLE

The Petri net for the heating and cooling facilities endowed with EFDIA is shown in Figure 12. It is a result of appending an EFDIA to each place with a monitor sensor in Figure 9, i.e. P_1 to P_9. The logic relations among all places in Figure 9 are still retained in Figure 12. At basic places, i.e. P_1 to P_6, the function for testing whether the error cause is from the next lower place or not becomes unnecessary. The following two situations are used to demonstrate the function of EFDIA in the employed system.

1. Suppose the monitored signal for cooling water flow, i.e. S_1 in Figure 12, exceeds the prescribed warning value. Subsequently, $T_{1\mathrm{S}}$ fires such that the 1st WARNING SIGNAL goes on and each of P_1^{T}, P_7^{B3} and P_1^{E} obtains a token. $M(P_1^{\mathrm{T}}) = 1$ represents the cooling water flow rate that is in an error situation and it is a transitional state between normal and faulty. There is a lead time from then until P_1 failure

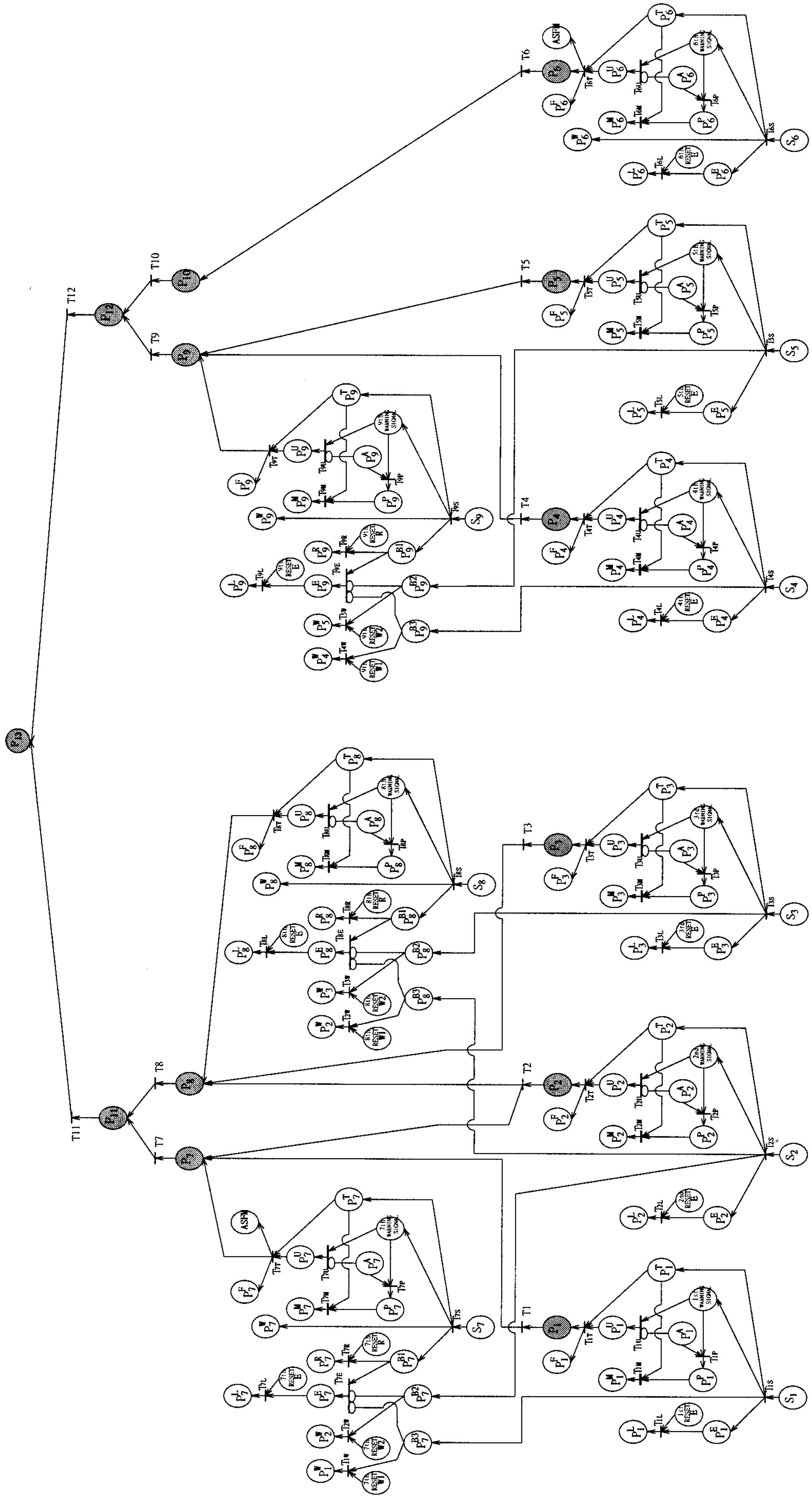


Figure 12. Petri net for DHC facilities endowed with EFDIA

really happens. If the PM action takes place during the lead time, then P_1^A generates a token such that T_{1P} fires so as to make the tokens in P_1^A and the 1st WARNING SIGNAL move to P_1^P. The subsystem is being maintained and the 1st WARNING SIGNAL goes off at this moment. T_{1M} fires if the PM action is finished. Subsequently, the tokens in P_1^P and P_1^T move to P_1^M, i.e. this error has been corrected. The marking of P_1^M, i.e. the maintenance times log number for P_1, increases by one. On the other hand, if the PM action does not take place in time, then T_{1U} fires such that P_1^U obtains a token. Consequently, the tokens in P_1^U and P_1^T move to P_1. Hence P_1 failure occurs. At the same time, P_1^F obtains a token, i.e. the failure times log number increases by one. Because of the logic relation between P_1 and P_7, the monitored signal for P_7, i.e. S_7, exceeds the prescribed warning value due to P_1 failure. Accordingly, the 7th WARNING SIGNAL goes on and each of P_7^T, P_7^{B1} and P_7^W, obtains a token. T_{7E} is inhibited by the token in P_7^{B3}, such that the tokens in P_7^{B1} and P_7^{B3} move to P_7^R and P_1^W after triggering the 7th RESET R and 7th RESET W1 respectively. Hence this error is located at P_1, whereas $M(P_7^L)$ does not increase.

2. Suppose the monitored signal for condenser pressure, i.e. S_7, exceeds the prescribed warning value spontaneously while both S_1 and S_2 are at normal condition. As a result, T_{7S} fires such that the 7th WARNING SIGNAL goes on. Simultaneously, each of P_7^T, P_7^{B1} and P_7^W obtains a token. In a similar manner, as S_1 exceeds the prescribed warning value, $M(P_7^M)$ increases by one if the PM action for P_7 takes place in time. Otherwise, P_7 failure occurs such that $M(P_7^F)$ increases by one. However, since P_7^{B2} and P_7^{B3} are both empty, T_{7E} fires such that P_7^E obtains a token. As a result, $M(P_7^L)$, i.e. the error times log number for P_7, increases by one.

ASFM is to prevent higher-level fault or system breakdown from happening by automatic shutdown or regulation. It should be incorporated with the places that may cause safety problems in a Petri net. In this example it can be triggered by either P_6 or P_7 failure, i.e. excess pump energy increased or condenser pressure high.

CONCLUSIONS

This paper has presented an early failure detection and isolation scheme for PM via the heating and cooling facilities example, by using a hybrid Petri net modelling method coupled with parameter trend and fault tree analysis. The Petri net dealing with system failure has to be constructed beforehand. The next task is to obtain trend charts for all fault places in the Petri net in order to prescribe thresholds and allowable margins. With these prerequisites the present method can be applied to any system. The proposed Petri net approach can not only achieve early failure detection and isolation for fault diagnosis but also facilitates event count, system state description and automatic shutdown or regulation. These capabilities can be very useful for health monitoring and preventive maintenance of a system.

REFERENCES

1. J. D. Patton Jr, *Preventive Maintenance*, Instrument Society of America, New York, 1983.
2. IEC 50(191), *International Electrotechnical Vocabulary (IEV)*, Chap. 191, *Dependability and Quality of Service*, International Electrotechnical Commission, Geneva, 1990.
3. M. Rausand and K. Oien, 'The basic concept of failure analysis', *Reliab. Eng. Syst. Safety*, **53**, 73–83 (1996).
4. W. J. Wang and P. D. McFadden, 'Early detection of gear failure by vibration analysis—I. Calculation of the time–frequency distribution', *Mech. Syst. Signal Process.*, **7**(3), 193–203 (1993).
5. W. J. Wang and P. D. McFadden, 'Early detection of gear failure by vibration analysis—II. Interpretation of the time–frequency distribution using image processing techniques', *Mech. Syst. Signal Process.*, **7**(3), 205–215 (1993).
6. R. Isermann, 'Process fault detection based on modeling and estimation methods—a survey', Automatica, **20**(4), 387–404 (1984).
7. G. G. Barna, 'Automatic problem detection and documentation for a plasma etch reactor', *IEEE Trans. Semicond. Manuf.*, **SM-5**(1), 56–59 (1992).
8. S. S. Rao, *Reliability-Based Design*, McGraw-Hill, New York, 1992.
9. A. Baccigalupi, A. Bernieri and A. Pietrosanto, 'A digital-signal-processor-based measurement system for on-line fault detection', *IEEE Trans. Instrum. Meas.*, **IM-46**(3), 731–736 (1997).
10. T. Kumamaru, T. Utsunomiya and Y. Yamada, 'A fault diagnosis system for district heating and cooling facilities', *Proc. IECON '91, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1991, pp. 131–136.
11. R. David and H. Alla, 'Petri nets for modeling of dynamic systems—a survey', *Automatica*, **30**(2), 175–202 (1994).
12. G. S. Hura and J. W. Atwood, 'The use of Petri nets to analyze coherent fault trees', *IEEE Trans. Reliab.*, **REL-37**(5), 469–474 (1988).
13. W. G. Schneeweiss, 'Mean time to first failure of repairable systems with one cold spare', *IEEE Trans. Reliab.*, **REL-44**(4), 567–574 (1995).
14. M. C. Zhou, H. S. Chiu and H. H. Xiong, 'Petri net scheduling of FMS using branch and bound method', *Proc. IEEE IECON, 21st Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1995, pp. 211–216.
15. R. Hilal and P. Ladet, 'Modelling, control, and simulation of flexible manufacturing systems through the use of synchronous Petri nets', *Proc. IECON '93, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1993, pp. 559–563.
16. H. Murakoshi, T. Kondo and Y. Dohi, 'Hardware architecture for hierarchical control of large Petri net', *Proc. IECON '93, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1993, pp. 115–120.
17. P. Esteban and M. Courvoisier, 'Multilevel hierarchical control applied to a demonstration flexible assembly cell', *Proc. IECON '91, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1991, pp. 878–883.
18. F. Anzai, N. Kawahara and T. Takei, 'Hardware implementation of a multiprocessor system controlled by Petri nets', *Proc. IECON '93, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1993, pp. 121–126.
19. H. Murakoshi, M. Sugiyama, G. Ding and T. Oumi, 'A high speed programmable controller based on Petri net', *Proc. IECON '91, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1993, pp. 1966–1971.
20. J.-F. Ereau and M. Saleman, 'Modeling and simulation of a satellite constellation based on Petri nets', *Proc. IEEE Ann. Reliability and Maintainability Symp.*, 1996, pp. 66–72.
21. H. Takami and M. Araki, 'Simulation-based scheduling package using generalized Petri net models', *Proc. IECON '93, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1993, pp. 451–456.
22. K. Barkaoui, G. Florin, C. Fraize and B. Lemaire, 'Reliability analysis of nonrepairable systems using stochastic Petri nets', *Eighteenth Int. Symp. on Fault-Tolerant Computing. Digest of Papers. FTCS-18*, 1988, pp. 90–95.
23. A. Chaillet, M. Combacau and M. Courvoisier, 'Specification of FMS real-time control based on Petri nets with objects and process failure monitoring', *Proc. IECON '93, Int. Conf. on Industrial Electronics, Control, and Instrumentation*, 1993, pp. 144–149.
24. S. K. Yang and T. S. Liu, 'Failure analysis for an airbag inflator by Petri nets', *Qual. Reliab. Eng. Int.*, **13**, 139–151 (1997).
25. Y. Manabe, M. Hattori, S. Tadokoro and T. Takamori, 'A model of human actions by a Petri net and prediction of human acts', *Trans. Jpn. Soc. Mech. Eng.*, **63**, 287–294 (1997).

Authors' biographies:

S. K. Yang was born in Taiwan. He received his BS and MS in automatic control engineering from Feng Chia University in 1982 and 1985 respectively. From 1985 to 1991 he was an assistant researcher and system engineer in the Flight Test Group, Aeronautic Research Laboratory, Chung Shan Institute of Science and Technology. Since 1991 he has been an instructor in the Department of Mechanical Engineering, Chin Yi Institute of Technology. Since 1994 he has been a PhD student majoring in Mechanical Engineering at National Chiao Tung University. His research interests are in reliability, data acquisition and automatic control.

T. S. Liu received his BS from National Taiwan University in 1979 and MS and PhD from the University of Iowa, USA in 1982 and 1986 respectively, all in mechanical engineering. Since 1987 he has been with National Chiao Tung University, where he is currently a professor. From 1991 to 1992 he was a visiting researcher in the Institute of Precision Engineering, Tokyo Institute of Technology, Japan. His current research interests include reliability, design, and motion control.