DIAGNOSABILITY OF HYBRID SYSTEMS[1]

G. K. Fourlas, K. J. Kyriakopoulos and N. J Krikelis

Control Systems Laboratory, Mechanical Eng. Dept.
National Technical University of Athens (NTUA), Athens, Greece
e-mail: {gfourlas,kkyria,nkrik}@central.ntua.gr

Keywords: Fault detection, fault diagnosis, diagnosability, hybrid systems.

Abstract

Fault diagnosis is a challenging task in the control of Hybrid Systems. In this work we introduce the notion of diagnosability of Hybrid Systems in the framework of Hybrid Input Output Automata (HIOA). We present a methodology for detection of faults imposing the conditions for a Hybrid System to be diagnosable. This approach is applicable to a wide rage of systems since Hybrid Systems involve both continuous and discrete dynamics. The states of the Hybrid System model reflect the normal and the failed status of the system components. The faults in our setting are modeled as either discrete or continuous (detrimental) state changes.

1 Introduction

The increasing requirements to achieve more reliable performance on complex systems such as air traffic management systems [9, 18], automated highway systems [10, 19], manufacturing systems [2], power systems [8] have necessitated the development of fault diagnosis schemes for accurate diagnosis of system failures. Such systems can be viewed as hybrid systems and therefore fault diagnosis is a challenging task in the control of hybrid systems. Hybrid systems are systems including both continuous and discrete dynamics influencing each other, and therefore the global dynamics. The issues of safe operation for such systems are of major importance and require their supervision in order to timely handle the occurrence of faults or failures. In fault detection, we have to answer whether a transition from the normal to a faulted state has occurred.

In this work, as in our previous contributions [4, 5], we are interested in the problem of failure diagnosis for hybrid systems. We introduce the notion of diagnosability of hybrid systems presenting a methodology for detection of faults using a diagnoser [5] and we impose the conditions for a hybrid system to be diagnosable. Although we share some ideas with [14] and [16] our approach is different in the sense that it addresses hybrid systems and not discrete event or continuous systems. In this framework both discrete and continuous dynamics are formally described. This approach is applicable to a wide rage of systems since hybrid systems involve both continuous and discrete dynamics. The states of the hybrid system model reflect the normal and the failed status of the system components. In our setting, faults are treated at two stages: first as a discrete state change and second as a continuous state change. The behavior of the system is modeled by a HIOA (Hybrid Input/Output Automaton) [11] since this is capable of describing both the continuous and the discrete behavior, with modest extensions of the original framework, so as to capture all interesting phenomena.

The system is assumed to consist of several distinct components (i.e. actuators, main structure and sensors) and a controller.

- We first built a HIOA for each component, to capture both normal and failed behavior.
- Next we compose these individual models using the same composition procedure as in [11]. The overall model will be the composition of a number of automata. (So the plant will be a hybrid automaton containing the dynamics of all components).
- The faults can be modeled as:
  - discrete transitions from the normal to faulted state, or
  - deviation of trajectories describing the continuous evolution from a predefined set point.

Although the proposed model is quite general and can be used for detecting different faults we are only interested in faults, which occur in the components of the plant, especially faults occurring to main structure. We assume that the actuators, controller and sensors are fail-safe and when a fault occurs it is only due to main structure.

In section II after some necessary definitions we present the overall model for diagnosis. In section III we introduce the notion of diagnosability of hybrid systems imposing the conditions for a hybrid system to be diagnosable. Finally, we show in a simple application of an electrical power transmission system the applicability of our approach.

2 Model of the system

Fault diagnosis is a procedure using the measurements of inputs and outputs of the system to be diagnosed. So it's very important to define the system model, which can be used for the description of the plant and enable the fault diagnosis process to detect the change in dynamics. The development of successful diagnosis models imposes certain requirements [13].

- The diagnostic scheme must describe both the normal and the faulty behavior of the system.

[1] Research partly supported by the European Commission through the HYBRIDGE (IST-2001-32460) project and the ARCHIMEDES Basic Research Initiative of the Institute of Communication and Computer Systems at NTUA.

- The model should incorporate sufficient behavioral detail of the system components.
- When faults cause transitions of the system from its normal steady state operation, the model should generate the dynamic behavior.

In fault diagnosis, an automated plant can be considered to consist of three major types of subsystems: actuators, main structure and sensors. A fault-monitoring scheme is usually designed especially to detect and correct faults in only one of those three subsystems [15]. The design of this fault diagnosis scheme has a different aspect depending on what kinds of models are used for the system and for the fault mode descriptions. Before presenting our framework, a few definitions will be provided.

We consider a number of pre-determined state-variables characterizing the dynamic behavior of the system.

Definition 1: *A process is said to be in a normal state of operation if its observed state-variables are in the neighborhood of a predefined set point*.

The state of fault or failure is observed by an output value of the pre-determined variables either if the operating point lies outside of the neighborhood of the predefined set point or certain functional criteria are violated.

Definition 2: *Faults (or failures) are malfunctions disturbing the normal operation of a system, causing an unacceptable decay of its performance and are modeled as transitions from a normal state to a failure state that corresponds to either a discrete or a continuous state change*.

The faults may occur at any of the components of the main structure, the actuators, or the sensors of the plant. The effects that can cause true or false alarms are due to [6]:

- Faults of the components (any of, the main structure, actuators, or sensors).
- Modeling errors between the actual system and its mathematical model and
- System or measurement noise.

The faults according to the mode, which may occur, are classified as:

- Abrupt faults that cause significant changes in the behavior of the system and play role in safety-relevant systems.
- Incipient faults that are small and are relevant in maintenance problems.

In the present paper we consider a Hybrid System (HS) including both continuous and discrete dynamics of each components of the system, since the components contain switching behavior. If limited to linear hybrid systems, the continuous dynamics are described by ordinary differential equations (ODE's). To model the discrete behavior we follow the standard practice and use automata [7] due to the fact that they provide useful tools to handle logical operations.

2.1 Model Construction

The whole system is model by HIOA [11], which capture both continuous and discrete behavior. The system to be diagnosed consists of the plant (decomposed as: actuators, main structure, sensors) and a controller. The subsystem of actuators is a set $A_i, i = 1,..., n_A$ and the subsystem of sensors is a set $S_j, j = 1,...n_S$.

Each of the aforementioned part that can be affected directly by any fault can be consider as a component. Thus a number of faults may occur for each of these components. According to [14] each of these faults can be classified into different fault modes. Apparently for each component only one fault mode may occur at a time.

For each element of the plant as well for the controller we construct a HIOA. The overall model will be the composition of a number of automata. The model discussed above can be structured according to the block diagram representation displayed in Figure 1.

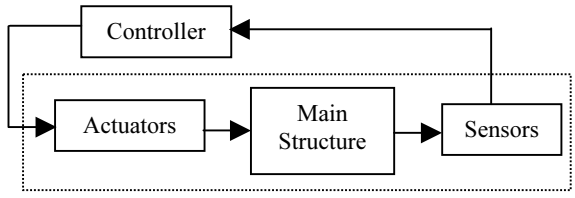


Figure 1: Conti presentation

In this work we are interested in faults, which occur in the components of the plant, especially faults occurring to the main structure. In order to simplify our framework we make the following assumptions:

Assumption 1: *When the system starts functioning all its subsystems are in normal mode*.

Assumption 2: *When a fault occurs the system will remain in that faulty state*.

Assumption 3: *The sensor and controller automata are simple input/output maps.*

Assumption 4: *There are no multiple faults.*

Assumption 5: T*here are no successive faults*.

A sensor automaton S_j reads the values of the main structure output variable as inputs and produces real valued output variables. A controller automaton C reads the corresponding sensor output variables and uses them to generate the input action of an actuator. An actuator A_i reads the corresponding controller output variables to generate the input action of the main structure.

Main Structure

As mentioned above the main structure is modeled by an automaton P that is:

$$P = \left(U_P, X_P, Y_P, \Sigma_P^{in}, \Sigma_P^{\text{int}}, \Sigma_P^{out}, \Theta_P, D_P, W_P\right)$$

The main structure automaton *P* has input and internal actions and has no output actions, hence $\Sigma_P^{out} = 0$. Therefore automaton P will take the form

$$P = \left(U_P, X_P, Y_P, \Sigma_P^{in}, \Sigma_P^{\text{int}} \Theta_P, D_P, W_P\right)$$

The input action set Σ_P^{in} is partitioned into subsets $\Sigma_{P_i}^{in}$ $i = 1,..., n_A$ one for each actuator. The main structure automaton *P* communicates with the automaton of each subsystem through the set of input actions and the set of output variables. These input actions might be characterized as either *normal* or *faulty* according to the effects, which affect to the plant behavior. The continuous system evolution is interrupted by the input actions. Using this hybrid automaton we can model the effects of faults captured from both the discrete transitions and the trajectories.

Plant

The plant is modeled as an automaton *H* that has no output actions

$$H = \left(U_H, X_H, Y_H, \Sigma_H^{in}, \Sigma_H^{\text{int}}, \Theta_H, D_H, W_H\right)$$

Based on assumption 3, sensors and controllers are modeled as automata that are simple input/output maps.

System

The system is modeled as an automaton *S* that has no input output actions and input output variables, so we have

$$S = \left(X_S, \Sigma_S^{\text{int}}, \Theta_S, D_S, W_S\right)$$

Actuators

An actuator is modeled as an automaton A_i that has no internal actions, so we have:

$$A_i = \left(U_i, X_i, Y_i, \Sigma_i^{in}, \Sigma_i^{out}, \Theta_i, D_i, W_i\right)$$

2.2 Fault Modeling

Due to space limitations, in this paper we only present the case where, when a fault occurs it is due to the main structure (actuators, controller and sensors are fail-safe). Consider a fault and assume that the same automaton models both the normal and the faulty behavior. We consider that the faults do not affect the system output, i.e. $Y_{SN} = Y_{SF}$ where the subscripts *N* and *F* indicate whether the system is normal or faulty.

When a fault occurs there is some kind of internal action. This means that $\Sigma_P^{\text{int}} = 0$ if the main structure operates in normal mode and $\Sigma_P^{\text{int}} \neq 0$ if the main structure malfunctions.

According to the definition of HIOA the states may change either continuously or discreetly. Thus the variables will evolve either continuously as functions of time or be subject to instantaneous "jumps". The continuous state evolution is modeled by trajectories while the discrete state evolution is representing by the actions.

Consider $s \in \boldsymbol{V_P}$ a state of the main structure. This state can keep evolving continuously, as long as:

$$\forall s_t \in \boldsymbol{V_P},\ s_t \in \omega_P \text{ then } s_{t+\Delta t} \in \omega_P$$

where s_t is the state of main structure the moment *t* and Δt is the time interval at which the state evolves continuously at the trajectory ω_P.

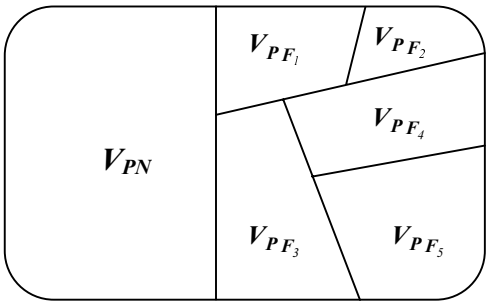
Whenever an input action occurs to the main structure its state will either jump to another state or remain to its current state and evolve continuously. The second case will take place whenever the main structure's output variables coincide with the desired ones. In our approach the information about the occurrence of a fault will be provided in the following stages.

Continuous Stage

The set W_P describes the continuous behavior of the HIOA. The information about the fault occurrence from this set will be based on a standard technique of analytical redundancy and more specifically at the new model based diagnosis framework suggested in [14]. According to this method and if disturbances affecting the system are ignored, the system model consists of a plant $G(f_G)$ and a vector valued signal $z(t, f_z)$, where the parameters f_G and f_z are used to describe possible faults. Therefore the set U_P of input variables is partitioned into two subsets U_{PN} and U_{PF} corresponding respectively to known inputs e.g. control signals and other unknown signals describing faults. Thus we have $U_P = U_{PN} \cup U_{PF}$.

Likewise the set X_P of internal variables is partition into two subsets X_{PN} and X_{PF} describing the normally and faulty operation respectively. Thus we have $X_P = X_{PN} \cup X_{PF}$.

According to the above partition the valuation of the vector $V_{PF} = [U_{PF} \quad X_{PF}]$ is called the *fault state* representing the faulty behavior of the main structure, while the vector $V_{PN} = [U_{PN} \quad X_{PN}]$ is called the *no fault state* representing the normal behavior of the main structure. The *fault state space* of V_{PF} will be denoted $\boldsymbol{V_{PF}}$ and the *no fault state space* will be denoted $\boldsymbol{V_{PN}}$. The different faults of main structure can be classified into different faulty modes. This classification corresponds to a partition of the fault space $\boldsymbol{V_{PF}}$ into subsets $\boldsymbol{V_{PF_i}} \subseteq \boldsymbol{V_{PF}}$ where *i* is the fault modes. All sets $\boldsymbol{V_{PF_i}}$ are pair-wise disjointed which means that only one fault mode can be present at the same time. The fault-free case appertains to $\boldsymbol{V_{PN}}$. Thus the total state space is divided into different subsets as illustrated in Figure 2.



Then the total state space can be expressed as

$$\boldsymbol{V_P = V_{PN} \cup V_{PF}}.$$

Discrete Stage

The set D_P determines the discrete evolution of the state. From all news states after the jumping only a certain number of them correspond to the commands and so they represent a normal behavior of the main structure. Therefore the set D_P of discrete transitions is partition into two subsets D_{PN} and D_{PF} respectively for the transitions, which correspond to the normally operation and faulty operation. Then

$$D_P = D_{PN} \cup D_{PF}$$

The two aforementioned sets are defined as follow:

$$D_{PN} = \bigcup \left\{ (s, \alpha, s') \mid (s, s') \in V_{PN}, \alpha \in \Sigma_P^{in} \right\} \subset D_P$$

is the set of transitions for which the main structure transits from normal to normal operation, while

$$D_{PF} = \bigcup \left\{ (s, \alpha, s'') \mid s \in V_{PN}, s'' \in V_{PF}, \alpha \in \Sigma_P^{in} \right\} \subset D_P$$

is the set of transitions for which the main structure transits from normal to fault operation.

Based on earlier definitions the transitions D_{PF} guide the main structure to the *fault state space* $\boldsymbol{V_{PF}}$. The classification of different faults into fault modes allows us to associate to every subset $\boldsymbol{V_{PF}}$ a transition or a set of transitions of D_{PF}. This means that the transitions can be classified into different *transition types*, each one for each fault mode. Consequently we have a partition of set D_{PF},

$$D_{PF} = \bigcup_{i \in E} D_{PF_i}$$

where E denote the set of all faults modes.

As we said above the main structure is modeled as an automaton P. Then the model with a fixed value of $\boldsymbol{V_{PF}}$ or/and transition type D_{PF_i} specifies exactly the system situation when a specific fault or no fault is present.

2.3 Faulty Guards

The methodology of fault diagnosis that we suggest is based on *faulty guards*. From the definition of HIOA we can extract the guards, which are defined as following:

$$G_{uard} = \left\{ v \in V \mid (v, \alpha, v') \in D, \quad for\ some \quad v' \right\}$$

The meaning of the guard is that a discrete transition is enabling when the guard is satisfying.

Definition 3: *The faulty guard is defined as following:*

$$G_{uard\,F} = \left\{ v \in V \mid (v, \alpha, v') \in D_F \quad for\ some \quad v' \right\}$$

These guards are the variables which valuations will give transitions to the faulty space.

2.4 Guard Measurement

At each guard is associated a variable. This variable it's either directly measurable (i.e. via a sensor) or depending on a combination of other variables or states, which are mutually linear independent. So we have a number of variables forming a set V_g, which is associated to guards. Therefore, the set V_g of these variables is partitioned into $V_{g_{ind}}$ the set of linear independent variables and V_{g_d} the set of linear dependent variables. Thus we have

$$V_g = V_{g_{ind}} \cup V_{g_d}$$

According to the above partition the following propositions of guard measurement are stated.

Proposition 1: *A guard is directly measurable if*

$$G_{uard} = \left\{ v \in V_{g_{ind}} \mid (v, \alpha, v') \in D, \quad for\ some \quad v' \right\}$$

and the system is observable.

Proof: Since the variable is linear independent it is a state variable. Moreover the system is observable and so this state variable can be determined from the knowledge of the outputs. Therefore the associated guard is also measurable. ■

Definition 4: *A guard is not directly measurable if*

$$G_{uard} = \left\{ v \in V_{g_d} \mid (v, \alpha, v') \in D, \quad for\ some \quad v' \right\}$$

Proposition 2: *If the variable associated to a guard is not linear independent and the system is observable then its valuation dependent to a combination of other state variables*.

Proof: Since the variable is linear dependent it is not a state variable. Then this variable can be expressed as combination of others variables, which are state variables. As the system is observable, the state variables can be determined from the knowledge of the outputs. Therefore the depended variable and consequently the associated guard could be evaluated. ■

2.5 Guard Properties

We now state a few properties of the guards that follow from the aforementioned definitions.

P1) The directly measurable guards are linear independent, thus for $g_{F_i} \in G_{uardF}$ there are x_i for which the condition $x_1 v_1 + x_2 v_2 + \cdots + x_i v_i = 0$ is satisfied only when $x_1 = x_2 = \cdots = x_i = 0$

P2) The measurable dependent guards, dependent from variables which are mutually linear independent, thus for $g_{F_i} \in G_{uardF}$ there are x_i and only one of them is different from zero, for which the condition $x_1 v_1 + x_2 v_2 + \cdots + x_i v_i = 0$ is satisfied.

3 Diagnosability of Hybrid Systems

In this section we introduce the notion of diagnosability of Hybrid Systems and we impose the conditions for a system to be diagnosable.

Simply speaking a system is said to be diagnosable if it is possible to detect the occurrence of a fault in a short period of time. Thus,

Definition 5: *A Hybrid System S is to be* ***diagnosable*** *if the following hold*

$$\forall F_i \in E,\ \exists k_i \in N,\ \forall g_{F_i} \in \alpha_i,\ \forall \alpha_i \in S \mid$$
$$\forall t \in htrace(a_i),\ \|t\| \geq k_i,\ g_{F_i} \in htrace(a_i)$$

The above definition means the following. For every fault $F_i \in E$, and for every faulty guard contained to a hybrid execution α there are k_i alternations of trajectories and actions after the occurrence of fault. Then for been the hybrid system *S* diagnosable should exist a certain hybrid trace with any sufficiently long continuation *t* from alternations of trajectories and actions after the occurrence of fault that contain the same faulty guard.

There is the case where it is impossible to conclude which fault mode has occur. To describe this situation we give the next definition.

Definition 6: *A hybrid faulty state is indistinct if it is not clear which fault mode has occurred*.

The following result is consequence of the guard definition.

Lemma 1: *If a state is indistinct, then* $\exists v \in V_g$ *such that:* $(v, \alpha, v') \in D_{F_i}, F_i \in a_i,\ (v, \alpha, v'') \in D_{F_j}, F_j \in a_j$ *and* $htrace(a_i) = htrace(a_j)$.

3.1 Diagnosability Conditions

We can now define the conditions under which a system is diagnosable. These conditions are necessary and sufficient for a hybrid system to be diagnosable.

Theorem 1: *A hybrid system without multiple failures of the same mode is diagnosable if and*

only if the following conditions are satisfied:

C1: *There is a measurable faulty guard*.

C2: *No state in a htrace(a) is indistinct*.

Proof: **Necessity:** First we prove that if the hybrid system is diagnosable then it satisfies condition C1. By contradiction assume there isn't a measurable faulty guard. As consequence we can't define the variable the valuation of which will give the discrete transition to a faulty state. That is $\exists v \in V,\ d_i \in D_F \mid g_{F_i} \notin G_F,\ g_{F_i} \in a_i,\ F_i \in a_i$ while $g_{F_i} \notin htrace(a_i)$ and $F_i \notin htrace(a_i)$. Therefore the definition of diagnosability is violated and the system is not diagnosable.

We now prove that if the hybrid system is diagnosable then it satisfies condition C2. By contradiction assume there exist a faulty guard g_{F_i} appertain in two different fault mode, that is $g_{F_i} \in V_{PF_i}$ *and* $g_{F_i} \in V_{PF_j},\ i \neq j$. Then for some *i* $\exists v \in V_g$ satisfying lemma 1. Since, by assumption, multiple failures from the same faulty state do not occur and only one fault mode can be present at the same time $g_{F_i} \in V_{PF_j}$, $g_{F_i} \notin V_{PF_i}$. Hence choosing $F_j \in a_j$ and since $htrace(a_i) = htrace(a_j)$ the $P^{-1}\{htrace(a_i)\}$ (where P^{-1} is the inverse projection operator) leads to $F_j \in a_i$. Therefore the definition 5 is violated and the system is not diagnosable.

Sufficiency: Assume that the system satisfies conditions C1 and C2. Pick any $g_{F_i} \in G_{uardF}$ and suppose there are no indistinct states. Then from propositions 1 and 2 there exist a state variable or a number of state variables $v \in V_g$ which valuations specifies exactly the faulty state that has occur and by lemma 1 $\forall v \in V_g$, $(v, \sigma, v') \in D_{F_i}, F_i \in a_i$, $(v, \sigma, v'') \notin D_{F_j}, F_j \in a_j$ and $htrace(a_i) \neq htrace(a_j)$. Since one fault mode corresponds at each faulty state, we can conclude which fault $F_i \in E$ has appeared. So the system is diagnosable. ■

4 Applications to an Electric Power Transmission System

Power systems often exhibit complex behavior in response to large disturbances. Such behavior is characterized by interactions between continuous dynamics and discrete events. Components such as loads drive the continuous dynamic while others components such as protection devices exhibit event-driven discrete dynamics. Therefore power systems are an important example for fault detection of hybrid systems.

In our example (Figure 4) a simple power system consisting of a voltage source, two-transmission lines, two current measurements, two voltage measurements, a relay and a circuit breaker. The system is built and simulated with, the Power System Blockset, which operates in the Simulink™ environment, and the Stateflow™, all running on top of Matlab™. The relay and threshold blocks act as an interface between the Power System Blockset blocks and the Stateflow™ block.

A power system is considered to exhibit different states, which are *normal state*, *emergency state* and *restorative state* [3]. Usually a typical system is found in its normal state. In this state certain inequalities must also be observed, such as the transmission lines must not be load above their limits. The hybrid behavior of this system is due to the on/off position change of the breaker and thus the energizing and de-energizing of line-2 and the overload of line_1. We are interested in capturing only abrupt faults occurring to the lines, ignoring the transients and considering only the steady state. All lines are modeled by pi-equivalents as shown in Figure 4. Their dynamics are described by specifying a number of discrete states as shown from their automata in Figure 3.

The overall model is a composition of a number of automata. Due to space limitations only the lines and diagnoser automata appear in Figure 3, which is a Stateflow chart. The chart consists of three parallel states (denoted by dash-dotted

boundaries) that represent concurrent modes of operation. The two parallel states at the top of the Figure 3 correspond to the two lines. Each state has sub-states that represent the status of that particular line. These sub-states are mutually exclusive. If the line-2 has de-energized then it is in the LINE_OFF state. Transitions determine how states can change and are guarded by conditions. The third parallel state corresponds to the diagnoser [5], which has two sub-states that represent the normal and fault operating mode of the system.

A disturbance was applied to the power system via the circuit breaker to allow energizing and de-energizing of line-2.

5 Conclusions

We have introduced the notion of diagnosability of hybrid systems and we impose the conditions for a Hybrid System to be diagnosable. The theory presented at [4, 5] has been completed appropriately in order to take into account the isolation of malfunctioning component. The contribution of this paper is mainly focused at notion of diagnosability. This approach was illustrated via a simple application to an electric power transmission system.

Our current directions include the algorithmic design of the diagnoser and how it can be used to diagnose failures in diagnosable systems, as well as the study of faults occurring at other system components. An important issue for investigation is that of complexity, in cases where large number of components and subsystems are present.

References

[1] M. S. Branicky, Studies in Hybrid Systems: Modeling, Analysis and Control, PhD thesis, Massachusetts Institute of Technology, Dept. of Electrical Eng. and Computer Science, (1995).

[2] C. G. Cassandras D. L. Pepyne, "Optimal control of a class of hybrid systems", in IEEE Conference on Decision and Control, San Diego, California, pp. 133-138, (1997).

[3] O. I. Elgerd, "Electric Energy Systems Theory", McGraw-Hill (1982).

[4] G. K. Fourlas, K. J. Kyriakopoulos, N. J. Krikelis, "Contribution to the Fault Detection for Hybrid Systems", Proceedings of the 8th IEEE Mediterranean Conference on Control and Automation, Rio, Patras, Greece, (2000).

[5] G. K. Fourlas, K. J. Kyriakopoulos, N. J. Krikelis, "A Framework for Fault Detection of Hybrid Systems", Proceedings of the 9th IEEE Mediterranean Conference on Control and Automation, Dubrovnik, Croatia, (2001).

[6] P. M. Frank, "Fault Diagnosis in dynamic Systems Using Analytical and Knowledge-based Redundancy, A Survey and Some New Results", Automatica, vol. 26, no. 3, pp. 459-474 (1990).

[7] T. Henzinger, "The theory of hybrid automata", Proceedings of 11th IEEE symposium on Logic in Computer Science, LICS, pp. 278-292 (1996).

[8] A. Hiskens, M. A. Pai, "Hybrid systems view of power system modeling" ISCAS 2000, May 28-31, Geneva, Switzerland (2000).

[9] J. Lygeros, G. J. Pappas, S. Sastry, "An approach to the verification of the Center-TRACON Automation System", in Hybrid Systems: Computation and Control, vol. 1386 of LNCS, pp. 289-304, Springer Verlag (1998).

[10] J. Lygeros, D.N. Godbole, S. Sastry, "Verified hybrid controllers for automated vehicles", IEEE Trans. on Autom. Contr, 43(4) pp. 522-539, (1998).

[11] N. Lynch, R. Segala, F. Vaandrager, H. Weinberg, "Hybrid I/O automata", Hybrid Systems III, no. 1066, LNCS, pp. 496-510, Springer Verlag (1996).

[12] Z. Manna, H. Sipma, "Deductive verification of hybrid systems using SteP", Hybrid Systems: Computation and Control, no 1386 in LNCS, pp. 305-318, Springer Verlag (1998).

[13] P. J. Mosterman, Hybrid Dynamic Systems: A hybrid bond graph modeling paradigm and application in diagnosis, PhD thesis, Graduate School of Vanderbilt University, (1997).

[14] M. Nyberg, Model Based Fault Diagnosis: Methods, Theory and Automotive Engine Applications, PhD thesis, Department of Electrical Engineering, Linkoping Univ., Linkoping, Sweden, (1999).

[15] R. Patton, P. Frank, R. Clark, "Fault Diagnosis in Dynamic Systems – Theory and Application", Prentice Hall (1989).

[16] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, D.C. Teneketzis, "Failure Diagnosis using discrete-event models", Trans. On Control System Techn., vol. 4, no.2 pp.105-124, (1996).

[17] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, D. C. Teneketzis, "Diagnosability of Discrete-Event Systems", Trans. On Control System Tech., vol. 40, no.9 pp.1555-1575, (1995).

[18] C. Tomlin, G. J. Pappas, S. Sastry, "Conflict resolution for air traffic management: A study in multi-agent hybrid systems", IEEE Transactions on Automatic Control, 42(4) pp. 509-521, (1998).

[19] P. Varaiya, "Smart cars on smart roads: problems of control", IEEE Transactions on Automatic Control, 38(2) pp. 195-207, (1993).

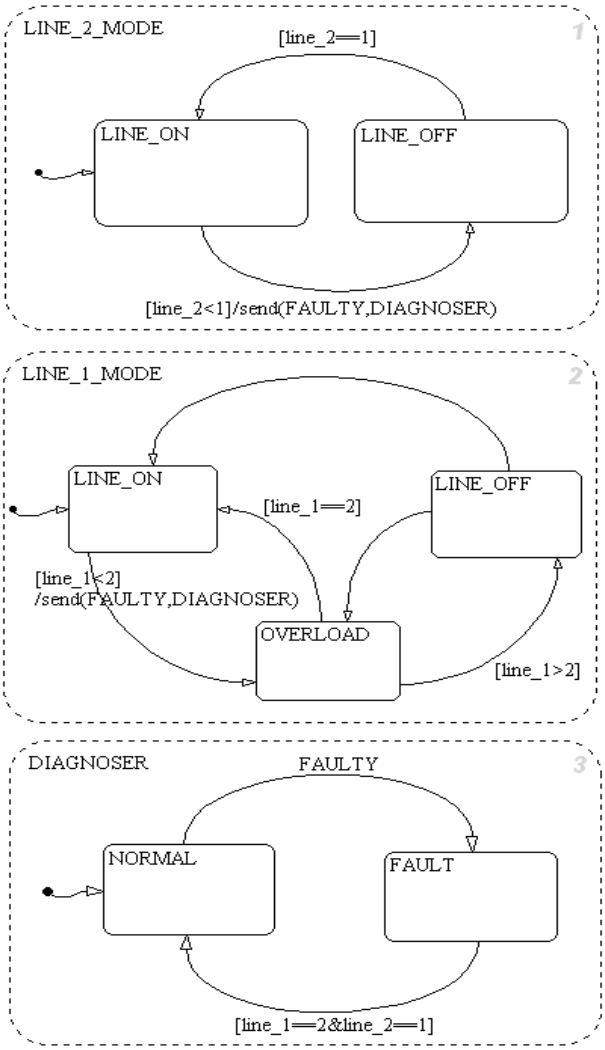


Figure 3: Lines and Diagnoser Automata

Figure 4: Electric Power Transmission System