FAULT DIAGNOSIS BASED ON BACKWARD TIME ANALYSIS

Michal KNOTEK, Doctoral Degree Programme (2)
Dept. of Control and Instrumentation, FEEC, BUT
E-mail: xknote02@stud.feec.vutbr.cz

Supervised by: Prof. František Zezulka and Assoc.Prof. Zineb Simeu-Abazi

ABSTRACT

We study the problem of fault diagnosis in the context of timed discrete event systems (TDES). If an incorrect behaviour of the system is detected, the second phase denotes to the fault location. The aim of the fault location is to find the cause of a system dysfunction. Proposed method for fault location works with the timed model (timed automata) and is based on a model-checking technique. This technique (also called verification) treat a model of a plant by backward time analysis, the coherent trace in a timed automata is searched. Our method is illustrated by an example of two-tank system.

1 INTRODUCTION

In the context of discrete event system the problem of fault diagnosis has been well-studied, but much less work has been done in the timed framework. Our interest lies in the fault diagnosis problem for *timed* plants. Here, we are given a plant modelled as a timed automaton. Let us note problem is considerably more difficult in the timed case than in the discrete case.

The problem of fault diagnosis involves to detect, locate and identify the considered faults occurring in the dynamical system (also we call a *plant*)[3].

Let us remind of the fault diagnostic purposes [1]:

Fault detection: The algorithm should determine if a fault has occurred in the system.

Fault location: If a fault has occurred, the faulty component in the system has to be determined.

Fault identification: The location of the fault and its magnitude should be determined.

If an incorrect behaviour of the system is detected by the fault detection system (alarms implemented in a plant), the second phase is fault location. Our aim is the fault location by the model-checking techniques. These techniques are based on verification of timed model (timed automata), where for the model of plant M the property ϕ is checked. We posed that property to check is length (elapsed time) of the trace in the timed automaton.

The diagnostic algorithm is also called *diagnoser*. Diagnoser is just a function which take sequences of observable events and the global time of fault occurrence to decide which fault was detected.

2 DISCRETE MODELLING TECHNIQUES

Discrete formalism To represent the continuous system dynamics in the discrete formalism, the first step is to discretise the state space. Each domain of the continuous system is partionned according to thresholds into a finite number of intervals that can be considered as qualitative states. Thresholds are defined from the expert knowledge. A level in the tank can be qualified as *low*, *medium*, *high* and *critical*.

The continuous model of the plant is first approximated using intervals and then translated into the timed automata formalism [2]. The step of approximation is based on the knowledge of plant evolution for all considered faults.

2.1 TIMED AUTOMATA

We use finite-state automata for description of the plant behavior [4], [5]. Our interest lies in the timed plant. Plant behavior corresponds to a run of the automaton, which corresponds to the execution of a sequence of events. The considered faulty behavior is implemented in the plant model.

3 FAULT DIAGNOSIS

Once we have prepared the model of the plant in the form of timed automata, we can deal with the diagnostic technique for fault location. Our diagnostic technique is based on time analysis for fault location, where the coherent trace is searched by the verification of elapsed time with global time of alarm.

Verification. The verification of timed automata is domain in huge research interest [7], [6]. The verification task is defined as follow: For given a timed system and a property, check whether the system satisfies the property. We pose that the property to check denotes the elapsed time in the timed automaton. The elapsed time of the trace which is searched is equal to the global time of fault occurrence. From all traces possible, by verification we obtain the set of coherent traces with the time of fault occurrence. So we expect that real alarm announces the fault and thus the coherent path in the model of all possible evolutions is searched. The aim is to find the coherent diagnostic path, which corresponds to the faulty evolution of the system.

3.1 BACKWARD TIME ANALYSIS

In our case verification (analysis) means searching accessible trace of timed automata (reverse path). This reverse path project the evolution of the system, from a final faulty state to the initial state. The reverse path is also called diagnostic path. We suppose the initial state is known. Our task can be seen as retrace the automaton graph from the faulty states to the known origin state. The aim is to find from the set of reverse path the coherent ones.

Illustrative example. Principle of the analysis is shown in automaton graph with fault model (See Figure 1). From fault model one can see that fault F_1 can occurs from states 2, and the fault F_2 from the state 3. The diagnostic model must be defined that if fault occurs in the system, fault must be located according the time instant. If the fault occurs in the time 5_{tu}, it's fault located as F_1. In another case, the fault occurs in the time 7_{tu}, the fault F_2 is located.

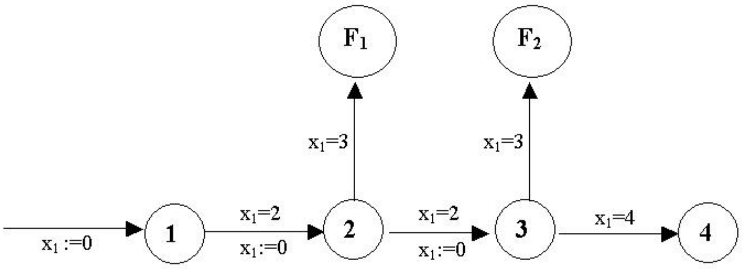

Figure 1: Principle of the backward time analysis.

3.2 DIAGNOSTABILITY

Not all plants are diagnosable. For example a plant which produces the two behaviours *aub* and afb, where u and f are internal (unobservable) events with f being faulty one and a and b are observable events. By observation of the sequence *ab*, it is impossible to tell whether f happened or not. The diagnosability in the context of timed plant we define: Let Σ be sequences of observable events, if the plant has own projection (the reverse path) for each mode (faultless and considered faulty modes) the plant is called diagnosable.

If we find that the plant is not diagnosable, it is not possible distinguish the considered fault, the additional information must be add to obtain the desired level of diagnosability. Add an additional information means an observable event (sensor), which must be inserted to distinguish the faults.

4 EXAMPLE

To illustrate the idea of backward time analysis, here is an example fault diagnosis on a batch process. Let us consider the trivial two-tank system in Figure 2. The system is equipped by the overflow sensor o , which produces an alarm. The events a, b are not observable. Alarm could be caused by valve V_1 stuck open or valve V_2 stuck close. The model of plant must consider these two causes and implement them into the diagnostic

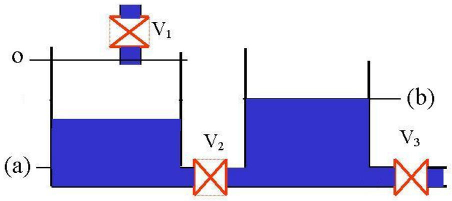

Figure 2: Tanks example.

model (automata graph). If an alarm is produced, cause of the fault is searched in the automata graph by time analysis.

The considered faults are:

1. valve V_1 being stuck open (fault f_1)
2. valve V_2 being stuck close (fault f_2).

4.1 THE MODEL OF TIMED AUTOMATA

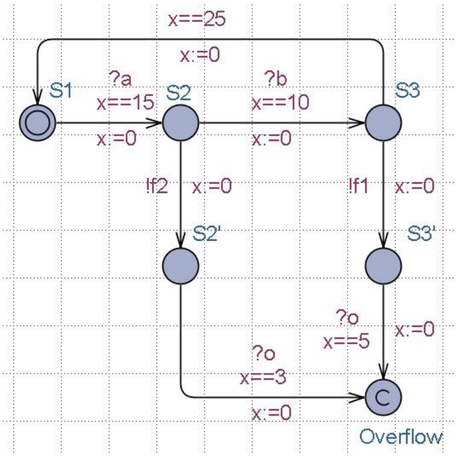

Figure 3: The model by the timed automata.

The states of the model are represented by the different dynamics. The dynamics is defined by the states of valves (See table 1). The states $2'$ and $3'$ represent the dynamics of the non-desired evolution. The fault origin is represented in the model by the unobservable events f_1 and f_2.

Backward time analysis If the reachable faulty state is f_1 the corresponding elapsed time from initial time must be in the interval as follow: $\mathrm{time}(f_1) = [30, 30]_{\mathrm{tu}}$. Similarly, for the case of f_2 the interval is $\mathrm{time}(f_2) = [18, 18]_{\mathrm{tu}}$. See the different diagnostic path on Figure 3. For fault diagnosis of cyclic case, we add to time $\mathrm{time}(f_1), \mathrm{time}(f_2)$ the time of one faultless cycle $t_{Cycle} = 50_{tu}$.

State	Valves position
1	$V_1, \overline{V_2}, \overline{V_3}$
2	$V_1, V_2, \overline{V_3}$
3	$\overline{V_1}, V_2, V_3$
$2'$	$V_1, \overline{V_2}, V_3$
$3'$	V_1, V_2, V_3

Table 1: States of the model.

5 CONCLUSION

Modern industry deals with efficient fault diagnosis to improve reliability relevant functions. In this paper, we have introduced the diagnostic method for fault location. Diagnostic algorithm also called diagnoser worked with timed model (timed automaton). This model contained all considered evolutions of the system (faultless and considered faulty modes). Diagnostic algorithm was based on backward time analysis. Our task was to find coherent path in the timed automaton model, which denotes such faulty evolution. Finding the path means timed automata verification, where the properties of length (elapsed time) of the automaton run was checked. Our diagnostic approach is attractive for the plant where alarm announces the failure and where more faults (causes of faults) are possible.

REFERENCES

[1] Blanke, M., Kinnaert, M., Lunze, J., Staroswiecki, M.: Diagnosis and Fault-tolerant Control. Springer Verlag, 2003.

[2] Hélias, A., Guerrinand, F., Steyer, J.-P.: Abstraction of continuous system trajectories into timed automata. In Workshop on Discrete Event Systems WODES'04, pages 319–324, Reims, France, 2004. IFAC.

[3] Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., Teneketzis, D.: Diagnosability of discrete event systems. IEEE Transactions on Automatic Control, 40(9):1555–1575, 1995.

[4] Tripakis, S.: L'Analyse Formelle de Systemes Temporisés en Pratique. PhD thesis, Université Joseph Fourier, Grenoble, France, 1998.

[5] Tripakis, S.: Fault diagnosis for timed automata. In FTRTFT, volume 2469, 2002.

[6] web-site Uppaal: `www.docs.uu.se/docs/rtmv/uppaal/`.

[7] Yovine, S.: Méthodes et outil pour la vérification symbolique des systemes temporisés. PhD thesis, VERIMAG – Institut National Polytechnique de Grenoble, 1993.