Chemical Engineering Science 113 (2014) 101–115

Contents lists available at ScienceDirect

Chemical Engineering Science

journal homepage: www.elsevier.com/locate/ces

Automata generated test plans for fault diagnosis in sequential material- and energy-transfer operations

An Kang, Chuei-Tin Chang*

Department of Chemical Engineering, National Cheng Kung University, Tainan, Taiwan 70101, Republic of China

HIGHLIGHTS

- A novel method is proposed to create diagnostic test plans for batch processes.
- An automata-based modeling strategy is adopted to build diagnosers.
- A systematic procedure is developed to synthesize SFCs of the tests.
- The non-unique fault origins of a trace in diagnoser may be differentiated.
- The effectiveness of this approach is demonstrated in three case studies.

ARTICLE INFO

Article history:
Received 17 October 2013
Received in revised form
18 March 2014
Accepted 28 March 2014
Available online 13 April 2014

Keywords:
Fault diagnosis
Test plan
Automaton
Material transfer
Energy transfer
Sequential function chart

ABSTRACT

Hardware failures are inevitable random events that occur in the operation life of a batch chemical plant. Based on the piping and instrumentation diagram (P&ID) of the given process and the sequential function chart (SFC) of its normal operating procedure, a system automaton and the corresponding "diagnoser" can be built to identify all observable fault propagation traces and, also, their root cause(s). Since the fault origin(s) of a trace may not be unique, there is a need to develop a nonconventional means to further enhance diagnostic performance. For this purpose, a novel approach is proposed in this study to synthesize the test plan of every undiagnosable trace on the basis of discrete-event system (DES) theory. In particular, all components at the failure-induced initial states and the required control specifications are first modeled systematically with automata and, then, an optimal supervisor (test plan) can be assembled accordingly so as to achieve the operation goal of differentiating the fault origins as much as possible. This proposed strategy has been tested successfully in a series of examples and the results of selected case studies are reported in this paper.

1. Introduction

Unexpected faults and failures in a chemical plant often result in undesirable consequences, e.g., deterioration in product quality, reduction in productivity and, in worse cases, fire, explosion, or toxic release, etc. Since the offline hazard assessment methods can limit the total expected loss of accidents only to a certain degree, online fault diagnosis is an alternative means for further improving operational safety.

According to Venkatasubramanian et al. (2003a; 2003b, 2003c), the available fault diagnosis methods could be classified into three general types: (1) quantitative model-based approaches; (2) qualitative model-based approaches; (3) process history based approaches. These available methods were developed primarily for the *continuous* chemical processes, while considerably less effort has been devoted to the batch operations. Nomikos and MacGregor (1994, 1995) developed a multi-way principal component analysis method for batch process monitoring, which has later been utilized in online diagnosis studies (Kourti and Macgregor, 1995; Kourti et al., 1995; Undey et al., 2003; Lee et al., 2004). In addition, other fault identification techniques based on the artificial neural networks, the knowledge-based expert systems and the observers (Ruiz et al., 2001a, 2001b; Pierri et al., 2008) have also been proposed for the batch operations. Although satisfactory results were reported, these methods are mostly effective for fault diagnosis in a system with relatively few interconnected units and, also, the diagnostic resolution in cases of coexisting failures may not always be acceptable.

In order to expand the scope of fault diagnosis, Chen et al. (2010) developed several Petri-net based algorithms in a recent study to configure online identification systems for batch plants with many more units. However, since the event sequences (or traces) in multi-failure scenarios cannot be conveniently generated with the

* Corresponding author.
E-mail address: ctchang@mail.ncku.edu.tw (C.-T. Chang).

http://dx.doi.org/10.1016/j.ces.2014.03.028

Petri-net models, this approach was limited to the single-failure accidents. Generally speaking, such model deficiencies can be improved (or avoided) with automata (Sampath et al., 1995, 1996, 1998; Baroni et al., 1999, 2000; Debouk et al., 2000; Benveniste et al., 2003; Zad et al., 2003; Qiu and Kumar, 2006; Yeh and Chang, 2011). With this alternative approach, a so-called “diagnoser” can be constructed on the basis of the automaton model to predict all observable multi-failure fault-propagation event sequences in the given system and to determine the corresponding fault origins. Since the root cause(s) of a trace may or may not be unique, there is *still* a need to enhance the diagnostic resolution with additional measures.

Generally speaking, the diagnostic performance of an existing system can always be improved by capturing more process information and gaining deeper insights of the current plant status. These goals are traditionally achieved with new sensors so as to secure extra online measurement data under abnormal process conditions. However, since execution of diagnostic test plans seems to be a feasible alternative which has not been systematically discussed in the chemical engineering literature, e.g., see Yeh and Chang (2011), it is the objective of this study to develop an effective method to synthesize the required operating procedures.

2. Model building principles

It should first be noted that a generic automaton construction method has already been developed by Yeh and Chang (2011, 2012) for modeling any given batch process with material- and/or energy-transfer operations. For the sake of illustration clarity, this method is reviewed here with a simple example. Specifically, let us consider a fictitious liquid transfer system represented by the piping and instrumentation diagram (P&ID) in Fig. 1 and also the sequential function chart (SFC) in Fig. 2 and Table 1. Notice that the components in this and any other batch process can always be classified into a hierarchy of 4 different levels: (1) the programmable logic controller (PLC); (2) the actuators, i.e., the three-way valves (V-1 and V-3) and the two-way valves (V-2 and V-4); (3) the processing units, i.e., tank and (4) the online sensor(s). If a three-way valve is closed in this liquid transfer system, the port connecting to the horizontal pipeline in Fig. 1, i.e., P-2 in the case of V-1 or P-3 in the case of V-3, is assumed to be blocked. Otherwise, its inlet flow(s) should be directed to every outlet pipeline. It is assumed that all valves *except* V-4 are placed at the “close” position initially. Thus, it is clear from the above SFC that, during the normal operation, the buffer tank is filled with liquid via P-1, P-3 and P-4 by manipulating V-3 and then drained via P-5 by gravity.

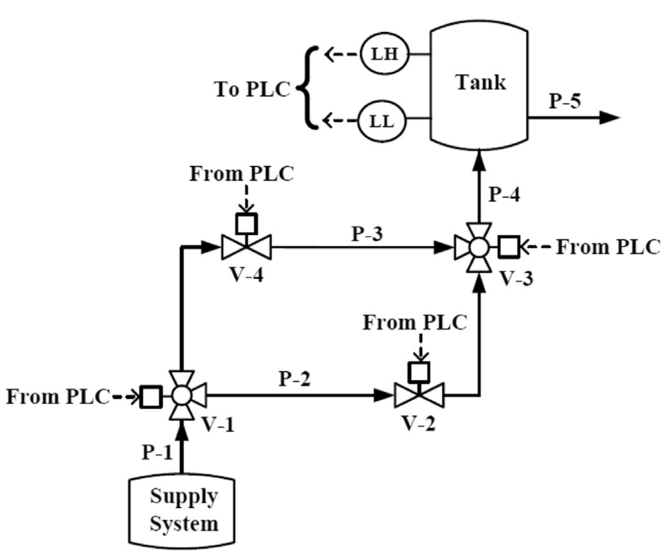

Fig. 1. P&ID of a liquid transfer system.

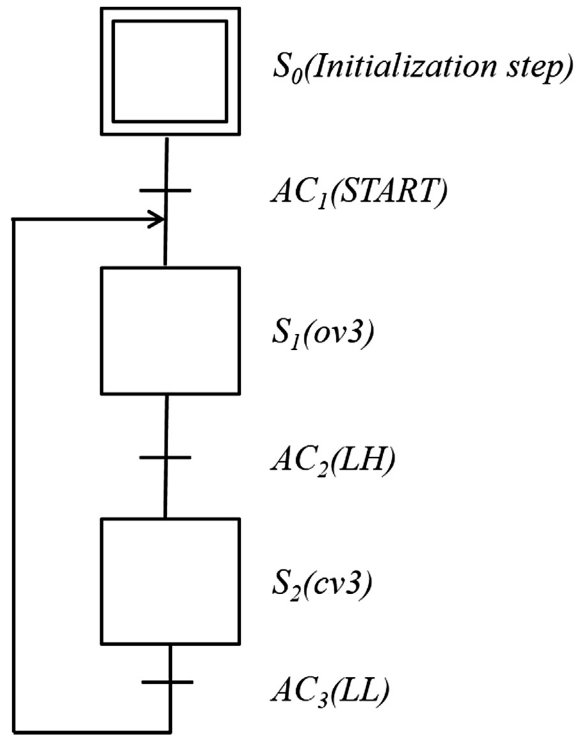

Fig. 2. Normal SFC of a liquid transfer operation.

Table 1
The normal transfer procedure: (a) operation steps; (b) activation conditions.

(a)

Operation step	Control actions
S_0	Initialization
S_1	Open V-3
S_2	Close V-3

(b)

Symbol	Conditions
AC_1	START
AC_2	LH
AC_3	LL

For the sake of brevity, only three failures are considered in this example.

- A large leak develops in tank (which is referred to as “*T1leak*” or F_1);
- V-3 fails at the “close” position (which is referred to as “*v3s_c*” or F_2);
- V-3 fails at the “open” position (which is referred to as “*v3s_o*” or F_3).

Based on the aforementioned assumptions, a total of 8 possible process configurations (*pc01–pc08*) can be identified and they are listed in Table 2. Note that, for valve V-3, there are four possible states: (1) state O, i.e., it is at the normally open position; (2) state C, i.e., it is at the normally close position; (3) state SC, i.e., it sticks at the close position; (4) state SO, i.e., it sticks at the open position. On the other hand, only two tank states are adopted depending on