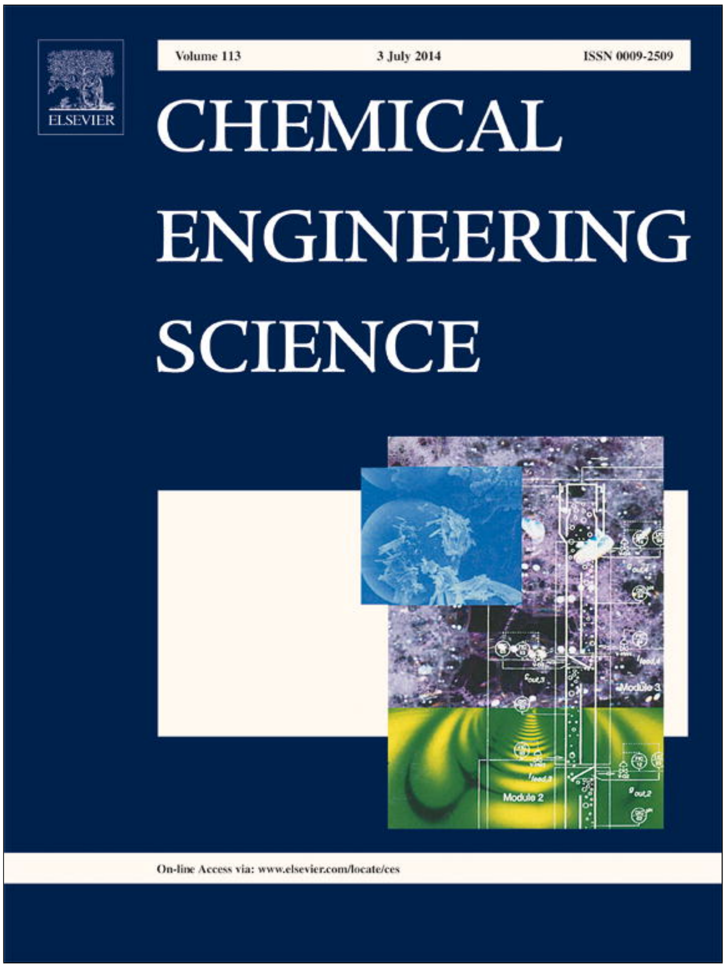

Volume 113 3 July 2014 ISSN 0009-2509

CHEMICAL ENGINEERING SCIENCE

On-line Access via: www.elsevier.com/locate/ces

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
0009-2509/© 2014 Elsevier Ltd. All rights reserved.

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.

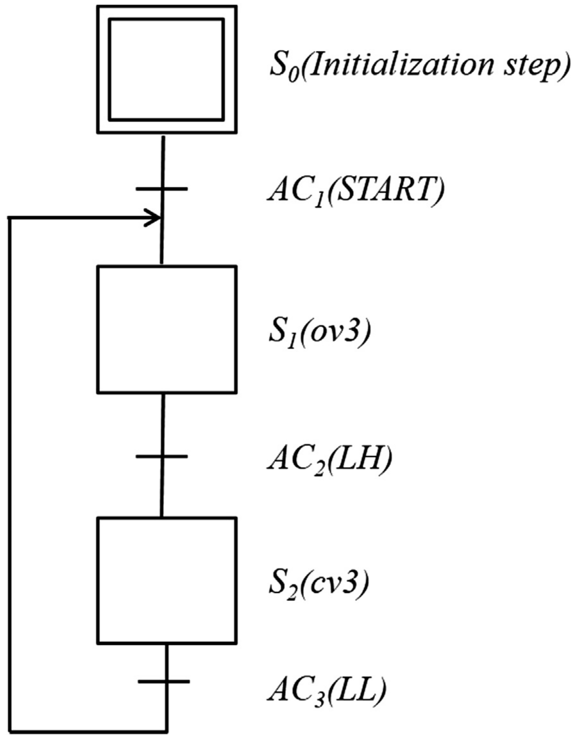

Fig. 2. Normal SFC of a liquid transfer operation.

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

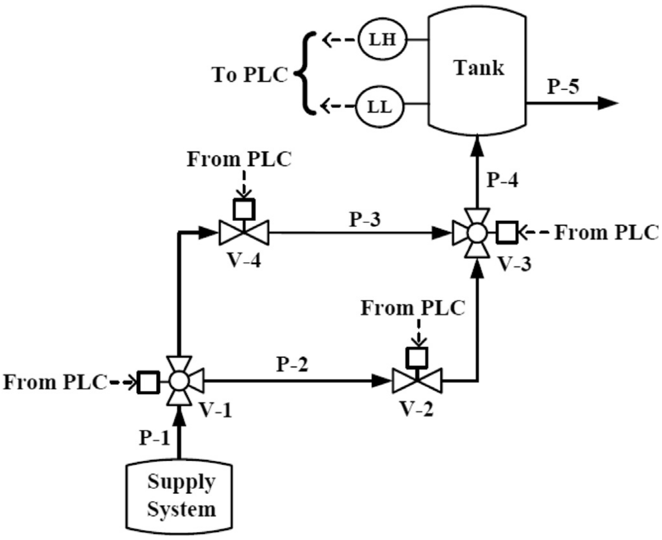

Fig. 1. P&ID of a liquid transfer system.

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

Table 2
Process configurations of the liquid transfer system without diagnostic tests.

V-1	V-2	V-3	V-4	*T1leak*	Symbol
C	C	C	O	N	*pc01*
C	C	O	O	N	*pc02*
C	C	SC	O	N	*pc03*
C	C	SO	O	N	*pc04*
C	C	C	O	Y	*pc05*
C	C	O	O	Y	*pc06*
C	C	SC	O	Y	*pc07*
C	C	SO	O	Y	*pc08*

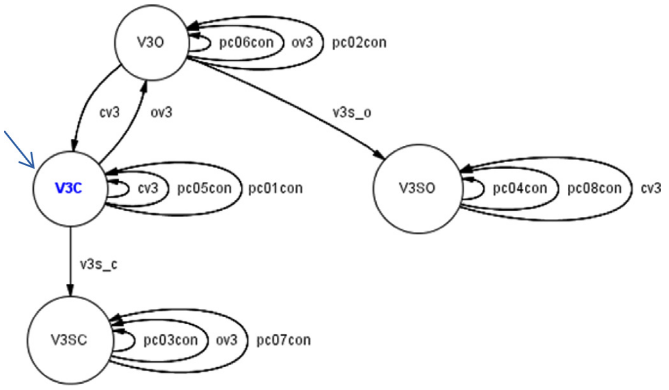

Fig. 3. The component model for valve V-3 in the liquid transfer system.

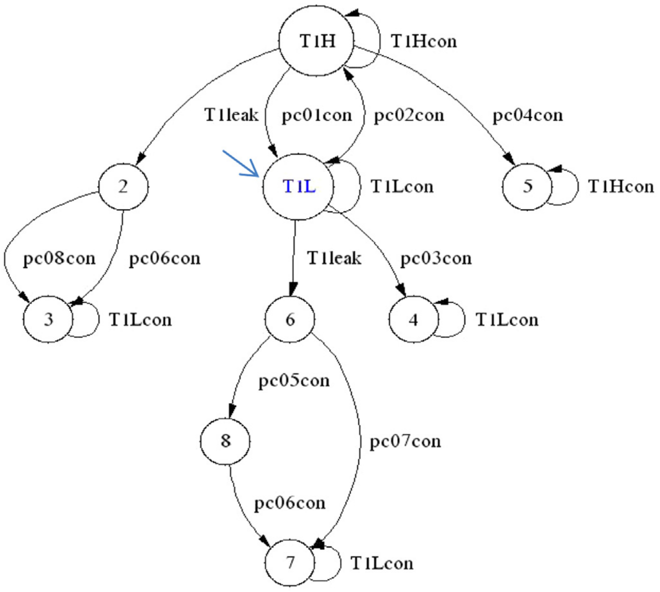

Fig. 4. The tank model in the liquid transfer system.

whether or not a leak develops. Finally, notice that the states of V-1, V-2 and V-4 are unchanged since they are not used in normal operation and also their failures are not considered in the present example.

The plant model can in general be obtained by first building automata to model all components in the given process and then integrating them via the standard parallel decomposition operation (Cassandras and Lafortune, 1999). In this work, the controller and the remaining components in a batch plant are modeled with two different approaches. The corresponding model building principles are illustrated below.

As a general rule, every component model in the last three hierarchical levels, i.e., the actuators, the processing units and the sensors, is used in this work to represent a finite set of identifiable states of the hardware item under consideration and also the specific events facilitating the state transitions. A transition from one state to another is caused by the so-called *state-transition event*, while a self-looping transition is resulted from the *state-maintaining event*. Notice that the latter event may (or may not) be bypassed if one or more former event is present at the originating state. To illustrate this model building principle, let us use the component model of V-3 (Fig. 3) as an example. Under the normal conditions, there are only two valve states (i.e., V3O and V3C) representing the open and close positions respectively. Note that the action to close or open V-3 (denoted as *cv3* and *ov3* respectively) can be either a state-transition or a state-maintaining event depending on the starting valve state. The eight (8) additional state-maintaining events in this model, i.e., *pc01con*–*pc08con*, represent the scenarios that the corresponding configurations are maintained for a sufficiently long period of time. Finally, notice that the initial state in this model is marked by attaching an incoming arrow without origins.

Another important feature is that the state-maintaining event at a higher hierarchical level may be used as a lower-level state-transition event. To illustrate this model building technique, let us use the tank model (Fig. 4) as an example. In this automaton, T1H and T1L denote the normal operating conditions when the liquid height reaches the designated maximum and minimum values respectively. The state-transition events between these two states, i.e., *pc01con* and *pc02con*, are the state-maintaining events in the automaton representing V-3. Note also that, since no sensor failures are considered here, it is assumed that the online measurements always accurately reflect the tank states and, thus, the sensor model can be omitted.

After building the automaton to model a normal component, additional mechanisms can be incorporated to describe its failures. Generally speaking, every failure can be modeled as a state-transition event, which triggers a change from one of the normal states to an abnormal one. Let us again consider the component models of V-3 and Tank in Figs. 3 and 4. In the case of V-3, the failure *v3s_c* activates the state transition from V3C (normal) to V3SC (abnormal) while *v3s_o* from V3O (normal) to V3SO (abnormal). In the case of tank, the failure *T1leak* induces two different transitions from the normal states T1H and T1L to the abnormal states 2 and 6 respectively. Since the lower-level component states are obviously affected by the upper-level failures, the impacts of *v3s_c* and *v3s_o* should also be described in the tank model by using the state-transition events *pc03con*–*pc08con*. Notice that each of these abnormal configurations can only be obtained after reaching a corresponding normal one, i.e., after the event *pc01con* or event *pc02con*. For illustration convenience, let us also assume that the effect of leak dominates that of inlet flow and, thus, the eventual liquid level is always low after *T1leak*. On the other hand, due to the absence of sensor failures, the state-maintaining events in the tank model, i.e., *T1Hcon* and *T1Lcon*, should be treated as the corresponding online level measurements as well. It should be emphasized that the practice of omitting the sensor models in this example is by no means restrictive. If a more comprehensive fault diagnosis is required, it is only necessary to build the neglected component models with the aforementioned techniques. The test-plant synthesis procedure described later in this paper is still directly applicable.

As mentioned before, the level-1 component should be modeled with a different approach. In particular, a subset of all events that are allowed in the remaining levels should be selected and assembled according to the operation steps and activation conditions specified in the given SFC. For example, the PLC model for the aforementioned liquid transfer system can be synthesized with this strategy (see Fig. 5). Notice first that the loop formed by states 0–5 represents the normal operation cycle (see Fig. 2). Since it is

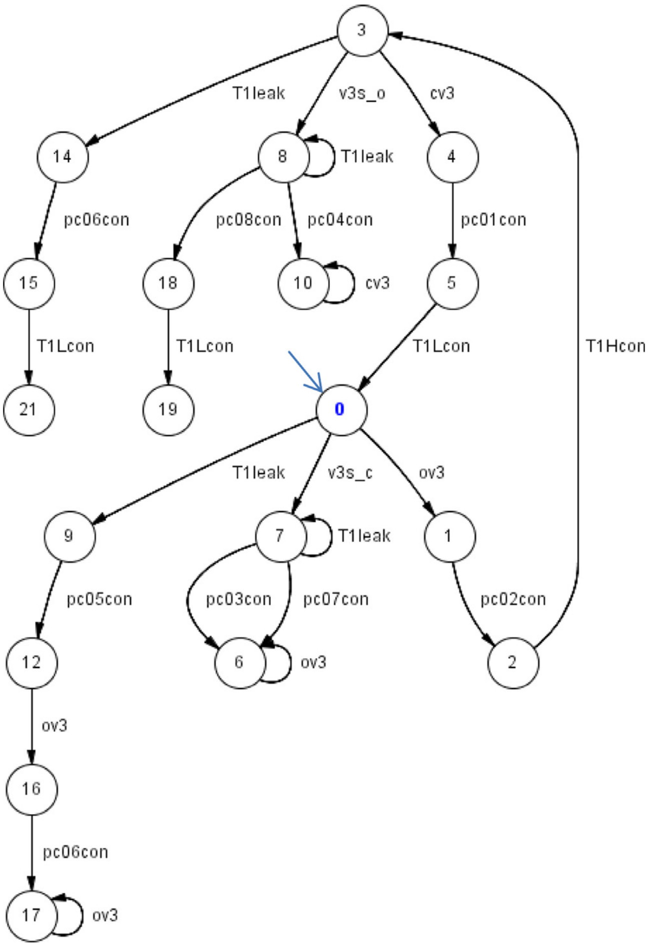

Fig. 5. The PLC model in the liquid transfer system.

also necessary to stipulate the controller behavior after one or more failure occurs, additional 6 branches are then attached to this loop to describe the fault propagation paths associated with configurations *pc03–pc08* respectively. The self-looping event at state 7 is placed simply to facilitate succinct representation of two different scenarios (with and without *T1leak*) after failure *v3s_c* occurs, while the same modeling approach is adopted at state 8 to characterize the event sequences after failure *v3s_o*. The self-looping events placed at state 6 and state 17 are used to describe the scenarios that the actuator action *ov3* is executed repeatedly without changing the persisting low liquid level and, for the same reason, a self-looping event *cv3* is introduced at state 10 to indicate that the liquid level is constantly high even after multiple attempts to close V-3. Finally, notice that the deadlock states 19 and 21 are adopted primarily to highlight the fact that no control actions are called for since the required activation condition cannot be met in these two scenarios.

3. Observable traces in diagnoser

After obtaining the system model, a diagnoser can then be produced by following the procedure given below (Cassandras and Lafortune, 1999):

(1) Assign a distinct numerical label to a selected state in the system model.
(2) Identify all paths between the initial state and the one selected in step (1). Consider these paths one at a time. If one or more failure is present on a path, then augment the numerical label with the corresponding failure label(s). Otherwise, augment the numerical label with the label “N”.
(3) Repeat steps (1) and (2) until all states are exhausted.
(4) Under the assumption that only the actuator actions and sensor measurements are observable, hide every unobservable event in the system model by merging its input and output states.
(5) Ensure the liveliness of the resulting diagnoser by adding a fictitious self-looping event “STOP” at every deadlock state.

Notice that the system model and the corresponding diagnoser can be easily generated from the constructed component models with existing free software DESUMA. The live diagnoser for the aforementioned liquid transfer system is presented in Fig. 6. In this case, the event “STOP” should be interpreted as “the sensor reading remains unchanged for a long time.”

It is well established that fault diagnosis can be rigorously performed according to the observable traces in the diagnoser. In the liquid transfer example, three traces can be extracted from Fig. 6 and they are sketched in Fig. 7. Notice that every trace starts with an initial transition “*i cycles*”, which denotes the event sequence in any number of complete normal cycles ($i=0,1,2,\ldots$). A detailed analysis of the corresponding fault propagation sequences is given below:

- **Trace 1** (Tr_{01}): If the actuator action *ov3* is first performed at the initial state (which may be reached after completing any nonnegative number of normal cycles), the resulting liquid level should be *T1Hcon* in normal operation. Since the sensor reading stays unchanged at *T1Lcon* in this case, the action *ov3* must be attempted again and again according to the SFC given

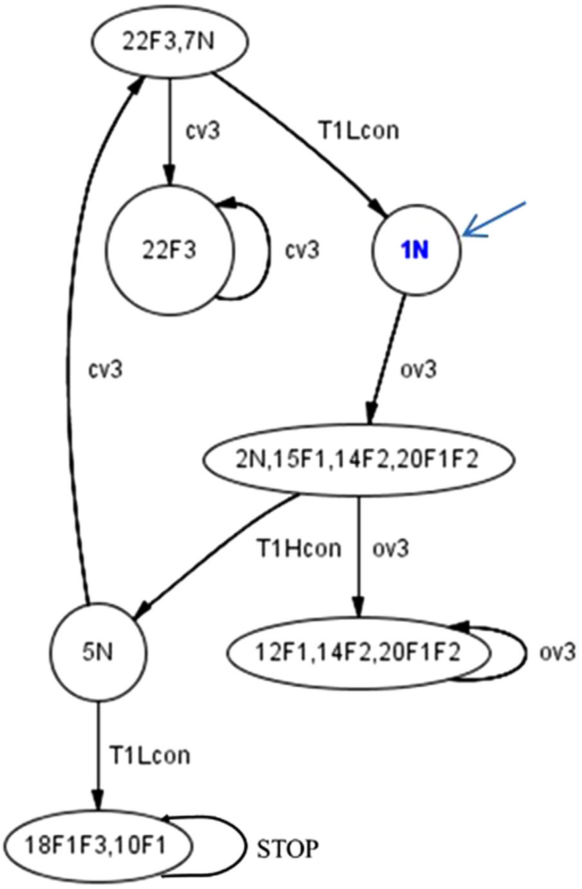

Fig. 6. Live diagnoser of the liquid transfer system.

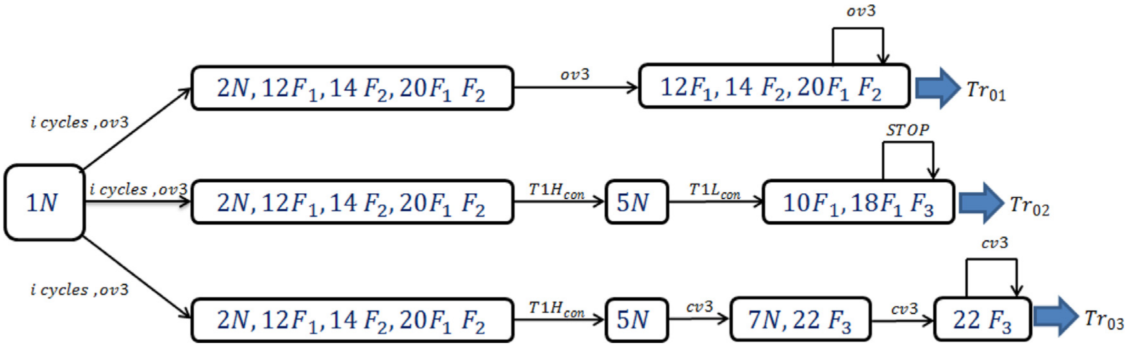

Fig. 7. Observable traces in the diagnoser of the liquid transfer system.

in Fig. 2. After observing this trace, one should be able to deduce that there are three possible fault origins, i.e., (1)F_1, (2)F_2 and (3)F_1F_2.

- **Trace 2** (Tr_{02}): After performing the actuator action $ov3$ at the initial state (which may be reached after completing any nonnegative number of normal cycles), the sensor reading shows *T1Hcon* (normal). However, the liquid level then quickly drops to *T1Lcon* (abnormal) before the actuator action to close V-3 ($cv3$) can be executed. Observation of this trace indicates that the fault origins could be (1)F_1or (2)F_1F_3.
- **Trace 3** (Tr_{03}): By performing the actuator action $ov3$ at the initial state (which may be reached after completing any nonnegative number of normal cycles), the sensor reading can be raised to *T1Hcon* (normal). However, the next actuator action $cv3$ fails to bring down the liquid level even after repeated attempts. There is only one explanation for these phenomena, i.e., V-3 sticks at the open position (F_3).

Since the implied fault origins are not unique whenever Tr_{01} or Tr_{02} is observed online, there is a need to further enhance diagnostic resolution. For this purpose, Yeh and Chang (2011) suggested to apply two complementary design options, i.e., installation of new sensors and implementation of extra operation steps. Since the latter alternative has never been systematically explored before, let us focus on only the related issues in the present example. Notice also that, due to the model building conventions adopted in this study, every observable trace in a live diagnoser ends at a self-looping event. It is thus assumed that the diagnostic tests can only be applied at the corresponding states.

4. Control specifications for diagnostic test

In the supervisory control paradigm (Ramadge and Wonham, 1987, 1989), the plant to be operated is represented with an automaton P and the supervisor S is viewed as a mapping from the language generated by P to the power set of E, i.e., $S: \mathcal{L}(P) \rightarrow 2^E$, where $\mathcal{L}(P)$ denotes the set of all traces generated from P and E is the event set of P. If $t \in \mathcal{L}(P)$, then $S(t)$ should be interpreted as the allowed actuator actions after executing trace t. A sketch of this conceptual framework can be found in Fig. 8. In the traditional applications, P can be assembled with component models in levels 2 to 4 under normal process conditions and its supervisor S is a model of the given SFC to be executed by a PLC.

Since multiple failure mechanisms are incorporated into automata in the present study and the diagnosability of the resulting system cannot always be guaranteed, it is therefore necessary to perform a distinct diagnostic test to differentiate the fault origins implied by each observable trace in the diagnoser. In this study, every test plan is essentially viewed as a unique SFC for online implementation in the corresponding scenario. In order to synthesize such a SFC, a set of control specifications for the corresponding supervisor must be stipulated in advance to eliminate the unacceptable traces in $\mathcal{L}(P)$. The general structures of these novel specifications are summarized below:

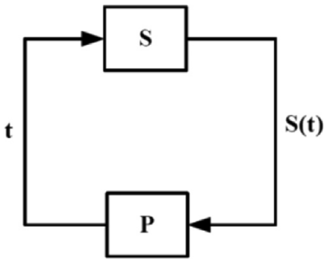

Fig. 8. Conceptual framework of a supervisory control system.

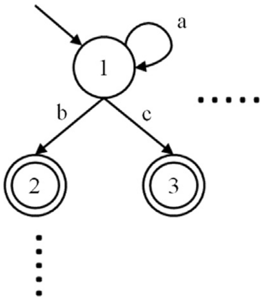

Fig. 9. Specification to facilitate reaching the operational target(s).

4.1. Operational target

The primary function of a diagnostic test is to create a unique observable pathway in the system automaton for each fault origin implied by an undiagnosable trace. The control specification to facilitate this operational goal can be characterized with the generalized automaton sketched in Fig. 9. The failures, actuator actions, online measurements and/or process configurations (which last for a sufficiently long period of time) may all be utilized as the self-looping events in this model, e.g., event a, while all possible sensor outputs should be adopted as the transition-causing events, e.g., event b and event c. Notice that this structure may be repeated for more than one layer, which can be determined on a trial-and-error basis. Notice also that the total number of layers (M) is bounded from above, i.e., $M \le F - 1$, where F is the number of fault origins implied by the undiagnosable trace under consideration.

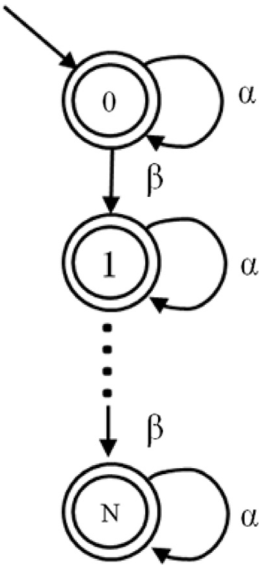

Fig. 10. Specification to facilitate identification of the optimal SFC.

4.2. Auxiliary constraint

The auxiliary constraint presented here is used mainly to facilitate identification of a feasible SFC for implementing the diagnostic test with the fewest steps. The generalized model structure of this constraint is given in Fig. 10. All sensor measurements and process configurations should be chosen as the self-looping events (α) in this automaton, while all actuator actions the transition-causing events (β). Notice that N is the number of assumed test steps and its lower limit is also identified with a trial-and-error approach.

5. Test-plan synthesis procedure

By using the proposed control specifications, a set of new supervisors can be constructed systematically for maximizing the diagnostic resolution of any given system. To every trace in diagnoser, the following test-plan synthesis procedure is applicable:

- Step 1: Set the initial state of every component in the last three levels by considering three possible scenarios:
  (a) If a component failure is confirmed by the observable trace under consideration, then set the corresponding failed state as the initial condition.
  (b) If a component failure can be neither confirmed nor rejected by observing the given trace, then set the normal state prior to this failure as the initial condition.
  (c) If it can be certain that the component is normal, the initial component condition should be the final state normally achieved by the actuator actions in the trace.
- Step 2: Identify all process configurations allowed in the test plan.
- Step 3: Modify and simplify the component models according to the results obtained in Steps 1 and 2.
- Step 4: Select the layer numbers (M and N) in the two control specifications, and then build the corresponding automata.
- Step 5: Produce the diagnostic supervisor by assembling the modified component models and the selected control specifications with parallel composition.
- Step 6: Repeat Steps 4 and 5 in a trial-and-error fashion until the best candidate is identified.

To illustrate this synthesis procedure, let us first consider trace 1 (Tr_{01}) in the diagnoser of the liquid transfer system (see Fig. 7). The implementation steps are summarized below

- Step 1:
  Since the three implied fault origins in this case are (1) F_1, (2) F_2 and (3) F_1F_2, the component failures *T1leak* (F_1) and *v3s_c* (F_2) can be neither confirmed nor rejected and thus the initial conditions of Tank and V-3 in the test plan should be set at T1L and V3C respectively. Since the other components are always normal, their starting states should be V1C, V2C and V4O, respectively.
- Step 2:
  Since the failure of V-3 cannot be ruled out, there is a need to provide an alternative means to fill the surge tank by opening V-1 and V-2. Thus, the allowed process configurations in this scenario should at least include those listed in Table 3. Note that all three fault origins are incorporated while, for the purpose of simplifying test steps, V-1 and V-2 are not permitted to be closed again after they are opened.

Table 3
Allowed configurations of the liquid transfer system for the test plan of Tr_{01}.

V-1	V-2	V-3	V-4	*T1leak*	Symbol
O	O	SC	O	N	*pc09*
O	O	SC	O	Y	*pc10*
O	O	O	O	Y	*pc11*

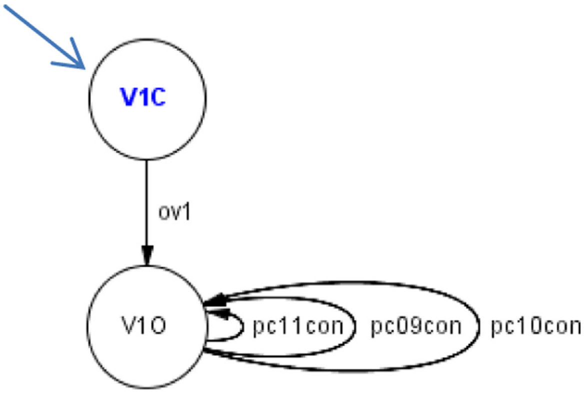

Fig. 11. The modified component model of V-1 for Trace 1 in the liquid transfer system.

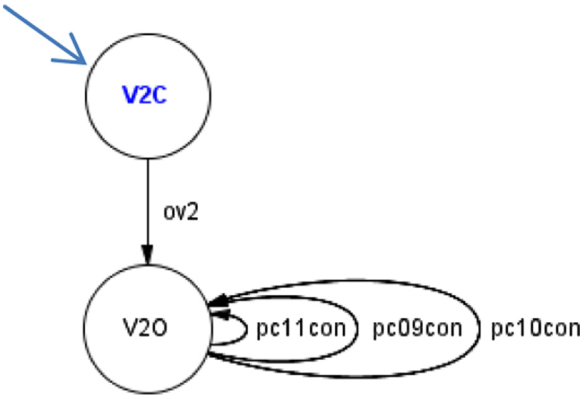

Fig. 12. The modified component model of V-2 for Trace 1 in the liquid transfer system.

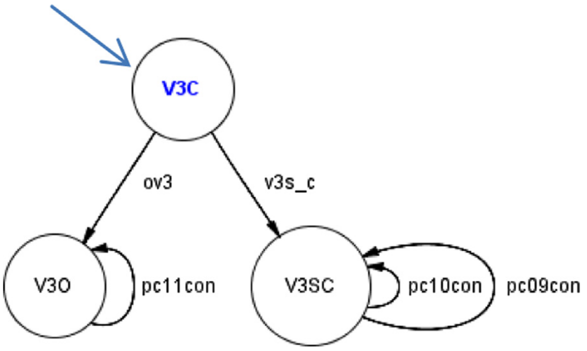

Fig. 13. The modified component model of V-3 for Trace 1 in the liquid transfer system.

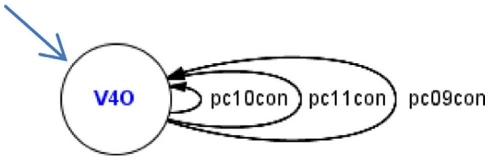

Fig. 14. The modified component model of V-4 for Trace 1 in the liquid transfer system.

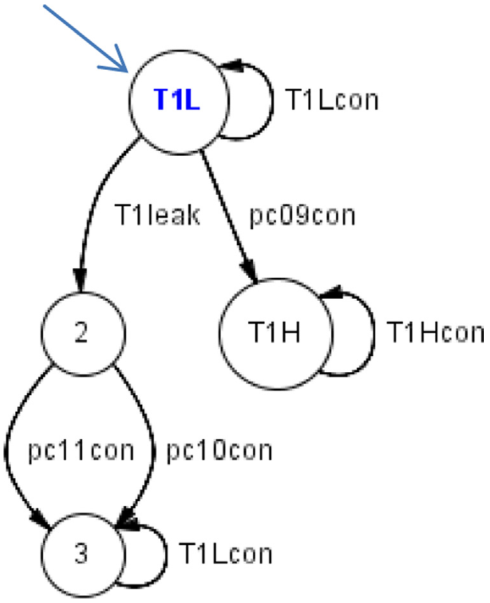

Fig. 15. The modified component model of tank for Trace 1 in the liquid transfer system.

- Step 3:
  For the liquid transfer system, the original component models are obtained without considering the diagnostic tests. These models should now be modified according to the initial component states and process configurations identified in Steps 1 and 2, and then simplified on the basis of specific process requirements (see Figs. 11–15). For reasons already mentioned in the previous step, the actuator actions to close V-1 and V-2 are not included in Figs. 11 and 12. Similarly, for model reduction purpose, the action *cv3* is also omitted in the automaton representing V-3 (Fig. 13). Since the state of V-4 is really irrelevant in the test plan, it is kept open in test plan to avoid considering pointless options (see Fig. 14). Finally, the same approach can be taken to produce the tank model in Fig. 15 by modifying and simplifying the automaton in Fig. 4.
- Steps 4–6:
  Since 3 possible fault origins are embedded in Tr_{01}, there should be at most 2 layers in the control specification for setting the operational target. The self-looping events in the corresponding automaton should be the actuator actions (*ov1*, *ov2* and *ov3*), the anticipated failures (*v3s_c* and *T1leak*), and the allowed process configurations (*pc09*–*pc11*), while the transition-causing events should be the possible sensor readings (*T1Hcon* and *T1Ccon*). As an example, a two-layer target model is provided in Fig. 16.

On the other hand, the self-looping events in the auxiliary constraint should be the allowed process configurations (*pc09*–*pc11*) and all possible sensor readings (*T1Hcon* and *T1Ccon*). The transition-causing events in this case should be the selected actuator actions (*ov1*, *ov2* and *ov3*) and implied failures (*v3s_c* and *T1leak*). As an example, a 3-layer (i.e., $N=3$) automaton is presented in Fig. 17.

By repeatedly composing the component models (Figs. 11–15) with the target model (Fig. 16) in parallel, it can be found that a two-layer specification is not effective for distinguishing all implied fault origins and the best performance can be achieved when $M=1$. The corresponding diagnostic supervisor is given in Fig. 18.

By repeatedly composing the diagnostic supervisor (Fig. 18) with the auxiliary constraint (Fig. 17) in parallel, it can be found that the smallest test plan can be identified at $N=2$ (Fig. 19) and the corresponding SFC is given in Fig. 20.

On the basis of the above discussion, let us summarize the identified test plan for trace Tr_{01} as follows: Trace Tr_{01} in Figs. 6 and 7 represents the scenario that the abnormal sensor reading *T1Lcon* persists after multiple attempts to open V-3 (*ov3*). Three possible fault origins, i.e., F_1 (*T1leak*), F_2 (*v3s_c*) and F_1F_2 (*T1leak* & *v3s_c*), can be deduced by observing this sequence. According to Figs. 19 and 20, the required operation steps at this

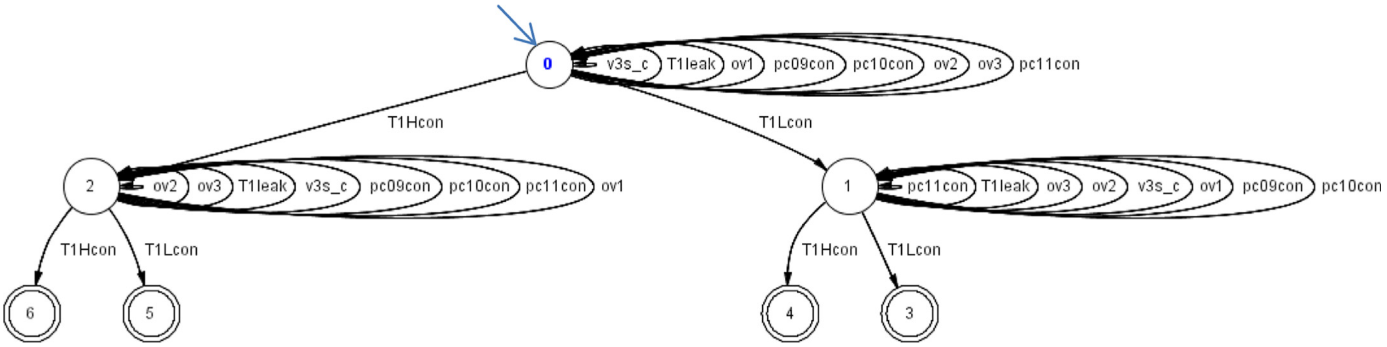

Fig. 16. Specification to achieve operational target for Tr_{01} in the liquid transfer system.

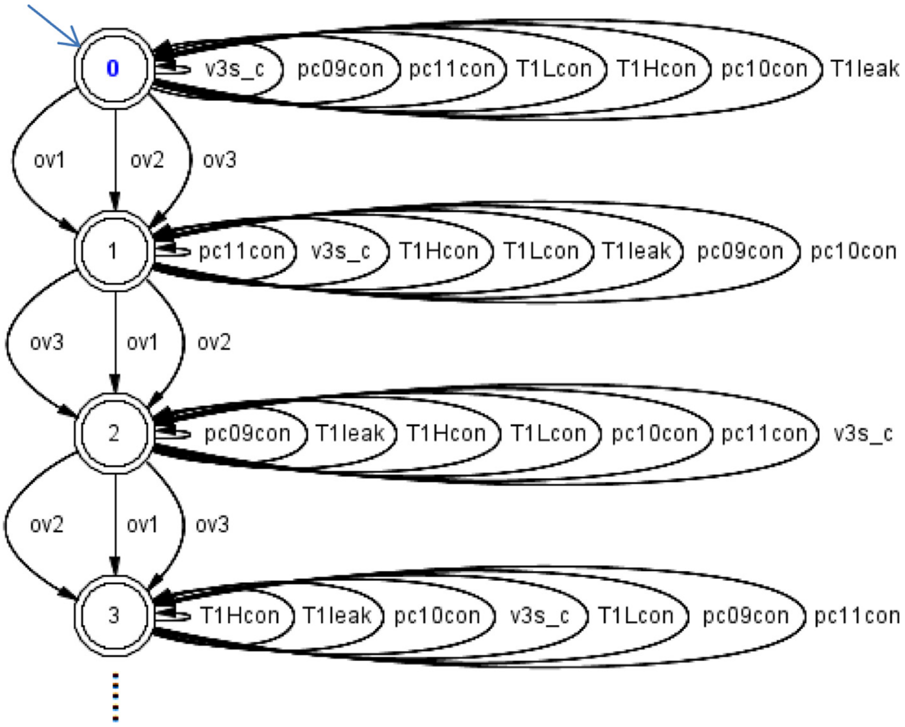

Fig. 17. Specification to identify SFC for Tr_{01} in the liquid transfer system.

point should be opening both V-1 and V-2 (i.e., *ov1* & *ov2*) to allow an alternative flow into the buffer tank. A resulting high liquid level indicates that the suspected leak (F_1) is not present and thus the correct fault origin should be F_2. Otherwise, the remaining two origins, i.e., F_1 and F_1F_2, should both be possible candidates but they are not distinguishable.

Finally, due to the assumption that the effect of leak dominates that of inlet flow, it can also be concluded that the two fault origins implied by Tr_{02}, i.e., F_1 (*T1leak*) and F_1F_3 (*T1leak* & *v3s_o*), cannot be made differentiable with any test plan.

6. Case studies

To verify the effectiveness of the proposed approach, a series of extensive case studies have been carried out and two of them are summarized below

6.1. A three-tank buffer system

Let us consider the P&ID in Fig. 21 and its normal operating procedure specified in Fig. 22. Notice that V-2 is a 3-way valve and the others are 2-way valves. The fluid in tank T-1 is directed to tank T-2 if V-2 is placed at the "+" position, while transported to T-3 if switched to the "−" position. All three tanks are equipped with level sensors. The one on T-1 is designed to detect three distinct states reflecting the low, intermediate and high liquid levels, i.e., *T1Lcon*, *T1Mcon* and *T1Hcon*, respectively, while that on T-2 (or T-3) is used to monitor only the states at low and high levels, i.e., *T2Lcon* (or *T3Lcom*) and *T2Hcon* (or *T3Hcon*). It is assumed that, initially, the liquid levels in all tanks are low, valves V-1 and V-3 are closed and V-2 is at the "−" position. In this example, let us consider the following seven failures:

i. F_1 (*v1s_c*): V-1 fails at the closed position;
ii. F_2 (*v1s_o*): V-1 fails at the open position;
iii. F_3 (*v2M-*): V-2 is mistakenly switched to the "−" position;
iv. F_4 (*v2M+*): V-2 is mistakenly switched to the "+" position;
v. F_5 (*v3s_c*): V-3 fails at the closed position;
vi. F_6 (*v3s_o*): V-3 fails at the open position;
vii. F_7 (*T2leak*): a leak develops in tank T-2.

The aforementioned model construction procedure has been followed to build the diagnoser, in which a total of 12 observable traces can be identified and, for the sake of brevity, only the undiagnosable ones are given in Fig. 23. Notice that the transition label "*i cycles*" also denotes the event sequence in any number of complete normal cycles and $i = 0, 1, 2, \ldots$. The proposed synthesis has been applied to the above three traces and the resulting test plans are summarized in the sequel:

- **Trace 7:** No effective test plan can be identified in this case. This is due to the fact that F_1 (*v1s_c*) is certain to occur. After observing the readings *T1Lcon*, *T2Lcon* and *T3Lcon*, there are really no ways to secure more fluid (by opening V-1) so as to render a change in the liquid level in T-2 for testing if failure F_6 (*v3s_o*) exists.
- **Trace 8:** After observing this trace in full, it is certain that failure *v2M-*(F_3) occurred at the time when the actions in step S_2 (see Fig. 22) were being executed during the current cycle. On the other hand, *v3s_o* (F_6) can be neither confirmed nor rejected and, if present, the failure should develop after step S_4 (in the previous cycle) and before the most recent S_1. The diagnostic test at this point (see Fig. 24) calls for three consecutive actions, i.e., (1) switching off the pump (*poff*), (2) switching V-2 to the "+" position (*tv2+*), and (3) switching on the pump (*pon*). If the sensor readings are *T1Lcon*, *T2Hcon* and *T3Hcon*, then V-3 should still be normal. If the sensor readings are *T1Lcon*, *T2Lcon* and *T3Hcon*, then V-3 must have already failed at the open position, i.e., *v3s_o* (F_6) is an existing failure.
- **Trace 9**: Two events in the current cycle can be confirmed with this observable trace, i.e., (1) *v1s_o* (F_2) occurred at a time after S_1 and before S_2, and (2) *v2M-*(F_3) occurred at the time when

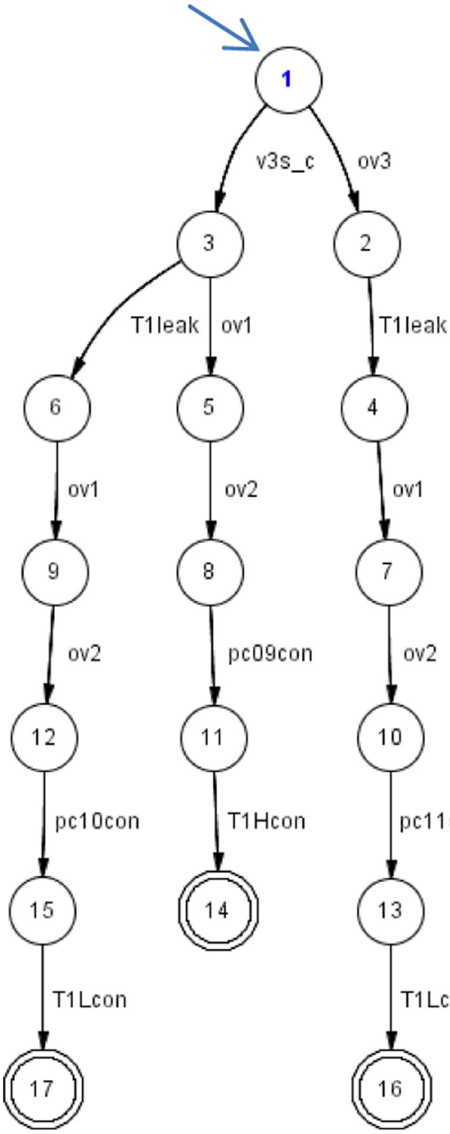

Fig. 18. Diagnostic supervisor for Tr_{01} in the liquid transfer system.

S_2 was being executed. However, the presence of a third failure $v3s\_o$ (F_6) is uncertain. The corresponding test actions are essentially the same as those for trace 8, i.e., *poff*, *tv2+* and *pon*, while the anticipated system responses differ slightly (see Fig. 25). If the sensor readings are *T1Hcon*, *T2Hcon* and *T3Hcon*, then V-3 should be regarded as normal. If the sensor readings are *T1Hcon*, *T2Lcon* and *T3Hcon*, then V-3 must have already failed at the open position, i.e., $v3s\_o$ (F_6) is present in the given system.

6.2. A beer filtration plant

The process flow diagram of beer filtration plant is shown in Fig. 26 (Lai et al., 2007; Chung and Lai, 2008). This system consists of two multi-micro-system filters (MMS-1 and MMS-2), two buffer tanks (T-1 and T-2), a supply and collection system for the cleanser (CIP), 17 double-disk piston valves (V-1–V-16 and V-18) and a gate valve (V-17). Notice that each valve can be switched to either ON or OFF position. When a valve is ON, the fluids entering the valve from vertical and horizontal pipelines will be mixed and then flow out via all outlet pipelines, whereas the fluids in vertical and horizontal pipelines flow separately when this valve is at the OFF

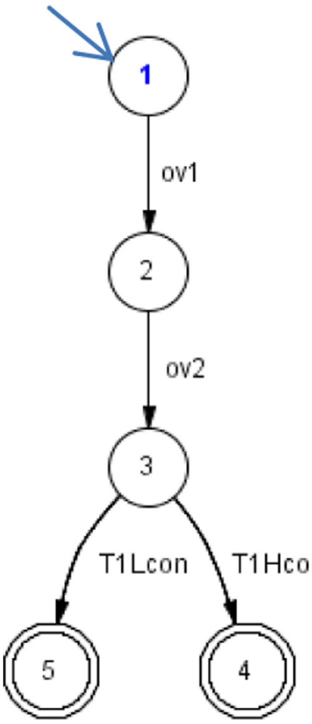

Fig. 19. Smallest diagnostic supervisor for Tr_{01} in the liquid transfer system.

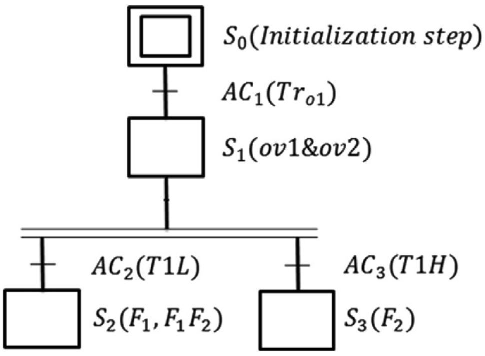

Fig. 20. Test plan for Tr_{01} in the liquid transfer system.

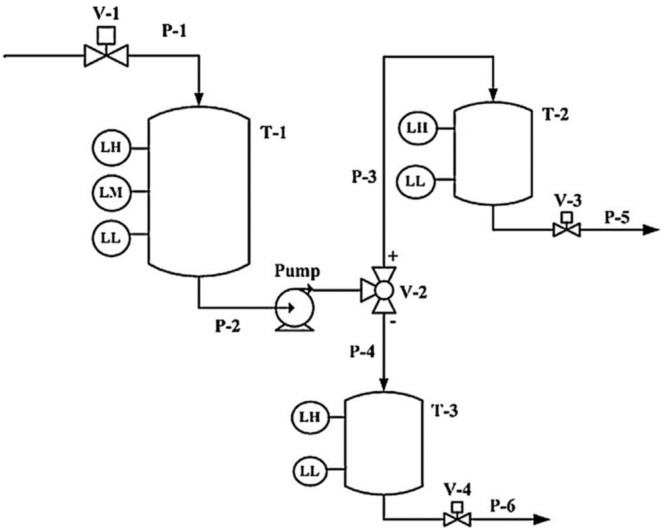

Fig. 21. P&ID of the three-tank buffer system.

position. There are four basic tasks to be performed in this plant, i.e., filling, filtration, bottling and cleaning. The purpose of filling is to transport fresh beer from a source tank to the buffer tank T-1 by opening either (1) V-2 and V-3 or (2) V-12 and V-13. In the filtration operation, beer is transferred from tank T-1 to T-2 via filter MMS-1 or MMS-2. Valves V-3 and V-4 should be both switched to the ON positions in the former case, while V-13 and V-14 must be ON in the latter. Clearly, the filtered beer in T-2 should be moved to the bottling station either by opening V-4 and V-5 or by opening V-14 and V-15. Finally, the tasks of cleaning processing units can also be considered as four different material-transfer operation**s** and they are listed below:

- Switch on V-8 and V-9 to clean T-1;
- Switch on V-7 and V-10 to clean T-2;
- Switch on V-1, V-6 and V-18 to clean MMS-1;
- Switch on V-11, V-16 and V-18 to clean MMS-2.

The normal operation steps and their activation conditions can be found in Fig. 27. Notice that, to enhance production efficiency, it is considered a good practice to clean equipment concurrently with one or more beer processing step. The initial beer level in each buffer tank is low and all 17 double-piston disk valves (V-1–V-16, V-18) are at the OFF positions when a cycle starts, while the gate valve (V-17) is always kept open during normal operation.

In this example, a total of five independent failures are considered:

i. F_1 (*v2s_c*): V-2 fails at the OFF (or CLOSE) position;
ii. F_2 (*v2s_o*): V-2 fails at the ON (or OPEN) position;
iii. F_3 (*v6s_c*): V-6 fails at the OFF (or CLOSE) position;
iv. F_4 (*v6s_o*): V-6 fails at the ON (or OPEN) position;
v. F_5 (*T1leak*): a leak develops in T-1.

The same model construction procedure has been followed to synthesize the diagnoser and its four undiagnosable traces are given in Fig. 28. Note that the transition label "*n cycles*" denotes the event sequence in more than one complete normal cycle, i.e., $n = 1, 2, 3, \ldots$. In other words, Trace 1 and Trace 2 can only be observed during the first cycle, while Trace 3 and Trace 4 should

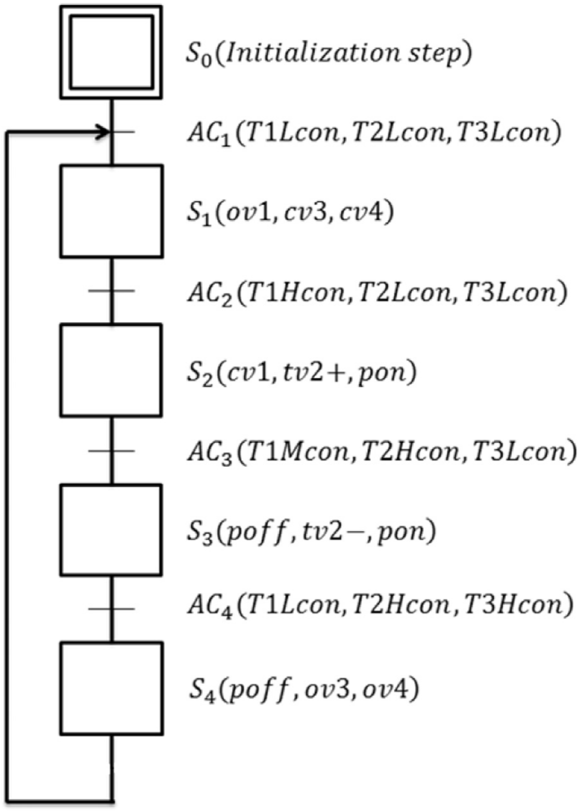
S_0(Initialization step)
$AC_1(T1Lcon, T2Lcon, T3Lcon)$
$S_1(ov1, cv3, cv4)$
$AC_2(T1Hcon, T2Lcon, T3Lcon)$
$S_2(cv1, tv2+, pon)$
$AC_3(T1Mcon, T2Hcon, T3Lcon)$
$S_3(poff, tv2-, pon)$
$AC_4(T1Lcon, T2Hcon, T3Hcon)$
$S_4(poff, ov3, ov4)$

Fig. 22. Normal SFC of the three-tank buffer system.

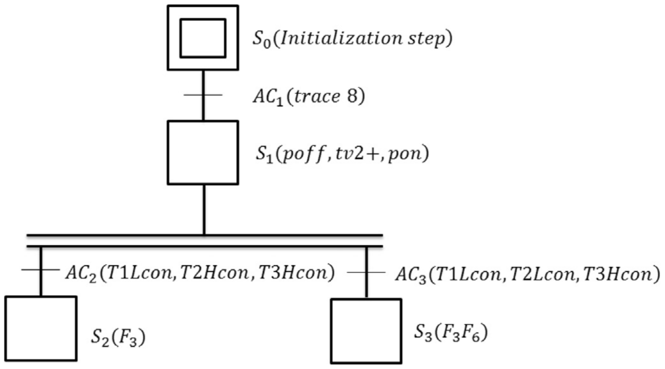
S_0(Initialization step)
AC_1(trace 8)
$S_1(poff, tv2+, pon)$
$AC_2(T1Lcon, T2Hcon, T3Hcon)$
$AC_3(T1Lcon, T2Lcon, T3Hcon)$
$S_2(F_3)$
$S_3(F_3F_6)$

Fig. 24. Test plan for Trace 8 in the three-tank buffer system.

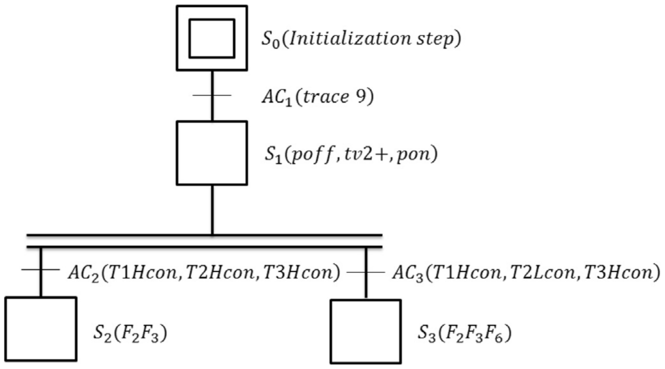
S_0(Initialization step)
AC_1(trace 9)
$S_1(poff, tv2+, pon)$
$AC_2(T1Hcon, T2Hcon, T3Hcon)$
$AC_3(T1Hcon, T2Lcon, T3Hcon)$
$S_2(F_2F_3)$
$S_3(F_2F_3F_6)$

Fig. 25. Test plan for Trace 9 in the three-tank buffer system.

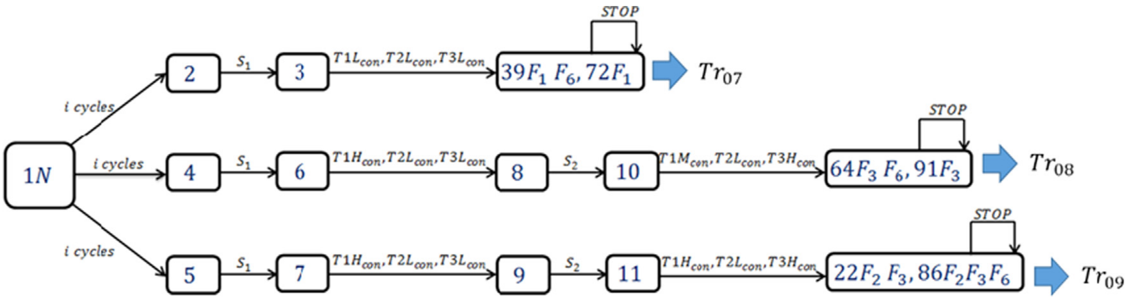
1N
i cycles
2
S_1
3
$T1L_{con}, T2L_{con}, T3L_{con}$
$39F_1\ F_6, 72F_1$
STOP
Tr_{07}
i cycles
4
S_1
6
$T1H_{con}, T2L_{con}, T3L_{con}$
8
S_2
10
$T1M_{con}, T2L_{con}, T3H_{con}$
$64F_3\ F_6, 91F_3$
STOP
Tr_{08}
i cycles
5
S_1
7
$T1H_{con}, T2L_{con}, T3L_{con}$
9
S_2
11
$T1H_{con}, T2L_{con}, T3H_{con}$
$22F_2\ F_3, 86F_2F_3F_6$
STOP
Tr_{09}

Fig. 23. Observable traces in the diagnoser of the three-tank buffer system.

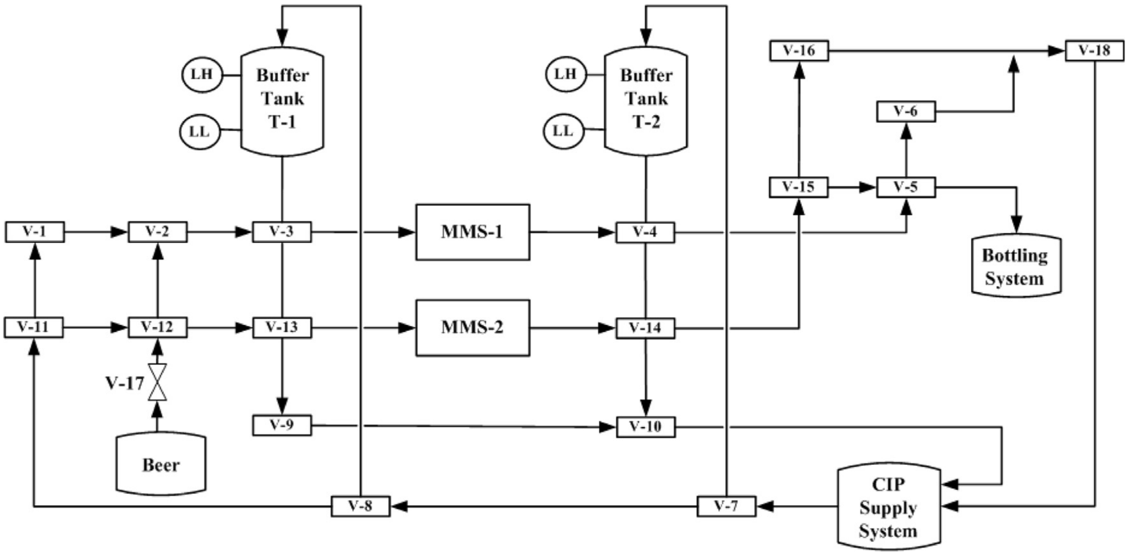

Fig. 26. Process flow diagram of beer filtration plant.

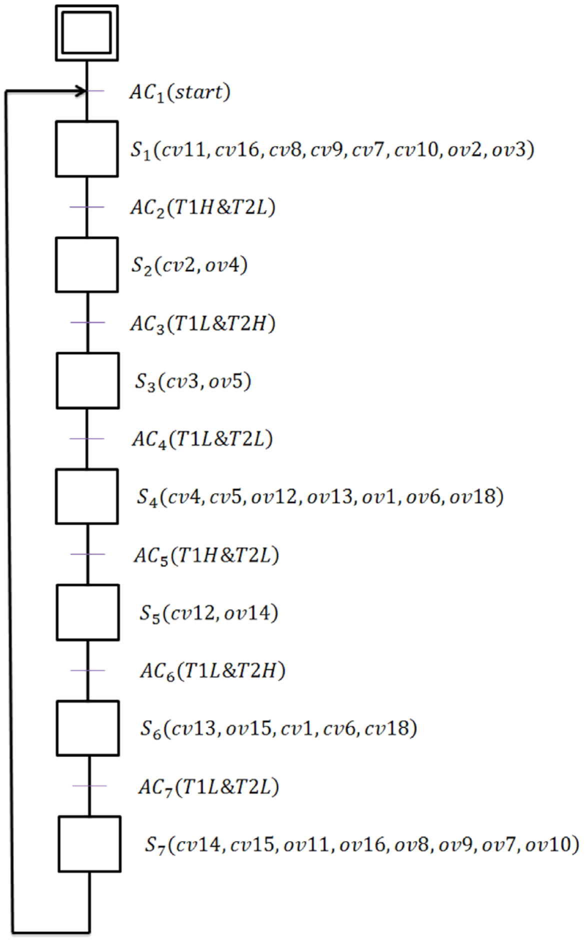
$AC_1(start)$
$S_1(cv11, cv16, cv8, cv9, cv7, cv10, ov2, ov3)$
$AC_2(T1H\&T2L)$
$S_2(cv2, ov4)$
$AC_3(T1L\&T2H)$
$S_3(cv3, ov5)$
$AC_4(T1L\&T2L)$
$S_4(cv4, cv5, ov12, ov13, ov1, ov6, ov18)$
$AC_5(T1H\&T2L)$
$S_5(cv12, ov14)$
$AC_6(T1L\&T2H)$
$S_6(cv13, ov15, cv1, cv6, cv18)$
$AC_7(T1L\&T2L)$
$S_7(cv14, cv15, ov11, ov16, ov8, ov9, ov7, ov10)$

Fig. 27. Normal SFC of beer filtration plant.

end in any of the later cycles. Note also that Trace 1 is basically a substring of Trace 3 and, thus, the fault origins in the former case are also included in the latter. Finally, notice that the same conclusions can be drawn from Trace 2 and Trace 4.

Since the given system is assembled with a large number of components (18 valves and 2 tanks), it is very difficult to evaluate all possible process configurations for the purpose of synthesizing a suitable emergency response procedure. To limit the search space and to avoid wasting beer, it is assumed that all diagnostic tests can be facilitated solely with cleanser and, thus, V-17 should be closed in every plan. Notice also that the test effects must be observed with the level sensors on T-1 and T-2. Although only two level readings on each tank are needed for implementing the normal operating procedure (see Fig. 27), a third is incorporated in the component models for T-1 and T-2 respectively, i.e., *T1Mcon* is added to characterize the abnormal condition that an intermediate level in T-1 has continued for some time, while *T2Mcon* is added for the corresponding scenario in T-2.

The proposed test-plan synthesis method has been applied to all four traces in diagnoser and the resulting SFCs can be found in Figs. 29–32. For the sake of brevity, only the first and third are explained below in detail:

- SFC for the test plan of Trace 1 (see Fig. 29):
  (A) Although the presence of *T1leak* (F_5) and the absence of *v2s_c* (F_1) and *v6s_o* (F_4) are verified by observing Trace 1 (AC_1) in full, the remaining failures, i.e., *v2s_o* (F_2) and/or *v6s_c* (F_3), can be neither confirmed nor rejected. Knowing that only V-1, V-6, V-12, V-13, V-17 and V-18 are ON or open at this point in normal operation, one can apply S_1 (*cv17* & *ov4*) to fill T-2 with cleanser via V-1 and V-4. It should also be noted that, without failure *v6s_c*, this flow is split into two at V-4 and one of them returns to the collection system via V-6 and V-18.
  (B) If the level sensor on T-2 detects *T2Mcon* (AC_2) after completing S_1, then *v6s_c* (F_3) can be ruled out but the status of *v2s_o* (F_2) is still uncertain. The subsequent test step S_2 calls for *cv1* and then *ov10* to disconnect the inlet flow and also allow the cleanser in T-2 to be drained into the collection system via V-4, V-14 and V-10. As soon as T-2 is emptied or *T2Lcon* (AC_4) can be observed, the next step S_4(*cv10* & *ov11*) should be performed to fill T-2 via V-11, V-12, V-2 and V-4.
  (C) If the condition *T2Hcon* (AC_3**)** is revealed with the level sensor on T-2 after executing all actions in S_1, then the presence of *v6s_c* (F_3) can be verified but the status of *v2s_o* (F_2) is still uncertain. Note that the subsequent event sequence for confirming/rejecting failure F_2 (see the events in S_3, AC_5 and S_5) is essentially the same as that described

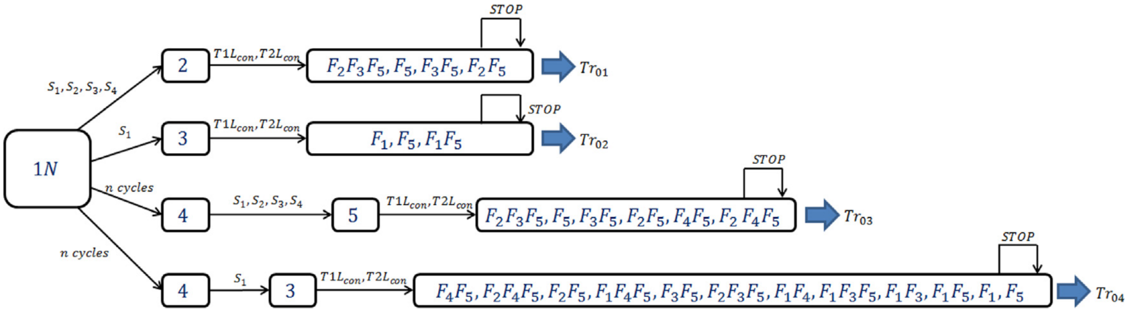

Fig. 28. Observable traces in the diagnoser of beer filtration plant.

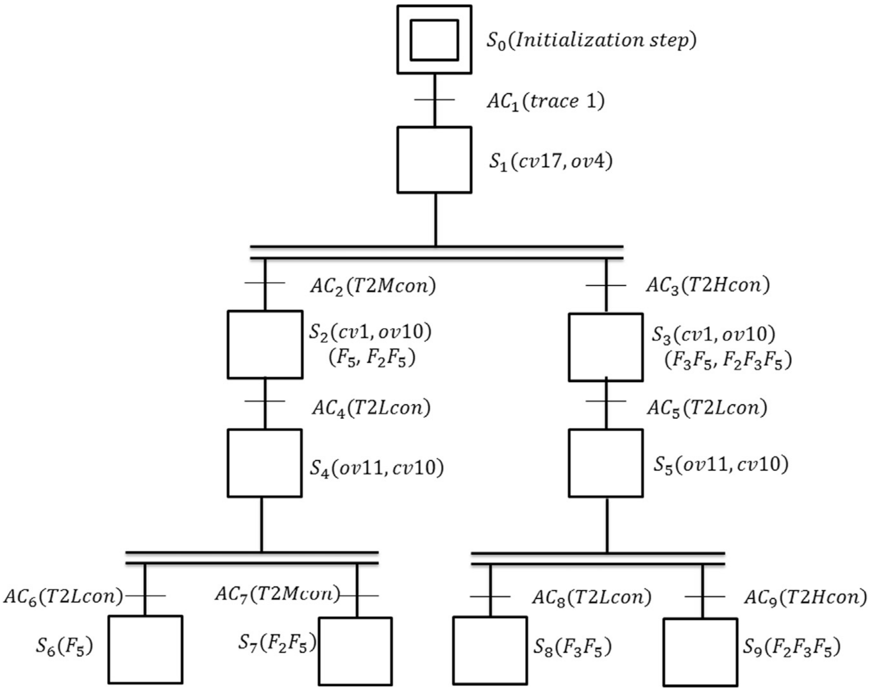

Fig. 29. Test plan for Trace 1 in beer filtration plant.

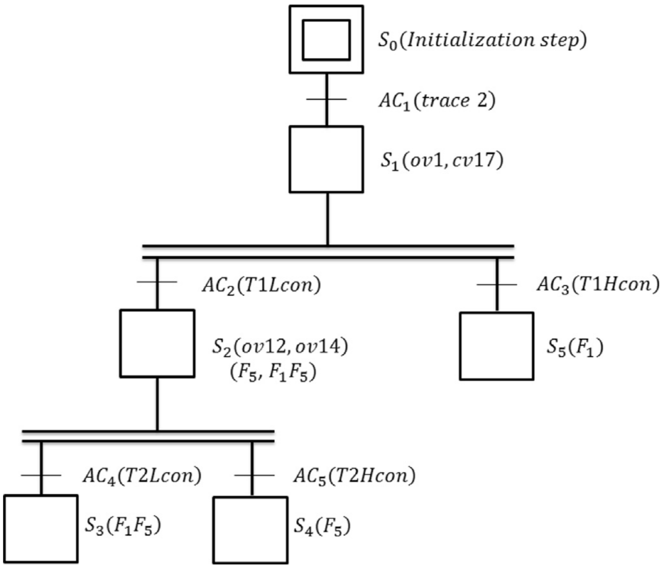

Fig. 30. Test plan for Trace 2 in beer filtration plant.

in (B), i.e., *cv1*, *ov10*, *T2Lcon*, *cv10* and *ov11* in S_2, AC_4 and S_4.

(D) There should be two alternative outcomes after implementing S_4. If the sensor reading on T-2 is *T2Lcon* (AC_6), then *v2s_o* (F_2) can be disregarded and the corresponding fault origin is simply *T1leak* (F_5). If *T2Mcon* (AC_7) is observed, then F_2 can be confirmed and the fault origin is F_2F_5 (*v2s_o* & *T1leak*).

(E) The two scenarios resulting from S_5 are similar to those described in (D). If the sensor reading on T-2 is *T2Lcon* (AC_8), then *v2s_o* (F_2) can be ruled out and the corresponding fault origin is F_3F_5. If the reading shows *T2Hcon* (AC_9), then F_2 can be confirmed and the corresponding fault origin should consist of three coexisting failures, i.e., $F_2F_3F_5$ (*v2s_o* & *v6s_c* & *T1leak*).

- SFC for the test plan of Trace 3 (see Fig. 31):

(A) Although the presence of *T1leak* (F_5) and the absence of *v2s_c* (F_1) are confirmed by observing trace 3 (AC_1), one still cannot be certain (a) whether V-2 is normal or fails at the ON position, i.e., *v2s_o* (F_2), and (b) whether V-6 is normal or fails at the ON or OFF positions, i.e., *v6s_c* (F_3) or *v6s_o* (F_4). Knowing that only V-1, V-6, V-12, V-13, V-17

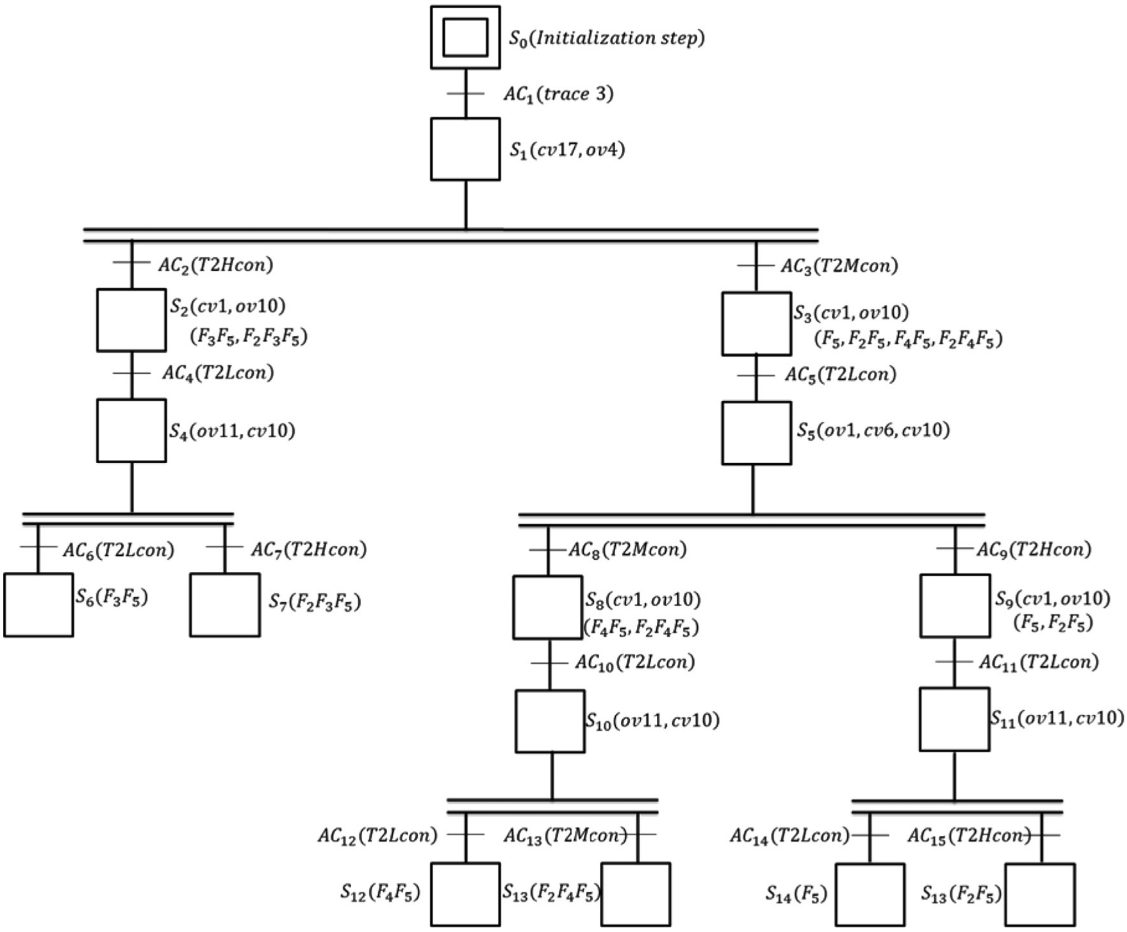

Fig. 31. Test plan for Trace 3 in beer filtration plant.

and V-18 are ON or open at this juncture in normal operation, one can try to implement S_1 (*cv17* & *ov4*) to fill T-2 with cleanser via V-1 and V-4. It should also be noted that, without failure *v6s_c*, this flow is split into two at V-4 and one of them should return to the collection system via V-6 and V-18.

(B) If the sensor reading on T-2 indicates *T2Hcon* (AC_2) after completing S_1, then *v6s_c* (F_3) can be confirmed but it is still uncertain if *v2s_o* (F_2) is present. The following step S_2 calls for *cv1* and then *ov10* to disconnect the inlet flow of T-2 and also allow cleanser to be drained into the collection system via V-4, V-14 and V-10. After T-2 is emptied or *T2Lcon* (AC_4) is observed, S_4 (*cv10* & *ov11*) should be performed to fill T-2 via V-11, V-12, V-2 and V-4.

(C) If the level sensor on T-2 shows *T2Mcon* (AC_3) after executing S_1, then *v6s_c* (F_3) can be rejected. However, one still cannot determine (a) whether V-2 is normal or fails at the ON position, i.e., *v2s_o* (F_2), and (b) whether V-6 is normal or fails at the ON position, i.e., *v6s_o* (F_4). The next step S_3 is essentially the same as S_2, i.e., *cv1* & *ov10*, which is adopted primarily for the purpose of draining T-2. As soon as the subsequent condition *T2Lcon* (AC_4) is detected with the level sensor on T-2, step S_5 (*ov1* & *cv6* & *cv10*) should be performed to fill T-2 via V-1 and V-4. Note also that, if the failure *v6s_o* (F_4) is present, an additional flow may be branched out at V-4 to the collection system via V-6 and V-18.

(D) Only two alternative outcomes can be expected after implementing S_4. If the sensor reading on T-2 is *T2Lcon* (AC_6), then *v2s_o* (F_2) can be disregarded and the corresponding fault origin is F_3F_5 (*v6s_c* & *T1leak*). On the other hand, if *T2Hcon* (AC_7) is observed, then F_2 can be confirmed and the fault origin is $F_2F_3F_5$ (*v2s_o* & *v6s_c* & *T1leak*).

(E) If the level sensor on T-2 detects *T2Mcon* (AC_8) after completing S_5, then *v6s_o* (F_4) can be confirmed but it is still uncertain if *v2s_o* (F_2) is present. The next test step S_8 again calls for *cv1* and then *ov10* to empty T-2 and transfer its content to the collection system via V-4, V-14 and V-10. After observing the subsequent condition *T2Lcon* (AC_{10}), S_{10}(*cv10* & *ov11*) should be performed to fill T-2 via V-11, V-12, V-2 and V-4.

(F) If condition *T2Hcon* (AC_9) can be observed after executing S_5, then the presence of *v6s_o* (F_4) can be rejected but the status of *v2s_o* (F_2) is still uncertain. The required event sequence for confirming/rejecting F_2 (see S_9, AC_{11} and S_{11}) is essentially the same as that described in (E), i.e., *cv1*, *ov10*, *T2Lcon*, *cv10* and *ov11* in S_8, AC_{10} and S_{10}.

(G) There should be two possible scenarios after implementing S_{10}. If the sensor reading on T-2 is *T2Lcon* (AC_{12}), then *v2s_o* (F_2) can be rejected and the corresponding fault origin is F_4F_5 (*v6s_o* & *T1leak*). However, if *T2Mcon* (AC_{13}) is observed, then F_2 should be included and the corresponding fault origin is only $F_2F_4F_5$ (*v2s_o* & *v6s_o* & *T1leak*).

(H) Only two possible outcomes can be produced by implementing S_{11}. If the sensor reading is *T2Lcon* (AC_{14}), then *v2s_o* (F_2) should be rejected and the corresponding fault origin is simply F_5 (*T1leak*). On the other hand, if *T2Hcon* (AC_{15}) is observed, then F_2 should be included and the corresponding fault origin is F_2F_5(*v2s_o* & *T1leak*).

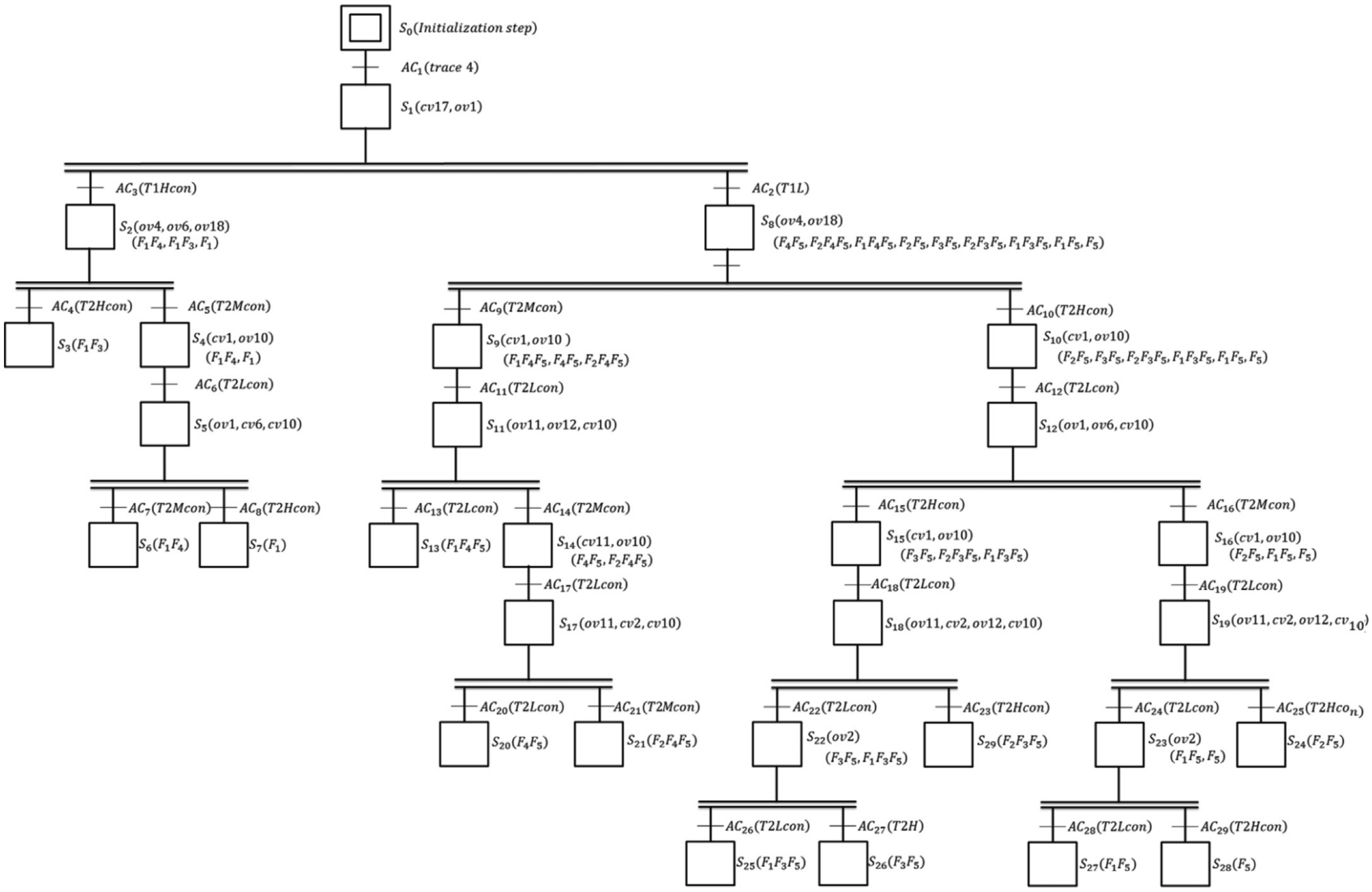

Fig. 32. Test plan for Trace 4 in beer filtration plant.

7. Conclusions and future works

A standardized methodology has been proposed in this work to systematically construct untimed automata for modeling sequential material- and/or energy-transfer operations in a batch plant, and to produce the corresponding diagnoser accordingly. A generic synthesis procedure has also been developed for creating the test plans of all undiagnosable traces in a diagnoser. Specifically, this novel procedure is used to

- set the initial components states in the test procedure,
- enumerate all allowed process configurations,
- modify all component models to address diagnostic needs,
- conjecture control specifications and represent them with automata, and
- generate the optimal SFCs for implementing the test plans.

It should be noted that, although the feasibility of the proposed approach has been successfully verified with several examples in this work, additional model features may be incorporated in the future to improve its effectiveness in more realistic environment. In particular, the timed automata may be utilized to model operation times of the test steps so as to further enhance diagnostic resolution of the test plans by making use of the online clocks.

References

Baroni, P., Lamperti, G., Pogliano, P., Zanella, M., 1999. Diagnosis of large active systems. Artif. Intell. 110 (1), 135–183.

Baroni, P., Lamperti, G., Pogliano, P., Zanella, M., 2000. Diagnosis of a class of distributed discrete-event systems. IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 30 (6), 731–752.

Benveniste, A., Fabre, E., Haar, S., Jard, C., 2003. Diagnosis of asynchronous discrete-event systems: a net unfolding approach. IEEE Trans. Autom. Control 48 (5), 714–727.

Cassandras, C.G., Lafortune, S., 1999. Introduction to Discrete Event Systems. Kluwer Academic Publisher, Boston.

Chen, Y.C., Yeh, M.L., Hong, C.L., Chang, C.T., 2010. Petri-net based approach to configure online fault diagnosis systems for batch processes. Ind. Eng. Chem. Res. 49 (9), 4249–4268.

Chung, S.L., Lai, Y.H., 2008. Process control of brewery plants. J. Chin. Inst. Eng. 31 (1), 127–140.

Debouk, R., Lafortune, S., Teneketzis, D., 2000. Coordinated decentralized protocols for failure diagnosis of discrete event systems. Discret. Event Dyn. Syst. Theory Appl. 10 (1–2), 33–86.

Kourti, T., Macgregor, J.F., 1995. Process analysis, monitoring and diagnosis, using multivariate projection methods. Chemom. Intell. Lab. Syst. 28 (1), 3–21.

Kourti, T., Nomikos, P., Macgregor, J.F., 1995. Analysis monitoring and fault-diagnosis of batch processes using multiblock and multiway PLS. J. Process Control 5 (4), 277–284.

Lai, J.W., Chang, C.T., Hwang, S.H., 2007. Petri-net based binary integer programs for automatic synthesis of batch operating procedures. Ind. Eng. Chem. Res. 46 (9), 2797–2813.

Lee, J.M., Yoo, C.K., Lee, I.B., 2004. Fault detection of batch processes using multiway kernel principal component analysis. Comput. Chem. Eng. 28 (9), 1837–1847.

Nomikos, P., MacGregor, J.F., 1994. Monitoring batch processes using multiway principal component analysis. AIChE J. 40 (8), 1361–1375.

Nomikos, P., MacGregor, J.F., 1995. Multivariate SPC charts for monitoring batch processes. Technometrics 37 (1), 41–59.

Pierri, F., Paviglianiti, G., Caccavale, F., Mattei, M., 2008. Observer-based sensor fault detection and isolation for chemical batch reactors. Eng. Appl. Artif. Intell. 21 (8), 1204–1206.

Qiu, W.B., Kumar, R., 2006. Decentralized failure diagnosis of discreteevent system. IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 36 (3), 384–395.

Ramadge, P.J., Wonham, W.M., 1987. Supervisory control of a class of discrete event processes. SIAM J. Control Optim. 25, 206–230.

Ramadge, P.J., Wonham, W.M., 1989. The control of discrete event systems. Proc. IEEE 77, 81–98.

Ruiz, D., Canton, J., Nougues, J.M., Espuna, A., Puigjaner, L., 2001a. On-line fault diagnosis system support for reactive scheduling in multipurpose batch chemical plants. Comput. Chem. Eng. 25 (4–6), 829–837.

Ruiz, D., Nougues, J.M., Calderon, Z., Espuna, A., Puigjaner, L., 2001b. Neural network based framework for fault diagnosis in batch chemical plants. Comput. Chem. Eng. 24 (2–7), 777–784.

Sampath, M., Lafortune, S., Teneketzis, D., 1998. Active diagnosis of discrete-event systems. IEEE Trans. Autom. Control 43 (7), 908–929.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., Teneketzis, D., 1995. Diagnosability of discrete-event systems. IEEE Trans. Autom. Control 40 (9), 1555–1575.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., Teneketzis, D.C., 1996. Failure diagnosis using discrete-event models. IEEE Trans. Control Syst. Technol. 4 (2), 105–124.

Undey, C., Ertunc, S., Cinar, A., 2003. Online batch fed-batch process performance monitoring, quality prediction, and variable contribution analysis for diagnosis. Ind. Eng. Chem. Res. 42 (20), 4645–4658.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., Kavuri, S.N., 2003a. A review of process fault detection and diagnosis, Part I: quantitative model based methods. Comput. Chem. Eng. 27 (3), 293–311.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., 2003b. A review of process fault detection and diagnosis, Part II: qualitative model and search strategies. Comput. Chem. Eng. 27 (3), 313–326.

Venkatasubranmanian, V., Rengaswamy, R., Kavuri, S.N., Yin, K., 2003c. A review of process fault detection and diagnosis, Part III: process history based methods. Comput. Chem. Eng. 27 (3), 327–346.

Yeh, M.L., Chang, C.T., 2011. An automaton-based approach to evaluate and improve online diagnosis schemes for multi-failure scenarios in batch chemical processes. Chem. Eng. Res. Des. 89, 2652–2666.

Yeh, M.L., Chang, C.T., 2012. An automata-based approach to synthesize untimed operating procedures in batch chemical processes. Korean J. Chem. Eng. 29, 583–594.

Zad, S.H., Kwong, R.H., Wonham, W.M., 2003. Fault diagnosis in discrete-event systems: framework and model reduction. IEEE Trans. Autom. Control 48 (7), 1199–1204.