Contents lists available at ScienceDirect

Chemical Engineering Research and Design

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

# Systematic generation of cyclic operating procedures based on timed automata

*Jeh-Hsuan Li*[a], *Chuei-Tin Chang*[a,*], *Da Jiang*[b]

[a] *Department of Chemical Engineering, National Cheng Kung University, Tainan, 70101, Taiwan, ROC*
[b] *Key Laboratory of Advanced Control and Optimization for Chemical Processes (East China University of Science and Technology), Ministry of Education, Shanghai 200237, PR China*

## ABSTRACT

Manual synthesis of cyclic operating procedure in a realistic system is widely regarded as a difficult task since it is both time-consuming and error-prone. It is thus desirable to develop a systematic approach to automatically generate the optimal schedule of operation steps so as to achieve one or more specific production goal. The timed automata are utilized in the present work for such a purpose. In particular, all components in a given system and the corresponding control specifications are characterized with automata according to the proposed modeling rules. By using parallel composition, a system automaton can be produced with these models and the most appropriate operation path can then be identified accordingly. For any practical application, a sequential function chart and the corresponding Gantt chart can also be easily extracted from this path. Three examples are presented in this paper to demonstrate the feasibility of the proposed approach.

*Keywords:* Timed automata; Modeling method; Cyclic operating procedure

## 1. Introduction

The operating procedure of a batch chemical process should be synthesized on the basis of the initial system condition(s) and also the ultimate operational goal(s). Its detailed steps are usually represented with a sequential function chart (SFC). Traditionally, the SFCs have been produced with an ad hoc manual approach which often becomes unmanageable as the process complexity increases. To overcome the difficulties caused by combinatorial explosion, there have been many published studies on systematic procedure synthesis. The original problem formulation was first proposed by Rivas and Rudd (1974), and extensive works concerning the design and verification of procedural controllers were then carried out in the later years. The related issues were basically addressed with various modeling/reasoning tools, e.g., the mathematical programming models (Crooks and Macchietto, 1992; Li et al., 1997), the symbolic model verifiers (Yang et al., 2001), the AI-based strategies (Foulkes et al., 1988), and other qualitative models such as Petri nets (Lai et al., 2007; Lee et al., 2011) and the untimed automata (Yeh and Chang, 2012a,b).

Although interesting results were presented in the aforementioned papers, the available methods are still not mature enough for realistic cyclic operations. In particular, every existing method was developed on the basis of a single pre-determined initial condition for batch operation. This approach may not be feasible in the present application if the given system could start at a different (and probably abnormal) state. In addition, the elapsed time of each operation step has not been considered rigorously in the previous work either. To characterize the periodic operating procedure unambiguously, it is desired to produce not only a SFC but also the corresponding Gantt chart to stipulate the time schedule for implementing the operation steps.

To address the aforementioned issues, an improved modeling strategy is developed in this work to build timed automata for characterizing components and specifications in all possible scenarios. A versatile system model can then be

[*] Corresponding author. Tel.: +886 6 275 7575x62663; fax: +886 6 234 4496.
E-mail addresses: ctchang@mail.ncku.edu.tw, chueitinchang@msn.com (C.-T. Chang).

Received 18 April 2013; Received in revised form 25 June 2013; Accepted 29 June 2013
0263-8762/$ – see front matter © 2013 The Institution of Chemical Engineers. Published by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cherd.2013.06.032

synthesized accordingly by applying the standard operation of parallel composition. The best operation path embedded in this model is identified with an existing software, i.e., UPPAAL (Behrmann et al., 2006), and the corresponding operating procedure can also be easily generated. Three examples are presented at the end of this paper to facilitate clear explanation of the proposed method.

The remaining paper is organized as follows. The general framework of automata-based procedure-generation strategy is first described in the following section. A unified hierarchical structure of the batch processes is then presented in Section 3. The systematic methods for constructing timed automata that model the components and also the control specifications are outlined in the next two sections. The desired cyclic operating steps can be identified by combining these automata according to the rules of parallel composition. This procedure-synthesis approach is illustrated with a simple example in Section 6. To demonstrate the effectiveness of the proposed strategy, additional case studies have also been carried out and two of them are presented in Section 7. Finally, the concluding comments are given in the last section.

## 2. Automata-based procedure-generation strategy

A timed automaton is a finite-state machine equipped with one or more clock (Alur and Dill, 1994). All clocks progress synchronously, and every one of them is described with a dense-time model in which the clock variable assumes a real positive value. To facilitate clear description of the proposed method, a brief summary of the automaton structure is given below. In particular, a timed automaton can be regarded as a six-tuple:

$$TA = (L, \ell_0, C, A, I, E) \quad (1)$$

where, $L$ is a set of locations; $\ell_0 \in L$ is the initial location; $C$ denotes the set of clocks; $A$ is a set of actions. In addition, $I : L \to B(C)$ denotes a function $I(l) = b(c)$ which assigns invariants to locations. Note that $B(C)$ is the set of conjunctions over simple conditions of the form:

$$\{x \oplus c\} \text{ or } \{x - y \oplus c\} \quad (2)$$

where, $x, y \in C$, $c \in \mathbb{N}$ and $\oplus \in \{<, \leq, =, \geq, >\}$. Finally, the set $E \subseteq L \times A \times B(C) \times 2^C \times L$ contains all edges in the automaton. Each edge represents a transition process from one location to another, which is enabled by an action in the set $A$, constrained by a guard in the set $B(C)$ and timed according to a collection of clocks which belongs to the power set of $C$, i.e., $2^C$.

The default verification tool in UPPAAL is used in the study to search for the best operation path within the real-time system (Pettersson, 1999). UPPAAL is an integrated tool environment for modeling, validation and verification of real-time discrete-event systems (Bengtsson and Yi, 2004; Kim et al., 2006). Although other alternatives, e.g., KRONOS (Bozga et al., 1998) and RED (Wang, 2001), are available, this software is adopted simply for its effectiveness and user-friendliness. More specifically, the optimal operating procedure is produced in four distinct steps in the present study:

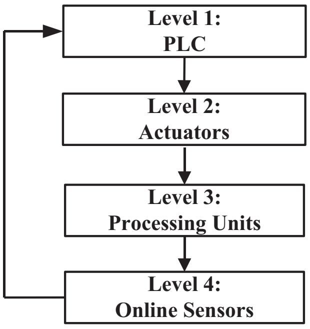


**Fig. 1 – Hierarchical structure of a batch process.**

(1) Build the automaton models of all components in the uncontrolled plant;
(2) Construct automata to represent the control specifications in all possible scenarios;
(3) Combine all automata created in the above two steps with parallel composition;
(4) Execute suitable property verification function in UPPAAL so as to locate the best operation pathway.

## 3. Hierarchical structure of batch processes

The hardware items in any batch process can all be depicted in a process flow diagram (PFD). They are treated in this study as components of the given system and classified into a 4-level hierarchy (see Fig. 1). The top-level component is usually a programmable logic controller (PLC) used for implementing a set of pre-determined actions to alter the actuator states in the second level. More than one actuator, e.g., solenoid valves, pumps, compressors, and switches, etc., may be used for adjusting the material and/or energy flow patterns in the given system. Every processing unit in PFD, such as the heat exchanger, separator, reactor and storage tank, is considered as a level-3 component, while every on-line sensor is treated as a component in level 4. The PFD of an uncontrolled batch process, i.e., levels 2 to 4, is assumed to be given in this work, while the SFC and the corresponding Gantt chart are not available. Let us use the simple liquid heating system given in Fig. 2

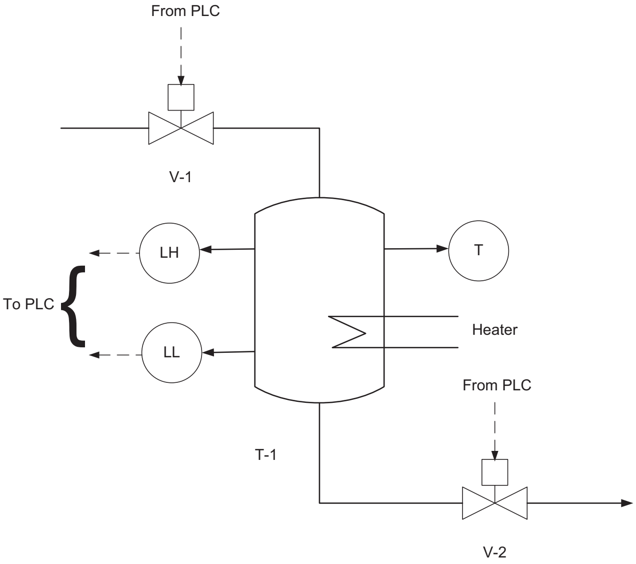


**Fig. 2 – PFD of a liquid heating system (Example 1).**

**Table 1 – Classification of components (Example 1).**

| Levels | Components |
|---|---|
| 1 | PLC |
| 2 | V-1, V-2, heater |
| 3 | T-1 |
| 4 | level and temperature sensors |

(which is referred to as Example 1 in this paper) to illustrate the aforementioned hierarchy. Specifically, the components in this system can be classified according to Table 1. Our goal is to systematically generate a cyclic operating procedure so as to satisfy some prescribed control specifications.

## 4. Construction of component models

The model-building principles for the components in an uncontrolled plant can be illustrated with Example 1. It is assumed that the initial liquid level in T-1 is low (LL), while the corresponding temperature is also low (TL). Additionally, let us assume that, before the operation starts, the inlet valve V-1 is closed, the outlet valve V-2 is open, and the heater is off. Following is a detailed description of the component models:

- **Level 2**: The automaton model of valve V-1 is shown in Fig. 3(a). The locations ‘Off’ and ‘On’, respectively denote the closed and opened valve positions. The edges ‘v1O?’ and ‘v1C?’, respectively represent the close-to-open and open-to-close transition processes and a binary variable v1 is adopted to facilitate their characterization. The component models of outlet valve and heater are similar to that of V-1, and they are given in Fig. 3(b) and (c).
- **Level 3**: The tank is the only level-3 component considered in this example. Two automata, Fig. 3(d) and (e), are used to respectively describe the liquid level and temperature in T-1. In Fig. 3(d), the edges ‘level_high!’ and ‘level_low!’ denote the level changing processes and $x$ is the corresponding clock variable. The prerequisites of the low-to-high process are set to be: (1) the inlet valve is open ($v1 == 1$), (2) the outlet valve is closed ($v2 == 0$), (3) the heater is off ($h == 0$), and (4) the elapsed time is no less than 3 ($x >= 3$). On the other hand, the prerequisites of the high-to-low process are chosen to be: (1) the inlet valve is closed ($v1 == 0$), (2) the outlet valve is open ($v2 == 1$), (3) the heater is off ($h == 0$), and (4) the required state transition time is no less than 1 ($x >= 1$). In addition, another binary variable $L$ is used to characterize the liquid level, i.e., its value is 1 when level is high (LH) and 0 if otherwise (LL). After completing each level changing process, the clock variable $x$ is required to be reset to 0. On the other hand, the edges ‘temp_high!’ and ‘temp_low!’ in Fig. 3(e) denote the temperature changing processes and $y$ is the corresponding clock variable. An extra binary variable $T$ is also used to describe temperature, i.e., its value is 1 when temperature is high (TH) and 0 if otherwise (TL). Since the automata in Fig. 3(d) and (e) can both be built on the basis of the same rationale, a detailed explanation of the latter is omitted for the sake of brevity.
- **Level 4**: For illustration clarity, the sensor models are omitted in the present example. The online measurements are assumed to be identical to the corresponding tank conditions.

A component state is usually represented with a distinct location in the corresponding automaton. Each location may fire an edge independently or synchronize with another state. Four location symbols can be found in the automata considered in this work: (1) a single circle denotes a regular location, (2) a double circle denotes an initial location, (3) a single circle with a letter “C” denotes a committed location, and (4) a double

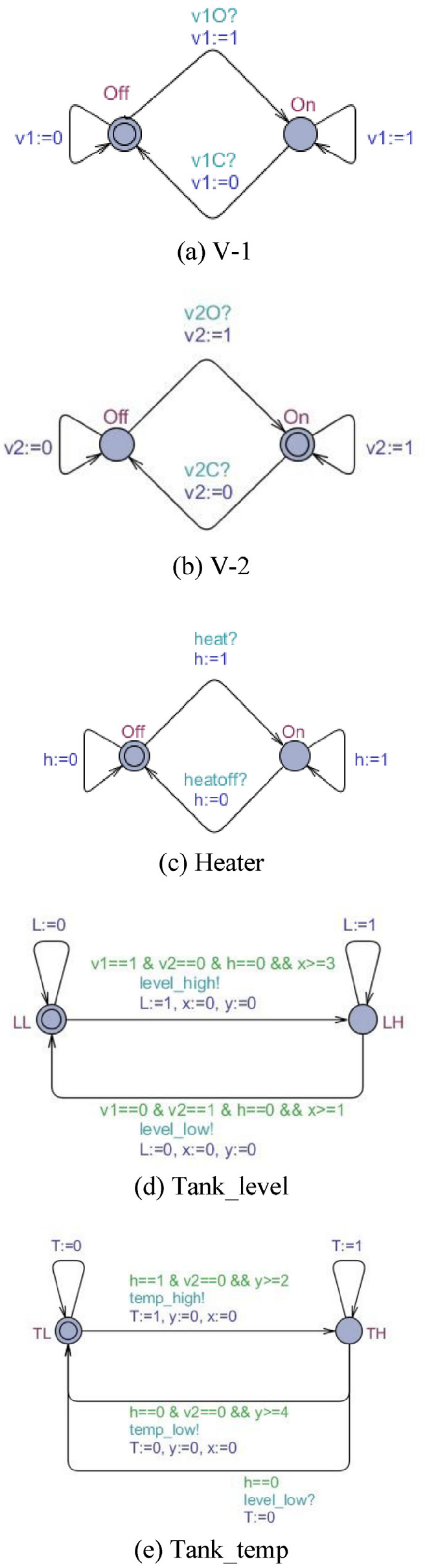
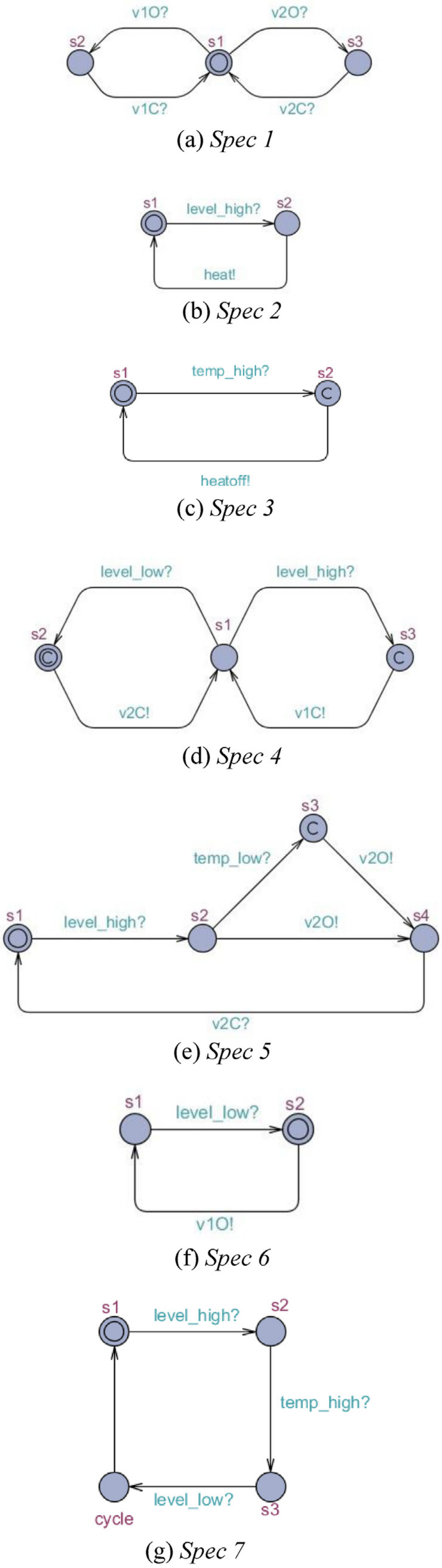


**Fig. 3 – Component models under normal conditions (Example 1).**



(a) *Spec 1*

(b) *Spec 2*

(c) *Spec 3*

(d) *Spec 4*

(e) *Spec 5*

(f) *Spec 6*

(g) *Spec 7*

**Fig. 4 – Control specifications under normal conditions (Example 1).**

circle with a letter "C" denotes a committed initial location. It should be noted that, given a component state, the next transition to be activated must involve an edge from one of the committed (or committed initial) locations.

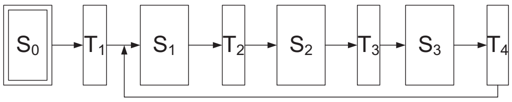


**Fig. 5 – SFC under normal conditions (Example 1).**

## 5. Representation of control specifications

The control specifications are used to ensure safety and/or operability. Specifically, it is used to forbid (or realize) a prescribed event/state sequence so as to avoid physically inadmissible or dangerous system behaviors, e.g., filling a tank when it is full, heating a vessel when it is empty, etc. Three different types of automata may be constructed for use in the following scenarios:

1. **Type A**: If more than one actuator action is allowed to drive the system away from (or toward) the same state, then at most one of them can be implemented.
2. **Type B**: Assign a desired sequence of actuator actions and/or state transition events.
3. **Type C**: Force the system to go through critical steps periodically.

For Example 1, a total of seven control specifications (referred to as *Spec 1*–*Spec 7*) are conjectured and represented, respectively with the automata in Fig. 4(a) and (g). These specifications are summarized as follows:

- *Spec 1* (Type A): Avoid opening the inlet and outlet valves at the same time, and close a valve only after opening it.
- *Spec 2* (Type B): Heat the liquid in tank only after level changing from low to high.
- *Spec 3* (Type B): Switch off the heater immediately after temperature changing from low to high.
- *Spec 4* (Type B): Close the inlet valve immediately after level changing from low to high; Close the outlet valve immediately after level changing from high to low.
- *Spec 5* (Type B): Open the outlet valve after either (1) level changing from low to high or (2) level changing from low to high and then temperature changing from high to low.
- *Spec 6* (Type B): Open the inlet valve only after level changing from high to low.
- *Spec 7* (Type C): A complete cycle should at least include the following three consecutive stages: (1) level changing from low to high, (2) temperature changing from low to high, and (3) level changing from high to low.

## 6. Synthesis of operation steps

After applying the standard operation of parallel composition to the aforementioned component and specification models, a system model can be produced for Example 1. The optimal path should then be identified with the verification tool of UPPAAL and the resulting SFC is given in Fig. 5. The corresponding operation steps and activation conditions are respectively presented in Tables 2 and 3, while the Gantt chart is plotted in Fig. 6. It can be observed that the optimal schedule within a complete cycle calls for four different tasks carried out sequentially in 3 consecutive periods: (1) level changing from low to high in 3 units of time; (2) temperature changing from low to high in 2 units of time; (3) both

**Table 2 – Operation steps and actions in normal procedure (Example 1).**

| Steps | Actions |
|---|---|
| $S_0$ | Initialization |
| $S_1$ | Close V-2; Open V-1. |
| $S_2$ | CloseV-2; Switch on heater. |
| $S_3$ | Open V-2; Switch off heater. |

**Table 3 – Activation conditions and events in normal procedure (Example 1).**

| Conditions | Events |
|---|---|
| $T_1$ | Start |
| $T_2$ | LH |
| $T_3$ | TH |
| $T_4$ | TL & LL |

level and temperature changing from high to low in 1 unit of time.

Note that the proposed synthesis strategy can be applied not only directly to the assumed initial system state for generating the "normal" operating procedure but also to other states which are not normally reachable. As an example, let us assume that the operation in Example 1 may start from an alternative set of component conditions, i.e., V-1 is open, V-2 is open, heater is on, level is high, and temperature is low. In this scenario, the automata in Fig. 3 must be modified and the revised component models can be found in Fig. 7(a)–(d) and Fig. 3(e), respectively. In order to drive the system back to the normal states, an additional control specification is introduced (see Fig. 8). In this automaton, the places 'Abnormal' and 'Normal', respectively denote the abnormal and normal system states. Notice that the requirements for realizing the desired transition are all stipulated in this new specification. i.e., the normal state can be achieved by manipulating the actuators, i.e., V-1, V-2 and heater, to alter the liquid level and temperature. Notice also that the edge "ok!" denotes a successful emergency operation which is reflected in the following conditions: (1) V-1 is closed, (2) heater is off, (3) V-2 is open; (4) level is low, and (5) temperature is low. Finally, every specification in Fig. 4 should also be slightly modified by adding a place (say s0) to represent the abnormal initial system state. This place is directed to a desired normal location with an edge "ok?" (see Fig. 9). By introducing the above modifications, the corresponding emergency response steps can be obtained with the proposed procedure-generation method (see Figs. 10 and 11, Tables 4 and 5). It can be observed from the Gantt chart in Fig. 11 that the required LH-to-LL transition lasts only 1 unit of time before resuming the normal cyclic

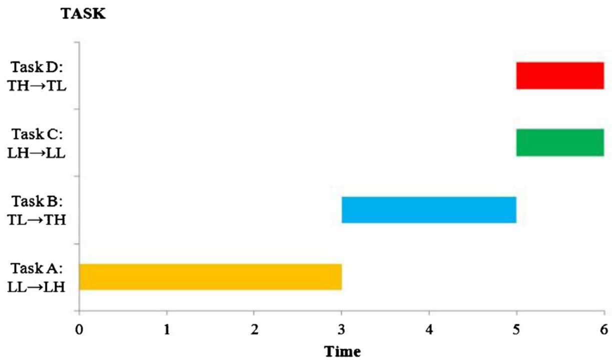
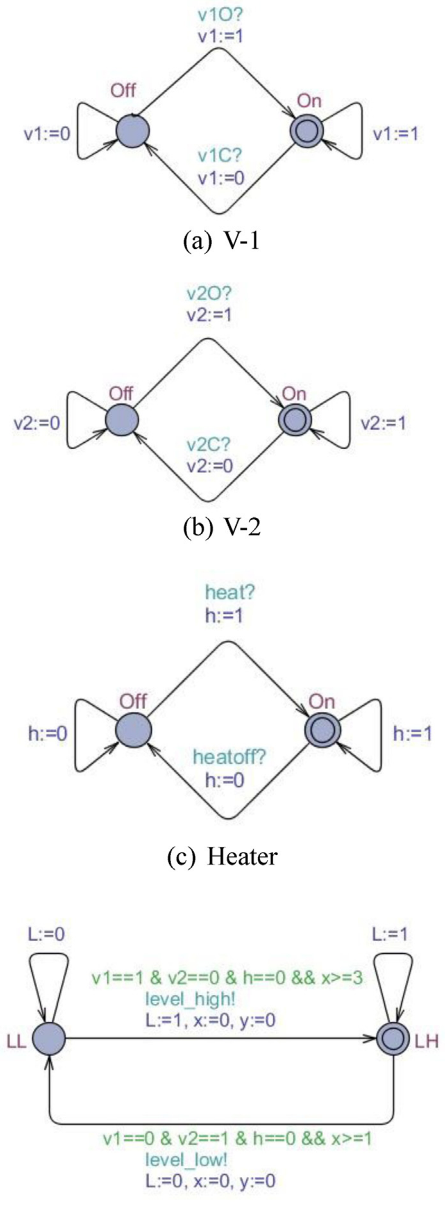


**Fig. 6 – Gantt chart of normal procedure (Example 1).**



(a) V-1

(b) V-2

(c) Heater

(d) Tank_level

**Fig. 7 – Component models under alternative initial conditions (Example 1).**

**Table 4 – Operation steps and actions in alternative procedure (Example 1).**

| Steps | Actions |
|---|---|
| $S_0$ | Initialization. |
| $S_1$ | Close V-1; Switch off Heater. |
| $S_2$ | CloseV-2; OpenV-1. |
| $S_3$ | Open V-1; Switch on Heater. |
| $S_4$ | Switch off Heater; Open V-2. |

**Table 5 – Activation conditions and events in alternative procedure (Example 1).**

| Conditions | Events |
|---|---|
| $T_1$ | Start |
| $T_2$ | LL |
| $T_3$ | TH |
| $T_4$ | TH |
| $T_5$ | TL & LL |

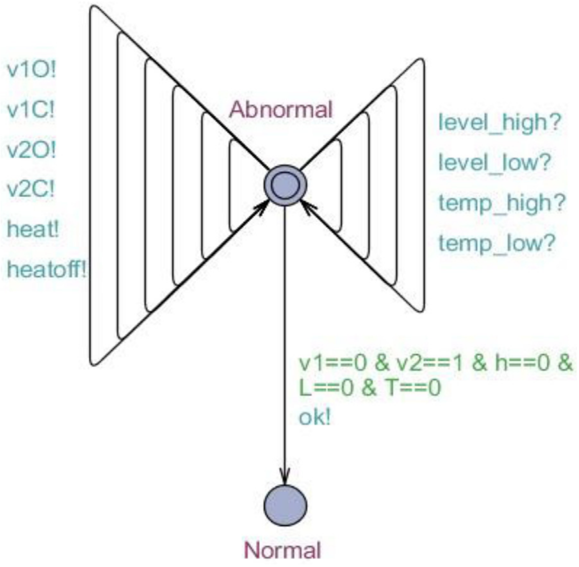


**Fig. 8 – Control specification facilitating return to normal conditions (Example 1).**

operation. Note that the operation schedule between time 1 and time 7 is exactly the same as that in Fig. 6.

## 7. Additional examples

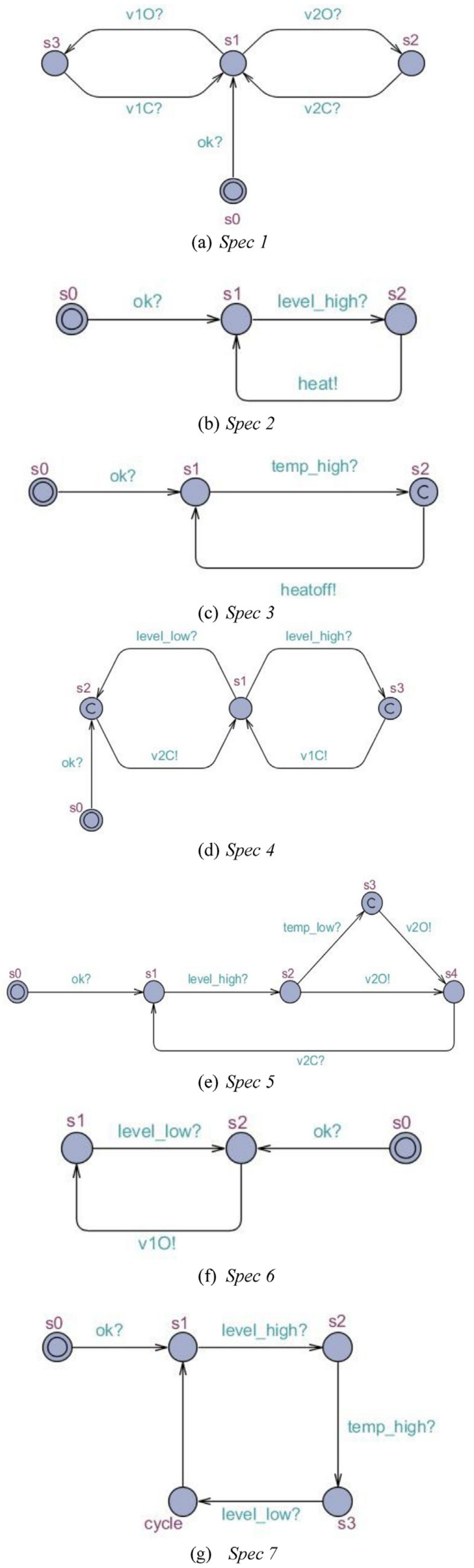
To demonstrate the feasibility of the proposed approach in practical applications, a number of more complex examples have been studied and two of them are presented in the sequel:

### 7.1. *Example 2*

Let us consider the air-drying process given in Fig. 12 (Shaeiwitz et al., 1977). Ambient air, which contains water vapor, enters the process in stream 9 and the air passes through a bed of alumina, where the water vapor is adsorbed. The dried air leaves in stream 25. Two beds (B-I and B-II) are used to maintain a continuous supply of dry air. The states of three valves, the 3-way valve 3W and the two 4-way valves 4W-I and 4W-II, determine the system configuration. When one bed is removing water from air, the other is being regenerated and then cooled. Since a saturated bed cannot be employed for dehumidification purpose, the regeneration operation should be executed to introduce hot air in the saturated beds to strip water from the alumina. The regenerated bed must then be cooled with the inlet air before returning to the air-drying operation. Both beds experience the same operation cycle. Thus, the states of each alumina bed can be characterized with two parameters: the bed temperature and water content. It is assumed in this example that regeneration, cooling and dehumidification, respectively require 2, 3 and 8 units of time.

The component models are first built according to the assumed initial conditions and a brief summary is presented below:

- **Level 2**: There are three components in this level, i.e., one 3-way valve (3W) and two 4-way valves (4W-I and 4W-II). Each can be switched to two alternative positions: 'On' and 'Off'. The relationships between valve positions and stream flows are shown in Table 6. The position of 3 W governs the



(a) *Spec 1*

(b) *Spec 2*

(c) *Spec 3*

(d) *Spec 4*

(e) *Spec 5*

(f) *Spec 6*

(g) *Spec 7*

**Fig. 9 – Control specifications under alternative initial conditions (Example 1).**

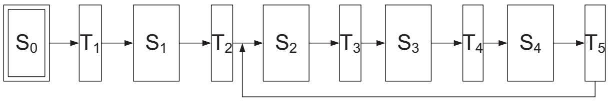


**Fig. 10 – SFC under alternative initial conditions (Example 1).**

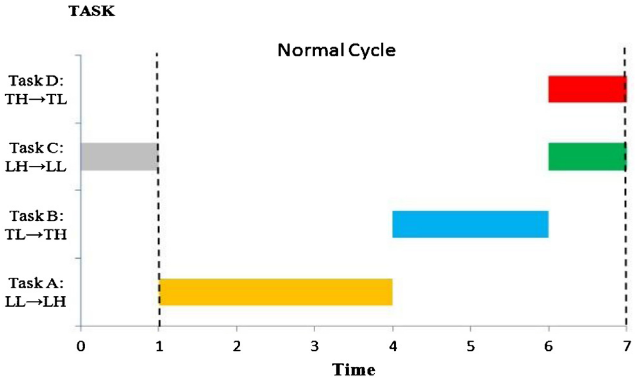


Fig. 11 – Gantt chart of alternative procedure (Example 1).

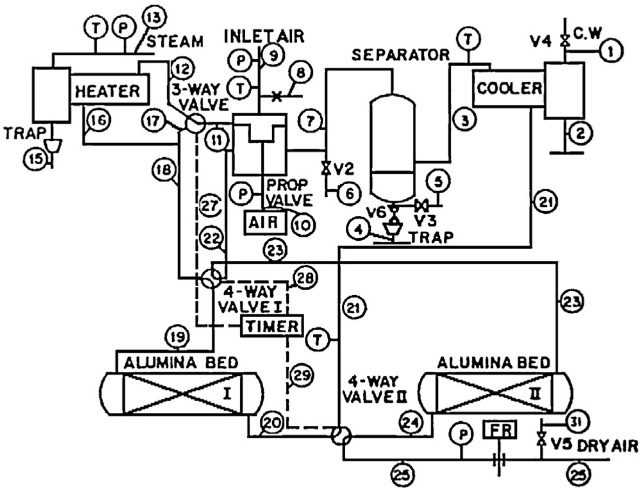


Fig. 12 – PFD of utility air drying system (Example 2).

route of inlet air flow, namely, the fresh air can either be directed to the heater or simply bypass it. The position of 4W-I defines the connections between the alumina beds and their air supplies. The air fed to each bed is originated either from the lower port of proportioning valve (for dehumidification) or from system inlet (for regeneration or cooling). The position of valve 4W-II determines whether the exit airs from these two beds should be discharged or recycled. Initially, all three valves are assumed to be at the 'Off' position and the corresponding models are presented in Fig. 13(a)–(c).

- **Level 3**: Two dehumidification beds, i.e., B-I and B-II, are considered here. The bed temperature is discretized into two distinct levels (hot and cold), and the water content is characterized with three qualitative values (unsaturated, half-saturated and saturated). The initial bed temperature and water content of B-I are assumed to be low and saturated, respectively, while those of B-II are low and unsaturated, respectively. The corresponding automata are presented in Fig. 13(d) and (e).

Table 6 – Stream connections in air drying process (Example 2).

| Valve | Position | Stream flow |
|---|---|---|
| 3W | On | 11 → 12 |
| | Off | 11 → 17 |
| 4W-I | On | 18 → 19 and 22 → 23 |
| | Off | 18 → 23 and 22 → 19 |
| 4W-II | On | 20 → 21 and 24 → 25 |
| | Off | 20 → 25 and 24 → 21 |

- **Level 4**: Although the system is equipped with only one timer, two clock models are adopted to respectively record the elapsed times of various state-transition processes in the two alumina beds, i.e., see Fig. 13(f) and (g).

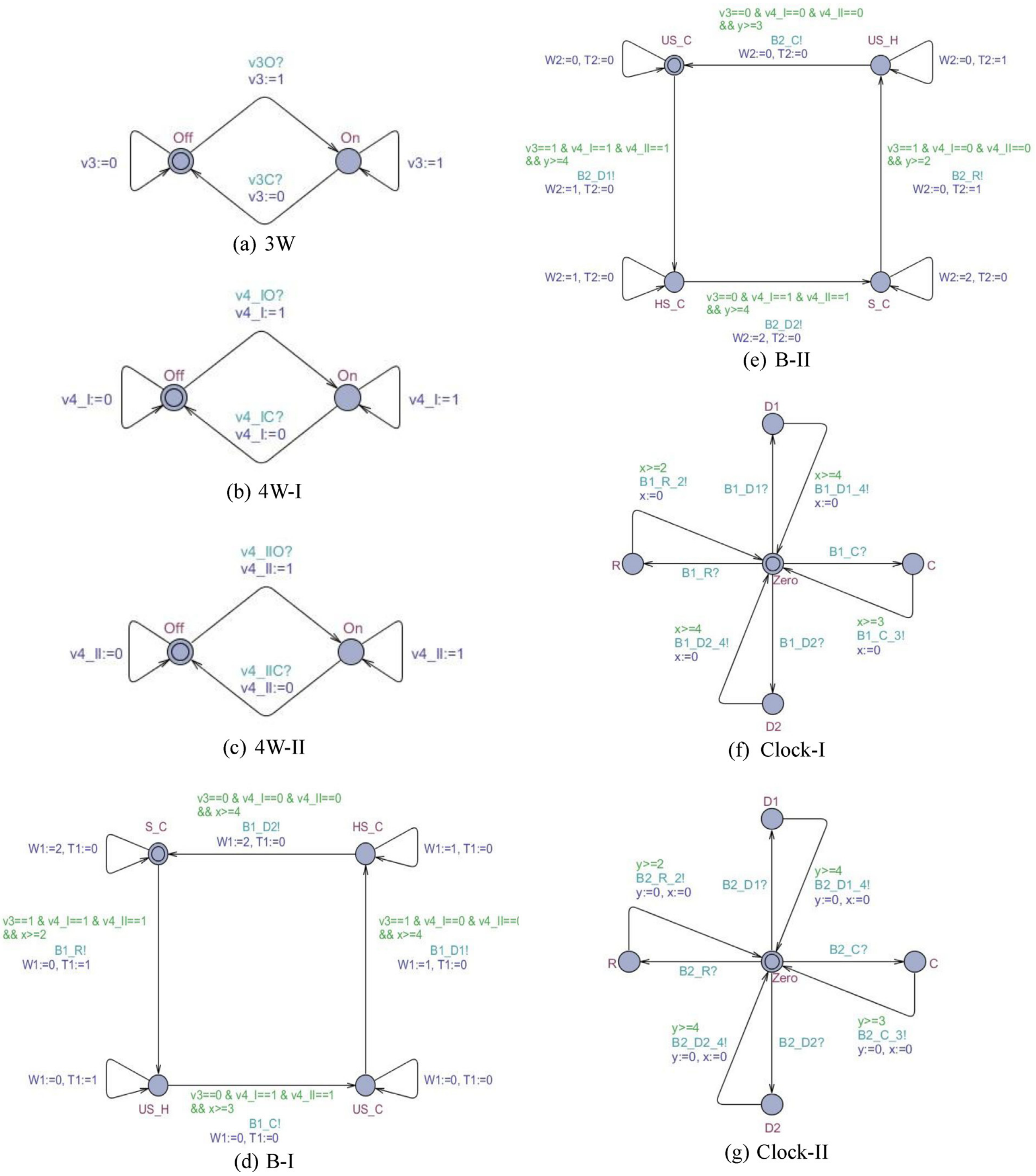
Five control specifications are adopted in the present example and they are modeled with the automata in Fig. 14. A brief description of these specifications is given below:

- *Spec 1*: As shown in Fig. 14(a), the 3-way valve (3W) should be switched to the 'Off' position after the timer shows that the times required for regeneration in one bed and first-stage dehumidification in another are both elapsed.
- *Spec 2*: As shown in Fig. 14(b), the 3-way valve (3W) should be switched to the 'On' position after the timer shows that the times required for cooling in one bed and second-stage dehumidification in another are both elapsed.
- *Spec 3*: Two specifications are incorporated in the automaton given in Fig. 14(c), i.e., (1) the first 4-way valve (4W-I) should be switched to the 'On' position after the timer shows that the time required for cooling the second alumina bed (B-II) is elapsed; (2) the first 4-way valve (4W-I) should be switched to the 'Off' position after the timer shows that the time required for the second-stage dehumidification in the second alumina bed (B-II) is elapsed.
- *Spec 4*: Two specifications are also embedded in the automaton given in Fig. 14(d), i.e., (1) the second 4-way valve (4W-II) should be switched to the 'On' position after the first 4-way valve (4W-I) is switched to the 'On' position; (2) the second 4-way valve (4W-II) should be switched to the 'Off' position after the first 4-way valve (4W-I) is switched to the 'Off' position.
- *Spec 5*: As shown in Fig. 14(e), a full operation cycle consists of 4 consecutive stages and at any stage different tasks are performed in two separate beds in parallel. These tasks are listed below:
  i. Stage 1: regeneration in B-I and first-stage dehumidification in B-II;
  ii. Stage 2: cooling in B-I and second-stage dehumidification in B-II;
  iii. Stage 3: first-stage dehumidification process in B-I and regeneration in B-II;
  iv. Stage 4: second-stage dehumidification in B-I and cooling in B-II.

By following the proposed procedure-synthesis method, the optimal operating procedure can be identified (see Figs. 15 and 16, Tables 7 and 8). Notice that every triggering event in Table 8 is represented with a 3-part code to respectively denote the bed (B-I or B-II) the operation mode, i.e., regeneration (R), cooling (C), first-stage dehumidification (D1) or second-stage dehumidification (D2), and the elapsed time. The operation schedules of two alumina beds within a single cycle are shown in Fig. 16. Note that a full cycle period is

Table 7 – Operation steps and actions in normal procedure (Example 2).

| Steps | Actions |
|---|---|
| $S_0$ | Initialization |
| $S_1$ | 3W, 4W-I and 4W-II to 'On' |
| $S_2$ | 3W to 'Off' |
| $S_3$ | 3W to 'On'; 4W-I and 4W-II to 'Off' |
| $S_4$ | 3W to 'Off' |



(a) 3W

(b) 4W-I

(c) 4W-II

(d) B-I

(e) B-II

(f) Clock-I

(g) Clock-II

**Fig. 13 – Component models under normal conditions (Example 2).**

16 time units and, within this period, each bed is required to stay idle after regeneration and cooling in order to wait for the other bed to finish the dehumidification operation.

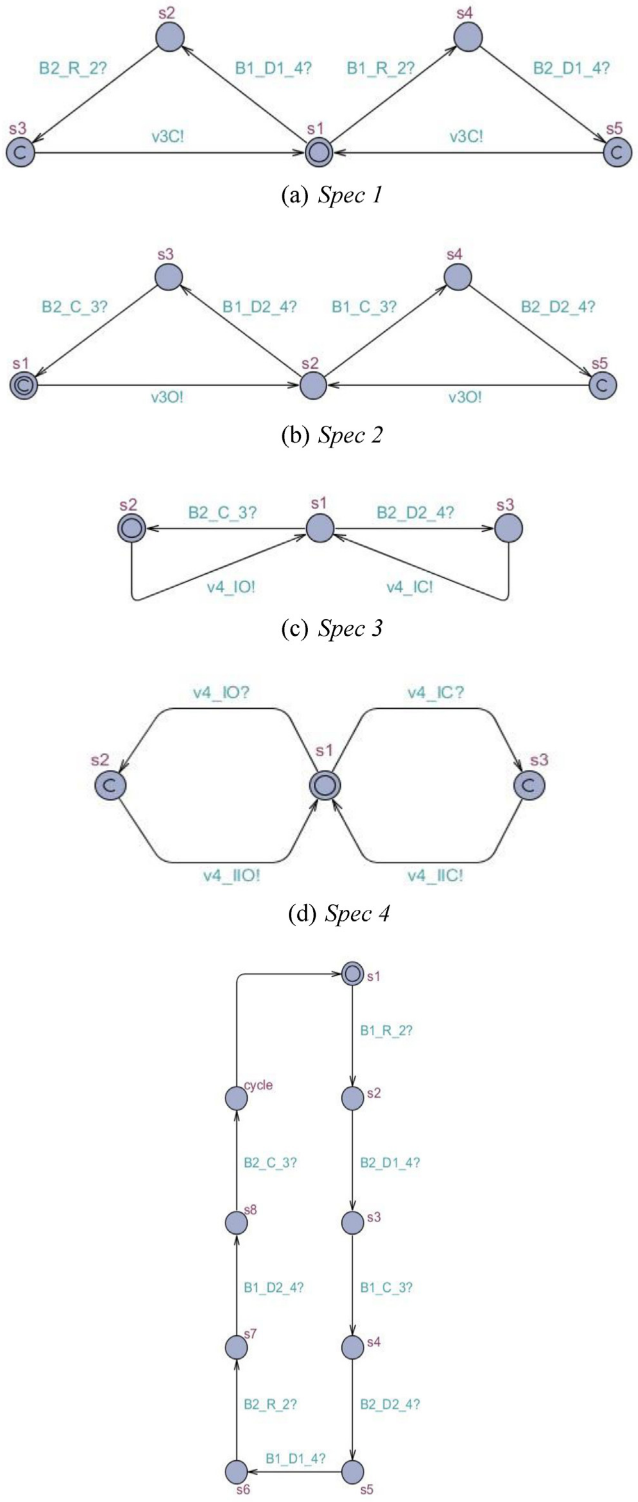
Let us next consider an alternative set of initial conditions:

- 3W, 4W-I and 4W-II are all placed at the 'Off' positions;
- B-I is unsaturated and hot, i.e., 'US_H';
- B-II is half saturated and cold, i.e., 'HS_C'.

**Table 8 – Activation conditions and events in normal procedure (Example 2).**

| Conditions | Events |
|---|---|
| $T_1$ | Start |
| $T_2$ | B-I.R.2 & B-II.D1.4 |
| $T_3$ | B-I.C.3 & B-II.D2.4 |
| $T_4$ | B-I.D1.4 & B-II.R.2 |
| $T_5$ | B-I.D2.4 & B-II.C.3 |

The aforementioned component models in Fig. 13 should be revised accordingly. Furthermore, with the same rationale used for building the control specification in Fig. 8, an additional automaton can be constructed for the present case to facilitate orderly return to the normal conditions (see Fig. 17). Since the component conditions reached after each step in a periodic operation should all be regarded as "normal," four sets of different normal conditions can be identified in every cycle according to Fig. 15 and Tables 7 and 8. For example, 'Normal2′ stands for the following conditions: 3W is 'Off'; 4W-I is 'On'; 4W-II is 'On'; Bed-I is 'US_C'; Bed-II is 'S_C'. Finally, an extra place s0 should be inserted into every specification model in Fig. 14 to represent the "abnormal" system state.



(a) *Spec 1*

(b) *Spec 2*

(c) *Spec 3*

(d) *Spec 4*

(e) *Spec 5*

**Fig. 14 – Control specifications under normal conditions (Example 2).**

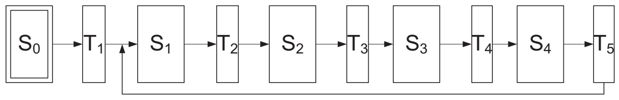


**Fig. 15 – SFC under normal conditions (Example 2).**

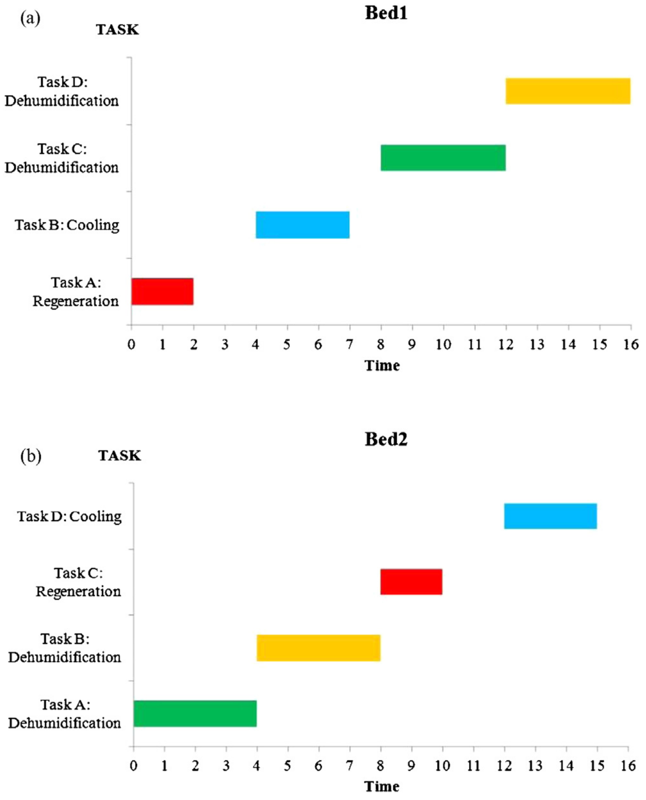


**Fig. 16 – Gantt charts of normal procedure (Example 2).**

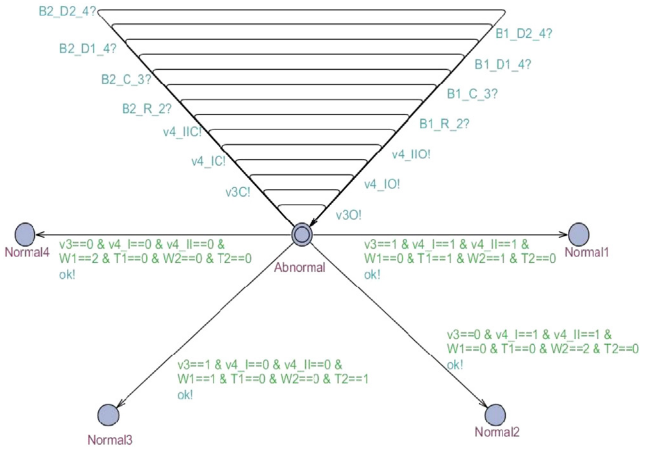

B2_D2_4?
B1_D2_4?
B2_D1_4?
B1_D1_4?
B2_C_3?
B1_C_3?
B2_R_2?
B1_R_2?
v4_IIC!
v4_IIO!
v4_IC!
v4_IO!
v3C!
v3O!
Normal4
v3==0 & v4_I==0 & v4_II==0 & W1==2 & T1==0 & W2==0 & T2==0 ok!
Abnormal
v3==1 & v4_I==1 & v4_II==1 & W1==0 & T1==1 & W2==1 & T2==0 ok!
Normal1
v3==0 & v4_I==1 & v4_II==1 & W1==0 & T1==0 & W2==2 & T2==0 ok!
v3==1 & v4_I==0 & v4_II==0 & W1==1 & T1==0 & W2==0 & T2==1 ok!
Normal3
Normal2

**Fig. 17 – Control specification facilitating return to normal conditions (Example 2).**

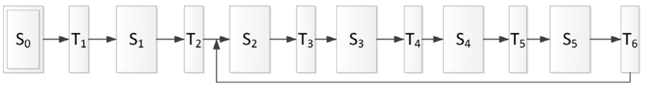


**Fig. 18 – SFC under alternative initial conditions (Example 2).**

The corresponding procedure can be fully described with Fig. 18, Tables 9 and 10 and Fig. 19. It should be noted that, before the system can be executed in regular cyclic operation, a transition period of 4 time units is required to steer the system from the alternative initial state back to the second set of normal conditions.

### 7.2. *Example 3*

In this last example, let us consider the six-tank blending/buffer system presented in Fig. 20. By blending the raw

Table 9 – Operation steps and actions in alternative procedure (Example 2).

| Steps | Actions |
|---|---|
| $S_0$ | Initialization |
| $S_1$ | 4W-II to 'On'; 4W-I to 'On' |
| $S_2$ | 3W to 'On'; 4W-I to 'Off'; 4W-II to 'Off' |
| $S_3$ | 3W to 'Off' |
| $S_4$ | 3W to 'On'; 4W-I to 'On'; 4W-II to 'On' |
| $S_5$ | 3W to 'Off' |

Table 10 – Activation conditions and events in alternative procedure (Example 2).

| Conditions | Events |
|---|---|
| $T_1$ | Start |
| $T_2$ | B-I.C.3 & B-II.D2.4 |
| $T_3$ | B-1.D1.4 & B-II.R.2 |
| $T_4$ | B-I.D2.4 & B-II.C.3 |
| $T_5$ | B-I.R.2 & B-II.D1.4 |
| $T_6$ | B-I.C.3 & B-II.D2.4 |

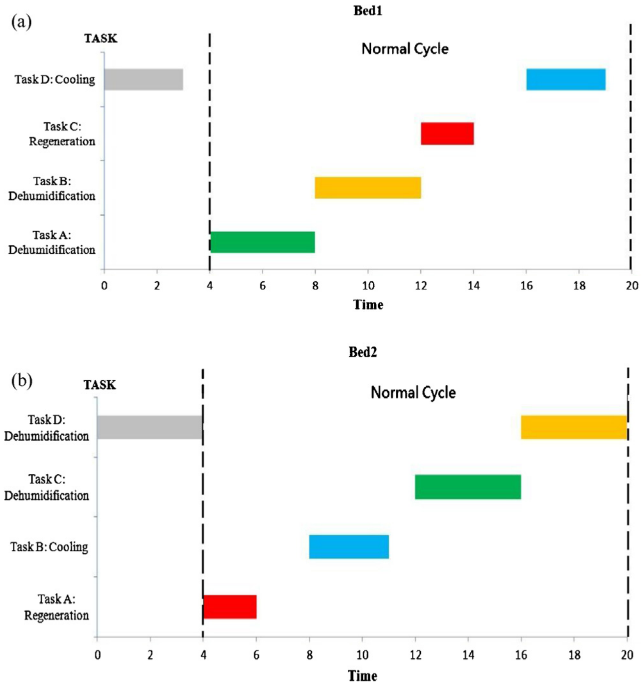


Fig. 19 – Gantt chart of alternative procedure (Example 2).

materials according to specified ratios, two distinct products can be produced in T-1 and T-2, respectively. The valves V-1 and V-3 in this system are used for manipulating the input flows that fill tank T-1, while V-2 and V-4 are for feeding tank T-2. Notice that a pump (Pump-1) is installed on the outlet pipeline of T-1, which is connected to a 3-way valve V-9. If Pump-1 is 'On', the material from tank T-1 can be transferred either to T-5 when V-9 is at the '+' position or to T-6 when V-9 is at '−'. Opening valves V-7 and V-8 facilitates discharge flows from tanks T-5 and T-6, respectively. Pump-2 is installed on the outlet pipeline of T-2, which is connected to another 3-way valve V-10. If Pump-2 is 'On', the liquid from tank T-2 can be transferred either to T-3 when the V-10 is at the '+' position or to T-4 when the V-10 is at the '−' position. Opening valves V-5 and V-6 facilitates discharge flows from tanks T-3 and T-4,

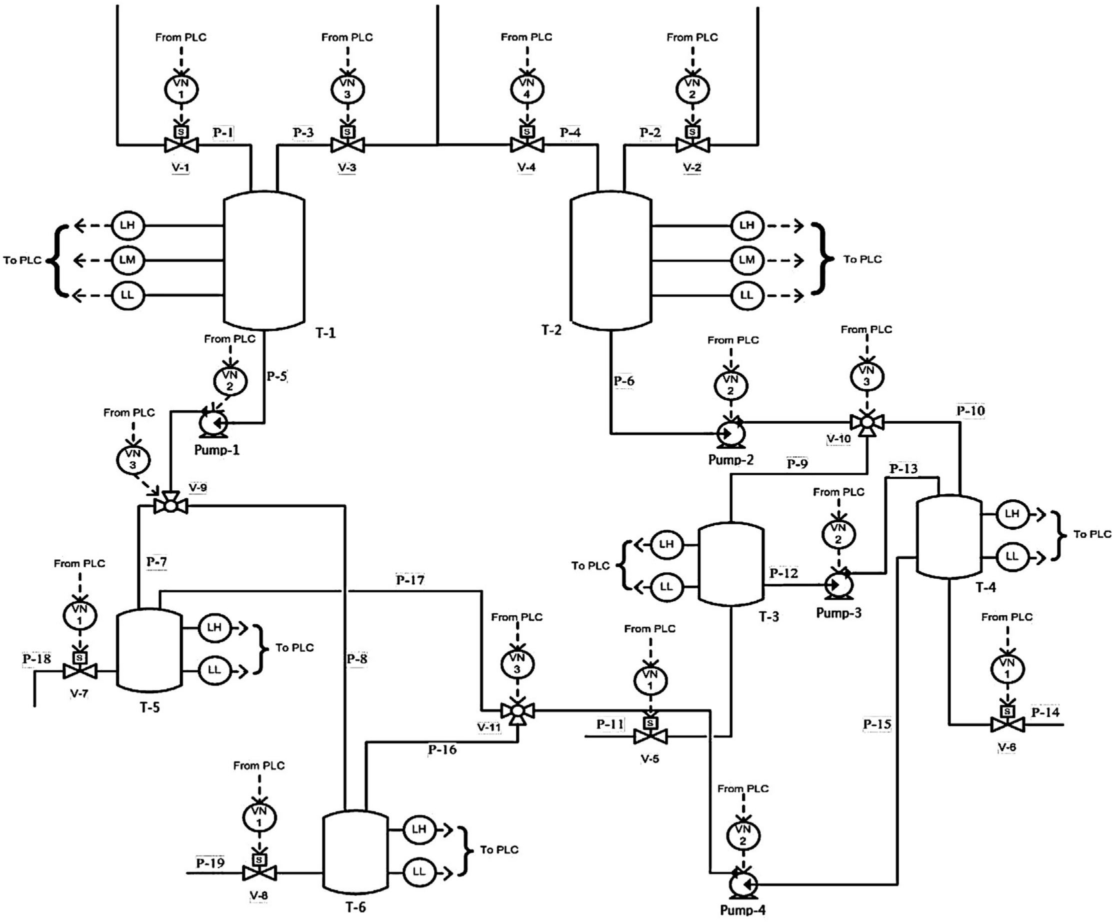


Fig. 20 – PFD of a six-tank blending/buffer system (Example 3).

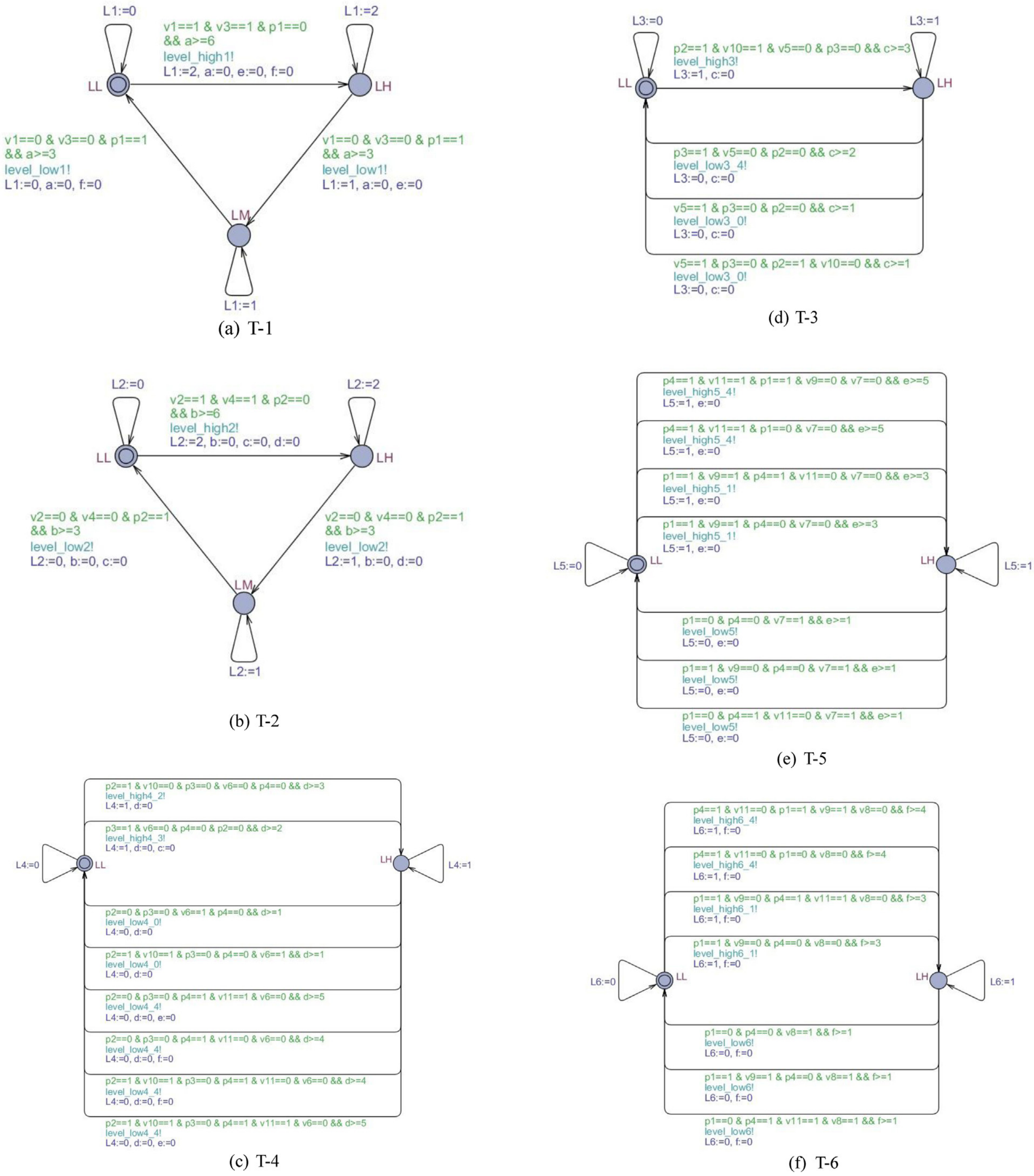
respectively. A third pump (Pump-3) is used to transferred liquid from T-3 to T-4, while the fourth one (Pump-4) is installed on the outlet pipeline of T-4, which is then connected to the 3-way valve V-11. If Pump-4 is 'On', the material from tank T-4 can be either delivered to T-5 when V-11 is at the '+' position or to T-6 when V-11 is at the '−' position.

To simplify model configuration, it is assumed in this example that

1. All six tanks are equipped with level sensors. Three discrete levels in both T-1 and T-2 are reported according to online measurements, i.e., LL (low level), LM (intermediate level), and LH (high level), while on the remaining tanks the level sensors are used to detect only two conditions, i.e., LL and LH.
2. Each tank is filled after sensor signal LL is issued, and discharged when reaching LH.
3. T-5 and T-6 can be used to store only one product at a time.
4. V-5 and V-6 are normally closed at all time.
5. A 3-way valve can be operated only at the time when the corresponding pump is not running.

The normal initial conditions are listed below:

- The 3-way valve V-9 is at the '+' position, while the other two (V-10 and V-11) are both at the '−' positions.
- The 2-way valves V-7 and V-8 are open, while all others are closed.
- All the pumps are 'off'.
- The liquid in every tank is at the low level.



(a) T-1

(d) T-3

(b) T-2

(e) T-5

(c) T-4

(f) T-6

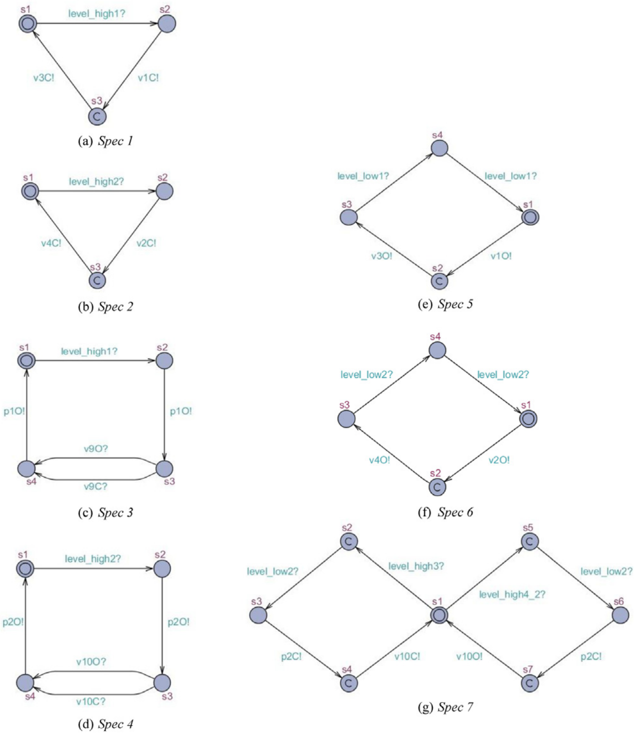
**Fig. 21 – Component models under normal conditions (Example 3).**

The component models under normal conditions are briefly described below:

- **Level 2**: All valves and pumps are components in this level. The corresponding models are basically the same as those reported in Example 1 and thus they are not repeated here for the sake of brevity.
- **Level 3**: All tanks are level-3 components and the corresponding automata are presented in Fig. 21. A brief summary of these models is provided in the sequel:
- The automaton model of T-1 (with the assumed initial condition LL) is given in Fig. 21(a). The edge 'level_high1!' in this model denotes the level-changing process from low to high, while 'level_low1!' represents either the high-to-middle or the middle-to-low process. The prerequisites of the low-to-high transition are: (1) V-1 is open ($v1 == 1$), (2) V-3 is open ($v3 == 1$), (3) Pump-1 is switched off ($p1 == 0$), and (4) the elapsed time is not less than 6 ($a >= 6$). On the other hand, the prerequisites of 'level_low1!' are: (1) V-1 is closed ($v1 == 0$), (2) V-3 is closed ($v3 == 0$), (3) Pump-1 is switched on ($p1 == 1$), and (4) the elapsed time is not less than 3 ($a >= 3$). Note that, after the above processes are completed, not only the clock variable of T-1 but also those of T-5 and T-6 (i.e., variables e and f) are all reset to 0. This is because these tanks are physically connected and thus their operations must be synchronized.
- The timed automaton of T-2 is given in Fig. 21(b). Since it is essentially the same as that of T-1, a repeated description is omitted for the sake of brevity.
- The automaton in Fig. 21(c) is used to model tank T-4 with the initial state LL. Two alternative edges are embedded in this model for characterizing the level-changing processes from low to high, i.e., 'level_high4_2!' and 'level_high4_3!'. The former edge is associated with the liquid transfer operation from T-2 to T-4 in 3 units of time ($d >= 3$), while the latter is from T-3 to T-4 within 2 units of time ($d >= 2$). Six possible liquid-transfer scenarios are considered in this model for the level in T-4 to go from high to low, and they can be classified into two types according to their destinations:
- 'level_low4_0!' denotes the liquid discharge operation to environment (by opening V-6) and the required time is 1 ($d >= 1$);
- 'level_low4_4!' denotes the liquid transfer operation to T-5 or to T-6 (by switching on Pump-4) and the required times are 5 ($d >= 5$) and 4 ($d >= 4$), respectively.
- Since no liquid is allowed to be injected into T-4 in the latter case, Pump-2 should be switched off ($p2 == 0$) or, in the case when the Pump-2 is on, V-10 should be switched to the '+' position ($p2 == 1$ & $v10 == 1$).
- The component models of T-3, T-5 and T-6 are presented in Fig. 21(d)–(f), respectively. Since they are all very similar to the automaton for modeling T-4, these models are not further elaborated here to save space.
- **Level 4**: The sensor models are neglected in the present example for illustration conciseness. The online measurements are assumed to be identical to the corresponding tank conditions.

The control specifications in this example are outlined below:

- *Spec* 1: As shown in Fig. 22(a), V-1 and V-3 are allowed to be closed only after the liquid level in T-1 reaches LH.
- *Spec* 2: As shown in Fig. 22(b), V-2 and V-4 are allowed to be closed only after the liquid level in T-2 reaches LH.
- *Spec* 3: Pump-1 is allowed to be switched on *twice* after the level in T-1 reaches LH. There should be one or more event takes place between these two successive actions, and one of them must be opening or closing V-9. This specification can be imposed with the automaton in Fig. 22(c).
- *Spec* 4: Pump-2 is allowed to be switched on *twice* after the level in T-2 reaches LH. There should be one or more event takes place between these two successive actions, and one



(a) *Spec 1*

(b) *Spec 2*

(c) *Spec 3*

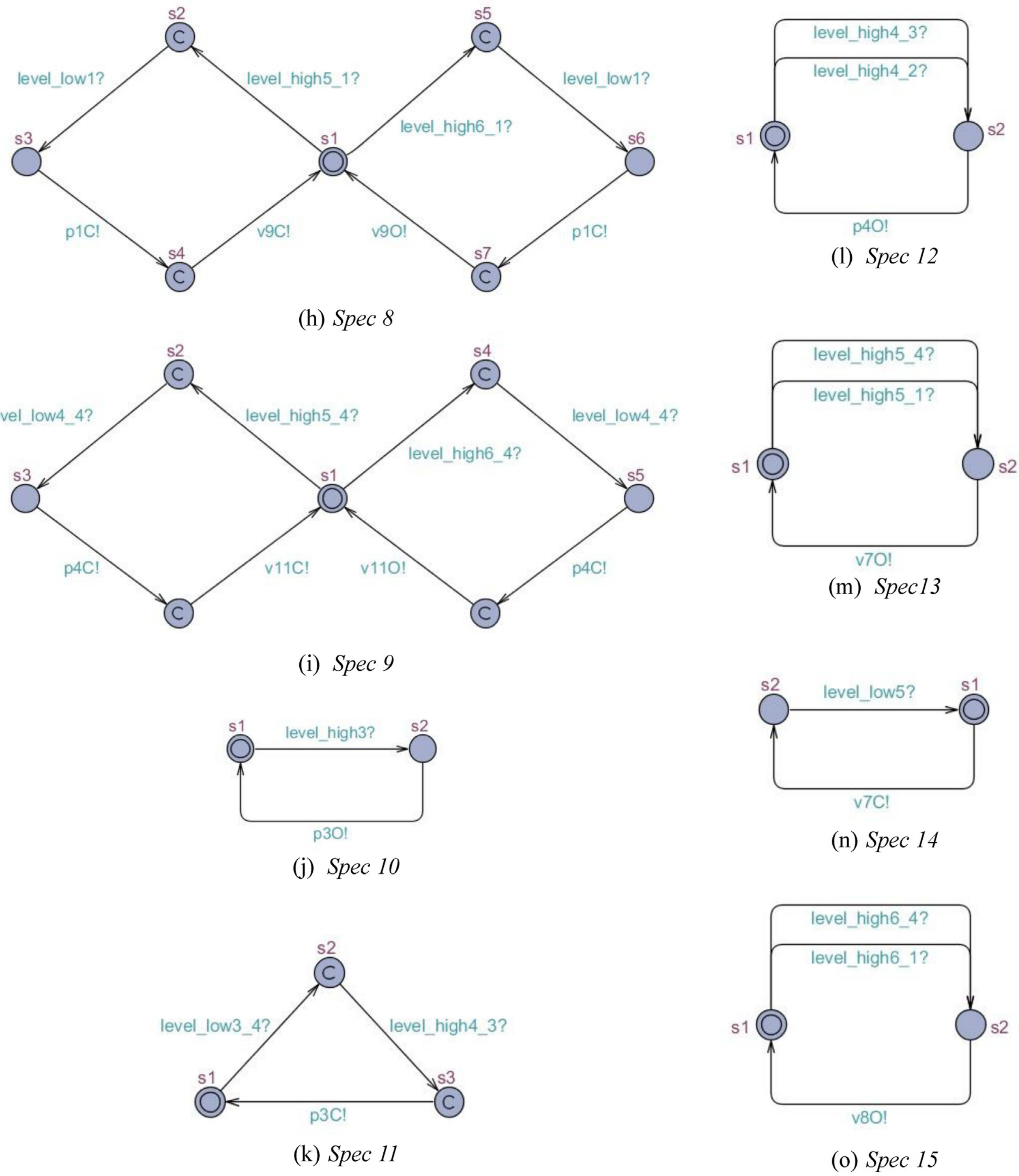
(d) *Spec 4*

(e) *Spec 5*

(f) *Spec 6*

(g) *Spec 7*

**Fig. 22 – Control specifications under normal conditions (Example 3).**



(h) *Spec 8*

(i) *Spec 9*

(j) *Spec 10*

(k) *Spec 11*

(l) *Spec 12*

(m) *Spec13*

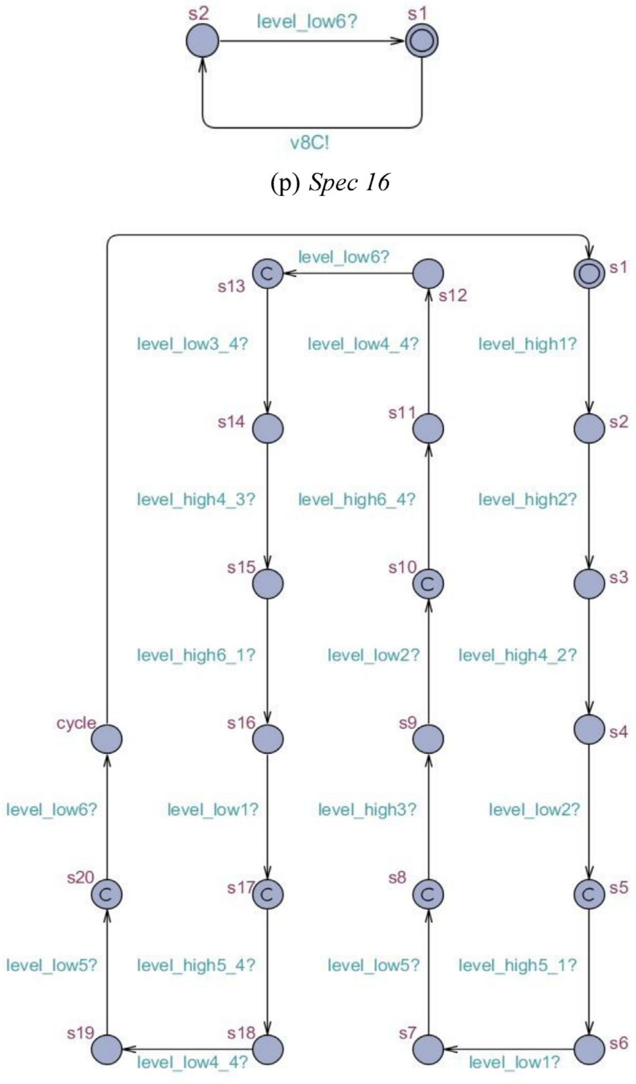
(n) *Spec 14*

(o) *Spec 15*

**Fig. 22 – (*Continued*)**

of them must be opening or closing V-10. This specification can be imposed with the automaton in Fig. 22(d).

- *Spec* 5: The blending operation in T-1 can be resumed (by opening V-1 and V-3) only after the tank is emptied via two consecutive level-lowering processes, i.e., 'level_low1′. This specification is given in Fig. 22(e).
- *Spec* 6: The blending operation in T-2 can be resumed (by opening V-2 and V-4) only after the tank is emptied via two consecutive level-lowering processes, i.e., 'level_low2′. This specification is given in Fig. 22(f).
- *Spec 7*: Switch off Pump-2 and then turn V-10 to the '–' position after the levels in T-3 and T-2 reach LH and LL, respectively; Switch off Pump-2 and then turn V-10 to the '+' position after the levels in T-4 and T-2 reach LH and LL, respectively. This specification in given in Fig. 22(g).
- *Spec* 8: Switch off Pump-1 and then turn V-9 to the '–' position after the levels in T-5 and T-1 reach LH and LL, respectively; Switch off Pump-1 and then turn V-9 to the '+' position after the levels in T-6 and T-1 reach LH and LL, respectively. This specification in given in Fig. 22(h).
- *Spec* 9: Switch off Pump-4 and then turn V-11 to the '–' position after the levels in T-5 and T-4 reach LH and LL, respectively; Switch off Pump-4 and then turn V-11 to the '+' position after the levels in T-6 and T-4 reach LH and LL, respectively. This specification in given in Fig. 22(i).



(p) *Spec 16*

(q) *Spec 17*

**Fig. 22 – (*Continued*).**

- *Spec 10*: As shown in Fig. 22(j), Pump-3 is allowed to be switched on only when the level in T-3 is LH.
- *Spec 11*: As indicated in Fig. 22(k), Pump-3 is allowed to be switched off only after the levels in T-4 and T-3 reach LH and LL, respectively.
- *Spec 12*: As shown in Fig. 22(l), Pump-4 is allowed to be switched on only after the liquid level in T-4 is raised from low to high.
- *Spec 13*: As shown in Fig. 22(m), V-7 can be opened only after the liquid level in T-5 is raised from low to high.
- *Spec 14*: As shown in Fig. 22(n), V-7 can be closed only after the inventory in T-5 is reduced from high to low.
- *Spec 15*: As shown in Fig. 22(o), V-8 can be opened only after the liquid level in T-6 is raised from low to high.
- *Spec 16*: As shown in Fig. 22(p), V-8 can be closed only after the inventory in T-6 is reduced from high to low.
- *Spec 17*: A full operation cycle consists of 6 consecutive stages and at every stage several different tasks must be carried out in parallel. Specifically, these stages can be summarized as follows: (1) Fill T-1 and T-2 to perform the blending operations, (2) Transfer materials, respectively from T-2 to T-4 and from T-1 to T-5; (3) Discharge product from T-5, and transfer material from T-2 to T-3 and from T-4 to T-6, respectively; (4) Discharge product from T-6, and transfer material from T-3 to T-4; (5) Transfer material from T-1 to T-6 and from T-4 to T-5, respectively; (6) Discharge products from T-5 and T-6, respectively. The corresponding control specification is represented with the automaton in Fig. 22(q).

The resulting optimal procedure can be fully described with Figs. 23 and 24, Tables 11 and 12. Note that a total of 14 different tasks are performed in this procedure within the shortest possible cycle period.

Let us next consider an alternative set of initial conditions. Specifically,

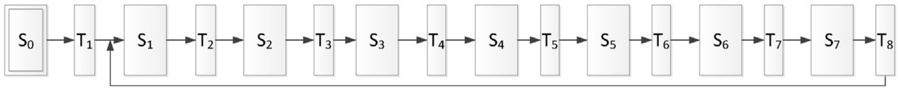


**Fig. 23 – SFC under normal conditions (Example 3).**

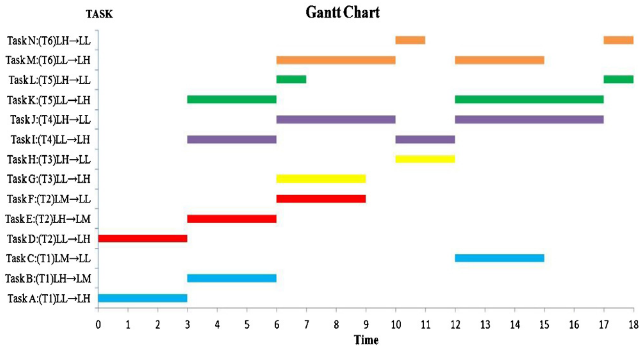


Fig. 24 – Gantt chart of the normal procedure (Example 3).

Table 11 – Operation steps and actions in normal procedure (Example 3).

| Steps | Actions |
|---|---|
| $S_0$ | Initialization |
| $S_1$ | Open V-1; (2) Open V-3; (3) Open V-2; (4) Open V-4; (5) Close V-7; (6) Close V-8 |
| $S_2$ | (1) Close V-1; (2) Close V-3; (3) Switch on Pump-1 |
| $S_3$ | (1) Close V-2; (2) Close V-4; (3) Switch on Pump-2 |
| $S_4$ | (1) Open V-7; (2) Switch off Pump-1; (3) Close V-9; (4) Switch off Pump-2; (5) Open V-10; (6) Switch on Pump-2; (7) Switch on Pump-4 |
| $S_5$ | (1) Open V-8; (2) Switch off Pump-2; (3) Close V-10; (4) Switch on Pump-3; (5) Switch off Pump-4; (6) Open V-11; (7) Close V-7 |
| $S_6$ | (1) Switch off Pump-3; (2) Switch on Pump-1; (3) Switch on Pump-4; (4) Close V-8 |
| $S_7$ | (1) Open V-7; (2) Open V-8; (3) Switch off Pump-1; (4) Open V-9; (5) Switch off Pump-4; (6) Close V-11 |

Table 12 – Activation conditions and events in normal procedure (Example 3).

| Conditions | Events |
|---|---|
| $T_1$ | Start |
| $T_2$ | T-1.LH |
| $T_3$ | T-2.LH |
| $T_4$ | T-1.LM & T-2.LM & T-4.LH & T-5.LH |
| $T_5$ | T-2.LL & T-3.LH & T-4.LL & T-5.LL & T-6.LH |
| $T_6$ | T-3.LL & T-4.LH & T-6.LL |
| $T_7$ | T-1.LL & T-4.LL & T-5.LH & T-6.LH |
| $T_8$ | T-5.LL & T-6.LL |

- The 2-way valves V-7 and V-8 are open, while V-1–V-6 are closed.
- The 3-way valve V-9 is at the '+' position, while V-10 and V-11 are at the '−' position.
- Pump-1 and Pump-2 are on, while Pump-3 and Pump-4 are off.
- The levels in all tanks are LH.

All component models should be modified accordingly. In order to steer the system back to the "normal" conditions, it is also necessary to incorporate the automaton in Fig. 25. Notice first that the 3-way valves V-9, V-10 and V-11 are not allowed to be operated if their upstream pumps are running. Since only Pump-1 and Pump-2 are switched on initially and each may be switched off in the subsequent operation steps, four separate locations, i.e., 'Abnormal1'–'Abnormal4', are adopted in this model to represent four distinct "abnormal" system states, respectively. The corresponding control specifications are summarized below:

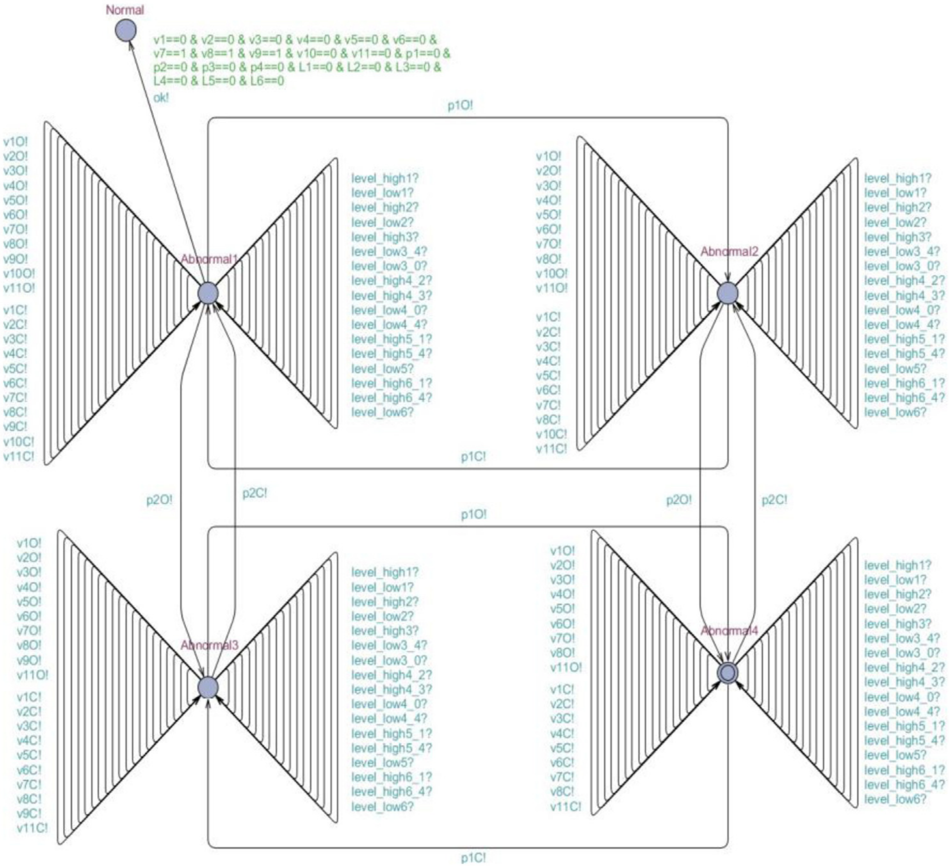


Fig. 25 – Control specification facilitating return to normal conditions (Example 3).

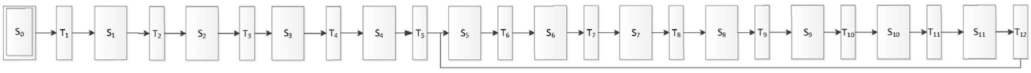


**Fig. 26 – SFC under alternative initial conditions (Example 3).**

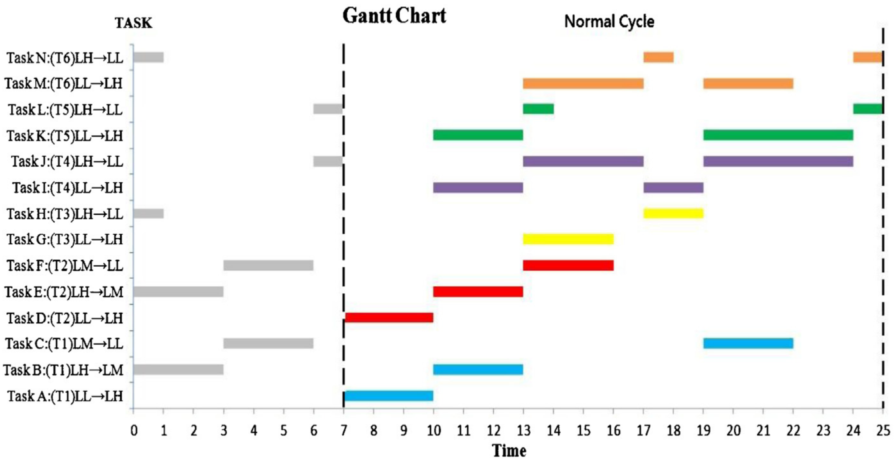


**Fig. 27 – Gantt chart of alternative procedure (Example 3).**

- At the state 'Abnormal1', both Pump-1 and Pump-2 are off and thus all valves are adjustable;
- At the state 'Abnormal2', only Pump-1 is running and thus all valves except V-9 are allowed to be operated;
- At the state 'Abnormal3', only Pump-2 is running and thus all valves except V-10 are allowed to be operated;
- At state 'Abnormal4', both Pump-1 and Pump-2 are switched on and thus all valves expect V-9 and V-10 are adjustable.

The edge "ok!" denotes the transition process from the state 'abnormal1' to the designated "normal" state at which

- V-7 and V-8 are open and V-9 is at the '+' position;
- All pumps are off;
- All tank levels are at LL.

Finally, an extra location s0 should be inserted into each specification model in Fig. 22 to serve as the initial abnormal state. After the system is driven back to the designated "normal" conditions, the original control specifications in Fig. 22 can then be enforced again to produce cyclic operation steps.

**Table 13 – Operation steps and actions in alternative procedure (Example 3).**

| Steps | Actions |
|---|---|
| $S_0$ | Initialization |
| $S_1$ | (1) Open V-5; (2) Open V-6. |
| $S_2$ | Close V-5 |
| $S_3$ | Switch off Pump-1 |
| $S_4$ | Switch off Pump-2 |
| $S_5$ | (1) Close V-6; (2) Open V-7; (3) Switch off Pump-1; (4) Close V-9; (5) Switch off Pump-2; (6) Open V-10; (7) Switch on Pump-2; (8) Switch on Pump-4. |
| $S_6$ | (1) Open V-8; (2) Switch off Pump-2; (3) Close V-10; (4) Switch on Pump-3; (5) Switch off Pump-4; (6) Open V-11; (7) Open V-2; (8) Open V-4; (9) Close V-7. |
| $S_7$ | (1) Switch off Pump-3; (2) Switch on Pump-1; (3) Switch on Pump-4; (4) Close V-8. |
| $S_8$ | (1) Close V-2; (2) Close V-4. |
| $S_9$ | (1) Open V-7; (2) Open V-8; (3) Switch off Pump-1; (4) Open V-9; (5) Switch on Pump-2; (6) Switch off Pump-4; (7) Close V-11; (8) Open V-1; (9) Open V-3. |
| $S_{10}$ | (1) Close V-7; (2) Close V-8. |
| $S_{11}$ | (1) Close V-1; (2) Close V-3; (3) Switch on Pump-1. |

**Table 14 – Activation conditions and events in alternative procedure (Example 3).**

| Conditions | Events |
|---|---|
| $T_1$ | Start |
| $T_2$ | T3.LL & T6.LL |
| $T_3$ | T1.LL & T2.LM |
| $T_4$ | T2.LL |
| $T_5$ | T4.LL & T5.LL |
| $T_6$ | T2.LL & T3.LH & T4.LL & T5.LL & T6.LH |
| $T_7$ | T3.LL & T4.LH & T6.LL |
| $T_8$ | T2.LH |
| $T_9$ | T1.LL & T4.LL & T5.LH & T6.LH |
| $T_{10}$ | T5.LL & T6.LL |
| $T_{11}$ | T1.LH |
| $T_{12}$ | T1.LM & T2.LM & T4.LH & T5.LH |

The resulting cyclic operating procedure is characterized with Figs. 26 and 27, Tables 13 and 14. It can be observed that, before the regular cyclic operation commences, a period of 7 units of time is required to drive the system to the designated normal conditions. During this period, the following eight tasks should be completed:

(1) Time 0 to 3: Tasks B, E, H and N;
(2) Time 3 to 6: Tasks C and F;
(3) Time 6 to 7: Tasks J and L.

## 8. Conclusions

A generic approach has been developed in this work for systematically creating cyclic operating procedures based on timed automata. The proposed procedure-synthesis steps include: (1) constructing automaton model for each component in a given PFD; (2) developing automata to represent the control specifications; (3) assembling the system model; (4) identifying the best operational pathway and the corresponding operating procedure with an available property verification tool, e.g., UPPAAL (Behrmann et al., 2006). Both the sequential function chart (SFC) and Gantt chart of the optimal periodic operation can be produced according to these steps. As shown in the presented examples, the proposed procedure-synthesis strategy is quite effective in various normal and abnormal scenarios with different initial conditions.

## References

Alur, R., Dill, D.L., 1994. A theory of timed automata. Theoretical Computer Science 126, 183–235.

Behrmann,G., David, A., & Larsen, K. G. (2006). A Tutorial on UPPAAL 4.0. http://www.ida.liu.se/~TDTS07/labs/uppaal_tutorial_long.pdf

Bengtsson, J., Yi, W., 2004. Timed automata: semantics, algorithms and tools. In: W. Reisig, G. Rozenberg (Eds.), Lecture Notes on Concurrency and Petri Nets. LNCS 3098, Springer-Verlag.

Bozga, M., Daws, C., Maler, O., Olivero, A., Tripakis, S., Yovine, S. (1998). Kronos: a model-checking tool for real-time systems. In: Proceedings of the 10th International Conference on Computer Aided Verification, No. 1427 in Lecture Notes in Computer Science, Springer-Verlag, pp. 546–550.

Crooks, C.A., Macchietto, S.A., 1992. A combined MILP and logic-based approach to the synthesis of operating procedures for batch plants. Chemical Engineering Communications 114, 117–144.

Foulkes, N.R., Walton, M.J., Andow, P.K., Galluzzo, M., 1988. Computer-aided synthesis of complex pump and valve operations. Computers & Chemical Engineering 12, 1035–1044.

Kim, J., Lee, Y., Moon, I., 2006. Graphical modeling for the safety verification of chemical processes. ESCAPE 16. Garmisch-Partenkirchen, Germany.

Lai, J.W., Chang, C.T., Hwang, S.H., 2007. Petri-net based binary integer programs for automatic synthesis of batch operating procedures. Industrial & Engineering Chemistry Research 46, 2797–2813.

Lee, Y.H., Chang, C.T., Wong, D.S.H., Jang, S.S., 2011. Petri-net based scheduling strategy for semiconductor manufacturing processes. Chemical Engineering Research and Design 89, 291–300.

Li, H.S., Lu, M.L., Naka, Y., 1997. A two-tier methodology for synthesis of operating procedure. Computers & Chemical Engineering 21, S899–S903.

Pettersson, P. (1999). Modeling and Verification of Real-Time Systems. Ph.D. Thesis. Uppsala University, Sweden.

Rivas, J.R., Rudd, D.F., 1974. Synthesis of failure-safe operation. AIChE Journal 20, 320–325.

Shaeiwitz, J.A., Lapp, S.A., Powers, G.J., 1977. Fault tree analysis of sequential systems. I&EC Process Design and Development 16, 529–549.

Wang, F. (2001). RED: Model Checkers for Timed Automata with Clock-Restriction Diagram. In: P. Pettersson, S. Yovine (Eds.), Workshop on Real-Time Tools, No. 2001-014 in Technical Report. Aalborg University of Denmark, Uppsala University.

Yang, S.H., Tan, L.S., He, C.H., 2001. Automatic verification of safety interlock systems for industrial processes. Journal of Loss Prevention in the Process Industries 14, 379–386.

Yeh, M.L., Chang, C.T., 2012a. An automata-based approach to synthesis untimed operating procedures in batch chemical processes. Korean Journal of Chemical Engineering 29 (5), 583–594.

Yeh, M.L., Chang, C.T., 2012b. An automata based method for online synthesis of emergency response procedures in batch processes. Computers & Chemical Engineering 38, 151–170.