ADCONIP
2014
Hiroshima

Synthesis of Periodic Operation Schedules with Timed Automata

Jeh-Hsuan Li and Chuei-Tin Chang, *Chemical Engineering Department, National Cheng Kung University, No. 1, University Road, Tainan 70101, Taiwan*

Abstract — **Manual synthesis of periodic operation schedule in a batch chemical process is considered as a difficult task since it is both time-consuming and error-prone. The timed automata are utilized in the present work to develop a systematic approach to automatically generate the optimal steps for achieving a specific goal. In particular, all components in a given system and the corresponding control specifications are characterized with automata constructed according to the proposed modeling rules. By using standard parallel composition, a system automaton can be constructed with these models and the most appropriate operation path can then be identified accordingly. For any practical application, a sequential function chart (SFC) and the corresponding Gantt chart can also be easily extracted from this path. Two examples are presented to demonstrate the feasibility of the proposed approach.**

I. INTRODUCTION

The most suitable operation schedule for a batch process is dependent upon on the initial system condition(s) and also the ultimate goal(s). Traditionally, the operating procedures are generated manually on an ad hoc basis. This laborious approach often becomes unmanageable with the increase of process complexity. The procedure synthesis problem was first formulated by Rivas and Rudd (1974). Extensive studies concerning the design and verification of procedural controllers were also carried out in the later years. This research issue has been addressed on the basis of various modeling/reasoning schemes, e.g., the mathematical programming models (Crooks and Macchietto, 1992), 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, 2006) and untimed automata (Yeh and Chang, 2012).

Although interesting results have been obtained in the aforementioned studies, the available methods are not mature enough for realistic applications. In particular, every existing method was developed on the basis of a single initial condition during normal operation and, also, the corresponding schedule was not analyzed in detail. The former practice is clearly inapplicable if the given system is at a different (and may be abnormal) state, while the latter may result in inefficient operation. To address these practical 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 synthesized accordingly by applying the standard operation of parallel composition. The best path embedded in this model is identified with existing software UPPAAL (Behrmann et al., 2006) and the corresponding sequential function chart and Gantt chart can also be easily generated. Two examples are presented in this paper to facilitate clear explanation of the proposed method.

II. AUTOMATA-BASED PROCEDURE-GENERATION STRATEGY

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

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

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, $E \subseteq L \times A \times B(C) \times 2^C \times L$ is a set of edges between locations with an action, a guard and a set of clocks to be reset, and $I : L \to B(C)$ is a function ($I(l) = b(c)$) which assigns invariants to locations. Elements of $B(C)$ is the set of conjunctions over simple conditions of the form:

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

where, $x, y \in C, c \in \mathbb{N}$ and $\oplus \in \{<, \le, =, \ge, >\}$. Element of 2^C is the power set of C that is, the set of all subset of C which is the set of reset clock.

The verification tool in UPPAAL is used in the study to search for the best operation path within a given real-time system. More specifically, the best cyclic operating procedure(s) of a given batch process can be produced in four distinct steps:

1. Model all components in the uncontrolled plant with timed automata;
2. Construct automata to represent the control specifications in all possible scenarios;
3. Combine all models created in the previous two steps by using the standard operation of parallel composition;

---

[1] J. H. Li was with Department of Chemical Engineering, National Cheng Kung University, Tainan, Taiwan, ROC (email:funny770206@hotmail.com)

C. T. Chang is with Department of Chemical Engineering, National Cheng Kung University, Tainan, Taiwan, ROC (corresponding author, phone: 886-6-2757575 ext. 62663; fax: 886-6-2344496; e-mail: ctchang@mail.ncku.edu.tw)

4. Execute suitable property verification function in UPPAAL so as to locate the best operation pathway.

III. HIERARCHICAL STRUCTURE OF BATCH PROCESSES

Every batch process can be fully represented with a piping and instrumentation diagram (P&ID) and a sequential function chart (SFC). All identifiable hardware items in P&ID 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 SFC to alter the actuator states in the next level. There may be more than one actuator, e.g., control valves, pump, compressor, and switches, etc., in a system and they are used for adjusting the process configuration, i.e., the material and/or energy flow patterns in the given system. Every unit in P&ID, such as 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 P&ID of an *uncontrolled* process, i.e., levels 2 to 4, is assumed to be *given* in this work, while the SFC is not available. Our goal is to systematically generate a proper SFC and the corresponding Gantt chart so as to satisfy the prescribed control specifications.

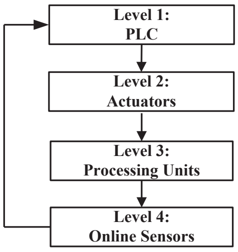


Figure 1. Hierarchical structure of batch processes

The simple liquid storage system given in Fig. 2 (Example 1) can be used to illustrate the aforementioned hierarchy. Specifically, the components in this system can be classified according to Table I.

TABLE I. CLASSIFICATION OF COMPONENTS IN EXAMPLE 1

Levels	Components
1	PLC
2	V-1, V-2, Heater
3	T-1
4	Level and Temp. Sensors

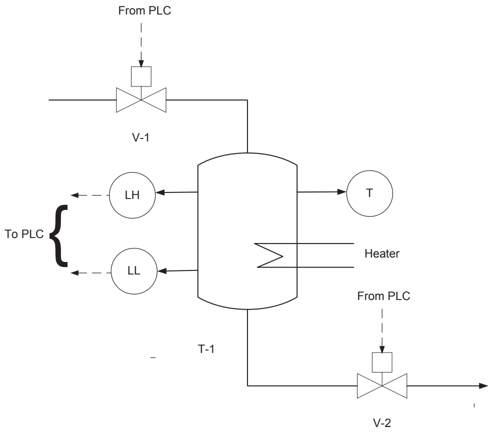
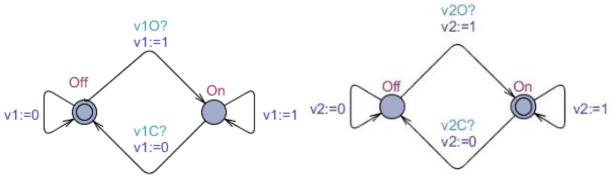


Figure 2. P&ID used in Example 1

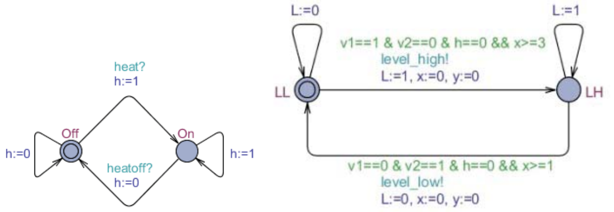
IV. CONSTRUCTION OF COMPONENT MODELS

The model-building principles for the components in an uncontrolled plant can be illustrated with Example 1. Let us assume that the initial liquid level in T-1 is low (LL), while the corresponding temperature is also low (TL). In addition, the assumed initial states of other components are: (1) the inlet valve V-1 is closed, (2) the outlet valve V-2 is open, and (3) the heater is off. Following is a detailed description of the component models:

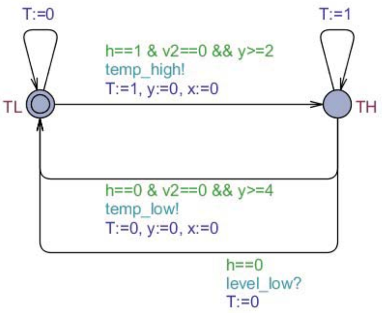
Level 2: The model of valve V-1 is shown in Fig. 3(a). The locations 'Off' and 'On' respectively denote the valve is at the close and open position. The edges 'v1O?' and 'v1C?' respectively represent the close-to-open and open-to-close processes. A binary variable v1 is also adopted to characterize the close-to-open process, where $v1{:=}1$ signifies that this process is finished. On the other hand, $v1{:=}0$ represents the completion of open-to-close process. The automaton models of V-2' and heater 'Heater' are similar to the inlet valve 'V-1', and they are given in Fig. 3(b) and Fig. 3(c).



(a) V-1 (b) V-2



(c) Heater (d) Tank_level



(e) Tank_temp

Figure 3. Component models used in Example 1 for normal initial states

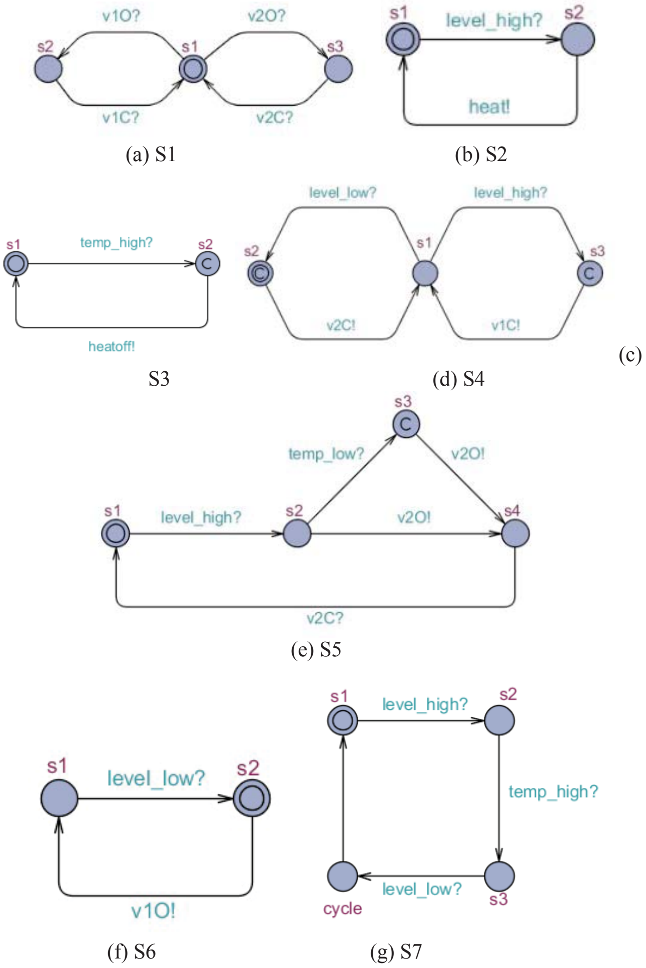
Level 3: The tank is the only element in this level. Two automata, Fig. 3(d) and Fig. 3(e), are used to respectively describe the states of level and temperature in tank T-1. And x and y are the corresponding clock variables. In Fig. 3(d), the edges “level_high!” and “level_low!” respectively denote the level changing processes from low to high and vice versa. The prerequisites of the former process are: (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 required state transition time is more than 3 ($x>=3$). On the other hand, the prerequisites of the latter process are: (1) the inlet valve is closed ($v1==0$), (2) the outlet valve is open ($v2==1$), (3) the heater is close ($h==0$), and (4) the required state transition time is more than 1 ($x>=1$). In addition, the binary variable L is used to represent the status of level changing process, i.e., its value is 1 when level is high (LH) and 0 if otherwise (LL). After the processes “level_high!” and “level_low!” are completed, the clock variables x and y will be reset to 0. Since the automaton in Fig. 3(e) can be built on the basis of the same rationale, a repeated explanation is omitted due to space limitation.

Level 4: For the sake of brevity, the sensor models are omitted in the present example. The online measurements are assumed to be identical to the corresponding tank states.

V. REPRESENTATION OF CONTROL SPECIFICATIONS

The control specifications are used to ensure safety and/or operability. Specifically, it is used to achieve or forbid 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. Four types of automata may be constructed for use in the following scenarios:

- Type A: If more than one control action is allowed at a given system state, select at most one to be executed.
- Type B: If more than one control action results in the same system state, select at most one to be executed.
- Type C: Assign a predetermined sequence of control actions.
- Type D: If periodic operation is required, force the system return to the initial state.



(a) S1

(b) S2

S3

(d) S4

(c)

(e) S5

(f) S6

(g) S7

Figure 4. Specification models used in Example 1 for normal initial states

The control specifications used in Example 1 are summarized as follows:

Spec 1: Avoid opening inlet and outlet valves simultaneously (Type A, see Fig. 4(a)).

Spec 2: Avoid heating except when level is high (Type C, see Fig. 4(b)).

Spec 3: Avoid switching off the heater except when temperature is high (Type C, see Fig. 4(c)).

Spec 4: Avoid closing inlet valve (V-1) except when level is high (LH); Avoid closing outlet valve (V-2) except when level is low (LL) (Type C, see Fig. 4(d)).

Spec 5: Opening outlet valve(V-2) only after one of the following conditions is satisfied: (1) level is high (LH), (2) level is high (LH) and temperature is low (TL) (Type C, see Fig. 4(e)).

Spec 6: Avoid opening inlet valve (V-1) except when level is low (LL) (Type C, see Fig. 4(f)).

Spec 7: A complete operation cycle should at least include the following three processes: (1) level changing from low to high, (2) temperature changing from low to high, and (3) level changing from high to low (Type D, see Fig. 4(g)).

VI. 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. The verification tool of UPPAAL can then be used to identify the optimal path with the shortest operation cycle. The resulting SFC can be found in Fig. 5. The corresponding operation steps and activation conditions are respectively presented in Table II and Table III, while the Gantt chart is given in Fig. 6.

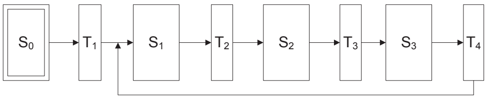


Figure 5. SFC for the normal initial states in Example 1

TABLE II. OPERATION STEPS IN EXAMPLE 1 (NORMAL INITIAL STATES)

Steps	Actions
S0	Initialization
S1	(1) Close V-2 (2)Open V-1
S2	(1)CloseV-1 (2)Switch on Heater
S3	(1)Open V-2 (2)Switch off Heater

TABLE III. ACTIVATION CONDITIONS IN EXAMPLE 1 (NORMAL INITIAL STATES)

Symbol	Condition
T1	Start
T2	LH
T3	TH
T4	TL & LL

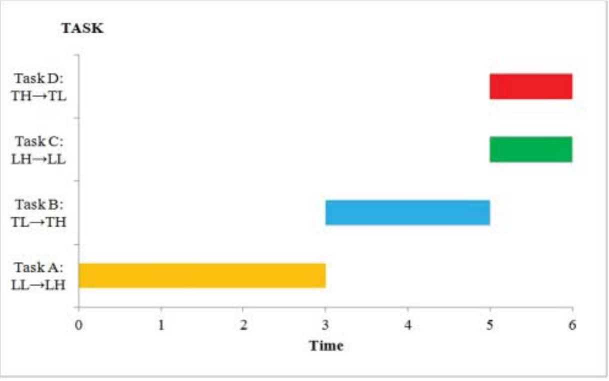


Figure 6. Gantt chart for the normal initial states in Example 1

The above results can be viewed as the "normal" operating procedure. The same modeling strategy is also applicable for the "abnormal" initial states. For example, let us consider the following initial conditions: (1) level is high (LH), (2) temperature is low (TL), (3) V-1 is open, (4) V-2 is open, and (5) heater is on. Obviously, the initial conditions of automata in Fig. 3 must be modified accordingly. In order to drive the system back to the normal states, an additional control specification should be introduced (see Fig. 7). 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 process are essentially 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 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 (LL), and (5) temperature is low (TL). Finally, each original specification (see Fig. 4) should be slightly modified by adding a place (say s0) to represent the abnormal initial system state. This place is directed to a proper place with an edge "ok?". By introducing the above modifications, the corresponding emergency response steps can be obtained with the proposed procedure-generation method (see Fig. 8, Fig. 5, Table IV and Table V).

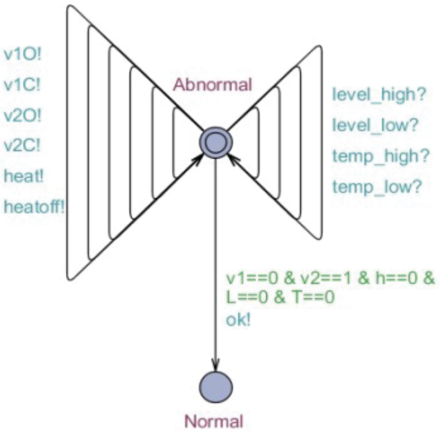


Figure 7. Control specification for the abnormal initial conditions in Example 1

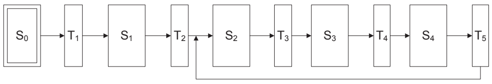


Figure 8. SFC for abnormal initial states in Example 1

TABLE IV. OPERATION STEPS IN EXAMPLE 1 (ABNORMAL INITIAL STATES)

Steps	Actions
S0	Initialization
S1	(1) Close V-1 (2) Switch off Heater
S2	(1) CloseV-2 (2) OpenV-1
S3	(1)Open V-1 (2)Switch on Heater
S4	(1) Switch off Heater (2) Open V-2

TABLE V. ACTIVATION CONDITIONS IN EXAMPLE 1 (ABNORMAL INITIAL STATES)

Symbols	Conditions
T1	Start
T2	LL
T3	TH
T4	TH
T5	TL & LL

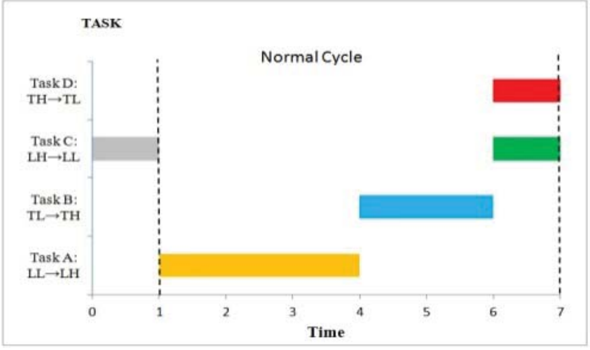


Figure 9. Gantt chart for the abnormal initial states in Example 1

VII. AN ADDITIONAL EXAMPLE

Let us consider the air-drying process given in Fig. 10 (Alur and Dill, 1994), which is referred to as Example 2 in this paper. 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. It is assumed that the in-service adsorption bed reaches the full saturation level during the two periods when the stripping and cooling operations are performed on the other bed. Thus, the states of each alumina bed can be characterized with two distinct parameters: the bed temperature and water content. It is assumed that both parameters can be measured online. Regeneration, cooling and dehumidification respectively require 2, 3 and 8 units of time.

Due to the space limitation, only qualitative descriptions of the components are 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 valve can be switched to two alternative positions: “On” and “Off”. The relationships between the valve positions and the stream flows are shown in Table VI. The position of 3W governs the 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 consumed in each bed can be taken 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 the destinations of the exit airs from these two beds: the air can be either discharged or recycled. Initially, all three valves are assumed to be at the “Off” position.

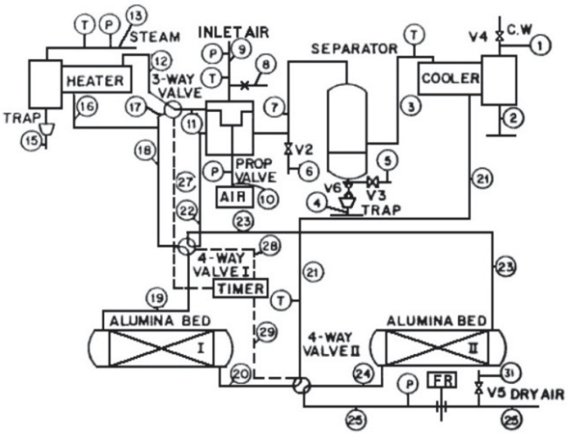


Figure 10. A utility air drying process

TABLE VI. RELATIONSHIPS BETWEEN VALVE POSITIONS AND STREAM FLOWS IN EXAMPLE 2

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

Level 3: There are two dehumidification beds in this level. Two distinct temperature states (high and low) and three separate water-content levels (unsaturated, half-saturated and saturated) are considered. The initial bed temperature and water content of B-1 are assumed to be low and saturated, respectively, while those of B-2 are low and unsaturated, respectively.

Level 4: The timer is the only component. It is used to measure the elapsed times of state-transition processes in the dehumidification beds.

In addition, the control specifications in this example are outlined below:

Spec 1: 3-way valve (3W) can be switched to the “Off” position only after the timer shows the times required for regeneration and first-stage dehumidification are both elapsed.

Spec 2: 3-way valve (3W) can be switched to the “On” position only after the timer shows the times required for cooling and second-stage dehumidification are both elapsed.

Spec 3: 4-way valve I (4W-I) can be switched to the "On" position only after the timer shows the time required for cooling bed II is elapsed; 4-way valve I (4W-I) can be switched to the "Off" position only after the timer shows the time required for the second-stage dehumidification is elapsed.

Spec 4: 4-way valve II (4W-II) can be switched to the "On" position only after 4-way valve I (4W-I) is switched to the "On" position; 4-way valve II (4W-II) can be switched to the "Off" position only after 4-way valve I (4W-I) is switched to the "Off" position

Spec 5: A full operation cycle should be performed repeatedly in 4 sequential steps: (1) to complete the regeneration process in B-I and the first-stage dehumidification process in B-II, (2) to complete the cooling process in B-I and the second-stage dehumidification process in B-II, (3) to complete the first-stage dehumidification process in B-I and the regeneration process in B-II, and (4) to complete the second-stage dehumidification process in B-I and the cooling process in B-II.

By following the proposed procedure synthesis method, the optimal operating procedure can be identified. This procedure is summarized in Fig. 11, Fig. 12, Table VII and Table VIII.

VIII. CONCLUSIONS

A systematic automata-based procedure is presented in this work to generate periodic operation schedule for any batch chemical process. The proposed procedure-synthesis steps include: (1) constructing automaton model for each component; (2) developing automata to represent control specifications; (3) creating the system model; (3) using property verification to find the best operational pathway and the corresponding operating procedure. As shown in the presented examples, the proposed approach is effective in various normal and abnormal scenarios with given initial conditions.

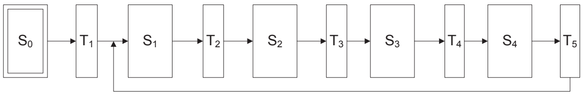


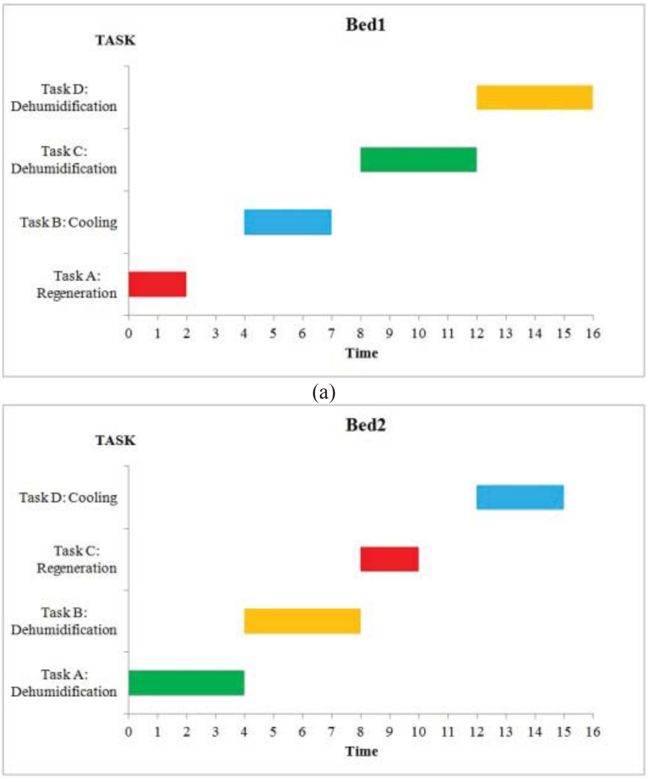
Figure 11. SFC obtained in Example 2

TABLE VII. OPERATION STEPS IN EXAMPLE 2

Operation step	Control actions
S_0	Initialization
S_1	(1) Switch 3W to "On" (2) Switch 4W-I to "On" (3) Switch 4W-II to "On"
S_2	(1) Switch 3W to "Off"
S_3	(1) Switch 3W to "On" (2) Switch 4W-I to "Off" (3) Switch 4W-II to "Off"
S_4	(1) Switch 3W to "Off"

TABLE VIII. ACTIVATION CONDITIONS IN EXAMPLE 2

Symbol	Condition
T_1	Start
T_2	B-I.Reg.2TimeUnit & B-II. Deh1.4TimeUnit
T_3	B-I.Cooling.3TimeUnit & B-II. Deh2.4TimeUnit
T_4	B-I. Deh1.4TimeUnit & B-II. Reg.2TimeUnit
T_5	B-I. Deh2.4TimeUnit & B-II.Cooling.3TimeUnit



(a)

(b)

Figure 12. Gantt charts in Example 2

REFERENCES

[1] J. R. Rivas and D. F. Rude, "Synthesis of failure-safe operation," *AIChE Journal*, vol. 20, pp. 320–325, 1974.

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

[3] S. H. Yang, L. S. Tan, and C. H. He, "Automatic verification of safety interlock systems for industrial processes," *Journal of Loss Prevention in the Process Industries*, vol. 14, pp. 379–386, 2001.

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

[5] J. W. Lai, "Petri-net based integer programs for synthesizing optimal batch operation procedures," M.S. thesis, Department of Chemical Engineering, National Cheng Kung University, Tainan, Taiwan, 2006.

[6] M. L. Yeh and C. T. Chang, "An automata based method for online synthesis of emergency response procedures in batch processes," *Computers & Chemical Engineering*, vol. 38, pp. 151–170, 2012.

[7] G. Behrmann, A. David, and K. G. Larsen, "A Tutorial on UPPAAL 4.0," Department of Computer Science, Aalborg University, Denmark, November 2006.

[8] R. Alur and D. L. Dill, "A theory of timed automata," *Theoretical Computer Science*, vol. 126, pp. 183–235, 1994.