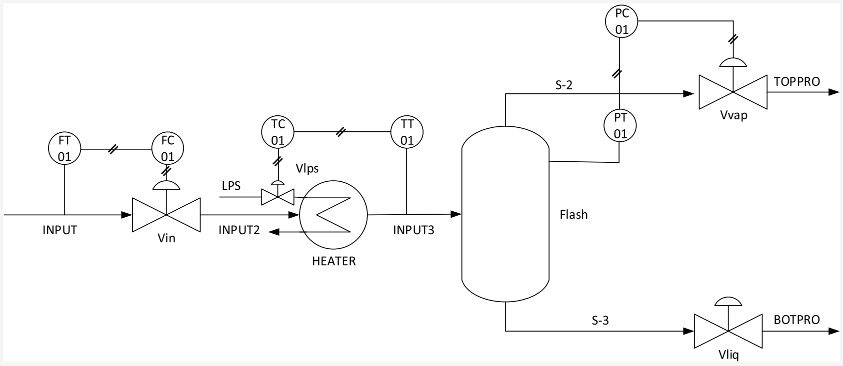
I&EC research
Industrial & Engineering Chemistry Research
pubs.acs.org/IECR
Article

Synthesis, Validation, and Evaluation of Operating Procedures Based on Timed Automata and Dynamic Simulation

Chun-Ren Zhang, Chun-Yu Yeh, and Chuei-Tin Chang*

Cite This: *Ind. Eng. Chem. Res.* 2020, 59, 8769−8782
Read Online



ABSTRACT: Manually generating the operating procedures is often laborious, time-consuming, and error-prone. Because the online sensors may not always be adequate for a designated operation in the plant, the elapsed times of its steps can be stipulated in the activation conditions of a sequential function chart to replace the needed instrument readings. With the timed automata [Alur, R.; et al.*Theoretical Computer Sci.* **1994**, *126*, 183−235] and dynamic simulation, the tasks of synthesizing, validating, and evaluating the operating procedures with insufficient measurements have been systemized in this work. Dividing the operating procedures properly into several stages and setting the reasonable control specifications facilitate the search for specific operation steps. By using the software UPPAAL [Behrmann, G.; et al.A Tutorial on UPPAAL. In *Formal Methods for the Design of Real-Time Systems*; Springer: Berlin, Heidelberg, 2004; pp 200 −236, Behrmann, G.; et al.*A Tutorial on Uppaal 4.0*; Department of Computer Science, Aalborg University: Denmark, 2006], all component automata can be integrated to form a system model and the shortest and/or quickest traces can then be extracted accordingly. These traces can be summarized with the sequential function chart and then verified with Aspen Plus Dynamics. Two examples are presented to validate the proposed approach.

1. INTRODUCTION

It is well recognized that the standard operating procedures (SOPs) are indispensable for running chemical plants. They are needed in performing a wide variety of essential tasks for the continuous processes, such as the startup and shutdown operations of processing units, the emergency response actions under abnormal conditions, and equipment maintenance routines, etc., and for virtually all production activities of the batch processes. Therefore, other than the process flow diagram (PFD) and the piping and instrumentation diagram (P&ID), the sequential function chart (SFC) of every SOP should also be documented thoroughly in process design. Despite the fact that modern chemical plants are becoming much more complex than they used to be, their operating procedures are still generated manually in most cases. Since this approach is clearly laborious, time-consuming, and error-prone, it is necessary to develop a systematic approach to automatically conjecture a set of reliable control actions to perform various tasks in realistic chemical processes.

Obviously, any operating procedure must be synthesized according to the initial system state and also the ultimate operational goal. To overcome the difficulties caused by the combinatorial explosion of all possible operation pathways, many published studies have focused on issues concerning systematic procedure synthesis. Since a comprehensive survey has already been given recently by Chen and Chang,[4] these studies are not enumerated here for the sake of brevity. On the other hand, notice that the common drawback of the aforementioned earlier studies is that they emphasized only upon the procedure synthesis aspects and thus the resulting SFCs may not be implementable in a realistic environment. In particular, these automatically synthesized SOPs were not validated either in simulation studies with credible software or in the pilot plant experiments.

Received: March 19, 2020
Accepted: April 11, 2020
Published: April 11, 2020

https://dx.doi.org/10.1021/acs.iecr.0c01427
Ind. Eng. Chem. Res. 2020, 59, 8769−8782

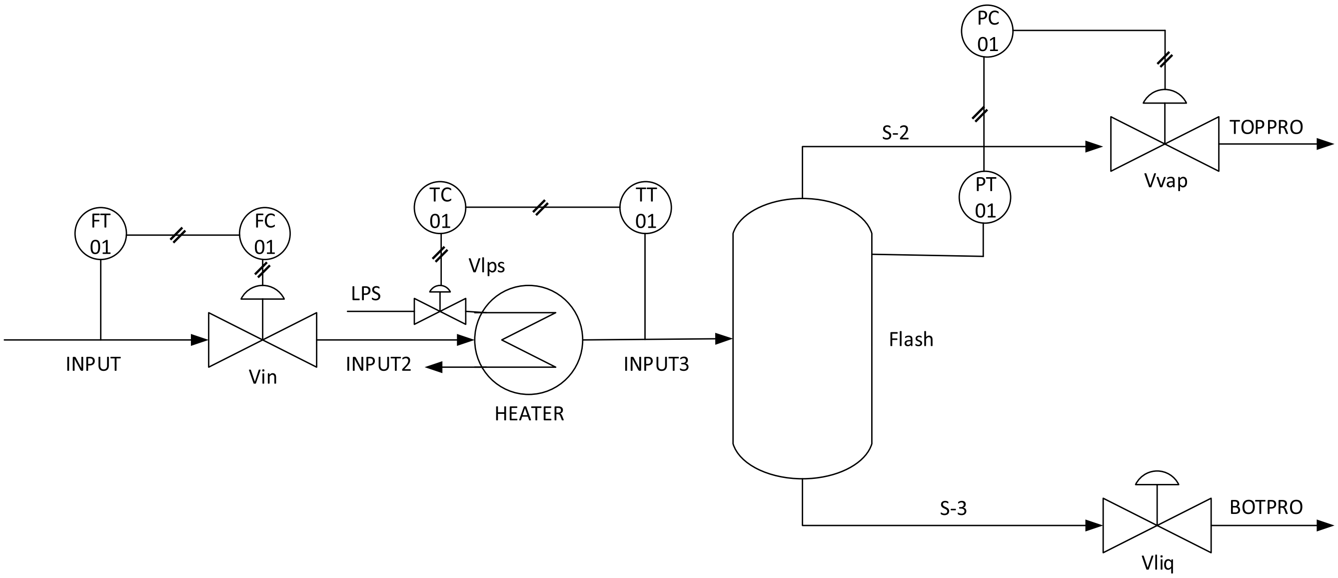


Figure 1. PFD of a continuous flash process.

Furthermore, if several candidates can be generated, it is necessary to evaluate them with reasonable criteria so as to identify the most suitable one. Generally speaking, previous works not only lacked efforts in verification and assessment of the synthesized procedures but also did not produce benchmark examples to establish their legitimacy for practical implementations. To fully address the above concerns, a design approach has been developed in a recent study[4] for the synthesis, validation, and evaluation of alternative SFCs based on the untimed automata and dynamic simulation. Although satisfactory results were reported in this recent work, there is still an unsettled practical issue that may hinder applications of the proposed approach in practice. Specifically, due to budget constraints or technical difficulties, some of the online measurements required in the operating procedure may not be obtainable.

The objective of this study is thus to circumvent the above problem by developing a new modeling approach to build the timed automata for the purpose of incorporating the elapsed times of various events (or actions) into the system model. By guiding the system with the so-called control specifications,[5] both the shortest-duration and fewest-event traces can be extracted with software UPPAAL[2,3] (version 4.0) and every such trace summarized with a sequential function chart. Note that, in the case when a needed online sensor is lacking, the elapsed time of an operation step can be stipulated in the corresponding activation condition of SFC, according to the information embedded in the trace mentioned above. Of course, this SFC should also be simulated and verified with Aspen Plus Dynamics (version 8.4). If the test results show that any SFC is unsafe and/or infeasible, one should discard/modify some of the control specifications and repeat the procedure synthesis steps. Two examples are presented in this paper to validate the proposed approach mentioned above.

2. TIMED AUTOMATA

A timed automaton is a finite-state machine equipped with one or more clock.[1] All clocks progress synchronously, and every one of them is described according to a dense-time model[1] in which the clock variable assumes a real positive value. To facilitate a 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

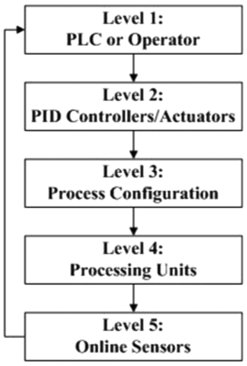


Figure 2. Hierarchical structure of a chemical process.

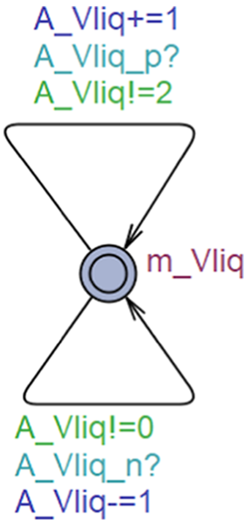


Figure 3. Component model of hand valve Vliq in the flash startup example.

$$TA = (L, l_0, C, A, I, E) \quad (1)$$

where L is a set of locations, $l_0 \in L$ is the initial location, C denotes the set of clock variables, and A is a set of actions. In addition, $I{:}L \rightarrow B(C)$ denotes a function $I(l) = b(c)$, which

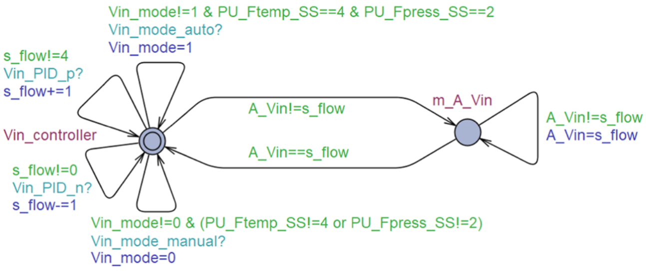


Figure 4. Component model of flow controller FC01 and control valve Vin in flash startup example.

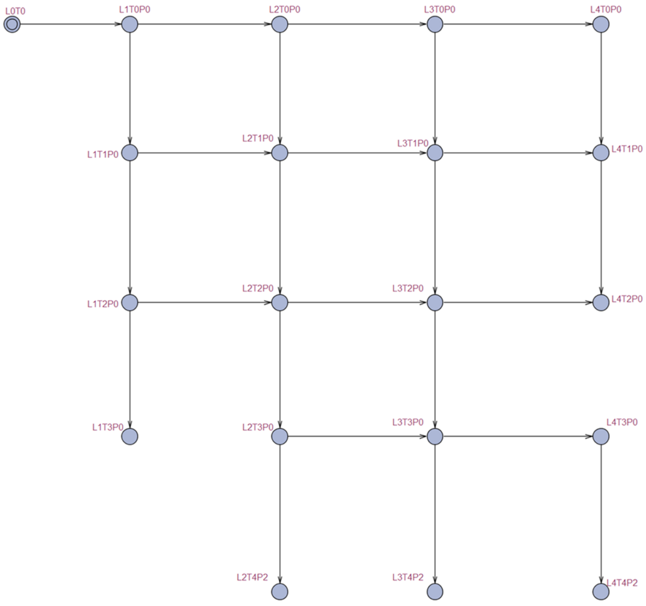


Figure 5. Component model of the flash drum in the flash startup example.

Table 1. Edge Specifications of Arc 1 in Figure 5

edge label	guards	updates
1.1	PU_Flevel == 0 & PU_Fin == 4 && x > = 1	PU_Flevel = 1, x = 0

Table 2. Edge Specifications of Arc 13 in Figure 5

edge label	guards	updates
13.1	PU_Ftemp == 1 & PU_Feng==1&A_Vvap==2&A_Vliq== 0 && x > = 8	PU_Ftemp = 2, x = 0
13.2	PU_Ftemp == 1 & PU_Feng == 2 & A_Vvap == 2 & PU_Fliq == 2 && x > = 6	PU_Ftemp = 2, x = 0

assigns invariant(s) to location l. Note that $B(C)$ denotes the set of conjunctions over simple conditions of the form $\{x \oplus c\}$ or $\{x - y \oplus c\}$, where $x, y \in C$, $c \in \mathbb{N}$, and $\oplus \in \{<, \leq, =, \geq, \geq\}$. 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 that belongs to the power set of C, i.e., 2^C.

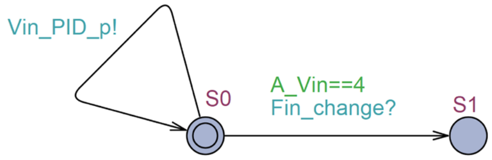


Figure 7. Automaton for supervision 1.

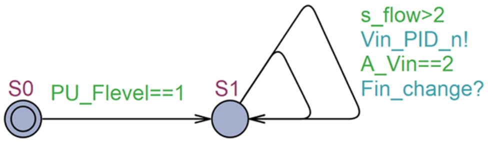


Figure 8. Automaton for supervision 2.

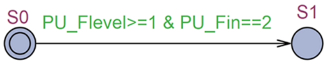


Figure 9. Automaton for supervision 7_stage 1.

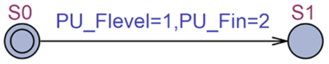


Figure 10. Automaton for stage 1_stage 2.

3. PROCESS STRUCTURE

To facilitate a clear illustration of the process structure, let us consider the startup operation of the continuous flash process in Figure 1 as an example. It is assumed that, in the steady state, the feed is a mixture of 30 wt % water and 70 wt % methanol and its flowrate, temperature, and pressure are kept at 1000 kmol/h, 25 °C, and 1.31 bar, respectively. The steady-state temperature and pressure of the top and bottom products are both set at 75 °C and 1.01 bar, respectively, while the corresponding liquid level is 2.5 m. It is also required that the concentration of methanol in the top product should not be lower than 87 wt %. In this system, there are three PID controllers (FC01, TC01, and PC01) for controlling the feed rate, the temperature, and the vapor pressure in the flash drum, respectively. The heating medium in the heater is assumed to be low-pressure steam. The corresponding actuators are control valves, i.e., Vin, Vlps, and Vvap. Notice that the level sensor and controller are not installed in this example for the purpose of demonstrating the use of elapsed time in the startup operation. Vliq is only a simple hand valve. It is also assumed that, initially, all valves are closed, all controllers are on MANUAL, and the flash drum is empty and at room temperature.

Every component in a given process is modeled with an automaton in this study. It has been well recognized that any chemical process can be described with a process flow diagram (PFD). Basically, every identifiable hardware item in the PFD is treated as a component in this work and they are classified into a five-level hierarchy as shown in Figure 2.

- Level 1: The top-level component is usually a human operator or a programmable logic controller (PLC).
- Level 2: The second-level components are the actuators, e.g., hand valves, control valves, and/or the corresponding PID controllers.

Figure 6. Ultimate target of the flash startup operation.

https://dx.doi.org/10.1021/acs.iecr.0c01427

Figure 11. Automaton for supervision 7_stage 2.

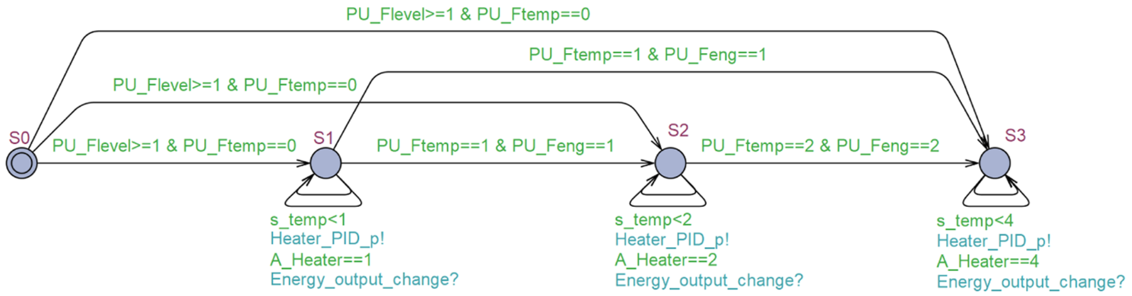


Figure 12. Automaton for supervision 3.

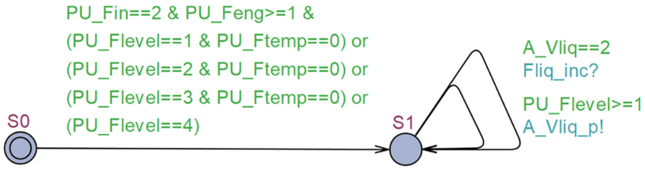


Figure 13. Automaton for supervision 4.

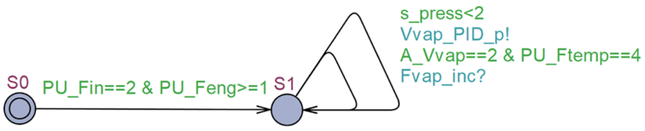
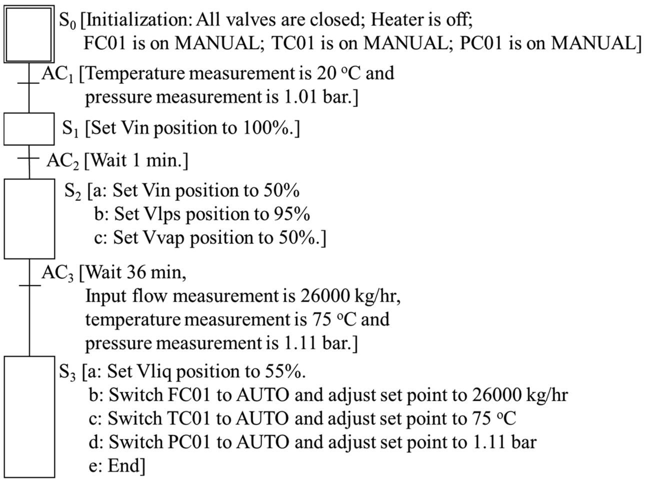


Figure 14. Automaton for supervision 5.

- Level 3: The material and energy flows among processing units in the given system are viewed as the components in the third level.
- Level 4: Every major unit operation in PFD, such as the flash drum itself in Figure 2, is treated as a fourth-level component.
- Level 5: Every online sensor in PFD, such as the flow, temperature, pressure sensors, etc., is a component in the last level.



S_0 [Initialization: All valves are closed; Heater is off;
FC01 is on MANUAL; TC01 is on MANUAL; PC01 is on MANUAL]

AC_1 [Temperature measurement is 20 °C and
pressure measurement is 1.01 bar.]

S_1 [Set Vin position to 100%.]

AC_2 [Wait 1 min.]

S_2 [a: Set Vin position to 50%
b: Set Vlps position to 95%
c: Set Vvap position to 50%.]

AC_3 [Wait 36 min,
Input flow measurement is 26000 kg/hr,
temperature measurement is 75 °C and
pressure measurement is 1.11 bar.]

S_3 [a: Set Vliq position to 55%.
b: Switch FC01 to AUTO and adjust set point to 26000 kg/hr
c: Switch TC01 to AUTO and adjust set point to 75 °C
d: Switch PC01 to AUTO and adjust set point to 1.11 bar
e: End]

Figure 18. Procedure to facilitate a flash startup within the shortest duration (SFC-1).

4. CONSTRUCTION OF COMPONENT MODELS

The building principles of component models on the platform of UPPAAL can be summarized as follows.

All possible states of the component are first enumerated and denoted with circles (locations) in the graphic representation of

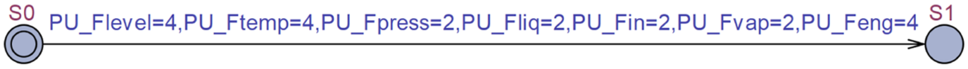


Figure 15. Automaton for stage 1_stage 2.

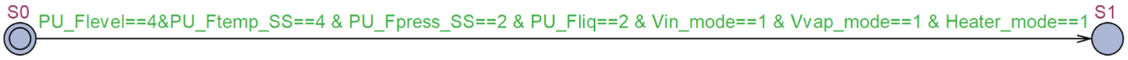


Figure 16. Automaton for supervision 7_stage 3.

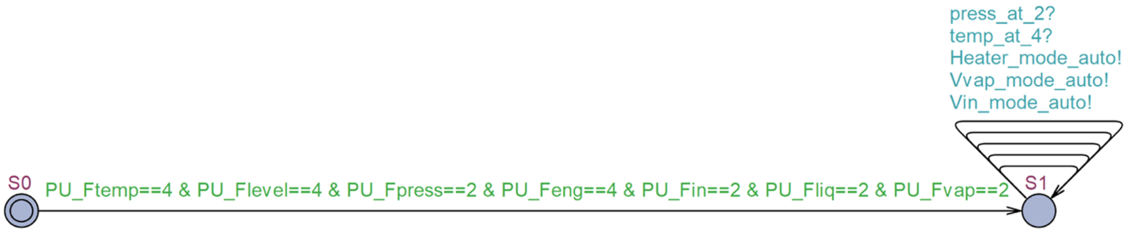
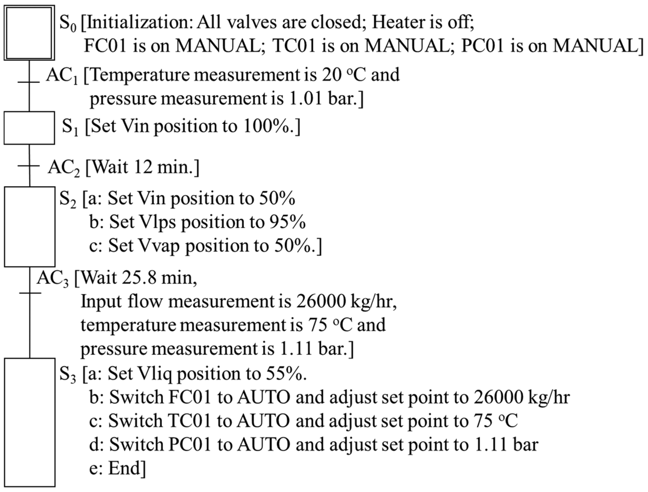


Figure 17. Automaton for supervision 6.



S_0 [Initialization: All valves are closed; Heater is off; FC01 is on MANUAL; TC01 is on MANUAL; PC01 is on MANUAL]

AC_1 [Temperature measurement is 20 °C and pressure measurement is 1.01 bar.]

S_1 [Set Vin position to 100%.]

AC_2 [Wait 12 min.]

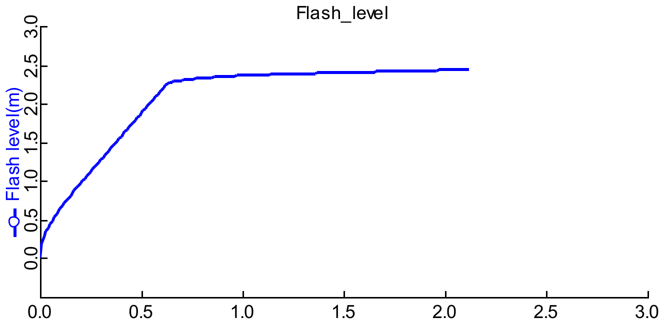
S_2 [a: Set Vin position to 50%
b: Set Vlps position to 95%
c: Set Vvap position to 50%.]

AC_3 [Wait 25.8 min,
Input flow measurement is 26000 kg/hr,
temperature measurement is 75 °C and
pressure measurement is 1.11 bar.]

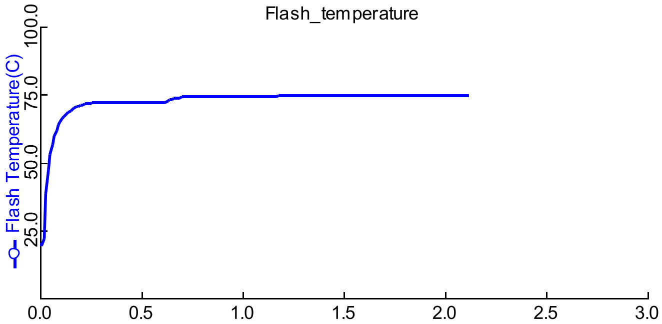
S_3 [a: Set Vliq position to 55%.
b: Switch FC01 to AUTO and adjust set point to 26000 kg/hr
c: Switch TC01 to AUTO and adjust set point to 75 °C
d: Switch PC01 to AUTO and adjust set point to 1.11 bar
e: End]

Figure 19. Procedure to facilitate a flash startup via fewest state transitions (SFC-2).

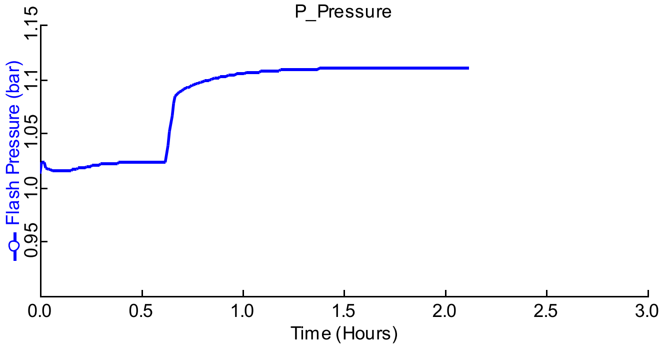
automaton. The initial state should be selected and the corresponding location indicated with double concentric circles. All events that facilitate state transition should then be identified and each described with a directed edge between two locations. The guards (marked in green), the update variable values (marked in purple), and the synchronization mechanism(s) should be next added on the corresponding edge. A synchronization mechanism is built with the event label (marked in blue). The "receiver" event is attached with a question mark (?), indicating that such an event must occur in other components at some prior instance. On the other hand, the exclamation mark (!) is used to specify an initiator or "sender" event that takes place in a component as long as all prerequisite conditions (guards) can be satisfied. Notice also that if an event takes place almost instantaneously, then it is not necessary to specify the elapsed time as one of the guards. In this study, only the state transition time of every event in the component model of each processing unit in the 4th level of the system hierarchy is estimated on the basis of ASPEN simulation results. For the sake



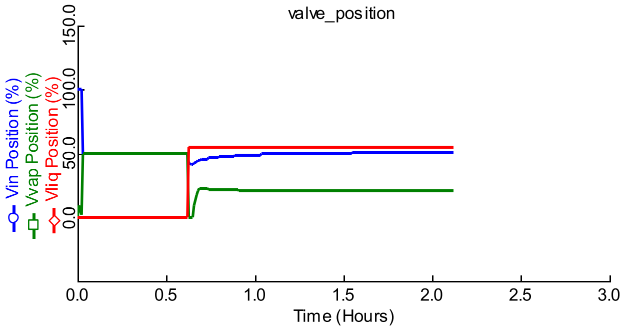
(a) Liquid level in flash drum



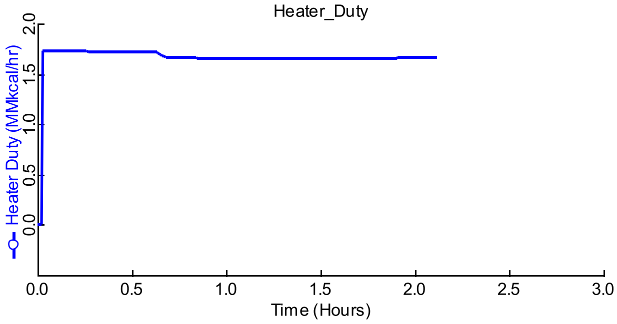
(b) Temperature in flash drum



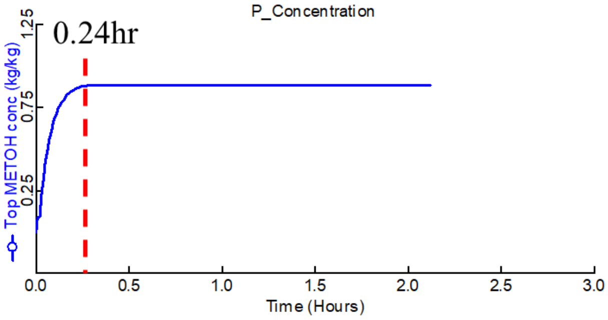
(c) Pressure in flash drum



(d) Inlet and outlet valve openings

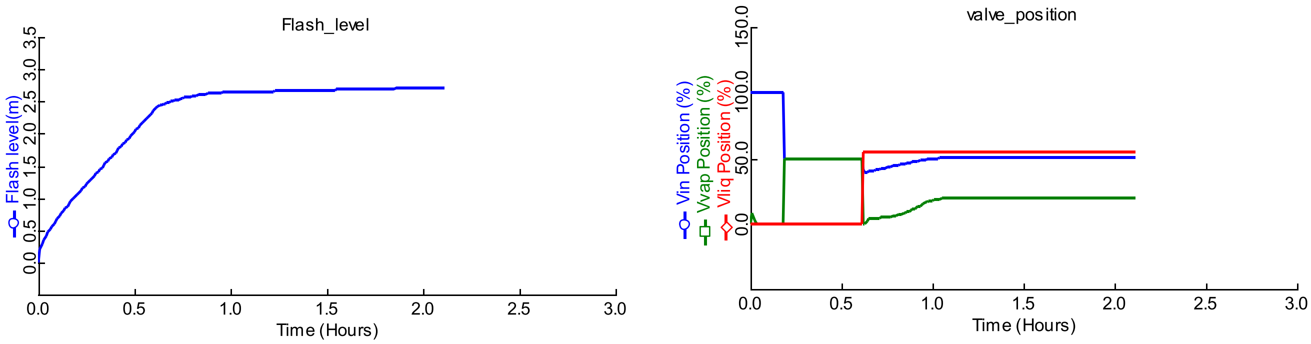


(e) Heater duty



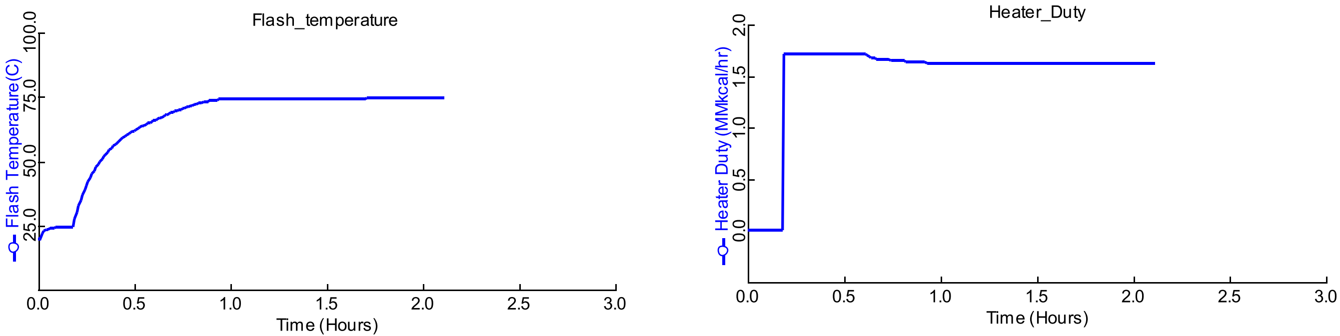
(f) Methanol concentration in overhead stream

Figure 20. Time profiles of state and manipulated variables simulated for SFC-1.



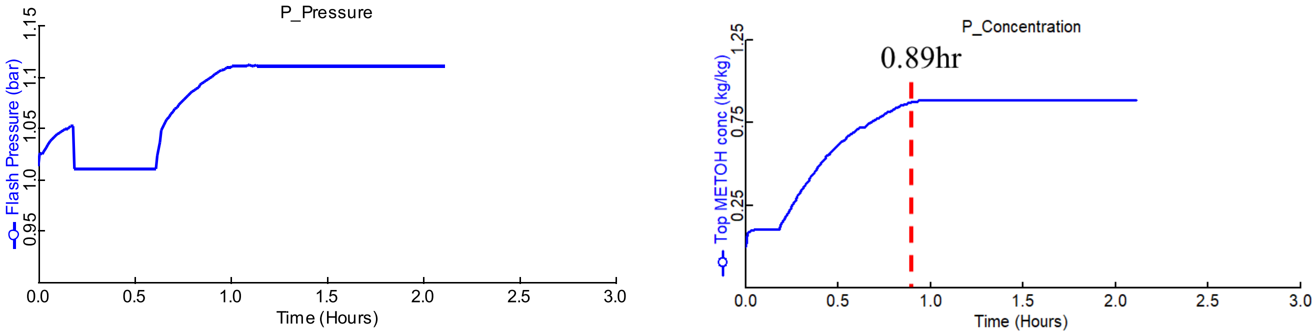
(a) Liquid level in flash drum

(d) Inlet and outlet valve openings



(b) Temperature in flash drum

(e) Heater duty



(c) Pressure in flash drum

(f) Methanol concentration in overhead stream

Figure 21. Time profiles of state and manipulated variables simulated for SFC-2.

of illustration brevity, the required discretization and simulation procedures are presented in Part A of the Supporting Information.

It is clearly not possible to construct an automaton at this point to describe the level-1 component, i.e., PLC or human operator, since the operating procedure is not available a priori. For illustration conciseness, let us consider in the present section only the components in level 2, i.e., the actuators and the PID controllers, and level 4, i.e., the flash drum, as examples. All component models in the other levels and a layer model for integration according to Figure 2 can be found in Part B of the Supporting Information.

4.1. Actuators and PID Controllers.

As an example, let us first construct a simple automaton for characterizing the outlet hand valve Vliq in the flash startup process, according to the model building principles presented above. This model is given in Figure 3. As described in Part A of the Supporting Information, the valve position is discretized into five levels (from 0 to 4) and, thus, the guards of the two events in this model, i.e., A_Vliq_p? (increase the valve opening) and A_Vliq_n? (reduce the valve opening), are specified as A_Vliq! = 4 and A_Vliq! = 0, i.e., the valve position is not fully open and closed, respectively. Notice also that the above two events are receivers and the corresponding senders can be found in the "layer" model given in Part B of the Supporting Information. Finally, note that the variable A_Vliq on either loop is updated with a C-like code, i.e., A_Vliq += 1 (or A_Vliq = A_Vliq + 1) and A_Vliq −= 1 (or A_Vliq = A_Vliq − 1),

The flow control valve Vin and the corresponding controller FC01 are next modeled with the automaton in Figure 4. The location Vin_controller and the edges attached to it in this model are used to describe the controller behavior of FC01, while location m_A_Vin and its corresponding edges are for characterizing valve Vin.

Note that there are four self-looping edges on location Vin_controller. The top and bottom ones are associated with receiver events Vin_mode_auto? and Vin_mode_manual?, respectively. These two events are actions to switch the controller mode from MANUAL (Vin_model = 0) to AUTO (Vin_model = 1) and vice versa. Note also that the guards of the former event are the targeted steady-state conditions reached

Table 3. Performance Indices of SFC-1 and SFC-2

	amounts of off-spec products (kg)			
SFC no.	top	bottom	total amount of energy consumed (MMkcal)	total operation time (min)
SFC-1	3490.89	34 445.95	3.51	37
SFC-2	2286.27	33 917.80	3.18	51

when the controller is still on MANUAL and those of the latter are conditions when the steady state is not reached.

On the other hand, the middle two loops are associated with receiver events Vin_PID_p? and Vin_PID_n? and they are actions to adjust the controller output toward positive (s_flow += 1) and negative (s_flow −= 1) directions, respectively. The guards of the two events are imposed to ensure that the adjustments are feasible. If either event is triggered, then the guard of the edge from location Vin_controller to location m_A_Vin should be satisfied and, subsequently, the prerequisite on the self-looping edge of the latter location is also met. Note that the event associated with the loop on m_A_Vin is to reset the valve opening to that corresponding to the adjusted controller output, i.e., A_Vin = s_flow. As a result, the guard on the edge from location m_A_Vin to location Vin_controller should be satisfied and, thus, the component state should then return to Vin_controller and wait for the next request to alter the controller output.

4.2. Flash Drum. As mentioned before, since the elapsed period of every state-transition event of flash drum is not negligible, it is necessary to estimate these time intervals via test runs using Aspen Plus Dynamics. The test procedure is detailed in Part A of the Supporting Information, and the corresponding simulation results (i.e., the time profiles of discretized liquid level, temperature, and pressure in flash drum) are presented in Figures A1−A4. By extracting the event times from these data, a timed automaton can be constructed to model the flash drum (see Figure 5).

In this automaton, the component states of the flash drum are represented by the locations and each is described with three variables, i.e., level, temperature, and pressure. For example, the initial location L0T0P0 denotes that the flash drum is at a state that can be characterized by the specific discretized values of the liquid level, temperature, and pressure, i.e., 0 (0 m), 0 (20 °C), and 0 (1.01 bar), respectively. Note also that every directed arc in Figure 5 may consist of more than one edge and a detailed listing of their guards and updated variables can be found in Part C of the Supporting Information. To further illustrate the structure of this automaton, let us consider arc 1 and arc 13 as examples. The specifications of the corresponding edges are given in Tables 1 and 2. Notice first that every event label of each edge is numerically represented since it is neither a sender nor a receiver.

From Figure 5 and Table 1, it can be observed that there is only one edge between L0T0P0 and L1T0P0, i.e., edge 1.1. Its guards imply that, to trigger the corresponding state transition, the liquid level should be at the lower bound (0) and inlet flowrate at the upper limit (4). Notice that these two prerequisites are connected by the AND operator (&), while the additional requirement on clock variable, i.e., $x \geq 1$, is incorporated with a double AND operator (&&). After all guard conditions are met, the liquid level can be updated to the discretized value of 1 and the clock variable is reset to 0.

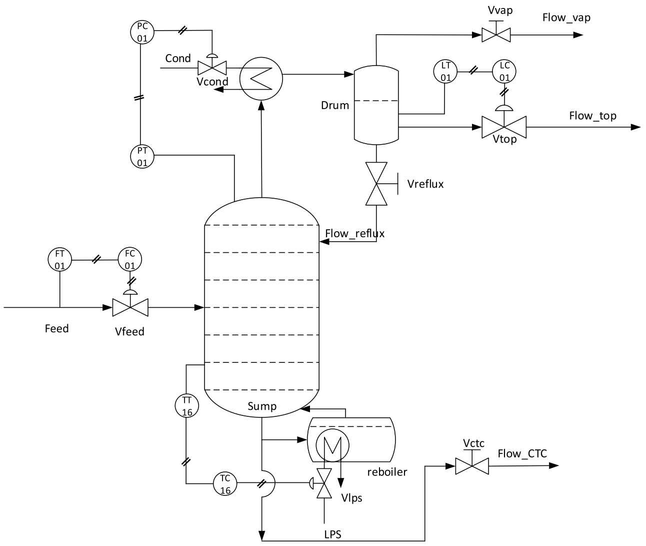


Figure 22. PFD of a continuous distillation process.

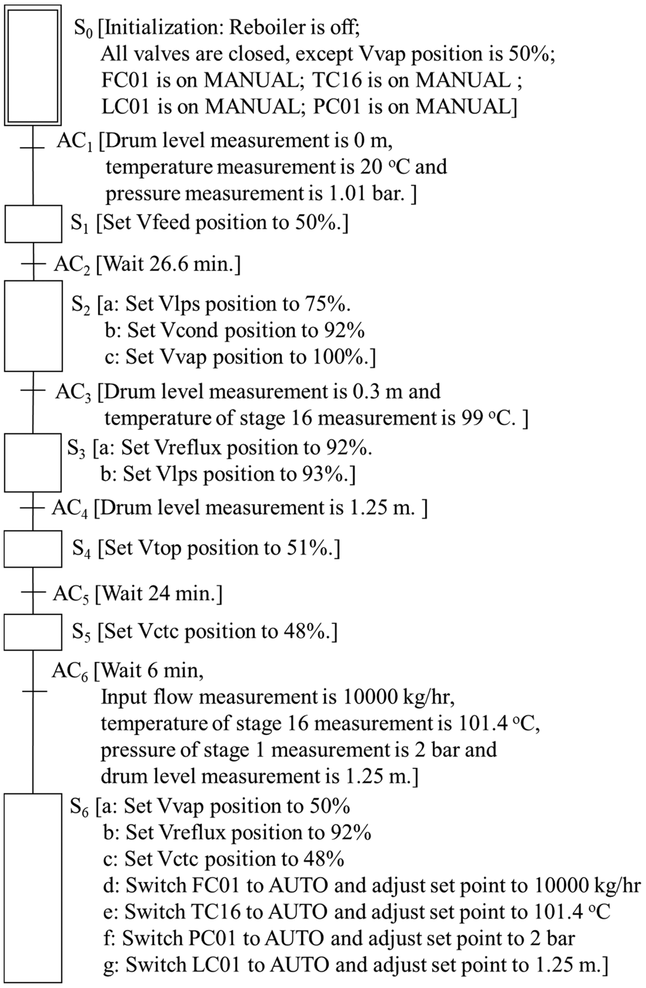
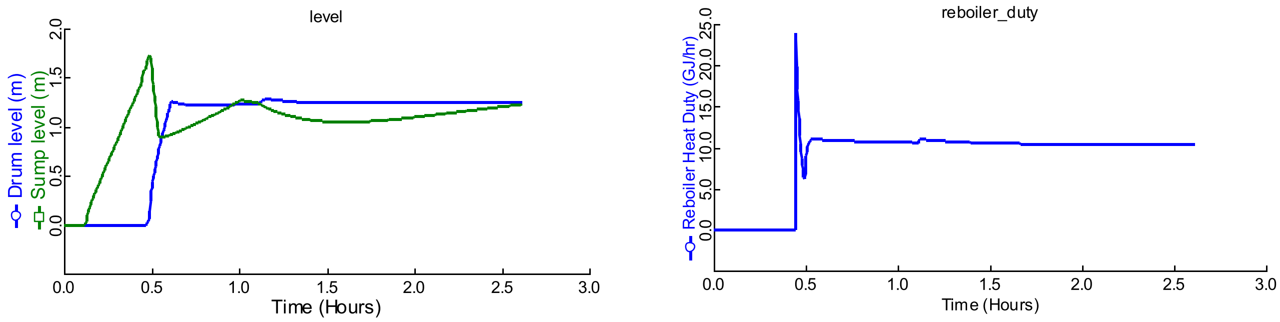

S_0 [Initialization: Reboiler is off;
All valves are closed, except Vvap position is 50%;
FC01 is on MANUAL; TC16 is on MANUAL ;
LC01 is on MANUAL; PC01 is on MANUAL]
AC_1 [Drum level measurement is 0 m,
temperature measurement is 20 °C and
pressure measurement is 1.01 bar.]
S_1 [Set Vfeed position to 50%.]
AC_2 [Wait 26.6 min.]
S_2 [a: Set Vlps position to 75%.
b: Set Vcond position to 92%
c: Set Vvap position to 100%.]
AC_3 [Drum level measurement is 0.3 m and
temperature of stage 16 measurement is 99 °C.]
S_3 [a: Set Vreflux position to 92%.
b: Set Vlps position to 93%.]
AC_4 [Drum level measurement is 1.25 m.]
S_4 [Set Vtop position to 51%.]
AC_5 [Wait 24 min.]
S_5 [Set Vctc position to 48%.]
AC_6 [Wait 6 min,
Input flow measurement is 10000 kg/hr,
temperature of stage 16 measurement is 101.4 °C,
pressure of stage 1 measurement is 2 bar and
drum level measurement is 1.25 m.]
S_6 [a: Set Vvap position to 50%
b: Set Vreflux position to 92%
c: Set Vctc position to 48%
d: Switch FC01 to AUTO and adjust set point to 10000 kg/hr
e: Switch TC16 to AUTO and adjust set point to 101.4 °C
f: Switch PC01 to AUTO and adjust set point to 2 bar
g: Switch LC01 to AUTO and adjust set point to 1.25 m.]

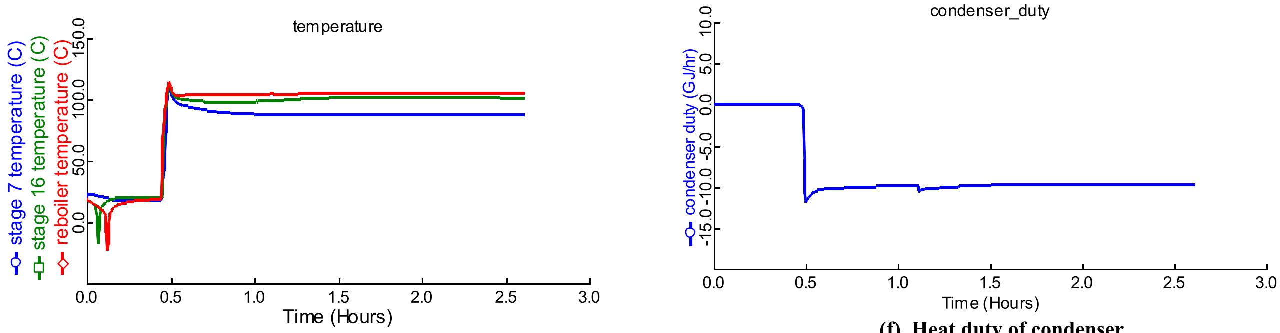
Figure 23. SFC-3: the best operating procedure for the distillation startup.

From Figure 5 and Table 2, it can be observed that there are two edges between L2T1P0 and L2T2P0, i.e., edge 13.1 and edge 13.2. The common guards of these two edges are PU_Ftemp == 1 (the temperature in the flash drum is at the discretized value of 1) and A_Vvap == 2 (the opening of vapor



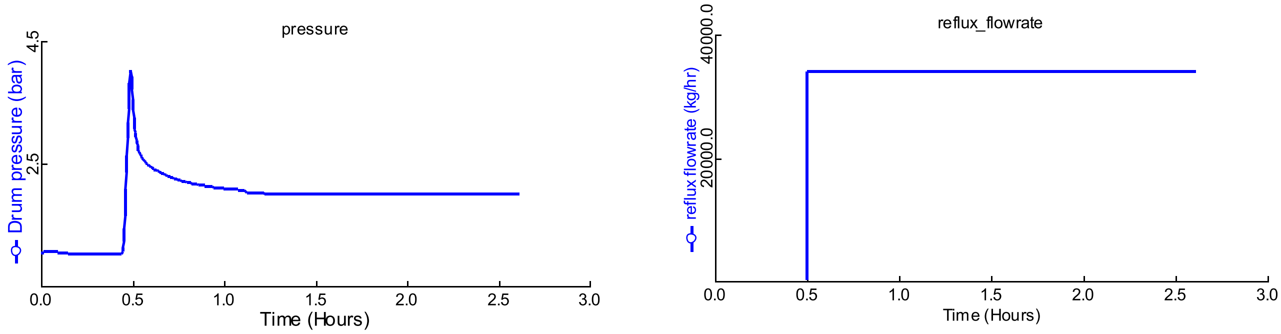
(a) Liquid levels in reflux drum and column sump

(e) Heat duty of reboiler



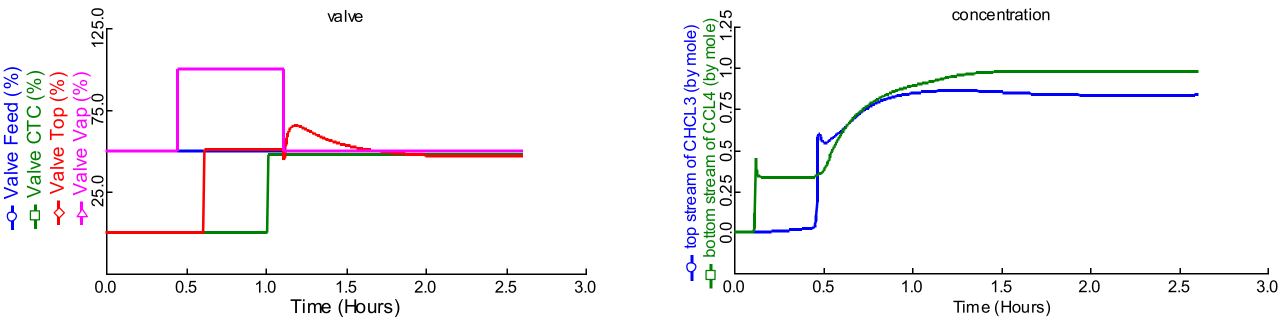
(b) Temperatures at plates 7, 16 and reboiler

(f) Heat duty of condenser



(c) Pressure in reflux drum.

(g) Reflux flow rate



(d) Valve openings of V_{feed}, V_{ctc}, V_{top} and V_{vap}

(h) Concentrations of light and heavy keys in the top and bottom product

Figure 24. Simulation results of the distillation startup operated according to SFC-3.

valve is at the discretized value of 2). On the other hand, the net effect of the energy input in the two scenarios should both be positive. Notice that although the heating rate of the former (PU_Feng == 1) is slower than that of the latter (PU_Feng == 2), the energy output rate via liquid outlet flow for edge 13.1 (A_Vliq == 0) is also smaller than that for edge 13.2 (PU_Fliq == 2). Notice also that the event time of the former ($x > = 8$) is longer than that of the latter ($x > = 6$). After all guard conditions on either edge are met, the drum temperature can be transferred from the discretized value of 1 to 2 and the clock variable is again reset to 0.

5. ADDITIONAL MODEL CONSTRAINTS

The proper operation paths can obviously be extracted from a system automaton obtained by synchronizing all component models with an automaton that specifies the final target of the operation. This target-setting automaton for the flash startup operation is given in Figure 6. However, since the above system automaton is only loosely constrained by the final goal, an overwhelmingly large number of unnecessary pathways may be generated. Specifically, the above synchronization operation performed by UPPAAL inevitably yielded a complicated and unmanageable pathway network for the flash startup example.

Although the ultimate goal of a specific operation can be unambiguously given (e.g., Figure 6), it can be appropriately approached via a series of intermediate stages with interim goals that are often not explicitly stipulated a priori. It is thus important to uncover these embedded subtasks and identify their operational features explicitly in advance. These features may be broadly classified as (1) material charging, (2) material unloading, (3) reaction, (4) state adjustment, (5) phase change, (6) stable operation, etc. All such features of a stage are expressed as the "control specifications" in the natural language in this study and then modeled with automata accordingly.[5]

For illustration purposes, let us revisit the flash startup process. Based on engineering knowledge and operational experience, it is clearly necessary to place a small quantity of raw material in the flash drum first and allow the liquid level reaching a height that is safe for intense heating. In the next stage, the temperature and pressure in the drum should be elevated to the set points and the input and output flow rates be raised to the steady-state levels. Finally, the stable operating conditions should be maintained for a relatively long period of time with the PID controllers.

The control specifications in all stages are detailed in the sequel.

5.1. Control Specifications for Stage 1. To save the charging time in stage 1, the inlet valve is opened fully before reaching the liquid level designated for heating to start. At this designated level, the inlet valve opening is supposed to be reduced to 50%, which is the steady-state value. These two requirements can be expressed by supervision 1 in Figure 7 and specification 2 in Figure 8, respectively. Also, the interim goals of stage 1 should be achieved if the liquid level in drum exceeds a discretized value of 1, i.e., between 0 and 0.8 m, and the inlet flowrate is adjusted to 2 (50%). This stage goal is represented by the automaton supervision 7_stage 1 in Figure 9.

5.2. Control Specifications for Stage 2. Since the second stage starts right after stage 1, it is necessary to build an automaton to facilitate pathway connection between the two (see Figure 10). Note that the critical initial conditions of stage 2 are updated on the arc from S0 to S1 directly in this automaton. On the other hand, the interim goals of stage 2 are to drive all operating conditions to their steady-state values. These goals are also specified as the guards on the arc from S0 to S1 in the corresponding automaton in Figure 11.

To achieve these interim goals, the valves Vlps, Vliq, and Vvap should be navigated according to Figure 12−14, respectively. As mentioned before, the heating is supposed to begin after the liquid level reaches a discretized value greater than or equal to 1 and the temperature is at 0 (20 °C). From Part A of the Supporting Information, it can be observed that the heating rate has been discretized into four values, i.e., 0 (0 MMkcal/h), 1 (0.5 MMkcal/h), 2 (0.9 MMkcal/h), and 3 (1.68 MMkcal/h). Thus, all heating sequences can be enumerated exhaustively as follows: (1) 0 → 3; (2) 0 → 2 → 3; (3) 0 → 1 → 3; and (4) 0 → 1 → 2 → 3. These sequences are described with the automaton in Figure 12 (i.e., supervision 3). Note that sequence (1) is facilitated by the arc pointing from place S0 to place S3. Note also that the guard of one of the self-looping arcs on S3, that is, s_temp < 4 (which means the output of temperature controller is lower than the discretized value of 4 or 94%), is satisfied initially, and the corresponding sender event Heater_PID_p! is then triggered repeatedly to raise the controller output signal until the guard of the other self-looping arc, i.e., A_Heater == 4 (which means the opening of the control valve of the heating medium equals the discretized value of 4 or 94%), is satisfied. At this point, the receiver event Energy_output_change? can be activated so as to complete the heating sequence 0 → 3. On the other hand, sequence (2) is facilitated first by the arc pointing from place S0 to place S2 and then by another from place S2 to place S3. Note that the guards of the former arc are the same as those of the initial arc in sequence (1) and the guards of the latter are PU_Ftemp == 2 and PU_Feng == 2, which imply that the discretized values of both temperature and heat input must be raised to 2 before changing the heating rate. Since the self-looping arcs on S2 can be interpreted in the same way as those on S3, their descriptions are not repeated for the sake of brevity. Finally, since sequences (3) and (4) can be characterized in a similar fashion as (1) or (2), their explanations are also omitted.

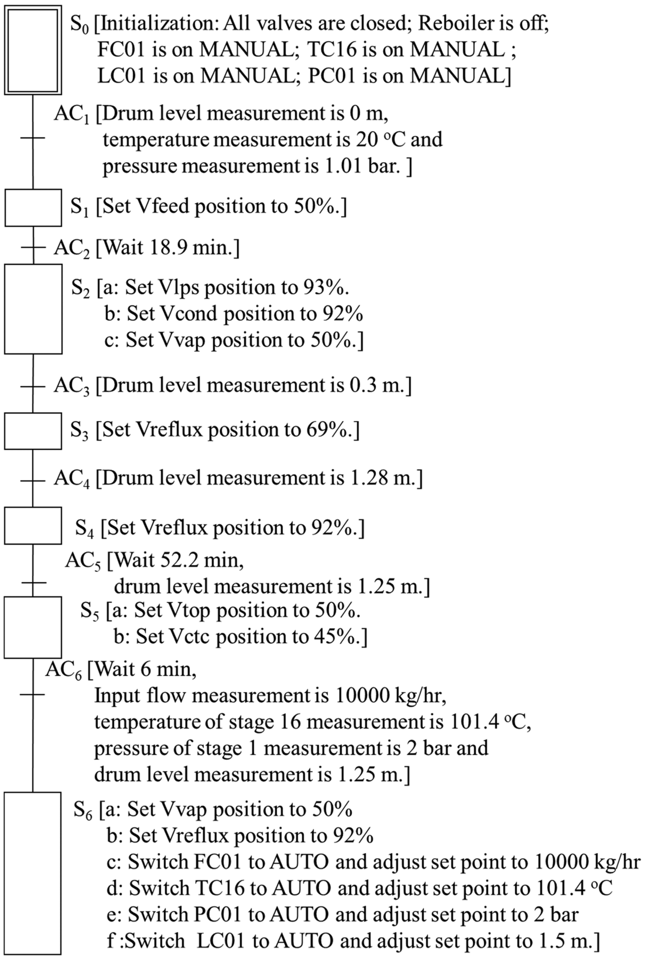


Figure 25. SFC-4: an unsafe operating procedure for the distillation startup.

5.3. Control Specifications for Stage 3. Because stage 3 immediately follows stage 2, it is necessary to use an automaton to forge a connection between the two (see Figure 15). Since stage 3 is also the final stage, its goal should be completing the startup operation (see Figure 16). To achieve this goal, all controllers should be switched from the MANUAL mode to the AUTO mode after the steady-state conditions are reached (see Figure 17).

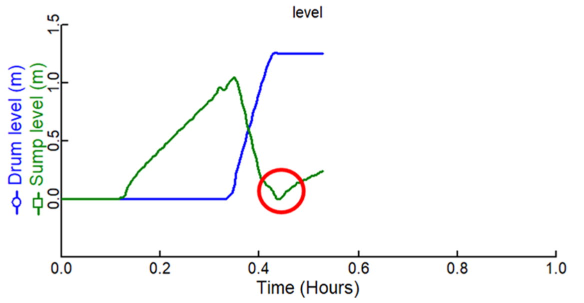


Figure 26. Simulated liquid levels in the reflux drum and column sump during the distillation startup operated according to SFC-4.

6. PROCEDURE SYNTHESIS

The verification tool of UPPAAL is used in the study to search for the proper operation path within the real-time system. Specifically, the optimal pathway in every stage is synthesized in four distinct steps:

(i) build the automaton models of all components in the uncontrolled plant;
(ii) construct automata to represent the control specifications in every stage;
(iii) synchronize all automata created in the above two steps with parallel composition for each stage; and
(iv) execute suitable property verification function in UPPAAL so as to locate the best operation pathway in each stage.

The aforementioned operation pathways in all stages can then be pieced together to produce a procedure to facilitate the shortest operation duration or fewest state transitions. The former procedure is summarized in the sequential function chart (SFC-1) in Figure 18, while the latter is expressed with SFC-2 in Figure 19.

The procedures in SFC-1 and SFC-2 can both be summarized as follows: The operator/PLC first opens the inlet valve Vin fully, waits for x ($x = 1$ or 12) min, and then adjusts the inlet valve Vin to a half-open position, the steam valve Vlps to 95%, and the overhead vapor valve to 50%. After waiting for another y ($y = 36$ or 25.8) min, the operator/PLC opens the bottom liquid valve to 55%, switches all PID controllers from the MANUAL to AUTO mode, and fixes their set points at the steady-state operating conditions.

7. SIMULATION STUDIES

SFC-1 and SCF-2 have been converted to the Task files for simulation runs in Aspen Plus Dynamics, and the simulation results are presented in Figures 20 and21, respectively. Note that the target concentration in the overhead stream (87 wt %) is reached at 0.24 h in the former case and 0.89 h in the latter. The above two procedures are also compared on the basis of several performance indices in Table 3. It can be observed that although the total operation time of SFC-1 is shorter than that of SFC-2, the total amounts of off-spec products and energy consumed in the former case are both greater than those in the latter.

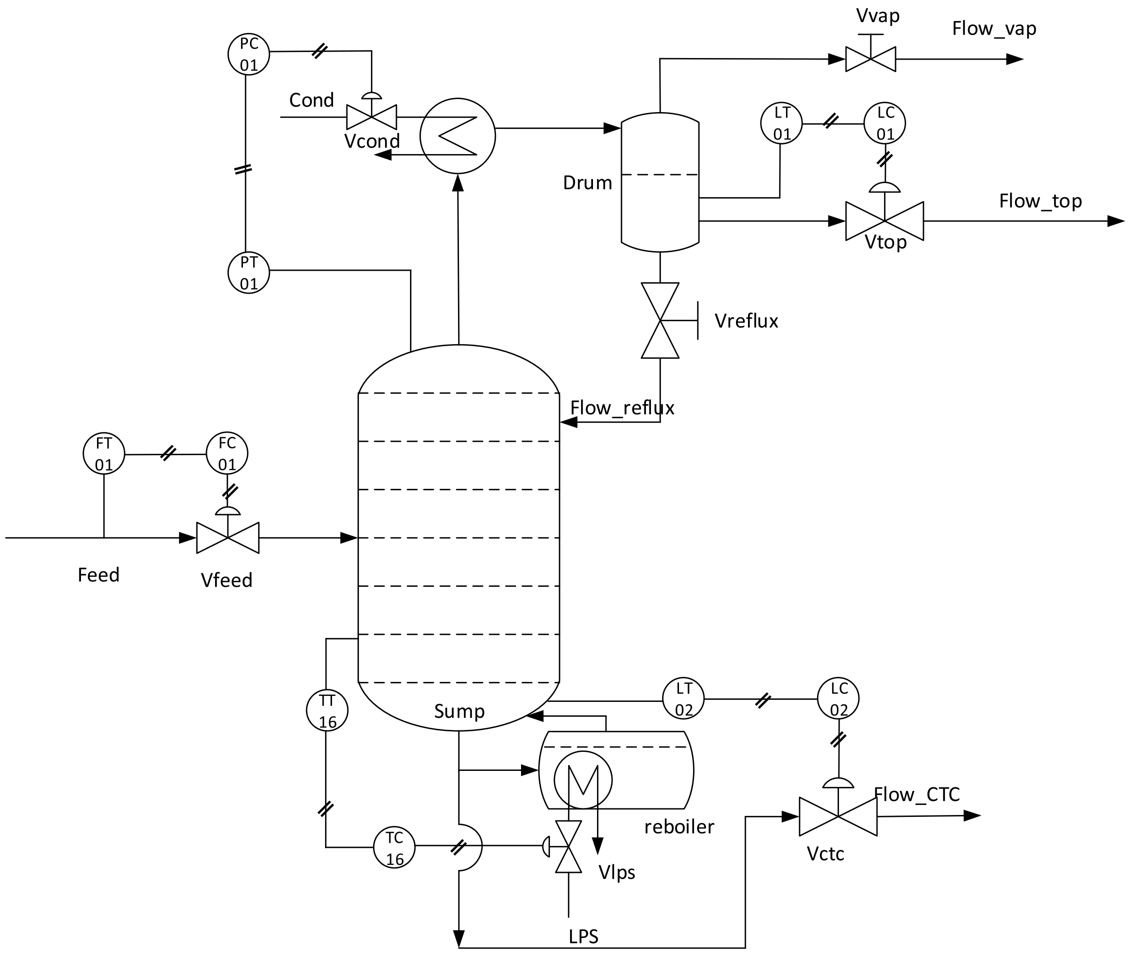


Figure 27. PFD of a continuous distillation process used in the ASPEN built-in example.

8. ADDITIONAL CASE STUDIES

To demonstrate the feasibility of the proposed approach in more practical applications, a realistic example is presented in this section. Let us consider the startup operation of the continuous distillation process described in Figure 22. It is assumed that, in the steady state, the feed is a mixture of 6 wt % CH_2Cl_2, 54 wt % $CHCl_3$, and 40 wt % CCl_4 and its flowrate, temperature, and pressure are kept at 10 000 kg/h, 20 °C, and 6 bar, respectively. The total number of plates in the distillation column is 20, while the feed is directed toward the 10th plate. The steady-state set-point temperatures at the condenser and reboiler are 80.3 and 105.0 °C, respectively. The steady-state reflux ratio is 5 mol/mol. The steady-state pressure settings at plate 1/condenser and plate 2 are chosen to be 2.00 and 2.02 bar, respectively, while the column pressure drop from the bottom is 0.235 bar. It is also required that the concentration of light key ($CHCl_3$) in the top product should be greater than 81 mol % and that of heavy key (CCl_4) in the bottom product should not be lower than 98 mol %. In this system, there are four PID controllers (FC01, TC16, PC01, and LC01) for controlling the feed rate, the temperature on the 16th plate, the top-plate pressure, and the liquid level in the reflux drum, respectively. The corresponding control valves are Vfeed, Vlps, Vcond, and Vtop. It is assumed that, before the startup operation, all valves are closed, all controllers are on MANUAL, and the reflux drum and column sump are both empty and at room temperature.

Finally, it should be noted that the startup operation of this system has also been used in Aspen plus Dynamics as a built-in example. Since the primary objective of the present case studies is to demonstrate the usefulness of the time-automata-based modeling approach, the sump level controller adopted in the ASPEN built-in example has been deliberately excluded (see Figure 22) for the illustration purpose.

8.1. Operation Stages Identified with Engineering Knowledge. Similar to the startup of the flash drum, it is also necessary to place a small quantity of the raw material in the column sump first and ensure the liquid level reaching a height that is safe for intense heating. To allow this inlet flow, the outlet vapor valve (Vvap) should be partially open in advance. During the second stage, the heat input into the reboiler and heat output from the condenser should both be started to facilitate countercurrent vapor and liquid flows in the column. The product flows at the top and bottom should then be drawn consecutively from the column in the third stage to initiate the continuous operation. Finally, the stable operating conditions should be maintained after all set points are reached for a relatively long period of time with the PID controllers.

8.2. Feasible Operating Procedures. By piecing together the automata-generated operation pathways obtained for achieving the interim goals of the aforementioned four stages, 33 different operating procedures were created. Among them, four were considered to be unsafe for the distillation startup on the basis of simulation results. The remaining feasible procedures were compared according to five performance indices. i.e., the total amounts of off-spec top and bottom products, the total amounts of heating and cooling utilities, and the total operation time. The best one is summarized by SFC-3 in Figure 23, while the corresponding ASPEN simulation results can be found in Figure 24. The corresponding Task file can be found in Part D of the Supporting Information.

Notice from both Figures 23 and 24 that all valves in this system are closed initially, except that Vvap is at the 50% position. After confirming the designated initial conditions in AC_1, the inlet valve Vfeed is set to the 50% position to fill the column sump with liquid. The next "activation condition" is the elapsed time of the subsequent waiting period (26.6 min). It can be observed from Figure 24a that, since the feed enters the column at the 10th plate, the height of the liquid level in the sump remains at 0 m initially for a period of approximately 10 min. In other words, it takes about the same amount of time for feed to travel from the inlet to the sump. Notice also from Figure 24b that the temperatures at plate 16 and the reboiler dip consecutively to below 0 °C during this 10 min period and then immediately recover to around 20 °C. These dips occur at instances when the simulated downward feed flow reaches the corresponding locations, and it should be noted that they may not be real in actual operation. During the next period from 10 to 26.6 min, the height of the liquid level in the sump rises continuously before heating in the reboiler and cooling in the condenser begin, i.e., the flows of heating and cooling media are started at this instance by opening *Vlps* (75%) and *Vcond* (92%), respectively. At the same instance when these two valves are opened, *Vvap* is adjusted to 100% to avoid drastic overpressure in the reflux drum. Notice also that the height of the liquid level in the column sump drops shortly afterward, while that in the reflux drum begins to rise simultaneously. Next, when there is enough liquid in the reflux drum (i.e., its level reaches 0.3 m) and the

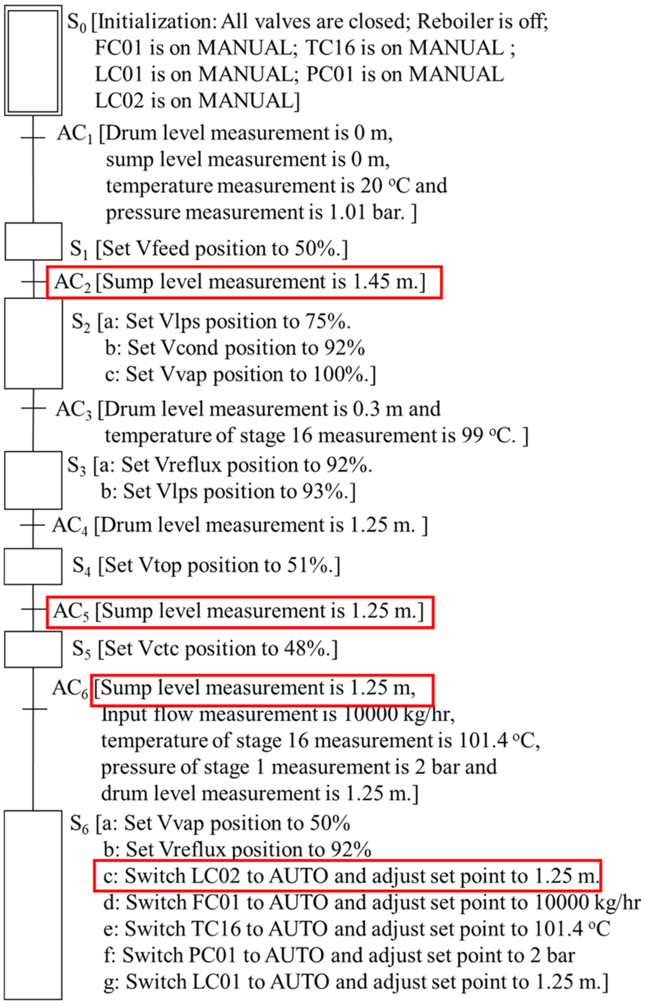
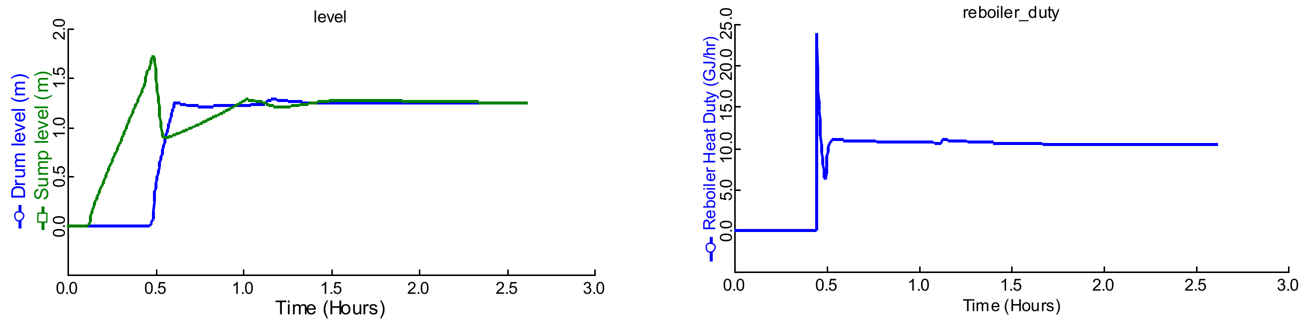
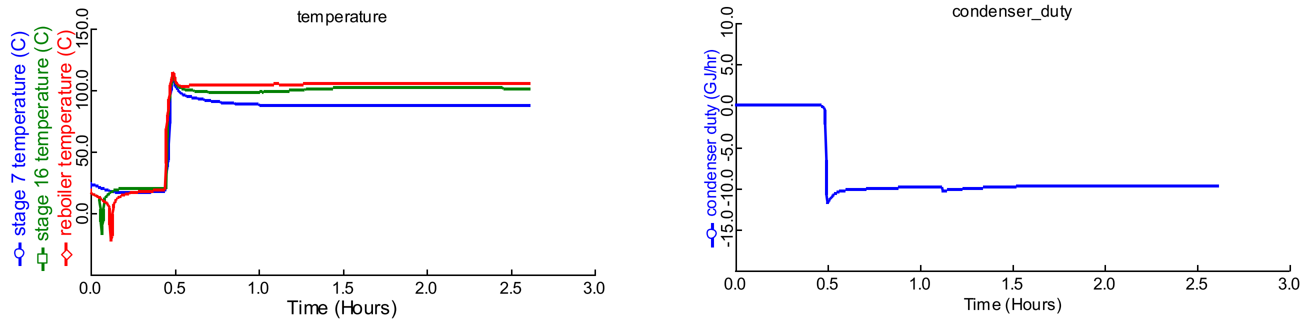


Figure 28. SFC-5: the best operating procedure for the distillation startup with an extra level control loop in the column sump.



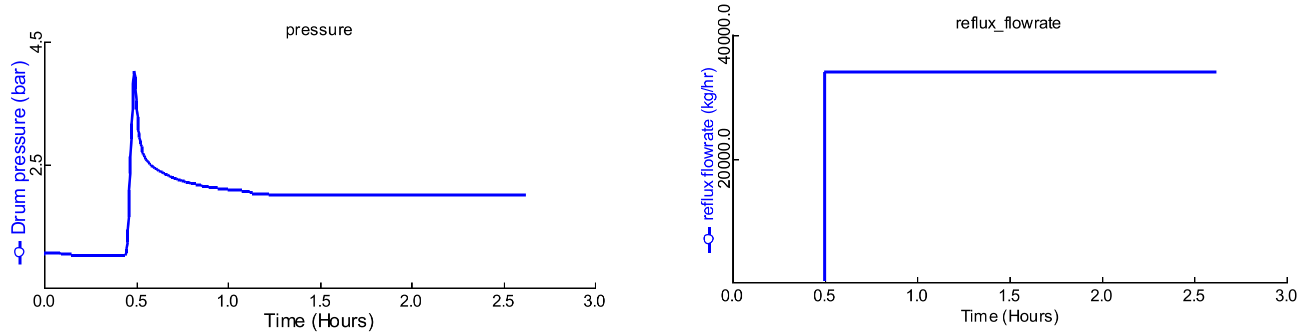
(a) Liquid levels in reflux drum and column sump

(e) Heat duty of reboiler



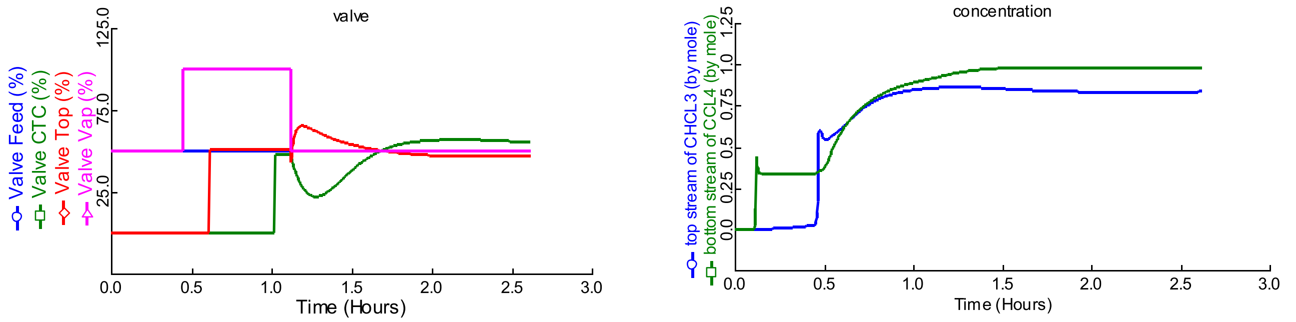
(b) Temperatures at plates 7, 16 and reboiler

(f) Heat duty of condenser



(c) Pressure in reflux drum.

(g) Reflux flow rate

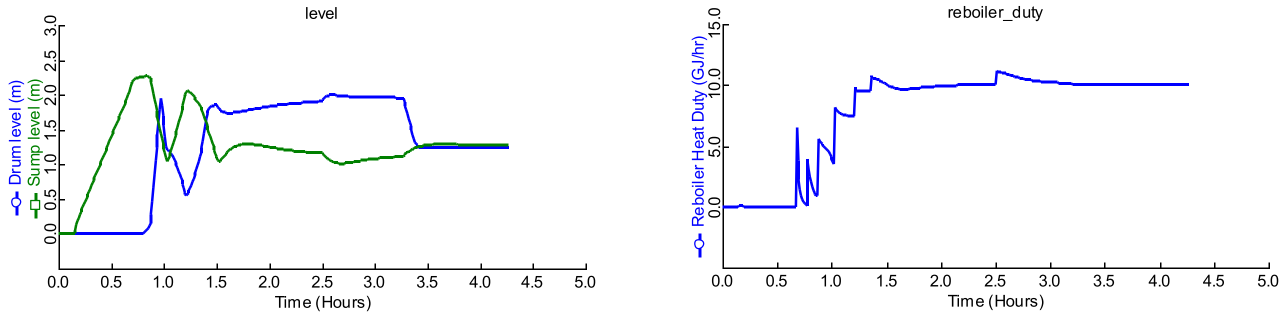


(d) Valve openings of V_{feed}, V_{ctc}, V_{top} and V_{vap}

(h) Concentrations of light and heavy keys in the top and bottom products

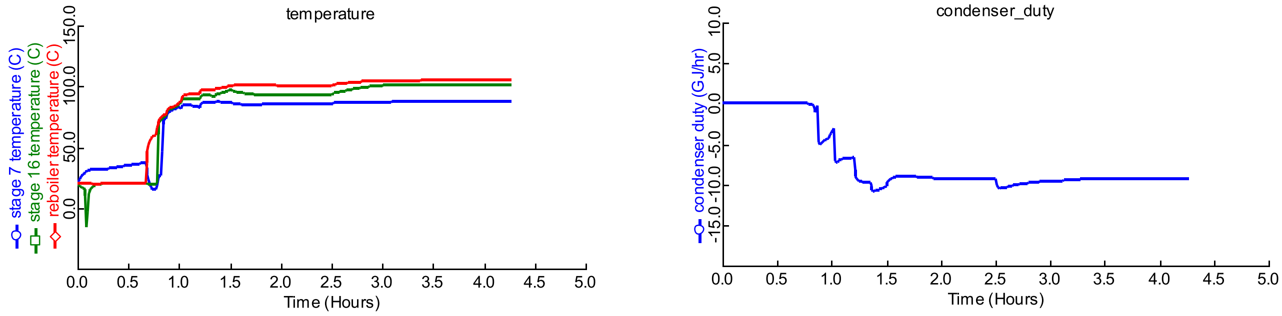
Figure 29. Simulation results of the distillation startup operated according to SFC-5.

temperature of plate 16 is at 99 °C, *V*reflux is opened to start the reflux flow going down to the column sump and, at the same time, *V*lps is adjusted to 93% to increase the heat input to the reboiler and also the resulting upward vapor flow. Since the liquid outflow of the reflux drum is still considerably lower than the inflow, the height of the liquid level continues rising quickly until it reaches 1.25 m. At this time, the overhead product is supposed to be drawn by opening *V*top (51%) to hold the liquid level roughly at a constant height. After opening *V*top, the operating procedure given in SFC-3 calls for a waiting period of 24 min. This is because the feed and reflux liquids slowly accumulate in the column sump during this period. Although



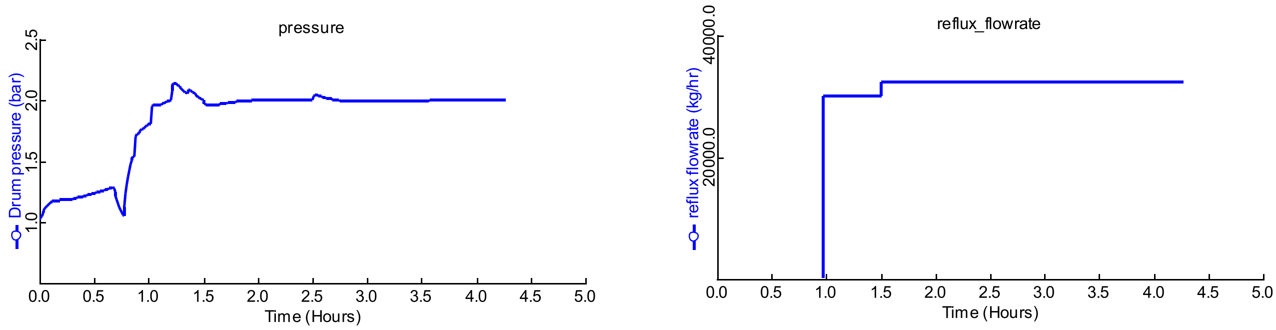
(a) Liquid levels in reflux drum and column sump

(e) Heat duty of reboiler



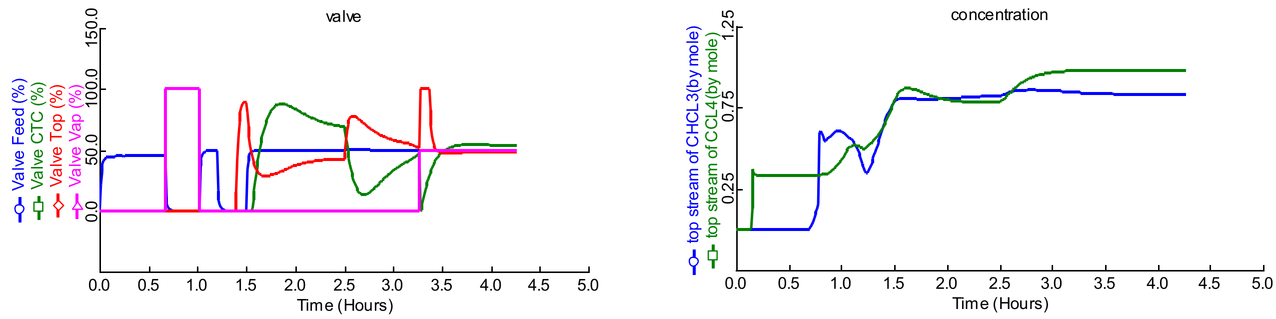
(b) Temperatures at plates 7, 16 and reboiler

(f) Heat duty of condenser



(c) Pressure in reflux drum

(g) Reflux flow rate



(d) Valve openings of V_{feed}, V_{ctc}, V_{top} and V_{vap}

(h) Concentrations of light and heavy keys in the top and bottom products

Figure 30. Simulation results of the distillation startup operated according to the ASPEN built-in procedure.

the liquid in the sump is partially lost in the rising vapor due to heat input to the reboiler, the downward trend of the liquid level can be eventually reversed in the waiting period and raised to approximately 1.25 m. At this time, *V*ctc should be opened (48%) to draw the bottom product. It is predicted, after 6 min, all online measurements should reach their set-point values. At this point, all controllers should be switched to the AUTO mode and all had valves that should be adjusted to their steady-state opening.

8.3. Unsafe Operating Procedures.

An automata-generated unsafe operating procedure is shown in SFC-4 in Figure 25, and the corresponding ASPEN simulated level heights of the liquids in the reflux drum and column sump are presented in Figure 26. In this procedure, after confirming the designated initial conditions in AC_1, the inlet valve Vfeed is set to the 50% position to fill the column sump with liquid. The subsequent waiting period is 18.9 min. At the end of this period, heating and cooling are started by directly opening *V*lps and *V*cond to their steady-state positions, i.e., 93 and 92%, respectively. Since the increase of heat input is too drastic in this case, the column sump becomes empty for a short period at around 27 min (see Figure 26). Based on this observation, SFC-4 should be regarded as unsafe and, thus, excluded from further consideration.

8.4. Comparison with the ASPEN Built-In Procedure.

As mentioned before, the sump level controller adopted in the ASPEN built-in example has been deliberately excluded from generating SFC-3 and SFC-4 in the above case studies. To be able to compare the ASPEN procedure used for the distillation startup (see Part E in the Supporting Information) and the procedures generated with the proposed approach on a consistent basis, additional studies have been performed according to Figure 27, which can be produced by adding back the sump level control loop to Figure 22. By following the proposed procedure synthesis method, the SFC-5 in Figure 28 can be obtained. Notice that, due to the extra level sensor and the corresponding PID controller in the column sump, the waiting periods required in SFC-3 are replaced with the new features in SFC-5, which are marked by red rectangles. The resulting simulation data can be found in Figure 29, while those obtained by executing the ASPEN built-in procedure are presented in Figure 30. It should be noted first that, by comparing Figures 24 and 29, the dynamic behaviors of distillation startup operations that are executed according to SFC-3 and SFC-5 are actually quite similar. On the other hand, by comparing Figures 29a and30a, it can be observed that the liquid levels of the drum and sump in the latter case fluctuates more frequently and in a larger range. This is because of the fact that there is an extra total reflux stage (after the second stage) in the ASPEN built-in procedure. This is essentially a more conservative measure to exclude the possibility of the emptying column sump. Furthermore, by comparing Figures 29c and30c, it can be seen that the drum pressure variation caused by implementing the ASPEN built-in procedure is less drastic than that by SFC-5. This is again due to the aforementioned less aggressive practice taken by the ASPEN procedure. Finally, by comparing Figures 29h and30h, one can see that product concentrations change more before reaching the steady state in the latter case, while those in the former are smoother and stabilize quicker.

Finally, the above procedures have also been compared on the basis of several performance indices calculated according to the simulation results (see Table 4). It can be found that the proposed SFC-5 (or SFC-3) outperforms the ASPEN built-in procedure in almost every aspect.

Table 4. Performance Indices of SFC-3, SFC-5, and ASPEN Built-In Procedure

	amount of off-spec product (kg)					
SFC #	top	ctc	vap	total amount of reboiler heat input (GJ)	total amount of condenser heat output (GJ)	total operation time (h)
SFC-3	12 834	5467	838	23.0	−21.0	1.11
SFC-5	12 882	5415	843	23.0	−21.1	1.12
ASPEN	18 640	9933	92	33.3	−31.0	3.27

9. CONCLUSIONS

A generic approach has been developed in this study for systematically generating operating procedures based on timed automata. The implementation steps include (1) constructing automata for modeling the basic components and processing units according to engineering knowledge and with preliminary dynamics simulation results, respectively, (2) dividing the given operation into several intermediate stages and stipulating their control specifications in natural language and then converting them into automata, (3) synthesizing the operating procedures after synchronization of all automata mentioned above, and (4) verifying the procedures with Aspen Plus Dynamics. This approach has been successfully applied to two realistic examples, i.e., the startup operations of the flash drum and distillation column. Furthermore, it has also been shown that the proposed approach is especially effective for systems without critical sensors.

■ ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acs.iecr.0c01427.

Exploratory and test runs on Aspen Plus Dynamics; component models and layer model used in the flash startup example; detailed listing of the guards and updates of every edge in the component model of flash drum; task file used for SFC-3 simulation; and ASPEN procedure used for the distillation startup (PDF)

■ AUTHOR INFORMATION

Corresponding Author

Chuei-Tin Chang − *Department of Chemical Engineering, National Cheng Kung University, Tainan 70101, Taiwan;* orcid.org/0000-0002-4143-1873; Email: ctchang@mail.ncku.edu.tw

Authors

Chun-Ren Zhang − *Department of Chemical Engineering, National Cheng Kung University, Tainan 70101, Taiwan*
Chun-Yu Yeh − *Department of Chemical Engineering, National Cheng Kung University, Tainan 70101, Taiwan*

Complete contact information is available at: https://pubs.acs.org/10.1021/acs.iecr.0c01427

Notes

The authors declare no competing financial interest.

■ REFERENCES

(1) Alur, R.; Dill, D. L. A theory of timed automata. *Theor. Comput. Sci.* **1994**, *126*, 183−235.

(2) Behrmann, G.; David, A.; Larsen, K. G. *Formal Methods for the Design of Real-Time Systems*, Springer: Berlin, Heidelberg, 2004.

(3) Behrmann, G.; David, A.; Larsen, K. G. *Tutorial on Uppaal 4.0*; Department of Computer Science, Aalborg University: Denmark, 2006.

(4) Chen, T.-Y.; Chang, C.-T. Design approach to synthesize, validate, and evaluate operating procedures based on untimed automata and dynamic simulation. *Ind. Eng. Chem. Res.* **2019**, *58*, 8172−8183.

(5) Cassandras, C. G.; Lafortune, S. *Introduction to Discrete Event Systems*, 2nd ed.; Springer Science+Business Media: New York, 2008.