Modeling of multilevel control system based on Event-B

Yutian Wang1*

1School of Computer Science, Xi’an Shi you University, Xi’an, Shaanxi, 710065, P. R. China
e-mail: 19212060623@stumail.xsyu.edu.cn

Abstract. Aiming at the problems existing in the traditional development method of multilevel control system, this paper proposes a formal modeling solution based on Event-B from the perspective of practical application. Based on the analysis of four synchronization modes and the principle of multilevel control system, a formal method is introduced. On this basis, by formulating the refined strategy of the multilevel control system model, the iUML-B model meeting the security requirements is established step by step. Through the automatic transformation function of the Rodin, the iUML-B model of multilevel control system is automatically transformed into Event-B mode. In order to ensure the safety of the system, this paper uses the ProB to simulate and record the event trajectory. The results show that the formal modeling method based on Event-B greatly improves the security and development efficiency of industrial control.

1. Introduction
In the era of highly digital development, multilevel control systems have been widely used in aerospace and Internet of Things. For most multilevel control systems, its safety requirements are as important as its function requirements. Therefore, the safety performance of the multilevel control system must be improved to avoid accidents. Due to the complexity of the multilevel control system, it is difficult to guarantee its safety performance. Therefore, in a variety of safety standards, it has been clearly stipulated that engineers must use formal methods when modeling and verifying multilevel control systems [1].

From the perspective of research development trends, the formal development method based on the Event-B design pattern is of great significance in improving the efficiency of multilevel control system development and the reusability of formal models [2]. Event-B design pattern plays an important role in system engineering and software engineering, but engineers need to have knowledge of discrete mathematics and mathematical logic to master the Event-B design pattern, which will lead to high learning costs [3]. When modeling control intensive system, we need to add a large number of guards and actions manually in Event-B design pattern, which is a time-consuming and error prone process [4]. If the iUML-B state machine model is established first, and then the Event-B model is automatically converted through the Rodin platform, it will greatly reduce the error rate and improve the modeling efficiency [5].

Therefore, this paper proposes a formal modeling solution based on Event-B. This method builds the iUML-B model of the multilevel control system by modeling and instantiating the four synchronization modes of the typical control system, and then automatically converts it to the Event-B model with the help of the Rodin platform. This method greatly improves the safety performance and modeling efficiency of the multilevel control system, and reduces the burden of manual coding in the modeling process, which is of great significance to the design and development of the multilevel control system.
2. Analysis of model principles
The multilevel control system has the following equipment: a motor, a clutch, a front door, four buttons, a controller, a vertical slide, a pressing tool, a rod connecting the motor and the slide. Among them, the controller controls and manages the operation of the equipment, the buttons B1 and B2 control the start and stop of the motor, and the buttons B3 and B4 control the engagement and disengagement of the clutch. When the motor is working, as long as the clutch is engaged, the motor will immediately trigger the lever and drive the slider to act up and down, which will drive the pressing tool to process the parts. In order to ensure the safety of workers, when the motor is working and the clutch is engaged, the front door must be closed; when the clutch is disengaged, the front door can be opened.

The most basic model in a multilevel control system is the "trigger-response" model. That is, the actuator sends an instruction to the reactor after executing an action event, and when the reactor receives the instruction, it will immediately feedback a response to the actuator [6]. When the four buttons of the multilevel control system are pressed, a pulse will be sent to the controller. After receiving it, the controller will send the corresponding command to the front door, engine and clutch. After receiving the command, these devices will send the corresponding response to the controller and complete the specific command, as shown in figure 1.

3. Modeling of Multilevel Control System
3.1 Synchronous Mode Modeling
The traditional Event-B modeling method models the synchronization mode by adding guards and actions to the event, which is easy to make mistakes [7]. This paper breaks through the original flaws, first establishes the iUML-B model of four synchronization modes, and then uses the automatic conversion function of the Rodin platform to generate the Event-B model, which greatly improves the modeling accuracy and modeling efficiency. This section illustrates the modeling method of synchronous mode through the modeling process of weak synchronous mode.

When building the iUML-B model of weak synchronous mode for a subsystem including actuator and reactor, firstly, the state machine of actuator and reactor is modeled with iUML-B. The model of actuator and reactor is shown in Figure 2. Under the limitation of weak synchronization mode, the reactor start event can only occur after the actuator start event. Therefore, it is necessary to add a reflexive edge link to the event r-on on the a1 state of the state machine a. At the same time, the event r-off must occur after the event a-off. Therefore, a reflexive edge is added to the a0 state of the state machine a to link to the event r-off, and the iUML-B state machine will automatically generate a guard, which can ensure the event r-off occurs after the event a-off. The iUML-B state machine model of weak synchronization mode is composed of figure 2(b) and figure 3. Using this general method, the iUML-B state machine model of the other three synchronization modes can be established.
3.2 Synchronization Mode Instantiation

Based on the analysis of the four synchronization modes and the principle of multilevel control system, the state machine model of multilevel control system can be obtained gradually by instantiating the four synchronization mode state machines and composing 15 state machines into 7 subsystems and state machine M. Because the strong synchronization mode and the strong-strong synchronization mode are respectively the refinement of the weak synchronization mode and the strong-weak synchronization mode, this section takes the weak synchronization mode and the strong-weak synchronization mode as examples to illustrate the method and process of instantiation.

### 3.2.1 Weak Synchronization Mode Instantiation

This paper take the modeling process of subsystem A1 (button B1-motor) as an example to illustrate the instantiation process of weak synchronization mode. According to the analysis of the principle of multilevel control system, it can be seen that there is weak synchronization between button B1 and controller in subsystem A1. Based on the established iUML-B state machine of the weak synchronization mode, the “a” and the “r” are directly instantiated into the iUML-B state machine of A1. Table 1 shows the corresponding transformation relationship between the weak synchronization mode and the sub-system A1 after instantiation.

**Table 1. Weak synchronization mode instantiation.**

| Mode state machine | Instantiate state machine                        |
|--------------------|-------------------------------------------------|
| a                  | Start-Motor-button                              |
| r                  | Start-Motor-impulse                             |
| a0                 | Start-mb-False                                  |
| a1                 | Start-mb-True                                   |
| r0                 | Start-mi-False                                  |
| r1                 | Start-mi-True                                   |
| a-on               | Push-start-Motor-button                         |
| a-off              | Release-start-Motor-button                      |
| r-on               | treat-start-Motor                               |
| r-off              | Treat-release-start-Motor-button                |

According to the corresponding relationship between the weak synchronization mode state machine and the state machine in the subsystem A1, two state machines can be obtained through instantiation, namely the start motor button state machine model and the start motor pulse state machine model. The example state machine model is shown in figure 4.
3.2.2 Strong-Weak Synchronization Mode Instantiation

From the analysis of the principle of strong-weak synchronization mode, it can be seen that the strong-weak synchronization mode includes not only the synchronization relationship within each subsystem, but also the synchronization relationship between different subsystems, so it will be more complex in the process of state machine instantiation. Based on the established iUML-B state machine of strong weak synchronization mode, the iUML-B state machine models of subsystems A5 (motor controller) and A7 (clutch controller) are directly instantiated. The corresponding transformation process of instantiation is shown in table 2.

Table 2. Strong-weak synchronization mode instantiation.

| Mode state machine | Instantiate state machine |
|--------------------|--------------------------|
| a                  | Motor-actuator           |
| r                  | Motor-sensor             |
| b                  | Clutch-actuator          |
| s                  | Clutch-sensor            |
| a0                 | ma-stopped               |
| a1                 | ma-working               |
| r0                 | ms-stopped               |
| r1                 | ms-working               |
| b0                 | ca-disengaged            |
| b1                 | ca-engaged               |
| s0                 | cs-disengaged            |
| s1                 | cs-engaged               |
| a-on               | Treat-start-Motor        |
| a-off              | Treat-stop-Motor         |
| r-on               | Motor-start              |
| r-off              | Motor-stop               |
| b-on               | Treat-start-clutch       |
| b-off              | Treat-stop-clutch        |
| s-on               | Clutch-start             |
| s-off              | Clutch-stop              |

As can be seen from the above table, after the state machine name, state name and conversion name of the strong-weak synchronization mode state machine are converted, according to the corresponding relationship, four instantiated state machines of subsystem A5 and subsystem A7 can be obtained, namely the motor actuator state machine model, motor reactor state machine model, clutch actuator state machine model and clutch reactor state machine model, as shown in figure 5.
3.3 State Machine after Instantiation of the Four Synchronization Modes

By instantiating the state machines of the four synchronization modes, the seven subsystems and the iUML-B state machine model between the subsystems can be obtained. The final model of the multilevel control system consists of 15 iUML-B state machines, among which 14 state machines are shown in Table 3, and the other state machine is to satisfy the strong-strong synchronization relationship between subsystem A6 and subsystem A7. In order to ensure the security and correct implementation of the model design, it is necessary to formulate a set of highly feasible and efficient refinement strategy. The basic idea of Event-B model refinement strategy is to gradually introduce more refinement details into the initial model [8]. In this paper, according to the state machine model of multilevel control system after four synchronous modes are instantiated, the seven-step refinement strategy is adopted to gradually introduce the functional requirements and security requirements of multilevel control system, which greatly reduces the uncertainties in the model, and realizes the establishment of the iUML-B model of multilevel control system.

| Subsystem            | iUML-B State machine | Sync mode          |
|----------------------|----------------------|--------------------|
| A1(Button B1-controller) | Start-motor-button | Start-motor-impulse | Weak-synchronization |
| A2(Button B2-controller) | Stop-motor-button   | Stop-motor-impulse | Weak-synchronization |
| A3(Button B3-controller) | Start-clutch-button | Start-clutch-impulse | Weak-synchronization |
| A4(Button B4-controller) | Stop-clutch-button  | Stop-clutch-impulse | Weak-synchronization |
| A5(Controller-Motor)   | Motor-actuator       | Motor-sensor       | Strong-synchronization |
| A6(Controller-door)    | Door-actuator        | Door-sensor        | Strong-synchronization |
| A7(Controller-Clutch)  | Clutch-actuator      | Clutch-sensor      | Strong-synchronization |

3.4 Event-B Model of Multilevel Control System

The final refined model is automatically transformed into Event-B model through Rodin platform. Variables and events are two essential elements in the Event-B model. When establishing the iUML-B state machine model, it is necessary to define the state of the variable and the event that triggers the state transition [9]. When the Rodin platform transforms the iUML-B state machine model of multilevel control system into Event-B model automatically, the corresponding Event-B code will be generated automatically.

This paper uses the motor as an example to explain the Event-B model of the multilevel control system. When the start motor button is in a failed state, if it becomes a successful state after pressing the start motor button, it means that the event of pressing the start motor button has occurred. When the start button is pressed, it will trigger the controller to send a start command to the motor. Only when the motor actuator and the motor reactor are in a stopped state, the start motor pulse is in a failed state, and the start motor button is in a successful state, can the start motor pulse be triggered to change to a successful state. At this point, the controller has successfully triggered the motor to start. When the motor actuator is in the working state and the motor reactor is in the stopped state, the motor is immediately started after the motor reactor is converted to the working state. After the execution of a series of events, the motor is started. The Event-B model of the motor is shown in figure 6. The Event-B model of other devices in the multilevel control system is similar to the motor.
4. Simulation of the model

During the formal simulation of the model, the ProB is used to track the events of the model to ensure that the whole event runs in accordance with the preset logic. In order to verify the validity and usability of the model, the whole model simulation process simulates the iUML-B state machine from the perspective of executability [10].

In this paper, the event sequence of multilevel control system is simulated on the Rodin platform, and the event trajectory is recorded to realize the simulation of the Event-B model of multilevel control system. The experimental results show that the logical sequence of events is consistent with the requirements of the multilevel control system model, and the experimental results are shown in figure 7. The results show that the multilevel control system model based on Event-B can accurately and effectively describe the functional requirements and security requirements of multilevel control system. It is an effective method, which can be widely used in aerospace and industrial control to enhance the safety of the system and improve the development efficiency.

5. Conclusion

By analyzing the principles of four synchronization modes and multilevel control system, this paper uses the iUML-B mode state machine to model the four synchronization design modes in embedded control system, and instantiates four iUML-B mode state machines. Finally, this paper obtains the Event-B model of complex multilevel control system. The simulation results show that the Event-B model event trajectory obtained by iUML-B pattern state machine is the same as that obtained by traditional design pattern, but its security and development efficiency have been greatly improved. This is of great significance to the design and development of multilevel control system, which can be widely used in aerospace and industrial control.
Acknowledgments
This work was supported by National Natural Science Foundation of China (61802301) and Natural Science Foundation of Shaanxi Province (2019JQ-056).

References
[1] Rahul, K., Biman, S.B. A Prototype Modeling of Smart Irrigation System Using Event-B. J. SN Computer Science, Volume 2, Issue 1. 2021.
[2] Bodeveix, J.P., Dieumegard, A., Filali, M. Event-B formalization of a variability-aware component model patterns framework. J. Science of Computer Programming, Volume 199, 2020.
[3] Zhu, C.Y., Butler, M., Cirstea, C., Trace semantics and refinement patterns for real-time properties in Event-B models. J. Science of Computer Programming, Volume 197, 2020.
[4] Kim, J., Park, M.G. Formal development of an operation monitoring and control system for nuclear reactors using Event-B method. J. International Journal of Energy Research, Volume 44, Issue 10. 2020. PP 8170-8180.
[5] Olszewska, M., Manninen, F.S., Edmunds, A., Wald, M. Applying guidelines for system modelling in Event-B - a systematic literature review. J. International Journal of Critical Computer-Based Systems, Volume 10, Issue 1. 2020.
[6] Shi, Y.X., Wang, H.B. Detailed requirement modeling and verification based on Event-B. J. Journal of Changzhi University. 2019, 36 (02).
[7] Fakhfakh, F. A refinement-based approach for verifying dynamic changes on time-aware processes. J. Procedia Computer Science, Volume 159, 2019. PP 1489-1498.
[8] Kobayashi, T., Ishikawa, F., Honiden, S. Consistency-preserving refactoring of refinement structures in Event-B models. J. Formal Aspects of Computing, Volume 31, Issue 3. 2019. PP 287-320.
[9] Zhu, C.Y., Butler, M., Cirstea, C. Formalizing hierarchical scheduling for refinement of real-time systems. J. Science of Computer Programming, Volume 189, 2020.
[10] Banach, R. Automated urban train control with hybrid Event-B: ‘Tackling’ the rugby club problem. J. Science of Computer Programming, Volume 190, 2020.