17th European Symposium on Computer Aided Process Engineering – ESCAPE17
V. Plesu and P.S. Agachi (Editors)

Modeling and Verification of Control Logics in Safety Instrumented System for Chemical Industrial Processes

Jinkyung Kim, Younghee Lee, Il Moon

Department of Chemical Engineering, Yonsei University, 134 Shinchon-dong Seodaemun-ku, Seoul 120-749, KOREA, E-mail : bayaba@yonsei.ac.kr

Abstract

This study focuses on automatic verification and validation methods for the safety and correctness of control logics of the safety instrumented system (SIS) in chemical process industry. The models of discrete events, system behaviors and control programs for chemical processes and SIS are developed using automata theory. Symbolic model checking method, an automatic error finding approach, is used to verify its safety and reliability. The strength of this method is to synthesize a feasible sequence through a counter-example and to verify its correctness using computation tree logic (CTL) simultaneously. This method can be applied to determine the error-free location of SIS, to find the logical errors automatically which is difficult to find manually, and to verify the safety and feasibility of SIS. This paper addresses the model development of the SIS control logics of chemical industrial processes and presents how model checking approach can be used efficiently in the verification of SIS control logics through several case studies.

Keywords

SIS control logics, Safety verification, Model checking, CTL, Chemical process

1. Introduction

A safety instrumented system (SIS) is one of the most important protective measurements in chemical industrial plants and provides automatic actions to correct an abnormal process event or behavior that has not been controlled by basic control systems and manual interventions. SIS is composed of any combination of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are violated. A SIS is commonly used on rare occasions including emergency shutdown system, safety shutdown system, and safety interlock system. A SIS, therefore, must be available to operate whenever needed. If SIS failure occurs, it is difficult to avoid from accidents such as explosion, process damage, environmental damage, loss of cost, and loss of human life. A SIS, thus, must be verified and validated thoroughly and systematically in design stage. No feasible design of the SIS causes the process to showdown or to lead abnormal situation. Most of existing methods such as HAZOP (hazard and operability study), FTA (fault tree analysis), FMEA (Failure mode and effect analysis), etc. for identifying hazards, safety and reliability of SIS are commonly used in industrial field. These methods, however, are usually very time consuming and only depend on manpower. Simulators are often used to analyze the behavior of control systems and process variables based on a determined model. Although examining the output of simulation is sometimes helpful, in practice, this method is not proper to deal with discrete event and behavior because the SIS control logics commonly consist of signals, discrete variable or behaviors.

The model checking verification method is an alternative approach that has achieved significant results recently. The main purpose of a model checker is verifying the model with regard to a requirement specification. Efficient algorithms are able to verify properties of extremely large systems. In these techniques, specifications are written as formulas in a proposition temporal logic and systems are represented by state-transition graph. The verification is accomplished by efficient searching techniques that views the transition system as a model for the logic, and determines if the specifications are satisfied by the model. There are several advantages to this approach. An important one is that the procedure is completely automatic. The model checker accepts a model description and specifications written as temporal logic formulas, and it determines if the formulas are true or not for that model.

These studies have been dealt with control logic program or operation of chemical industrial processes. In this paper, we apply this approach to provide design of safety instrumented system in chemical industrial processes. This method is tested by two examples to determine the error-free location of SIS, to find the logical and unfeasible errors automatically which is difficult to find using manual methods.

2. Model checking Method

Model checking is the most successful approach that is emerged for verifying requirements. A model-checking tool (UPPAAL is used in this paper) accepts system requirements or design (called model) and a property (called specification) that the final system is expected to satisfy. The tool then output yes if the given model satisfies given specifications and generates a counterexample otherwise. The counterexample details why the model doesn't satisfy the specification. By studying the counterexample, we can pinpoint the source of the error in the model, correct the model, and try again. The idea is that by ensuring that the model satisfied enough system propertied, we increase our confidence in the correctness of the model. The systems requirements are called models because they represent requirements or design.

Likely SIS in chemical process, control-oriented systems occur in a wide variety of safety problems in design stage. For the control-oriented systems, finite stat machines are widely accepted as a good, clean, and abstract notation for defining requirements and design. For modeling the systems, the followings are also needed to:

- be able to modularize the requirements to view them at different levels of detail
- have a way to combine requirements or design of components
- be able to stat variable and facilities(for example, valve or pump) to update them in order to use them in guards on transitions.

Model checking tool (UPPAAL) has its own rigorous formal language for design models.

3. Case study

Raw water supplying system is ubiquitous process in chemical industrial plants. Figure 1 is a part of P& ID (Piping & Instrumentation Diagram) for utility process design of HOU project in petrochemical plant. Raw water from a river is stored in raw water pond. The water flows to raw water tank through one pump. The water runs into the plant through three valves (V22, V23, and V14). The water is used for cooling water of process through valve 22, for clarifier feed through valve 23, and for fire water or emergency shower through valve 14. Valve 14 is directly connected to the by pass pipeline between pump and raw water tank. Valve 14 is always opened because it is used for emergency situation. The system has two pumps, one is operated at ordinary time and another is standing by pump. If one pump is out of order, another pump will be operated instantly. These pumps get a signal from indicator I-100. I-100 is controlled by pressure controller PI-101 or level controller LIC-101. PI-101 gets a signal form pressure translator PT1, monitoring the pressure of flow from raw water pond to the pump. If PI-101 indicates low low pressure, the pump turns off automatically; otherwise the pump is operated normally. In case of I-100 is

connected to LIC-101 (Case A), I-100 get a signal from LIC-101when level of raw water tank is high high, and the pump turns off by this signal. Another case is that LIC-101 is connected to valve LV (Case B). If raw water tank has high high level, LV is closed. There is no situation that two pumps turn off at the same time because the water is always prepared to use for emergency. At least, one pump needs to be operated. This example represents to search these unsafe control logics of safety instrumented system of all possible control logics in early design stage.

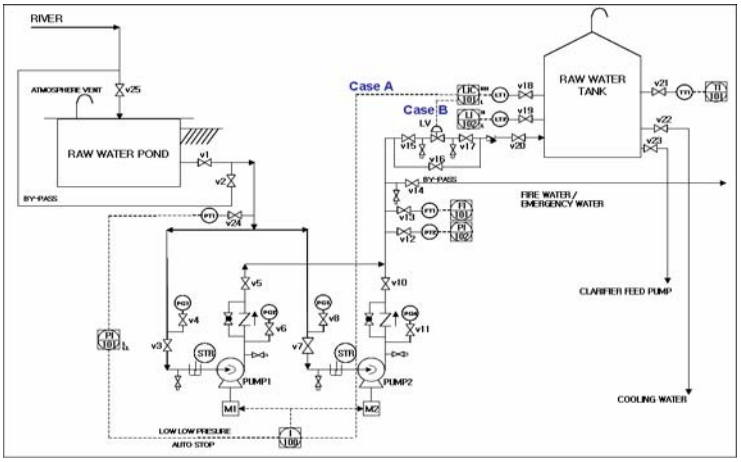

Figure 1.Raw water supplying system in HOU (Heavy Oil Upgrading) plant

Normal operation sequence of the system is following;

1. The water flows from raw water pond when valve V1.
2. If the pressure is not low low, one of two pumps turns on.
3. If pump1 turns on, valve V5 is opened and if pump2 turns on, valve V10 is opened.
4. If valve V5 or V10 is opened, valve LV is opened.
5. The water flows into raw water tank.
6. Valve 14 is always opened to prepare emergency.
7. The water flows into the process through valve V22 or V23.

Model description consists of 10 modules. Units or facilities do not exist below are not modeled because these can be omitted as a matter of analyzing control logics of the system. Figure 2 illustrates the model description of Case A.

Specifications for verification are;
Case A: A[] !(PI101==1 && Pump1==0 && Pump2==0 && Lv==1 && (!(Pump1_fail==1) && !(Pump2_fail==1)))

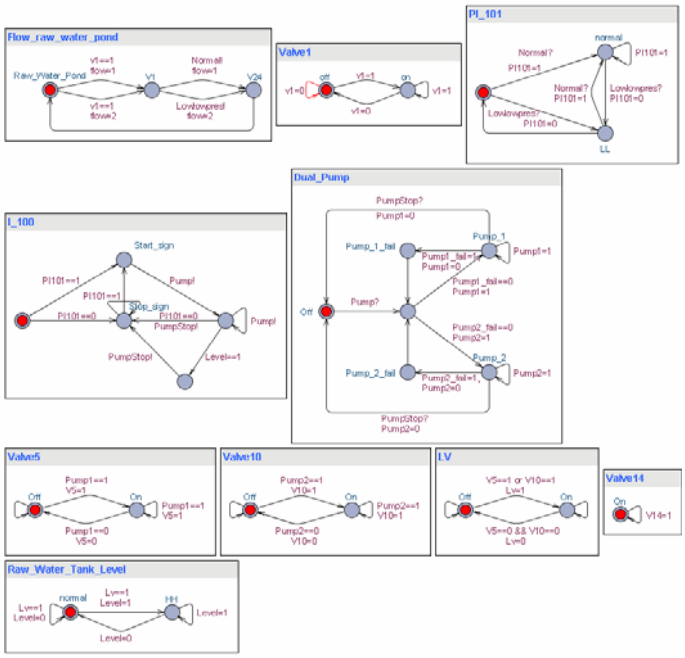

Figure 2. Model description of Case A.

This specification represents there is no situation that inlet flow from raw water pond is not low low pressure, two pumps are not operated without failure. The result for the specification is not satisfied. A counter example trace is shown in figure 3. Two pumps are not operated simultaneously when the level of raw water tank leads to high high. This control logic has an unsafe state, the system needs to redesign.

Case B: A[] !(PI101==1 && (Pump1==1 or Pump2==1) && Level==1 && Lv==0 && (!(Pump1_fail==1) && !(Pump2_fail==1)))

This specification means there is no situation that inlet flow from raw water pond is not low low pressure, one pump is operated without failure, valve LV is closed, and the level of raw water tank leads to high high. The answer for this query is not satisfied and the reasonable trace is shown in figure 3. This situation is less unsafe than Case A, but it is also an error because the water cannot flow only through V14. If emergency water or fire water is not used, the water cannot flow anywhere. Then, a safety valve next to valve V14 will pop up when the pressure in the pipeline is over set point of the safety valve. Reinstallation is needed. It is necessary to modify this control logic of safety instrumented system.

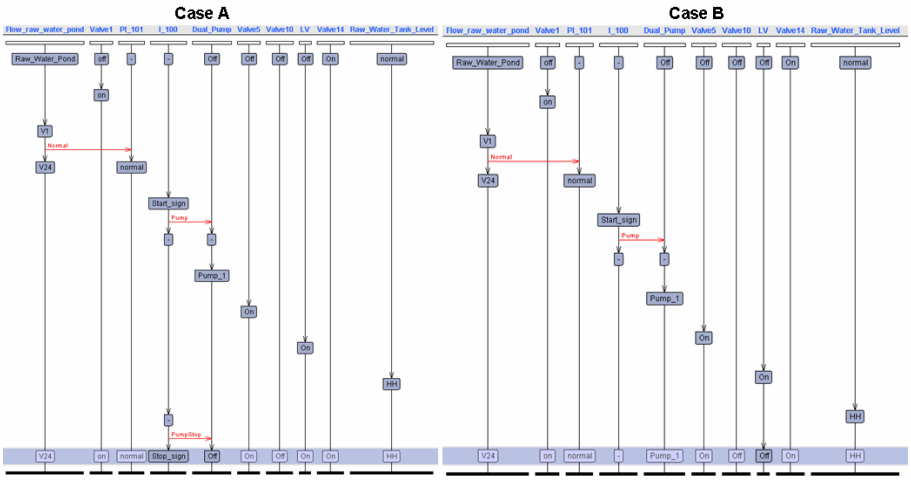

Figure 3. A counter example trace of specification for Case A and Case B.

4. Conclusions

This study represents a novel approach to verify the design of SIS control logic for chemical industrial processes using model checking. This method is applied to find the control logic error of SIS and unsafe procedures of SIS control operation. Based on the results, we can verify and validate the error-free SIS control logic and the right control location. We introduce a systematic technique to provide and modify the P&ID design of SIS control logics in chemical industrial processes. An automatic verification method of SIS control logic is proposed to make sure that the control operations achieved by SIS are safe.

References

1. R. Alur and D. Dill, Theoretical Computer Science B 126 (1994) 183
2. G. Behrmann, A. David and K.G. Larsen, A Tutorial on Uppaal. Available at http://www.uppaal.com
3. J. Kim and I. Moon, Computers and Chemical Engineering, 24 (2000) 385
4. J. Kim, Y. Lee and I. Moon, ESCAPE 16 meeting Jul. 9-13 (2006)
5. I. Moon, G. J. Power, J. R. Burch and E. M. Clarke, AIChE Journal, 38 (1992) 67
6. J. Kim and I. Moon, AIChE Annual Meeting, San Francisco, Dallas, Nov. 12-17 (2006)
7. S. H. Yang, L. S. Tan and C. H. He, Journal of Loss Prevention in the process industries, 14 (2001) 379