Proceeding of Korean Nuclear Society Spring Meeting
Kwangju, Korea, May 1997

A Formal Safety Analysis for PLC Software-Based Safety Critical System using Z

Jung Soo Koh
Nuclear Regulatory Inspection Division
Korea Institute of Nuclear Safety(KINS)

Poong Hyun Seong
Han Seong Son
Department of Nuclear Engineering
Korea Advanced Institute of Science and Technology(KAIST)

Abstracts

This paper describes a formal safety analysis technique which is demonstrated by performing empirical formal safety analysis with the case study of beamline hutch door Interlock system that is developed by using PLC (Programmable Logic Controller) systems at the Pohang Accelerator Laboratory. In order to perform formal safety analysis, we have built the Z formal specifications representation from user requirement written in ambiguous natural language and target PLC ladder logic, respectively. We have also studied the effective method to express typical PLC timer component by using specific Z formal notation which is supported by temporal history. We present a formal proof technique specifying and verifying that the hazardous states are not introduced into ladder logic in the PLC-based safety critical system.

1. Introduction

Software used in digital safety critical systems must be of sufficient quality to assure a safe and reliable design. Quality of software is measured in terms of its ability to perform its intended functions. Software can be evaluated by examining and approving the production process or by directly evaluating the software product. There is an extensive set of safety and reliability assessment methods that have been developed. Quantifying reliability and safety judgements including probabilistic approaches is inherently difficult. Therefore, mathematical proof techniques using symbolic logic (Formal Methods) have been suggested to be appropriate for assessment of reliability and safety of software [1].

This paper describes a formal safety analysis technique which is demonstrated by performing empirical formal safety analysis with the case study of beamline hutch door Interlock system that is developed in a PLC (Programmable Logic Controller) at the Pohang Accelerator Laboratory. In order to perform formal safety analysis, we have built the Z[2,3] formal specifications representation from user requirements written in ambiguous natural language and target PLC ladder logic, respectively. We have also investigated Z formal notations in order to describe the temporal constraints effectively. We demonstrate the proposed formal proof technique specifying and verifying that the hazardous states do not exist in the ladder logic in the PLC-based safety critical system.

2. Formal Safety Analysis

2-1. Description of Beamline Hutch door Interlock System

The Pohang accelerator laboratory is a facility which consists of a full energy (2 Gev) Linear Accelerator and a Storage Ring. There are 32 available beamports in the storage ring, and as of December 1996, the two initial beamlines are in operation, and 4 beamlines are under construction.

A schematic diagram of beamline hutch door interlock system is shown in Figure 1.

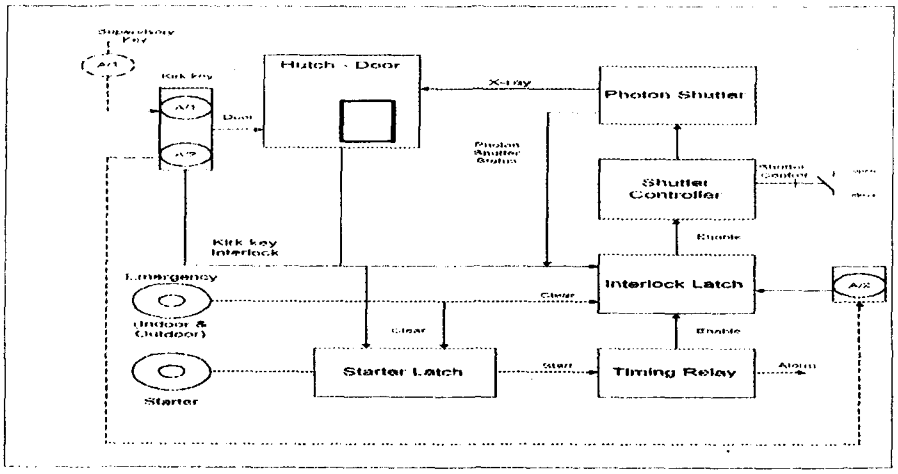

Figure 1. Schematic diagram of Beamline Hutch Door Interlock System

Followings are the user requirement specifications for beamline hutch door interlock system in Pohang Accelerator Laboratory.

(1) Pushing the start button installed inside the hutch activates a flashing lamp and an audible alarm. Within predetermined period (15 seconds), the operators key must be inserted in control panel. Otherwise, the procedure to exit must be returned to the beginning step.

(2) Pushing the interlock switch activates an alarm within preset period (5 seconds), photon shutter is enabled to be manipulated.

(3) In the case of emergency, anyone is able to use emergency button installed on inside or outside of the hutch and photon shutter must be closed.

(4) The photon shutter shall be closed by opening the hutch door or removing the operator's key.

(5) The start latch is enabled by pressing start push button installed inside hutch, but it is not functioning in case that the hutch door is closed.

2-2. Safety Analysis Method

Our formal safety analysis strategy is as follows :

Forward step : Transform the user requirements written in natural languages into Z formal specifications

Backward step : Transform the target program written in graphical notation of PLC ladder logic into Z formal specifications

Analyzing step : examining the specific user requirements are correctly incorporated into the target PLC program by analyzing the results from Forward step and Backward step.

2-3. Z formal specification

The major components of the beamline personal protection system have "on" and "off" digital states.

State

Beam_State ::= ON/OFF
Alarm_State ::= Silent/Beeping
Door_State ::= Open/Closed
Interlock_State ::= Pressed/Depressed

```
Emergency_State ::= Pressed/Depressed
Start_State ::= Pressed/Depressed
Timer1_State ::= ON/OFF
Timer2_State ::= ON/OFF
Shutter_Button_State ::= Open_Pressed/Closed_Pressed
Shutter_State ::= Open/Closed
Photon_Shutter_State ::= Enable/Disable
Key_State ::= Inserted/Ejected
Procedure-1 ::= (Key = inserted) ∧ (Interlock_button = pressed)
Procedure-2 ::= (Shutter_button = Open_pressed) ∨
                (Shutter_button = Close_pressed)
```

The functional requirements are explained in the following schema which reflects the user functional requirements described by natural language.

```
Beam_Personal_Protection

Beam : Beam_State
Alarm : Alarm_State
Door : Door_State
Interlock : Interlock_State
Emergency : Emergency_State
Start : Start_State
Timer1 : Timer1_State
Timer2 : Timer2_State
Shutter_Button : Shutter_Button_State
Shutter : Shutter_State
Key : Key_State
--------------------------------------------------
(Door = Open)∧(Start_Button = pressed)
      → (timer1= on )
      → (light=on) ∧ (alarm = on )
(Timer 1 = On) ∧ Max_wait__15 → (Timer 2 = On)
      → (timer2= on )
      → (light=on) ∧ (alarm = on )
      → (photon_shutter = enable)
(Emergency_Button = pressed)
      → (Beam_state = off )
(Door = Closed)∧(Start_Button = pressed)
      → (timer1= off )
      → (light=off) ∧ (alarm = off )
(Timer 2 = On) ∧ After_5 ∧ (Shutter_button = Open_pressed)
      → (Beam = On)
(Beam = on ) ∧ { (door = Open) ∨ (Key=ejected) }
      → (Beam = off)
```

2-4. Formal Safety Analysis

An formal safety analysis for the functional requirement and the target PLC ladder logic of this case study has been performed at the equivalent domain Z so as to compare them mathematically. Both the user requirements and PLC ladder logic are translated into the equivalent circumstances expressed by Z specifications in order to formally verify and specify the consistency and completeness of safety functional requirements and also to identify whether implemented system meets the user requirements. Two critical hazardous situations for this case study are considered for the beamline personal protection system.

(1) If the beamlike is "ON" state while the hutch door is open, it is possible for human to be exposed by the radiation.

(2) Though the emergency push button is pressed in any circumstances, the beameline is still "ON" state.

In order to perform the safety analysis specifying and verifying that these hazardous states are not introduced in PLC ladder logic, we have investigated the Z specifications translated from ladder logic by analyzing hazardous states. This procedure allows the formal proof.

- Specifying and verifying the hazard situation 1. The hazard situation 1 can be expressed as follows ;

$$(\text{Door} = \text{open}) \wedge (\text{Beam} = \text{on}) \tag{1}$$

$$(\text{Door} = \text{open}) \Rightarrow (\text{P07} = \text{False}) \tag{2}$$

Introducing this expression into the following operation of Door_Open schema then gives.

$$\{\text{P03} \wedge \text{M5}\} \wedge T_1 \wedge \text{P07} \wedge (\neg\text{P06}) \Rightarrow \text{M5} \tag{3}$$

$$\text{M5} = \text{False} \tag{4}$$

Introducing this value into the next operation of press_button_shutter_open schema

$$\{\text{P04} \vee \text{P023}\} \wedge \text{T2} \wedge \text{M5} \wedge (\neg\text{P05}) \wedge (\text{P00}) \Rightarrow \text{P23} \tag{5}$$

$$\text{P23} = \text{False} \tag{6}$$

where $(\text{Beam} = \text{on}) \Rightarrow (\text{P23} = \text{True})$ (7)

According the above discussion, then, hazard situation of (Door = Open) $\wedge$ (Beam = On) becomes

$$(\text{P23} = \text{True}) \wedge (\text{P23} = \text{False}) \Rightarrow \text{False} \tag{8}$$

The complete solution of hazard situation 1 is always False. So, it means that it is guaranteed that this hazardous state do not exist in PLC ladder logic. In the process of analyzing the Z formal specifications transformed from user requirements and PLC ladder logic, we found some errors in the

PLC ladder logic For example, the self-holding circuits design for PLC are designed in order to maintain the "ON" state of M5 relay. Considering T1 timer is designed to be reset after 15 second (preset time), we recommend the PLC Ladder Logic to be changed to meet the following equation.

$$\{(P03 \wedge T1) \vee M5\} \wedge P07 \wedge (\neg P06) \Rightarrow M5$$

3. RESULTS

We have proved mathematically the Beamline Hutch Door Interlock System at Pohang Accelerator Laboratory is free from hazard situations. We have however found some errors and mismatches between user requirements and final target product written in PLC ladder logic in the process of constructing the Z formal specifications and performing the completeness and consistency checks. In conclusion from this work, we believe that, in the case of relatively small systems like beamline hutch door interlock system, a formal verification and analysis is highly recommended so that the safety of PLC-based critical system may be enhanced and guaranteed.

Through our work using formal safety analysis, the following benefits are confirmed in assessing the safety and reliability of the safety critical PLC-based system :

- With the explicit proof, it is convinced whether the target system has hazardous conditions or not.
- It provides helpful method to comprehend user requirements which is written by ambiguous natural languages.
- It gives valuable consistency and completeness checkout results between the user requirement specifications and target PLC ladder logic.

References

[1] Digital Instrumentation And Control Systems In Nuclear Power Plants, Committee on Application of Digital Instrumentation And Control Systems to Nuclear Power Plant Operations and Safety, National Academy Press, 1995.

[2] J.M. Spivey, The Z Notation ; A Reference Manual, 2nd Edition, Prentice Hall, 1992.

[3] C.J. Fidge, Specification And Verification Of Real-Time Behaviour Using Z And RTL, Key Centre For Software Technology, The University Of Queensland.