ISBN: 978-3-95450-200-4 doi:10.18429/JACoW-PCaPAC2018-THP13

THE DEVELOPMENT OF A FPGA BASED FRONT END SAFETY INTERLOCK SYSTEM

J. Y. Chuang, Y. Z. Lin, C. M. Cheng, Y. C. Yang, C. C. Chang, I. C. Sheng
National Synchrotron Radiation Research Center, 300 Hsinchu, Taiwan

Abstract

A front end (FE) safety interlock control system was designed to protect humans and the machine integrity during operation. Since stability and reliability are an important requirement in this system, we developed a FPGA based system to control a safety logic for interlock protection. The integration of the FPGA, Real-time and redundant fail-safe system in the FE interlock system enables us to provide a safe protection with EPICS communication and hardware protection functions.

INTRODUCTION

In the phase II TPS project, there are seven insertion device FEs, three bending magnet FEs, and one diagnostic FE. After the first two years of TPS operation, an event occurred when the interlock system crashed in the TPS FE05, 23, 41, and 45 [1] (see Fig. 1). As a consequence, some safety control system design faults were reviewed and modified. In order to enhance the stability of the interlock system, the original Real-time system with systematic risks was replaced by the FPGA based safety interlock system.

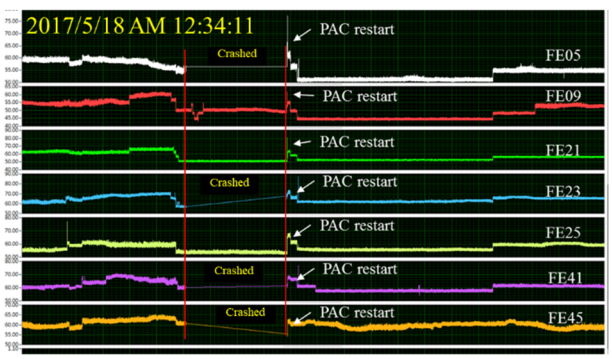

Figure 1: Record of a safety interlock controller crash (verified by CPU loading percentage).

STRUCTURE DESIGN OF THE SAFETY CONTROL SYSTEM

In the original TPS FE design, we used the National Instrument compact-RIO 9074 as the main controller for the safety interlock system and the logic program deployed in the Real-time system was operated by VxWorks. This design may cause a crash of the safety interlock system due to CPU loading or network risk [2]. In case of the TPS, the CPU loading of the cRIO 9074 was increased by using the distributed system manager (DSM) software to monitor the controller status. Due to safety concerns, the system needs to be separated into a safety logic program and a network protocol function into two independent systems. Therefore, the TPS FE interlock was upgraded from cRIO 9074 to cRIO 9030 and the logic program is now located on a field programmable gate array (FPGA) system. The Real-time system, operated by Linux, is engaged to publish the FE status by EPICS protocol. FPGA I/O nodes were created and its indicator for each corresponding share variable in the Real-time system to publish the EPICS protocol by cRIO 9030 network function. This structure means that the connection between FPGA and Real-time is a one-way transmission with no system resource concerns when the safety interlock system is operating as Fig. 2 shows. Therefore, the FPGA based safety interlock system combined with Real-time results in both stability and feasibility of safety and network function.

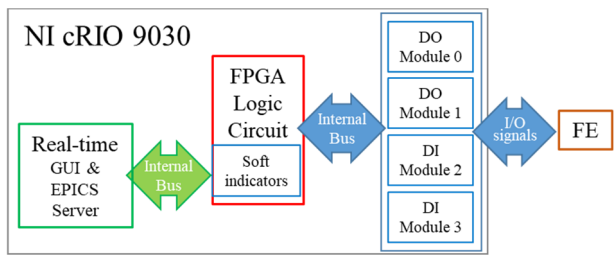

Figure 2: The structure of the FPGA based safety interlock control system.

In the TPS FE, the personal protection system (PPS) and machine protection system (MPS) were integrated into one safety controller NI cRIO 9030. Considering a fail-safe feature, a redundant system, which is controlled by a YOKOGAWA programmable logic controller (PLC) FAM3, is used to monitor the NI cRIO 9030 by hardwiring signal connections. The main controller for the safety interlock system NI cRIO 9030 and the redundant system FAM3 monitor each other by a 2 Hz heartbeat and watchdog individually. If any signal check detects a failure, the other controller will shut down the FE until FE staff resets the system manually. The control logic flow is shown in Fig. 3.

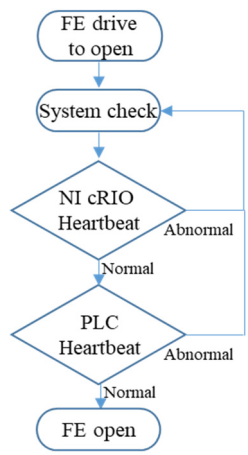

Figure 3: NI cRIO9030 and PLC FAM3 heartbeat logic checking flow.

ISBN: 978-3-95450-200-4 doi:10.18429/JACoW-PCaPAC2018-THP13

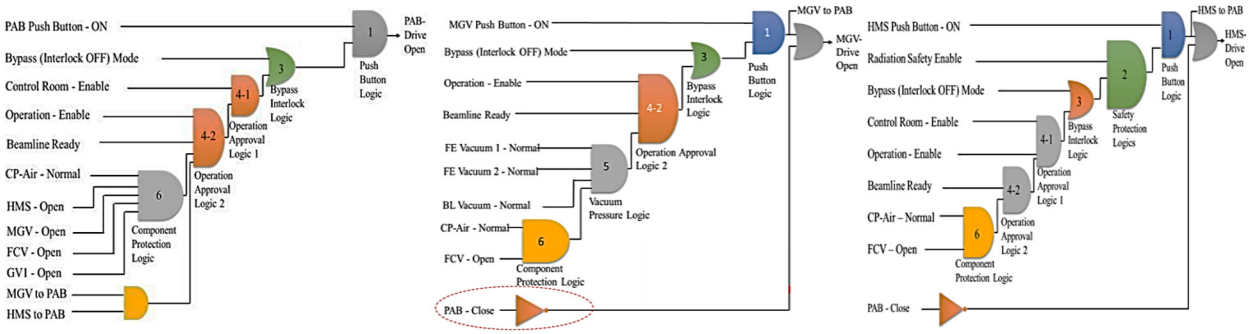

Figure 4: The main logic of PAB, MGV and HMS in TPS FE.

INTERLOCK LOGIC PROGRAMMING

The interlock program is a product of LabVIEW (LV) 2015 SP1 and was used to create the project in FPGA mode for all I/O node safety controls. This project is managed by auto-populating functions so that all sub-functions (in LV, it calls sub-VI) can be managed systematically without any effect when the file dictionary is changed. The main logic is divided into three main parts which are as follows:

- FE enable logic: this logic controls the photon absorber (PAB), all-metal gate valve (MGV) and heavy metal shutter (HMS) open or closed and also relates to beamline user operation allowance (as shown in Fig. 4) [3]. The logic contains all essential conditions of FE operation, such as cooling water, vacuum pressure, BL status, radiation safety enable, and central control system permission. All conditions in this logic are detected by TTL signals with 24 VDC and hardwire connections. The PAB, MGV, and HMS logic is shown in Fig. 5.

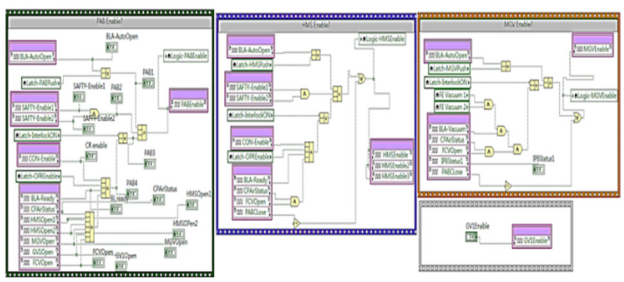

Figure 5: Program for the safety interlock logic in FPGA.

- Emergency control logic: because of the FE location being between BL and storage ring, its control system becomes an important link for machine safety protection. For personal protection, the FE belongs to the accelerator side and when a BL emergency is triggered, the FE is the first protector to block radiation by HMS and the electron beam is tripped at the same time. Therefore, the emergency logic must be very stable and reliable for operation. The emergency logic diagram is shown in Fig. 6.

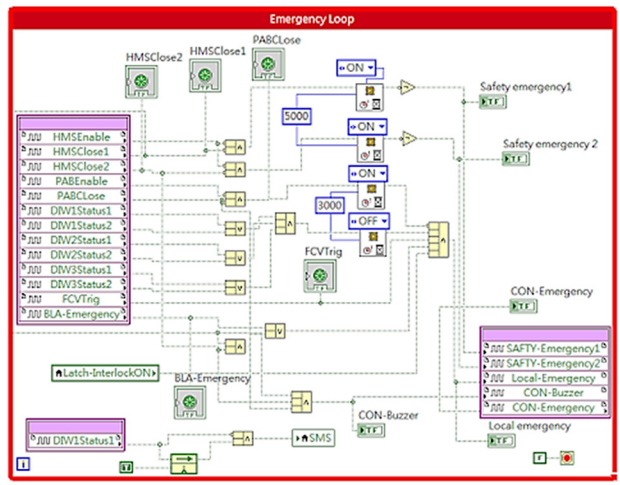

Figure 6: Emergency logic program for the safety interlock logic in FPGA.

- Interface logic: there were some control signals from others subsystems, the flip-flop logic and the denounced logic was widely used in the FPGA program to detect many different kinds of signals from subsystems such as BL or central control group. A self-hold circuit logic was used to detect the falling edge or rising edge status and complete the FPGA based safety interlock system. Figure 7 shows the status monitor for the logic program.

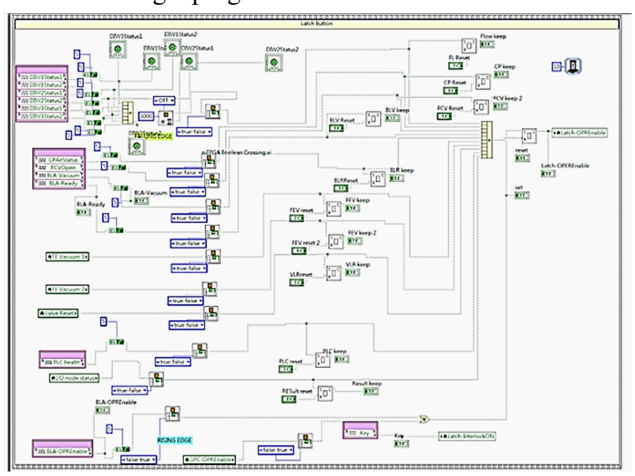

Figure 7: Interface signal detection program for the safety interlock logic in FPGA.

ISBN: 978-3-95450-200-4 doi:10.18429/JACoW-PCaPAC2018-THP13

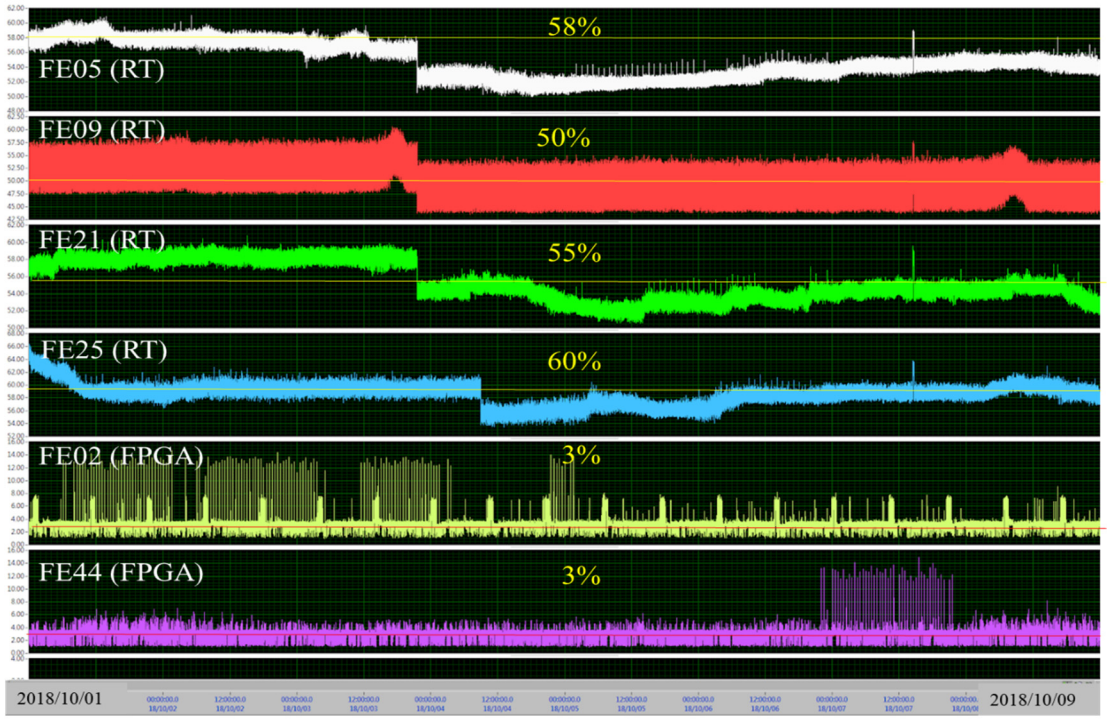

Figure 8: CPU loading comparison between RT based and FPGA based safety interlock system.

SYSTEM STABILITY ANALYSIS

The FPGA based safety interlock system was installed in phase II FE 02, 07, 44, and 39 respectively. To compare with phase I FE, the CPU loading of the FPGA based system is obviously lower than the Real-time based system. Figure 8 shows the CPU loading record, where the Real-time based system operated on average at 55%, while the FPGA based system was below 10 %. Although the FPGA based system is an independent safety interlock system without affecting the Real-time system, there are concerns about the NI cRIO 9030 being integrated into the same controller and we monitor the CPU loading to make sure the controller status and the EPICS system operate normal. To prevent network risks due to interlock instability, the communication system EPICS and Modbus servers are used as high-level firewall controllers between the server and the safety interlock controller. Finally, a redundant PLC system for the safety control system is utilized to monitor the main system and to prevent the crash of the safety interlock system. In addition, there is a hardwired connection between the FE HMS, BL and central control room, thus representing a highly reliable protection loop for beamline users.

CONCLUSION

From TPS FE commissioning experience, we find the NI cRIO 9030 provides a higher flexibility for EPICS communication and user interface development than traditional PLCs, but one has to separate the safety interlock and network function for safety concerns. The FPGA system in the cRIO 9030 can be a reliable hardware solution for safety interlock functions and it can also publish EPICS variables for monitoring system records and user information. After the upgrade of the TPS FE interlock system, the risk of failure is minimized with a redundant monitoring system and hardwired protection. This system should largely improve safety in TPS.

REFERENCES

[1] J.C. Liu, C.R. Chen, J.Y. Chuang, "TPS Beamline Radiation Safety Interlock, a Bizarre Incident and its Remedy Actions", 9th international workshop on Radiation safety at synchrotron radiation source, Hsinchu, Taiwan, Apr. 2017.

[2] National Instrument, https://forums.ni.com/t5/FIRST-Robotics-Competition/cRIO-Flashing-Error/td-p/3372316

[3] J.Y. Chuang, C.K. Kuan, I.C. Sheng, Y.Z. Lin, Y.M. Hsiao, Y.C. Yang, C.K. Chan, "Development and Construction of Safety and Control System for The TPS Front End Interlock", in *Proc. IPAC'17*, Copenhagen, Denmark, May 2017, paper TUPIK101.