SAFETY INTERLOCK IMPLEMENTATION USING FPGA

[1]CHAITANYA MUMMADI, [2]ARATI PADHKE, [3]ADELLI RAMESH, [4]GEETHA S KUMAR, [5]K P SARKAR

[1,2]Department of Electronics Engineering, K.J.Somaiya College of Engineering, Vidyavihar, Mumbai 400077.
[3,4,5]Reactor Control Division, BARC, Trombay, Mumbai 400085
E-mail: [2]aratipadhke@somaiya.edu, [1]c.mummadi@somaiya.edu

Abstract— The Fuel Handling Control System (FHCS) of Advanced Heavy Water Reactor (AHWR) is used for the refueling operation and control of Fueling Machine (FM), Fuel Transfer Machine (FTM) and other fuel handling equipments. The FHCS is designed to operate in Auto as well as in Manual mode. FHCS deploys two sets of Control Computers for FM and FTM auto operations respectively. Control Computers issue command to the field after verifying the interlocks coded in software. This paper summarizes the safety operation of Fuel handling equipments by checking these output commands given by Control Computer after verifying again through a separate standalone hardwired Manual Safety Logic (MSL) Unit. Manual Safety Logic Unit implements the interlocks using Field Programmable Gate Array (FPGA). This provides an independent and diversified implementation to prevent any maloperation of the system and takes the system to the safe state during any fault conditions.

Index Terms— Control System, Modes of Operation, MSL Unit.

I. INTRODUCTION

With the increase in growth of population and improvement in quality of life, the need of electricity has also increased rapidly. The traditional energy resources are limited to meet this ever increasing demand for long term. The electricity generated from sources such as coal, petroleum or gaseous based substances emits a large amount of greenhouse gases which makes the climate warmer. So the nuclear power plants came into existence. Nuclear power plants consist of various types of reactors such as Pressurized Water Reactor (PWR), Boiling Water Reactor (BWR), Sodium Cooled Fast Reactor (SCFR), Pressurized Heavy Water Reactors (PHWR), Fast Breeder Reactor (PFBR) etc to generate electricity with less emission of greenhouse gases.

Nuclear Power Plants (NPPs) depend heavily on Instrumentation and Control (I&C) systems for its protection, and reliable, efficient & safe operation.

The fundamental safety systems that are required for safe operation of NPPs are as follows [2]:
(1) Systems that allow reactor to be shutdown automatically during an abnormal event.
(2) Systems that cool the reactor and carry heat away from reactor core.
(3) Barriers that keep the radioactivity from escaping into the environment.
As per Atomic Energy Regulatory Board (AERB) safety guide [1], I&C systems of a NPP can be broadly classified as:
1. Safety Critical Systems - IA
2. Safety Related Systems - IB
3. Non-Nuclear Safety Systems – IC

For the purpose of refueling with fresh fuel and transfer of highly radio-active spent fuel from reactor to Fuel Storage bay (FSB) FM, FTM and other equipments are required. To control these equipments Fuel Handling Control (FHC) system is required. Considering the safety of fuel handling equipments which are operated remotely, the interlocks have been designed to prevent any maloperation and damage to its components. Interlocks are the instrumented functions that protect the machine and its components against failures of the plant system components, sensors, electronics etc. or incorrectly initiated operation. FHCS is categorized as safety class IB system.

Manual Safety Logic (MSL) Unit implements the interlocks for safe operation of Fuelling Machines in Reactor using Field Programmable Gate Array (FPGA). FPGA based design approach was chosen because of its advantages such as all the digital integrated circuits (ICs) will be implemented on one single FPGA, fast processing time, Long-term maintenance and its reliability.

II. CONTROL SYSTEM

Fuel Handling Control (FHC) system is used for controlling Fueling Machine (FM), Fuel Transfer Machine (FTM), and other fuel handling equipments. The shielded fuelling machine, picks up the new fuel cluster from fuel port, takes it to the reactor and loads into the pre-selected coolant channel. Spent fuel cluster removed from the channel by the fuelling machine is transferred to the Temporary Fuel Storage Bay from where it is taken to the Fuel Building using Fuel Transfer Machine. FM and FTM are operated mainly by oil and water hydraulic systems. Oil hydraulic power pack is provided on the fuelling machine for oil hydraulic actuators of the machine. Light water at various pressures and flows is required for operation of Fuelling Machine.

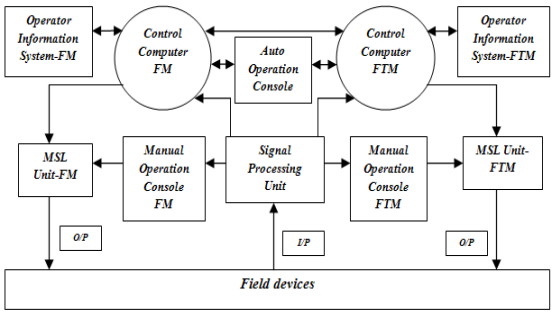

Figure 1: Block Diagram of Control System

Control Computers controls all FM and FTM related refueling and fuel transfer operations. The control computer receives inputs from field devices, carries out control algorithm (to check safety interlocks) and processes them in conjunction with commands entered by the operator & drives output to operate field devices. Control computer have number of external interfaces. Electronic devices used for interfacing input and outputs, such as signal conditioners, Isolation relays, signal multipliers, signal comparators. The inputs can be either in the form of digital or analog signals. Field inputs are sensing devices such as LVDT & Potentiometer (for analog signals), Reed/ Limit switches and push buttons (for digital signals). Field outputs are drive outputs and panel outputs are indicators.

III. MODES OF OPERATION OF CONTROL SYSTEM

Refueling and transfer operation are carried out remotely and automatically from the Main Control Room of the reactor. The Control Computer checks the interlocks and accordingly issues the commands. These commands are issued to the field devices only after checking of the interlocks by the hardwired MSL Unit which is independent of Control Computer.

The control system is operated in following modes:

a. Auto / semi-auto mode

In the auto mode, operator initiates the refueling sequence from the Operator Information System (OIS). The control computer executes the predefined and preprogrammed logic sequentially issuing required commands to field devices for the step-by-step operation. The status of operation is displayed in OIS.

b. Manual Mode

For situations when the computerized system is not functional, manual mode is provided. In this mode, the operator issues the commands from the main control panel by means of pushbutton switches which will energize the actuators/ drives directly after fulfilling the interlocks as implemented in Manual Safety Logic Unit. The status of operation will be displayed using indicating lamps.

IV. MANUAL SAFETY LOGIC UNIT

The commands issued by control computers in auto-mode or by the operator from the main control panel / local panels in manual mode are fed to Manual Safety Logic Unit to check for the safety interlocks.

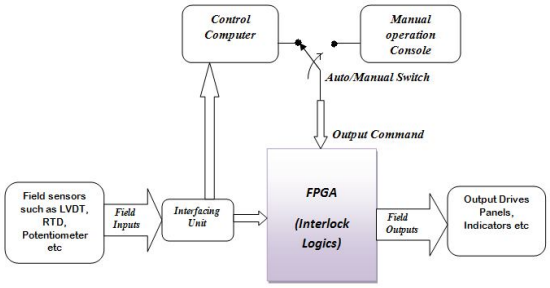

Figure 2: Manual Safety Logic Unit

Interlocks are provided to ensure safety during operation. Software Interlocks are provided in Control Computer, Hardware Interlocks are provided in MSL Unit. If there is any deviation from the normal /safe operation due to any cause, it would be detected and compensated by initiating corrective actions. Interlocks provided for the safe operation of various actuator/ drives/ equipment/ process systems are derived by logical combination of various field signals.

Earlier technologies used to implement interlocks are relay-based logic, wired logic with dedicated logic cards and programmable logic controllers (PLCs). Comparative study of various technologies used for implementing interlocks is discussed in [3,4]. Even though the PLCs were able to integrate safety and non-safety related programs and components within a single system, making communication between the two parts seamless, it has still not been widely used for implementing safety functions in NPPs. It has few drawbacks such as: Upgrading any of the system components, including patching firmware and software even for security reasons can be a complicated and risky affair, which will almost inevitably incur a period of unavailability of the entire system. Programmability of PLC systems in production environments is easy.

The oldest and still a highly relevant method of building reliable hard-wired logic systems is to use relays. All basic logic gates can be implemented in simple relays with hardwired connections. Implementation of a relay-based interlock is quite straightforward: standard electrical wiring, connectors, and relays are installed in a rack. Generally relay-based systems are quite robust and resistant to external disturbances. However, relay-based systems have several serious drawbacks compared to more modern approaches: Relay based systems are bulky requiring plenty of rack space even for a small amount of logic, which limits the practical complexity of the application. Safety relays are expensive and implementation and maintenance of

the system is quite labour intensive and time consuming.

Another way of implementing a hard-wired interlock is by using dedicated electronic logic (TTL/ MOSFET) cards. Logic gates are implemented in standard modular sub-rack-mounted cards and interconnections between these gates are realized by wiring the card inputs and outputs on the sub-rack backplane either by soldering or wrapping. A faulty card can easily be exchanged without having to touch the logic at all. One of the drawbacks of this technology is that switching times are relatively long for active gates ranging from 2-15ms. Therefore, complicated logic may introduce a considerable delay of up to tens or hundreds of milliseconds. Electronic logic based systems are susceptible to noise and also requires quite a good amount of rack space depending on the complexity of the application. Maintenance of these systems is also complex, time consuming and labour intensive.

In this paper, the interlocks will be implemented using programmable logic devices such as Field Programmable Gate Arrays (FPGA). Although FPGAs have fixed logic cells but they can hold a very large amount of logic implementation in a single IC, thereby reducing space requirement. In FPGA the required functions and the interconnections between them are determined by the user. The amount of wiring required is meager. The most important feature of FPGAs is it has the ability of parallel processing. VHDL being a strongly typed programming language was preferred for the design of MSL Unit. Since strongly typed programming languages permit a high level of checking by the compiler and reduce the probability of faults in the design. Various tools and techniques are presently available for independent verification and validation of the implementation of the requirements.

In critical areas 2/2 logic are used to ensure safety so that failure of a single component will not lead to issue of wrong operate commands to the field. The FPGA takes the data from the input modules and implements the diagnostic of these modules then the results are passed through a drives, which is also verified internally, and the outputs are generated after the corresponding verification of the output modules, if all the diagnostics and results are correct. The output of Control Computers once again verified using hardware interlocks in MSL Unit. Independent and diversified double checking of interlocks ensures the safe operation of fuel handling equipments.

CONCLUSION AND FUTURE WORK

In this paper, MSL Unit is used to protect the fuel handling equipments of the system by verifying the commands issued in auto or manual mode. These commands issued by Control Computer passes through the Interlocks implemented in FPGA. Interlocks provided for the safe operation will detect the change in normal operation and compensate by initiating corrective actions and under fault conditions system will be taken to a safe state by selecting safe outputs.

REFERENCES

[1] Atomic Energy Regulatory Board, Mumbai-400094,India, “AERB safety guide No. AERB/NPP-PHWR/SG/D-1 safety classification and seismic categorization for structures, systems and components of Pressurized Heavy Water Reactors”, January 2003

[2] Manoj Kumar Misra1, N. Sridhar and D. Thirugnana Murthy,"Design and Implementation of Safety Logic with Fine Impulse Test System for a Nuclear Reactor Shutdown System” pp. 198-203, 2014 IEEE

[3] T. Hakulinen, F. Havart, P. Ninin, F. Valentini “Building An Interlock: Comparison Of Technologies For Constructing Safety Interlocks” pre-press release -oct-2015, ISBN 978-3-95450-148-9

[4] Aditya Gour, Ramesh Sanga, R P Behera, P Sahoo, N Murali, SAV Satyamurty, “Design & Development of FPGA & FPAA based Remote Terminal Units for Nuclear Power Plants” pp. 44-48, DOI 10.1109/ISED.2014.17.

★★★