Modeling the Instrumentation and Control Systems of Fast Breeder Nuclear Reactor

P. Swaminathan
Director, Electronics & Instrumentation Group
Indira Gandhi Centre for Atomic Research Kalpakkam, Tamil Nadu India 603102
Tele : 044 27480090; Fax : 044 27480228
E-mail : swamy@igcar.gov.in

Abstract

Improper design of Instrumentation & Control (I&C) systems is one of the main reasons for human errors during the operation and maintenance phase of Nuclear reactors. It is very important to carry out detailed failure/safety analysis of I & C systems. The design shall be such that any single failure of I&C system should not unnecessarily shut down commercial nuclear reactor. It is necessary to provide sufficient redundancy to ensure the specified high reliability of I&C systems. On-line testability shall be provided during the design stage itself for I&C systems. Fast Breeder Nuclear Reactor uses plutonium oxide as fuel and liquid sodium as coolant. Due to high power density (500 KW/litre) in the reactor core, computer based supervision and control systems are used to detect flow blockage in the fuel subassemblies. Physically and functionally distributed computer systems process nearly 15000 process signals in the nuclear reactor. The processed information is routed to the control room through optical fibre based plant area network. This paper explains distributed embedded systems, neutronic systems, diverse safety logic systems, etc. The on-line diagnostics to detect both safe failure and unsafe failure are explained with illustrations. The architecture of safety instrumentation and reliability analysis are detailed in this paper. The criteria for selecting the testing interval of I&C system is explained for neutronic system, safety logic system and real time computer system. The plant operator should be well trained in both normal and transient behaviour of various subsystems of nuclear reactors. Abnormal behaviour of subsystems is categorized based on probability of occurrence. Architecture of Training Simulator for nuclear reactor shall also take into account simulation of failure modes of I & C systems. Modeling of both normal and failure mode of operation of I&C systems of Fast Breeder Nuclear reactor are explained with typical examples. Format for display of fault messages in Large Video display units at control room should take into account psychology of plant operator. Details of typical comfortable formats of display, which are developed in consultation with Nuclear Power Plant operators, are illustrated.

Key words: Fast breeder nuclear reactor, Real time computer system, Neutronic system, Safety logic system, Safe and unsafe failure, Testing interval failure rate

I. INTRODUCTION

Nuclear power plants rely on instrumentation and control (I & C) systems for monitoring, control and protection of the plant. In any non nuclear power plant, conventional instruments are used to measure and control process parameters like temperature, pressure, level, flow etc. In Nuclear Power Plants (NPP), in addition to these, special instruments are used to monitor neutron flux, radiation levels etc. Further, instrumentation and control systems provided for post shutdown monitoring, isolation of reactor containment building during accident conditions and post accident monitoring etc play critical roles in nuclear power plants. In fast reactors, the core being not in the most reactive configuration, fast response for reactivity, core temperature measurement and failed fuel detection are very crucial. The instrumentation for sodium level, flow, leak detection from capacities and pipelines and for detection of water/steam leak in the steam generators is very specific to fast breeder nuclear reactors. Signals acquired from sensors are conditioned, processed and presented to the operator for smooth running during normal operation as well as to protect the plant during design basis events.

II. BRIEF DESCRIPTION OF PROTOTYPE FAST BREEDER REACTOR

Prototype fast Breeder Reactor (PFBR) is a 500 MWe capacity, pool type reactor utilizing sodium as the main heat transport medium. The reactor core consists of fuel sub assemblies made up of (Uranium, Plutonium) mixed oxide fuel. The heat transport system consists of primary sodium circuit, secondary sodium circuit and steam water system. Primary heat transport from the core is facilitated by two pumps, which drive sodium from the cold pool through the core. The hot pool sodium flows through the IHX, transferring heat to the secondary sodium and finally returns to the cold pool at the bottom, completing the flow circuit (Refer Fig.1).

The steam water system adopts a reheat and regenerative cycle using live steam for reheating. The operating temperatures of superheated steam at turbine inlet are 16.7 MPa, 763 K and 1805 t/h and of reheated steam are 3 MPa, 613 K and 1706 t/h. The regenerative feed water heating is done in six stages consisting of three low pressure heaters of surface type, one deaerator of direct contact type and two high pressure heaters of surface type. The turbine exhaust steam is condensed in a

surface type condenser by sea water at 305 K. Turbine bypass capacity of 60% is provided to facilitate the startup and the shutdown of the turbine and reloading after a turbine trip.

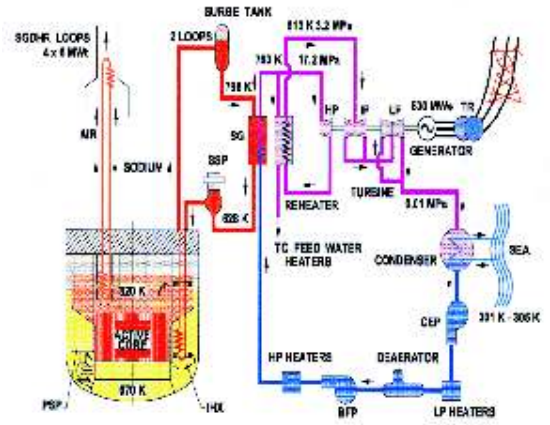

Fig. 1. PFBR flow sheet

Condenser cooling water system is used as a once through system for dissipating the heat load of 755 MW into the sea. The system is designed for temperature rise of 10 K at full power operation.

Decay heat removal under normal conditions is done using the operation grade decay heat removal system of maximum 20 MWt capacities in the steam water system. In case of off-site power failure or non-availability of steam-water system, the decay heat is removed by passive safety grade decay heat removal (SGDHR) circuit consisting of four independent loops. Each SGDHR loop is rated for 8 MWt and consists of a dip heat exchanger (DHX) immersed in the hot pool, one sodium / air heat exchanger (AHX), associated sodium piping, tanks and air dampers. Diversity is provided for DHX, AHX and dampers. The circulation of sodium and air is by natural convection

III. INSTRUMENTATION AND CONTROL SYSTEM

The I&C system of PFBR can be broadly classified into Computer based system and non-computer based system. The alarm and trip orders are generated by CategoryIA computer based systems such as core temperature monitoring system. Alarms in the control room are generated by CategoryIB computer based systems such as start up authorization system, start up fuel handling system, discordance supervision system, etc. CategoryIC computer based systems simply process the process signals and provide information for human machine interface systems. Non-computer based systems are neutronic systems and sodium instrumentation systems. Fission chambers are located inside the reactor vessel to measure the population of neutrons. During the low power operation, the neutronic sensors operate in pulse mode. For every neutron striking the sensor, a pulse is generated at the output of the sensor. As the power of the reactor increases, the pulses merge with each other. The fluctuation in the signal, measured as standard deviation, provides the information about the neutronic power of the reactor. From the rate of rise of the neutronic signal, both period and reactivity are derived. At higher power level of the reactor, the information from in vessel neutronic sensor is not reliable. Hence neutronic sensors are also located outside the bottom of the main reactor vessel. The information from ex-vessel sensors is processed to provide the information about the power of the reactor and reactivity of the process (Refer Fig.2).

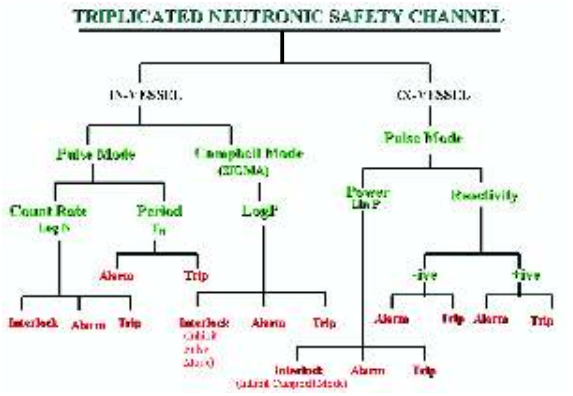

Fig. 2. Triplicated neutronic safety channel

The various neutronic signals are compared against alarm as well trip threshold by conventional comparator circuit. If the process signal crosses the alarm threshold, alarm will be generated in the control room with corresponding display of error messages in the display terminal. If the neutronic parameters cross the trip threshold, the trip order will be generated. For ensuring the high availability and reliability of neutronic system, neutronic sensors and signal processing systems are triplicated. The trip orders from these channels are routed through two out of three voting safety logic system. The output of safety logic system will drive the control rod downwards thus shutting down the reactor.

The health of safety logic system is monitored online by injecting a test pulse through different channels and detecting the presence or absence of the same at EM coil of the control rods (Refer Fig.3).

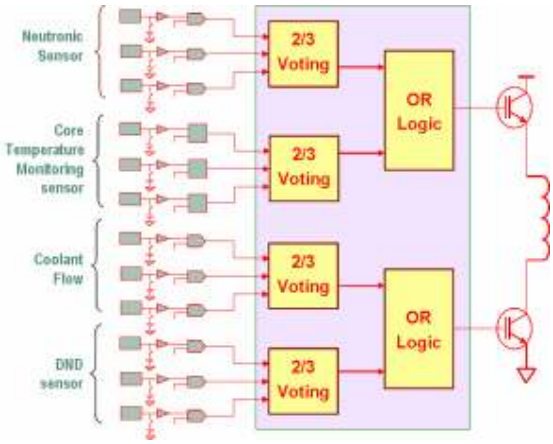

Fig. 3. Safety logic circuit

If the test pulse is injected at one channel before two out of three voting stage, the pulse is not expected at EM coil. If pulse is detected, then the fault is termed as 'safe fault'. This is repeated for all the channels of all the parameters. If a pulse is injected in any two channels of a parameter, then the pulse is expected at EM coil. If pulse is not detected then the fault is termed as 'unsafe fault'. If unsafe fault is detected by the online testing system, corresponding alarm will be energized in the control room with a display of detailed message in the display terminal. If the fault is not rectified within half-an-hour, the nuclear reactor will be manually shut down by the operator.

As part of diverse reactor shut down mechanism, diverse shut down rods are driven down by a Diverse Safety Logic System called 'Pulse Coded Safety Logic' system. The trip parameters are wired to conventional safety logic system and diverse pulse coded safety logic system. The diversity of safety logic systems ensures the required reliability of safety instrumentation system. In pulse coded safety logic system (Refer Fig.4), three different code patterns are generated for the three channels of each parameter.

Fig. 4. Pulse coded safety logic system

As long as the process parameter is within the safety limit, the SET and RESET pulses are propagated through the GUARD LINE LOGIC. The continual presence of SET and RESET pulses keeps the EM coil in the energized state. If any process parameter crosses the safety threshold, the propagation of SET and RESET pulses will be stopped. The EM coil will be deenergized, thus dropping the neutron absorbing control rods into the nuclear reactor thus shutting down the nuclear reactor. Nearly ninety real time computer systems (RTCS) are physically and functionally distributed through out the nuclear reactor. The output of process sensors are connected to three-port signal isolation and amplification units which in turn are connected to the nearest RTCS. After processing the signals, RTCS will generate the necessary analog and digital output for supervision and control of the nuclear reactor plant. Both the scanned process signal data and generated error messages if any are routed to control room through dual optical fiber.

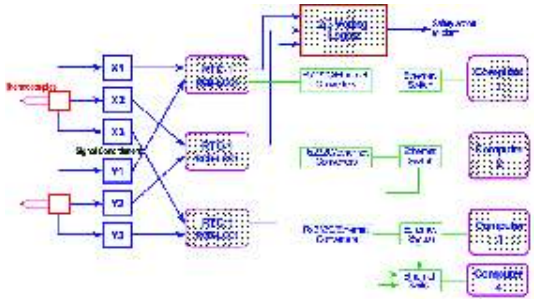

Fig. 5. Architecture of core temperature monitor system

Based on the importance to safety, process signals are classified as class-1 or class-2 or non-safety signals. Neutronic signals, the reactor inlet temperature signal, fuel sub-assembly outlet temperature, flow of coolant through the reactor, etc. are classified as class-1 signals. If any class-1 signal crosses the trip limit, the reactor will be shutdown. For ensuring the specified high availability and reliability, class-1 sensors are either duplicated or triplicated.

Architecture of typical real time computer systems deployed for supervision of reactor core is shown (Refer Fig.5). for details. The signal from process sensors are connected to three RTCS. The output from RTCS are processed by two out of three voting logic system. The level of coolant in the reactor, cover gas pressure, the flow of coolant in the secondary sodium system, flow of feed water, etc. are classified as class-2 signals. The architecture of corresponding RTCS consists of one main system and another hot standby system (Refer Fig.6).

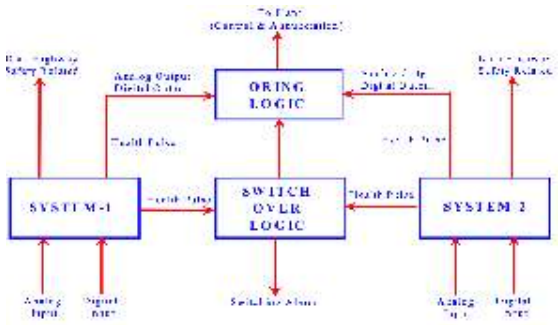

Fig. 6. Architecture of safety related system

The output information from class-1 RTCS are routed to the control room through a dedicated Plant Area Network. Similarly, separate Plant Area Network exits for class-2

Fig. 7. Networking of RTCS

RTCS. A fault tolerant process computer system receives the information from all the networks and stores the information in relational database for future retrieval. Large video display screens are connected to process computers (Refer Fig.7) for retrieval of information. Various process conditions are checked before starting the nuclear reactor. The start up authorization is issued by a dedicated RTCS. Similarly, the various process conditions are checked by a separate RTCS for authorizing the fuel handling operation in the nuclear reactor. The health of triplicated neutronic channels are checked by a dedicated discordance supervision system (Refer Fig.8).

The difference between Channel-A and Channel-B, the difference between Channel-B and Channel-C and the difference between Channel-C and Channel-A will be computed online. If the modulus of difference exceeds the allowable limit, then discordance alarm will be generated in the control room and corresponding error message will be displayed in the display unit.

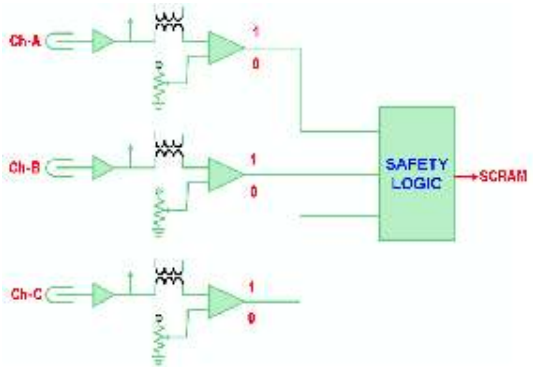

Fig. 8. Discordance supervision system

A Typical hardware architecture (Refer Fig.9). of the RTCS consists of asynchronous back panel bus, CPU card with ECC memory; analog input cards, digital input and digital out cards and communication controller,

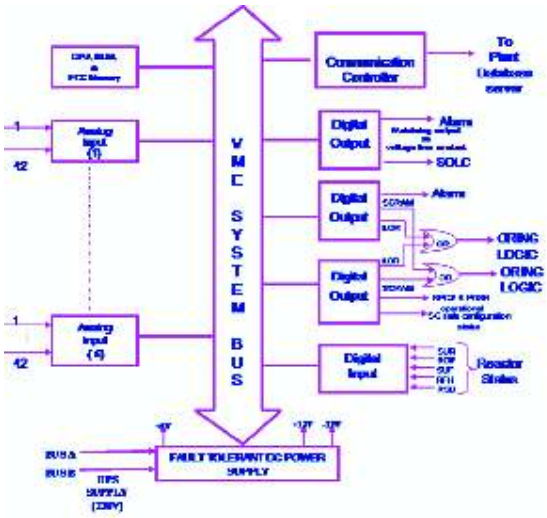

Fig. 9. Hardware architecture of RTCS

The application program is stored in the read only memory. The analog input card consists of multiplexer, amplifier, analog to digital converter, onboard memory and sequencer. The multiplexing and storage of digital data in the onboard memory is controlled by the sequencer. The onboard calibration signals are used to detect any drift in the amplifier or failure of analog to digital converter. The digital input board is provided with online testability feature which forces all the inputs to logical zero or logical one. The digital output board is provided with read back facility and watch dog timer. If the microprocessor hangs or application program enters into endless loop, the watch dog will time out thus forcing the output signals to fail safe state.

No operating system is used for the RTCS. The powers on RESET will SELF TEST which in turn checks all parts of RTCS. If any error is detected, the corresponding code will be displayed in the LED display on the facia panel. If no error is detected, the control will be transferred to the application software (Refer Fig.10).

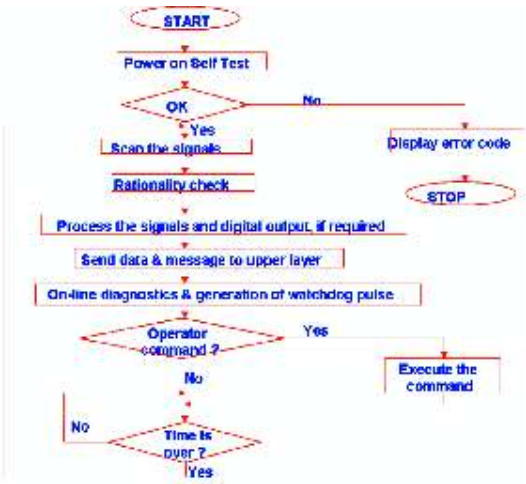

Fig. 10. Software architecture of RTCS

The application software consists of scanning the process signals, rationality check, processing the signal, generating the outputs and messages, communicating to upper layer and online diagnostics of the entire system. There is also provision to process the input from dumb terminal. Based on the input command, the corresponding software threshold will be edited. The software threshold is periodically transmitted to the upper layer for surveillance.

IV. SAFETY ANALYSIS OF INSTRUMENTATION AND CONTROL SYSTEM

It is very important to carry out safety analysis of I & C system during the design stage itself. Sufficient redundancy should be provided such that any random single failure should not either shutdown commercial nuclear reactor or place it in unsafe state. Hence neutronic sensors and signal processing systems are triplicated. RTCS for carrying out safety critical reactor core supervision are also triplicated. If p is the probability of failure then probability of failure of triplicated system is $3p^2$. Overall safety analysis of I&C system should address the effect of failure of power supply, failure of sensors, over range of sensors, reversal of sensor leads, electromagnetic interference, power supply with spikes, process noise, change in sensor characteristics with temperature or ageing, etc. Failure analysis of neutronic system should address failure of neutronic sensors, drift in the amplifier and failure of trip card. Failure analysis of safety logic system should analyze the effect of fault in two out of three voting stage, grouping stage, and power transistor and memorization circuit. Fault analysis of pulse coded safety logic should take into consideration the failure of clock generator, code generator, power transistor driving the coils and the optical link with other safety logic system.

Failure analysis of RTCS should address the failure of microprocessor, memory, bus transaction, etc. in CPU card, failure of multiplexer, amplifier, ADC sequencer, etc. in analog input card, failure of opto-coupler in the digital input card and failure of control logic in digital output card [1].

A detailed online diagnostics should be designed to periodically check the healthiness of the embedded system such that any hardware fault or software fault should result in generation of failsafe output to the nuclear reactor. The fault-tree analysis as shown (Refer Fig.11). should be verified by independent regulatory committee.

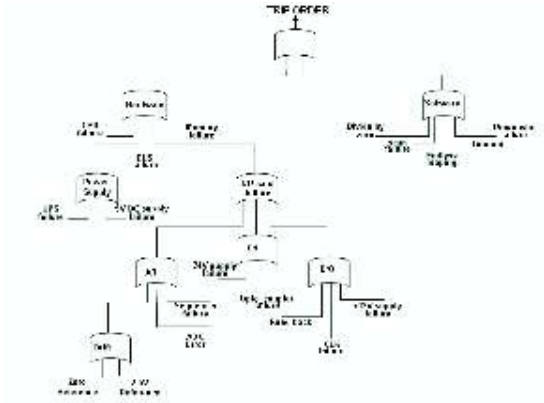

Fig. 11. Fault tree analysis

The testing interval should not be smaller than the required one as testing process itself may introduce unreliability in the smooth functioning of instrumentation and control. The testing interval is a function of the specified probability of failure, failure rate, time to complete the test and time to repair the faulty system as shown below:

$$P_{uf} = \lambda_{uf}(T_i + T_t + T_r) \quad [2]$$

λ_{uf} = Failure rate of unsafe failure
P_{uf} = Probability of unsafe failure
T_t = Time to complete the test
T_i = Time to complete the testing of the system
T_r = Time to repair the faulty system

The testing time for different parts of I&C systems of nuclear reactor is carefully arrived as shown below.

Table 1. Testing time for different parts of I&C systems

System	Testing Time	Test duration	T me to repair
Neutronic System	8hrs	0.5hrs	8hrs
Core Temperature sensor	1sec	-	8hrs
EM Flow sensor	1 sec	-	8hrs
Safety Log c System	3 min	-	8hrs
Real Time Com puter System	1 sec	-	8hrs

Development of application software shall follow water fall model. Documents shall be generated at different development stages as per applicable IEEE standards and shall be verified by independent committee as shown below.

Waterfall model for software development

The code shall be verified by static analyzer against unused variables; uninitialised variables etc [3].The number of parallel paths in flowchart should be preferably less than ten. Good coding practices like honoring MISRA-C guidelines shall be followed. (Refer Fig.12). for details.

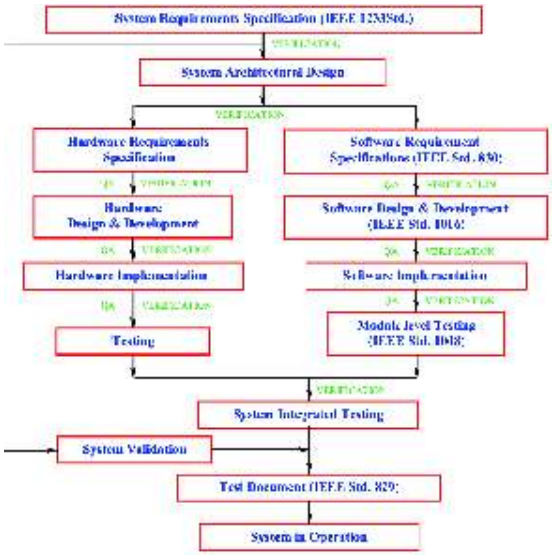

Fig. 12.Waterfall model

V. PFBR FULL-SCOPE TRAINING SIMULATOR

Most of the accidents in nuclear reactors are finally traced to inadequate design of I&C system, faulty operation of I & C system and human errors. To avoid accidents in nuclear reactors, it is very important to model the normal functioning as well as faulty functioning of instrumentation and control system. Modeling includes safety analysis and simulation in training simulator.

Full scope Training Simulator is required with the objective of providing comprehensive training to operators in the Prototype Fast Breeder Reactor plant operations. The scope of simulator covers the entire plant. Being a replica simulator, it completely replicates the reference plant configuration, control system, operator interface and information systems. It will have the control room identical to the actual plant.

The simulator is essentially made up of mathematical models of PFBR subsystems running in a computer system to replicate the operational characteristics of the plant. PFBR simulation involves developing models for various sub-systems like Neutronics, Primary & Secondary Sodium Systems, Steam Water System, Electrical System and associated control logics. PFBR Training Simulator is designed to simulate the steady state and dynamic responses of the plant in real-time to operator actions. The simulator is helpful in teaching the operators about the process dynamics, operations in normal and abnormal situations, various malfunctions & incidents as well as plant start-ups etc.

VI. SIMULATOR ARCHITECTURE

The full-scope, replica simulator consists of Simulation Computer, Process Computers, I / O system, DDCS, Instructor Station and Control Room Panels & Consoles, with a Simulator Network to interconnect all the components.

The simulation computer executes the integrated simulator code in real time to mimic the plant dynamics. It is based on powerful system with UNIX operating system. The process computers receive the plant information from Simulator system, process, and update the stored plant parameter database. The graphic display stations on the operator console and panels receive the data from these process computers and display the plant information in different formats.

The input/output system takes commands from the control panel/console, perform appropriate action and show the results on the panel/console. The I/O system contains the required number of digital input, digital output, analog input, analog output signal boards, and is placed behind the control panel. The I/O systems are connected to the simulator network (Gig-E) along with simulation computer, process computer etc.

The instructor station is used by instructor to control and monitor the operations of simulator and create various incidents/malfunctions during training sessions. The simulator control room panels and consoles provide the human-machine interface using which the trainees

operate and monitor the plant operations. They are exact replica of PFBR control room panels and consoles. It includes hardwired instruments, windows annunciations and display stations. Hardware layout of the simulator is shown in (Refer Fig.13).

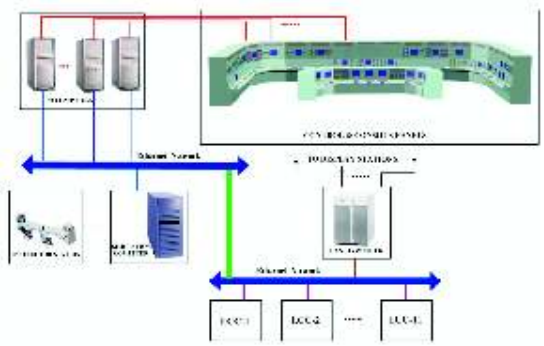

Fig. 13. Simulator hardware layout

The modeling software provides simulation model libraries, tools to build and integrate components and environment for running the simulator in real time. It includes Instructor, Executive, Database Server, IC logger and Messaging & Data Sharing Mechanism. (Refer Fig.13).

The Executive controls and synchronizes operation of the various simulator components. It ensures process synchronization and exchange of messages and data between real-time processes of the simulator. The Instructor module provides user interface to the simulator executive to control and monitor operations of simulator and conduct training sessions. The Messaging and Data Sharing Mechanism is an essential part of simulator which enables processes to exchange messages and share data between them. The Database server provides a single database for all the components of the simulator with multi-user access. The Logger provides a uniform, centralized mechanism to save and restore information about the state of the simulator and the user input. The modeling software provides the application-specific tools for:

- simulating the process models of conventional plant systems
- simulating plant controls
- emulating control panels and FDT with soft-screens

`Process models for non-conventional nuclear subsystems are developed as External or Foreign models and integrated into the simulator environment. The organization of simulator software components is shown in (Refer Fig.14).

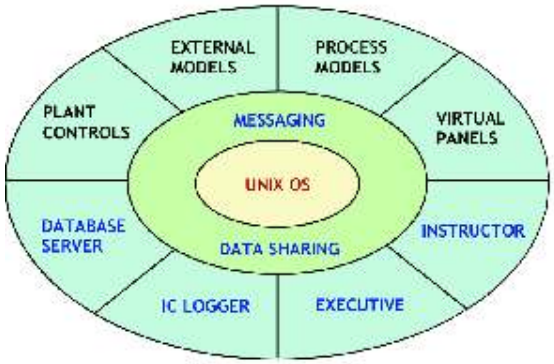

Fig.14. Architecture of simulator software

The malfunctions and incidents represent the unusual occurrences experienced during the plant operation which require adequate handling by the plant operator. In order to train the operator for such an eventuality, an exhaustive list of such possible incidents and malfunctions related to PFBR has been identified for modeling.

VII. DEVELOPMENT OF MODELS

All conventional sub-systems like hydraulic, steam air/gas and electrical as well as non-process elements such as actuators and transducers are simulated using the modeling software. Process Models for nuclear subsystems such as Neutronics, Core, Primary Sodium, Secondary Sodium, and Safety Grade Heat Removal Systems are developed from scratch and adopted as external models in the simulator environment.

During the development stage of simulator, the functions of the reference plant control room and operator interface are emulated using VDU based graphics systems called virtual panels. Virtual Panels are screen based soft-panels which emulate control panels and consoles with animated panel equipment icons. The virtual panels of the simulated subsystems of PFBR are shown in (Refer Fig.15).

In most of the training simulators, the normal operation of the nuclear reactor as well as the transient operation of nuclear reactor due to the failures of coolant pumps, station blackout, flow blockage in the fuel sub-assembly, etc. will be modeled.

The various faults identified during safety analysis of I&C system are modeled in the training simulator. One by one, all the faults will be introduced by instructor. For example, if unsafe fault in safety logic is introduced by instructor, corresponding alarm will be energized in the control panel and relevant error message will also be displayed.

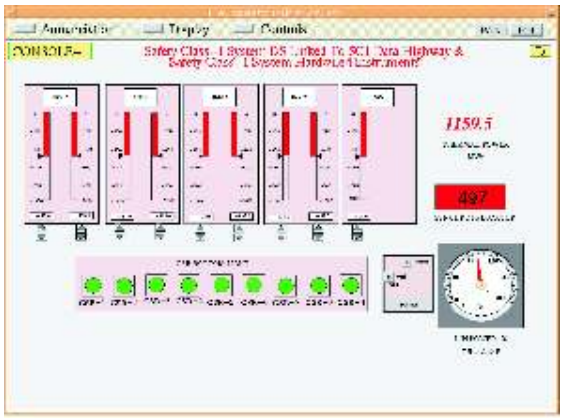

Fig.15. Neutronics modeling

The display format for data and messages shall be carefully chosen such that operator feels comfortable. Blue color should be avoided. Operator friendly menu driven display is preferred. Separate menu is preferable for mimics, trend, messages etc. Fault message should be in red color. The message should be flickering until operator acknowledges. Fault clear message should be in green color .There should be indication to show the presence of waiting messages. Page scroll facility is essential. The messages should also be stored in hard disk for retrieval. Screen print facility is required for operator to take print out of important displays. A typical display format is shown in (Refer Fig.16). for trend of process data.

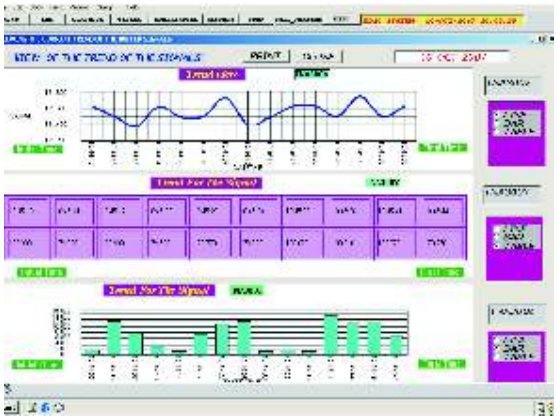

Fig.16. typical display format

VIII. CONCLUSION

Modeling of normal as well as abnormal functioning of I&C system is necessary to provide adequate training to operators of fast breeder Nuclear Reactor. Modeling also ensures proper fault analysis is carried out in I & C systems. Modeling also helps to provide adequate redundancy such that random failures do not shut down commercial Fast Breeder Nuclear reactor. Modeling itself shall be verified by Independent committee for licensing from regulatory authorities.

REFERENCES

[1] P.Swaminathan, Nov 2005, "Design aspects of safety critical Instrumentation of nuclear installations", International journal of nuclear energy Science and Technology Vol.1, pp 254-263

[2] P.Swaminathan, 2004, "Computer based online monitoring system for fast breeder test reactor". Entract.iaea.org/Ic/TM_HPP_Abstracts%5C Swaminathan.pdf

[3] T.Sridevi, P.Swaminathan March 2007, "Static analyzer for computer based safety systems" Journal of the Instrument Society of India Vol 37, pp 41-*48*