Abstract—Computer based Instrumentation & Control (I&C) systems are extensively deployed in the 500 MWe Prototype Fast Breeder Reactor (PFBR), which is under construction at Kalpakkam. They are employed in safety critical and safety related systems. Further, the hardware designed and developed for PFBR has already been deployed in Fast Breeder Test Reactor (FBTR) at Kalpakkam as part of refurbishment of aging Computerised Data Processing System (CDPS) based on Unipower-30 computer system.

Index Terms—TMR, VME, PLD, IS9000, IEC61000

I. INTRODUCTION

The I&C systems of PFBR are categorized as safety critical, safety related and non nuclear safety systems. Safety critical systems play a principal role in achievement of nuclear power plant safety by safe shutdown of the reactor followed by heat removal from the core and containment of radioactivity. Safety related systems play a complementary role in achievement of nuclear power plant safety. The efficient operation of safety related systems reduce the demand on safety critical system thus enhancing the availability of plant operation. Hence, in order to achieve high degree of safety and availability, redundancy and fault tolerance are employed.

Safety critical systems employ Triple Modular Redundancy (TMR) architecture to ensure the safety and availability of the plant is ensured and Safety related systems employ hot standby architecture to ensure high availability. In PFBR, the safety critical I&C systems are developed purely as hardwired based systems thus eliminating the unreliability factor of software. On the other hand Computer Core Temperature Monitoring (CTM) system is the only safety critical system employing computer. CTM system is used to detect flow blockage in fuel sub assemblies and initiate safety action. The large number of thermocouples (423 no’s) and the computations required to determine flow blockage forced the usage of computer based system for CTM.

Further computers are employed in safety related systems like control systems of Control & Safety Rod Drive and Diverse Safety Rod Drive Mechanisms to guide the removal / insertion of control and safety rods for safe operation of the reactor, drop time measurement and rod exercising.

Networking technology was conceived at design stage and incorporated in the design of the computer system. In PFBR all the safety critical, safety related and non nuclear safety systems are inter-connected via Distributed Digital Control System (DDCS) which is an integrated plant wide Local area network (LAN).

Since computer based systems are used for safety critical / safety related systems, the hardware and software reliability are of paramount importance in ensuring availability and safety of the plant. Hence, this calls for a hardware design and development methodology as well as robust software development cycle.

The computer based systems deployed in the safety critical and safety related applications needs to be designed as per Atomic Energy Regulatory Board (AERB) safety guides for deployment in Indian nuclear reactors. The hardware and software for the computer based systems have been designed and developed on the following criteria: Simplicity in design and based on proven principles, Procedure to detect faults in the system, Notify the occurrence of faults, Surveillance, Testability and Fail-safe capability.

A typical configuration of the system has successfully undergone qualification tests for environmental conditions as per IS9000, Electro magnetic interference / electro magnetic compatibility (EMI/EMC) as per IEC61000 Seismic qualification is in progress. This paper presents the system design and development process followed to ensure that a reliable and qualified safety critical / safety related I&C system is realized.

II. SYSTEM DESIGN AND DEVELOPMENT METHODOLOGY

The design and development of systems for safety applications is a disciplined process controlled at each step. It is organized as an ordered collection of distinct phases and each phase uses the information developed in previous phase. Modular design is followed for both hardware and application software. This enables easy up gradation and refurbishment of obsolete modules without affecting the overall architecture of the system. Verification is employed at each step to ensure that in the translation from one phase to the next phase, traceability to safety and functional requirements are met. The flowchart below provides the flow for system design adhering as per AERB safety guide for computer based systems.
III. HARDWARE DESIGN AND DEVELOPMENT METHODOLOGY

To achieve high availability of the computer based I&C system, it becomes essential to design the individual hardware modules to ensure high Mean Time Between Failure (MTBF). High MTBF is achieved by providing proper design margins, designing for noise immunity, providing proper cooling, using Industrial grade components only adhering to stringent quality policy on component selection and quality control at manufacturing phase.

For board designs, to begin with, the I/O interfaces, analog / digital portions and the digital blocks, which are amenable for implementation in PLD are identified. SPICE simulation is carried out for analog design. The digital logic design is carried out using schematic entry / hardware description language and simulated to ensure functional and timing correctness. De-rating is employed in design to improve the reliability thus enhancing availability.

As present day electronic devices have sharp rise / fall times, conventional Printed Circuit Board (PCB) design process followed for layout is inadequate. Hence, Signal Integrity, Cross-talk & emission analysis have been carried out. Thermal analysis is also carried out to determine operating temperatures. Further, to ensure a defect free product, stringent quality control measures have to taken up in the manufacturing phase as per IPC standards Class-3 criteria.

IV. SOFTWARE DESIGN AND DEVELOPMENT METHODOLOGY

The software performing safety critical and safety related systems are designed and developed using CASE tools. The application software is implemented in C language conforming to MISRA guidelines and this is the only component running on the hardware.

The Verification and Validation (V&V) is carried out by an independent committee and the following documents are generated in the process: System Requirements Specification as per IEEE-1233, Software Requirement Specifications as per IEEE-830, Software Test Documentation as per IEEE-829, Software Quality Assurance Plan as per IEEE-730, Software Design Description as per IEEE-1016 and System Test and Integration Plan.

V. QUALIFICATION TESTS

A representative computer system consisting of a fully loaded VME backplane with all the above types of cards with simulated inputs / outputs was subjected to testing and qualified as per IS-9000 standard for environmental conditions and IEC61000 standard for EMI/EMC.

VI. CASE STUDY: REFURISHMENT OF CDPS

CDPS of FBTR is a hot standby computer based system performing the safety critical function of detecting flow blockage in the reactor core, safety related function and non nuclear safety functions also. Failure of components due to aging, maintenance became difficult. Hence, the Unipower-30 based computer system was replaced with the in-house designed and developed hardware and software.

Modularity was adopted in design to split the safety critical, safety related and non-nuclear safety functions. After an independent V&V of the system, regulatory clearance was obtained for operating the plant with the new computer system (Fig.3). The system has been in operation for about two years and the operational experience has been good. Based on this feedback, it is also planned to replace the PDP11/84 system.

VII. CONCLUSION

The development of computer based systems for PFBR for achieving the high reliability and availability has been described. The deployment of the developed hardware in the central data processing system of FBTR has given good operational experience with regard to computer-based systems designed using PLDs. This operational experience has given the confidence for the usage of computer based systems in PFBR.

ACKNOWLEDGEMENT

The authors express thanks to Dr.P.Swaminathan, Director Electronics and Instrumentation Group for his constant encouragement and support during the design and development process.

REFERENCES