CONF-950397--

DESIGN AND TESTING OF INTEGRATED CIRCUITS FOR REACTOR PROTECTION CHANNELS*

R. E. Battle, R. I. Vandermolen, U. Jagadish, and B. K. Swail
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, Tennessee 37831-6010

J. Naser
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94303

I. Rana
Southern Company Services
P.O. Box 2625
Birmingham, AL 35202

To be presented at the
Joint DOE/EPRI International Conference on
Cost-Effective Instrumentation and Control Technology
Upgrades for Nuclear Power Plants

---

*Research sponsored by the U.S. Department of Energy under contract DE-AC05-84OR21400 with Martin Marietta Energy Systems, Inc.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

DESIGN AND TESTING OF INTEGRATED CIRCUITS FOR REACTOR PROTECTION CHANNELS*

R. E. Battle, R. I. Vandermolen, U. Jagadish, and B. K. Swail
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, Tennessee 37831-6010

J. Naser
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94303

I. Rana
Southern Company Services
P.O. Box 2625
Birmingham, AL 35202

ABSTRACT

Custom and semicustom application-specific integrated circuit design and testing methods are investigated for use in research and commercial nuclear reactor safety systems. The Electric Power Research Institute and Oak Ridge National Laboratory are working together through a cooperative research and development agreement to apply modern technology to a nuclear reactor protection system. The purpose of this project is to demonstrate to the nuclear industry an alternative approach for new or upgrade reactor protection and safety system signal processing and voting logic. Motivation for this project stems from (1) the difficulty of proving that software-based protection systems are adequately reliable, (2) the obsolescence of the original equipment, and (3) the improved performance of digital processing.

INTRODUCTION

Most nuclear power plants in the United States are operating with their original analog instrumentation and control (I&C) equipment. This equipment is approaching or exceeding its life expectancy, resulting in increasing maintenance efforts to sustain system performance. Decreasing availability of replacement parts and the accelerating deterioration of the infrastructure of manufacturers that support analog technology exacerbate obsolescence problems and resultant operation and maintenance (O&M) cost increases.

Instrumentation and control systems in nuclear power plants need to be upgraded in a reliable and cost-effective manner to replace obsolete equipment, to reduce operation and maintenance costs, to improve plant performance, and to enhance safety. The major drivers for the replacement of the safety, control, and information systems in nuclear power plants are the obsolescence of the existing hardware and the need for more cost-effective power production. Competition between power producers is dictating more cost-effective power production. The increasing operation and maintenance costs to maintain many

---

*Research sponsored by the U.S. Department of Energy under contract DE-AC05-84OR21400 with Martin Marietta Energy Systems, Inc.

of the analog systems is counter to the needs for more cost-effective power production and improved competitiveness.

Technological improvements, particularly the availability of digital systems, offer improved functionality, performance, and reliability; solutions to obsolescence of analog equipment; reduction in operation and maintenance costs; and the potential to enhance safety. Modern digital technology holds a significant potential to improve cost-effectiveness and productivity of nuclear power plants. Digital systems have the potential for solving the utilities* current problems of increasing analog equipment obsolescence; rapidly escalating operation and maintenance costs; lost generation due to system unavailability, spurious operation, and human error; and the inability to increase plant capacity due to equipment limitations.

The test for future digital I&C system upgrades will be whether they are cost beneficial to the plant and if they can offer a payback to the utility in an acceptable time period. Digital systems with their inherent advantages will be implemented in nuclear power plants only if reliable and cost-effective implementation and licensing acceptance is achieved and if the upgraded system supports reduced power production costs. Reliance on proprietary system suppliers coupled with new licensing and design issues have resulted in high implementation costs when digital upgrades have been performed in nuclear power plants.

Reactor protection systems will have the highest level of scrutiny by the Nuclear Regulatory Commission when they are upgraded and will potentially have the highest licensing acceptance costs. Concerns about software in protection systems, such as common mode failure and unintended functions, may be very costly to address in early microprocessor based system implementations. An alternative to a microprocessor-based reactor protection system is to develop an application specific integrated circuit (ASIC) based system. It is expected that the simplicity of the ASIC system will assure its reliability and will support easier and more economic licensing acceptance.

Application-specific integrated circuits (ASICs) in the form of field-programmable gate arrays (FPGAs) are being developed to demonstrate the feasibility of using ASICs in a reactor protection system. The demonstrator implements the pressurizer pressure channel and ΔT (core outlet temperature minus the core inlet temperature) / T_{avg} (average of the core inlet and outlet temperatures) channel computations and trip outputs of a typical pressurized water reactor (PWR). The pressure computations are relatively simple, and the $\Delta T/T_{avg}$ are the most complicated. The voting logic that would process the trip outputs is not implemented in the demonstrator. The concept used in the demonstration—based on a modular design—is an important part of the task. The modular concept, which uses digital processing, may offer advantages in maintenance, spare parts inventory, obsolescence, and verification and validation (V&V).

The concept uses modules that perform basic operations, such as multiply or add, as well as a controller that directs these basic modules in the performance of higher level functions. A few basic modules can perform all the safety functions required for a reactor protection system. Most of the reactor protection system channels are relatively simple and require only a few computations. In the demonstrator, the controller includes an FPGA and programmable read-only memory (PROM). The PROM contains sequential instructions that are sent to enable the basic modules. Intermediate results calculated by the basic modules are stored in random access memory (RAM), and constants used by the basic modules are stored in nonvolatile read-only memory (ROM). The modular concept was selected because it can be used to implement many higher level functions with only a few basic modules. These basic modules are standardized for use in any of the safety system channels. Only the controller PROMs are changed to implement a different channel.

WHY DEVELOP ASICS FOR SAFETY APPLICATIONS?

Because of obsolescence and maintenance costs, personnel at many of the older operating power plants will be deciding soon whether to replace or continue maintaining analog equipment. Options include continuing to maintain or refurbishing the analog equipment or purchasing new computer-based equipment. An ASIC-based design offers another alternative for consideration. ASICs have some advantages over computers and analog systems. Features that may be beneficial in licensing include the following: There is no software in an ASIC system, independent functions can be separated, and only the functions needed are included in the design. Each basic function is in hardware that is sequentially controlled by a controller that is in firmware. There are no interrupts in the system. Separation of simple modules and use of only the needed modules should simplify V&V.

Obsolescence is difficult to address and to solve, but a feature of ASICs may reduce the likelihood of having this problem. This feature is that ASIC designs use standard formats that are compatible with many different vendors' products, and fabrication of ASICs is within the capability and budget of many utilities. As long as the design format remains standard and supported by many vendors, it is feasible that a utility could move the design between several different products.

The compactness and modular design are also advantages of ASICs. Functions done by several different analog modules can be combined into one ASIC module, or the ASIC can replace the analog modules one for one. This option would be based on a trade-off between the need for more space and the cost of rerouting intercabinet wiring. In a reactor, each channel would contain the identical printed circuit cards and components except for the controllers that would be loaded with instructions specific for each channel. This concept requires fewer spare parts to maintain. The number of spare parts could be reduced further by the system operator loading instructions in the controller just prior to installing it. This eliminates the need to maintain different controller modules in inventory.

SYSTEM DESIGN

A simplified block diagram of the demonstrator that shows the modular design of an ASIC-based protection system is illustrated in Fig. 1. The basic modules in this design are add/subtract, multiply, square root, trip comparators, and a piecewise linear function. Other modules process the analog signals from the field by converting them into digital signals that are sent to a monitoring computer. The integrated circuits pass information over a data bus, and they are enabled for operation by separate control lines. The controller, shown in Fig. 1, consists of an FPGA and a PROM that manipulate the control lines to the basic modules. The dashed line encloses the components that are mounted on the ASIC printed circuit cards. The computer connects to the ASIC circuits with a 50-conductor cable. The FPGA includes a counter that increments the PROM instructions and controls RAM and ROM, and the PROM instructions actually manipulate the control lines that enable the FPGAs. The counter sequentially increments the instructions without any branches or interrupts. Constants, such as those used in filters and trip comparators, are stored in ROM. Intermediate results calculated by the basic modules are stored in RAM. The controller directs the RAM and ROM to place these constants and intermediate values on the data bus for use by the basic modules.

EXAMPLE MODULE OPERATION

An example of the operation of one of the basic modules is shown in Fig. 2. The operation of this multiplier module is implemented in hardware as enabled by the controller. The multiplier performs a 42- by 42-bit multiplication using a parallel-serial multiplier circuit, which requires one clock cycle for each bit of output. The multiplier operates as follows:

Two input storage registers, X and Y, load the numbers to be multiplied from the data bus. The X

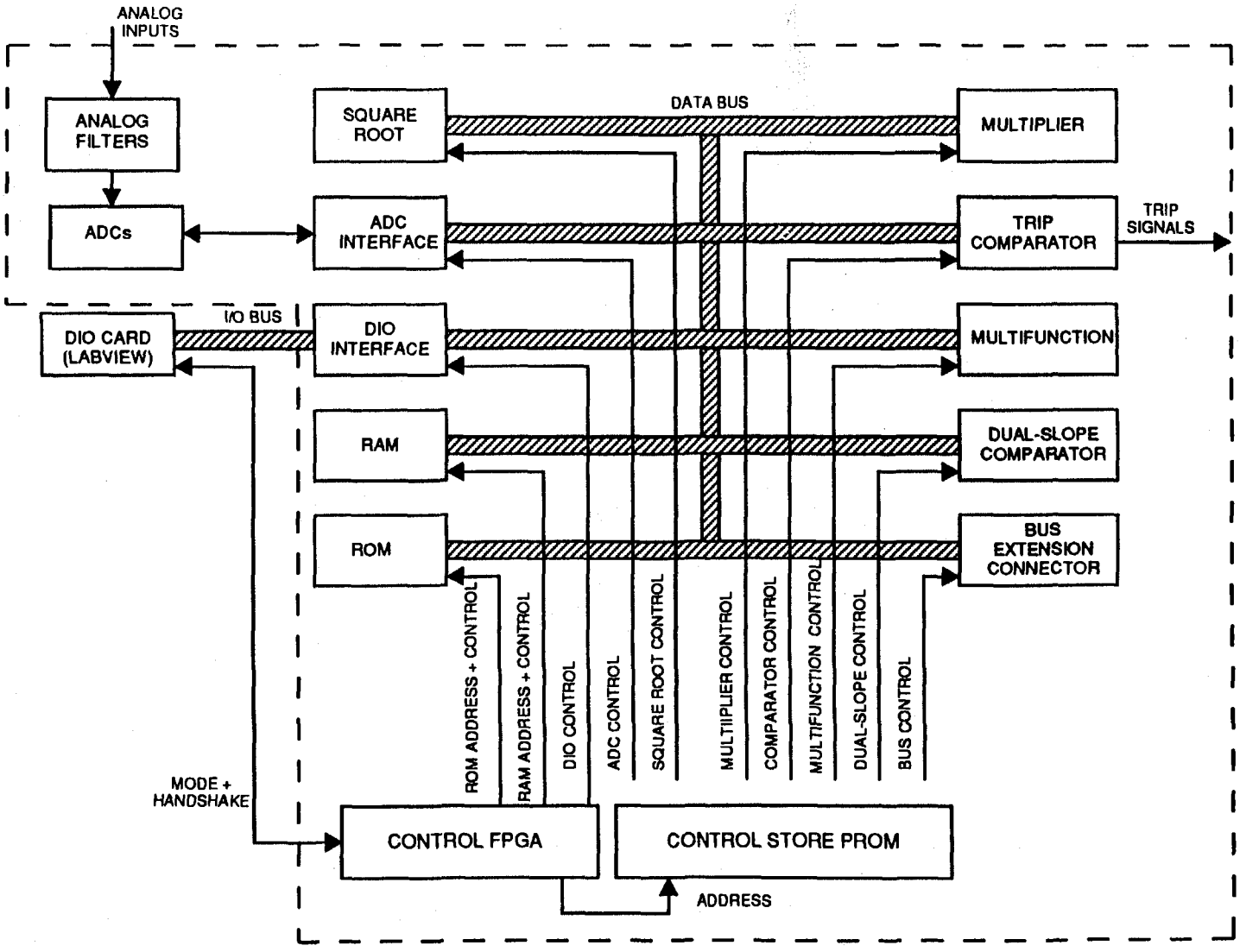

Fig.1. Modules composing an ASIC-based reactor protection channel.

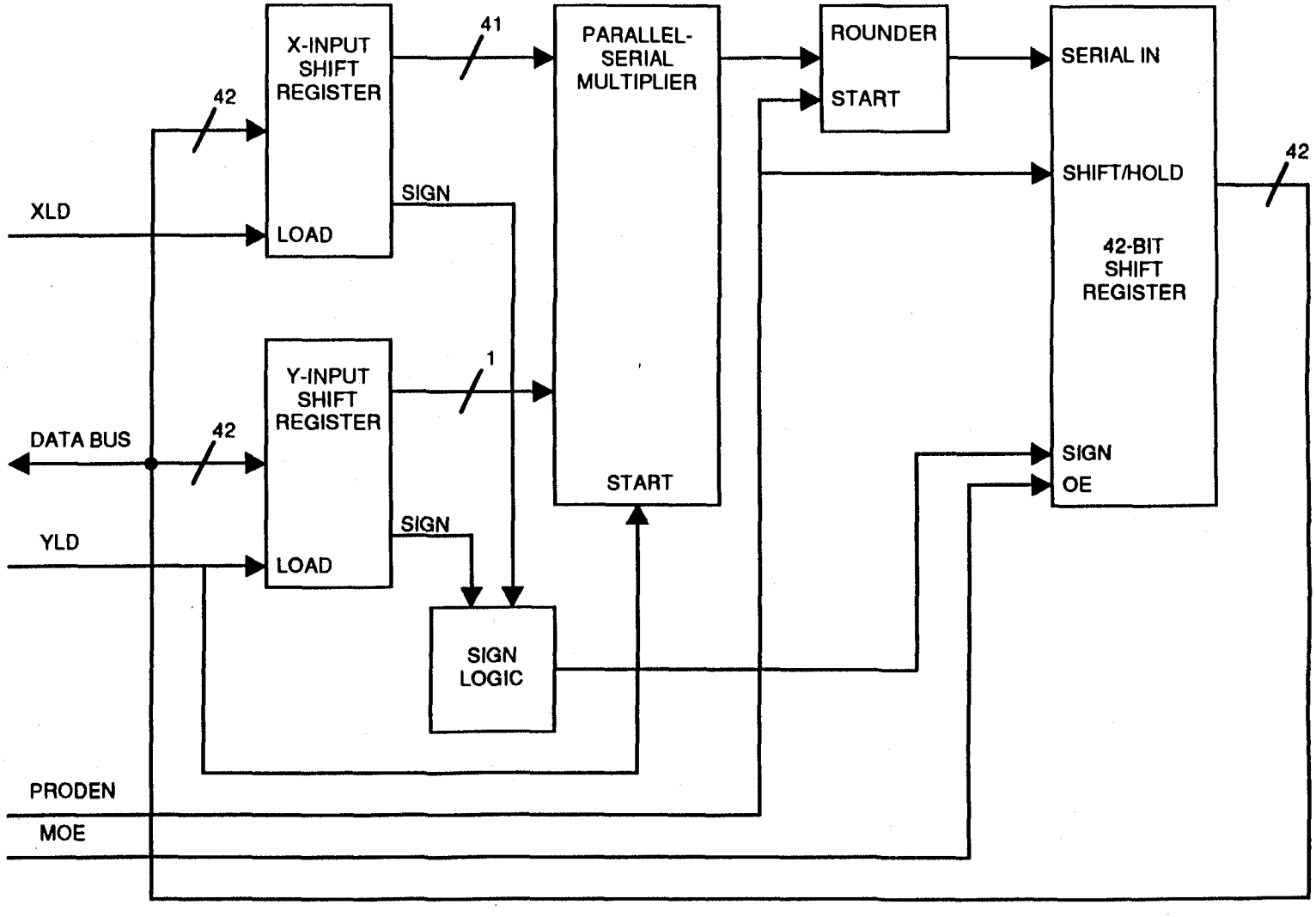

Fig.2. Functional blocks in the multiplier FPGA.

register is loaded first because the control signal that loads the Y register also starts the multiplication. The least significant bit (LSB) of the product appears at the output of the multiplier block on the clock cycle that YLD signal returns low and appears at the LSB of the output shift register on the following clock cycle. The multiplier output is 84 bits, of which only 42 bits (41 bits magnitude plus sign) are passed to the output. The PRODEN signal is driven high on the bit cell before the LSB of the desired 41-bit output and is held high for a total of 42 clock cycles. The multiplier output is available on the data bus any time after the PRODEN signal returns low. The rounder block automatically rounds off the product at the output's LSB. The 42-bit sign and magnitude result is placed on the bus for the controller to enable another module to use.

All the basic modules are controlled in a similar manner. Control signals enable a basic module, the module performs its hardwired function, and the result is put on the data bus. The controller enables RAM or other modules to read data from the data bus.

The demonstrator implements the safety and control computations for pressurizer pressure and for $\Delta T/T_{avg}$. The demonstrator currently does not include interface and isolation components to other systems, trip logic circuits, or special testing features. There is a human–machine interface (HMI), which is a computer accepting data from the ASICs, for users to monitor the performance of the demonstrator. This HMI software improves the quality of the demonstrator because it displays many parameters to an audience, but the software in the HMI has not been qualified for a safety system. The design does have a bus extension that can drive digital-to-analog converters (DACs) for dedicated safety grade displays. Selected parameters are sent to the HMI for display.

PRESSURE CHANNEL FUNCTIONS

For the pressure channel the safety and control computations include filtering the input pressure signal with a lead/lag filter and comparing the measured and filtered signals to trip set points. The pressure channel functions are simple, but they are typical of many reactor trip channels. The comparators include low and high trips, and the comparators have ~1% hysteresis to preclude rapid switching (chatter) of the output for a noisy or varying signal. The pressure channel functions are high-pressure trip, lead/lag filter prior to low-pressure trip, safety injection (SI) actuation on low pressure, and SI block permissive for pressure below its set point.

The pressure computations performed by the ASICs are given in Eqs. (1a–e). An infinite-impulse response digital filter implements the lead/lag filter. The algorithm for this filter is Eq. (1e).

$$\text{Reactor trip if } P(1) > P_h \tag{1a}$$

$$\text{Reactor trip if } P_f(1) < P_l \tag{1b}$$

$$\text{SI permissive } P(1) > P_p \tag{1c}$$

$$\text{SI actuation } P(1) < P_s \tag{1d}$$

$$P_f(1) = C1 * P(1) + C2 * P(0) + C3 * P_f(0) \tag{1e}$$

where

P_h = high-pressure trip set point,
P_l = low-pressure trip set point,
P_p = SI block permissive set point,
P_s = SI actuation set point,
$P_f(1)$ = the most recent (current) filter output,
$P_f(0)$ = the previous filter output,
$P(1)$ = the most recent measured pressure (current) input value,
$P(0)$ = the previous measured pressure input,
$C1$, $C2$, and $C3$ = constants calculated for the lead/lag filter.

Equations (1a–e) are performed in the following manner. Prior to running the safety and control algorithm, the system operator loads set points and filter coefficients into ROM and the pressure control algorithm into PROM. The hardware initializes RAM to zero on the first cycle. The controller directs the analog-to-digital converter (ADC) to read the pressure signal and store it in RAM. Next, the controller loads the pressure signal into the X register of the multiplier, loads $C1$ into the Y register, initiates multiplication, and stores the result in RAM. The controller performs the same operation with the previous filter output, $P_f(0)$, multiplied times $C3$, and performs it again with the previous pressure input, $P(0)$. It then adds the three terms together, two at a time, and stores the result, $P_f(1)$, in RAM. The controller moves $P(1)$ into the RAM location for $P(0)$ and $P_f(1)$ into the RAM location for $P_f(0)$ for the next iteration. The trip comparators are implemented last, as follows. Read the measured pressure from RAM into the trip comparator Q register and the set point from ROM into the P register. Place the hysteresis set point on the data bus. The trip comparator selects the trip set point or the hysteresis set point depending on the trip status of the output. Compare the numbers and set the trip. The trip comparator stores the trip condition in a register for output.

The basic modules used in the pressure channel are the multiplier, multifunction (add), and trip comparator. RAM stores intermediate values, ROM stores constants, and the controller directs operation. The $\Delta T/T_{avg}$ channels use all the basic modules several times because they include several lead/lag, lag, and rate filters, square root to linearize resistive-temperature devices (RTDs), and piecewise linear functions to account for flux tilt.

HARDWARE

The system is composed of three printed circuit cards (6.75 × 8.25 in.), a triple power supply (±15 V and +5 V), and a monitoring computer. The input signal conditioning board, card 1, contains analog antialiasing filters with dip switches to set the cutoff frequency, one 12-bit ADC per input signal, and an ADC input FPGA. The memory board, card 2, contains PROMs for storing the coefficients and set points, RAM for storing intermediate values, and the digital input/output (I/O) FPGA. The control board, card 3, contains the control PROMs and six FPGAs. Printed circuit cards 2 and 3 are mounted in one nuclear instrumentation module (NIM), and card 1 is mounted in a separate NIM. The power supply is mounted in a third NIM module. All are located in a 19-in. NIM rack.

The monitoring computer connection to the ASICs is through a 32-bit, digital data acquisition I/O card. Numerical values read from this card are converted to floating point and displayed on the computer monitor. The trip conditions and discrete inputs are read from the data acquisition card and converted to software indicator lights on the computer monitor.

SOFTWARE TESTS

The individual FPGA designs were tested with inputs that tested normal, extremes, and positive and negative values of the range of inputs. The outputs of the simulation tools were studied to verify proper functioning of the FPGAs.

After the individual modules were tested, the integrated design was tested. To test the functional results of the entire algorithm, the separate files describing each FPGA were combined along with test signals for simulation purposes. Because the simulation tools can handle only 1000 signals at a time, the test description file for the entire algorithm was written as four major integrated test files. The test vectors describing the algorithm were applied sequentially to the FPGA description files, and the intermediate results were routed between the test files to achieve a total test simulation. The entire algorithm was simulated for steady state response and for a transient response of the first 20 iterations. The steady state and transient responses were compared to a computer model of the protection algorithms. The computer model used double-precision, floating point computations, and the FPGAs used fixed-point computations. The responses were within 0.02%, which is sufficiently accurate for the reactor protection system.

HARDWARE TESTS

Each of the individual FPGA modules was subjected to individual tests to observe its functional behavior. The test vectors used for the simulation were applied to the FPGAs through a hardware test setup, and the test results on the data bus were observed and compared to the simulated software results.

The ADC board, the system board, and the digital I/O board were each tested separately. The boards were then connected and tested for continuity and functionality using a simple test routine in the controller that sequentially tests all the components in each of the three boards. After this, the setup was tested for the actual case by using the controller sequence that computes the entire protection system algorithm.

SUMMARY

A demonstration model of the pressurizer pressure and $\Delta T/T_{avg}$ channels of a typical PWR reactor protection system has been designed and built using FPGAs. The purpose of this demonstration is to evaluate the features of FPGAs and to demonstrate these features and capabilities to potential users in the nuclear industry. The demonstrator is connected to a computer for demonstration purposes to display the safety system parameters to those testing or monitoring its performance. The design concept uses modular components that can be used in many different protection system channels. The modular concept can be used to combine the functions of several analog modules into one FPGA module. It can also be used to separate independent functions. This concept has maintenance advantages because fewer different components must be kept in the spare parts inventory. A licensing advantage of the design is that the individual components are kept relatively simple so that V&V is less difficult.

DISCLAIMER