CONF-970649--2

TEST AND VERIFICATION OF A REACTOR PROTECTION SYSTEM APPLICATION-SPECIFIC INTEGRATED CIRCUIT

R. E. Battle
G. W. Turner
R. I. Vandermolen
Oak Ridge National Laboratory[1]

C. Vitalbo[2]
Westinghouse Electric Corporation

J. Naser[3]
Electric Power Research Institute

MASTER

Paper to be presented at the
1997 Embedded Topical Meeting on Advanced Reactor Safety (ARS '97)
Orlando, Florida
June 1-5, 1997

[1] Managed by Lockheed Martin Energy Research Corp. for the U.S. Department of Energy under contract number DE-AC05-96OR22464.
[2] Westinghouse Electric Corporation, Energy Center Site, P.O. Box 355, Pittsburgh, PA 15230-0355.
[3] Electric Power Research Institute, 3412 Hillview Ave., P.O. Box 10412, Palo Alto, CA 94303.

DISCLAIMER

TEST AND VERIFICATION OF A REACTOR PROTECTION SYSTEM APPLICATION-SPECIFIC INTEGRATED CIRCUIT

R. E. Battle, G. W. Turner, R. I. Vandermolen
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6010
(423) 574-5531
battlere@ornl.gov

C. Vitalbo
Westinghouse Electric Corporation
Energy Center Site, P.O. Box 355
Pittsburgh, PA 15230-0355
wx-vitablc@westinghouse.com

J. Naser
Electric Power Research Institute
3412 Hillview Ave.
P. O. Box 10412
Palo Alto, CA 94303
Jnaser@msm.epri.com

ABSTRACT

Application-specific integrated circuits (ASICs) were utilized in the design of nuclear plant safety systems because they have certain advantages over software-based systems and analog-based systems. An advantage they have over software-based systems is that an ASIC design can be simple enough to not include branch statements and also can be thoroughly tested. A circuit card on which an ASIC is mounted can be configured to replace various versions of older analog equipment with fewer design types required. The approach to design and testing of ASICs for safety system applications is discussed in this paper. Included are discussions of the ASIC architecture, how it is structured to assist testing, and of the functional and enhanced circuit testing.

I. INTRODUCTION

Application-specific integrated circuits (ASICs) were selected by the designers to simplify design and testing of a high-performance digital system, to achieve high reliability, to simplify maintenance, and to reduce spare parts and inventory costs for the users. Design is simplified by structuring the ASIC to consist of simple modular circuits that can be designed and tested independently of each other. Testing of the ASIC is simplified by implementing the safety algorithms with the simple hardware modules with access to the inputs and outputs. Component reliability is achieved by selecting a reliable manufacturing process. ASIC designs can be manufactured to have very high reliability. Installation costs are reduced by designing the equipment to replace existing analog protection system modules with minimal structural and wiring changes. Inventory reduction and maintenance simplification are accomplished with a single standard design that replaces many analog modules.

ASICs were designed for a reactor protection system (RPS) to avoid some of the problems associated with a software-based system. Significant advantages of ASICs are that only the required functions are included in the device and these functions are "hardwired." Because these functions are hardwired and because the ASIC is designed to have access to the inputs and outputs of these functions, test vectors can be designed to detect component failures. The ASIC circuits and their control components are designed such that there are no undefined states where the system can "hang." If there are no component hardware failures, the ASIC-based system implements its safety algorithm continuously. There are no interrupts, loops or branches that make decisions based on measured data, or undefined states. Each step is defined and repeated continuously in a loop. The ASIC design is structured to avoid these problems that may occur in software and that are difficult to find by testing.

II. ARCHITECTURE

The ASIC architecture contains circuits organized in functional and physical modules that can be accessed from the input and output pins of the ASIC package. Access to each of these modules is

beneficial in the operation and testing of the ASIC. Each modular circuit is constructed hierarchically to simplify design, testing, and operation of the ASIC. The basic modules include functions such as add, subtract square root, shift left, shift right, two's complement, multiply, divide, along with other functions necessary for process control. At the very top of the hierarchical design is the ASIC with its inputs and outputs, and the next lower level contains the basic modules, such as an adder, along with the external connections to the high-level blocks. At the level of the hierarchy containing the adder as a block, the adder inputs and outputs are included without other details of the adder. At this level, a user who is testing or operating the block needs to know only what the inputs and outputs are but not the details of operation. The next lower level contains the submodules used in the adder. Each submodule can be isolated for testing or design without affecting or knowing the operation of other submodules at the same level. This hierarchical structure continues until eventually at the bottom of the hierarchy are the primitive cells used to implement the hardwired logic required to add two numbers. This approach was used throughout the design and testing of the ASIC. This hierarchical structure is a technique used to manage the design and testing of the ASIC.

III. FUNCTIONAL SIMULATION TESTING

Functional testing of the design was based on ensuring that each of the ASIC submodules performed properly, which was done from the low level modules up to the high level modules. The requirements for the basic functional modules in the ASIC came from the ASIC specifications to replace analog cards functionally. The ASIC specifications were written based on the requirements to replace analog safety system modules currently in use in nuclear power plants i.e., one ASIC-based card was designed to be a functionally equivalent replacement for multiple analog cards. First, the ASIC designer made a functional logic block and tested it to confirm that it performs as required. If it did not operate properly, the design was modified until it performed as required. After the functional logic blocks were designed and tested, the blocks were assembled as a unit, and tested with a functional command file and revised if necessary. Finally, all the architectural blocks were assembled into the ASIC core and tested. The final design then consisted of modular organizations of hierarchical components that were designed and tested at each stage. All of these simulations were functional tests that do not involve performance characteristics of the electronics on the ASIC.

The core layout is done after the ASIC core design is complete as described in the previous paragraph. The layout, which is still part of the design phase, is tested using a timing-based simulator. Because the ASIC is much slower than its tested capability, timing will not be a problem with this application. If problems or improvements are identified during the timing simulations, the design can be revised and retested. After the core design and layout are complete, the input and output pads are added to the design and the design is tested again with the timing-based simulator. The functional tests used for logical and timing performance were selected to test the design for normal and for extreme or boundary conditions. When these tests are completed, the design is submitted to a foundry for fabrication.

Testing of the fabricated ASIC involves functional testing to confirm that the design is correct and enhanced testing to detect failed components within the ASIC after fabrication. The enhanced test vectors applied to the fabricated ASIC are developed with the intention of operating every gate in the ASIC. It is not feasible to test every combination of inputs, but it is feasible to test all gates within the ASIC. Although it is possible to develop test vectors that operate all gates in an ASIC, there may be problems observing these gates operating because they can be monitored only from the output pins. The number of gates that can be observed during factory acceptance testing was increased by including a "monitor bus" in the ASIC design. This monitor bus adds circuitry and some complexity, but it increases the fault-coverage. The fault coverage is the ratio of the number of gates tested divided by the total number of gates in the ASIC. The monitor bus is an eight-bit wide data bus, which is used for factory acceptance testing only, that is connected to internal circuits. The monitor bus can be made to run at a higher speed than the clock controlling the other modules in the ASIC such that it can observe transitions of the internal circuits. It monitors asynchronous circuits, and it monitors internal circuits that operate in more than one clock cycle. The monitor bus increases the fault-coverage of the test vectors, but it is still possible that the operation of some gates cannot be observed from the output pins including those connected to the monitor bus.

The operation of these gates are confirmed by the results of the functional testing of the ASIC.

IV. ENHANCED TEST VECTOR DEVELOPMENT

The functional tests developed for design testing are subsets of the vectors that will be used in the enhanced test set. The purpose of the enhanced test set is to prove that a fabricated ASIC does not have any defective components. The enhanced test vectors are made by an ASIC designer using special knowledge of the circuits that help to test the circuits completely. Although the first set of enhanced vectors generally do not result in sufficient fault-coverage, there are tools to perform fault grading and to enhance the coverage after the first set is developed. This technique is discussed below. Each input test vector has an output result that is compared at the output of the ASIC. These comparison results are derived by inputting the vectors to the ASIC design, which has been thoroughly tested previously. Testing of the fabricated ASIC is done by inputting these test vectors and observing the ASIC's standard and monitor bus outputs. This monitoring and comparison can be automated by the vendor fabricating the ASIC. This test facility is described below.

After the input and output vector sets are developed, a test facility is made as shown in Fig. 1. This test facility includes mounting devices for the ASIC, hardware to interface to the input and output pins of the ASIC, a simulator that generates input vectors and acquires output vectors, and a workstation to control the operation of the simulator. Prior to testing the fabricated ASIC, the test vectors and the ASIC responses are thoroughly reviewed by observing operation of the ASIC simulation. The simulations are used to compare to the results of the simulations. The workstation compares the output of the ASIC to the output vectors developed on the design. Errors are identified, and defective devices are rejected. ASICs that pass this test are sent to the printed circuit board manufacturer.

V. TEST VECTOR GENERATION

There are features in this design that improve testability and enhance the reliability of the ASIC. One feature is that the design is hierarchical and modular such that it is simpler to access inputs and outputs of each module. The entire hierarchical design is based on primitive gates, which have output results for all inputs. The circuit uses a single clock , which avoids the problems associated with phasing of multiple clocks. Also, all but some of the lower level circuits operate synchronously. Because the clock runs slowly compared to the capability of the circuits and because the circuits operate synchronously, there are no problems with racing between different circuits that can cause intermittent operation depending on which circuit finishes first. There are only a few basic modules in the ASIC, and the responses of each of these modules is well defined. There is an internal monitor bus included for the purpose of improving fault-coverage. By toggling the inputs to all gates the gates and their connectivity are tested. The toggling of all gates will detect stuck-at-one, stuck-at-zero, or shorted outputs.

An example of simple tests of a register are shown in Fig. 2. Data are input to the register under control of the Write Data command, and the data are output by the Read Data command. The input data is varied to test that the register stored the data correctly. Steps 1 through 5 in the figure are repeated until the register is tested sufficiently. This technique is applied to each modular circuit in the ASIC.

After an original set of test vectors is generated, they are applied to the design with the assistance of a fault grader. The fault grader determines the gate coverage, i.e. the percentage of gates tested divided by the total number of gates in the ASIC. The fault grader also helps locate gates that were not tested by the original test vectors. The designer, with the assistance of an automatic test vector generator (ATVG) makes additional vectors to increase the coverage. It is a goal to get 100% coverage, but this is not always feasible because some gates may not be observable from the output pins. The RPS ASIC includes a monitor bus to access internal gates, but even with this bus some gates may not be observable. It is then up to the designer to evaluate whether the coverage is acceptable.

The vectors developed by this method are evaluated on a test facility, they are refined for manufacturing acceptance testing, and then they are applied to the fabricated devices as acceptance test vectors. The test vectors may be refined by the manufacturer to eliminate redundant tests because the user must pay for the test vectors. This refinement is a tradeoff between the cost of reducing the test vector set and the cost of testing. Only if there is a large number of ASICs being fabricated is there a cost advantage to eliminate some of the test vectors.

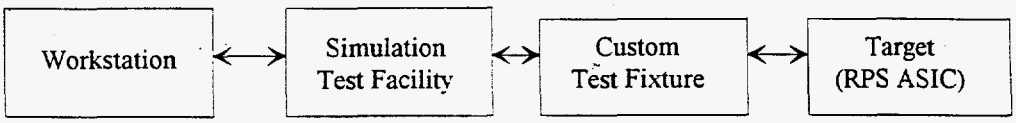
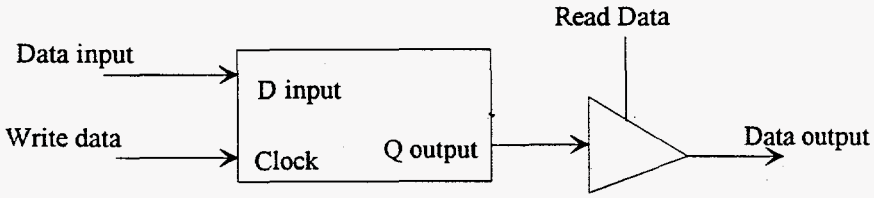


Figure 1. Prototype test facility.



Steps to test.
1. Load data bus.
2. Write input data
3. Clear data bus
4. Read data bus
5. Compare results

Figure 2. Register test to write, read, and compare data.

VI. CONCLUSION

An application-specific integrated circuit was designed for high reliability service in a reactor protection system. High reliability was achieved by designing the ASIC modularly so that it can be thoroughly tested. This was done by making the design synchronous with a single clock without interrupts so that the results are deterministic. The test vectors were developed in the same sequential, modular structure as the circuits. Also a monitor bus was included to increase the fault coverage and make the circuits highly observable. The first set of test vectors were developed by the designer using data patterns, data path, and statistical deductions. These vectors are then applied to the ASIC design and evaluated using a fault grader to determine the coverage of these vectors. Next an automatic test vector generator is used to increase the coverage. After these vectors are refined they are applied to the fabricated ASICs and compared to the results of the vectors applied to the design. These tests prove that the manufactured ASIC has no defects.