Warren A. Hunt, Jr.

FM8501: A Verified Microprocessor

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Jaime G. Carbonell
School of Computer Science, Carnegie Mellon University
Schenley Park, Pittsburgh, PA 15213-3890, USA

Jörg Siekmann
University of Saarland
German Research Center for Artificial Intelligence (DFKI)
Stuhlsatzenhausweg 3, D-66123 Saarbrücken, Germany

Author

Warren A. Hunt, Jr.
Computational Logic, Inc.
1717 West 6th Street, Suite 290
Austin, TX 78703-4776, USA

CR Subject Classification (1991): B.6, I.2.2-3, F.4.1, B.2.4, B.4.4, B.7.2

ISBN 3-540-57960-5 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57960-5 Springer-Verlag New York Berlin Heidelberg

CIP data applied for

Typesetting: Camera ready by author
SPIN: 10132079 45/3140-543210 - Printed on acid-free paper

Acknowledgements

My colleague Bill Young reformatted this document from Scribe™ to LaTeX. He also remade all of the drawings. This conversion was a larger job than either of us expected. I am quite thankful for his effort, because without it this book would not have been possible.

This work originally appeared as the author's dissertation, Department of Computer Science, the University of Texas at Austin. The work was partially sponsored by the National Science Foundation (Grants DCR-8202943 and DCR-8122039), the Department of the Navy, Space and Naval Warfare Systems Command (Contract N00039-85-K-0085), and British Petroleum North America, Inc. It appeared as Technical Report 47, Institute for Computing Science, the University of Texas at Austin, February, 1986.

W. A. H.

Preface

The hardware specification and verification ideas presented in this monograph germinated while I was taking a graduate class from Boyer and Moore in 1982. It was during their class that I was first introduced to logic. By the end of this class, I had written an instruction-interpreter specification for a Z80 microprocessor [51]. At this point, I had not seen any other work for mathematically specifying digital hardware except Boolean logic and ISP descriptions. At this point also, I was a digital design engineer for Cyb Systems, Inc., where I was designing Multibus[26] compatible cards for a Unix minicomputer. These designs were based upon the Motorola 68000 microprocessor [35]. During 1983 and 1984 I worked full time as a board designer, but I continued to be interested in formalizing a microprocessor. This interest was motivated both from an intellectual curiosity and from my personal frustration at attempting to engineer correctly designed boards. Each time I designed a board, I had to agglomerate specifications provided by device manufacturers in an attempt to produce some board with greater functionality. This was performed in a "rigorous" manner, but without any mathematical connecting tissue.

In 1985 I returned to the University of Texas to complete my degree. Originally, I had hoped to mathematically specify an existing microprocessor for my dissertation work, but I felt that the documentation available to me did not adequately specify all their operational aspects. I also realized that to specify and verify an existing microprocessor would require me to have access to a commercial design – this would require a non-disclosure agreement which would prevent me from publishing the results of my effort, thus no degree could result. In the beginning of 1985, I began the FM8501 effort which resulted in this monograph and this monograph was submitted as a dissertation at the end of 1985 in partial fulfillment of the PhD degree requirements at the University of Texas at Austin under the advisorship of Bob Boyer and J Moore.

The FM8501 microprocessor was invented as a generic microprocessor somewhat similar to a PDP-11 [13] — "FM" stood for functional machine and "8501" stood for the first machine of 1985. This was an optimistic naming convention; the FM8502, a 32-bit variant of the FM8501, wasn't completed until 1987. The principal idea of the FM8501 effort was to see if it was possible to express the user-level specification and the design implementation using a formal logic,

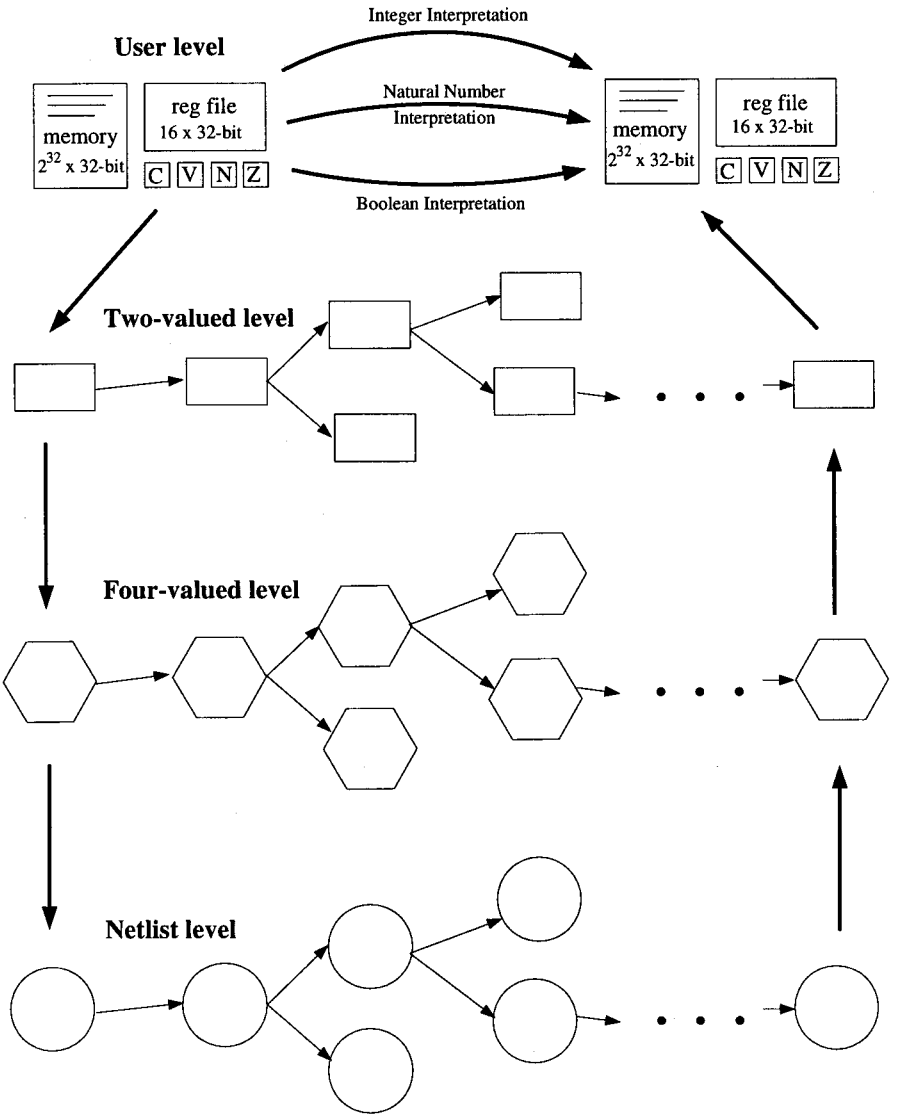

Figure 0.1: Specification Levels

the Boyer-Moore logic; this approach permitted us to complete a mechanically checked proof that the FM8501 implementation fully implemented its specification.

The implementation model for the FM8501 was inadequate for industrial hardware design. Circuits were expressed by overloading functions in the Boyer-Moore logic. This modeling technique allowed the specification of the necessary combinational connecting gates and registers, but did not allow wires to be named explicitly. Further, this approach did not provide a direct migration path to CAD languages, from which a physical device could be built. Since the FM8501 effort Bishop Brock and I have formalized a simple hierarchical, occurrence-oriented hardware description language (HDL) [25, 9]. The formalization of this HDL made the hardware circuits explicit – a formal circuit semantics and syntax exists for the HDL – and provides a simple means of converting designs into commercial CAD languages. Our HDL semantics include four logical values: true, false, undefined, and floating, thus providing a richer modeling capability than used with the FM8501.

Our current approach can be contrasted with the FM8501 effort by comparing our recent FM9001 microprocessor verification. Figure 0.1 shows the four specification levels we used for the FM9001; only the top two levels exist in the FM8501 effort. The two-valued level was the implementation level for the FM8501. The FM8501 had separate data input and data output busses because we were not able to model bidirectional wires. For the FM9001, the two-valued level is a Boolean model of the implementation with the tri-state memory interface bus abstracted away. The four-valued level is functionally equivalent to the netlist level. The netlist level describes the actual gates, wires, I/O pads, and test logic that are actually needed to construct the FM9001 microprocessor. The FM9001 design verification takes into consideration the I/O pads and test logic as well as the functional gates and registers. We had LSI Logic, Inc., fabricate the FM9001 design using one of their gate-array families. We have not discovered any errors in the fabricated devices after several months of testing.

The FM8501 effort was an important step in our evolution to the design verification methodology we now employ.

Warren A. Hunt, Jr.
Austin, Texas

January, 1992

Contents