The Knowledge Engineering Review, Vol. 10:3, 1995, 305–306

Book review

A safety licensable computing architecture by W. A. Halang, S.-K. Jung, B. J. Kramer and J. J. Scheepstra, World Scientific, USA, 1993, pp 251, £63.00 (h/b), ISBN 981-02-1628-9

Embedded computer systems are now in widespread use in safety-critical applications: for example in nuclear plant monitoring, flight control systems and process control. They are displacing purely hard-wired systems because of the power and flexibility offered by software based control. Such power does come with a price: if the components of software can be combined in many more ways, then as one might expect, the ways in which failures can occur increase too. It becomes very difficult to analyse the safety and reliability of such systems, and since such analysis is essential if systems are to be "certified" for use then undisciplined use of software is unacceptable.

The authors present a computer architecture and disciplined development approach, in which control applications can be produced such that developers and assessors can achieve greater confidence in system integrity. The approach is based around fault tolerant hardware, utilising formally developed micro-processors (for example, VIPER), with a set of general-purpose and application-specific functional primitives frozen in ROM. Application programs become very simple: a set of calls to the functional primitives. The functional primitives can be formally developed, and their heavy use should ensure a large amount of operational evidence on their reliability. Application programs can be built graphically (with adequate tool support) from these components, and the object code subjected to diverse back-translation for its verification. The whole approach rests on the premise that it is possible to identify a set of general and application specific functional primitives, and the authors' experience seems to bear this out (principally in the chemical processing industry). The first chapter provides a brief introduction to the approach and, at eight pages, is a worthwhile read. The second chapter, however, is a rather uninspiring 50 page overview of "State of the Art in High Integrity Computing" (or should it be State of Affairs). Some rather cumbersome use of English makes this chapter and the book as a whole a laboured read—editing by a native English speaker familiar with the domain would make the book more reader-friendly.

Then we have a very reasonable overview of Programmable Logic Controllers (PLC), with details of Instruction Lists, Ladder diagrams, Functional Block Diagrams, Sequence Function Charts and Structured Text as means of designing their behaviour.

The next two chapters, probably the best of the book, describe the approach in more detail, and give a high level description of hardware. The chapter devoted to the latter was, for me, rather too brief, and could have used some of the pages taken up by the "State of the Art" chapter.

We are treated to an in depth look at "Rigorous Firmware Development" in Chapter 6. We learn how the algebraic specification language, OBJ, may be used in the specification of programs, and also get a sprinkling of theory in weakest pre-conditions, and Hoare style proof rules. This is by far the longest chapter in the book, 60 pages. It will appeal to the theorists, but anyone else would be justified in feeling this chapter was too long. The balance is not right. There are also some printing errors: an unexpanded reference "Kirchner-EtA188:OBJ3" that should have been converted to "[76]", and a stray "defterm" which adds to the impression that the book was not adequately reviewed prior to printing.

The other significant parts of the book are a description of the toolset for building control software, and an appendix detailing the hardware in KAiserslautern Register transfer Language (KARL III).

I would say that the book is more appropriate for an interested practitioner rather than a student. It reads very much like a converted thesis, a significant number of the entries in the

bibliography are in German (a major problem for UK monoglots), the English is rather laboured, and the effort devoted to the subject areas could be better balanced.

The problem addressed in this book is a rich vein of research, the approach suggested a promising one, the presentation is, however, a little disappointing. Parts of the book are well worth dipping into, but when it comes to obtaining the book I would rather use a library card than a credit card. An improved second edition may change my views.

Reviewed by Stephen Wilson, University of York, UK