A formal specification of the steam-boiler control problem by algebraic specifications with implicit state

M.-C. Gaudel P. Dauchy C. Khoury

LRI, Université de Paris-Sud & CNRS, Orsay, France

1 Abstract

This paper concentrates on the specification of the requirements for the Steam-Boiler Control System. It contains a detailed analysis and specification of the sent and received messages, the different states the system can be in, etc. Special emphasis is put on the analysis of checking the physical devices and detecting failures in the system environment.

The paper uses an original approach that combines algebraic specification techniques with a notion of state where state changes are achieved by so-called modifiers.

The paper begins with a brief survey of the implicit state approach. Then two parts are devoted to the requirement analysis for the fundamental cycle of the system and the messages exchanged with the environment. The first version of the specification is a simple sketch which is then gradually refined following closely the informal specification and the addendum. The fourth part of the paper elaborates on the specification of failure detections and the checks of the physical devices. Then, in part five, the detection of transmission failures is described. Finally, the different functioning modes of the system and the changes of mode are specified in part six. We conclude by summarizing some incompletenesses and ambiguities discovered in the original informal specification.

2 Answers to the evaluation questions

1. Which parts of the system are specified at which level and in which way? (verbally, rigorously, formally?)

The paper provides a formal requirements specification for the control program.

2.a. Does the solution comprise an implementation of a control program?

b. Has the control program been linked to the FZI simulator?

c. Has some experimentation been done with the control program?

No for a,b,c.

3. What are the comparable other solutions and what are the major differences wrt them? What other solutions complement the given solution and in which respect?

BCPR. M. Bidoit, C. Chevenier, C. Pellen, J. Ryckbosch: An algebraic specification of the steam-boiler control system.

BBDGR. C. Beierle, E.Boerger, I.Durdanovic, U. Glaesser, E. Riccobene: An evolving algebra solution of the steam-boiler problem

OKW. P.C. Olveczky, P. Kosiuczenko, M. Wirsing: An object-oriented algebraic steam-boiler control specification

(answers to be elaborated later on)

4. a. How much time has been spent on producing the solution? Give the number of person-months, if possible for the various parts of the solution.

About 1.5 person-month.

b. How much preparation is needed to become sufficiently expert of the used specification framework in order to be able to produce a solution to such a problem in that framework? Indicate the number of weeks of training which you believe is needed for an average programmer to learn the method.

We estimate 8 weeks of personal experience, including a 2-week course on logic, algebraic specifications, and implicit states.

5. What are the premises for a good understanding of the proposed solution?

Logic.

a. Is a detailed knowledge of the used formalism needed?

No.

b. Can an average programmer understand the solution?

Yes.

c. How much time do you believe is necessary for the average programmer without knowledge of the used specification method to learn what is needed to be able to understand the solution?

2 weeks.