The Dagstuhl Steam-Boiler Controller-Problem The TLT Solution

Jorge Cuéllar*, and Isolde Wildgruber

Siemens R&D, ZFE T SE 1, D-81730 Munich, Germany

Abstract. This paper presents the TLT specification of the steamboiler control-program described in [Abr95] *together* with a rigorous model of the dynamics of the physical process and of the embedding of the discrete program in the continuous environment. The text of the TLT specification of the control program is short and easily understandable. The proofs that it satisfies the specification of [Abr95] are very simple. This is basically due to the chosen abstraction level. Program constants and variables are clearly distinguished from physical quantities, and it is shown, that under some conditions the program variables approximate the physical quantities. Hybrid and real-time aspects of the system are also considered, including several positive and negative results regarding the expected properties of the system.[2]

* Correspondence to: Jorge.Cuellar@zfe.siemens.de

[2] Supported in part by a BMBF grant from the German Federal Ministry of Education, Science, Research and Technology under contract number 01IS519A (project KORSYS).

1 Evaluation

In this section, we answer the evaluation questions posed by the editors.

1. Does the solution comprise a requirements specification?
   Yes. As explained in section **??** the informal specification text has been translated (quite trivially) to a formal requirement specification. (The text of this requirement specification as such is not presented here).

2./3. Does the solution comprise a functional/an architectural design?
   Yes. The specification in the sections **??** and **??** may be seen as both.

2'.3'. Has the functional/architectural design of the solution been verified against the requirements specification?
   Formally: proofs were performed by hand in a formal setting.

4.a. Does the solution comprise an implementation of a control program?
   Yes, a C implementation has been derived from the TLT specification.

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

4.c. Has some experimentation been done with the control program?
   Yes, experimentation showed that some assumptions on the environment (see Section **??**, Footnote 19) were incorrect. We also found some errors in the simulator. For instance, the simulator did not handle properly detected failures that, according to his perspective, had not happened. These detected but not really existing errors occur as we have seen because under some situations some errors may be confused, or after a REPAIRED we expected the pumps to be in a state different from the one by the simulation.

7.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.
   The first version of the program (which is slightly different from the one presented here) required 2-3 person months, including the C program and the experimentation.

7.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.
   Assuming familiarity with first order logic and basic automata theory, about 1 week.

8.a. What are the premises for a good understanding of the proposed solution? Is a detailed knowledge of the used formalism needed?
   Familiarity with the syntax of first order logic.

8.b. Can an average programmer understand the solution?
   Yes.

8.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?
   1 hour.

References

[Abr95] Jean-Raymond Abrial. Steamboiler Specification Problem. *Dagstuhl Seminar 9523*, June 1995.

This article was processed using the LaTeX macro package with LLNCS style