Abstract

We specify a controller for a steam boiler as described in an informal requirements document that served as the basis of a competitive case study in formal methods in computer science. We emphasize the use of modules as a means to make the task of writing a detailed specification manageable and enhance confidence in the correctness of the resulting product. Our formal language is Lamport's Temporal Logic of Actions. The specification is intended to be unbiased with respect to later implementation. We show how such a specification can be obtained by stepwise refinement from an initial high-level description, and discuss open and closed system specifications. Although we do not give a concrete implementation of our specification, we derive an analysis of the data flow in the control program from our specification and prove that it can be implemented.