A Combined Approach to the Steam Boiler Problem Using FOCUS, LUSTRE and Probability Theory for the Design of a Reliable Control Program – DRAFT –

Christoph Andriessens and Thomas Lindner

Forschungszentrum Informatik (FZI)

Abstract. This paper describes a combined formal approach to the Steam Boiler Problem. We show how the problem of specification correctness can be addressed using a careful initial phase which we call *system identification*. In this phase we use a rigorous refinement approach and apply the formal method FOCUS to decompose the task of implementing and verifying the control program into three components:
First, a *Communicator* module is identified and designed using the synchronous language Lustre. The correctness of this module, which deals with the message exchange with the console of the system, is proved using symbolic model checking.
The second module is the *Failure Manager* which deals with the detection of equipment failures and the estimation of the water level. We argue that a deteministic model makes no sense for this module and present a probabilistic approach based on Probability Theory. We calculate probablilities for the correctness of the failure detection and thereby quantify its reliability.
The third module is the *Pump Controller*, which must be treated with the same methods as the Failure Manager. With a slight extension of our model for the Failure Manager, it would be possible to calculate the mean time between failure of the Steam Boiler given a simple control strategy.