Model Checking of the Process Control Program for a Hydrogen Pilot Plant

Burak Ökten, Halit Oğuztüzün

Address:

Middle East Technical University,
Department of Computer Engineering,
Çankaya, Ankara

E-Mail: burak.okten@ceng.metu.edu.tr
oguztuzn@ceng.metu.edu.tr

Abstract

Formal verification can play an important role to enhance safety in chemical industry. Verification should be applied before committing to any plant design decision, because fixing design faults later can be very costly. Determining the safety critical points of chemical process systems is a vital issue. In this work, a hydrogen pilot plant designed by Arizona Public Service in 2003 is examined. This plant produces hydrogen, stores it and dispenses it for hydrogen fuel vehicles. Hydrogen is produced from high-purity water using electrolysis and sent to low and high pressure storage tanks. All equipment are instrumented with proper sensors to track critical conditions, such as pressure levels, flow amounts, incipient fires, hydrogen leaks and equipment health. These sensors are wired to a control room to monitor the plant processes. Model checking is performed using Promela and iSpin to verify the safety features of the process control system. Modeling of the plant control software and the defects found during its verification will be discussed.