Title: Application of formal verification and falsification to large-scale chemical plant automation systems

Author: Blake C. Rawlings John M. Wassick B. Erik Ydstie

PII: S0098-1354(17)30405-2
DOI: https://doi.org/doi:10.1016/j.compchemeng.2017.11.004
Reference: CACE 5948

To appear in: *Computers and Chemical Engineering*

Received date: 31-5-2017
Revised date: 26-10-2017
Accepted date: 7-11-2017

Please cite this article as: Blake C. Rawlings, John M. Wassick, B. Erik Ydstie, Application of formal verification and falsification to large-scale chemical plant automation systems, *<![CDATA[Computers and Chemical Engineering]]>* (2017), https://doi.org/10.1016/j.compchemeng.2017.11.004

APPLICATION OF FORMAL VERIFICATION AND FALSIFICATION TO LARGE-SCALE CHEMICAL PLANT AUTOMATION SYSTEMS

Blake C. Rawlings*[1,2], John M. Wassick[3], and B. Erik Ydstie[1]

[1]Department of Chemical Engineering, Carnegie Mellon University, Pittsburgh, PA
[2]Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI
[3]The Dow Chemical Company, Midland, MI

Abstract

In this paper, we apply formal verification and falsification of temporal logic specifications to analyze chemical plant automation systems. We present new results, obtained by applying a recently-developed approach to handle combined invariance and reachability requirements. In addition, we develop a set of tests that can be generated automatically for a given control system, some of which have the same form as those in the existing literature, and some of which combine invariance and reachability, to which we apply the new approach mentioned previously. In both cases, we work with abstractions of the automation systems in order to apply symbolic model checking to industrial-scale problems. We demonstrate the results using a series of small illustrative examples, and also report results from an industrial case study. The methods that we apply are implemented in a pair of open-source software tools, which we describe briefly.

Keywords

Formal methods; Hybrid systems; Programmable logic controllers; Supervisory control; Model checking; Abstraction

1 Introduction

1.1 Background and Motivation

Automating a modern chemical plant involves repeatedly making a large number of discrete decisions to guide the evolution of the process along the desired trajectory. This task is performed by a logical control system that observes and manipulates the process and the continuous control system. The coupling between these three major components of a chemical plant results in a cyber-physical system, a type of hybrid (continuous and discrete) dynamical system, as described by Engell et al. (2000).

Due to the lack of systematic tools that can be used to design the discrete automation logic, the current industrial practice is to do so by hand, relying on a combination of engineer skill and intuition, semi-formal guidelines and best practices, rules of thumb, and simulation. Such an approach is both time consuming and error prone; this is a critical issue when it comes to the behavior of the plant, as described in the perspective by Leveson and Stephanopoulos (2013), which advocates the viewpoint that the various elements that make up the overall system are inextricably linked. The importance of developing tools to design hybrid process control systems is also highlighted in the perspective by Grossmann and Westerberg (2000). Analyzing existing systems is the first step toward systematically designing correct logic. The objectives of this work are to extend the class of specifications that can be tested, and to apply the methods to industrial-scale systems.

1.2 Analysis of Logical Control Systems

A significant body of research has focused on verifying the correctness of logical control systems. This includes modeling programmable logic controllers (PLCs) so that a formal specification of the desired behavior can be verified (Moon 1994; Rausch and Krogh 1998; Canet et al. 2000; Gourcuff et al. 2008; Biallas et al. 2010; Darvas et al. 2013). The basic approach consists of the following steps:

*To whom all correspondence should be addressed: bcraw@umich.edu. This work was completed in part while the first author was a Ph.D. candidate at CMU, and in part while he was in his current position as a postdoctoral research fellow at U-M.