

Верификация программ управления киберфизическими системами с временными штампами

Шатров В. В., Университет ИТМО, г. Санкт-Петербург
Научный руководитель – Чивилихин Д. С., к.т.н., научный сотрудник ФИТиП
Университета ИТМО

Введение

Применение распределенной архитектуры интернета вещей (IoT) в промышленных системах управления ставит вопросы об обеспечении надежности системы при выполнении программного обеспечения в различных IoT-конфигурациях, а также о свойстве системы поддерживать запрограммированное поведение физического процесса несмотря на возможные помехи из физического окружения. Данное свойство называется киберфизическим агностицизмом. Для обеспечения свойства киберфизического агностицизма используется расширение языка функциональных блоков (ФБ) описанного стандартом IEC 61499 программами с временными штампами. Для обеспечения требований надежности, предъявляемых к промышленным системам управления, используется формальная верификация на этапе проектирования системы. Формальная верификация программ на языке функциональных блоков, как правило, проводится путём перевода исходной программы в модель на входном языке программных средств, называемых моделчекерами. Для поддержки верификации систем функциональных блоков существует открытая инструментальная система FB2SMV. Однако данная система не поддерживает программы с временными штампами.

Цель работы

Целью данной работы является разработка метода формального моделирования программ на языке ФБ с временными штампами, демонстрация его в действии на примерах, а также реализация генератора моделей.

Базовые положения исследования

В ходе данной работы предполагается определить синтаксис и семантику языка функциональных блоков с временными штампами; реализовать на этом языке несколько моделей систем; предложить формальную модель этого языка на одном из языков общепринятых для моделчекинга; разработать автоматический генератор формальных моделей из программ с временными штампами.

Промежуточные результаты

Синтаксис и семантика языка функциональных блоков заданные стандартом IEC 61499 расширены для поддержки программ с временными штампами. На предложенном языке реализованы модели системы лифта, а также системы управления поршнем с пропорционально-интегрально-дифференцирующим (ПИД) регулятором.

Основной результат, практические результаты

Реализован автоматический генератор формальных моделей программ с временными штампами на языке верификатора NuXMV путем расширения инструментальной системы FB2SMV. С помощью разработанного комплекса программных средств продемонстрировано решение задачи устойчивости ПО на примере ПИД-регулятора.

Список литературы

1. V. Vyatkin, C. Pang, S. Tripakis, "Towards Cyber-Physical Agnosticism by Enhancing IEC 61499 with PTIDES Model of Computations", International Annual conference of IEEE Industrial Electronics Society, Yokohama, November, 2015

2. D. Drozdov, S. Patil, V. Vyatkin, “Towards Formal Verification for Cyber-physically Agnostic Software: a Case Study”, International Annual conference of IEEE Industrial Electronics Society IECON’17, Beijing, 2017

Автор _____ / _____ /

Научный руководитель _____ / _____ /

Руководитель образовательной программы _____ / _____ /