ВЕРИФИКАЦИЯ СВОЙСТВА КИБЕРФИЗИЧЕСКОГО АГНОСТИЦИЗМА В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Шатров В. В., магистрант Факультета Информационных Технологий и Программирования, Университет ИТМО, vvshatrov@yandex.ru

Аннотация

В работе рассматривается метод верификации свойства киберфизического агностицизма. Киберфизический агностицизм достигается посредством использования временных меток событий. Предлагается расширение стандарта IEC61499 для работы с временными метками. Для верификации системы применяется генерация моделей верификатора NuSMV.

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 метками.

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 модел-чекерами. Для поддержки верификации систем функциональных блоков существует открытая инструментальная система FB2SMV [1], которая позволяет генерировать модели базисных и составных функциональных блоков на языке верификатора NuSMV. Однако данная система не поддерживает программы с временными метками.

Симуляция временных меток

Для верификации киберфизического агностицизма с помощью системы FB2SMV в работе [2] использовалась симуляция временных меток.

В качестве недостатков данного подхода можно выделить следующие пункты:

1. Верифицируемая модель не соответствует реальной системе
2. Способ требует проведения большого количества изменений в исходной системе.
3. Нельзя использовать все возможности временных меток. Например, не представляется возможным упорядочить события на основе временных данных.
4. Способ использует сервисные блоки, которые зависят от конкретного аппаратного обеспечения, а также не поддерживаются генератором моделей.
5. Время верификации значительно увеличивается из-за добавления большого количества блоков для симуляции меток.

Синтаксис программ с временными метками

Для использования временных меток необходимо изменение синтаксиса языка функциональных блоков. События рассматриваются как составные структуры данных:

```
E = (TB, TL, V)
V - событийная переменная
TB - время зарождения события
TL - время последнего изменения события
```

Для обращения к временным меткам из программы управления модифицирован синтаксис языка Structured Text, определенный в стандарте IEC 61131-3.

Изменены продукционные правила:

```
primary_expression ::=
    constant | enumerated_value | variable
    | '(' expression ')'
    | function_name  '(' param_assignment
             { ',' param_assignment} ')'
    | structured_event | time_reference
time_reference ::= 'Systemclock'
```

```
structured_event ::= event_reference
                              [“.” time_attribute]
event_reference ::= ‘INVOKEDBY’ | identifier
time_attribute ::= “ts_last” | “ts_born”
```

Метод верификации

Описание метода

1. Составление модели системы в ФБ в замкнутом цикле
2. Добавление корректировок программы управления, используя новый синтаксис
3. Генерация SMV моделей
   3.1. Добавление очередей с вероятностными задержками для выбранных событий
4. Запись спецификации с помощью LTL-формул
5. Верификация модели в NuSMV
6. Анализ контрпримера с помощью визуализатора

Составление модели системы в ФБ в замкнутом цикле

Формальная верификация модели контроллера с проверкой всех возможных комбинаций входных переменных может быть затруднительной из-за проблемы большого пространства состояний для таких моделей. Чтобы сократить пространство состояний, используют технику моделирования в замкнутом цикле [3]. Модель контроллера верифицируют в связке с моделью управляемого устройства. Таким образом переменные будут приобретать только те значения, которые могут встретиться при реальном исполнении системы.

Добавление корректировок программы управления

Чтобы обеспечить киберфизический агностицизм, управляющей программе необходимо учитывать возраст событий. На основании этих данных программа может либо проигнорировать событие как не актуальное, либо произвести корректировку управления. Например, если событие о том, что лифт приехал на этаж, доставлено с определенной задержкой, контроллер лифта может включить мотор в обратном направлении, чтобы скорректировать позицию кабины.

Генерация SMV моделей

Для генерации моделей программ с временными метками модифицировано инструментальное средство FB2SMV. Для верификации устойчивости программы к временным задержкам необходимо произвести эмуляцию временных задержек в модели верификации. С этой целью при генерации моделей к выбранным событийным входам добавляются очереди событий с недетерминированным выбором времени задержки события в очереди.

К сгенерированным моделям добавляется спецификация модели, выраженная в виде LTL-формул. Полученная модель передается в качестве входных данных верификатору NuSMV.

Анализ контрпримера

Верификатор NuSMV не обладает какой-либо информацией об исходной системе функциональных блоков, поэтому контрпример, выдаваемый в результате верификации, выражен в терминах SMV модели. В процессе генерации SMV модели названия объектов исходной системы изменяются. Анализ контрпримера является затруднительным и требует вспомогательных средств. В связи с этим предлагается использование визуализатора контрпримера в исходной системе функциональных блоков.

Заключение

В работе представлен метод верификации свойства киберфизического агностицизма. Определен синтаксис программ с временными метками. Для применения метода было модифицировано инструментальное средство FB2SMV.

Литература

1. Дроздов Д. Н., Дубинин В. Н., Вяткин В. В. СИСТЕМА ПОДДЕРЖКИ ВЕРИФИКАЦИИ СИСТЕМ ФУНКЦИОНАЛЬНЫХ БЛОКОВ IEC 61499 НА ОСНОВЕ МЕТОДА MODEL CHECKING //Федеральная служба по интеллектуальной собственности.–Свидетельство о гос. регистрации программы для ЭВМ. – 2015. – №. 2015616383.
2. Drozdov D. et al. Towards formal verification for cyber-physically agnostic software: A case study //IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society. – IEEE, 2017. – С. 5509-5514.
3. V. Vyatkin, H.-M. Hanisch, C. Pang, and C.-H. Yang, “Closed-loop modeling in future automation system engineering and validation,” IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 39, no. 1, pp. 17–28, 2009.

4. Vyatkin V., Pang C., Tripakis S. Towards cyber-physical agnosticism by enhancing IEC 61499 with PTIDES model of computations //IECON 2015-41st Annual Conference of the IEEE Industrial Electronics Society. – IEEE, 2015. – С. 001970-001975.