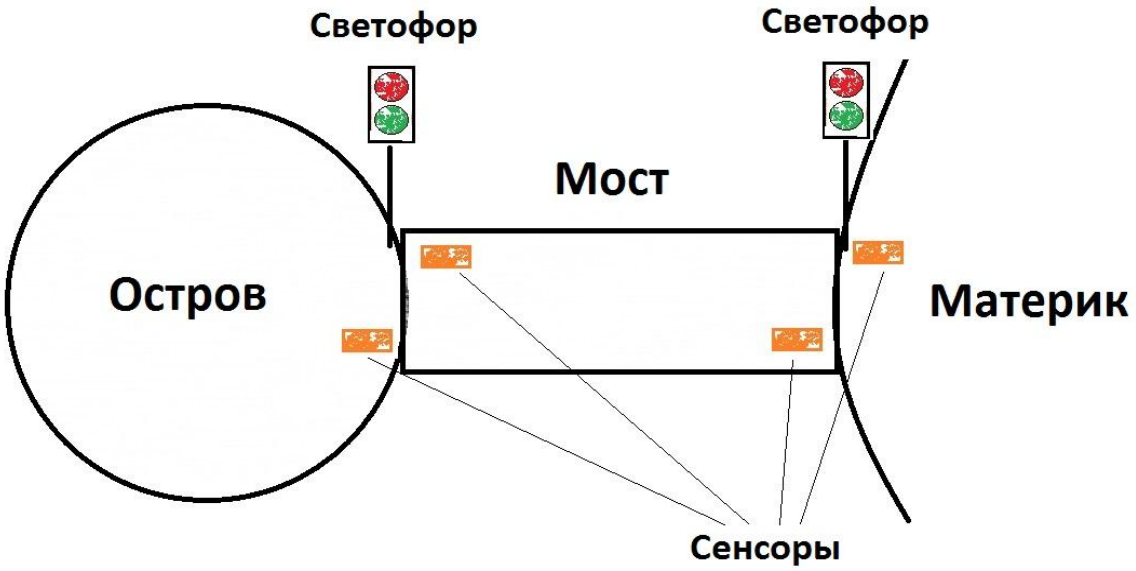
Разработка и верификация систем управления методом автоматного программирования на базе системы моделирования Event-B

Автоматное программирование ориентировано на разработку и верификацию программ из класса систем управления, в том числе распределенных с асинхронным взаимодействием. Язык автоматного программирования может быть легко построен расширением любого базисного императивного или функционального языка. На базисе языка спецификаций Event-B построен новый язык автоматного программирования. Тем самым средства моделирования и верификации Event-B усилены более общими и гибкими возможностями автоматного программирования.

Методы автоматного программирования, доказавшие свою эффективность, разрабатываются только в России (Санкт-Петербург, Новосибирск) с начала 1990-х. Интеграция автоматного программирования с Event-B приобретает особую важность для разработки программ критической инфраструктуры с повышенными требованиями к надежности и информационной безопасности. В соответствии с Российскими стандартами [3] для сертификации таких программ необходимо разрабатывать программу на базе модели (model-based & model-driven engineering) и проводить формальную верификацию модели в таких системах, как Event-B. Для разработки и формальной верификации автоматных программ не требуется других инструментов, кроме хорошо известной и доступной платформы Rodin, реализующей Event-B.

Применение технологии автоматного программирования для задачи управления автомобилями на мосту [1] дает более адекватное и простое решение, чем в руководстве по Event-B, где эта задача приведена в качестве начального показательного примера. В этой задаче требуется реализовать управление светофорами на мосту с односторонним движением, используя показания сенсоров, фиксирующих прохождение автомобилей.



Программисты, даже наиболее опытные, не способны построить адекватную модель для систем управления критической инфраструктуры и верифицировать модель. Здесь нужны специалисты – инженеры-верификаторы, каких мало в России. Начальный этап овладения специальностью инженера-верификатора (специалиста по формальным методам) реализуется в рамках магистерского курса "Формальные методы в программной инженерии" [2], который читается в Новосибирском государственном университете (НГУ) на механико-математическом факультете уже семь лет. Опыт преподавания курса "Формальные методы" в разных университетах Новосибирска показал, что данный курс по силам лишь студентам университетов первой десятки Российского рейтинга.

В качестве примера задач, которые даются магистрантам в качестве индивидуальных заданий, здесь приведена задача 14, где требуется построить модель взаимодействия дронов, решающая поставленную задачу и гарантирующая невозможность столкновения дронов.

Публикации, учебные материалы, стандарты:

1. Шелехов В.И. Автоматное программирование на базе системы моделирования и верификации Event-B / Программная инженерия, Том 13, №4, 2022 — С. 155-167. https://persons.iis.nsk.su/files/persons/pages/atomeventb.pdf
2. Формальные методы в программной инженерии. Видеолекции и презентации. — ИСИ СО РАН, Новосибирский государственный университет. Новосибирск, 2021. http://wasp.iis.nsk.su
   Часть 4. Автоматное программирование. Система Event-B. http://wasp.iis.nsk.su/page3.html
3. Российские стандарты ГОСТ Р 59453.1-2021, ГОСТ Р 59453.2-2021 «Защита информации. Формальная модель управления доступом и рекомендации по ее верификации».

Задача 14

Стая дронов ищет пропавшую в лесу девочку. Обследуется односвязный участок леса. Территория леса снабжена квадратной сеткой, разделяющей местность на квадраты небольшого одинакового размера. Территорию леса определим в виде набора горизонтальных рядов квадратов: для каждого горизонтального ряда, имеющего свой номер внутри некоторого отрезка вертикальной оси координат, задаются номера начального и конечного квадрата в ряду.

Внутри каждого квадрата допускается не более одного дрона. Дрон может двигаться по вертикали или горизонтали на соседние квадраты.

В начальный момент все дроны находятся на горизонтальной оси ниже обследуемого участка леса. Дроны размещаются по горизонтальным рядам не более одного дрона на ряд. Находясь внутри ряда, дрон последовательно обследует каждый квадрат, проводя съемку местности квадрата. При обнаружении объекта, похожего на девочку, дрон посылает в штаб МЧС координаты квадрата и результаты съемки. Каждый дрон, когда он оказывается вне обследуемого участка леса, движется к одному из концов свободного необследованного горизонтального ряда.

Дроны завершают работу после обследования всей территории участка леса, либо по сигналу от МЧС.

Построить модель процесса поиска девочки в лесу в виде автоматной программы с реализацией в Event-B. Необходимо избежать столкновения дронов и обеспечить полноту обследования территории леса.