ИСП РАН
Институт системного программирования имени В.П.Иванникова Российской академии наук

Виртуальный стенд демонстрации результатов проекта

«Исследование и разработка технологий производства и сертификации программного обеспечения с повышенными требованиями к надежности и безопасности на основе формальных методов моделирования и верификации»

Проект поддержан грантом Минобрнауки РФ **RFMEFI60719X0295**

SYRCoSE-2020, 28-29 мая 2020 года

Цель проекта

Создание новых технологий производства и сертификации программного обеспечения, обеспечивающих высокую надежность и информационную безопасность вычислительных систем ответственного назначения, включая операционные системы, встроенные системы управления, системы обработки данных и роботизированные системы, используемые в критических областях (космосе и авиации, атомной энергетике, медицине).

Практические задачи проекта

- Разработка инструментов построения и верификации моделей программных систем
- Разработка инструментов верификации программных систем ответственного назначения.

Инструменты построения и верификации моделей программных систем

Ключевые особенности:

- Нацеленность на создание и верификацию многоуровневых моделей, которые по необходимости используются в крупных программных комплексах.

Формальные языки и нотации

- B, Event-B

Базовые инструменты верификации

- Rodin, ProB

Инструменты построения и верификации моделей программных систем

Примеры индустриального применения:

- Разработка и верификация формальной модели политики управления доступом в операционных системах, СУБД, маршрутизаторах и других критических компонентах программного стека
- Функциональная спецификация интерфейса (АПИ) системных вызовов операционных систем
- Доказательство согласованности функциональной спецификации заданной политике управления доступом.

Инструменты верификации программных систем ответственного назначения

Ключевые особенности

- Адаптация инструментов верификации к особенностям промышленного программного кода в системном ПО, в частности, в ядрах операционных систем

Языки и нотации

- Язык реализации Си
- Язык спецификации ACSL

Базовые инструменты

- Isabelle/HOL, Frama-C

Инструменты верификации программных систем ответственного назначения

Примеры индустриального применения:

- Модули ядра операционной системы Astra Linux
- Операционная система реального времени JetOS
- Базовые библиотеки для технологии smart-contract

Индустриальные партнеры

- АО «НПО РусБИТех»

- ФГУП «ГосНИИАС»

Сайт проекта

Проект «Исследование и разработка технологий производства и сертификации программного обеспечения с повышенными требованиями к надежности и безопасности на основе формальных методов моделирования и верификации», проводимого ИСП РАН в партнерстве с АО «НПО РусБИТех» и ФГУП «ГосНИИАС» при поддержке Министерства науки и высшего образования РФ (уникальный идентификатор проекта: RFMEFI60719X0295).

Приглашаем к сотрудничеству организации, заинтересованные в перспективных средствах моделирования, верификации и тестирования ПО.

http://astraver.linuxtesting.ru/