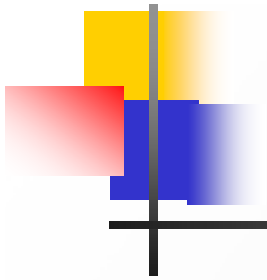


АНАЛИЗ ИНФОРМАЦИОННЫХ ПОТОКОВ ДЛЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СИСТЕМ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ

Чечулин А.А.

Лаборатория проблем компьютерной безопасности Санкт-Петербургского Института Информатики и Автоматизации РАН

Санкт-Петербург, Россия

Фидж К.

Технологический Университет Квинсленда

Брисбен, Австралия

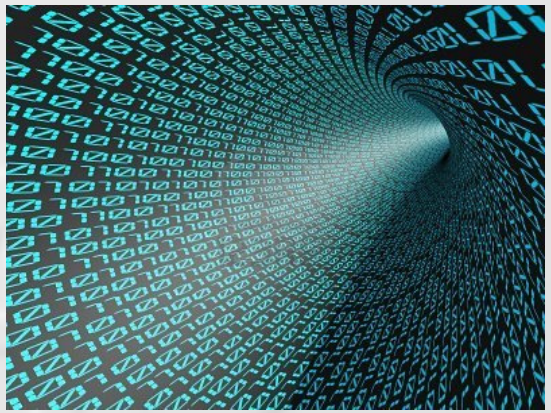
РусКрипто'2012, 28-31 марта 2012 г.

Применение встроенных устройств

- Автомобили
  - Контроль двигателя, АКП, АБС …
- Авиация
  - Управление полетом, системы диспетчерского контроля …
- Связь
  - Коммутация, мобильные телефоны, маршрутизаторы, IP телефония, КПК …
- Бытовая техника
  - Телевизоры, холодильники, СВЧ печи …
- Коммерческая техника
  - Автоматизированный контроль, кассовые аппараты, системы управления запасами…

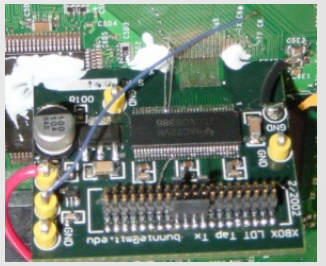
Информационные потоки

- **Информационный поток** – это совокупность передаваемой информации между двумя и более взаимодействующими объектами
- **Безопасность информационных потоков** – это набор требований и правил, направленных на определение того, какие информационные потоки в системе являются разрешёнными, а какие нет
- **Модель безопасности** должна описывать все возможные информационные потоки, определять критерий безопасности системы и формулировать правила управления информационными потоками

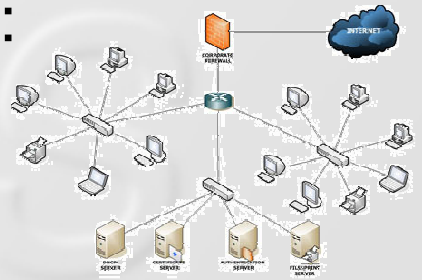


Типы сетевых потоков

- **Три типа информационных потоков:**
  1. Программные потоки
     - (h:=…; l:=false; if h then l:=true else skip; out(l))
  2. Аппаратные потоки
     - Незащищенные интерфейсы, инженерные интерфейсы, ошибки проектирования…
  3. Сетевые потоки
     - Транспортный, сетевой и прикладной уровни соединений



- **Объектом** анализа потоков может быть:
  - Отдельное встроенное устройство
  - Система содержащая встроенные устройства

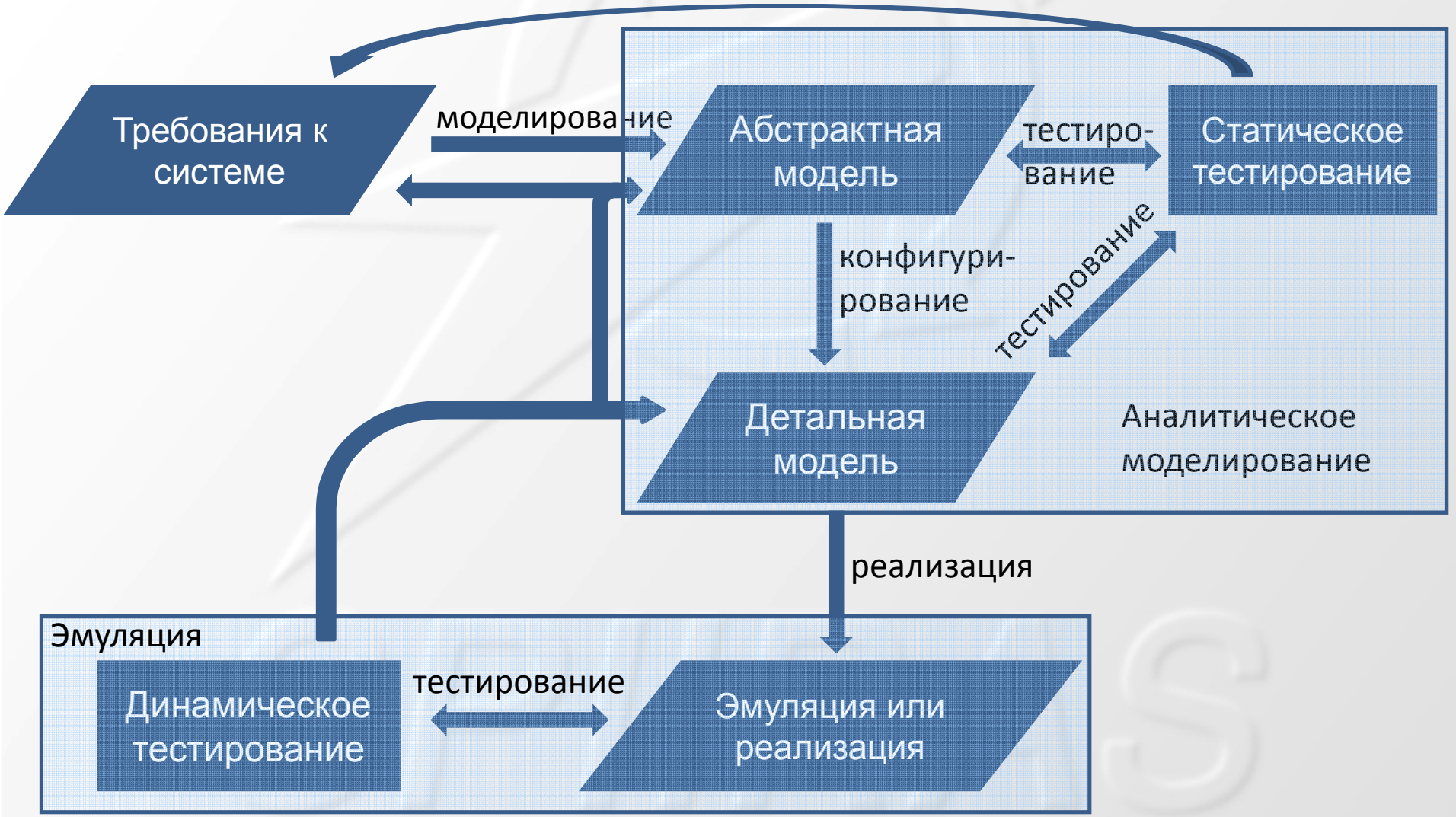


Подходы к анализу потоков

- **Основные подходы** к анализу информационных потоков:
  - **Статический** – анализ модели системы
  - **Динамический** – отслеживание реальных потоков информации внутри системы в рабочем режиме

- **Источники данных** для анализа информационных потоков:
  - Архитектура микросхем
  - Исходный код программ
  - Сетевые политики
  - Реальные сетевые соединения

Процесс построения системы



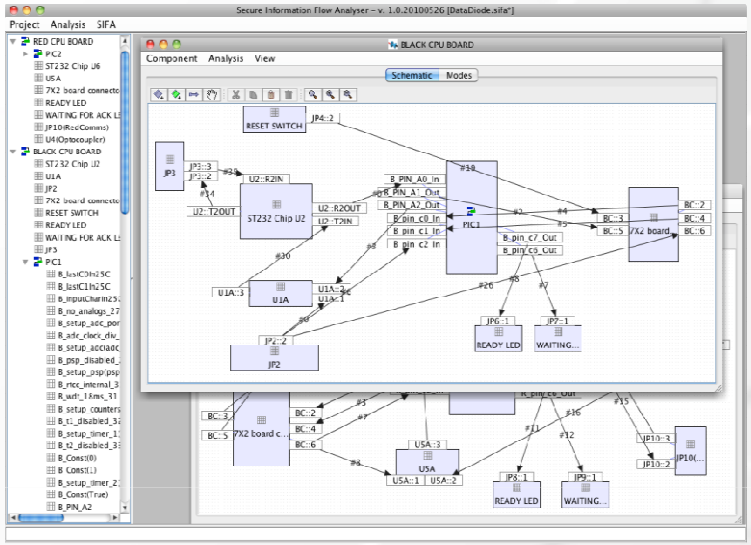
Разграничение зон

Внешняя зона (незащищенная)

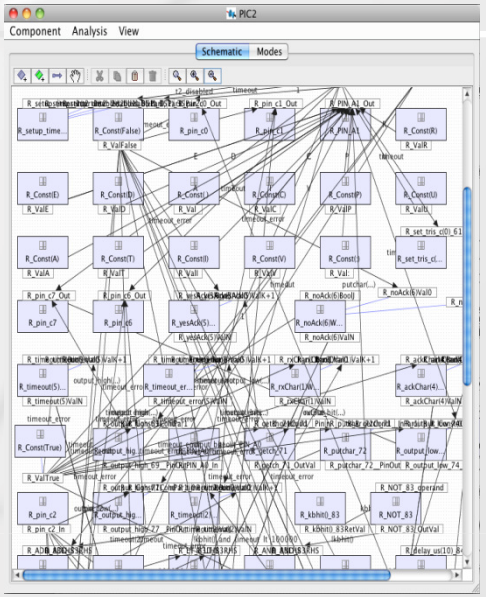
Система разграничения потоков (не самый лучший пример!)

Внутренняя зона (защищенная)

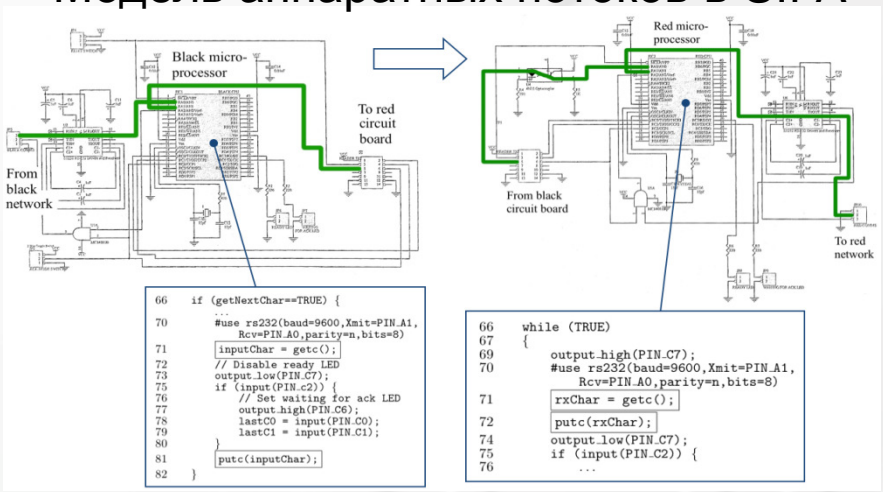
Анализ потоков (1/4)
Hardware и Software потоки



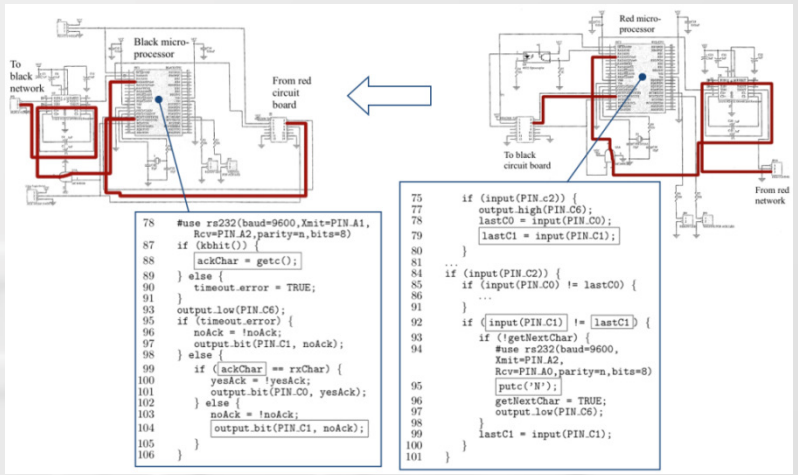
Модель аппаратных потоков в SIFA



Модель программных потоков в SIFA



Входной поток в микросхеме



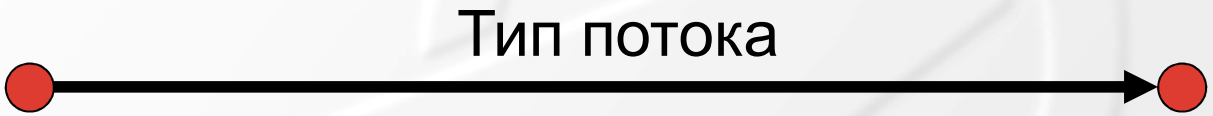
Выходной поток в микросхеме

Анализ потоков (2/4)
Hardware и Software потоки

1. Идентификация всех компонентов, которые лежат между двумя выбранными точками на графе.
2. Нахождение минимального множества компонентов между критически важным источником и незащищенным получателем, устранение которых превратит граф в набор несвязных подграфов
3. Расчет "надежности" пути между двумя точками графа на основе некоторых числовых значений, присвоенным узлам
4. Обнаружение всех возможных путей информационных потоков между двумя выбранными узлами на графике

Анализ потоков (3/4)
Сетевые потоки

FSL: Flow Security Language – язык описания потоков

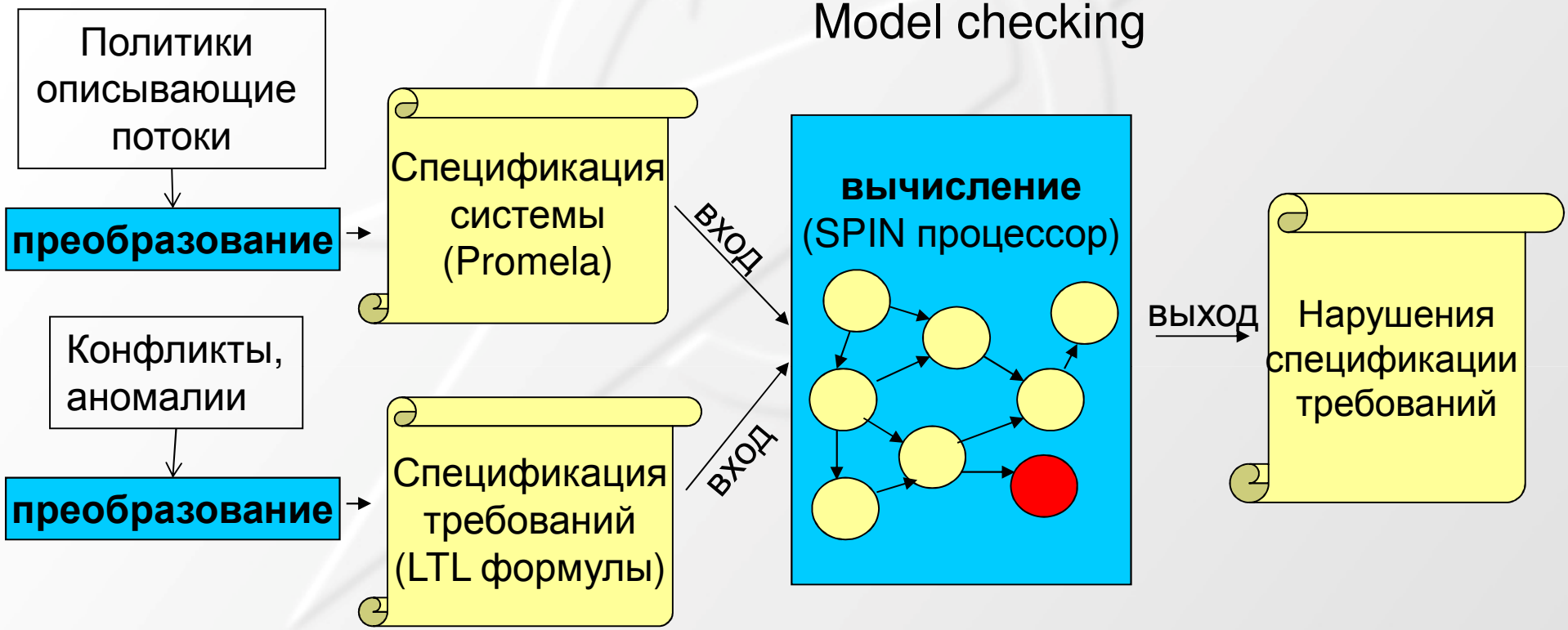


Источник:
- Пользователь
- Хост
- Интерфейс

Получатель:
- Пользователь
- Хост
- Интерфейс

- allow
  - allow(Us,Ns,Is,Ud,Nd,Id, T) <= (Us = TSN administrator) & (Ns = Administrator server) & (Nt = TSMC) & (T=Management)
  - allow(Us,Ns,Is,Ud,Nd,Id, T) <= (Ns = TSMC) & (Nt = Operator server) & (T=Measurements)
- deny
  - deny(Us,Ns,Is,Ut,Nt,It, T) <= (Ns <> Administrator server) & (Nt = TSMC) & (T=Management)
  - deny(Us,Ns,Is,Ud,Nd,Id, T) <= (Ns = TSMC) & (Nt <> Operator server) & (T=Measurements)

Анализ потоков (4/4)
Сетевые потоки



Promela – язык верификации моделей
LTL (Linear Temporal Logic) – темпоральная логика линейного времени

Заключение

- Проанализированы основные виды информационных потоков
- Предложен комплексный подход для анализа информационных потоков, позволяющий проводить автоматизированную проверку систем содержащих встроенные устройства
- Проведена серия экспериментов
- Проведен начальный анализ реальных систем предложенных в проекте SecFutur

Дальнейшие исследования

- Проведение экспериментов на реальных моделях и устройствах
- Разработка программно-аппаратного прототипа реализующего предложенные подходы к анализу информационных потоков
- Интеграция предложенных подходов в общую систему тестирования систем, содержащих встроенные устройства
- Расширение списка поддерживаемых языков программирования для анализа исходных текстов программ

Контактная информация

Фидж Колин
c.fidge@qut.edu.au
http://staff.qut.edu.au/staff/fidgec

Чечулин Андрей Алексеевич
chechulin@comsec.spb.ru
http://comsec.spb.ru/chechulin

Благодарности

Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект № 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.