ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ

Ruiz Rodríguez José Francisco, **Десницкий В.А.**, Котенко И.В., Antonio Maña, Чечулин А.А.

Departamento de Lenguajes y Ciencias de la Computación
University of Malaga, Malaga, Spain,

Лаборатория проблем компьютерной безопасности, СПИИРАН, Санкт-Петербург, Россия

РусКрипто'2012, 30 марта 2012 г.

Введение

- Проблема проектирования защиты систем со встроенными устройствами
  1. Отсутствие комплексного, комбинированного подхода к проектированию защиты
     - Ограниченность набора выдвигаемых требований к защите
       - идентификация пользователей, безопасное хранение данных внутри устройства, стойкость установленного ПО к модификациям, безопасный доступ к сети, безопасные сетевых соединений, и т.п.
     - Необходимость принятия решений поддержки безопасности на каждой стадии процесса проектирования
  2. Ограничения на доступные ресурсы устройств
     - Сложность применения традиционных средств защиты
     - Необходимость комбинирования компонентов защиты с учетом их нефункциональных, ресурсных требований и ограничений устройств

Актуальность

- **Возрастающее количество устройств, концепции «Интернет вещей», «Цифровой дом»**
- **Новые функциональные требования – потребность в дополнительной защиты устройств и сервисов**
- **Требования «рынка»: компромисс между защищенностью и производительностью устройств**

Задачи

- Разработка обобщенного процесса проектирования защищенных систем со встроенными устройствами
  - Разработка и уточнение действий процесса проектирования в рамках «компонентного подхода» к проектированию
  - Помощь разработчикам в принятии решений поддержки безопасности на различных стадиях проектирования, интеграции, реализации и развертывания системы
  - Специфика проектирование встроенных устройств:
    - Существенные ограничения на ресурсы устройств => слабая производительность
    - Устройства узкоспециализированного назначения => специфичные угрозы
    - Мобильность устройств, отличающиеся окружения => специфичные множества атак

Решаемые задачи

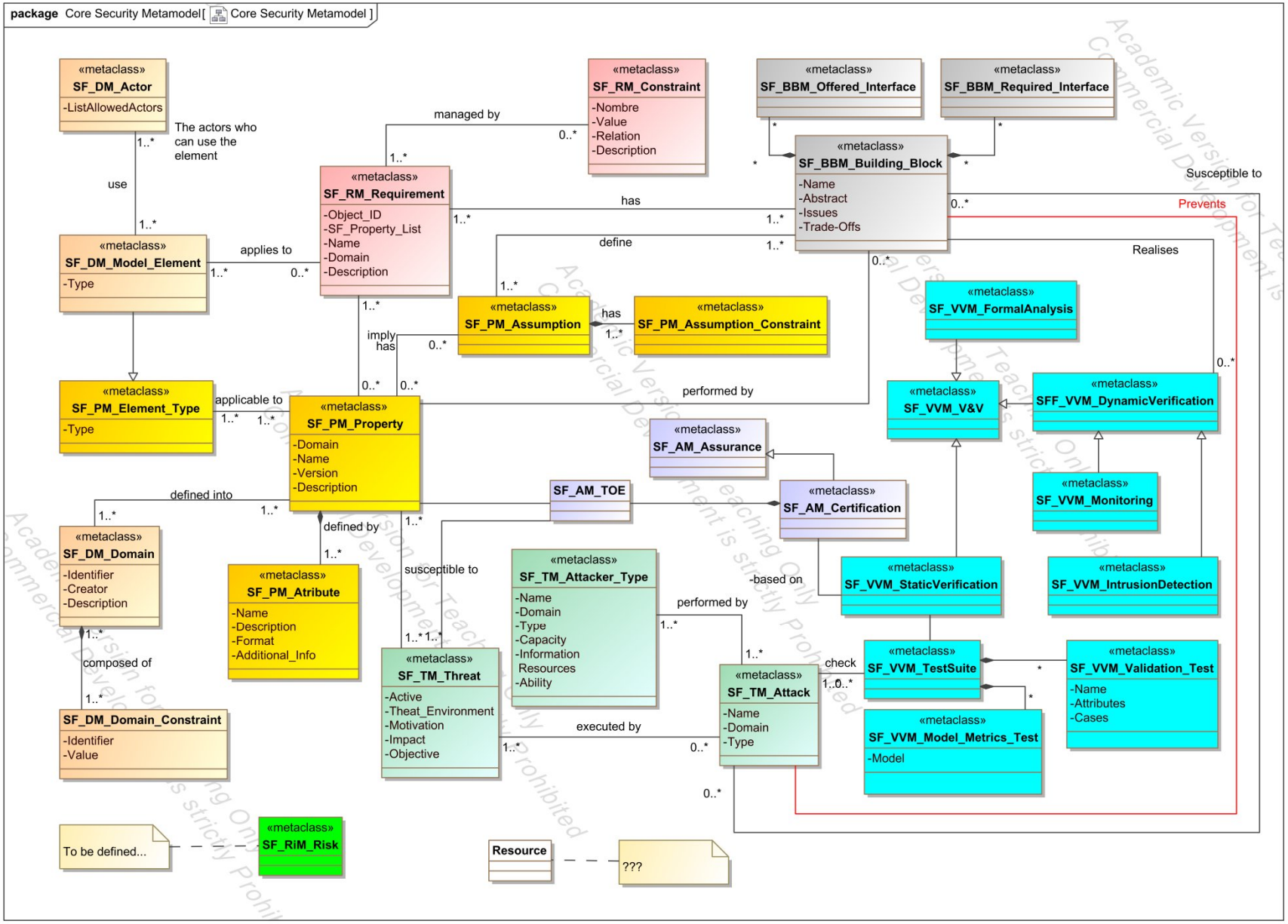
- Примеры применения (use cases)
- Формальная декомпозиция требований на основе SeMF
- Конфигурационная модель
- Статическое и динамическое тестирование
- Программное моделирование защиты (“симуляция”)
- Анализ информационных потоков
- Анализ несовместимостей компонентов защиты

Процесс проектирования

Модель CSM

- CSM (Common Security Meta-model) - Общая метамодель безопасности
  - Представляется на основе диаграмм классов UML
  - Предназначена для описания элементов процесса проектирования систем со встроенными устройствами
  - В т.ч. охватывает моделирование:
    - свойств безопасности и инженерные свойства
    - требований
    - угроз
    - компонентов защиты
    - алгоритмов композиции
    - алгоритмов верификации и тестирования защиты

Фрагмент CSM-модели

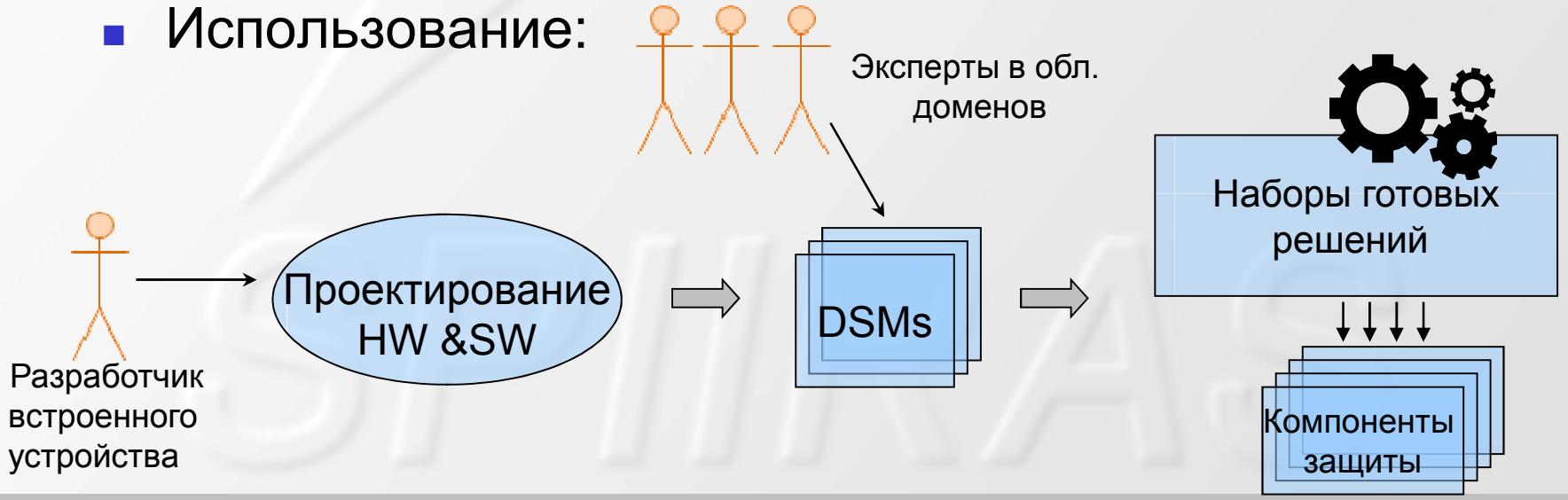


Модель DSM

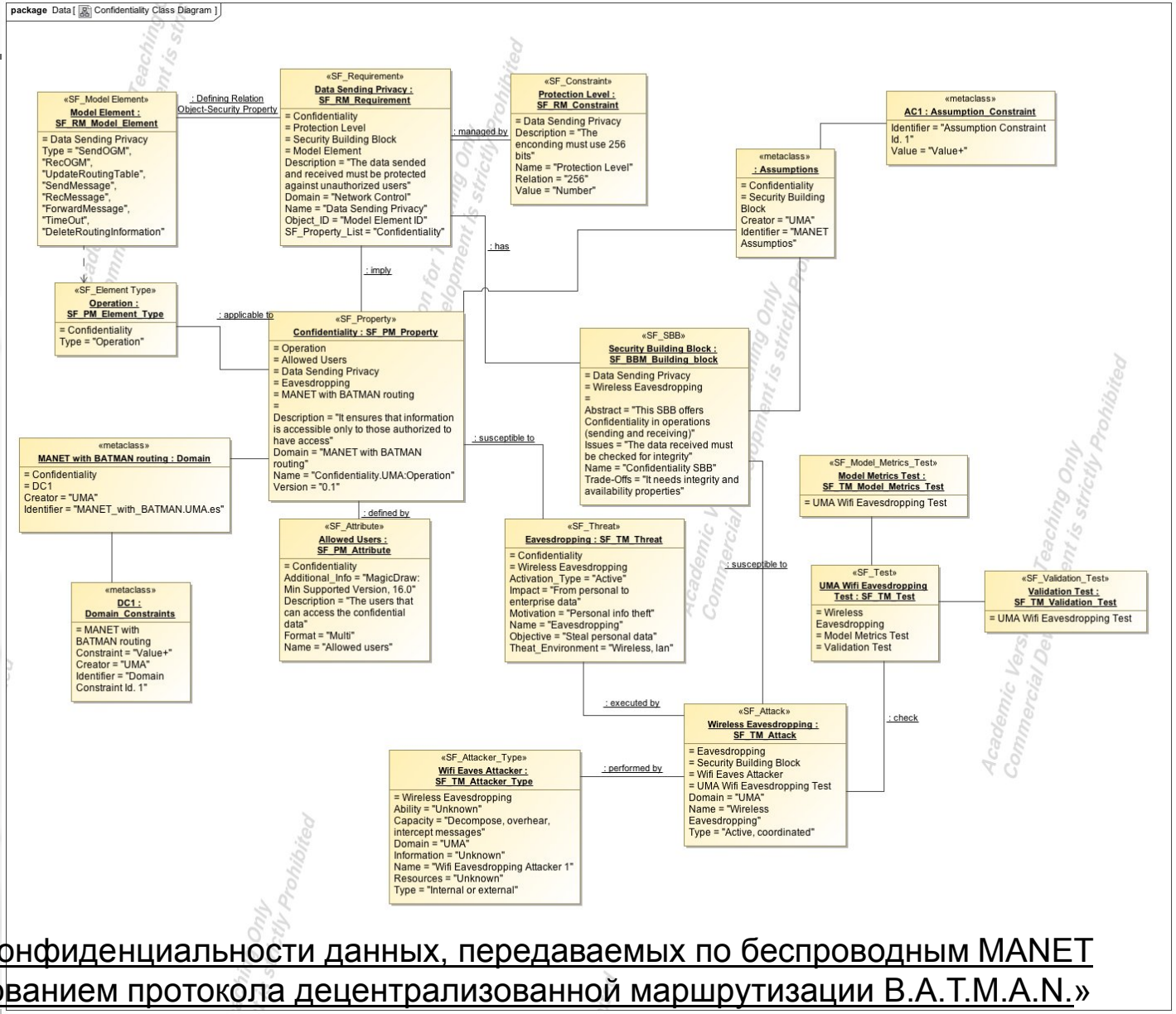
- DSM-модель (Domain Specific Model) – Доменно-специфичная модель
  - Формируется экспертом в сфере некоторого проблемно-предметного домена в области безопасности
  - Модель реализует метамодель CSM для определенного домена

CSM	«уровень классов» UML
DSM	«уровень экземпляров классов» UML

- Использование:



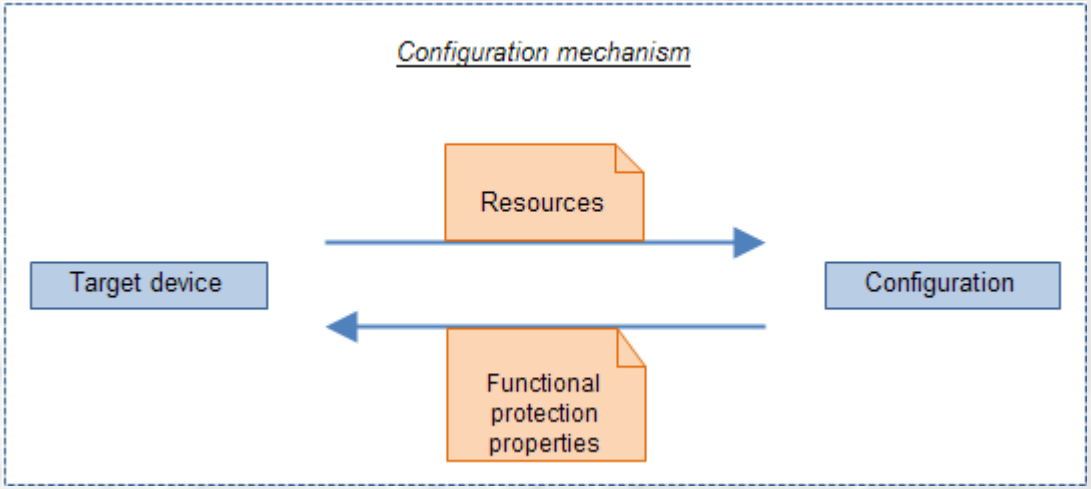
Пример DSM-модели



Домен: «Проблема конфиденциальности данных, передаваемых по беспроводным MANET сетям с использованием протокола децентрализованной маршрутизации B.A.T.M.A.N.»

Конфигурационная модель

- Конфигурирование устройства – процесс выбора необходимых компонентов защиты
- Конфигурирование встроенных устройства системы на основе решения оптимизационной задачи
- Конфигурация – набор программных и программно-аппаратных компонентов защиты встроенных устройств



Конфигурационная модель – свойства

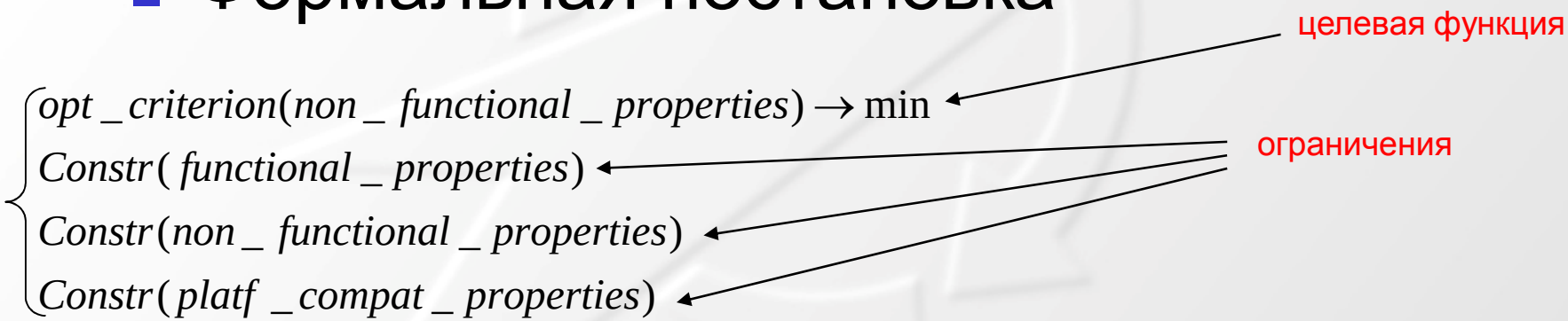
- Бинарные функциональные свойства защиты, предоставляемые компонентом защиты
  - *E.g.: целостность данных, хранимых временно на устройстве, наличие функции удаленной аттестации и пр.*
- Численные нефункциональные свойства, определяющие потребность компонента защиты в ресурсах устройства (*worst-case consumption values*)
  - *E.g. объем памяти, расходуемой компонентом; требуемая величина пропускной способности сетевого интерфейса устройства и пр.*
- Бинарные свойства программно-аппаратной совместимости
  - *E.g. тип и версия операционной системы/виртуальной машины; наличие коммуникационных интерфейсов и пр.*

Конфигурационная модель

- Цель: сформировать конфигурацию, которая
  - предоставляет все требуемые функциональные свойства защиты
  - удовлетворяет нефункциональным ограничениям устройства
  - удовлетворяет программно-аппаратным ограничениям совместимости устройства
  - является оптимальной
    - Критерии оптимальности базируются на значениях нефункциональных свойств компонентов защиты и ограничений устройства

Оптимизационная задача

- Формальная постановка



- Решение оптимизационной задачи
  - Методы на основе полного перебора возможных комбинаций компонентов защиты
  - Динамическое программирование

Критерии оптимальности

- Однокритериальная оптимизация
  - Минимизация показателя на основе нефункционального свойства
    - e.g.: $consumed\_memory(configuration) \rightarrow \min$
- Многокритериальная оптимизация
  - Минимизация серии нефункциональных нефункциональных показателей (*«цепочка свойств»*)
  - Интегральные критерии

Интегральный критерий

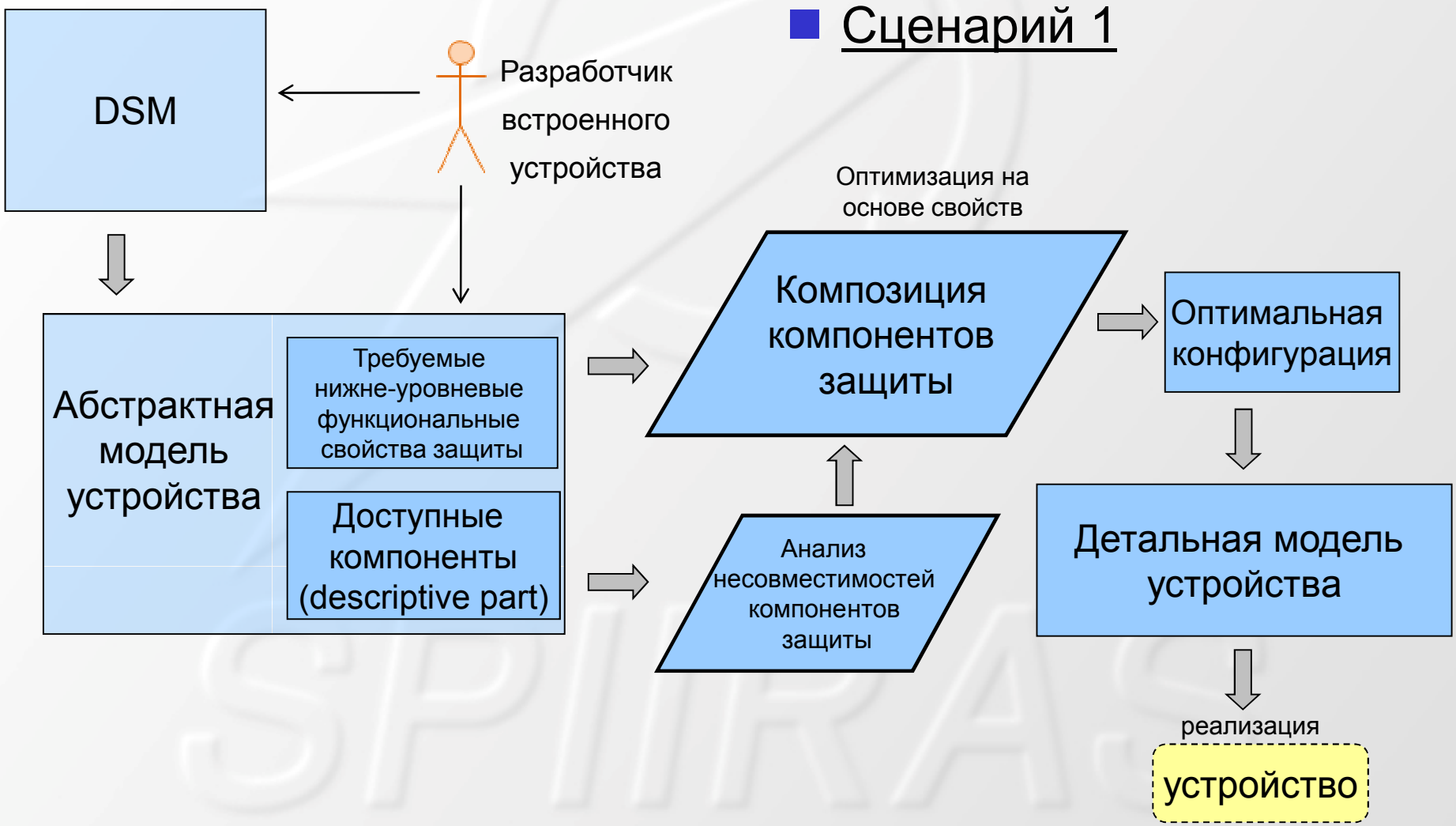
- Критерий: минимальность (на множестве конфигураций) максимального значения нефункциональных свойств конфигурации *(в %)*

Значение критерия: $\min_i\{\max_{p \in NonFunc\,\mathrm{Pr}\,operties}\{percent(p(configuration_i))\}\}$,

где $percent(p) = \frac{constr(p) - p}{constr(p)}$,

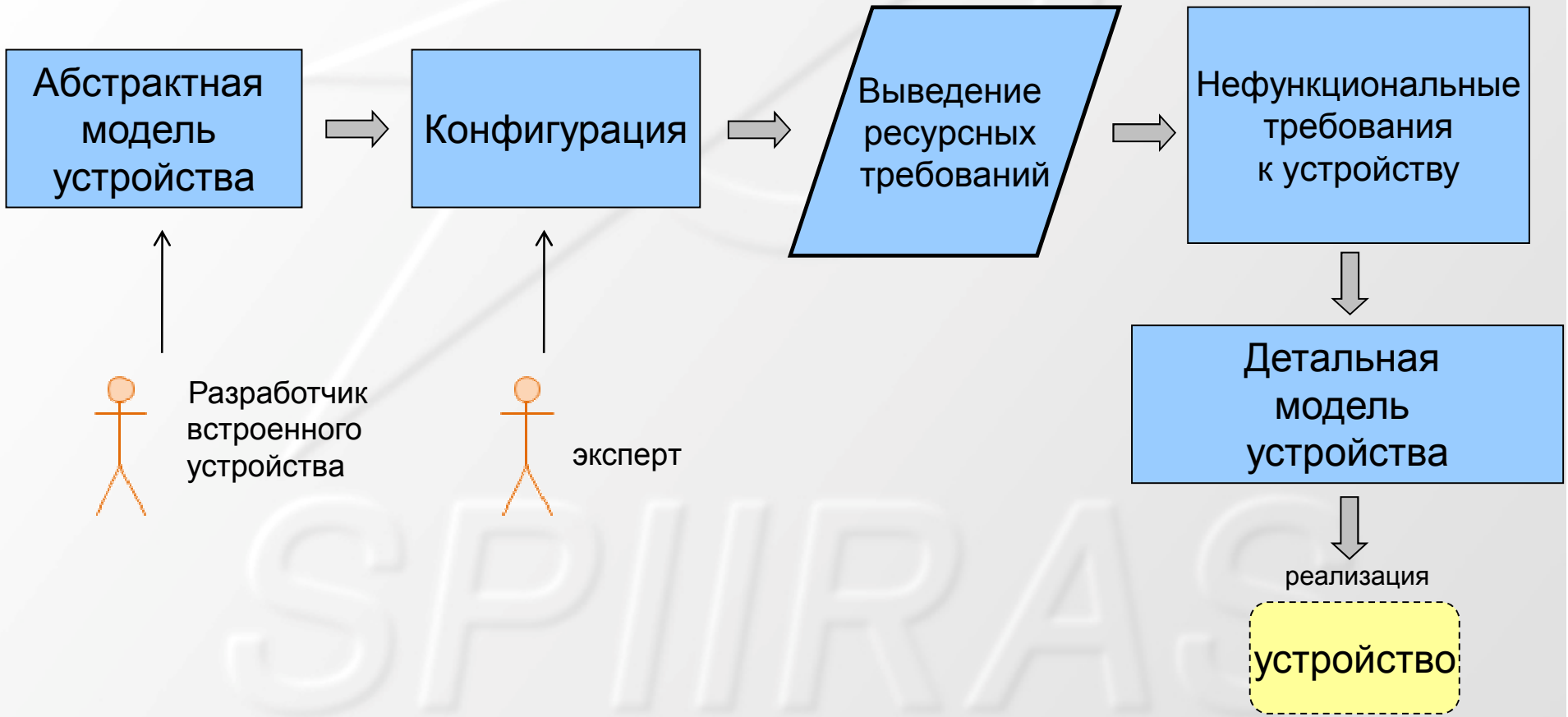
$constr(p)$ *- Значение ограничения устройства на свойство p.*

Сценарии конфигурирования (1/3)



Сценарии конфигурирования (3/3)

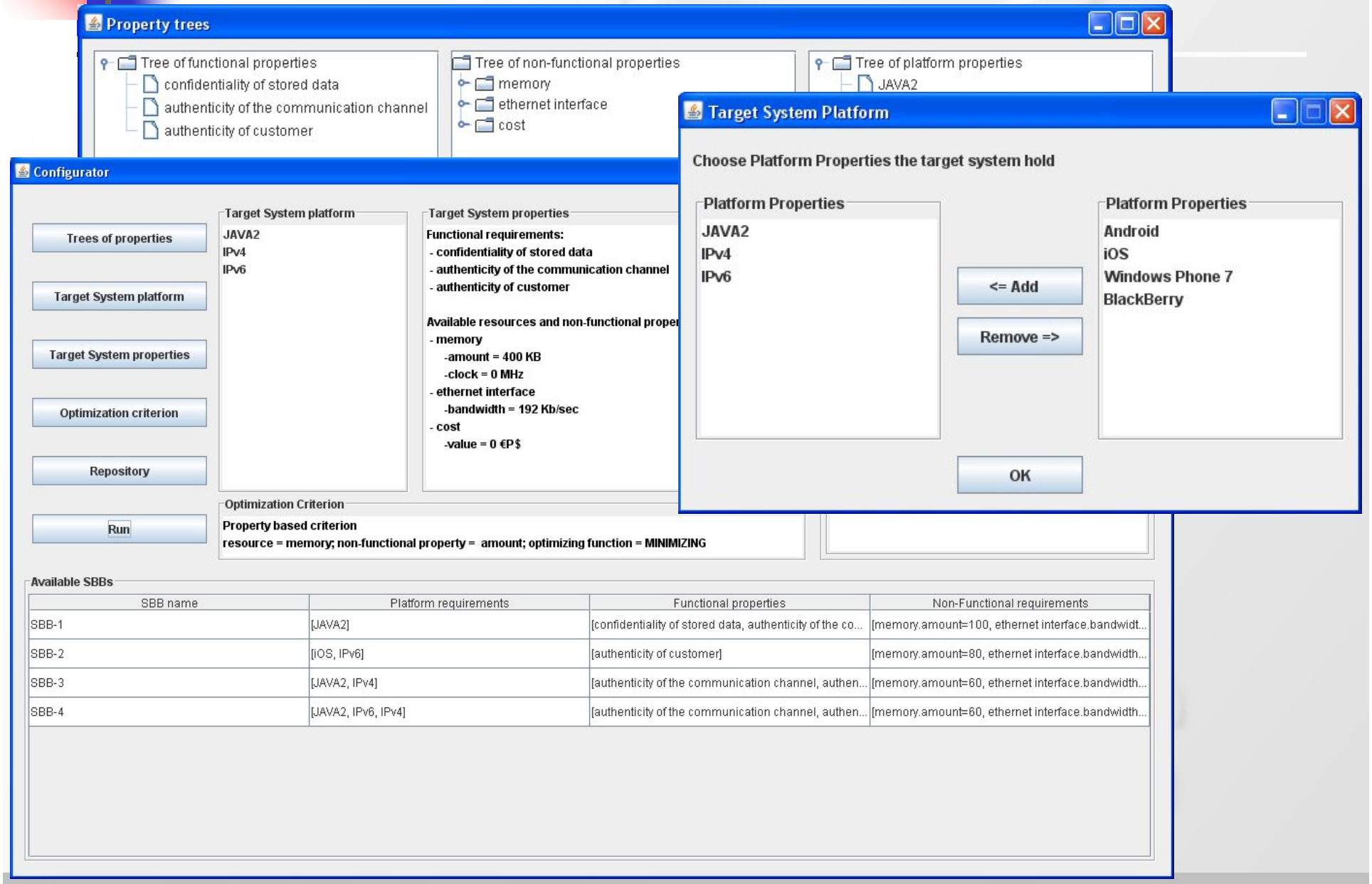
- Сценарий 2



Программный прототип

- Программный инструмент «Конфигуратор»
  - Инструмент автоматизации принятия решений на стадии проектирования встроенных устройств
  - Предназначен для разработчиков встроенных систем и экспертов в области компонентов защиты
  - Позволяет получить наиболее эффективную конфигурацию для развертывания на заданном устройстве
  - Позволяет вывести минимально необходимые ресурсные требования к устройству при заданной конфигурации

Графический интерфейс пользователя (GUI)



Заключение

- Процесс проектирования защищенных систем со встроенными устройствами
- Конфигурационная модель для встроенных устройств
- Архитектура механизма конфигурирования и программный прототип

Контактная информация

Десницкий Василий Алексеевич (СПИИРАН)
desnitsky@comsec.spb.ru
http://comsec.spb.ru/Desnitsky

Благодарности

Работа выполняется при финансовой поддержке РФФИ (проекты 10-01-00826-а и 11-07-00435-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2) и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

ВОПРОСЫ?