РусКрипто'2020

XXII международная научно-практическая конференция, посвященная актуальным вопросам криптографии и информационной безопасности

Комплексный подход к моделированию железнодорожных объектов

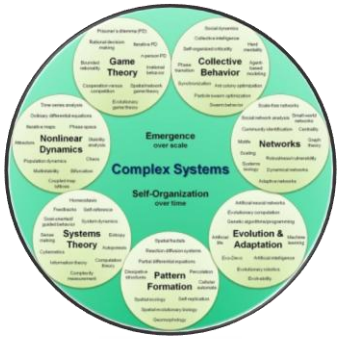
Чечулин Андрей[1,2], Бахтин Юрий[1]

[1] Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
[2] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Солнечногорск, 19 марта, 2020RuS

Содержание

Введение



Сложные системы

Вектора атак

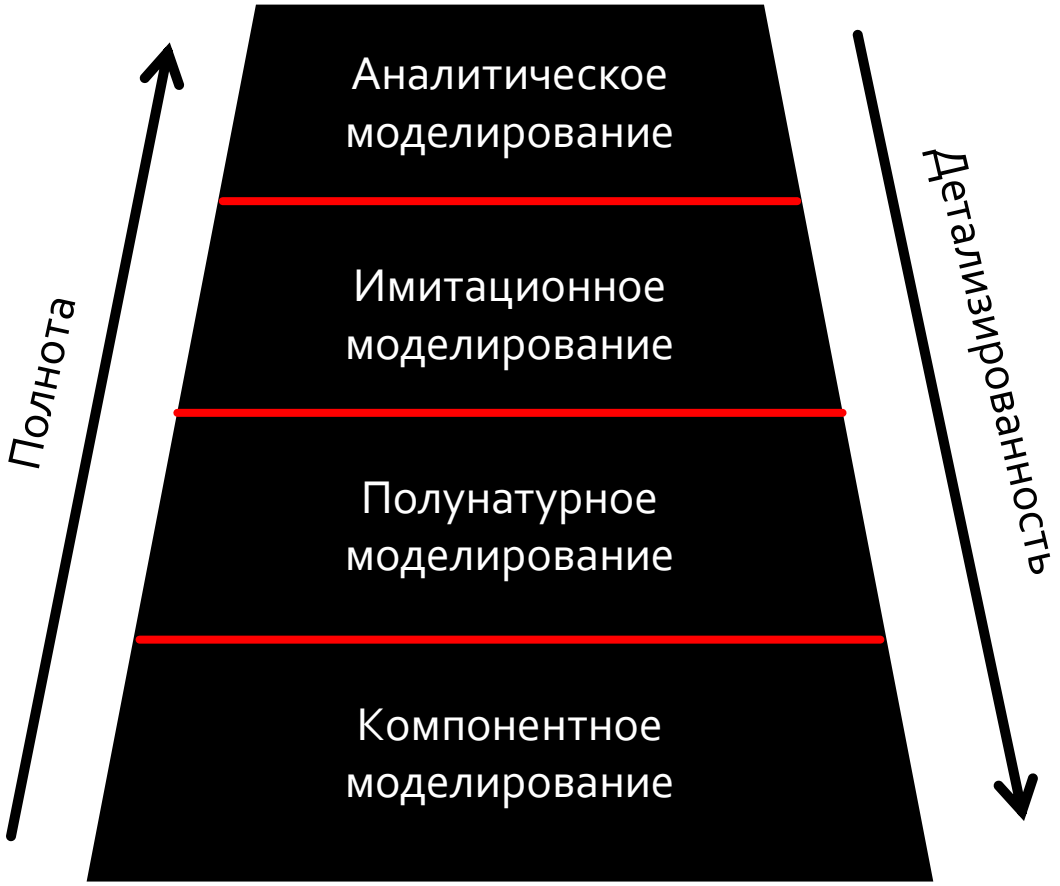
Проблема

- Железная дорога представляет собой сложную техническую систему
- Гетерогенность инфраструктуры обуславливает большое разнообразие возможных векторов атак
- Существующие подходы позволяют провести анализ только отдельных аспектов общей инфраструктуры

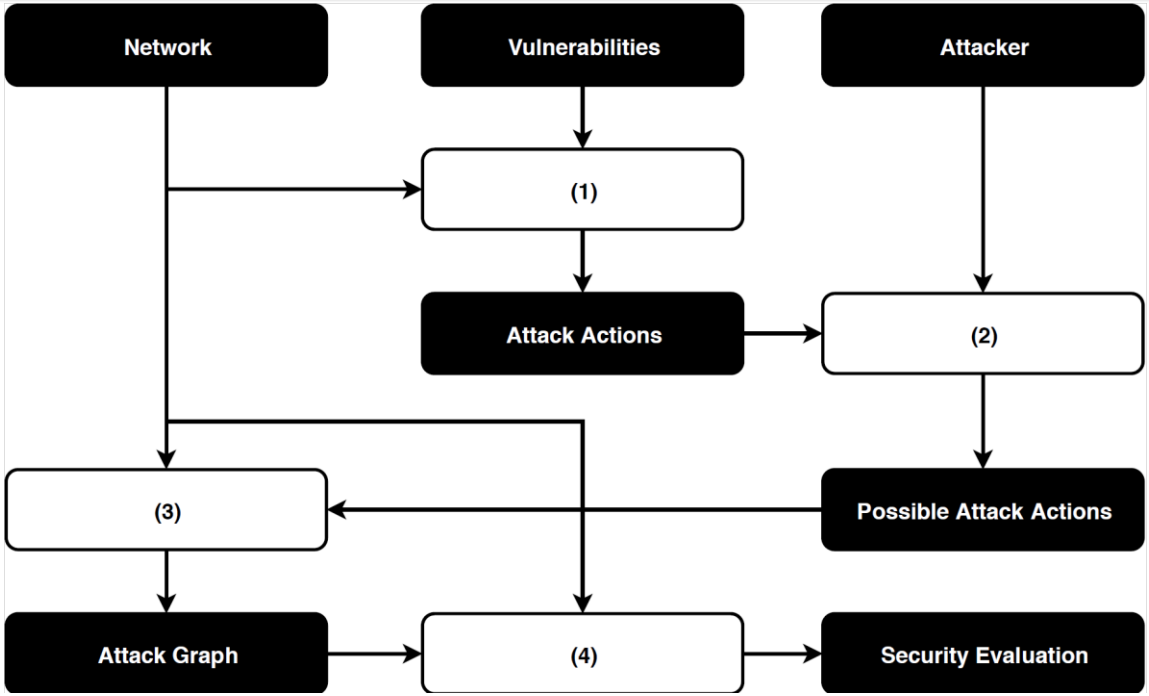
Решение

- Комплексный подход к моделированию инфраструктуры железной дороги и ее отдельных элементов
- Применение различных способов моделирования для учета разных векторов атак

Подход к моделированию (1/5)
Общая архитектура



Подход к моделированию (2/5) Аналитическое моделирование



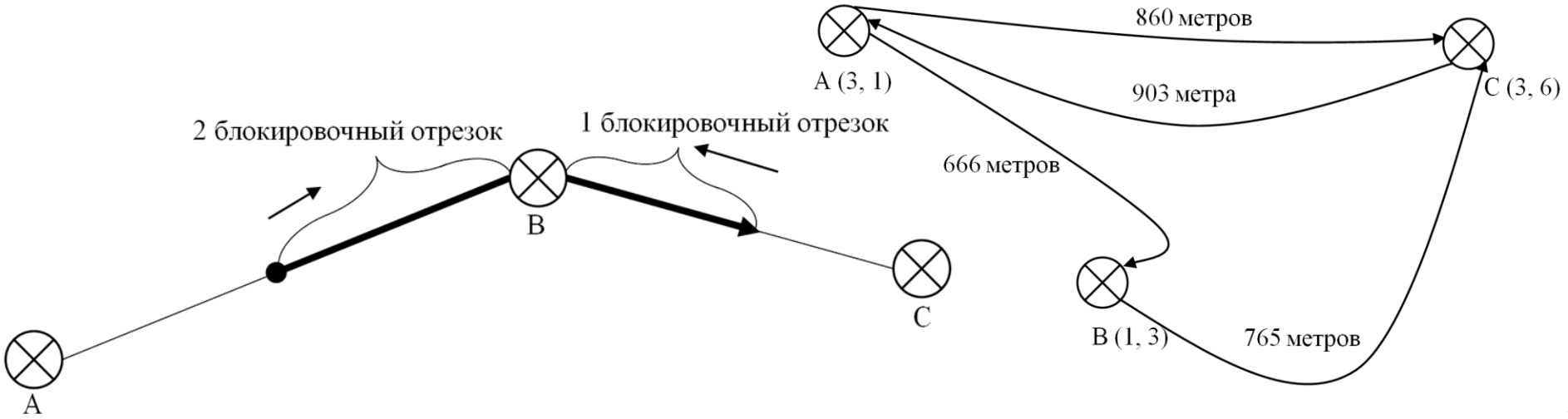
Область применения

- Представление общей сетевой топологии железнодорожной инфраструктуры
- Моделирование взаимодействия между элементами сетевой инфраструктуры
- Выявление недостатков в архитектуре взаимодействия между сервисами

Недостатки

- Отсутствие учета времени
- Специфичность используемой базы данных для устройств железнодорожной инфраструктуры

Подход к моделированию (3/5) Имитационное моделирование



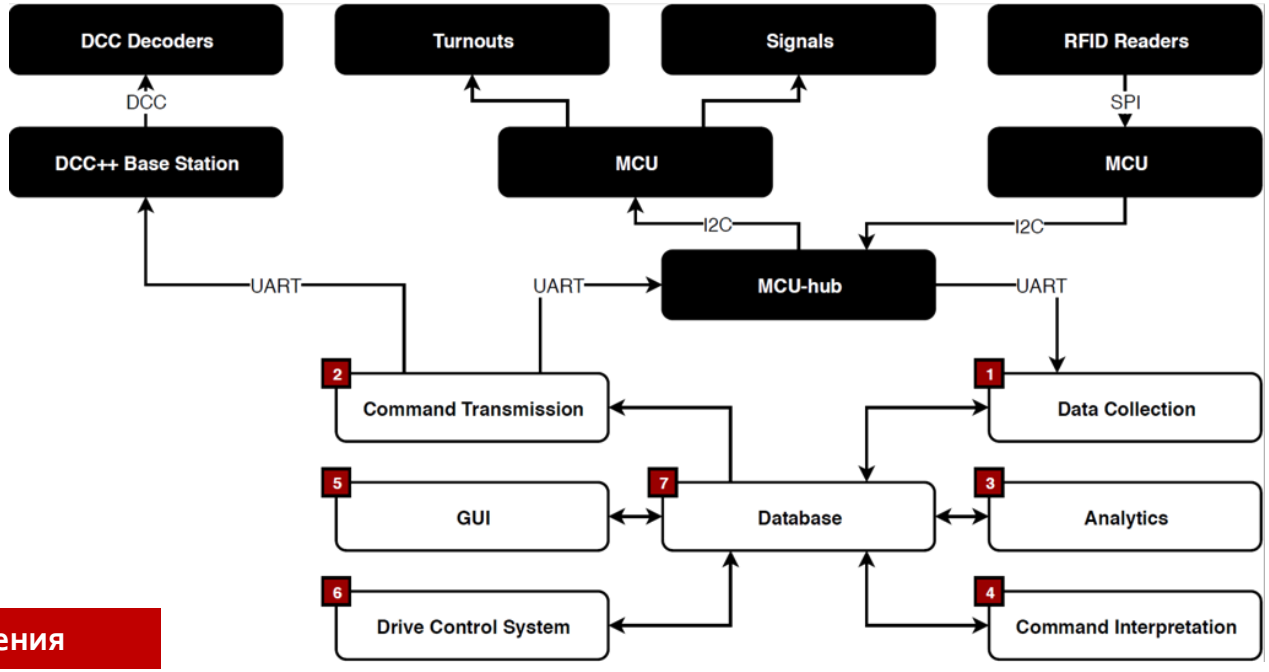
Область применения

- Представление групп поездов и сегментов железнодорожной инфраструктур
- Моделирование взаимозависимостей групп поездов и элементов инфраструктуры
- Выявление недостатков на уровне одновременного управления группами объектов

Недостатки

- Сложность моделирования большого количества объектов
- Сложность повышения детальности моделей

Подход к моделированию (4/5) Полунатурное моделирование



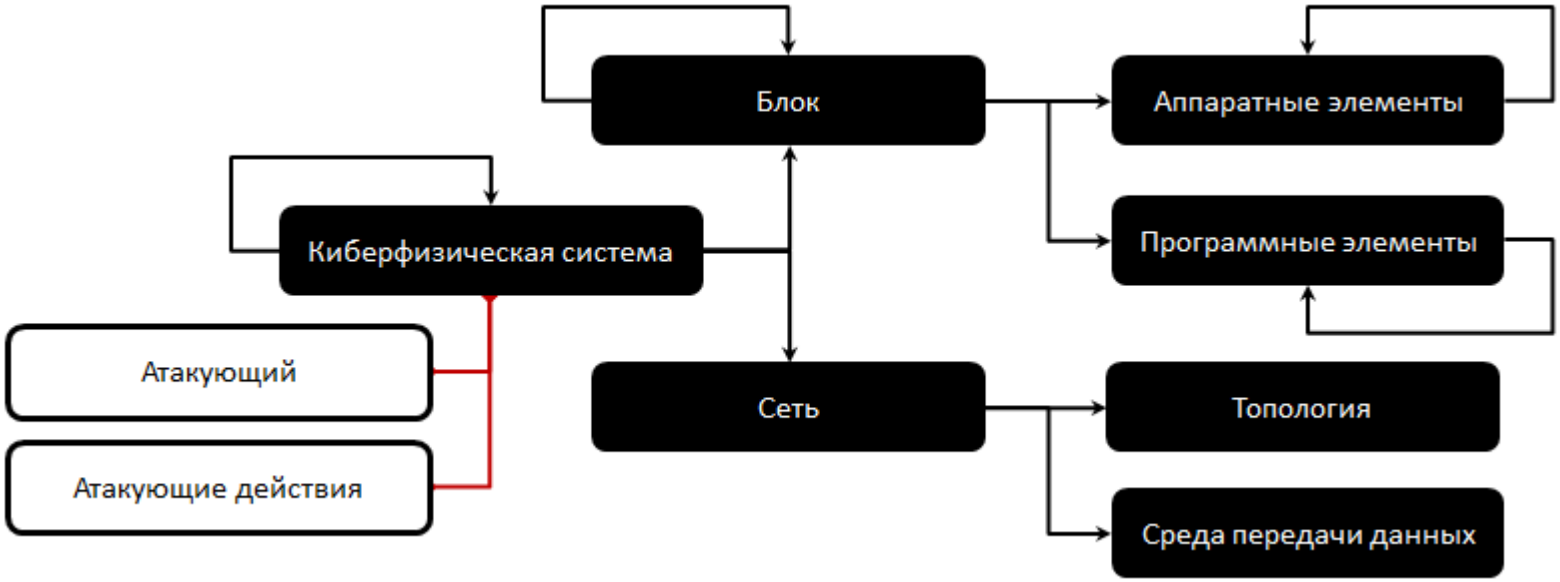
Область применения

- Представление отдельных поездов и крупных объектов дорожной инфраструктуры
- Моделирование взаимодействия инфраструктуры с отдельными устройствами
- Выявление недостатков в архитектуре взаимодействия между поездами и инфраструктурой

Недостатки

- Сложность моделирования специфических устройств
- Невозможность моделирования большого количества объектов

Подход к моделированию (5/5)
Компонентное моделирование



Область применение

- Представление отдельных аппаратных и/или программных компонентов
- Верификация информационных потоков
- Выявление слабых мест архитектурных решений

Недостатки

- Специфичность используемой базы данных
- Невозможность формальной верификации сложных систем

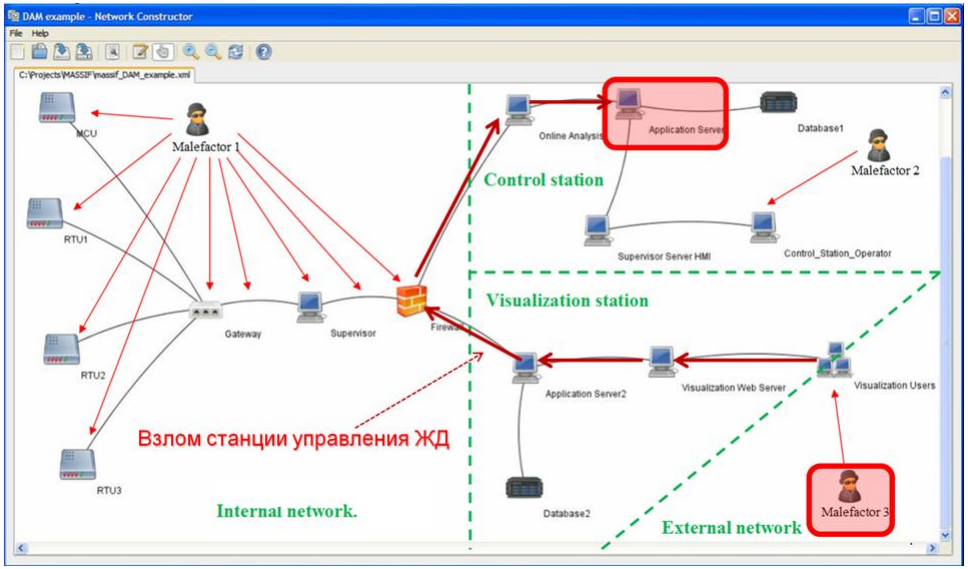
Применение подхода (1/4)
Аналитическое моделирование

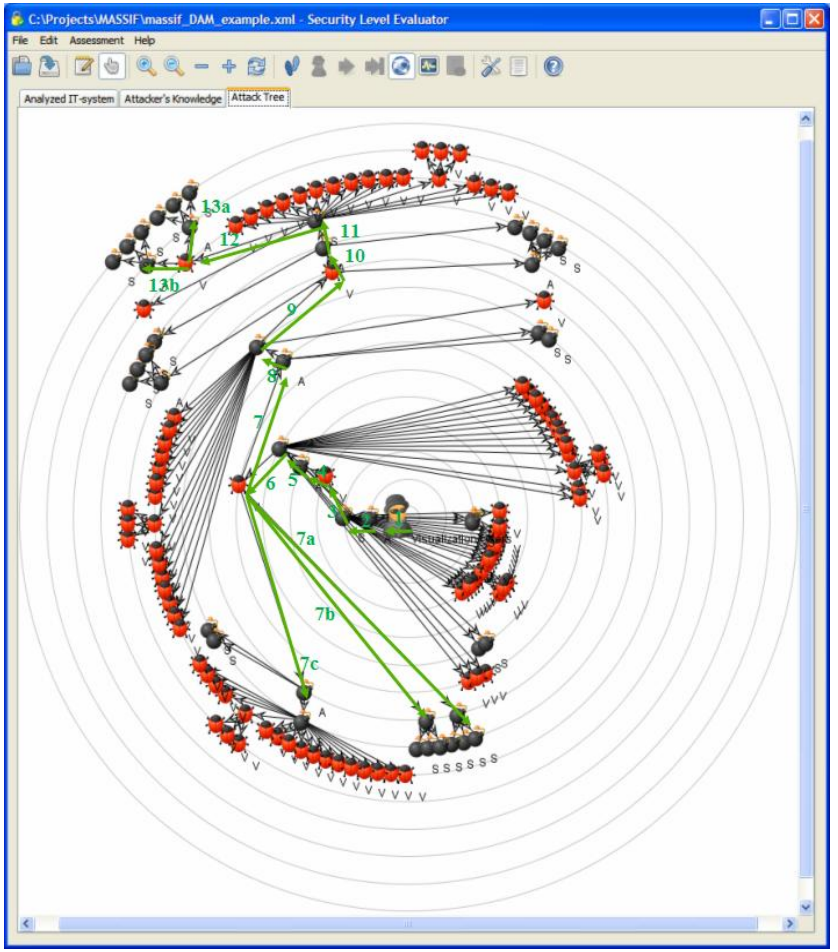
Исходные данные:

- Топология сети и спецификации ее элементов
- База данных уязвимостей
- Характеристики атакующего

Цель:

- Выявление слабых мест инфраструктуры, оценка защищенности по отношению к сетевым атакам





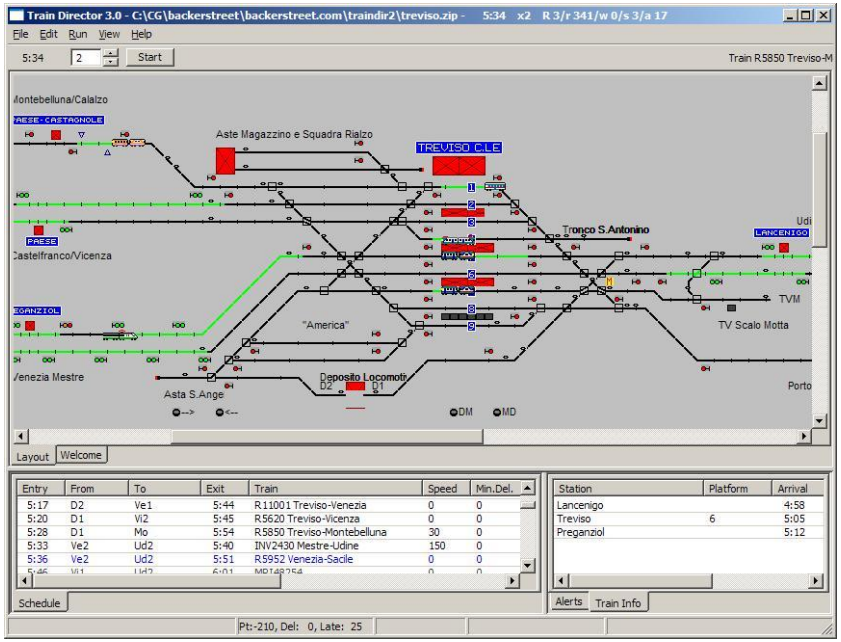
Применение подхода (2/4)
Имитационное моделирование

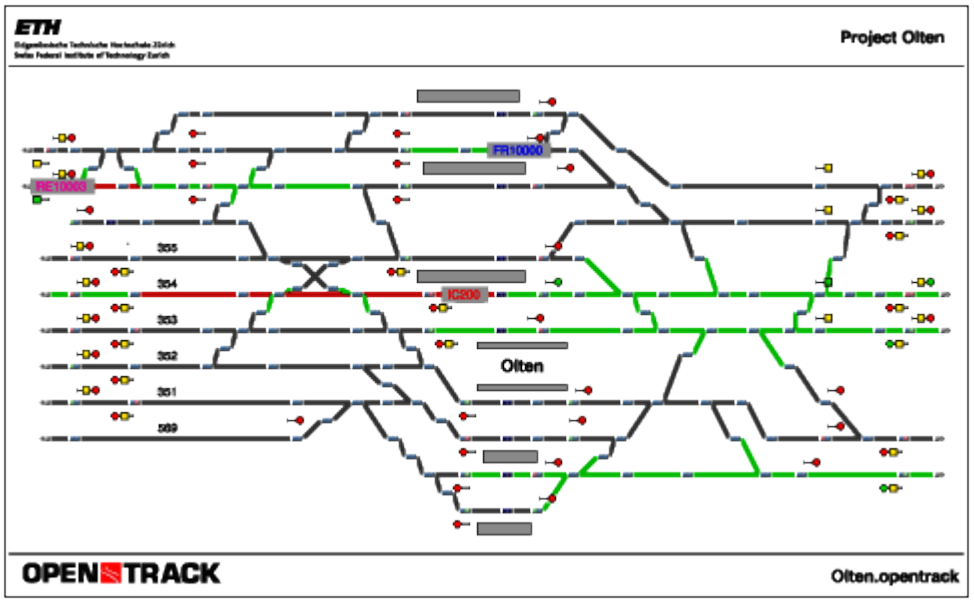
Исходные данные:

- Схема железнодорожной инфраструктуры и характеристики ее отдельных элементов и поездов
- Система или алгоритмы управления
- Характеристики проверяемых нарушений

Цель:

- Выявление слабых мест системы управления, оценка защищенности по отношению к сбоям





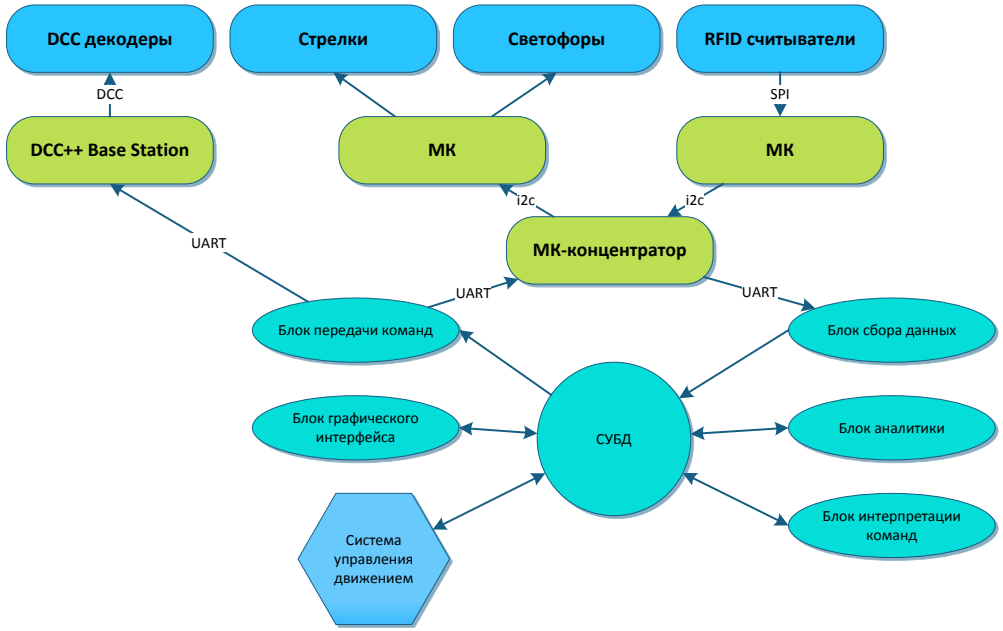
Применение подхода (3/4)
Полунатурное моделирование

Исходные данные:

- Схема сегмента железнодорожной инфраструктуры и характеристики ее отдельных элементов и поездов
- Аппаратные модели поездов и отдельных элементов инфраструктуры
- Характеристики проверяемых нарушений

Цель:

- Выявление слабых мест элементов инфраструктуры, оценка защищенности по отношению к атакам, направленным на элементы инфраструктуры



Применение подхода (4/4)
Компонентное моделирование

Исходные данные:

- Топология связей между устройствами и их элементами
- База данных компонентов устройств и их интерфейсов
- Характеристики атакующего

Цель:

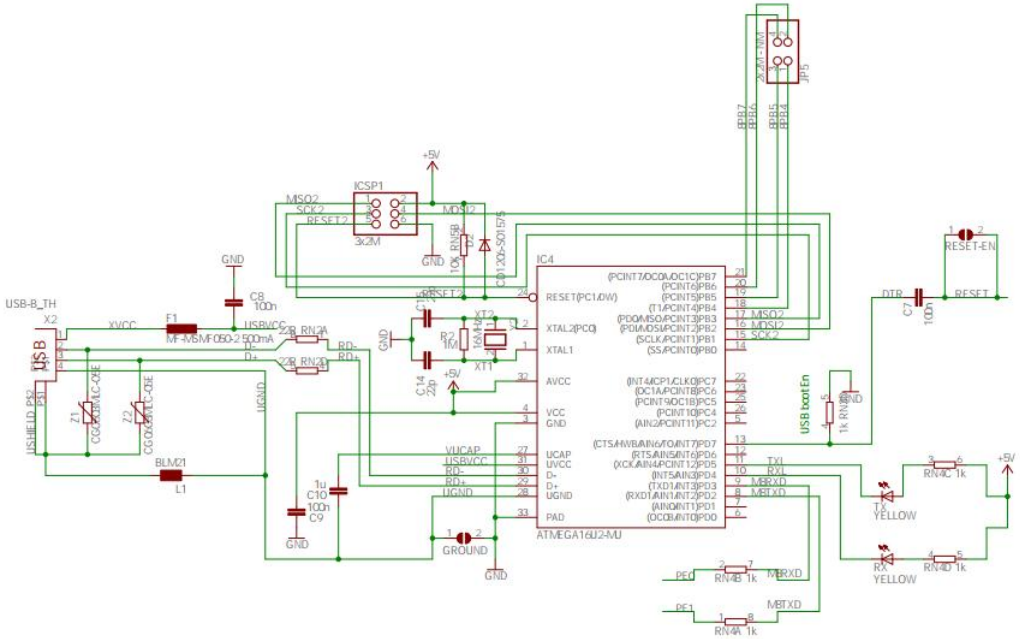
- Выявление слабых мест устройств, оценка защищенности по отношению к кибер-физическим атакам

Microsoft SDL

Cisco SDL

Zachman

Проект SecFutur



Область применения

- Подход позволяет разработчикам проектировать **сложные элементы железнодорожной инфраструктуры**
- Перечень возможных **моделируемых элементов** зависит от качества **базы знаний**
- **Эксперт** может использовать только часть способов моделирования, в зависимости от поставленной задачи
- Подход может быть **полезен** эксперту в качестве инструмента для **автоматизации** отдельных **рутинных** задач
- Подход может быть **полезен** эксперту как **дополнительный способ проверки**, принимаемых решений по модернизации программных и/или аппаратных элементов инфраструктуры

Заключение

Заключение:

- Разработанный подход представляет собой **объединение** различных видов моделирования **железнодорожной инфраструктуры**.
- **Универсальность** разработанного подхода **подтверждается** учетом различных аспектов железнодорожной инфраструктуры, начиная со спецификации отдельных устройств до топологии сети

Дальнейшие исследования:

- Проведение дополнительных экспериментов по применению разработанного подхода к анализу защищенности и надежности железнодорожной инфраструктуры
- Расширение уже существующей базы моделей отдельных устройств железнодорожной инфраструктуры
- Расширение базы данных уязвимостей для повышения эффективности процесса аналитического моделирования

Контакты

Лаборатория проблем компьютерной безопасности
ФГБУН СПИИРАН:

- Почтовый адрес: 199178, Санкт-Петербург, 14-я линия В.О., д.39
- Телефон: +7(812)328-26-42
- Факс: +7(812)328-44-50
- URL: http://comsec.spb.ru

Международная лаборатория информационной безопасности киберфизических систем Университета ИТМО:

- Почтовый адрес : 191002 , Санкт-Петербург, Ломоносова д. 9

Авторы:

- Чечулин Андрей, chechulin@comsec.spb.ru, http://comsec.spb.ru/chechulin
- Бахтин Юрий, bakhtin@comsec.spb.ru, http://comsec.spb.ru/bakhtin

Работа выполнена при поддержке проекта Минобрнауки России
№ 05.607.21.0322