Технология верификации программных интерфейсов

Петренко Александр Константинович,
зам.руководителя Центра верификации ОС Linux,
Института системного программирования РАН (ИСП РАН)

www.ispras.ru
www.linuxtesting.org
www.unitesk.com

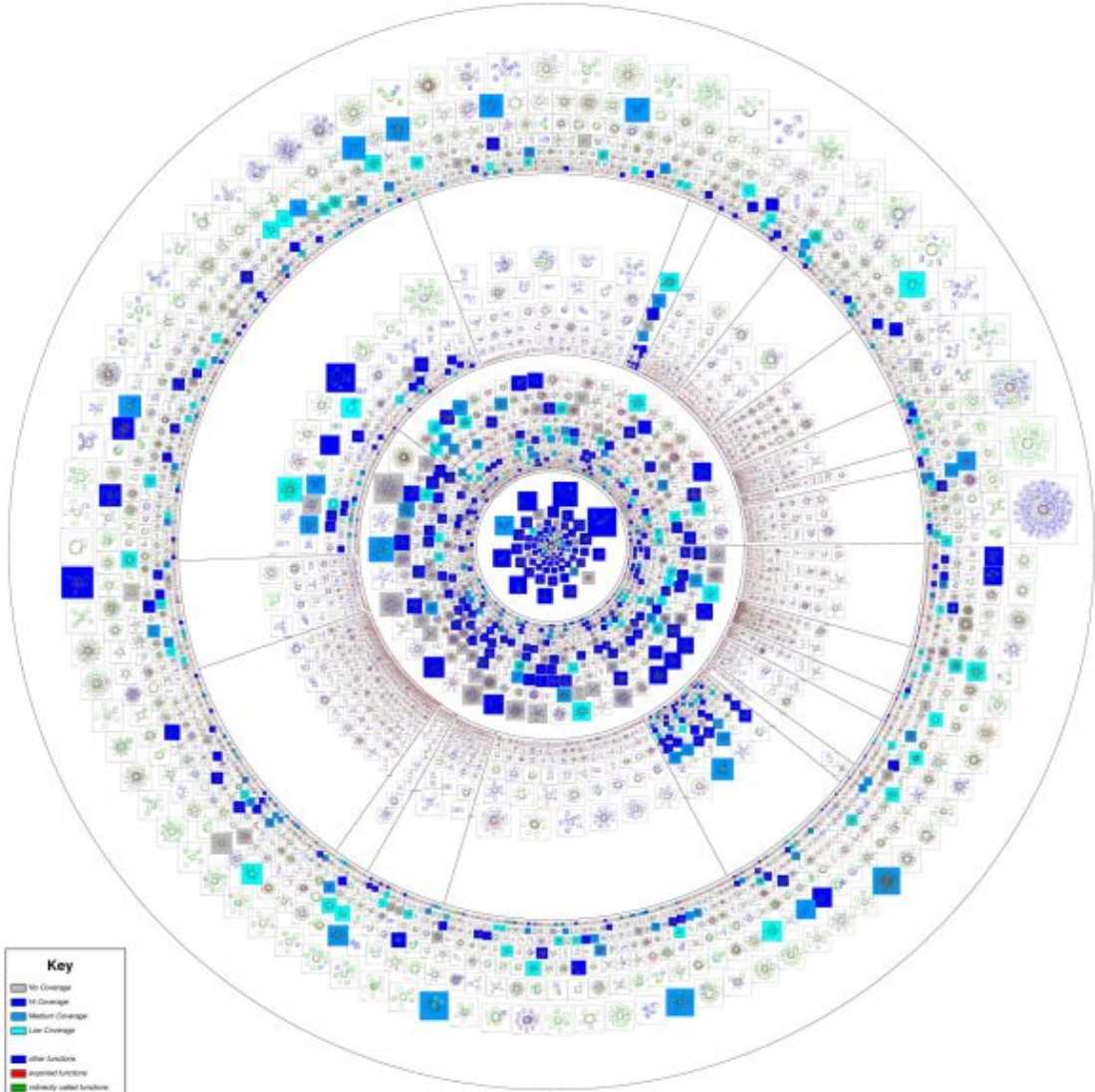
Москва, 4 сентября 2006

Проект OLVER: разработка открытого верификационного набора для LSB 3.1

- Верификация – проверка на соответствие требованиям (спецификациям требований)
- LSB – Linux Standard Base
- Подробности на стенде Центра Верификации ОС Linux ИСП РАН, см.

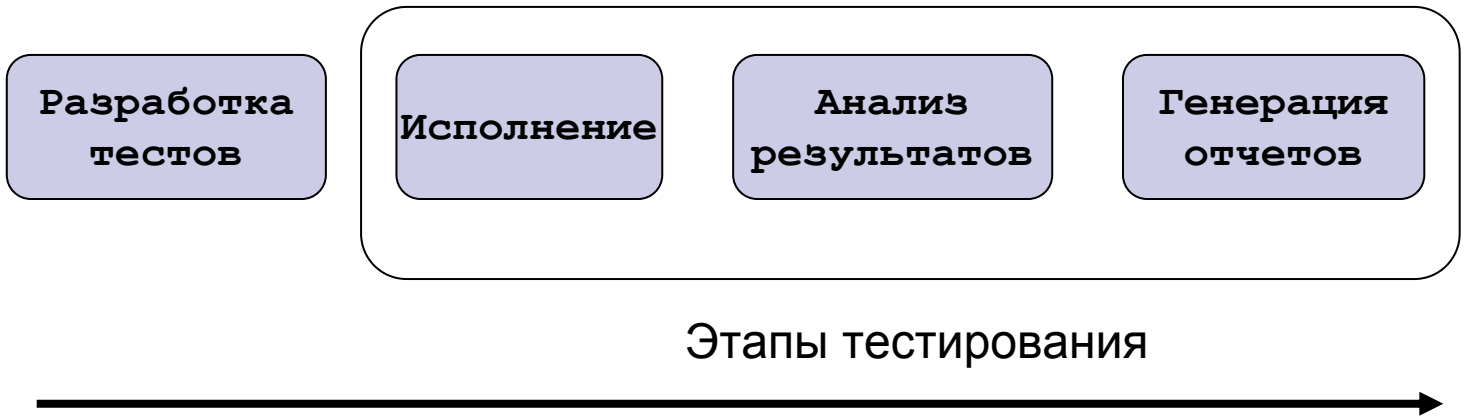
linuxtesting.org

LinuxTestProject.org
Kernel: 2.6.0 - LTP Coverage Analysis
Arch: i386, PPC, s390

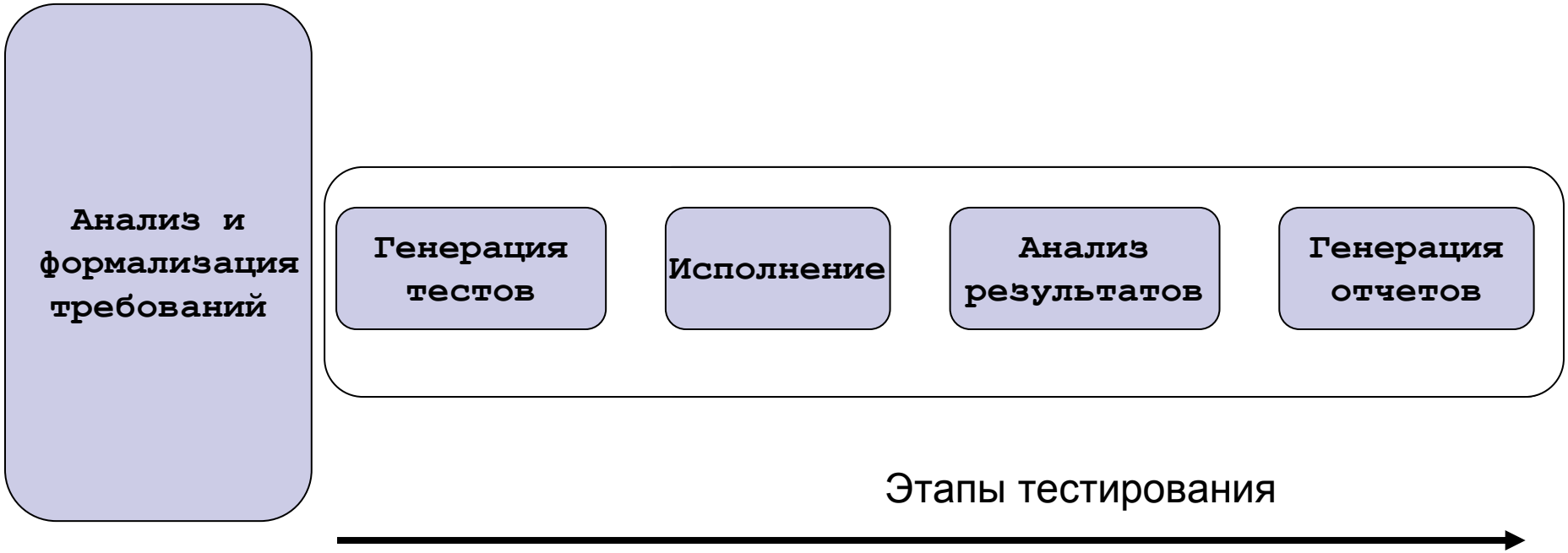


By James M. Kenefick Jr.
Based on work by Rusty Russell, Christian Reiniger

Традиционные технологии тестирования



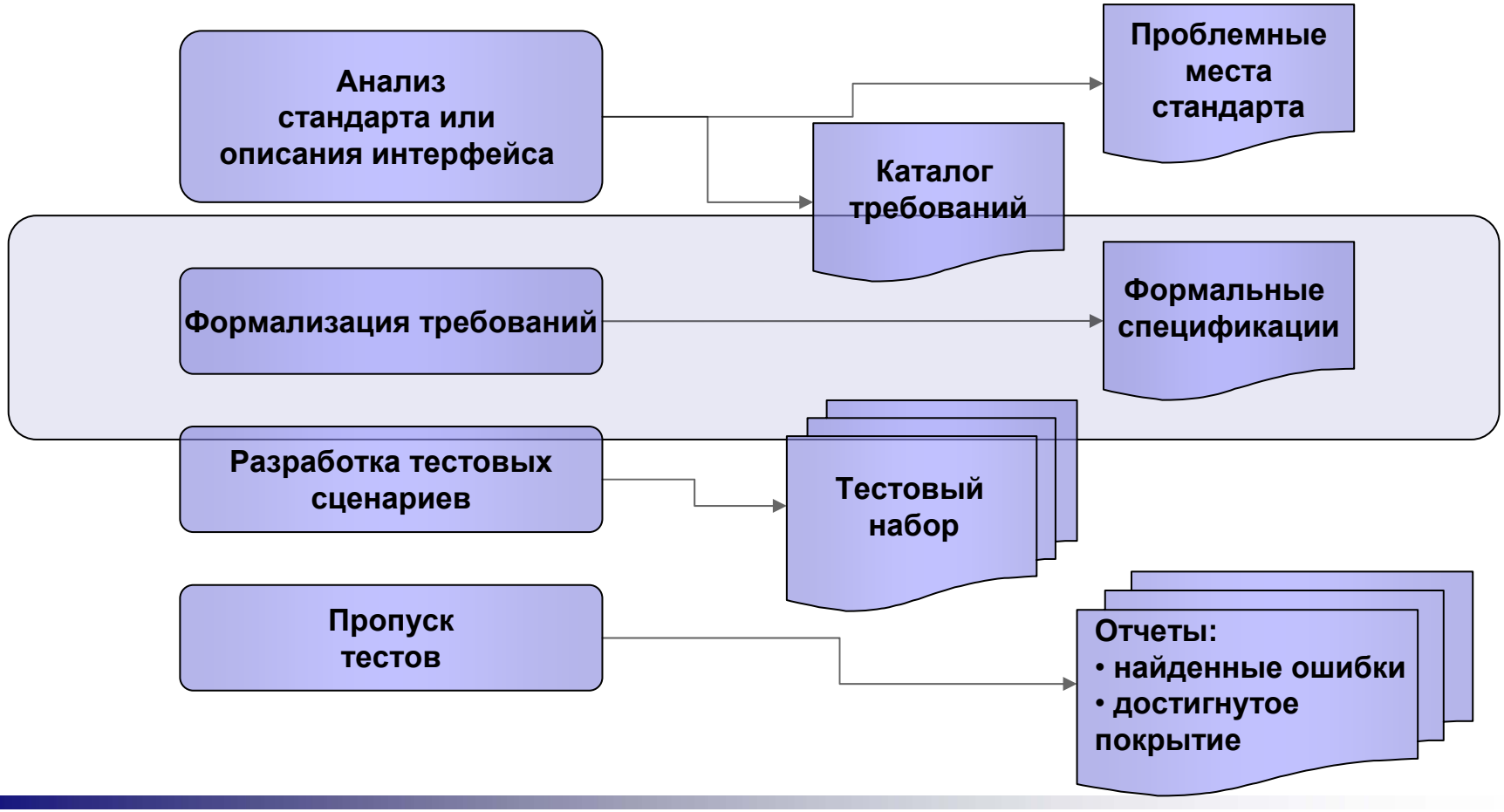
Технологии тестирования на основе спецификаций



Примеры применения UniTesK

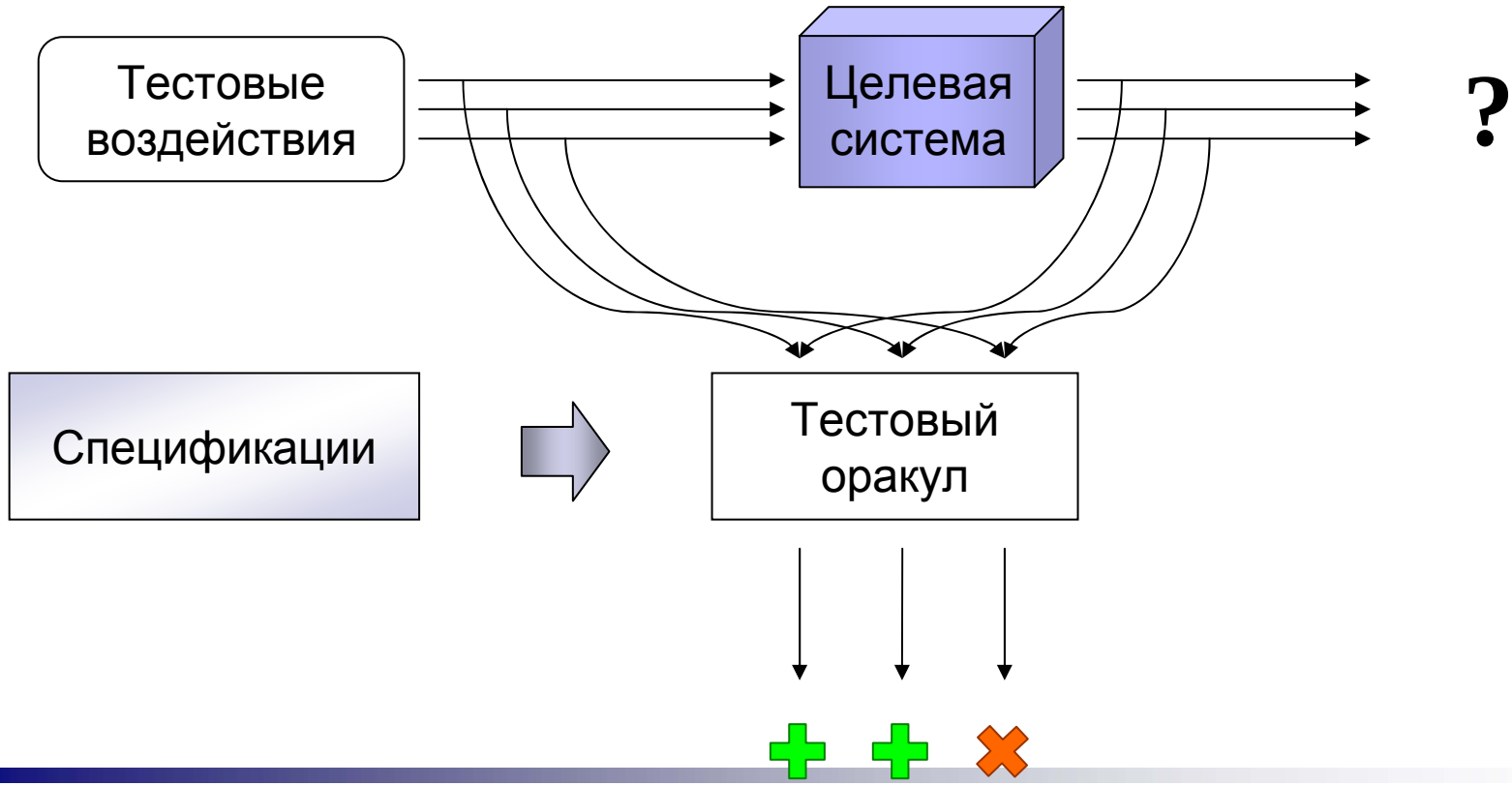
- Тестирование ядра ОС реального времени - 1994-2000
- Реализации IPv6 - 2001-2003
- Компиляторы Intel - 2001-2004
- Java платформа - 2005
- Стандарт IPMP (MPEG-2, MPEG-21) - 2004
- Части инф.системы (ВымпелКом) - 2005
- ОС реального времени (ОС2000, Arinc 653)- 2005-2006
- Simulink оптимизатор (Daimler Chrysler) - 2005
- Пилотные проекты - 2003 - 3005
  - Блок системы реального времени (ГосНИИАС)
  - Банковская система ведения данных о клиентах (Люксофт)
  - Tiny OS (ОС сенсорных сетей) (Berkeley Univ/Люксофт)

Технологический процесс (1)



Тестовые оракулы

Автоматический анализ правильности результатов



Пример из POSIX. Спецификация на расширении C

```
specification  void* realloc_spec( void *ptr, size_t size) {
post {
   if (ptr != NULL) {
    if (size > 0) {
      if (realloc_spec != NULL) {
        // The contents of the object shall remain unchanged up to the lesser of
    the new and old sizes.
        return is_unchanged( old_value, realloc_spec, min(old_size,size) )
           // Each such allocation shall yield a pointer to an object disjoint from
    any other object.
           && ( (ptr != realloc_spec) => is_disjoint_object(
    remove_Chunk(@memory,ptr), realloc_spec, size ) );
      } else /* realloc == NULL */ {
        // If the space cannot be allocated, the object shall remain unchanged.
```

. . .

Пример:
Спецификации стандарта LSB

Условия применимости UniTesK

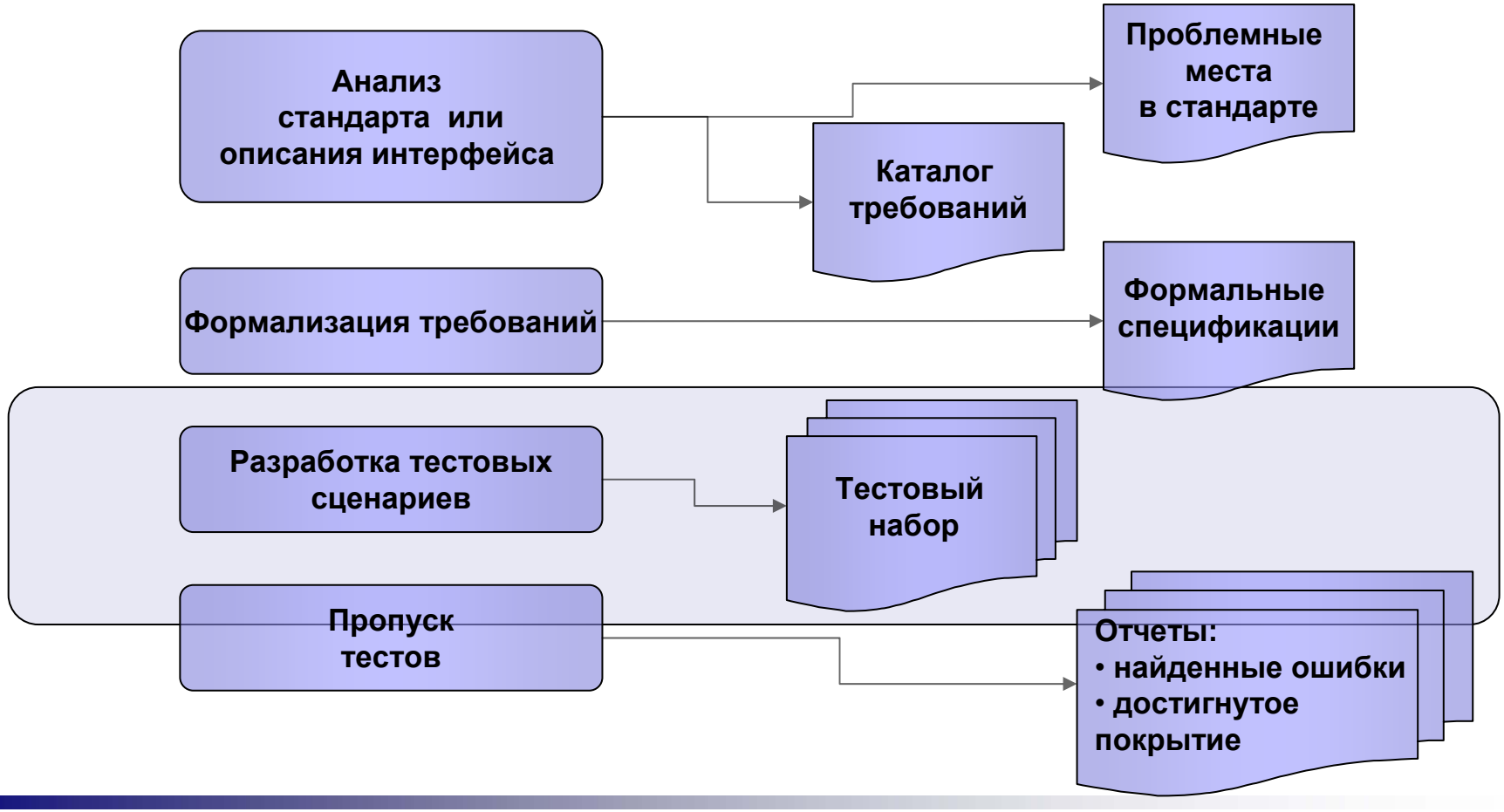
- Интерфейсы системы достаточно стабильны
- Есть потребность в высокой надежности реализации

- Предполагается развитие системы (и интерфейсов)
- Вероятна разработка многих вариантов системы с аналогичными интерфейсами

Применимость UniTESK для различных видов тестирования

- Тестирование соответствия
- Функциональное тестирование
- Тестирование интероперабельности
- Нагрузочное тестирование
- Стрессовое тестирование
- Тестирование производительности

Технологический процесс (2)

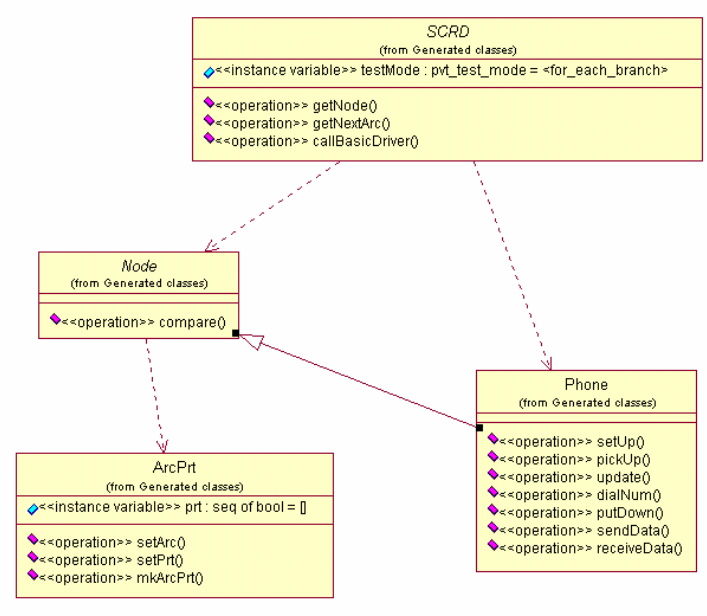


Контакты

- Сайт Института
  http://www.ispras.ru
- Сайты проектов UniTESK
  http://unitesk.com
  http://linuxtesting.org
- Электронный адрес
  Петренко Александр Константинович
  petrenko@ispras.ru
- Телефон: (095) 912-5317 доб. 4404

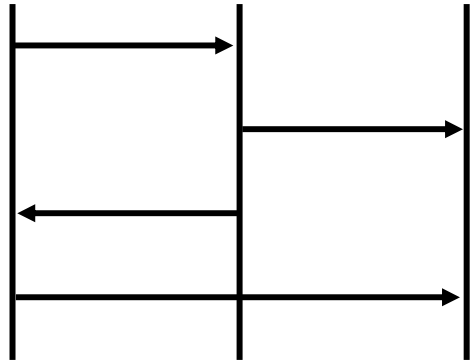
Приложения

Виды спецификаций

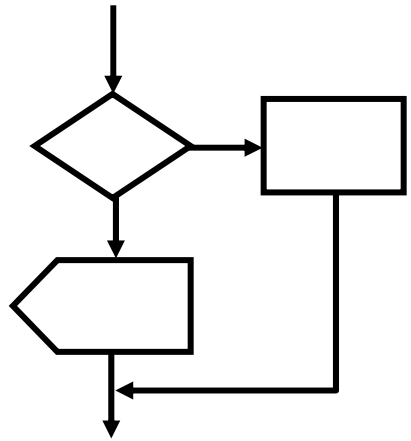


UML

MSC



SDL



Пример:
Функция day_of_week на языке C

```
int
day_of_week (int tday, int tyear, rc * rc) {

    if( tyear < 0 || tday <= 0 || tday > 366 ||
     ( tday == 366 && is_leap( tyear ) ) ) {
     *rc = nok;
     return 0;
   } else {
     *rc = ok;
     return
        ( days_after_initial_year( tyear, tday )
         + initial_day_of_week )
        % days_in_week;
   }
}
```

«Полуформальная»спецификация

Требования к входным параметрам

tyear > 0

И

tday > 0

И

tday <= 366

И

tday ~= 366

ИЛИ

tyear is a leap year

В случае некорректных входных параметров (*BRANCH "Bad parameters"*):

Результатом функции должен быть 0

И

Код ответа rc = NOK

В случае корректных входных параметров (*BRANCH "OK"*):

Результатом функции должен быть остаток от деления суммы результата функции «number of days after initial year» и константы «weekday of the initial year» на номер дня tday в неделе

И

Код ответа rc = OK

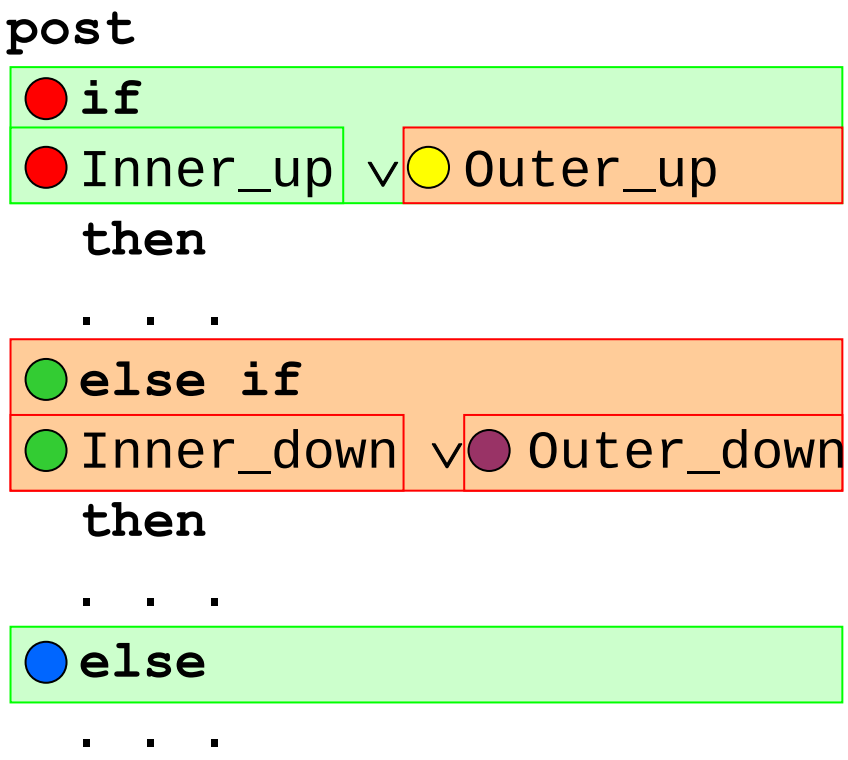
Спецификация на языке RAISE

```
DAY_OF_WEEK : INT >< INT -~-> RC >< WEEKDAY
DAY_OF_WEEK( tday, tyear ) as ( post_rc, post_Answer )
post
    if      tyear <= 0 \/ tday <= 0 \/
            tday > 366 \/ tday = 366
            /\ ~a_IS_LEAP( tyear )
    then
            BRANCH( bad_param, "Bad parameters" );
            post_Answer = 0 /\ post_rc = NOK
    else
            BRANCH( ok, "OK" );
            post_Answer = (a_DAYS_AFTER_INITIAL_YEAR(tyear, tday ) +
                                    a_INITIAL_DAY_OF_WEEK ) \
            a_DAYS_IN_WEEK /\ post_rc = OK
    end
```

Критерии тестового покрытия

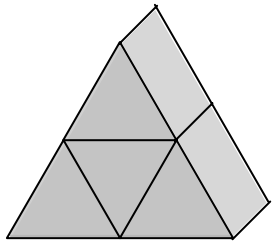
Качество тестирования измеряется степенью

- покрытия тестируемой системы и
- покрытия логических ветвей спецификаций требований



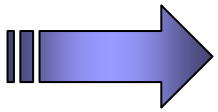
UniTESK: схема тестирования

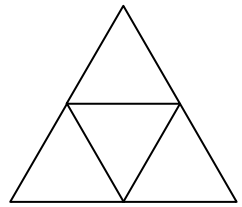
Тестируемая система



Спецификация

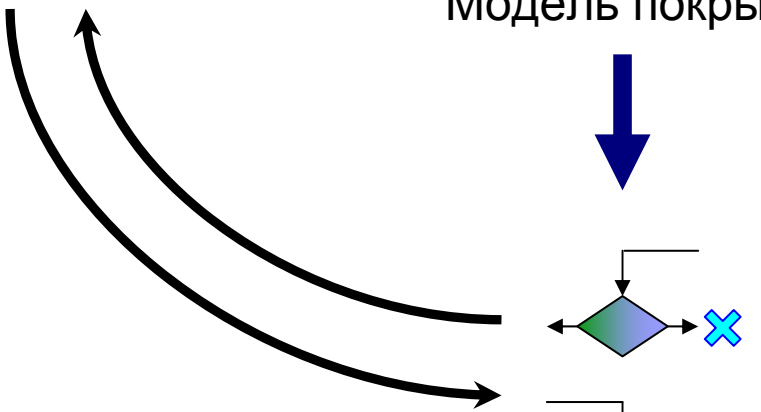
Модель покрытия





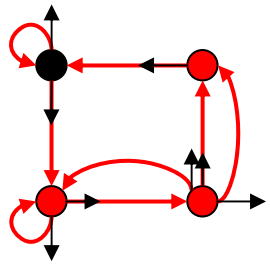
Модель теста

Тестовый сценарий

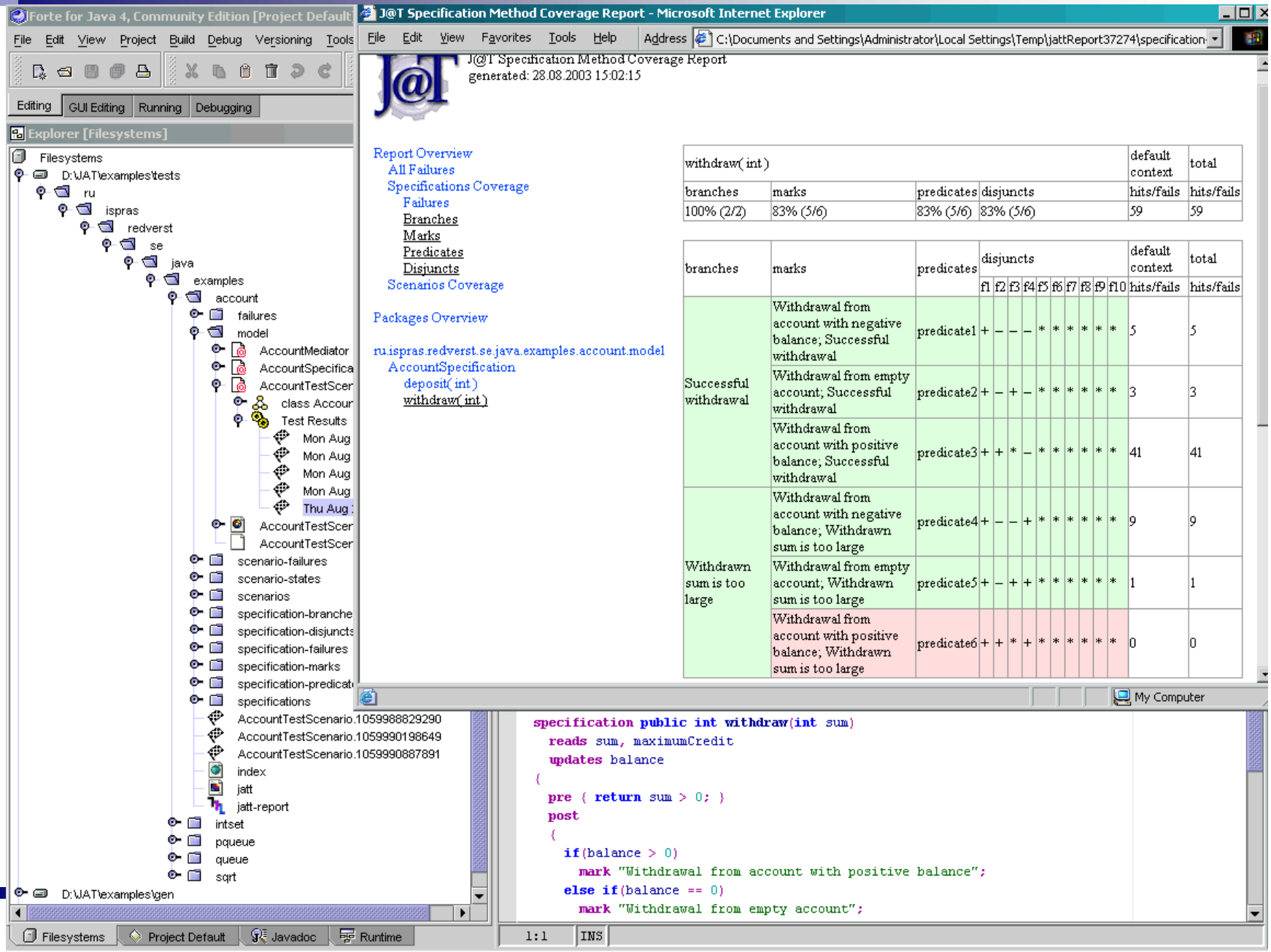


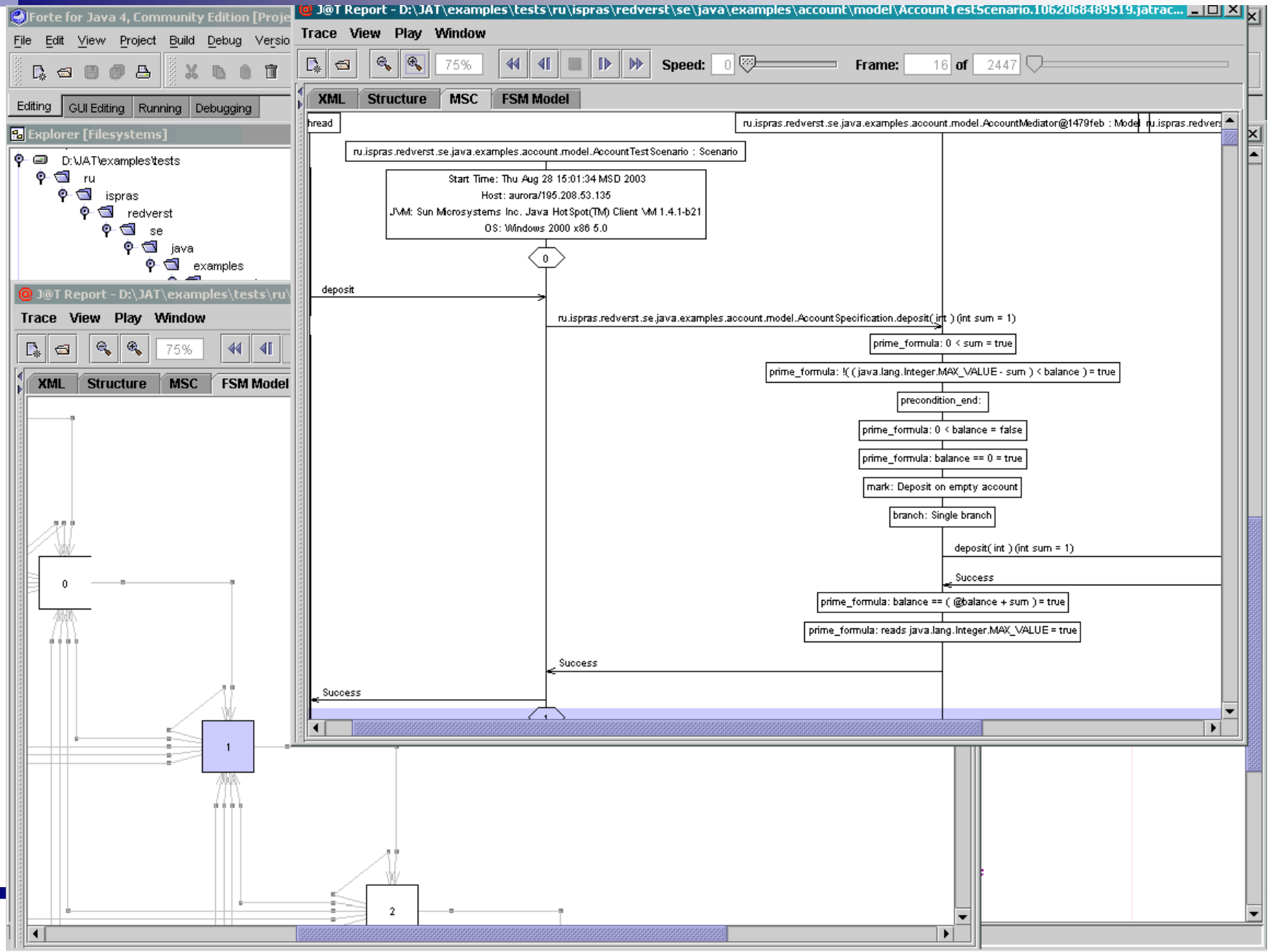
Анализ результатов

Трасса покрытия



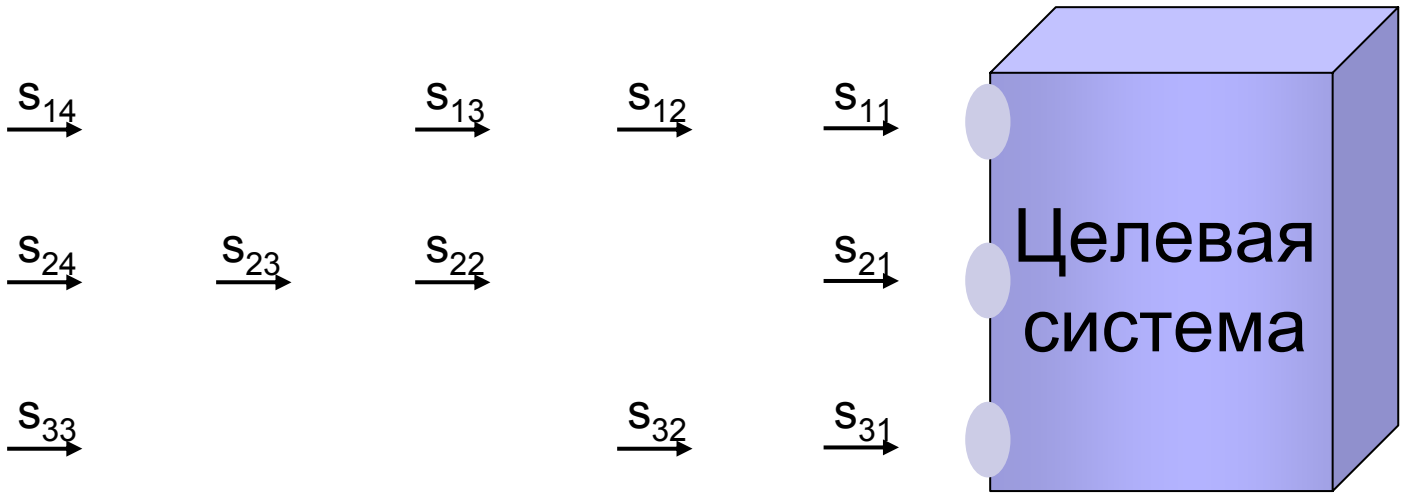
Генератор тестовых стимулов


Forte for Java 4, Community Edition [Project Default]
File Edit View Project Build Debug Versioning Tools
Editing GUI Editing Running Debugging
Explorer [Filesystems]
Filesystems
D:\JAT\examples\tests
ru
ispras
redverst
se
java
examples
account
failures
model
AccountMediator
AccountSpecifica
AccountTestScer
class Accour
Test Results
Mon Aug
Mon Aug
Mon Aug
Mon Aug
Thu Aug
AccountTestScer
AccountTestScer
scenario-failures
scenario-states
scenarios
specification-branche
specification-disjuncts
specification-failures
specification-marks
specification-predicat
specifications
AccountTestScenario.1059988829290
AccountTestScenario.1059990198649
AccountTestScenario.1059990887891
index
jatt
jatt-report
intset
pqueue
queue
sqrt
D:\JAT\examples\gen
Filesystems
Project Default
Javadoc
Runtime
J@T Specification Method Coverage Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address C:\Documents and Settings\Administrator\Local Settings\Temp\jattReport37274\specification-
J@T Specification Method Coverage Report
generated: 28.08.2003 15:02:15
Report Overview
All Failures
Specifications Coverage
Failures
Branches
Marks
Predicates
Disjuncts
Scenarios Coverage
Packages Overview
ru.ispras.redverst.se.java.examples.account.model
AccountSpecification
deposit(int)
withdraw(int)
withdraw(int)
default context
total
branches
marks
predicates
disjuncts
hits/fails
100% (2/2)
83% (5/6)
83% (5/6)
83% (5/6)
59
59
f1 f2 f3 f4 f5 f6 f7 f8 f9 f10
Successful withdrawal
Withdrawal from account with negative balance; Successful withdrawal
predicate1
+ – – – * * * * * *
5
5
Withdrawal from empty account; Successful withdrawal
predicate2
+ – – + – * * * * * *
3
3
Withdrawal from account with positive balance; Successful withdrawal
predicate3
+ + * – * * * * * *
41
41
Withdrawn sum is too large
Withdrawal from account with negative balance; Withdrawn sum is too large
predicate4
+ – – + * * * * * *
9
9
Withdrawal from empty account; Withdrawn sum is too large
predicate5
+ – + + * * * * * *
1
1
Withdrawal from account with positive balance; Withdrawn sum is too large
predicate6
+ + * + * * * * * *
0
0
My Computer
specification public int withdraw(int sum)
reads sum, maximumCredit
updates balance
{
pre { return sum > 0; }
post
{
if(balance > 0)
mark "Withdrawal from account with positive balance";
else if(balance == 0)
mark "Withdrawal from empty account";
1:1
INS


Forte for Java 4, Community Edition [Proje
File Edit View Project Build Debug Versio
Editing GUI Editing Running Debugging
Explorer [Filesystems]
D:\JAT\examples\tests
ru
ispras
redverst
se
java
examples
J@T Report - D:\JAT\examples\tests\ru\
Trace View Play Window
75%
XML Structure MSC FSM Model
0
1
2
J@T Report - D:\JAT\examples\tests\ru\ispras\redverst\se\java\examples\account\model\AccountTestScenario.1062068489519.jatrac...
Trace View Play Window
75%
Speed: 0
Frame: 16 of 2447
XML Structure MSC FSM Model
thread
ru.ispras.redverst.se.java.examples.account.model.AccountMediator@1479feb : Model
ru.ispras.redverst.se.java.examples.account.model.AccountTestScenario : Scenario
Start Time: Thu Aug 28 15:01:34 MSD 2003
Host: aurora/195.208.53.135
JVM: Sun Microsystems Inc. Java HotSpot(TM) Client VM 1.4.1-b21
OS: Windows 2000 x86 5.0
0
deposit
ru.ispras.redverst.se.java.examples.account.model.AccountSpecification.deposit(int) (int sum = 1)
prime_formula: 0 < sum = true
prime_formula: !((java.lang.Integer.MAX_VALUE - sum) < balance) = true
precondition_end:
prime_formula: 0 < balance = false
prime_formula: balance == 0 = true
mark: Deposit on empty account
branch: Single branch
deposit(int) (int sum = 1)
Success
prime_formula: balance == (@balance + sum) = true
prime_formula: reads java.lang.Integer.MAX_VALUE = true
Success
Success

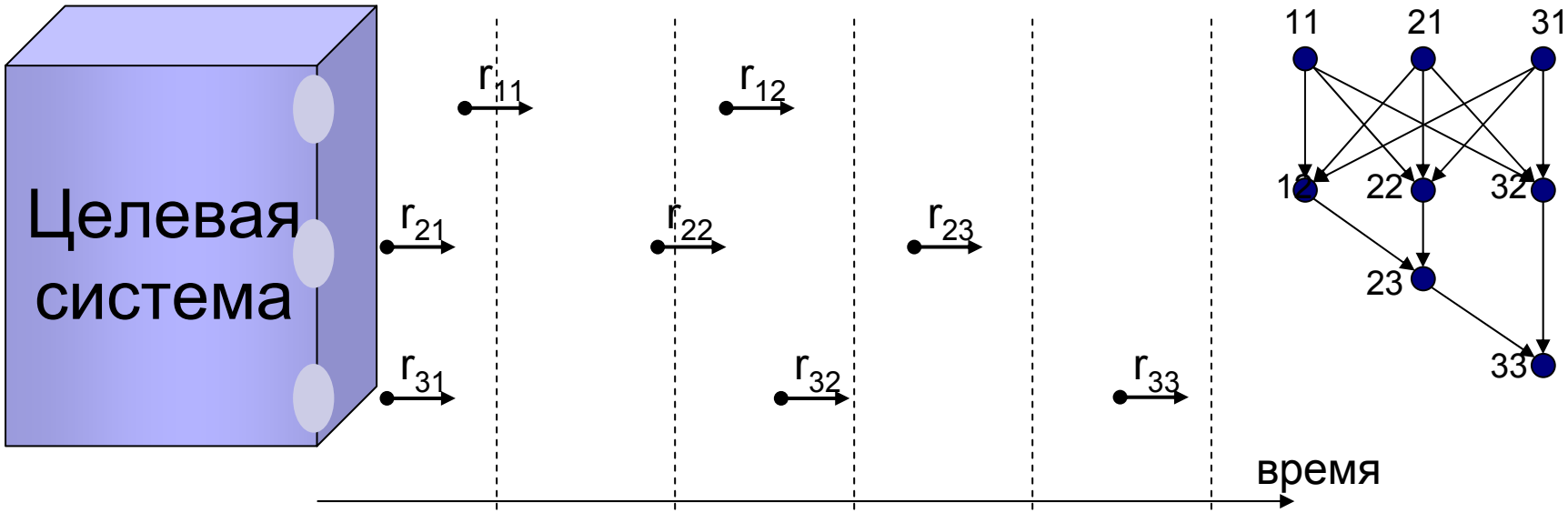
Тестирование компонентных асинхронных систем

Генерация тестовых входов



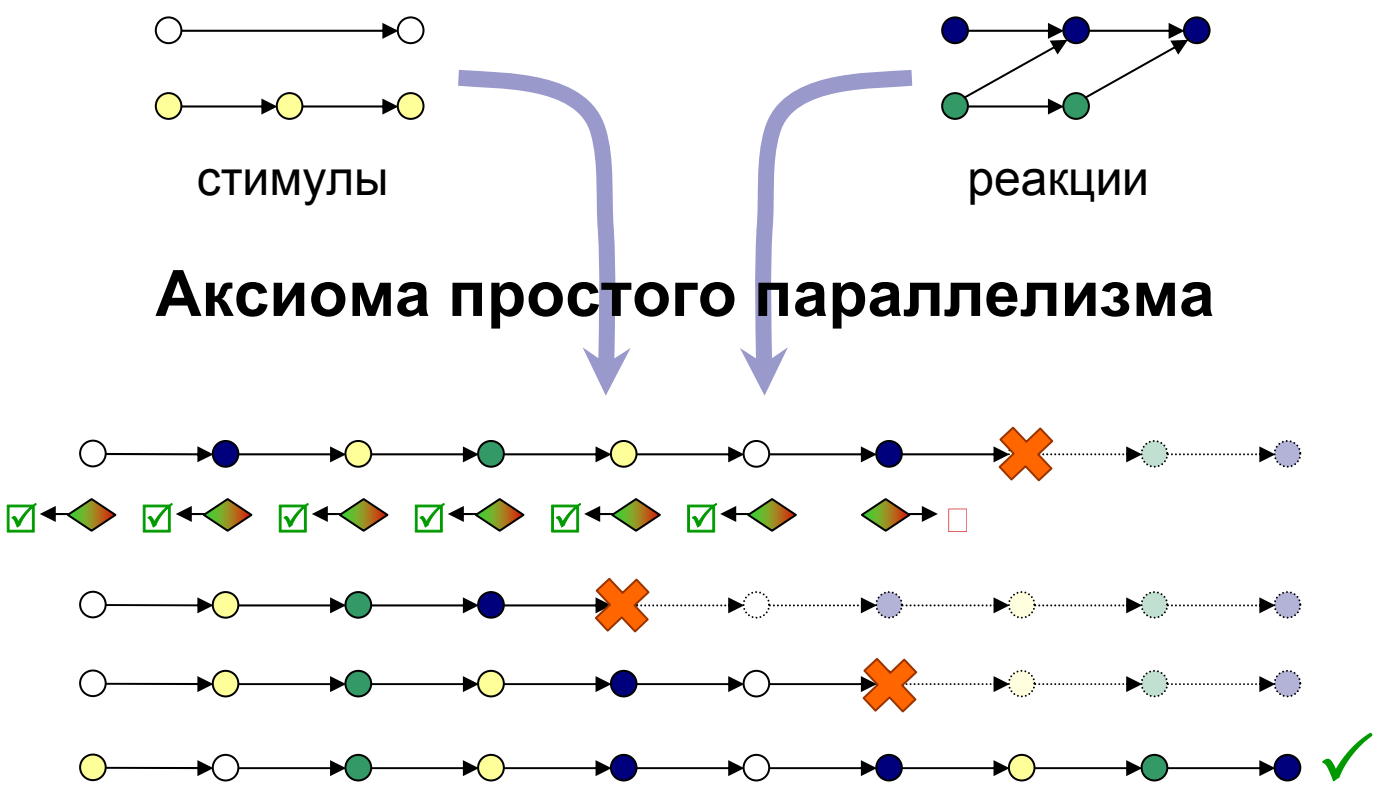
Вместо тестовой последовательности используется набор последовательностей

Сбор реакций



Реакции образуют частично упорядоченное множество

Проверка корректности поведения



Решения UniTesK

- Контрактные спецификации:
  Предусловия и постусловия операций
  Инварианты типов данных
- Спецификации описываются на расширениях языков программирования (имеется поддержка для Java, C/C++ и C#; в перспективе: Delphi, SystemC, VHDL,…)
- Основной критерий качества тестирования – покрытие спецификаций (вариантов выполнения постусловий)
- Построение цепочки тестовых вызовов во время выполнения теста; логика построения - обход конечного автомата, который строится полуавтоматически
- Спецификации и конечный автомат рассматриваются как модели реализации

Решение задач внедрения

- Спецификации и другие компоненты тестов разрабатываются на расширении целевого языка
- Интеграция с привычными средами разработки
- Внедрение
  - Интенсивные тренинги
  - Пилотные проекты
  - Обучение в режиме мастер-подмастрье
  - Консультации

Литература

- В.В.Кулямин, А.К.Петренко, А.С.Косачев, И.Б.Бурдонов. Подход UniTesK к разработке тестов. *Программирование*, т. 29, № 6, 2003, стр. 25-43.
- Е.Н.Бритвина,С.Г.Грошев,А.Монахов, А.К.Петренко, О.Л.Петренко. Тестирование на основе моделей// «Открытые системы», Москва, № 9, 2003, стр. 41-47 стр.
- http://unitesk.ispras.ru/papers
- http://linuxtesting.ru

Спасибо!