

*20 Марта 2012*

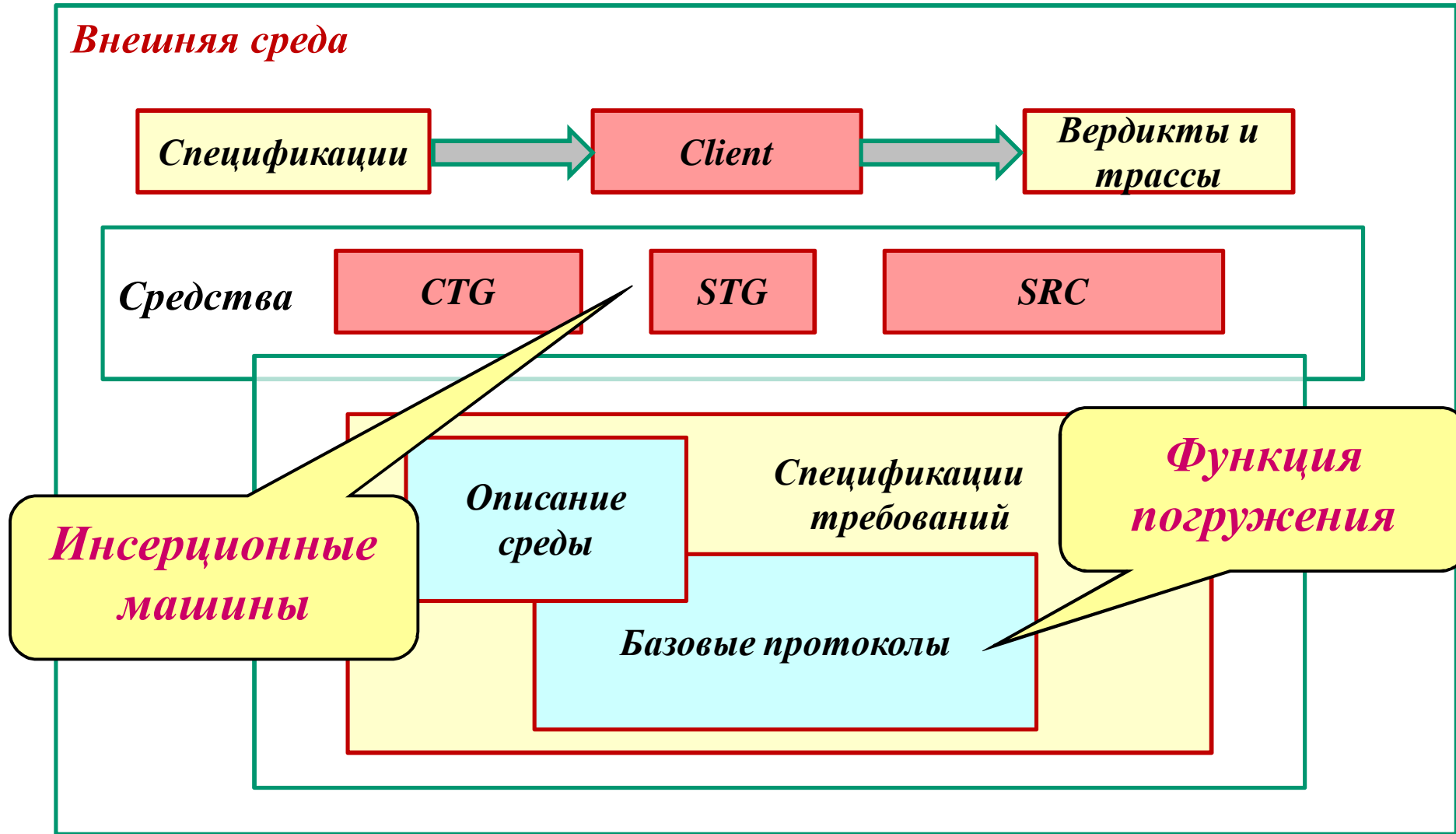
# **Инсерционное моделирование 2**

## **Лекция 5**

### **Система верификации требований VRS (Verification of Requirement Specifications)**

# Система VRS

среда для верификации требований к распределенным программным системам



# Базовые протоколы

Фрагменты программы  
В методе Флойда

*Кванторы первого  
порядка с  
типизированным  
и переменными*

Комбинация Хоаровских троек с моделью взаимодействия агентов и сред  
Другая аналогия: **продукционные системы**  
Метод определения **функции погружения** (look-ahead)

$$\forall x(\alpha(x, r) \rightarrow \{P(x, r)\}\beta(x, r))$$

*Предусловие*

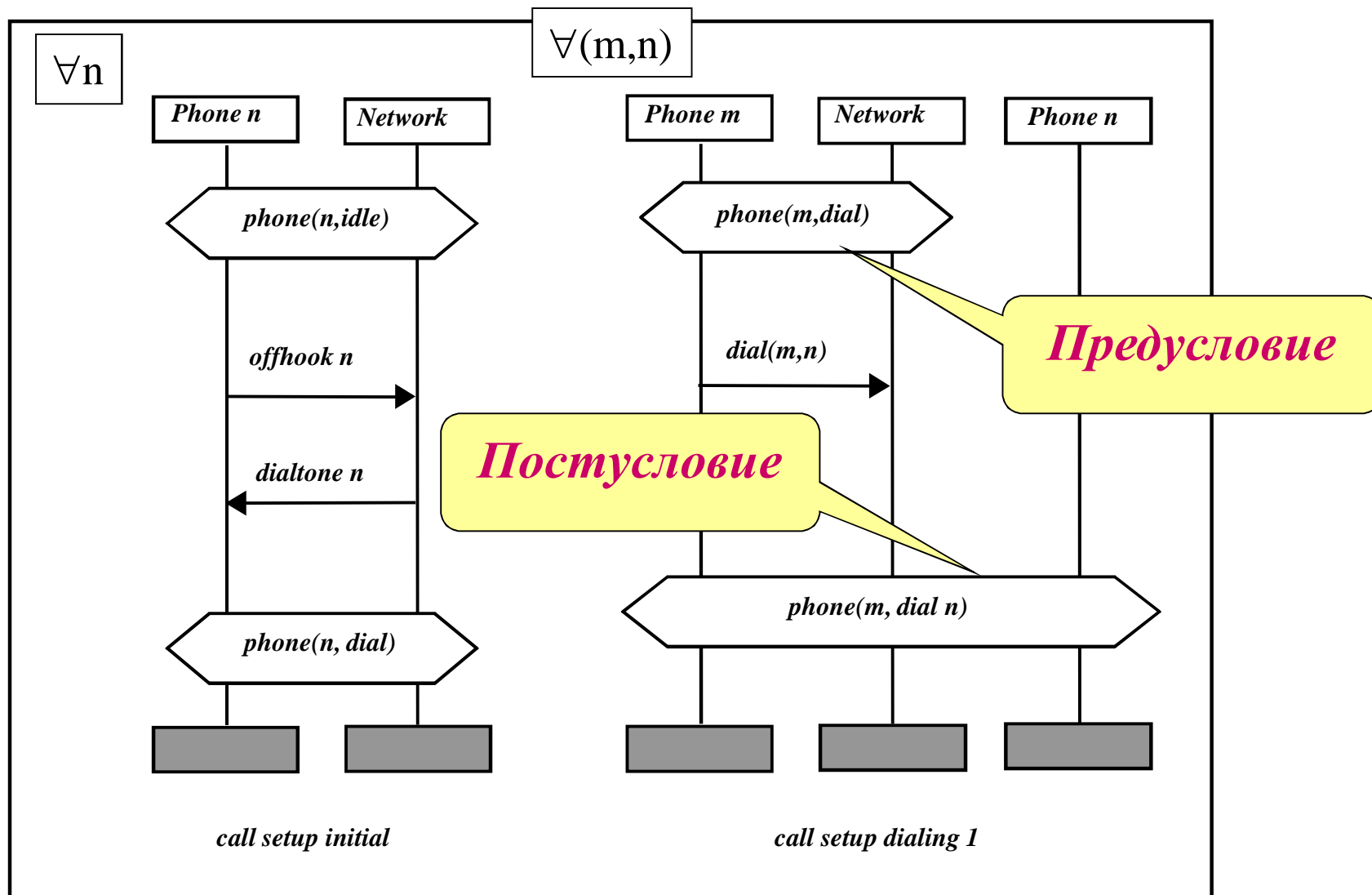
*Атрибутные  
выражения*

*Постусловие*

*Конечный процесс (поведение)  
атрибутивной среды с погруженными в  
нее агентами (MSC)*

*Свойства  
среды*

## Два базовых протокола для модели телефонной связи



# Средства системы VRS

## Формализация требований (Client)

Интерактивная система разработки требований и управления процессом верификации

## Статическая проверка требований (SRC)

Доказательство полноты требований (отсутствие тупиков)

Доказательство непротиворечивости требований

(детерминированность)

Доказательство условий целостности (безопасности, safety)

## Доказательство динамических свойств

Конкретный генератор трасс (CTG)

Символьный генератор трасс (STG)

## Дедуктивная система

Специализированные пруверы + алгоритмы проверки выполнимости и решения задач в смешанных арифметико-логических теориях.

## Генерация тестов

# Язык формальных требований BPSL

## **Basic Protocol Specification Language**

Спецификация системы с помощью совокупности локальных свойств (Базовых Протоколов) взаимодействия агентов, погруженных в среду, где они функционируют.

# Атрибутная среда и атрибутные инсерционные машины

**Состояние среды определяется наборами значений атрибутов или их свойствами.**

**Атрибуты:** простые и функциональные

**Атрибуты среды и атрибуты агентов**

**Типы атрибутов:**

простые: int, real, Bool, symb, behavior, ...

функциональные:  $(\tau_1, \tau_2, \dots) \rightarrow \tau$

ограничения на области определения функциональных атрибутов  
(массивы)

**Функции и предикаты на типах**

**Типы агентов:** определяются наборами атрибутов и действий

# Конкретные и символьные модели

## Конкретные модели:

Все атрибуты имеют конкретные значения в состоянии среды и состояниях агентов. Правила переходов **STG** сохраняют это свойство. Постусловие состоит из присваиваний рассматриваемых как формулы темпоральной логики.

## Символьные модели:

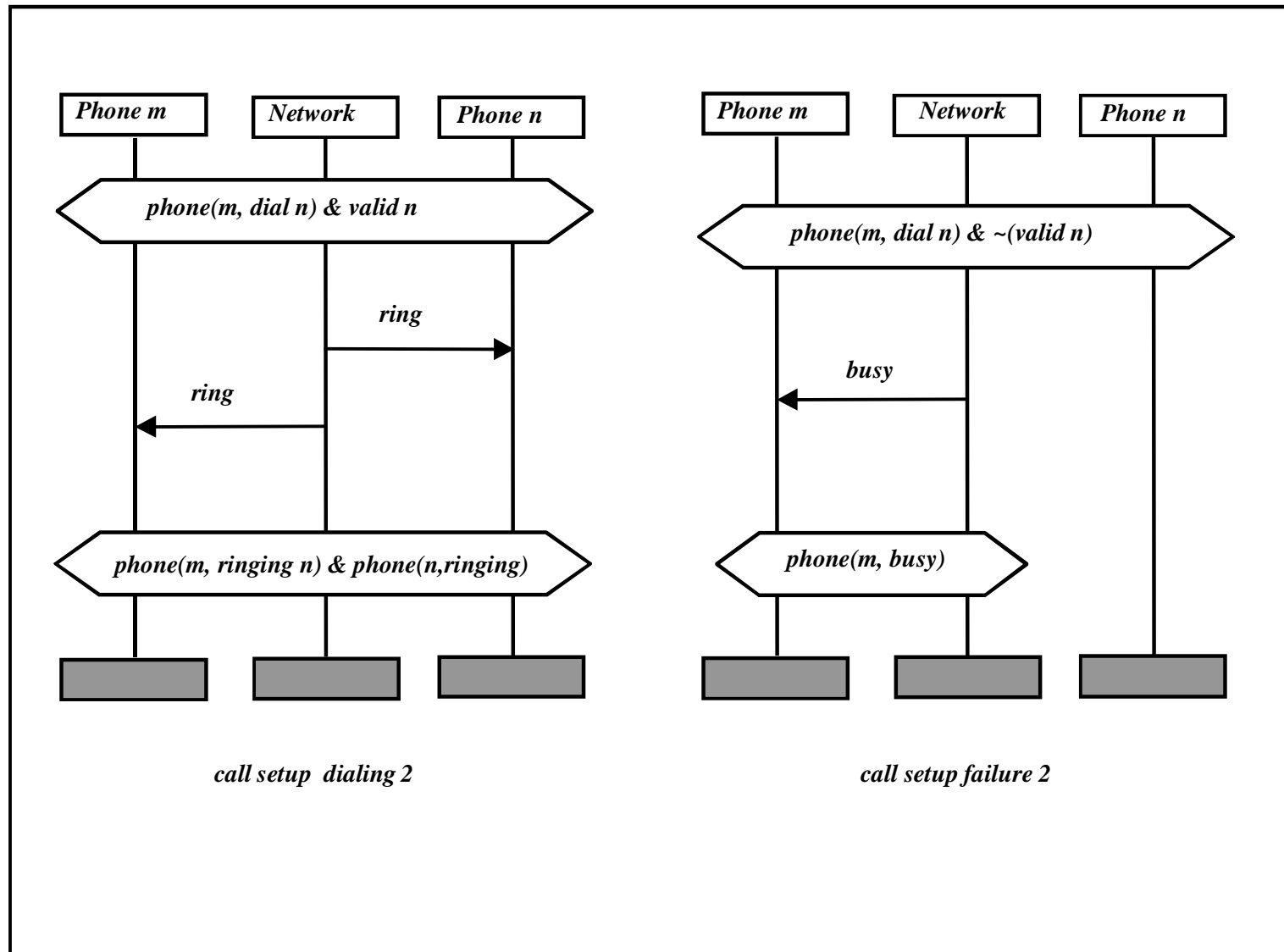
Возможные значения атрибутов среды и атрибутов агентов в состоянии среды определяются формулой исчисления предикатов. Постусловия могут содержать формулы. Правила переходов **STG** определяются с помощью дедуктивной системы.

## Символьное состояние:

Формула покрывает множество конкретных состояний и может быть отождествлена с ним. Статическая проверка требований **SRC** рассматривает предусловия как предположения, а условия целостности как утверждения.



# Еще два протокола



**Аннотированный сценарий**

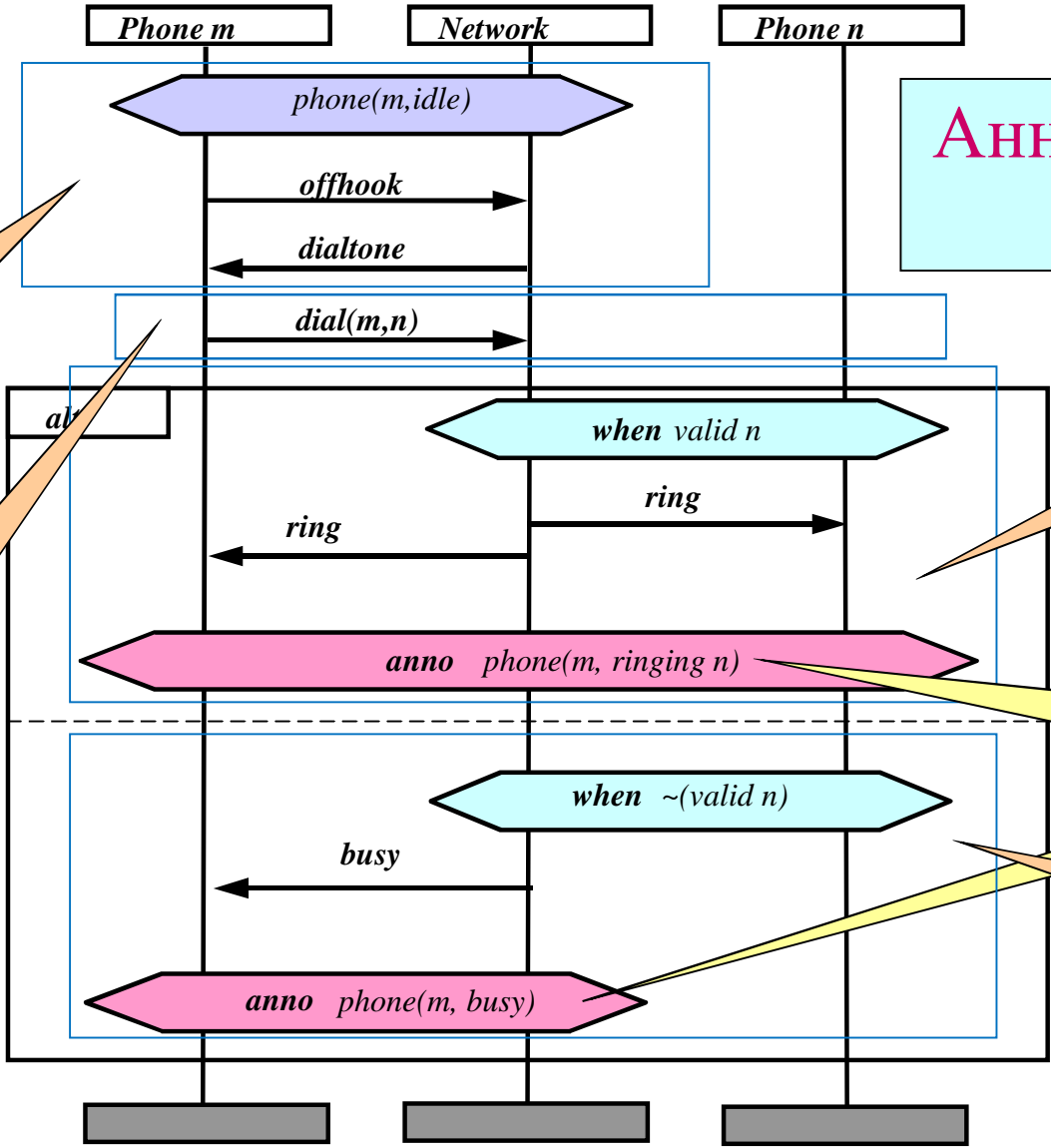
Call setup initial

Call setup dialing 2

Call setup dialing 1

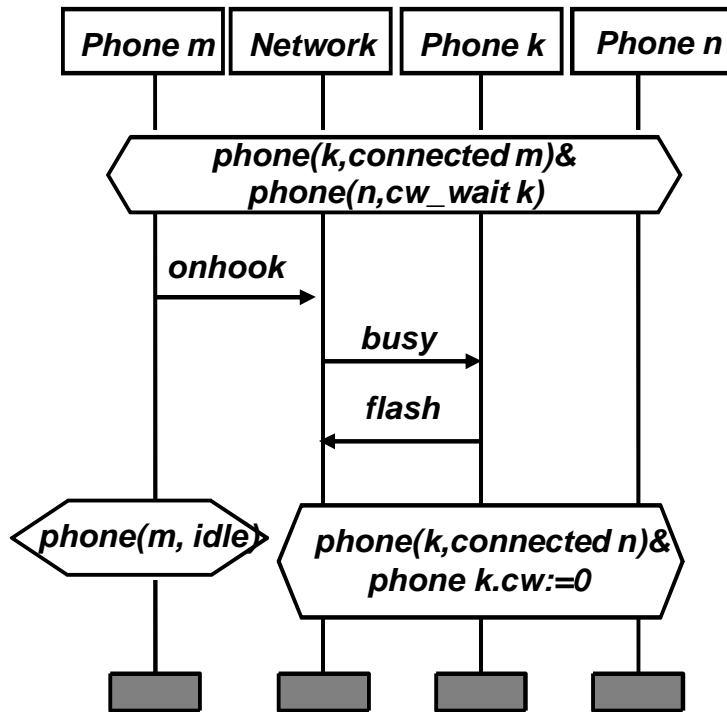
**Аннотации**

Call setup failure 2

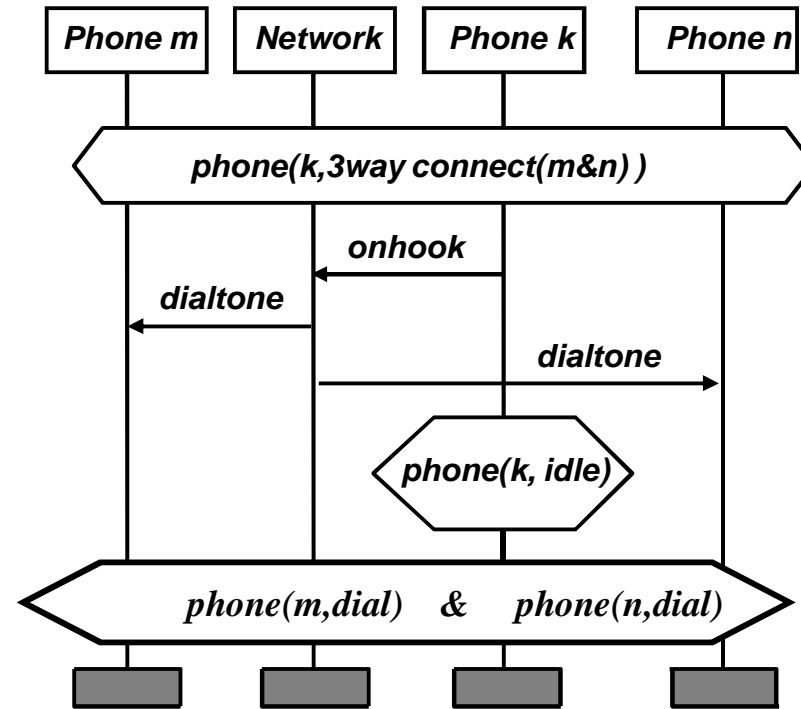


# Противоречивые протоколы

(противоречие функциональностей 3way Calling и Call Waiting)

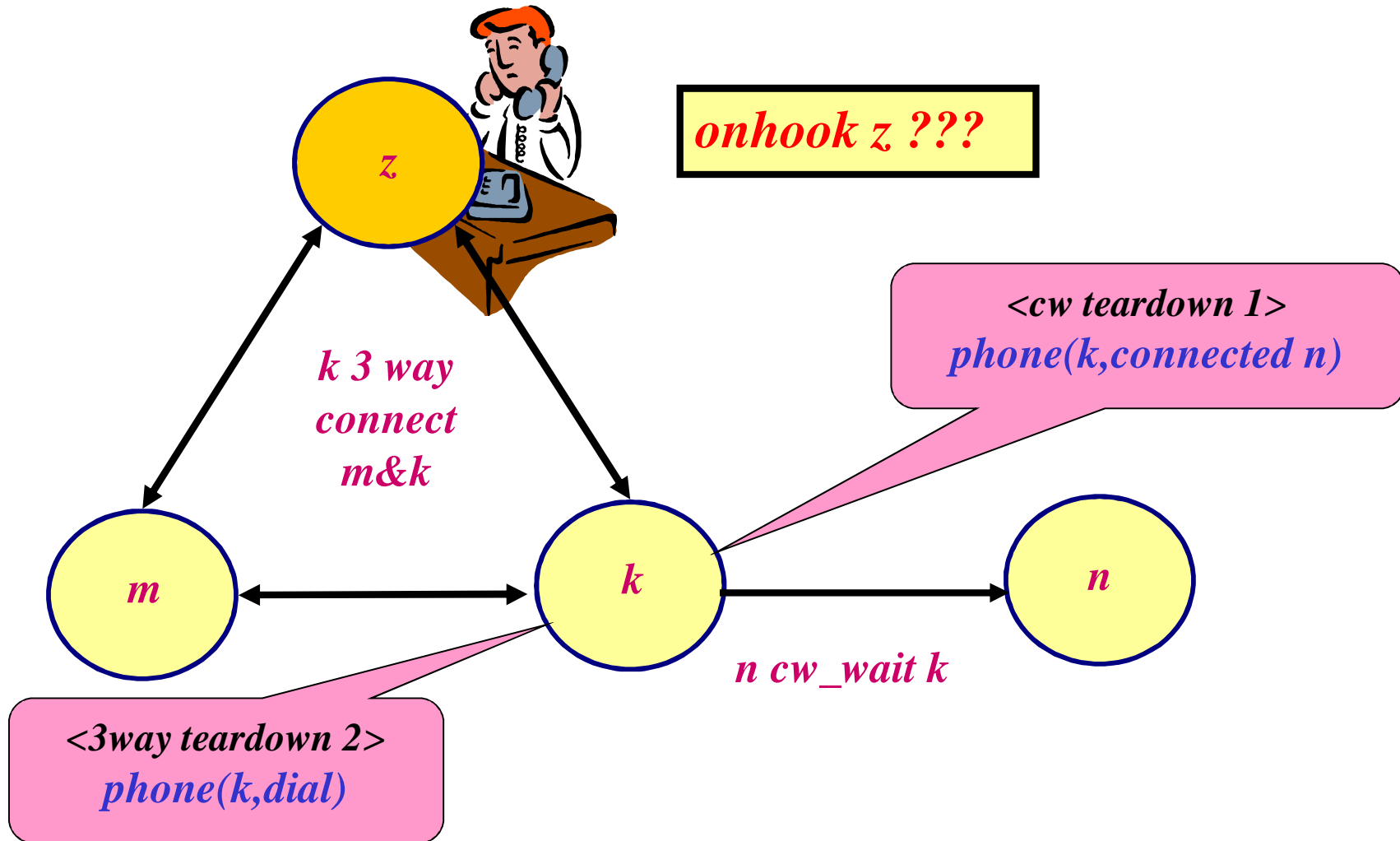


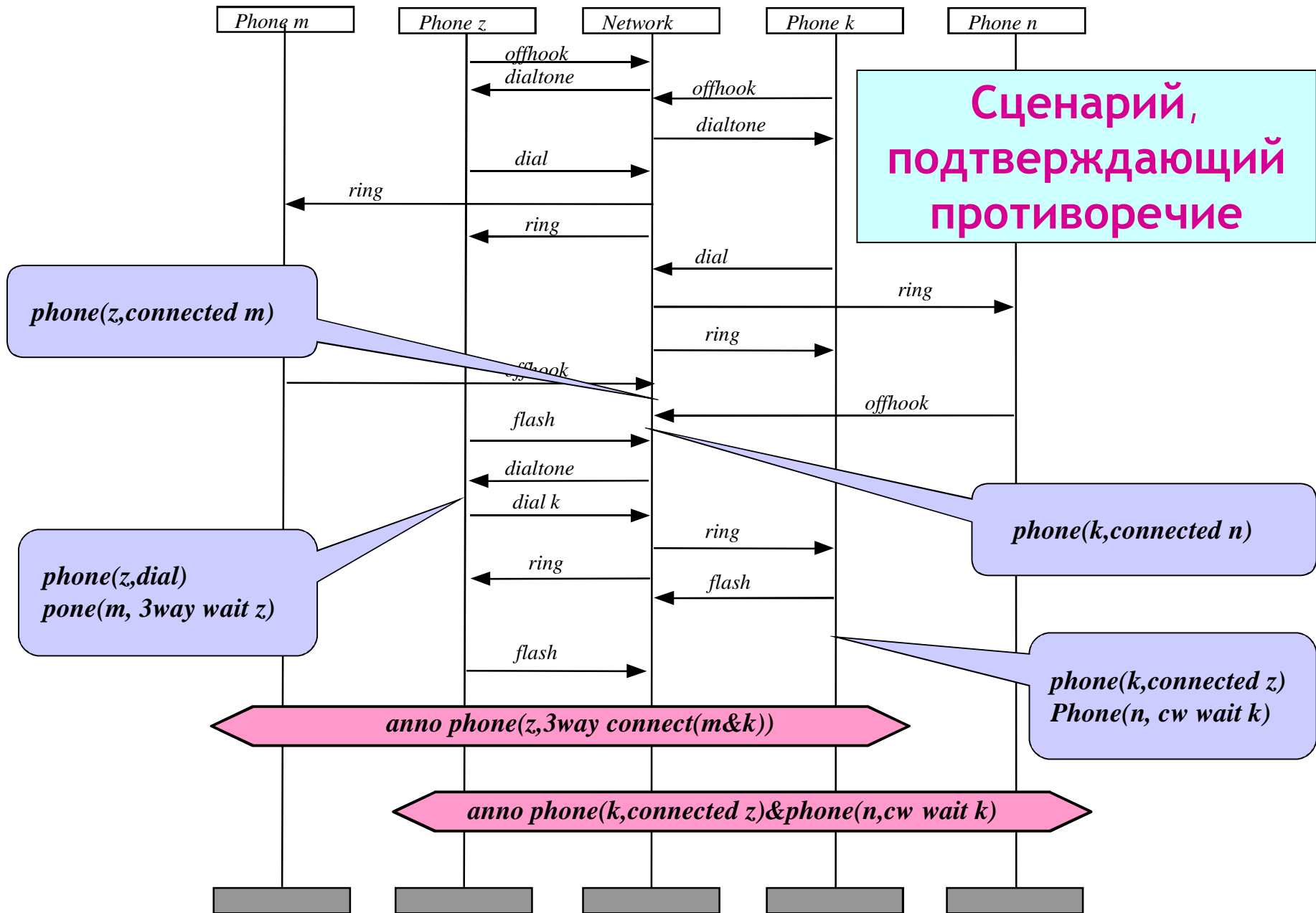
*Protocol cw teardown 1*



*Protocol 3way teardown 2*

# Противоречивое состояние





# Опыт применения системы VRS

**Десятки реальных систем из областей:**

**Телекоммуникации**

**Встроенных систем**

**Систем реального времени**

**Объемы формальных требований**

**Тысячи базовых протоколов**

**Сотни атрибутов**

**Сотни ошибок, найденных в документации.**

**Тысячи тестов, обеспечивающих полное покрытие требований (по заданному критерию).**

**Переход от пилотирования к коммерческому использованию.**

**Motorola => UniqueSoft**

# POTS + features