24 Ноября 2012

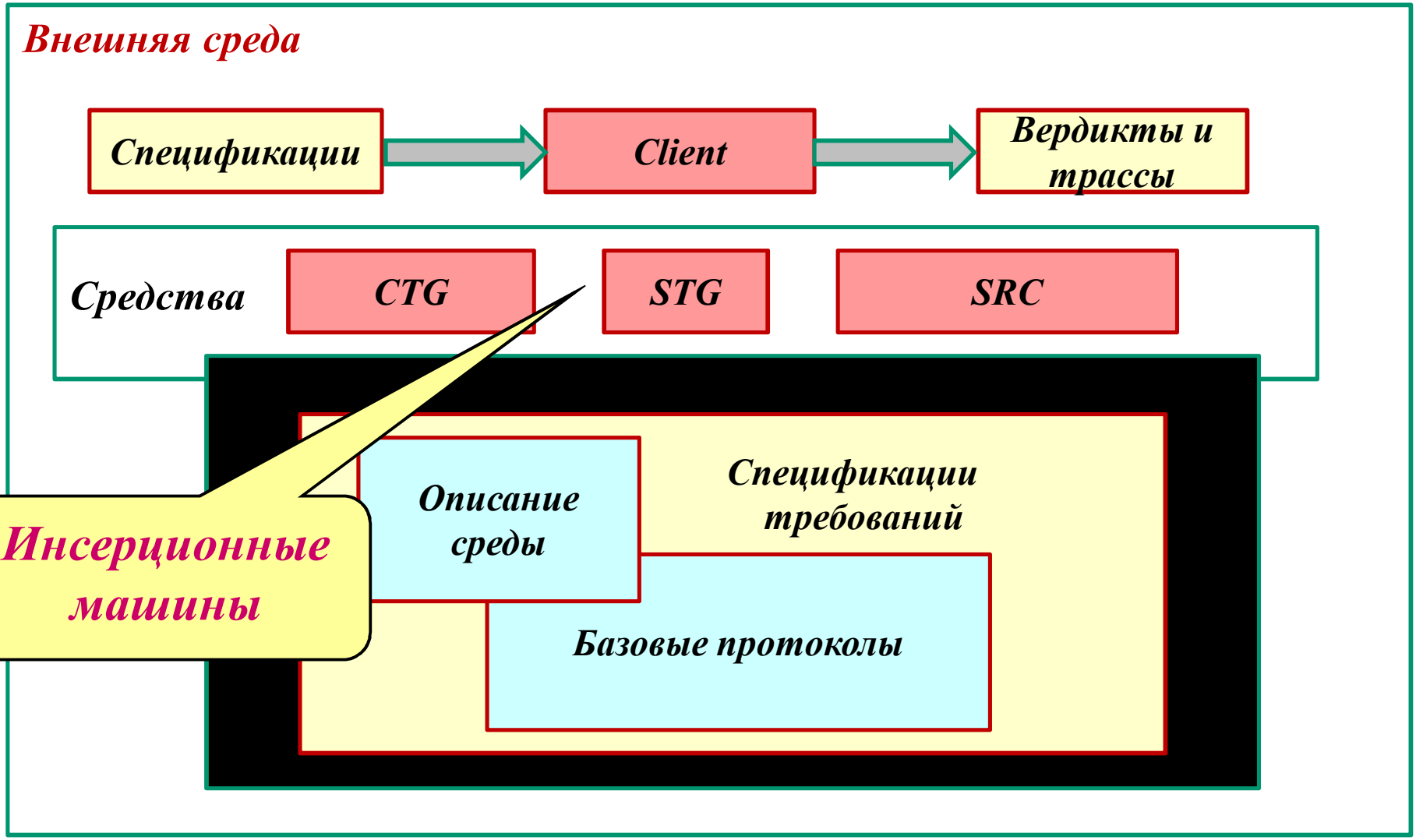
Инсерционное моделирование 1

Лекция 11

Система верификации требований VRS
(Verification of Requirement Specifications)

Система VRS

среда для верификации требований к распределенным программным системам



Средства системы VRS

Формализация требований (Client)

Интерактивная система разработки требований и управления процессом верификации

Статическая проверка требований (SRC)

Доказательство полноты требований

Доказательство непротиворечивости требований

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 смешанных арифметико-логических теориях.

Генерация тестов

Язык формальных требований BPSL

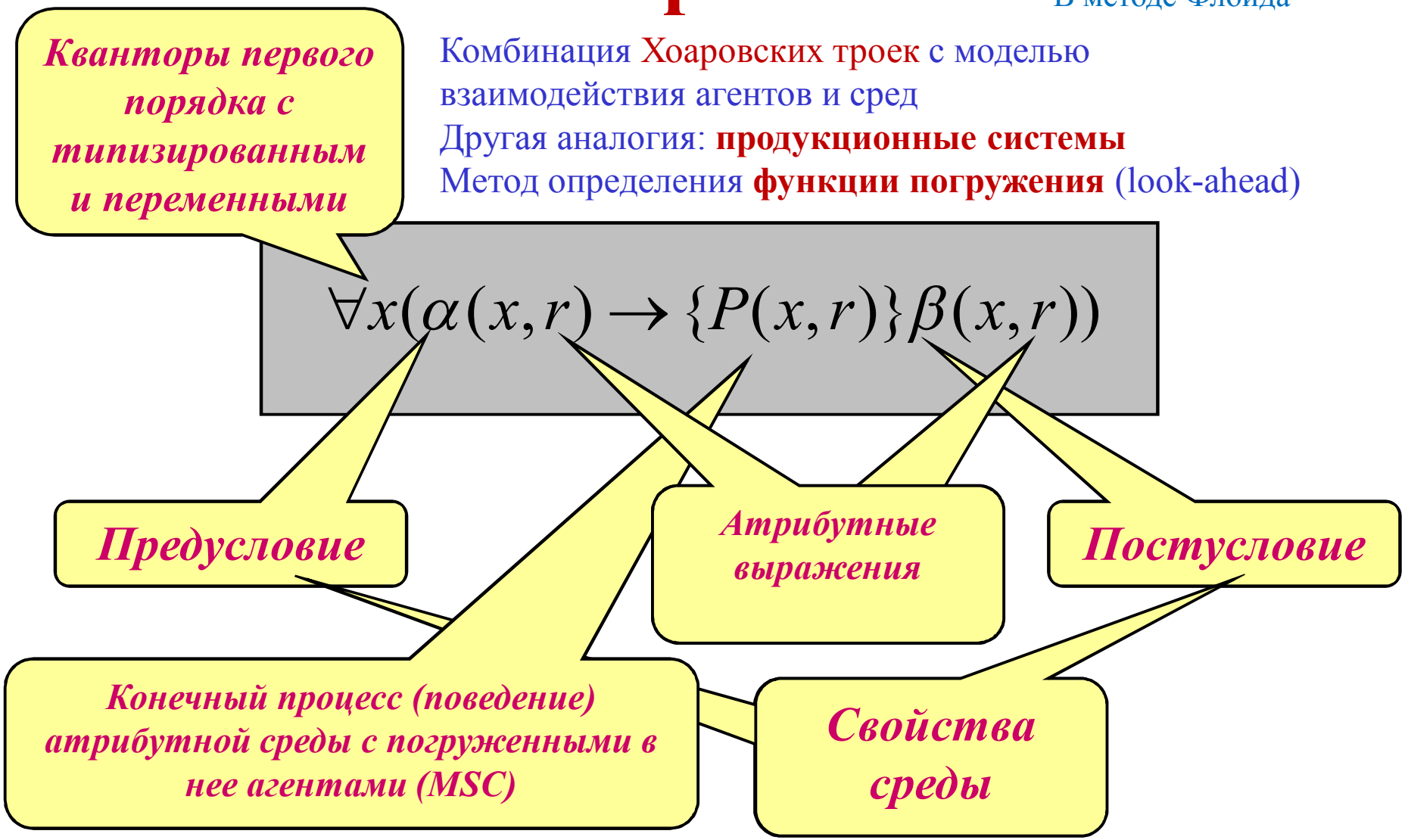
Basic Protocol Specification Language

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

Базовые протоколы

Фрагменты программы
В методе Флойда

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



Атрибутная среда и атрибутные инсерционные машины

Состояние среды определяется наборами значений атрибутов или их свойствами.

Атрибуты: простые и функциональные

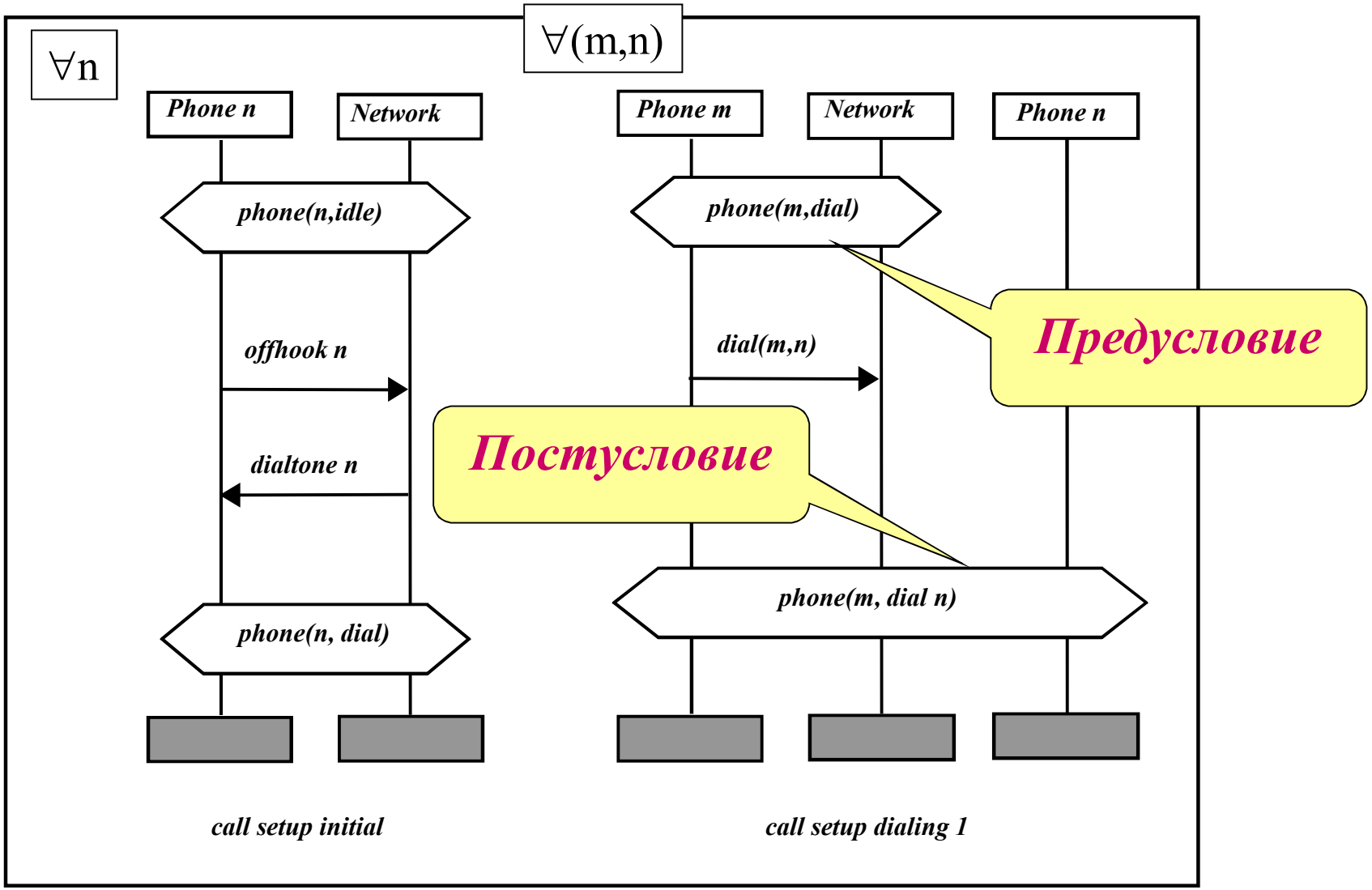
Атрибуты среды и атрибуты агентов

Типы атрибутов:

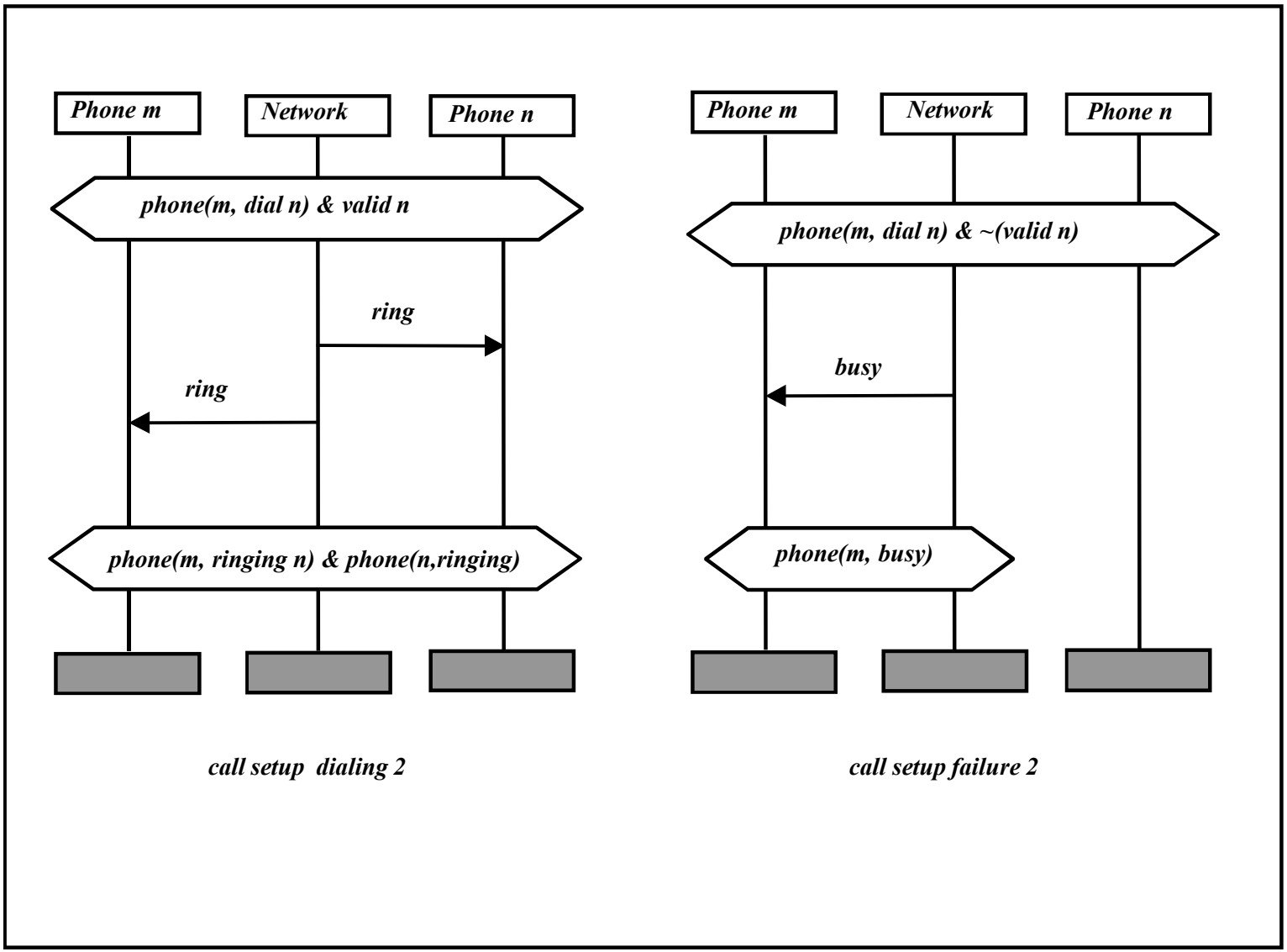
- простые: int, real, Bool, symb, behavior, …
- функциональные: $(\tau_1, \tau_2, ...) \to \tau$
- ограничения на области определения функциональных атрибутов (массивы)

Типы агентов: определяются наборами атрибутов и действий

Два базовых протокола для модели телефонной связи



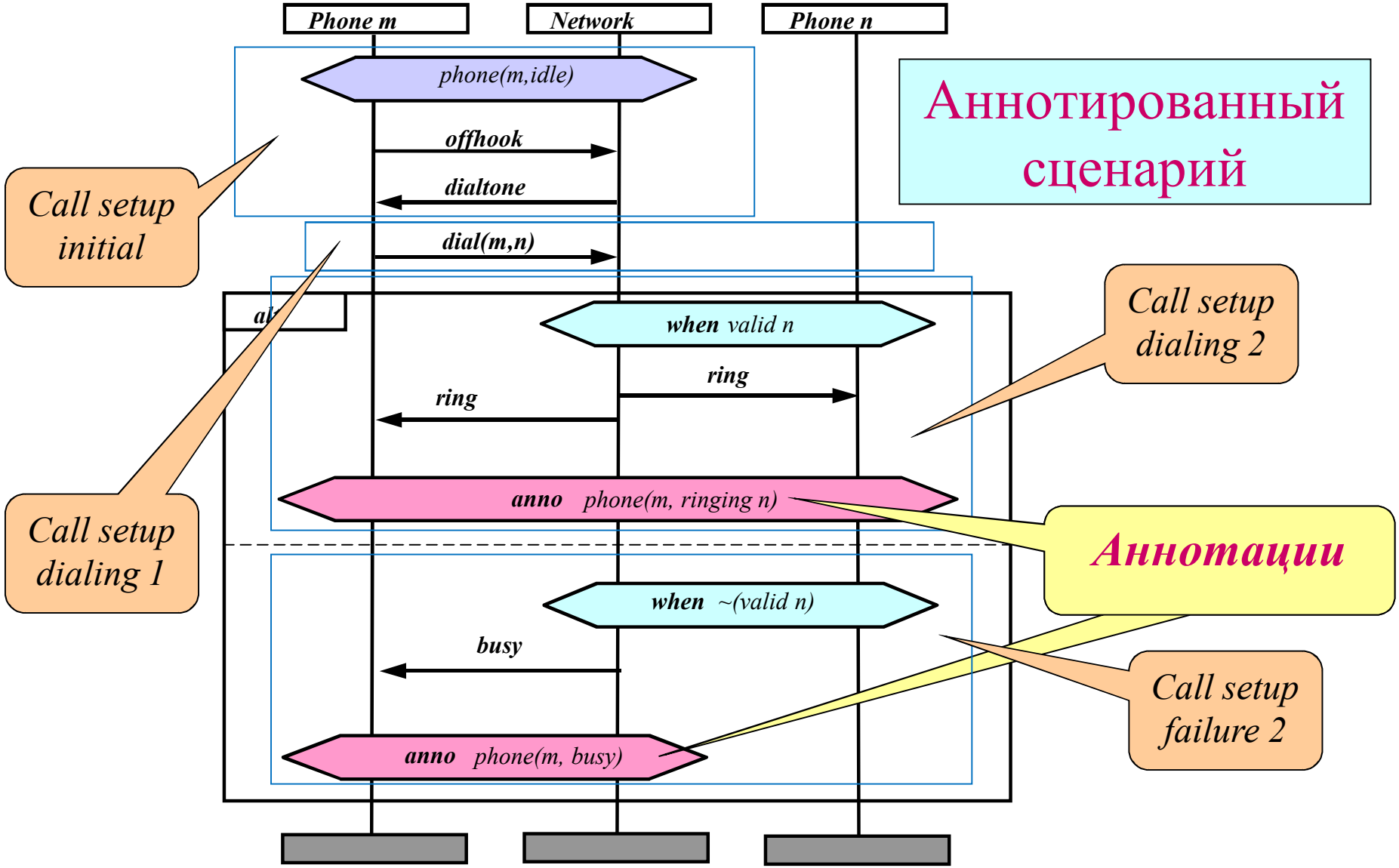
Еще два протокола



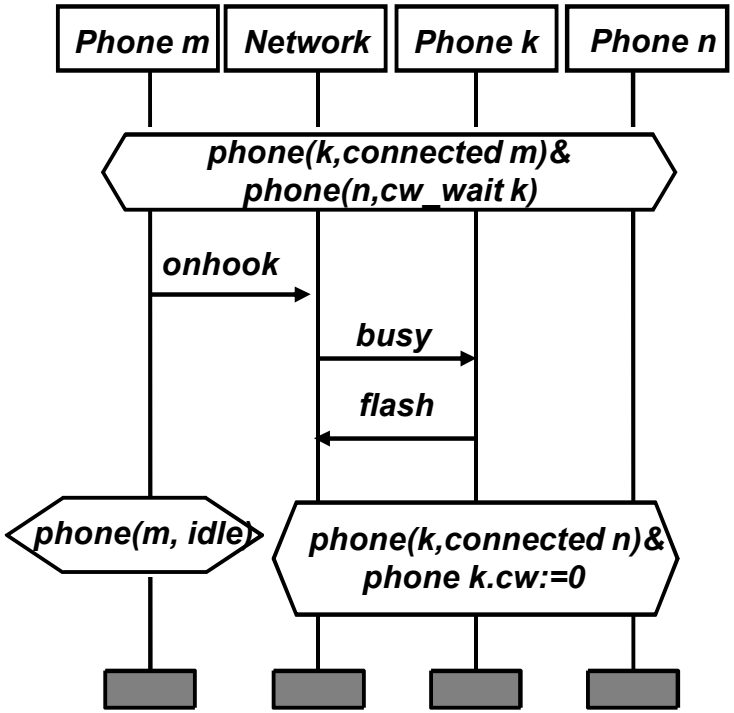
call setup dialing 2

call setup failure 2

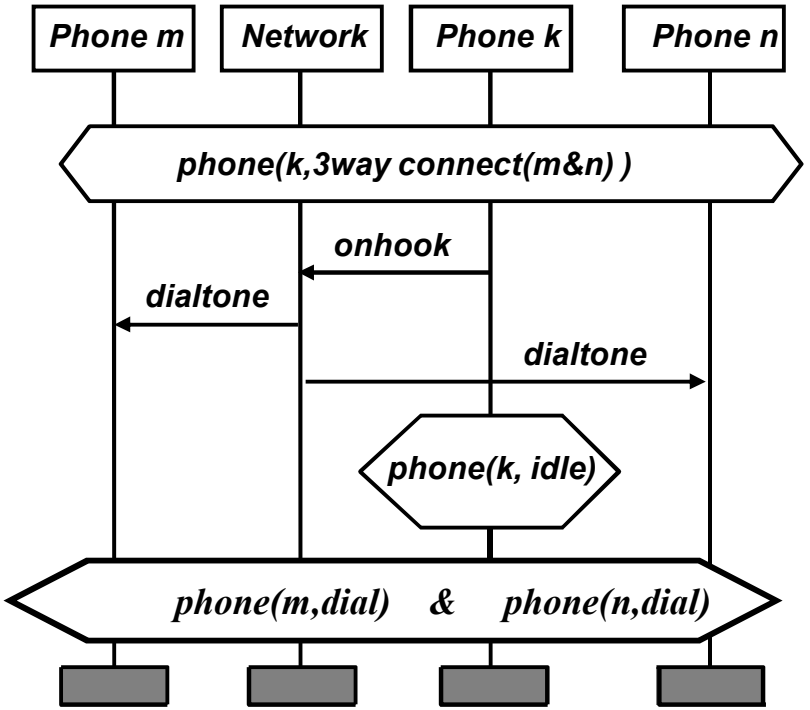
Аннотированный сценарий



Противоречивые протоколы
(противоречие функциональностей 3way Calling и Call Waiting)

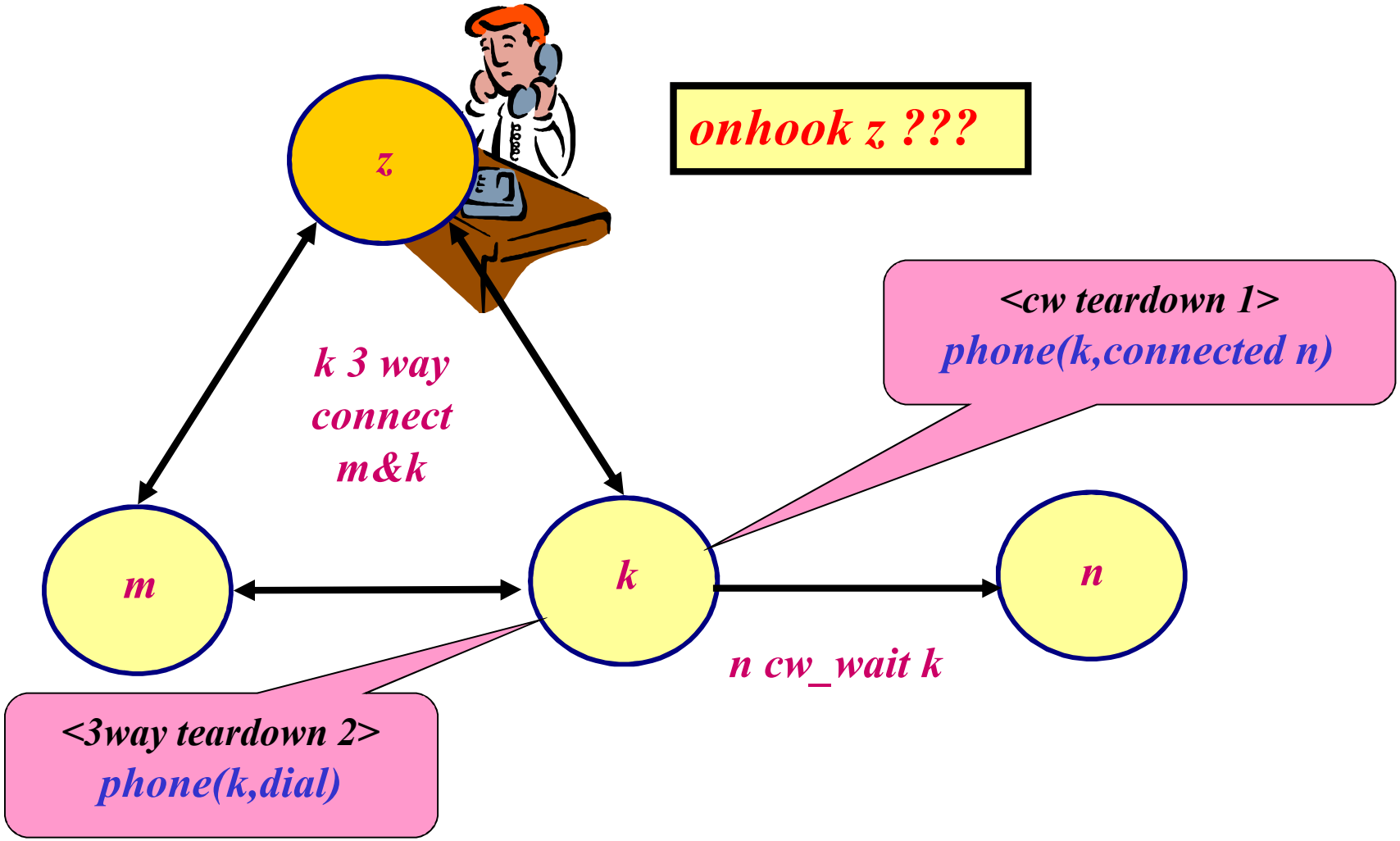


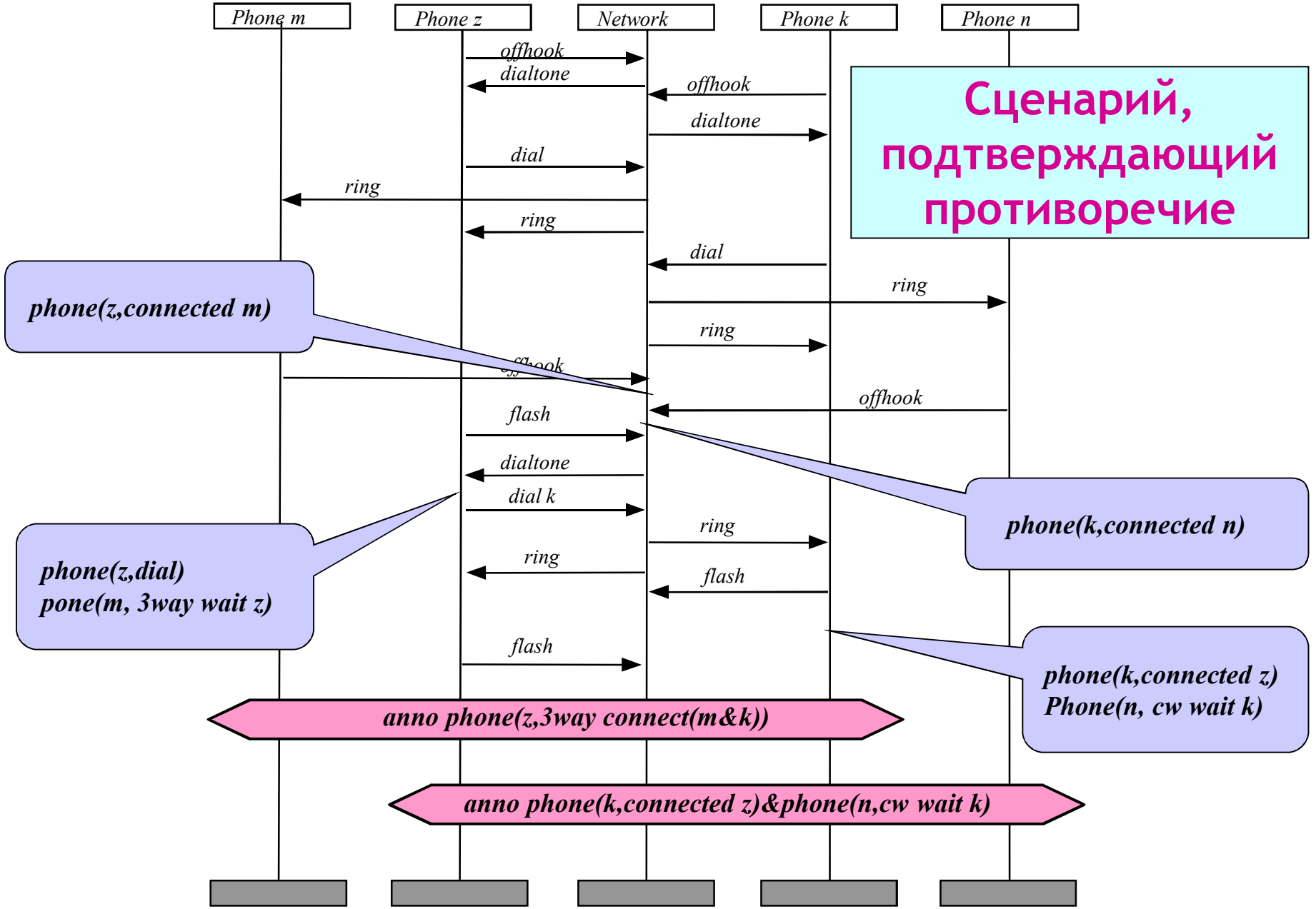
Protocol cw teardown 1



Protocol 3way teardown 2

Противоречивое состояние




Phone m
Phone z
Network
Phone k
Phone n
offhook
dialtone
offhook
dialtone
dial
ring
ring
dial
ring
ring
offhook
flash
dialtone
dial k
ring
ring
flash
flash
anno phone(z,3way connect(m&k))
anno phone(k,connected z)&phone(n,cw wait k)
Сценарий, подтверждающий противоречие
phone(z,connected m)
phone(k,connected n)
phone(z,dial)
pone(m, 3way wait z)
phone(k,connected z)
Phone(n, cw wait k)

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