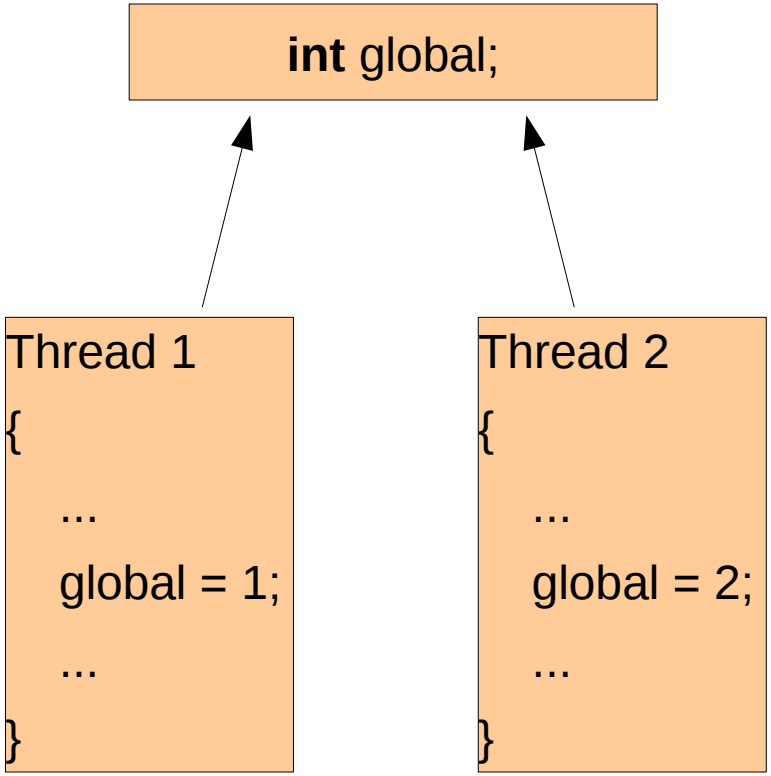
LinuxTesting.org

Конфигурируемый метод поиска состояний гонок в операционных системах с использованием предикатных абстракций

Павел Андрианов, Вадим Мутилин, Алексей Хорошилов
http://linuxtesting.org/project/ldv/

ISP RAS
Institute for System Programming of the Russian Academy of Sciences

Состояние гонки



Ситуация, при которой имеет место одновременный доступ к одной ячейке памяти из нескольких потоков, один из доступов является записью.

Мотивация

- Ошибки, связанные с параллельным выполнением, составляют 20% от всех ошибок в файловых системах ОС Linux (*A Study of Linux File System Evolution*, FAST'13)
- Состояния гонок составляют 17% от всех ошибок в драйверах ОС Linux (Анализ типовых ошибок в драйверах ОС Linux, Труды ИСП РАН)

Алгоритм Lockset

Потенциальным состоянием гонки называется ситуация, в которой доступ к одним и тем же разделяемым данным происходит с непересекающимся множеством блокировок из двух параллельных потоков, при этом одно из обращений является записью.

Состояние гонки

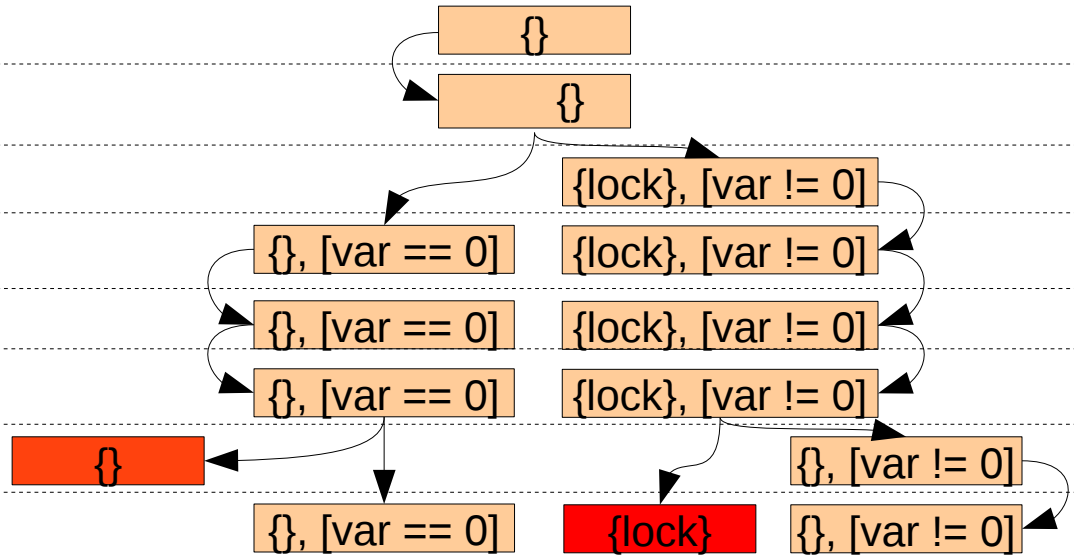
```
...
*a = 1;
...
```

```
...
mutex_lock();
*a = 1;
mutex_unlock();
...
```

- Непересекающийся набор используемых примитивов синхронизации
- Одни и те же разделяемые данные
- Доступ из разных потоков, которые могут выполняться параллельно
- Реальные (достижимые) пути

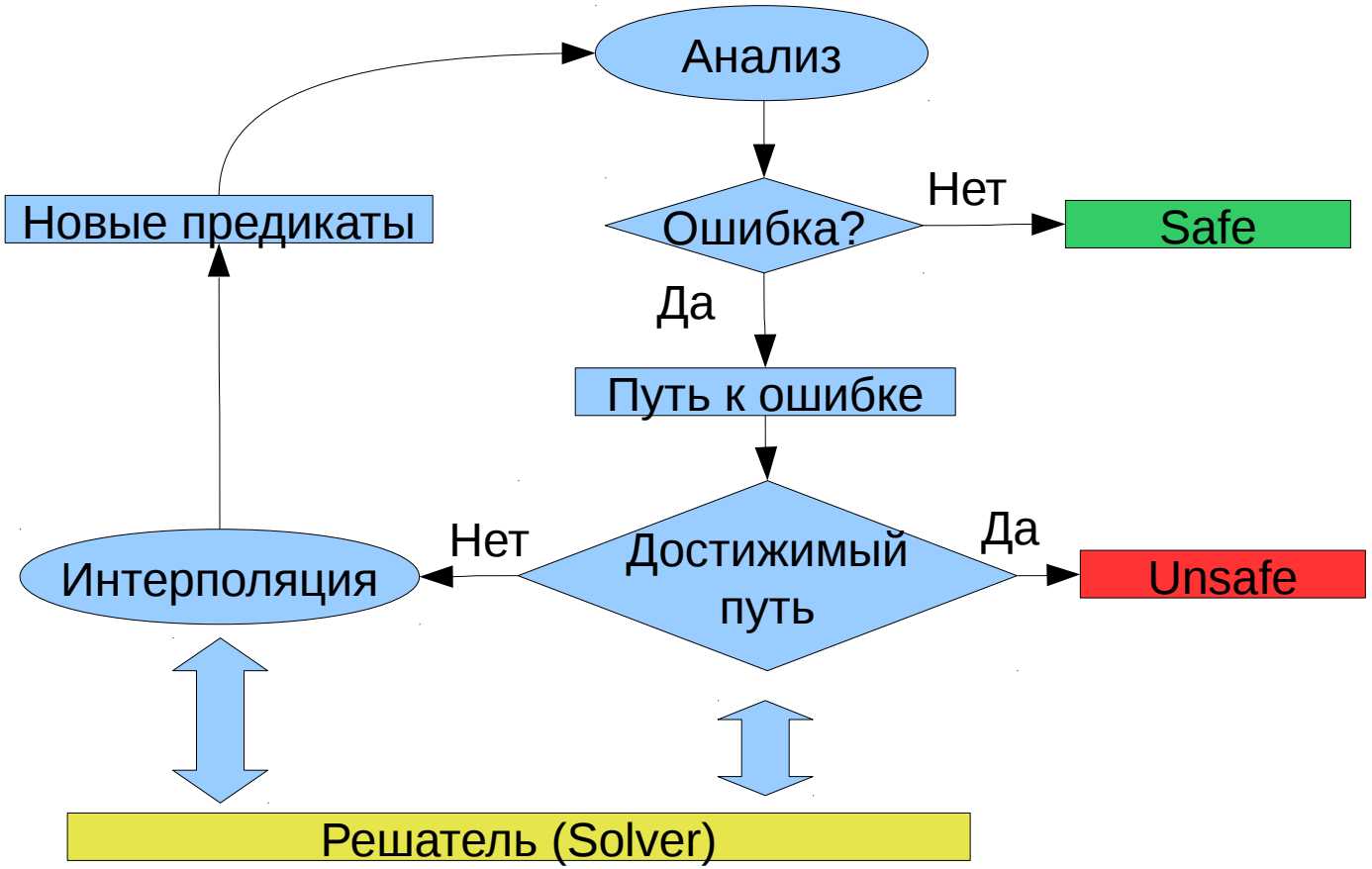
Анализ достижимости
с использованием предикатных абстракций

```
int global;
int func(int var) {
        if (var) {
            lock();
        }
        global++;
        if (var) {
            unlock();
        }
}
```

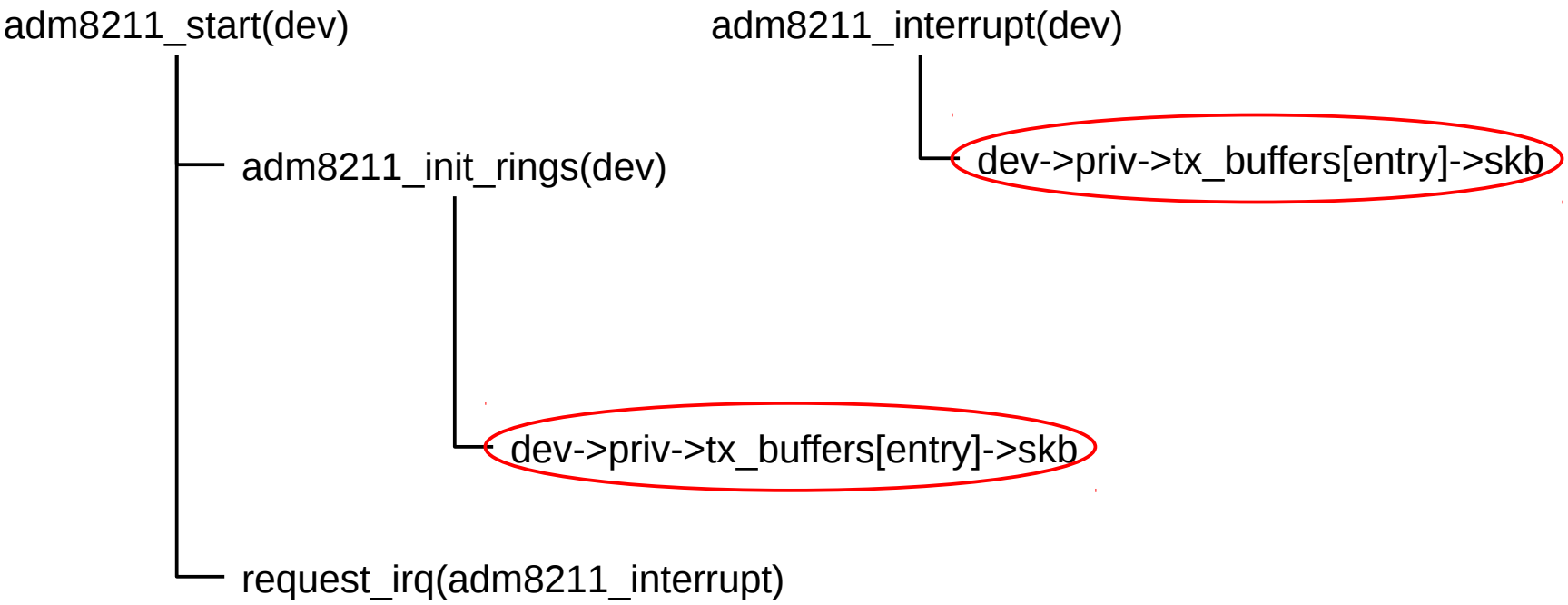


Уточнение

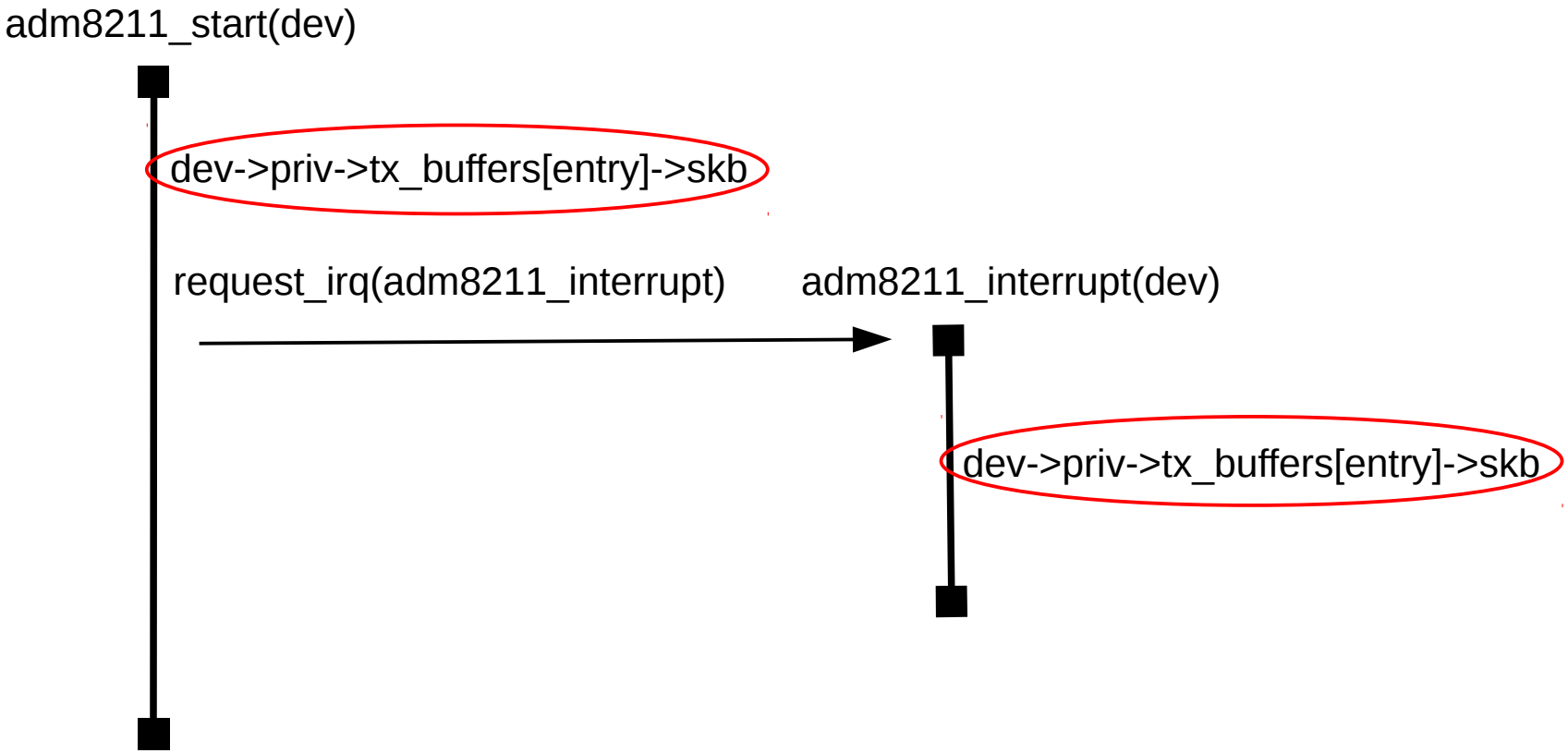
Counter Example Guided Abstraction Refinement



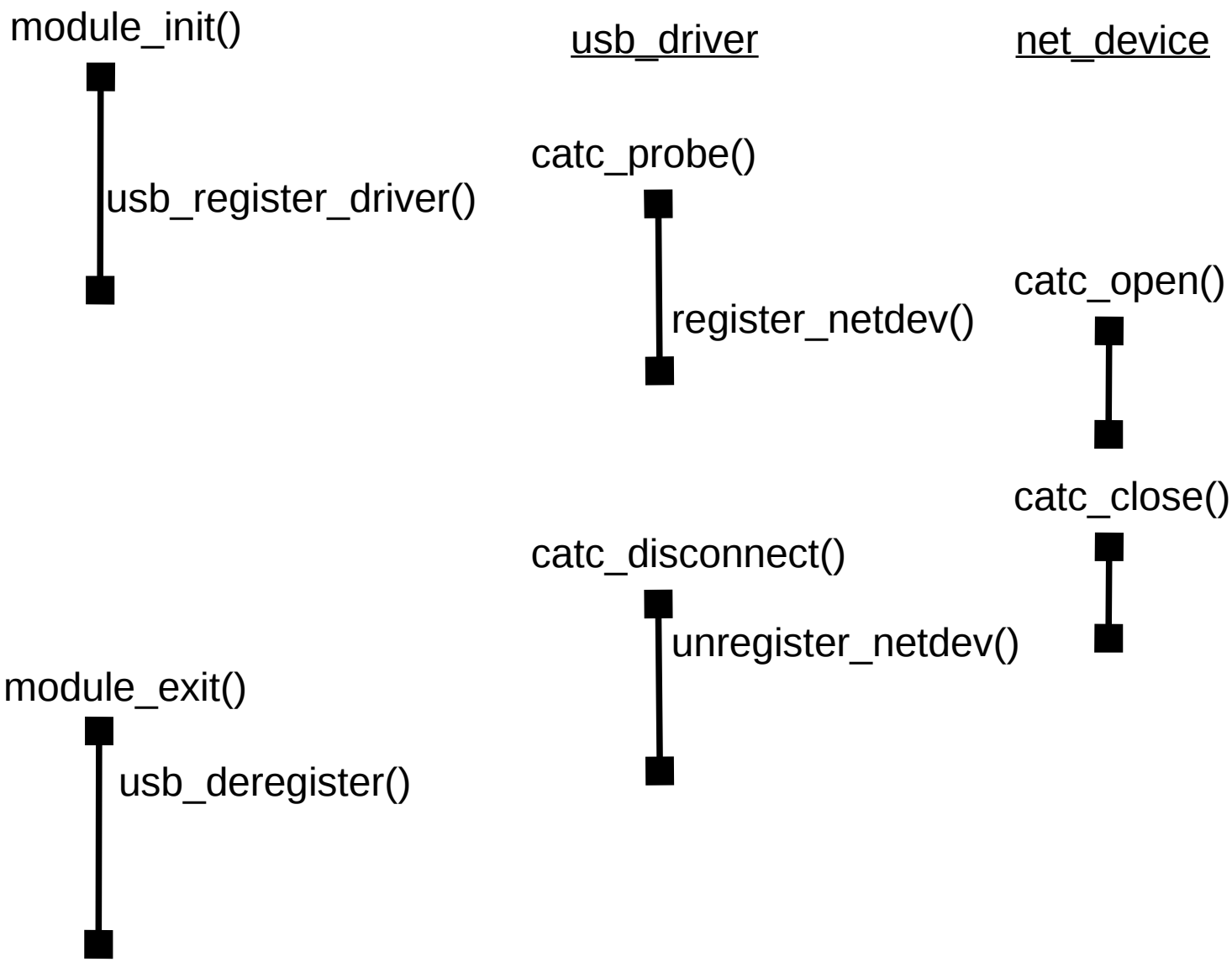
Пример ложного предупреждения



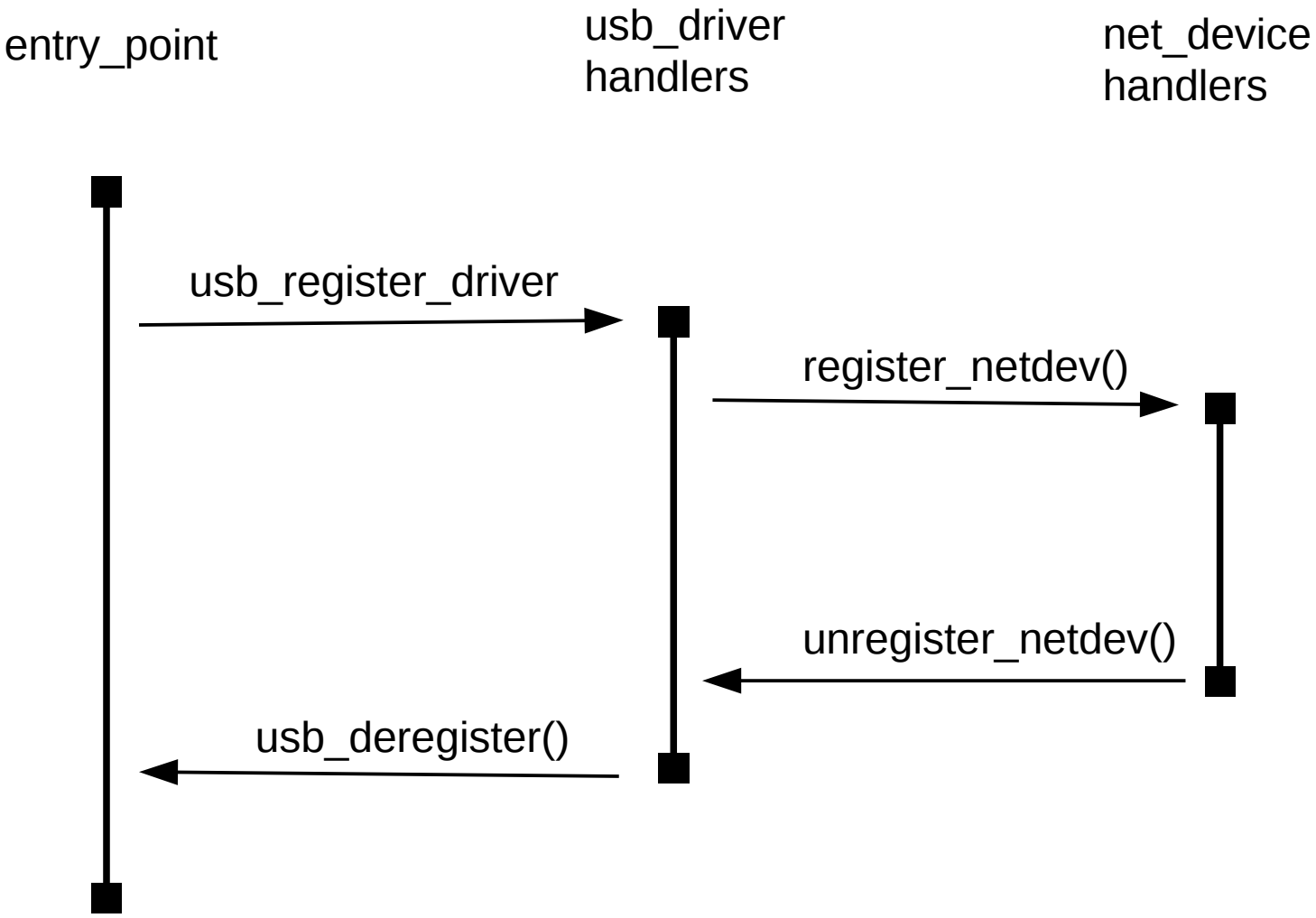
Пример ложного предупреждения



Пример работы драйвера Linux

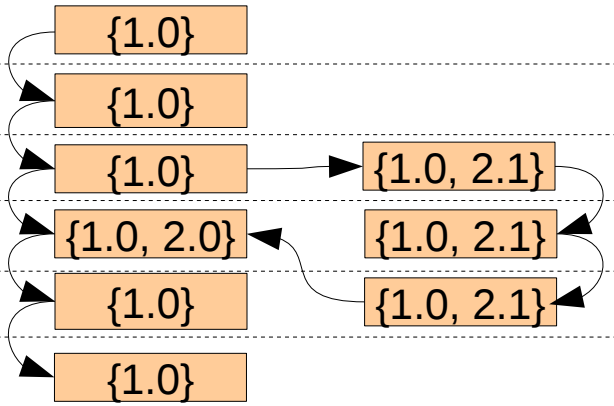


Пример модели



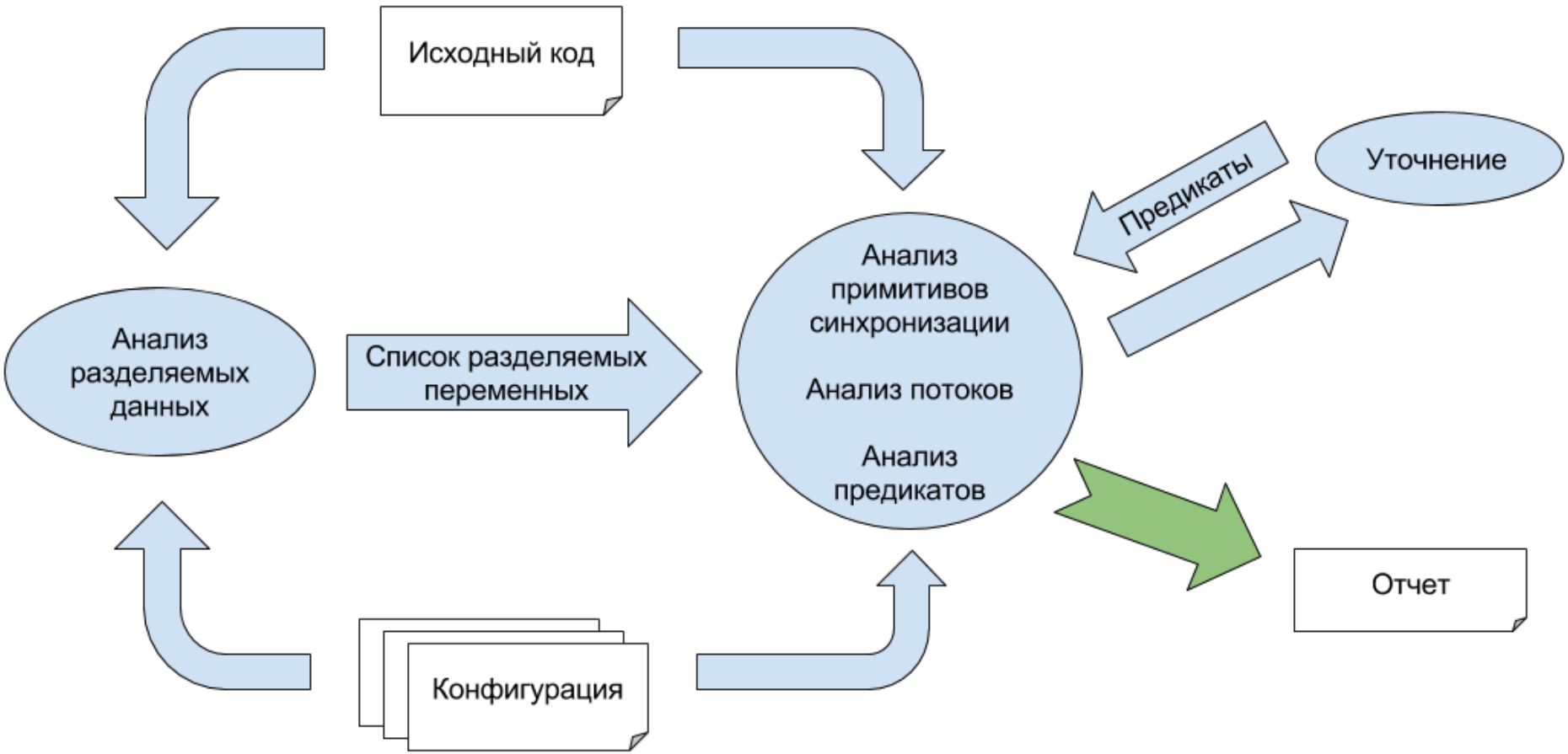
Анализ потоков

```
int global;
Int start() {
    global = 0;
    pthread_create(&thread, .., worker, ..);
    pthread_join(&thread);
    result = global;
}
```




```
int worker() {
        global++;
}
```

Схема метода в общих чертах



Результаты

113 модулей ядра ОС Linux 4.5-rc1 подсистемы drivers/net/wireless

	Предупреж-дения	Незавершен-ный анализ	Корректные модули	Время ч	Память Гб
+ Потоки, + Уточнение	5	61	51	3.2	8.1
- Потоки, + Уточнение	6	67	44	4.1	4.0
+ Потоки, - Уточнение	27	57	49	2.3	8.2
- Потоки, - Уточнение	186	54	43	2.1	3.5

Заключение

- Предложенный легковесный подход допускает гибкую настройку баланса между ресурсами и точностью анализа
- Реализованный метод позволил найти несколько состояний гонки, которые были признаны и исправлены разработчиками

Спасибо за внимание

Вопросы?