Создание критически важных приложений на основе микросервисов.

Журнал: “Открытые системы СУБД” , номер 1, 2017 год.
Издатель: ООО “Россия, 127254, Москва”.

Кристоф Фетцер

Стандартный подход к созданию ответственных приложение для бизнеса и критически важно Инфраструктуры Это подход "снизу вверх ", когда начинаешь надёжного фундамента, выбирая аппаратный архитектуру и системная П О, а поверх него разрабатывают приложение и обеспечивает его безопасное выполнение. Убедиться в надёжности микропрограммного системного ПО помогают формальные методы доказательства корректности микроядерной системы.
Паду правлением Linux, операционной системы с монолитным ядром, сегодня работают многие современные системы устройства: облачные инфраструктуры, смартфоны, автомобильный компьютер и другие устройства, Критичным безопасности встроенного программного обеспечения. Однако доказать корректность работы ОЭС Linux современными формальными методами практически нереально – – если в самом микроядре насчитывается лишь 10 тыс. Строк кода, то для ядра Linux пришлось бы верифицировать более 20 М Л Н строк. Более того, Опыт показал, что Linux всегда содержит: исправим мои ошибки, так что формально доказательство корректности в любом случае даст отрицательный результат. Статистический анализ Репозиториев открытого кода обычно выявляет в среднем ноль,61 дефекта на 1000 строк, и, несмотря на постоянное проводимость правления, число не устраненных ошибок в едре остается на уровне примерно 5000 правда не все Могут использоваться для проведения так. Другое исследование показало что за последние пять лет в Linux было исправлено около 500 ошибок, связанных с нарушением безопасности, и не присутствовали в едре в течение пяти лет. В проприетарном коде плотность дефектов несколько выше, Чем в открытых проектах, а значит коммерческое по тоже не застрахован отличие уязвимостей.