Космический багхантинг

Алексей Федулаев
DevSecOps Lead
Wildberries
@int0x80h

Андрей Моисеев
DevSecOps
Bimeister
@not_s0_s3c

$whoarewe

12+ лет в ИБ

Астролог гуру

Руководитель направления автоматизации безопасной разработки

Wildberries

$whoarewe

5 лет в ИБ

Астролог подмастерье

DevSecOps в продуктовой IT-компании

Bimeister — Разработка, инжиниринг и внедрение инновационных цифровых решений для промышленности

О чем мы поговорим сегодня

- Космические путешествия
- Какие опасности поджидают нас в космосе
- Какие механизмы должны предусматриваться в космических аппаратах
- Как их протестировать и на что обратить внимание

Космос это

- Опасная
- Агрессивная
- Неизвестная среда

Сложности среды

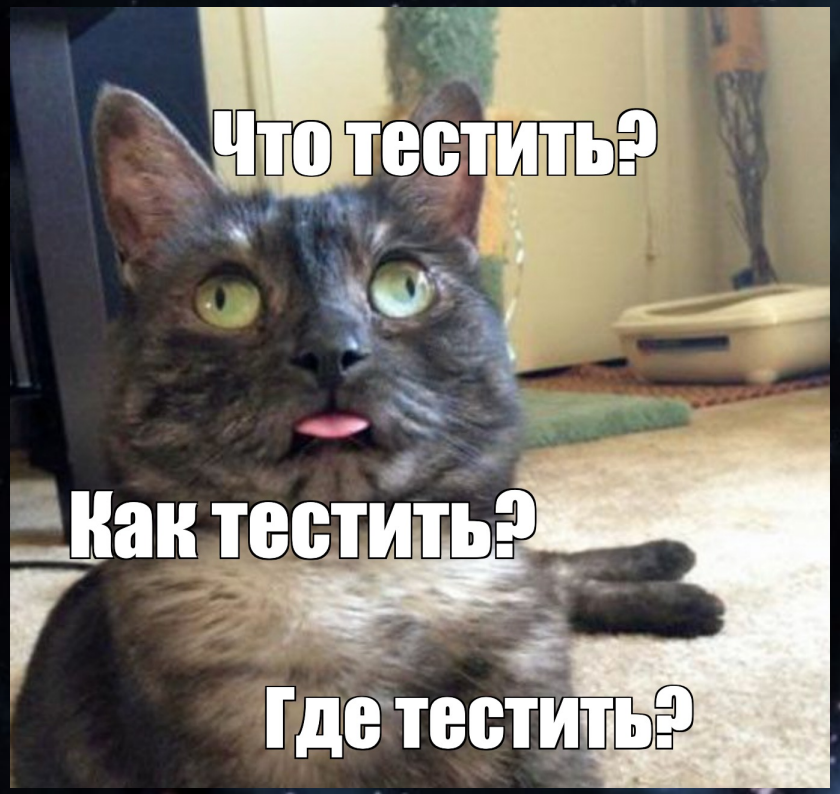
- Сложно дослать аппаратные модули
- Можно дослать патчи, но скорость распространения волн конечна
- Невозможно отремонтировать при сбое
- Цена ошибки слишком высока

Космос непредсказуем

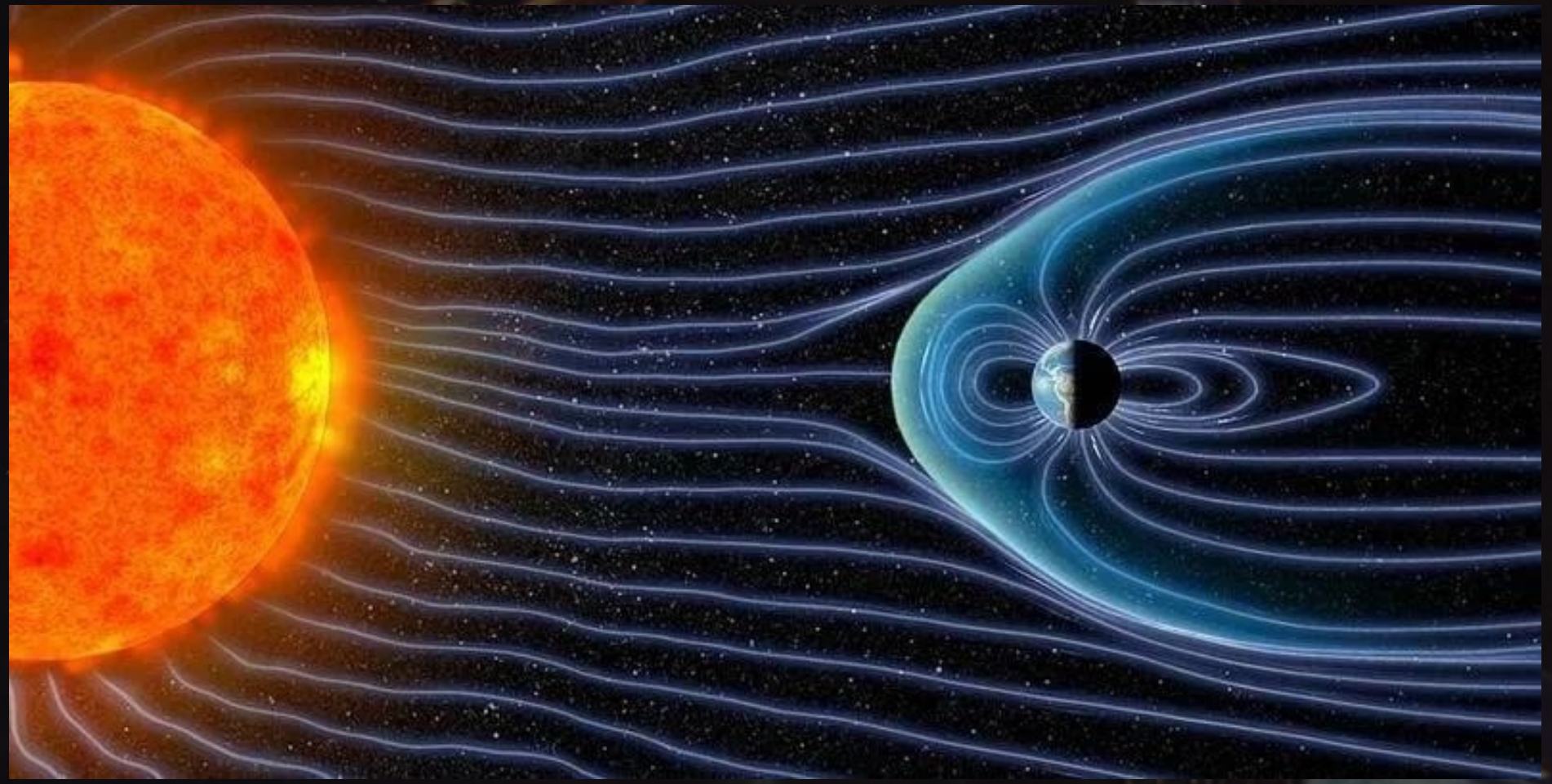
- Геомагнитная буря уничтожила 40 спутников Starlink
- Бури могут спровоцировать отказы спутниковой навигации
- Может прерваться высокочастотная радиосвязь

Ограничения

- Можно воспроизвести только приближенные условия
- Зачастую мы не знаем чего ожидать
- Тесты напоминают отладку на проде
- Часть проблем невозможно предсказать
- А некоторые вообще не известны



Солнечный ветер



Что может выйти из строя?

- Система навигации
- Система связи
- Система обработки результатов
- Система контроля корректности работы
- Система регистрации событий
- Система опроса состояний подсистем
- …

Особенность покрытия тестами

- Железо уже давно самостоятельно выполняет низкоуровневые проверки
- Как правило повторно их не проводят
- Но в условиях когда стоимость ошибки велика это должно быть обязательной частью тестов

Ошибки arithmetic logic unit

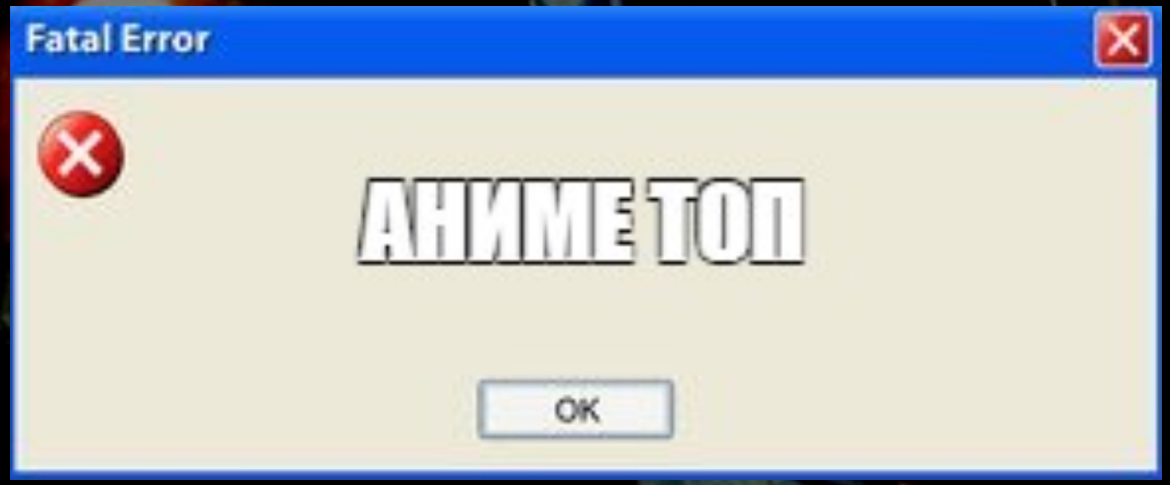
Могут провоцировать

- Неверное вычисление траектории движения
- Преждевременное отключение устройств
- Не срабатывание контролей, блокировок, смены режима работы

Ошибки random access memory

Могут провоцировать

- Некорректную работу программ
- Возникновение непредсказуемых ситуаций при считывании или записи искаженных данных



Особенности тестирования

- JTAG всему голова
- Все проверки только в реальном времени
- Все проверки на боевых образцах

Важный момент

Необходимо подтвердить

- Наличие проверки
- Факт обнаружения аномалий
- Факт корректной обработки аномалий
- Корректность восстановления

Базис тестов

- Блокировки вышедших из строя юнитов
- Блокировки подсистем работы с данными при получении некорректных данных
- Переход в «спящий режим» после блокировки
- Выход из спящего режима
- Корректность восстановления всех систем и их самоконтроль

А что с температурой в космосе

- Космос – место экстремальных температур
- Привычные способы термоконтроля не работают

А что с температурой в космосе

- Все мы знаем что средняя температура в космосе -270,45°C
- Проблемы нагрева или охлаждения не решаются привычными методами
- А перед запуском, все нужно проверить на Земле

Как протестировать?

Все гораздо сложнее

- Охлаждение возможно только излучением в инфракрасном диапазоне
- Температура на МКС колеблется от −157°C до +121°C
- Температура на поверхности меркурия колеблется от −190°C до +430°C
- В некоторых случаях может потребоваться активное охлаждение

Перегрев может повредить приборы

- Изменение температуры влияет на показания приборов
- Реагировать необходимо незамедлительно
- Нужен термостат который отключит часть систем или приборов
- Следовательно надо проверить его корретность

Проверки Джеймса Уэбба

- 10 июля 2017 года — начало финального испытания телескопа на воздействие криогенных температур со значением -236°C
- 30 мая 2019 в специальной вакуумной камере подвергались воздействию температуры от −148°C до +102°C. Во время испытаний для охлаждения использовался жидкий азот, а для нагрева — термобатареи

Поговорим о темной стороне луны

Поговорим о темной стороне луны

- Ночь на луне длится 354 часа
- Активная элементы не могут поддерживать работоспособность в течении такого количества времени без солнечной энергии
- У техники должна быть возможность перерыва (сна)
- При этом требуется поддерживать работоспособность отдельных систем, экономя на других

Интересные кейсы

- 25 января 2013 года из-за высокой радиации произошел сбой систем лунохода «Юйту», из-за чего не удалось перевести его в спящий режим перед наступлением темноты

Интересные кейсы

- Грунт луны имеет абразивную структуру и хорошо поглощает свет
- Солнечные батареи и радиатор охлаждения Лунохода-2 засыпало лунной пылью, это привело к недопустимому росту температуры и уменьшению тока зарядки аккумуляторов, как следствие он не смог пережить следующую лунную ночь
- Во время миссии «Аполлон» астронавты обнаружили, что лунный грунт прилипает ко всему из-за статического электричества и буквально «проедал» скафандры и контейнеры

Важно помнить

- Устройства имеют свой диапазон допустимого напряжения
- При превышении порога, рассыпуха может просто сгореть
- При работе на напряжении ниже порога – могут возникать аномалии
- Основной источник энергии в космосе – солнце
- Чтобы компенсировать недостаток энергии ночью применяют аккумуляторы либо ядерные источники энергии

Базис тестов

- Корректность отслеживания уровней напряжения на всех «умных» элементах устройства
- Блокировка при выходе за допустимые диапазоны
- Если используются резервные механизмы – корректность их включения выключения

Восстановление после сбоев

- Некоторые приборы и подсистемы должны отключаться на время, чтобы оставаться в рабочем состоянии
- Их необходимо отключать во время помех, при перегреве или переохлаждении, либо для экономии энергии для других важных систем
- Должна быть отдельная подсистема контроля состояния других подсистем

Базис тестов

- Корректность реакции датчиков на внешние воздействия
- Возможность отправки датчиками своих состояний в подсистему контроля
- Возможность отправки подсистемами своих состояний в подсистему контроля
- Включение/отключение всех подсистем при получении сигналов от датчиков
- Наличие самоконтроля состояния

Стоит помнить

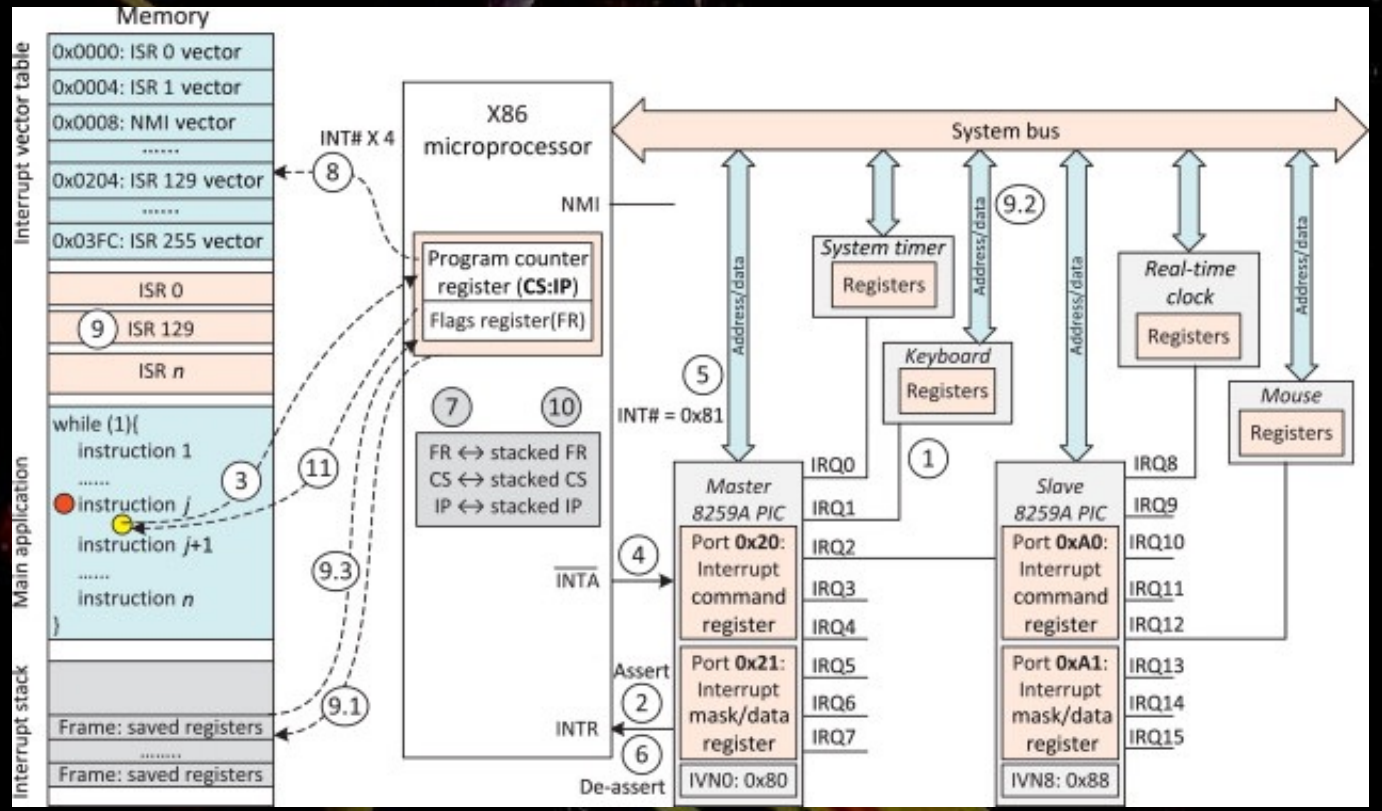
- Размещая все системы на одном кристалле мы получаем сильную точку отказа
- Для обеспечения отказоустойчивости может потребоваться дублирование процессоров
- Проверки должны быть выполнены для всех аппаратных модулей

Соединяем все вместе

- Подсистема термоконтроля
- Подсистема контроля питания
- Подсистема безопасности
- Подсистема восстановления после сбоев
- Подсистема управления

Где-то могут использоваться самописные ОС

- Вектора прерываний
- Центральный узел управления
- Критерии важности



Тестируем взаимодействие между контроллерами

- Асинхронные взаимодействия
- Команды от разных контроллеров выполняются в нужном порядке, с корректным приоритетом внутри главного контроллера

Timeout ответов

- Любая система может зависнуть, выпасть в ошибку, на эти события необходимо незамедлительно реагировать

Timeout ответов

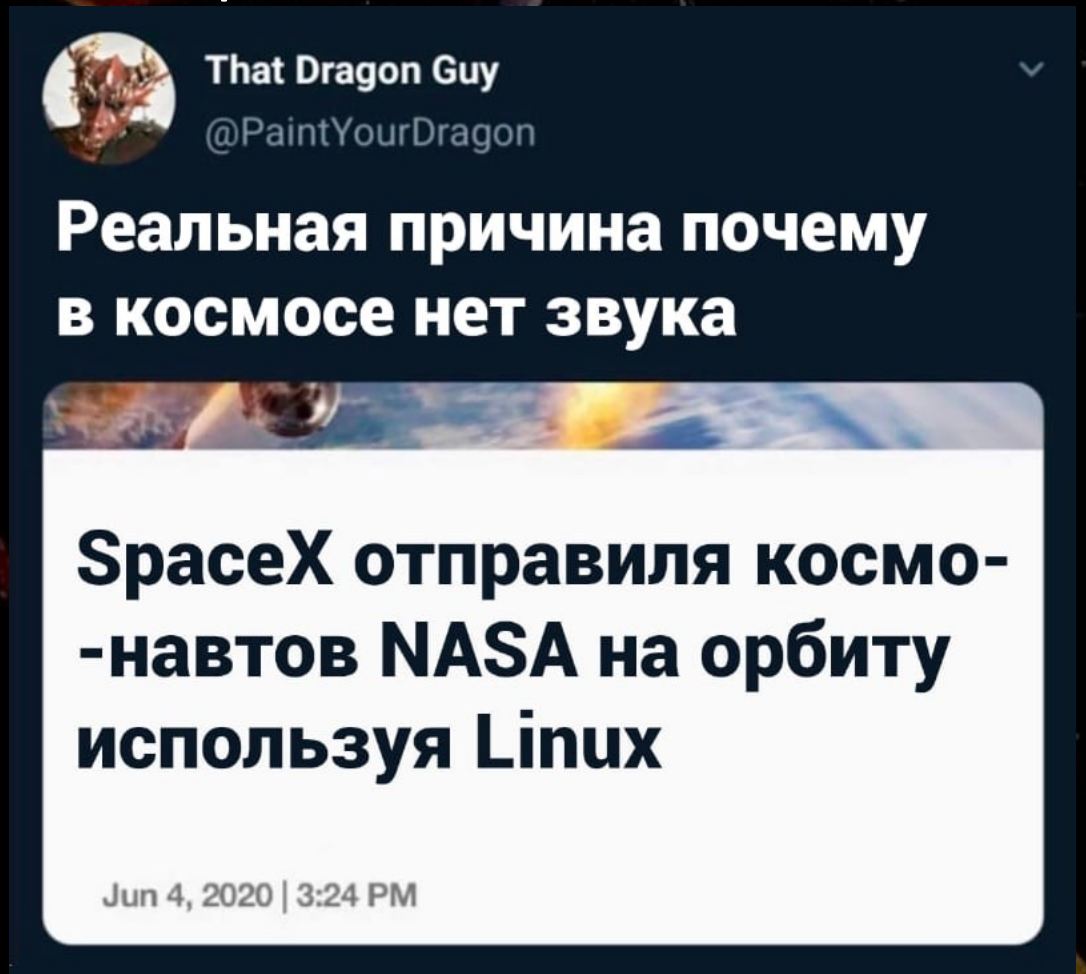
- Любая система может зависнуть, выпасть в ошибку, на эти события необходимо незамедлительно реагировать
- Иногда может помочь простой перезапуск систем

Теперь немного сложнее

- Во всю отправляются в космос аппараты
- Под управлением Linux

Теперь немного сложнее

- Во всю отправляются в космос аппараты
- Под управлением Linux



Усложняем еще: Real-time OS

- OS с жестким квотированием ресурсов
- Процессорное время, ресурсы памяти
- Все ресурсы должны выдаваться на определенные квоты времени
- Все вышеперечисленное должно выполняться без задержек
- Подвисание произвольной подсистемы опасно потенциальной утерей аппарата

А тестить еще сложнее

- Если наша RTOS зависнет, то аппарат превратится в «кирпич»
- Для контроля времени отклика применяют аппаратные таймеры

Необходимо проверять:

- корректность выделения квот времени
- корректность работы аппаратных таймеров
- корректность механизмов восстановления при зависании

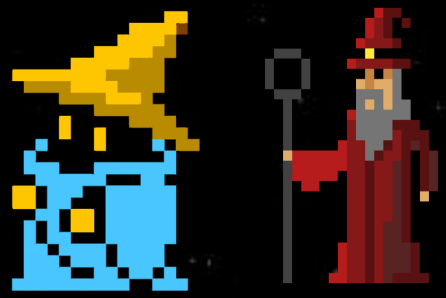
И еще сложнее

- Физическое дублирование подсистем
- Может потребоваться дублирование нескольких порядков
- А для всего этого нужна еще отдельная система сверки

Знаете что самое интересное?

- Аппараты Вояджер-1 и Вояджер-2 запущенные в 1977 до сих пор работают
- Изначальная длительность миссии была определена в 5 лет

Выводы



- Нельзя предвидеть всевозможные проверки
- Аппараты должны быть secure-by-design
- Правильно построенная архитектура и качественно протестированная техника может приятно удивить своей долговечностью

Еще увидимся

Федулаев Алексей
@int0x80h

Моисеев Андрей
@not_s0_S3c

https://disk.yandex.ru/d/usSgY4SmSExbSg

Подписывайтесь на наш канал

@ever_secure