

Отладка последовательных шин встраиваемых систем с помощью осциллографа

Алекс Климадж, Keysight Technologies

Стремление к сокращению размеров, потребляемой мощности и цены электронных изделий привело к широкому применению во встраиваемых системах последовательных шин. И хотя последовательные шины позволяют сократить число контактов интегральных схем, а также энергопотребление и занимаемое пространство, они заметно усложняют конструкцию. Инженерам, работающим с последовательными шинами, нужен быстрый способ отладки и проверки разрабатываемых схем.

Асинхронная природа многих последовательных интерфейсов порождает проблемы захвата и декодирования сигналов. И хотя анализаторы протокола отлично справляются с поиском функциональных проблем и ошибок синхронизации последовательных шин, осциллографы, помимо этого, позволяют выявлять источники шумов, захватывать переходные процессы, проводить тесты на соответствие спецификациям физического уровня и измерять мощность. Благодаря встроенной функции запуска по сигналам и декодирования данных последовательных шин, осциллографы становятся мощными универсальными приборами для разработчиков встраиваемых систем.

Захват и декодирование

До того как декодеры данных последовательных шин стали встраивать в осциллографы, инженеры были вынуждены декодировать последовательные кадры вручную. Это требовало

глубокого понимания протокола последовательной шины и некоторой «удачи» в попытке захватить нужный кадр. На рисунке 1 показан захваченный осциллографом кадр шины I²C с линией тактовой частоты (SCL) в канале 1 и линией данных (SDA) в канале 2. Для ручного декодирования этой информации необходимо использовать следующую процедуру.

1. Захватить один кадр осциллографом.
2. Сделать снимок экрана.
3. Открыть его на компьютере и добавить вертикальные линии вдоль каждого положительного перепада тактовой частоты.
4. Записать уровень сигнала SDA (1 или 0), соответствующий каждому положительному перепаду сигнала SCL.

В соответствии со спецификацией I²C преобразовать двоичные значения в шестнадцатеричные. Подсчитывая перепады тактовой частоты и зная, что протокол I²C использует стартовый импульс, 7 бит адреса, бит подтвержде-

ния, 8 бит данных, ещё один бит подтверждения и, наконец, стоповый бит, можно рассчитать шестнадцатеричные значения. В данном случае этот записанный кадр содержит адрес 0x29 и данные 0x04.

Этот метод, конечно, имеет право на существование, но он отнимает много времени и вполне может оказаться, что это вовсе не тот кадр, который был нужен. Если инженеру придётся декодировать вручную несколько последовательных кадров, то затраты времени могут стать неприемлемыми. Вот тут-то и становятся очевидными преимущества встроенного в осциллограф декодера последовательных данных. На рисунке 2 показана работа встроенного в осциллограф декодера данных шины I²C. Кроме того, использована функция запуска по сигналам последовательной шины для быстрого поиска нужного пакета данных. Декодированный кадр показан синим цветом в нижней части экрана осциллографа, а сверху виден оранжевый указатель точки запуска. Инженеры могут пользоваться этой функцией для быстрого поиска интересующих их данных, не вдаваясь в подробности спецификаций последовательной шины.

Захват непериодических сигналов последовательной шины

Предположим, что схема состоит из нескольких ИС (интегральных схем),



Рис. 1. Ручное декодирование данных шины I²C



Рис. 2. Запуск по сигналам шины I²C и автоматическое декодирование данных

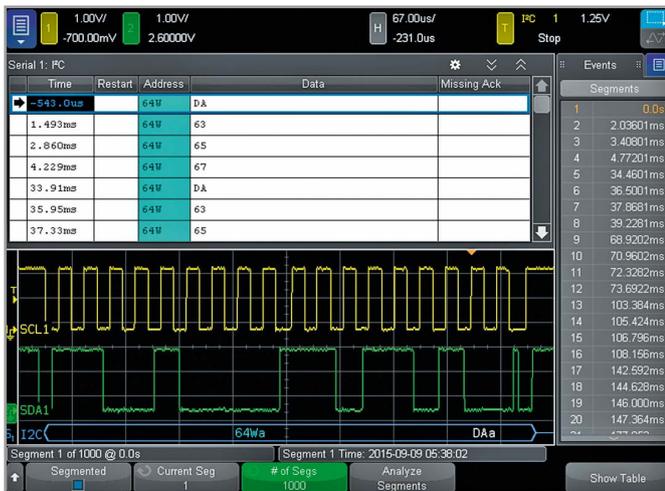


Рис. 3. Декодирование данных последовательной шины в режиме сегментированной памяти



Рис. 4. Сигнал USB с наведённой помехой



Рис. 5. Локализация наведённой помехи с помощью запуска по выделенной области

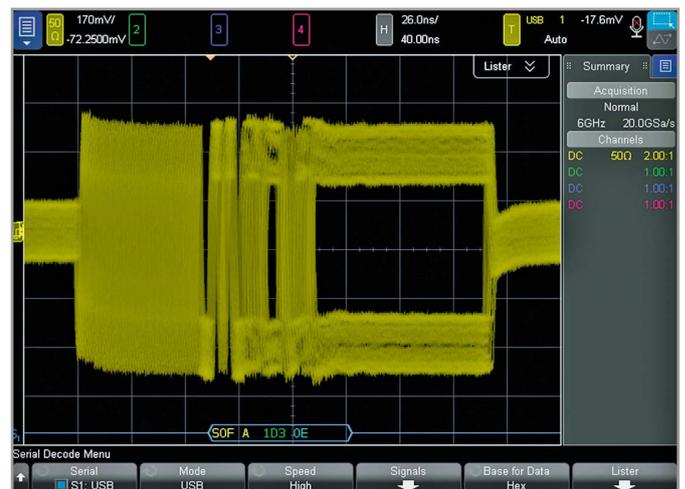


Рис. 6. Сигнал USB с низкочастотным шумом

которые взаимодействуют с контроллером через шину I²C, и необходимо увидеть все данные, которые записываются в определённую ИС. Это делается очень легко путём настройки запуска по адресу записи этой ИС. В результате осциллограф будет запускаться при каждом появлении этого адреса на шине, но получить общее представление о передаваемых данных по одной осциллограмме будет по-прежнему нелегко. Вот здесь-то и приходит на помощь сегментированная память. В режиме сегментированной памяти осциллограф ждёт появления заданных условий запуска, сохраняет осциллограмму в памяти, снабжает её меткой времени, снова производит запуск и ожидает следующего появления заданных условий. На рисунке 3 осциллограф настроен на запуск по каждой записи данных в ИС с шестнадцатеричным адресом 64, при этом включён режим сегментированной памяти с настройкой захвата 1000 сегментов. С помощью этого инструмента инженер может

увидеть, какие данные записывались в данную ИС, как часто они записывались, и изучить форму сигнала каждого кадра. Если один или несколько кадров содержат некорректные данные, инженер может выбрать этот кадр из списка и проверить целостность физического сигнала. Ошибка может порождаться шумом или переходными процессами.

Локализация наведённых помех

Случайные помехи, наведённые на последовательную шину, могут породить ошибки или вызывать сброс встроенного процессора. Используя традиционные методы запуска осциллографа, обнаружить их очень трудно. Наличие цифрового последовательного сигнала, который уже сам по себе содержит неперiodические события, дополнительно усложняет запуск по ещё более редким случайным помехам. Один из способов обнаружения помехи заключается в установке бесконечного послесвечения

развёртки сигнала. В режиме бесконечного послесвечения осциллограф не очищает экран между последовательными захватами сигнала. Новые сигналы продолжают накладываться на экран поверх старых. Использование запуска по последовательному сигналу для отображения всех переданных кадров и режима постоянного послесвечения создаст изображение, в котором все битовые позиции окажутся заполненными. При появлении помехи, её будет сразу видно: она выбивается из общей картины.

Обнаружив помеху, следует настроить запуск по ней. Как уже говорилось, осуществить это традиционными методами может оказаться весьма непросто. С появлением осциллографов с сенсорным экраном появились и новые методы запуска. С помощью функции запуска по выделенной области (Zone Trigger) помехи и переходные процессы захватываются очень легко. На рисунке 4 показан сигнал шины USB с неперiodической помехой.

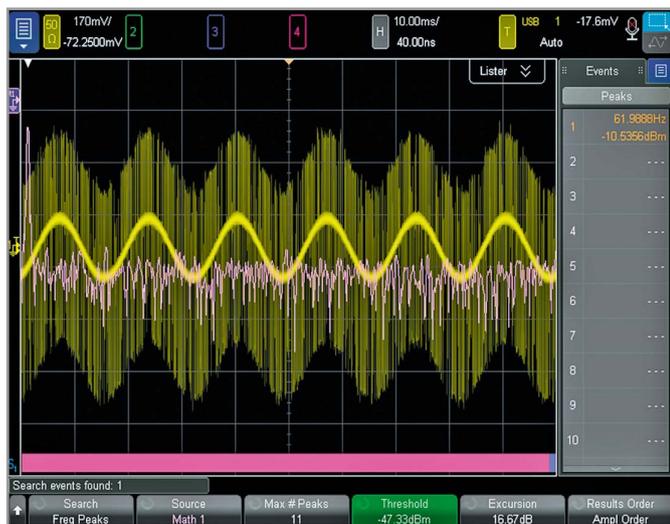


Рис. 7. БПФ сигнала USB с наведённым низкочастотным шумом

Чтобы настроить запуск по этой помехе нужно всего лишь нарисовать на сенсорном экране рамку и выбрать режим Zone 1 Must Intersect (пересечение зоны 1). Осциллограф запускается уже по началу кадра USB. Включение запуска по выделенной области говорит осциллографу, что он должен запускаться, только когда увидит начало кадра USB и сигнал внутри обозначенной зоны. Эта ситуация показана на рисунке 5. После успешного запуска по наведённой помехе можно выполнить необходимые измерения и установить источник её происхождения.

Поиск источника шума

А что если отлаживаемая последовательная шина не подвержена влиянию помех, а вместо этого на ней присутствует постоянный наведённый шум? Чтобы выявить источник этого шума нужно использовать иной подход, поскольку по шуму запускаться нельзя. В этом случае пригодится встроенная

в осциллограф функция быстрого преобразования Фурье (БПФ). БПФ преобразует сигналы из временной области в частотную. Это позволяет увидеть частотные составляющие наведённого шума. На рисунке 6 показан сигнал USB с наведённым шумом.

Уже по этому изображению начала кадра USB можно увидеть, что здесь присутствует шум с амплитудой около 150 мВ_{пик-пик}. Чтобы выявить источник этого шума можно использовать функцию БПФ и пиковые маркеры. При первом включении БПФ не наблюдается частотной составляющей, которую можно было бы назвать шумом. Это значит, что частота шума значительно ниже частоты сигнала USB.

Чтобы найти основную частотную составляющую, необходимо уменьшить скорость развёртки до 10 мс на деление. В этом режиме БПФ может обнаруживать низкие частоты. На рисунке 7 видно, что частота шума примерно равна 61 Гц. Это шум, наведённый на сигнал



Рис. 9. Сигнал USB с шумом частотой 2,4 ГГц от беспроводной сети



Рис. 8. Сигнал USB с шумом тактовой частоты 16 МГц

го сигнала 16 МГц. Устройства Интернета вещей со встроенным адаптером беспроводной сети могут подвергаться воздействию шумов, создаваемых радиостанциями. На рисунке 9 показан сигнал USB с пиком спектра на частоте 2,4 ГГц – это типичная частота беспроводной сети.

ЗАКЛЮЧЕНИЕ

Инженеры, занятые разработкой встраиваемых систем, вынуждены создавать недорогие энергоэффективные устройства малого размера. Это вызывает острую потребность в мощных средствах измерения и отладки. Для этого отлично подходят современные цифровые осциллографы со встроенной функцией декодирования данных последовательных шин. С появлением встроенных функций декодирования ручное декодирование отдельных кадров кануло в Лету. Расширенные режимы запуска по сигналам последовательных шин позволяют легко захватывать интересные кадры. Режим сегментированной памяти можно использовать вместе с декодированием данных последовательных шин для захвата конкретной передаваемой информации в течение длительных периодов времени. Новые методы запуска, ставшие возможными с появлением сенсорных экранов, существенно упрощают локализацию неперiodических помех. И, наконец, источники шума можно идентифицировать с помощью функции БПФ. Обзаведясь современным осциллографом, инженеры, занятые разработкой встраиваемых устройств, получают полный набор инструментов для отладки.

Новости мира News of the World Новости мира

УЦ «КУДИЦ» станет первым российским разработчиком учебных курсов IBM

Учебный центр «КУДИЦ» подписал соглашение с компанией Global Knowledge о создании серии авторизованных курсов по полной линейке продуктов IBM для специалистов по всему миру, на русском и английском языках. Это первый опыт отечественных специалистов в качестве разработчиков авторизованных курсов IBM.

УЦ «КУДИЦ» намерен разрабатывать курсы по всей линейке IBM, уже сейчас в разработке находятся курсы по продуктам – IBM DataPower, IBM DB2, IBM Tivoli Storage Manager. Курсы будут разработаны на русском и английском языках и станут доступны партнёрам и студентам Global Knowledge по всему миру.

Аньес Серантола, руководитель направления IBM Business в регионе EMEA компании Global Knowledge, заявила: «Учебный центр «КУДИЦ» является единственным УЦ на территории СНГ, способным проводить обучение по всей линейке продуктов вендора. В компании работает уникальная команда высокопрофессиональных специалистов, самостоятельно разработаны и внедрены множество курсов IBM, накоплен колоссальный опыт. Мы намерены экспортировать интеллектуальный продукт, разработанный в России, по всему миру».

Михаил Солохин, генеральный директор Учебного центра «КУДИЦ», отметил: «Особое внимание планируем уделить «узким» местам распространённых решений, состоящих из нескольких продуктов, чего ранее никто в мире не делал, ведь курсы по IBM почти всегда читаются по одному продукту, а у заказчика установлены несколько интегрированных между собой решений».

УЦ «КУДИЦ» получил право на проведение авторизованного обучения IBM в рамках новой глобальной концепции IBM Global Skill Initiative в 2014 году. Программа Global Skill Initiative была разработана и анонсирована корпорацией IBM годом ранее. Её основная цель – повышение доступности авторизованного обучения по продуктам и решениям IBM. В рамках программы были выбраны четыре глобальных партнёра, одним из которых стала компания Global Knowledge, им был присвоен статус IBM Global Training Provider (GTP). В рамках инициативы GTP стали центрами обучения и авторизации тренинг-партнёров корпорации во всём мире. IBM же оставила за собой функции разработки авторизованных учебных материалов,

предоставления доступа к удалённым учебным ресурсам, надзора за качеством обучения и проведения отдельных курсов по сложным темам. При этом GTP могут как осуществлять обучение своими силами, так и делегировать это право на отдельных территориях локальным компаниям через предоставление им авторизации на основании партнёрского соглашения. Именно такое партнёрское соглашение было подписано между Global Knowledge и Учебным центром «КУДИЦ» в начале 2014 года.

<http://qdts.ru/wps/portal/>

Микроэлектроника и станкостроение являются «ахиллесовой пятой» импортозамещения в оборонке

Вице-премьер Дмитрий Rogozin признаёт, что в ОПК есть компоненты, по которым пока проблематично обеспечить импортозамещение.

«Две ахиллесовых пяты, которые у нас есть, – это микроэлектроника и станкостроение», – сказал Д. Rogozin в интервью телеканалу НТВ.

При этом он отметил, что абсолютное большинство комплектующих, используемых в военной технике, должно производиться на территории России. По словам Rogozina, «нельзя допустить, чтобы в вопросах национальной безопасности и боеспособности Вооружённых сил Россия зависела от западных поставок».

Новости ВПК

Будущее технологий мобильной аутентификации в биометрии?

Будущее мобильной идентификации, как утверждают некоторые специалисты, в биометрических технологиях. С их точки зрения, это самый простой способ снизить риск потери или кражи гаджетов.

Сегодня в обзорах справедливо называются риски слабой идентификации мобильных устройств. Хотя смартфоны поддерживают идентификацию с помощью числовых PIN-кодов уже более десяти лет, более 20% пользователей iPhone, согласно исследованию Champion Solutions Group, все ещё не считают нужным применять PIN. Более 30% компаний не требуют, чтобы их сотрудники использовали по меньшей мере алфавитно-цифровые пароли на своих мобильных устройствах.

Но даже те, кто применяют PIN-защиту, не могут быть уверены в своей безопасно-

сти. PIN-коды и алфавитно-цифровые пароли относительно тривиальны и достаточно просто вычисляемы на основе анализа поведения пользователя. Кроме того, PIN-коды могут использоваться повторно и на разных устройствах. Согласно исследованию 2011 г., каждый седьмой iPhone может быть взломан перебором десяти наиболее широко используемых PIN.

Именно по этой причине политика мобильной идентификации включает требования по длине и сложности пароля, максимальному количеству повторных использований. На это обращают внимание производители смартфонов и планшетов. Так в iOS 9 и Windows Phone 10 длина PIN увеличена с четырёх до шести символов, что увеличило число возможных комбинаций с 10 000 до 1 000 000. Соответственно, время взлома путём перебора выросло с четырёх до 400 дней.

Популярной альтернативой PIN-кодам всё чаще становится биометрическая аутентификация, впрочем, она скорее более удобна, чем безопасна.

Вот несколько примеров.

Несколько лет назад в Android опробовали технологию биометрического распознавания лица, используя камеру мобильного устройства. Однако ранние версии этого ПО легко обходились. Для идентификации достаточно было использовать фотографию нужного лица.

Apple, используя технологию биометрической аутентификации на основе отпечатка пальца, добились большего. Последние версии Android также поддерживают дактилоскопическую аутентификацию. Вместе с тем необходимо отметить, что до сих пор не решена основная проблема этого метода. Как отличить живое от неживого? Ведь на сегодня большинство датчиков отпечатков пальцев легко обманывается муляжами.

Единственный выход, который на сегодня можно предложить – использовать датчик отпечатка вместе с PIN-кодом или паролем. Другие методы предполагают ввод PIN, посланного с помощью SMS на смартфон пользователя, или приложение-генератор одноразового пароля.

Безусловно, методы биометрической аутентификации будут развиваться. Однако пока заявлять, что данные технологии могут реально заменить пароли и PIN-коды, несколько преждевременно.

**Microsoft MVP,
Microsoft Security Trusted Advisor**