Защита интеллектуальных счетчиков на всем протяжении жизненного цикла

В статье рассматриваются различные механизмы атак на интеллектуальные счетчики на разных стадиях их жизненного цикла: при производстве, во время и после монтажа и в ходе эксплуатации. Описываются реальные способы предупреждения подобных атак, в частности применение защищенных начальных загрузчиков в процессе производства и измерительных плат при монтаже, аппаратное (а не программное) асимметричное шифрование данных на стадии эксплуатации; также возможно использование ядра с кумулятивной аттестацией (cumulative attestation kernel, CAK) для долгосрочной защиты. Представлена однокристальная система (SoC) ZEUS[1] компании Maxim как надежное решение для конструктивного обеспечения безопасности интеллектуальных счетчиков.

Дэвид ЭНДИН (David ANDEEN)

Введение

Интеллектуальные счетчики нового поколения выполняют в электрических сетях гораздо больше функций, чем их предшественники всего несколько лет назад, по первоначальному замыслу обеспечивавшие лишь передачу данных. Современные интеллектуальные счетчики — это оконечные узлы крупномасштабных межмашинных сетей связи, взаимодействующие не только с инфраструктурой интеллектуальных энергосистем, но и с громадным парком машин и устройств, которые подключены к этим энергосистемам и будут подключаться к ним в дальнейшем. Помимо защиты в пределах электросети данных, принадлежащих поставщикам и потребителям электроэнергии, интеллектуальные счетчики вместе с сопутствующим комплексом технических средств обеспечивают управление критически важной энергетической инфраструктурой, ее мониторинг и даже защиту. Такое расширение круга задач, выполняемых интеллектуальными счетчиками, порождает качественно новые проблемы безопасности в контексте администрирования сетей. Неудивительно, что несложное шифрование и пароли более не способны обеспечить требуемый высокий уровень безопасности. В нынешних условиях необходимы комплексные меры по защите интеллектуальных счетчиков на всем протяжении их жизненного цикла — от производства до утилизации.

В этом указании по применению исследуются угрозы безопасности, возникающие на различных стадиях жизненного цикла интеллектуальных счетчиков (производство, монтаж, ввод в эксплуатацию и весь период эксплуатации). Попутно описываются соответствующие риски и способы противодействия перечисленным угрозам.

Насущная потребность в защищенных интеллектуальных счетчиках

Внимание всем! Безопасность интеллектуальных энергосетей наконец-то признана важной общественной проблемой.

Еще несколько лет назад обсуждение вопросов безопасности интеллектуальных энергосетей сосредоточивалось в основном вокруг выработки стандартов приватности и предотвращения кражи данных. Сегодня центральной темой этих дискуссий стала реальная угроза энергетическим системам общего пользования. Проблемы информационной безопасности, инфраструктурных угроз, подобных Stuxnet, а также организованных атак на электросчетчики, как в Пуэрто-Рико [1, 2], часто находят отражение в сообщениях телеграфных агентств и в новостных программах популярных телевизионных каналов [3]. Чтобы обеспечить необходимый уровень защиты систем, многие авторитетные международные организации трудятся над выработкой рекомендаций и критериев, применимых, в частности, к инфраструктуре автоматизированного учета (AMI). В Европе это немецкая Федеральная организация по безопасности в сфере информационных технологий (Bundesamt fur Sicherheit in der Informationstechnik, BSI), опубликовавшая профиль защиты шлюзов в интеллектуальных системах учета [4]. На территории Северной Америки это Национальный институт стандартов и технологий США (NIST), который выпустил спецификацию NISTIR 7268, содержащую рекомендации по защите инфраструктуры автоматизированного учета [5].

СМИ продолжают акцентировать внимание на проблемах, связанных с интеллектуальными счетчиками, и выражать серьезную озабоченность. Но они не предлагают решений. BSI и NISTIR предоставляют описания желательных и возможных вариантов защищенной архитектуры, но практических воплощений крайне мало. По сути, на сегодня в отрасли отсутствуют многие важнейшие защитные механизмы, которые позволяли бы на системном уровне обеспечивать безопасность интеллектуальных счетчиков.

Угрозы безопасности интеллектуальных счетчиков в электросетях разнообразны и постоянно видоизменяются. Следовательно, не существует какого-то единого, универсального решения для противодействия ситуации. Любая устойчивая стратегия защиты интеллектуальных счетчиков должна быть рассчитана на борьбу с меняющимися угрозами. Потенциальные проблемы начинаются еще на стадии изготовления, сборки и калибровки аппаратной части счетчиков и продолжаются на всем протяжении их эксплуа-

[1] ZEUS — товарный знак компании Maxim Integrated Products, Inc.

тации, плановый срок которой на предприятиях энергоснабжения составляет обычно от 10 до 20 лет. Для устранения этих проблем на каждой стадии существуют свои аппаратные и программные решения. Аппаратные решения отличаются большим вычислительным быстродействием и лучшей физической защищенностью, а программные — большей гибкостью. Лучший вариант — сбалансированное сочетание аппаратных и программных мер защиты инфраструктуры системы. Одно такое оптимизированное решение для интеллектуальных счетчиков уже существует. Однокристальная система (SoC) для ZEUS компании Maxim представляет собой ультрасовременный комплекс программно-аппаратных средств защиты инфраструктуры интеллектуальных счетчиков. В настоящей статье данная система будет служить основным примером практической реализации защищенной архитектуры.

Защита на стадии производства

Центральной темой дискуссий о безопасности интеллектуальных энергосистем зачастую становятся алгоритмы шифрования, применяемые в ходе эксплуатации. Подобный метод нельзя не признать чрезвычайно ценным средством защиты, но это лишь часть решения [6]. Шифрование позволяет уберечь данные в процессе работы, но не решает проблем, возникающих на этапе производства и монтажа. На самом деле, логистическая цепочка производственного предприятия — первое уязвимое место.

Как и большинство компаний — изготовителей электроники, поставщики интеллектуальных счетчиков главным образом отдают производство на субподряд и зачастую не в те страны, где осуществляется проектирование. В большинстве случаев такой процесс безопасен и эффективен, но для тех, кто выпускает защищенные устройства, он влечет возникновение определенных внешних угроз. Сторонние подрядчики получают низкоуровневый доступ к архитектуре, аппаратной части и программному обеспечению системы. А потому неудивительно, что первым условием защищенности производства является защищенная логистическая цепочка. Комплектующие изделия, например полупроводниковые компоненты, должны приобретаться через доверенные каналы поставок, которые позволяют взаимно удостоверить подлинность поставщика компонентов и изготовителя комплектного оборудования. Схема «запрос – ответ» с криптографическим хэшированием — наиболее эффективный метод проверки подлинности участников логистической цепочки.

Доступ к системе и управление ею в ходе производственного процесса должны быть разрешены только доверенным лицам. Здесь идут в ход цифровые подписи и криптографические алгоритмы. Взлом защиты счетчиков, произошедший в Пуэрто-Рико, стал результатом несанкционированных манипуляций — вероятно, в ходе производственного процесса. Очень эффективное средство защиты системы на данной стадии — защищенный начальный загрузчик (secure bootloader). Рассмотрим его более детально.

При помощи защищенного начального загрузчика производитель комплектного оборудования управляет доступом к контроллеру интеллектуального счетчика во время производства. Код, загруженный на заводе-изготовителе, проверяется при начальной загрузке. Этот код не выполняется, если он не прошел идентификацию по асимметричному алгоритму шифрования с криптографическим хэшированием. Такой процесс позволяет удостовериться, что код происходит из доверенного источника. Аналогией в промышленности может служить доступ к корпоративной компьютерной сети: вход в систему разрешается только уполномоченному персоналу (то есть после проверки подлинности), и только этот персонал может выполнять в системе определенные команды (например, запускать код, проверенный криптографическими методами).

Защищенный начальный загрузчик — бесценное средство обеспечения безопасности, объединяющее несколько уровней защиты. Без защищенного начального загрузчика в аппаратной части злоумышленникам достаточно будет одной уязвимости, например скомпрометированного ключа, чтобы проникнуть в систему. Именно поэтому сегодня столь актуально использование интеллектуальных счетчиков с однокристальной системой ZEUS, оборудованной защищенным начальным загрузчиком. В такой конфигурации только уполномоченные лица с соответствующими закрытыми ключами, прослеживаемыми по надлежащей цепочке сертификатов, смогут передавать сообщения, которые будут загружаться и выполняться системой ZEUS (а значит, и интеллектуальным счетчиком).

Защита на стадии монтажа

Большинство предприятий энергоснабжения не располагает достаточным количеством персонала, чтобы за приемлемое время смонтировать нужное количество счетчиков. Соответственно, для монтажа систем автоматизированного учета обычно приходится привлекать сторонних подрядчиков, которые опять-таки получают доступ к критически важной инфраструктуре. Во время монтажа возможен физический несанкционированный доступ через оптические порты или попросту изменение схемы подключения счетчиков. Проверить корректность монтажа в этой ситуации позволяет защищенная измерительная плата.

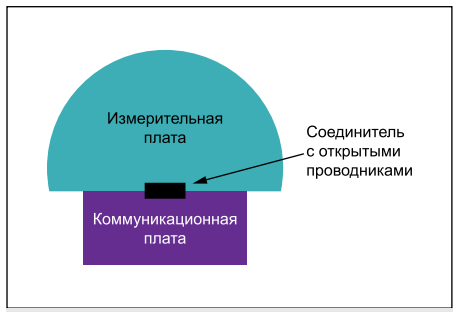

Рис. 1. В двухплатном счетчике с незащищенной измерительной платой данные передаются по открытым проводникам соединителя

Многие современные счетчики конструктивно состоят из двух плат: измерительной и коммуникационной (рис. 1).

Через них потенциально возможен доступ к данным измерений прежде, чем они будут зашифрованы для дальнейшей передачи. Другой подход — использовать одноплатный счетчик с защитными функциями (например, инкапсуляцией), реализованными в самой измерительной микросхеме. Шифрование данных со счетчика в отдельном блоке измерительной микросхемы позволяет сразу после измерения защитить их от несанкционированного доступа. Эта мера закрывает потенциальные бреши в системе безопасности между измерительной и коммуникационной частью. Данные, полученные непосредственно после монтажа, можно считать надежными. Для проверки корректности предприятие энергоснабжения может сравнить их с показаниями старого счетчика. Благодаря реализации функций шифрования в измерительной микросхеме однокристальная система ZEUS закрывает брешь между измерительной и коммуникационной частью (рис. 2), не позволяя злоумышленникам проникнуть в сеть. После монтажа защитная инкапсуляция гарантирует целостность сведений на протяжении всего срока службы счетчика.

Рис. 2. В одноплатном счетчике функции защиты реализованы в самой измерительной микросхеме

Защита на стадии эксплуатации

Электросчетчики, в том числе интеллектуальные, монтируются снаружи каждой квартиры и офиса, зачастую в физически неза-

щищенных местах, где у злоумышленников есть масса времени на их изучение. Учитывая масштабы энергосетей и длительный срок службы счетчиков, интеллектуальные счетчики в составе инфраструктуры автоматизированного учета уязвимы для различных угроз как в пространственной, так и во временной перспективе.

Большая поверхность атаки

Инфраструктура автоматизированного учета имеет большую поверхность атаки, то есть множество уязвимых мест, через которые можно атаковать интеллектуальный счетчик. На рис. 3 показано графическое представление такой сети, состоящей обыкновенно из сотен тысяч счетчиков, которые сообщаются с концентраторами по линиям электропередачи или радиоканалам (роль транспортной сети, осуществляющей связь концентратора с предприятием энергоснабжения, часто играет сотовая сеть). Связь концентраторов с предприятиями энергоснабжения выполняется по транспортным сетям того или иного вида (сотовым или волоконно-оптическим). Многосвязная маршрутизация и/или переадресация входящих и исходящих сообщений между счетчиками и концентраторами позволяет счетчикам автоматически расширять сеть. Такая архитектура снижает инфраструктурные издержки за счет сокращения числа концентраторов, обслуживающих то же количество счетчиков. Вместе с тем многосвязная сеть более уязвима, так как создает возможность для перехвата и модификации данных, передаваемых между интеллектуальными счетчиками. Такой вид вмешательства называется атакой типа «тайный посредник» (man in the middle, MiTM).

Интеллектуальные счетчики не наделены высокоразвитыми защитными функциями и большой вычислительной мощностью, свойственными концентраторам и другому крупному сетевому оборудованию. Теоретически это означает, что атаковать счетчики легче, чем концентраторы или транспортную сеть. Более того, атака на многосвязную сеть может осуществляться на обширной территории, если сеть достаточно велика. Учитывая, что счетчики многократно обмениваются данными между собой без контроля со стороны какой-либо дополнительной сетевой инфраструктуры, каждый счетчик должен быть надежно защищен на индивидуальном уровне.

Для того чтобы наделить отдельные счетчики защитными функциями, необходимо выбрать алгоритм такой индивидуальной защиты. AES и другие симметричные алгоритмы шифрования обеспечивают великолепную защиту, но обладают тем недостатком, что все счетчики имеют один и тот же ключ. Соответственно, любой злоумышленник, завладевший закрытым ключом, сможет атаковать все счетчики. Для индивидуального шифрования данных лучше всего подходят асимметричные алгоритмы, поскольку в них шифрование и дешифрование данных производится с применением уникального набора секретных ключей. Ключи, используемые для многократно выполняемых защищенных операций (например, проверки подлинности), должны генерироваться внутри микросхемы, находиться в защищенной памяти и встраиваться в само защищенное изделие, чтобы сохранить в тайне секретный ключ и избежать необходимости передавать его за пределы счетчика. Если потребовать, чтобы в каждом счетчике использовалась уникальная комбинация ключей, то завладение одним секретным ключом позволит получить доступ только к определенному счетчику. Таким образом, асимметричное шифрование кардинально уменьшает поверхность атаки на инфраструктуру автоматизированного учета и значительно снижает отдачу от приложенных усилий для атакующего. Проще говоря, такая атака может теперь не оправдывать затрат времени и труда злоумышленника.

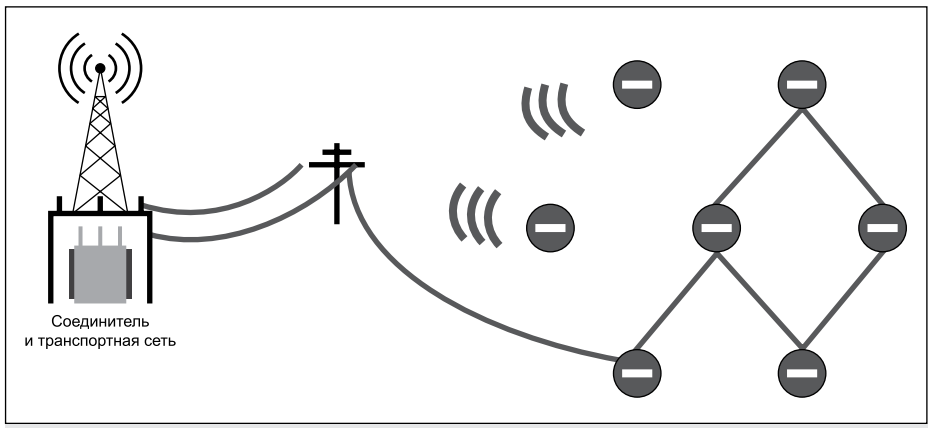

Рис. 3. В инфраструктуре автоматизированного учета счетчики сообщаются с концентратором по линиям электропередачи или радиоканалам (обратите внимание, что отношение числа концентраторов к числу счетчиков на этом графике гораздо ниже)

Но вычисления производятся не мгновенно, а замедлять работу критичной ко времени системы не хочется никому. Поэтому важнейшая проблема при асимметричном шифровании — объем вычислений, требуемых от каждого счетчика. В этих обстоятельствах значительный выигрыш дает аппаратная реализация. Аппаратные шифрование и дешифрование с применением аппаратных ускорителей сокращают временные затраты на вычисления по сравнению с аналогичными функциями, реализованными программно. Теперь можно свести к минимуму затраты системных ресурсов на шифрование и дешифрование сообщений, высвободив эти ресурсы для решения других задач.

В однокристальной системе ZEUS интегрировано несколько уровней аппаратного асимметричного шифрования, а также функции генерации и хранения секретных ключей. Для повышения стойкости асимметричного шифрования секретные ключи создаются истинным генератором случайных чисел, чтобы нельзя было получить ключи посредством атак повторного воспроизведения. Реализован и ряд симметричных алгоритмов (в частности, AES), которые предоставляют еще один уровень шифрования поверх описанных выше асимметричных методов и обеспечивают соответствие стандартам защиты, требующим применения таких алгоритмов.

Гибкость в отношении будущих угроз

Защищенные интеллектуальные счетчики должны быть достаточно гибкими, чтобы справляться с угрозами безопасности, которые будут возникать на протяжении многих лет после развертывания инфраструктуры автоматизированного учета. Соответственно, обнаружение и ликвидация угроз на стадии долгосрочной эксплуатации становятся следующим — и притом непростым — шагом к обеспечению жизнеспособности и безопасности счетчика и электрической сети.

Как утверждают предприятия энергоснабжения, главные причины, по которым многие современные реализации инфраструктуры автоматизированного учета не оснащены системами обнаружения вторжений, — это высокие издержки и отсутствие зрелых технических решений [9]. Проблемы производителей интеллектуальных счетчиков сводятся к очевидному, но не столь простому вопросу: насколько большой вычислительной мощностью следует наделять счетчик для целей обнаружения угроз? Во многих научных статьях предлагаются решения, которые предусматривают интеграцию средств обнаружения угроз, реализованных непосредственно в счетчике и в сети [9, 10]. Одно многообещающее решение заключается в использовании ядра с кумулятивной аттестацией (CAK) — выполняемого в счетчике программного кода, который осуществляет аудит версий

микропрограммы и тем самым образует дополнительный рубеж обнаружения угроз на случай, если злоумышленникам удалось преодолеть шифрование и проверку подлинности. САК может выполняться на 8- или 32-разрядном микроконтроллере и требует минимального количества памяти. Эксперты, в частности специалисты Исследовательского института электроэнергетики (Electric Power Research Institute), соглашаются, что интеллектуальные счетчики следует наделять определенной дополнительной функциональностью для обеспечения безопасности и поддержки будущих решений.

Данность на сегодня такова, что для устранения последствий несанкционированного проникновения в систему необходимо дорогостоящее вмешательство. Соответственно, текущая эксплуатация защищенной сети интеллектуальных счетчиков требует чего-то большего, нежели просто обнаружения и ликвидации угроз. Проблема заключается в реагировании. Способы, которыми счетчик реагирует на текущие и будущие угрозы, влияют на эффективность, а также с высокой вероятностью на экономическую рентабельность инфраструктуры автоматизированного учета.

Рассмотрим защищенные системы. Многие защищенные системы, такие как финансовые терминалы, немедленно выключаются в случае вторжения, не позволяя злоумышленнику проникнуть дальше в сеть. При очевидных неудобствах такого решения выгоды от него перевешивают риск потери финансовой информации, находящейся под защитой системы. Другое дело — интеллектуальные счетчики: они контролируют лишь энергоснабжение соответствующего потребителя, поэтому в данном случае необходимо взвесить все «за» и «против» любой реакции на угрозу. Немедленное выключение не лучший ответ на воспринимаемую угрозу. Правильным для сети будет оперативно оценить потенциальную угрозу, прежде чем как-то реагировать. Более того, вся инфраструктура автоматизированного учета должна продолжать работу в присутствии угроз, эффективно оценивая серьезность каждой из них. Большинство сочтет временное прекращение обслуживания одиночного потребителя менее серьезным делом, чем крупномасштабные перебои или массовые злоупотребления по всей коммуникационной инфраструктуре. Учитывая, что наибольшую угрозу для инфраструктуры автоматизированного учета представляют масштабные кибератаки, интеллектуальные счетчики должны быть в состоянии в любое время определять приоритетные способы противодействия.

К тому же интеллектуальный счетчик должен обеспечивать надежную аппаратную защиту, нейтрализацию угроз и поддержку будущих программных решений без глубокой модернизации системы. Архитектура однокристальной системы ZEUS основана на 32-разрядном процессорном ядре ARM. Любая коммуникация, которая не дешифруется надлежащим образом или не проходит проверку подлинности, может игнорироваться, регистрироваться в журнале или инициировать оповещение по выбору конструктора счетчика и сетевого архитектора. Отделение измерительной части от ядра ARM гарантирует бесперебойную работу счетчика во время выполнения разнообразных программных процедур. Такая организация работы счетчика в полной мере соответствует стандарту WELMEC [11] и другим стандартам, требующим отделения измерительной аппаратуры и/или программного обеспечения от программных и аппаратных элементов с иным функциональным назначением. Более того, описанная выше аппаратная защита обеспечивает максимально быстрое выполнение коммуникационных операций, освобождая ядро ARM для выполнения системных задач. Дополнительно ядро ARM может оснащаться решениями завтрашнего дня наподобие САК, которые функционируют поверх уже и без того надежно защищенной системы. Сочетание повышенной вычислительной мощности, аппаратной защиты и обновлений программного обеспечения для противодействия новым угрозам — вот суть высокоэффективного решения для защиты энергосистем, в котором соблюден правильный баланс между аппаратной и программной функциональностью.

Перспективные возможности

Интеллектуальная энергосистема — впечатляющий результат развития энергосистемы образца двадцатого века. Но, оснастив такую огромную систему функциями сетевого взаимодействия и управления, мы тем самым значительно увеличили ее уязвимость для атак на систему безопасности, и в первую очередь кибератак. Международные организации трудятся над стандартизацией характеристик таких систем, а СМИ сообщают о технологических достижениях в этой сфере и случаях взлома системы безопасности. Однако ответственность за защиту от атак ложится на производителей интеллектуальных счетчиков. Упреждающий подход к проектированию интеллектуальных счетчиков заключается в разделении аппаратной и программной функциональности, а также в обеспечении защиты счетчика на всем протяжении его жизненного цикла — от приобретения сторонних комплектующих и производства до монтажа и долгосрочной эксплуатации. На основе глубокого знания проблематики интеллектуальных счетчиков и развивающейся электроэнергетической отрасли компания Maxim Integrated спроектировала однокристальную систему ZEUS — передовое элегантное решение для интеллектуальных счетчиков сегодняшнего и завтрашнего дня.

Автор благодарит своих коллег Бена Смита (Ben Smith), Кристофа Тремлета (Christophe Tremlet) и Грегори Гуэса (Gregory Guez) за их технический вклад в написание этой статьи.

Литература

1. FBI: Smart Meter Hacks Likely to Spread. Krebs on Security, апрель 2012 — http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/
2. Tutorial 5445. Stuxnet and Other Things that Go Bump in the Night.
3. Senators Aim To Protect Electric Grid From Hackers. CBS News, April 30, 2012 — www.cbsnews.com/8301-503544_162-4981641-503544.html
4. Protection Profile for the Gateway of a Smart Metering System. Bundesamt fur Sicherheit in der Informationstechnik, Gateway PP v01.01.01 (final draft), 2011.
5. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. and Guidelines for Smart Grid Cyber Security. volumes 1–3, The Smart Grid Interoperability Panel-Cyber Security Working Group, National Institute of Standards and Technology, U.S. Department of Commerce, September and August 2010 — http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf
6. Tutorial 5486. Securing the Life Cycle of the Smart Grid.
7. Tutorial 3675. Protecting R&D Investment with Secure Authentication.
8. Intrusion Detection System for Advanced Metering Infrastructure, Electric Power Research Institute, December 31, 2012 — www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026553
9. LeMay M., Gunter C. A. Cumulative Attestation Kernels for Embedded Systems. IEEE Transactions on Smart Grid, vol. 3, no. 2, June 2012 — http://seclab.web.cs.illinois.edu/wp-content/uploads/2011/03/LeMayG09-esorics.pdf.
10. McLaughlin S., Holbert B., Zonouz S., Berthier R. AMIDS: A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructure. Paper presented at the IEEE Third International Conference on Smart Grid Communications (SmartGridComm), in Tainan City, Taiwan, Nov. 5–8, 2012, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6486009&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F6479749%2F6485945%2F06486009.pdf%3Farnumber%3D648600.
11. Software Guide (Measuring Instruments Directive 2004/22/EC). WELMEC Working Group 7, March 2012, Issue 5, www.welmec.org/fileadmin/user_files/publications/WELMEC_07.02_Issue5_SW_2012-03-19.pdf
12. Application note 5631 — http://www.maximintegrated.com/an5631
13. www.maximintegrated.com/distributors