«ИНТЕРНЕТ ВЕЩЕЙ» БЕЗ ПРОСТОЕВ: БЕЗОПАСНОЕ УПРАВЛЕНИЕ ПО ДОПОЛНИТЕЛЬНОМУ КАНАЛУ

ДЭНИЕЛ МЕСАК (DANIEL MEESAK)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

В статье представлены преимущества управления по дополнительному каналу (Out-of-band Signaling, OBS[1]) внеполосной связи для устройств «Интернета вещей», которое поддерживают твердотельные накопители со встроенными микроконтроллерами Azure Sphere. Рассмотрим, как такое решение справляется с проблемами управления IoT-устройствами, их обслуживания и безопасности, обеспечивая в итоге сокращение непроизводительных простоев и затрат на обслуживание для операторов IoT-систем [1].

Микроконтроллеры Azure Sphere надежно подключаются к облаку и сети благодаря специальной службе безопасности. Служба гарантирует, что на устройство загружается только авторизованная версия подлинного, утвержденного программного обеспечения (ПО). Кроме того, она предоставляет защищенный канал, через который Microsoft позволяет автоматически загружать и устанавливать обновления ОС для развернутых устройств, чтобы устранить проблемы с безопасностью. При этом не требуется вмешательство ни производителя, ни конечного потребителя, благодаря чему можно закрыть брешь в системе безопасности [2].

ВВЕДЕНИЕ

Если говорить кратко, «Интернет вещей» — это концепция подключения существующих и добавления новых устройств в любую сеть, будь то Интернет или локальные сети. Для компаний, стремящихся к цифровизации, «Интернет вещей» может быть чрезвычайно полезным с точки зрения оптимизации операций и сбора данных, поскольку может упростить управление и значительно сократить общие непроизводительные расходы.

Однако нельзя забывать и об одной важной проблеме. Дело в том, что при внедрении IoT игнорируются связанные с этим осложнения, вызванные увеличением количества устройств при относительном сокращении числа людей-операторов. Рост затрат на обслуживание неизбежно повлечет за собой рост количества устройств, равно как и рисков простоя и неэффективного управления. По данным исследовательской и консалтинговой компании Gartner, до 80% затрат на информационные технологии приходится на первоначальную покупку, при этом самыми большими проблемами в этой сфере считаются время простоя и техническое обслуживание [3].

К счастью, правильно организованные системы управления могут значительно снизить эти риски. В идеале система предоставляет пользователю хороший обзор текущей ситуации и позволяет выполнять удаленное резервное копирование и восстановление, а также обеспечивает предсказуемость поведения. Поэтому многие компании внедрили функции мониторинга состояния системы и процедуры управления в свои продукты и соответствующее ПО. Однако все эти функции основаны на рискованном предположении, что само устройство остается работоспособным. В большинстве случаев при сбое ОС такие системы управления больше не могут получить доступ к устройству. Единственное решение в таком случае — прислать техника, чтобы исправить это вручную. Вполне понятно, что это дорогостоящее и трудоемкое решение, которое просто неприемлемо в мире, где количество подключенных к Интернету устройств растет с экспоненциальной скоростью [4].

В этой статье объясняется, как решения хранения данных с коммуникацией по дополнительному каналу помогают преодолеть эти проблемы за счет использования независимого канала, встроенного в твердотельные накопители (solid-state drive, SSD) устройств IoT.

ВНУТРИПОЛОСНАЯ И ВНЕПОЛОСНАЯ СИГНАЛИЗАЦИИ

Внутриполосная (in-band) сигнализация, по сути, охватывает все типичные способы подключения компонентов и периферийных устройств к IoT-устройству. Если использовать в качестве примера твердотельные накопители, внутриполосное соединение можно облегчить с помощью стандартных разъемов SATA, M.2, mPCIe, которые есть на большинстве материнских плат, или даже через порты USB и слот SD-карты. Внутриполосная

[1] Out-of-band Signaling, OBS — букв. «внеполосная сигнализация». В данном контексте подразумевается метод передачи служебных сигналов (сигналов управления) на частотах за пределами основного канала или протокола, обычно используемого для передачи информации. — Прим. пер.

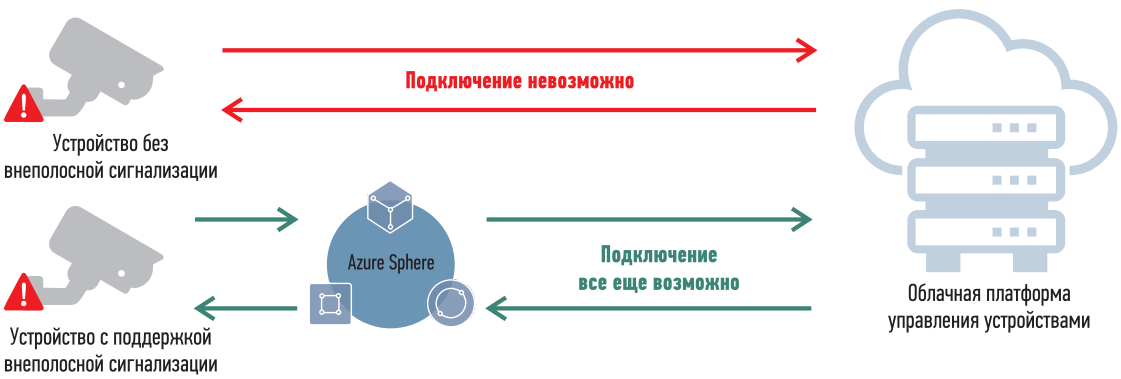


РИС. 1. ◄ Твердотельный накопитель InnoAGE компании Innodisk со встроенным контроллером Azure Sphere

передача сигналов устройству зависит от аппаратной реализации и, как следствие, от ОС.

Напротив, внеполосная (out-of-band) сигнализация охватывает решения с соединениями, которые формируют независимый канал связи, так сказать, обходя систему стороной. Современные проприетарные технологии, встроенные, например, в решение InnoAGE SSD компании Innodisk (рис. 1), позволяют SSD выполнять такие команды, как восстановление, резервное копирование и безопасное стирание, независимо от работоспособности остальной системы. В сочетании с усовершенствованным микроконтроллером (таким как Azure Sphere), оснащенным передатчиком Wi-Fi, эти технологии дают пользователю возможность удаленного доступа и управления SSD, независимо от общего состояния системы.

Проблему удаленного управления неисправными устройствами лучше всего иллюстрирует пример, представленный на рис. 2.

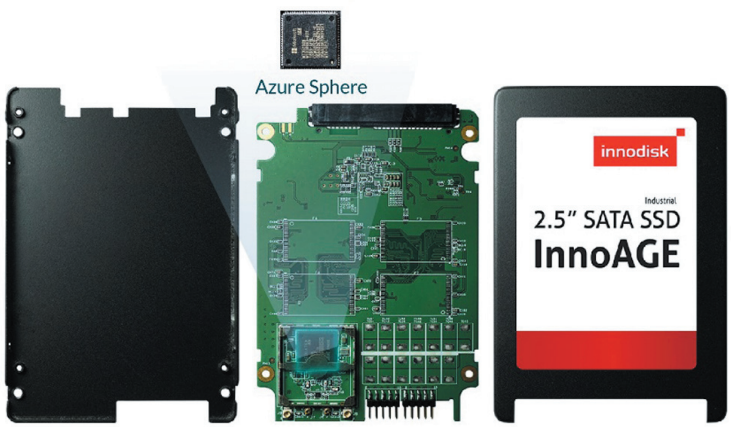


РИС. 2. ◄ Для устройства с внеполосной сигнализацией через Azure Sphere доступно удаленное восстановление

КЛЮЧЕВЫЕ ПРОБЛЕМЫ РАСШИРЕНИЯ «ИНТЕРНЕТА ВЕЩЕЙ»

Проблемы управления

Проблему управления IoT можно условно разделить на две части. Одна ее сторона связана с простой обработкой всех данных устройства по мере их создания [7]. Если разрыв между численностью устройств и операторами продолжает увеличиваться, то сложность сохранения полного контроля над системой также возрастает. Без предсказуемости планирование эффективного управления практически невозможно и подвергает систему риску неожиданного непроизводительного простоя.

Это подводит нас ко второй стороне проблемы управления IoT, а именно зависимости от внутриполосной сигнализации. Чтобы с IoT-устройства можно было собирать данные, оно и его ОС должны быть в рабочем состоянии. При использовании внутриполосной сигнализации это означает, что после сбоя устройства или ОС системный интегратор должен послать кого-нибудь разобраться с забарахлившим устройством.

Большинство систем управления, доступных сегодня на рынке, не решает эту проблему или решает только отчасти. Рис. 3 наглядно иллюстрирует проблему, показывая ее развитие с ростом числа устройств IoT.

Проблемы обслуживания и технической поддержки

Неправильное обслуживание может привести к значительным расходам, которые понесет систем-

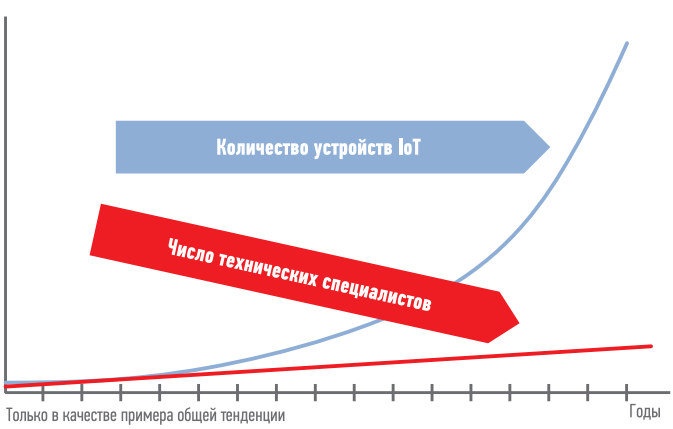
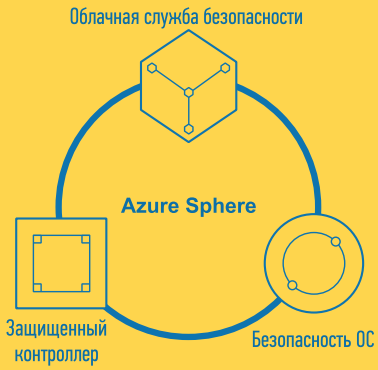


РИС. 3. ◄ Экспоненциальный рост устройств IoT значительно опережает рост численности обслуживающего эти устройства технического персонала

AZURE SPHERE



Azure Sphere — это микроконтроллер, разработанный корпорацией Microsoft и предназначенный для использования в устройствах «Интернета вещей» [5]. Azure Sphere работает под управлением ОС Azure Sphere, которая позволяет устройству не зависеть от ОС хост-устройства. Чтобы гарантировать полную защиту IoT-устройства от внешних угроз, таких как попытки несанкционированного доступа, корпорация Microsoft создала пакет безопасности для обеспечения целостности устройства и защиты оборудования от злоумышленников. Этот пакет также включает безопасный и зашифрованный доступ к облачным службам Azure [6].

Azure Sphere [7] — защищенная платформа приложений высокого уровня со встроенными функциями взаимодействия и обеспечения безопасности. Предназначена для устройств, подключенных к Интернету. Платформа состоит из защищенного подключенного перекрестного микроконтроллера, специализированной высокоуровневой ОС на базе Linux и облачной службы безопасности, которая обеспечивает непрерывную возобновляемую безопасность.

Использование Azure Sphere дает следующие преимущества:

- Микроконтроллер Azure Sphere объединяет возможности обработки данных в реальном времени и запуска высокоуровневой ОС. Наряду с ОС и платформой для приложений он позволяет создавать защищенные подключенные к Интернету устройства, которые можно обновлять, контролировать, отслеживать и поддерживать удаленно. Подключенное устройство с микроконтроллером Azure Sphere (либо одновременно с существующим микроконтроллером, либо вместо него) помогает получить повышенную безопасность, производительность и расширенные возможности: защищенная среда приложений, аутентифицированные соединения и согласованное использование периферийных устройств минимизируют риски безопасности из-за спуфинга, мошеннического ПО или атак с отказами в обслуживании.
- Обновления ПО можно автоматически разворачивать из облака на любом подключенном устройстве для устранения проблем, обеспечения новых функций или противодействия новым методам атак, что повышает производительность персонала службы поддержки.
- Данные об использовании продукта могут передаваться в облако по защищенному соединению, чтобы помогать в диагностике проблем и разработке новых продуктов, что увеличивает возможности для обслуживания продукта, положительного взаимодействия с клиентами и разработок в будущем.

ный интегратор. Например, если внезапно перестанет работать торговый автомат, этот непроизводительный простой ударит по всему бизнесу. Кроме того, необходимость отправлять кого-то устранять возникшую проблему ведет к дополнительным расходам. А при худшем раскладе может потребоваться даже замена неисправного оборудования [8]. В масштабе компании, которая, например, управляет десятками тысяч торговых автоматов, такая ситуация быстро превращается в слишком дорогостоящую проблему.

Таким образом, фундаментальные требования для эффективного обслуживания IoT — это доступность и быстрое восстановление системы. Доступ к системе должен быть простым, даже если она выйдет из строя. Также для предотвращения отказов и обеспечения эффективного и своевременного обслуживания система должна обеспечивать определенный уровень предсказуемости, давая возможность организовать прогнозное техническое обслуживание. Такое обслуживание можно провести во время планового простоя оборудования, что минимально отразится на показателях прибыли для бизнеса. Наконец, в случае сбоя системы необходимы инструменты для ее быстрого исправления и восстановления — желательно без загрузки специализированного ПО непосредственно на месте установки оборудования.

Проблема обеспечения безопасности на периферии

Большое количество взаимосвязанных устройств в одной сети позволяет получить больше данных и более эффективное приложение. Обратной стороной этой медали является то, что с каждым устройством, добавленным в сеть, появляется еще одна потенциальная точка входа, которую можно использовать в неблаговидных целях.

Поскольку IoT-устройства обычно не укомплектованы персоналом с ограниченным физическим управлением и контролем таких устройств, т. е. практически находятся в широком доступе, риски безопасности, угрожающие как самому устройству, так и сетям, к которым оно подключено, должны устранять системные интеграторы. Как правило, они

РИС. 4. ◄
Снимок экрана платформы управления InnoAGE SSD компании Innodisk

используют для этого многосторонние решения, которые касаются локально хранимых данных, а также каналов связи устройства.

Если задействован интегрированный микроконтроллер, проблема безопасности на периферии усложняется. Если у микроконтроллера есть отдельный канал подключения, этот путь должен быть защищен так же, как и само устройство.

РЕШЕНИЯ ПРОБЛЕМ РАСШИРЕНИЯ «ИНТЕРНЕТА ВЕЩЕЙ»

Интуитивно понятная платформа управления

Первым шагом к обеспечению эффективного управления IoT может стать объединение всех подключенных устройств на одной платформе, такой как, например, iCAP компании Innodisk.

Благодаря тому что выходные данные представлены через простой пользовательский интерфейс на основе браузера, информация становится легко доступной, вне зависимости от устройства и его расположения. Устанавливая пороговые значения для определенных параметров, например температуры или количества циклов записи SSD, система управления также обеспечивает предсказуемость поведения устройства в обозримом будущем, что, в свою очередь, упрощает планирование работы на устройствах системы и их технического обслуживания. Снимок экрана платформы управления InnoAGE SSD компании Innodisk показан на рис. 4.

Однако эти фундаментальные аспекты управления IoT по-прежнему оставляют систему уязвимой при внезапных сбоях общей системы. Когда система не работает, внутриполосное управление становится невозможным и в ожидании ручного сброса система является попросту бесполезной. Вот почему внеполосная сигнализация является важным дополнением к любому решению для управления IoT. При постоянном доступе к устройству оно всегда готово к обновлению прошивки, встроенного микроконтроллера и других компонентов.

У внутриполосного управления есть еще одно преимущество, кото-

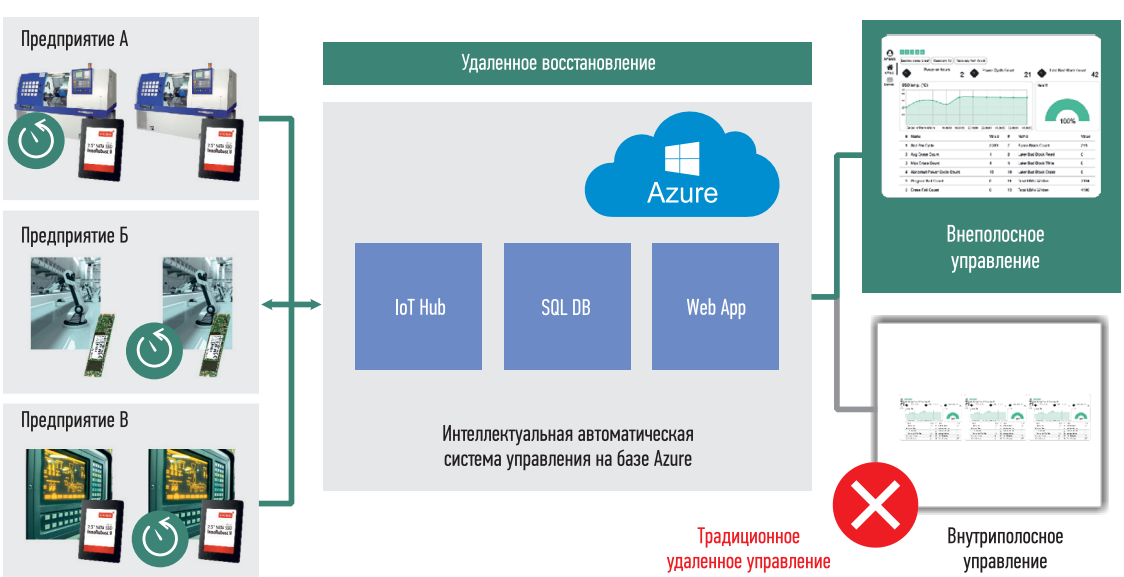


РИС. 5. ◄
Пример удаленного восстановления «упавшей» системы с помощью внеполосного управления

рое касается настройки ввода / вывода общего назначения (GPIO). Если на схеме, например в SSD, расположены настраиваемые сигнальные контакты и их поведение может изменить системный интегратор, это позволяет применять дополнительные меры безопасности, такие как безопасное стирание и уничтожение данных.

Удаленное обслуживание посредством внутриполосной и внеполосной сигнализации

Цель любого системного интегратора — свести к минимуму техническое обслуживание при обеспечении максимальной работоспособности. Планирование технического обслуживания также должно включать планирование непредвиденных аварий. Это означает, что в любой системе IoT для гарантии ее надежности должны быть приняты надлежащие меры, готовые справиться с внезапной потерей функциональности устройством.

Например, у нас есть три фабрики с устройствами, подключенными к центральной облачной службе через установленные внеполосные SSD (рис. 5). При использовании только внутриполосной сигнализации внезапный сбой устройства лишь генерирует уведомление о том, что устройство перестало отправлять данные. Оператору потребуется физический доступ к устройству для запуска соответствующих тестов и самостоятельного устранения проблемы.

Благодаря внеполосному решению можно получить доступ к устройству и запустить диагностику удаленно. Кроме того, у всех внеполосных SSD есть раздел диска, выделенный для восстановления, т. е. образ восстановления для ОС устройства доступен в любое время (рис. 6).

Безопасность микроконтроллера и запоминающих устройств

Устройства хранения с внеполосной сигнализацией необходимы для обеспечения безопасности данных по двум направлениям: локальные данные и облачная передача данных.

Для локально хранящихся данных есть несколько вариантов обеспечения безопасности. Например, в таких устройствах, как InnoAGE SSD компании Innodisk, доступно шифрование AES (Advanced Encryption Standard) с помощью встроенного механизма. Этот механизм гарантирует, что все данные, поступающие во флэш-память NAND, зашифрованы с помощью недоступного ключа. Добавив систему управления безопасностью, можно легко настроить пользовательскую систему с различными уровнями допуска и доступа.

Для критически важных приложений также есть варианты безопасного стирания и уничтожения данных. Этот процесс можно запустить удаленно, как по внутриполосным, так и по внеполосным каналам, чтобы быстро удалить или уничтожить данные, которые могут скомпрометировать компанию.

Второй уровень — это безопасность передачи данных в облако. Azure Sphere включает многогранную систему безопасности, гарантирующую жесткую защиту данных, находящихся между облачными службами и микроконтроллером.

ЗАКЛЮЧЕНИЕ

Твердотельные накопители с современным ПО и встроенными микроконтроллерами, такие как InnoAGE SSD компании Innodisk, оснащенные Azure Sphere корпорации Microsoft, предоставляют системным интеграторам эффективный способ решения ряда серьезных проблем «Интернета вещей». Включение в InnoAGE SSD внеполосной сигнализации позволяет значительно упростить управление и обслуживание накопителей при сохранении безопасности на периферии на самом высоком уровне. Такие решения с поддержкой внеполосного управления могут обеспечить светлое будущее для постоянно растущего числа подключенных устройств, а также снизить общие затраты на поддержку и техническое обслуживание для операторов IoT-систем. ⬣

ЛИТЕРАТУРА

1. Avoiding IoT Downtime and Cost Overruns with Secure Out-of-band Signaling. White Paper. January 2020 Innodisk Corporation. www.techonline.com/tech-papers/avoiding-iot-downtime-and-cost-overruns-with-secure-out-of-band-signaling.
2. Что такое Azure Sphere. https://docs.microsoft.com/ru-ru/azure-sphere/product-overview/what-is-azure-sphere.
3. Third-Party Maintenance Providers. www.gartner.com/en/documents/3871235.
4. Stack T. Data Center. Internet of Things (IoT) Data Continues to Explode Exponentially. Who Is Using That Data and How? https://blogs.cisco.com/datacenter/internet-of-things-iot-data-continues-to-explode-exponentially-who-is-using-that-data-and-how.
5. Azure Sphere. Unlock the value of IoT with confidence in your device security. https://azure.microsoft.com/en-us/services/azure-sphere/.
6. What is Azure Sphere? https://docs.microsoft.com/en-us/azure-sphere/product-overview/what-is-azure-sphere.
7. Future of IoT. https://invest-india-revamp-static-files.s3.ap-south-1.amazonaws.com/s3fs-public/2019-06/EY-future-of-Iot.pdf.
8. Three Ways the IoT Is Changing Field Service. www.zinier.com/2019/03/20/three-ways-the-iot-is-changing-field-service.

РИС. 6. ▶ SSD, разбитый на разделы для реализации возможности восстановления в будущем