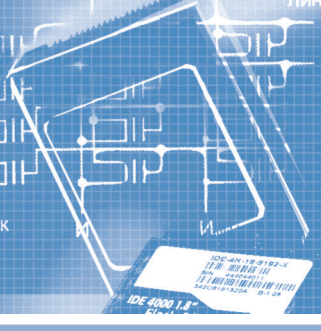




InnoAGE SSD – ИННОВАЦИОННЫЙ ПОДХОД Innodisk к Интернету вещей

Анна Клекот

Каждый год к Интернету вещей подключаются миллиарды новых устройств, поэтому защитить устройства теперь важнее, чем когда-либо. InnoAGE SSD с поддержкой Azure Sphere поможет обеспечить безопасность данных и инфраструктуры, а также конфиденциальность и физическую безопасность. Это комплексное решение для устройств Интернета вещей создано на основе многолетнего опыта в области аппаратного и программного обеспечения, а также облачных технологий компаний Innodisk и Microsoft.

ВВЕДЕНИЕ

В общем понимании Интернет вещей (IoT) – это концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключаяющие из части действий и операций необходимость участия человека. Для компаний, стремящихся к цифровизации, Интернет вещей может быть чрезвычайно выгодным с точки зрения оптимизации процессов и сбора данных, что часто упрощает управление и позволяет значительно снизить затраты.

Однако зачастую трудности, вызванные увеличением количества устройств и относительным сокращением числа людей (операторов), игнорируются.

Имеется в виду, что увеличение количества IoT-устройств обязательно будет сопровождаться ростом затрат на техническое обслуживание, а также появлением риска простоя и неэффективного управления, как отдельных частей, так и системы в целом.

По данным Gartner, до 80% расходов на ИТ приходится на период после первоначальных вложений, при этом простои и техническое обслуживание считаются самыми дорогими. К счастью, системы управления могут значительно уменьшить эти проблемы. Система пре-

доставляет пользователю полную картину работы устройств, позволяет совершать удалённое резервное копирование и восстановление, а также предлагает дальнейшие сценарии работы с оборудованием. В результате многие компании внедряли такую систему управления на базе программного обеспечения своих устройств. Однако все эти функции основаны на рискованном предположении, что само устройство остаётся работоспособным. В тех случаях, когда компьютер выходит из строя, подобные системы управления больше не могут получать доступ к устройству. Следовательно, единственное решение – отправить техника, чтобы устранить неисправность вручную, – дорогостоящее и трудоёмкое решение, которое просто неприемлемо

в мире, где количество устройств, подключённых к Интернету, растёт экспоненциально.

В статье объясняется, как устройства хранения данных могут решить эти проблемы путём использования независимого подключения к накопителю по Wi-Fi-каналу, получения данных и возможности управления ими при помощи микроконтроллера (MCU – Microcontroller Unit), встроенного в твердотельный накопитель (SSD – Solid State Disk).

ПОДКЛЮЧЕНИЕ К НАКОПИТЕЛЮ

Как все мы знаем, твердотельные накопители без проблем можно подключить к компьютеру с помощью различных интерфейсов на материнской плате, таких как SATA, M.2, mPCIe, или да-

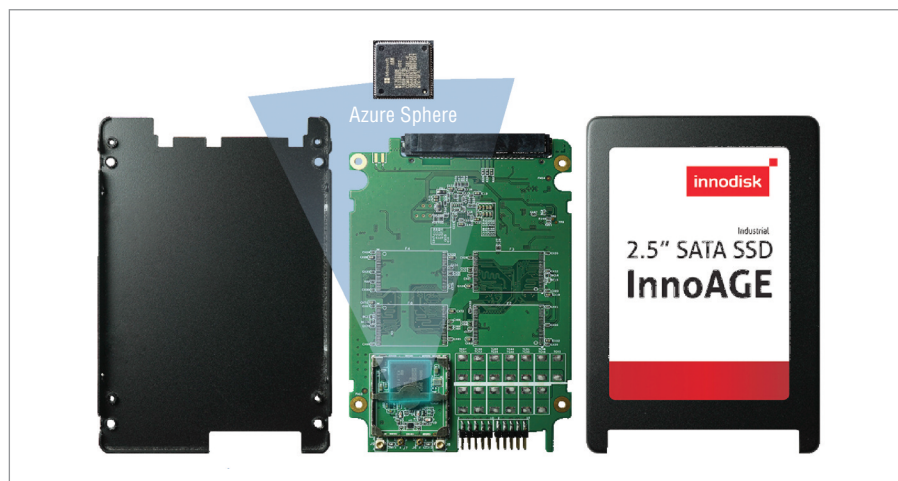


Рис. 1. Демонстрация твердотельного накопителя InnoAGE со встроенным контроллером Azure Sphere

же через USB. Однако при использовании такого способа подключения доступ к данным, хранящимся на SSD, будет возможен только при исправно работающем компьютере, включая операционную систему.

Компания Innodisk предлагает решение, позволяющее подключиться к данным в обход системы с помощью независимого канала связи.

Благодаря передовой запатентованной технологии InnoAGE SSD пользователь всегда может выполнять такие команды на накопителе, как восстановление, резервное копирование и безопасное стирание, вне зависимости от исправности платформы и наличия или отсутствия доступа к самой системе.

Это стало возможным в результате сочетания технологии InnoAGE SSD с передовым микроконтроллером MT3620, оснащённым локальными интерфейсами — цифровым вводом-выводом для управления диском и каналами Wi-Fi и Ethernet для передачи данных в облако, в частности, Azure Cloud (рис. 1).

Аппаратная поддержка

Если рассмотреть используемый Innodisk MCU, то мы увидим, что он оснащён процессором приложений Arm Cortex-A7, работающим на частоте до 500 МГц, и включает в себя большой кэш L1 и L2, а также интегрированную память SRAM для высокоэффективной работы. Две подсистемы ввода-вывода общего назначения, построенные на Arm Cortex-M4F с частотой работы до 200 МГц, поддерживают требования многих периферийных устройств на кристалле, включая 5×UART / I²C / SPI, 2×I²S, 8×ADC, до 12 счётчиков PWM и до 72 GPIO, что позволяет использовать самые различные возможности. Эти две подсистемы ввода-вывода Cortex-M4F в первую очередь предназначены для поддержки обработки ввода-вывода в реальном времени, но также могут использоваться для вычислений общего назначения и управления.

Помимо этих трёх ядер, доступных конечному пользователю, микропроцессор содержит изолированную подсистему безопасности с собственным ядром Arm Cortex-M4F, которое обеспечивает безопасную загрузку и работу системы.

Кроме того, двухдиапазонная радиосистема Wi-Fi 802.11a/b/g/n 1×1 управляется выделенным 32-разрядным ядром RISC Andes N9. Эта подсистема содержит радиосвязь, основную полосу

частот и MAC (Medium Access Control — протокол управления доступом к среде передачи) и предназначена для приложений с высокой пропускной способностью и повышенной энергоэффективностью.

Функции безопасности MCU и работа в сети Wi-Fi изолированы от приложений конечных пользователей и работают независимо от них. Конечным пользователям напрямую доступны только аппаратные функции, поддерживаемые InnoAGE SSD. Таким образом, функции безопасности и Wi-Fi доступны только через определённые API-интерфейсы Azure Sphere и устойчивы к ошибкам программирования в приложениях конечных пользователей, независимо от того, работают ли эти приложения на ядрах Cortex-A7 или доступных для пользователя ядрах Cortex-M4F.

Microsoft предоставляет мощную среду, которую в полной мере использует приложение InnoAGE SSD.

Управление и обслуживание

На сегодняшний день уже видно, что тенденция к увеличению количества IoT-устройств по отношению к числу операторов развивается в прогрессии (рис. 2), и, в то время как количество людей, обслуживающих системы, уменьшается, количество Интернет-вещей значительно увеличивается, — это показано на рис. 2. Данная ситуация приводит к затруднениям в возможности осуществлять полный контроль над всей системой, прогнозировать неисправности, поэтому становится практически невозможным эффективное управление, что подвергает систему риску непредвиденного простоя.

Это подводит нас ко второй части проблемы управления IoT: чтобы собирать данные с пользовательского IoT-устройства, оно должно быть работоспособно, с функционирующей операционной системой устройства. Это означает, что, как только устройство даёт сбой или произошёл сбой ОС, системный интегратор должен отправить сотрудника к устройству. Большинство систем управления, доступных сегодня на рынке, не решают эту проблему или предлагают только частичные решения.

Неправильное обслуживание приводит к значительным расходам, понесённым предприятием, к примеру, торговый автомат, который внезапно перестаёт работать, из-за чего данное

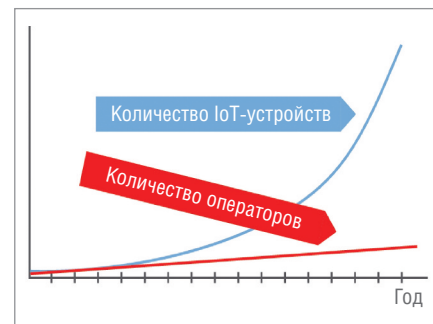


Рис. 2. Соотношение количества IoT-устройств и операторов

устройство не приносит прибыль во время его простоя. Нельзя забывать и про дополнительные расходы, возникшие в связи с необходимостью посещения объекта квалифицированным сотрудником для решения выявленной проблемы, и, в худшем случае, связанные с заменой вышедшего из строя оборудования. В масштабе компании, которая управляет десятками тысяч торговых автоматов, такого рода проблемы приводят к непомерным расходам. На основе изложенного можно сформулировать фундаментальные требования к эффективному Интернету вещей в плане обслуживания, а именно: доступность и быстрое восстановление системы. Устройство должно быть легкодоступным, даже если система выйдет из строя. Также необходимо обеспечить определённый уровень прогнозирования для предотвращения будущих сбоев и обеспечения эффективного и своевременного обслуживания. И в заключение можно сказать, что если система выйдет из строя, необходимы доступные инструменты для быстрого исправления и восстановления системы, желательно без выезда специалиста к неисправному устройству.

Безопасность

Чем больше устройств взаимодействует в сети, тем больше данных поступает от них и тем более эффективным должно быть приложение. Использование дополнительного канала связи с устройством даёт положительные результаты и новые возможности для предприятия. Обратной стороной служит то, что с каждым новым устройством, добавленным к сети, появляется ещё одна точка входа, являющаяся потенциальной уязвимостью, которой может воспользоваться злоумышленник.

Компаниям нужен механизм, позволяющий сбалансировать это уравнение и снизить риск за счёт внедрения новой

модели безопасности в дизайн системы. По мере того как ценность подключения возрастает, предприятиям становится необходим механизм для безопасного подключения этих устройств, вводимых в эксплуатацию.

Накопитель серии InnoAGE, используя контроллер Azure Sphere, открывает доступ к Интернету вещей, создавая основу, с которой предприятие может уверенно эксплуатировать свои устройства в любой среде и может быть уверенным в их безопасной работе. Azure Sphere обеспечивает безопасность за счёт объединения возможностей независимого контроллера MCU, операционной системы и облачных сервисов, специально созданных для безопасных приложений Интернета вещей. Azure Sphere поднимает планку для производителей и предприятий, позволяя обеспечить безопасное подключение новых устройств и используя существующие порты на подключённом устройстве. Ключом к безопасности в этих сценариях является то, что непосредственно контроллер Azure Sphere, а не устройство взаимодействует с облаком. Отделив устройство от сети, модуль защиты, включённый в Azure Sphere, может защитить оборудование от атак, гарантировать, что данные передаются только между доверенным облаком и партнёрами по обмену данными с устройством, а также обеспечить целостность и безопасность программного обеспечения модуля и оборудования.

Единая платформа

Первый шаг к обеспечению эффективного управления IoT — собрать все подключённые устройства на единой

платформе, например iCAP™ от Innodisk (рис. 3). Полученные с этих устройств данные должны быть представлены в легкодоступном виде. Этого можно достичь путём предоставления пользователям возможности входа в систему через браузер на компьютере, что позволит иметь доступ к информации независимо от местоположения. Установив пороговые значения для соответствующих параметров, например, температуру или количество циклов записи SSD, система управления также предлагает прогноз возможных отказов диска, что, в свою очередь, упрощает планирование дальнейшей работы с устройствами.

Однако эти фундаментальные аспекты управления IoT по-прежнему оставляют систему уязвимой для внезапных сбоев. Когда система выйдет из строя, удалённого доступа к ней не будет, что делает всю систему управления бесполезной, пока не будет совершён ручной сброс. Вот почему независимый канал связи имеет решающее значение. Особенно важно здесь то, что в случае сбоя устройства или системы у операторов есть возможность быстро вернуть настройки по умолчанию с облачной панели управления.

Для пользователей также предоставляется доступ к настройке встроенных в MCU интерфейсов ввода-вывода общего назначения (GPIO — General-Purpose Input/Output).

Диагностика

Цель любой компании — свести техническое обслуживание к минимуму при обеспечении максимальной работоспособности. Планирование технического обслуживания также должно

включать прогнозирование непредвиденных аварий. Это означает, что любая система IoT должна иметь наготове надёжные меры для восстановления работоспособности при внезапной потере функциональности устройства.

Без независимого канала связи при внезапной неисправности устройства будет выдаваться только уведомление о том, что оно неработоспособно. В результате оператору потребуются физический доступ к устройству для запуска тестирования и устранения проблемы. С помощью решения InnoAGE SSD запустить диагностику можно удалённо. Кроме того, у всех SSD, поддерживающих данную технологию, есть один раздел диска, предназначенный для восстановления ОС устройства, и он также доступен в любое время

Защита информации

Новая технология нацелена на обеспечение безопасности по двум направлениям: локальные данные и непосредственно передача данных в облако.

Для локально хранимых данных существует несколько вариантов обеспечения безопасности. Например, шифрование возможно с помощью встроенного механизма AES в твердотельных накопителях Innodisk серии InnoAGE. Это гарантирует, что все данные, хранящиеся во флэш-памяти NAND, будут зашифрованы с помощью секретного ключа.

Второй слой — безопасность передачи в облако. Azure Sphere позволяет реализовать семь основных свойств, необходимых для надёжной защиты устройств в своей инфраструктуре Интернета вещей.

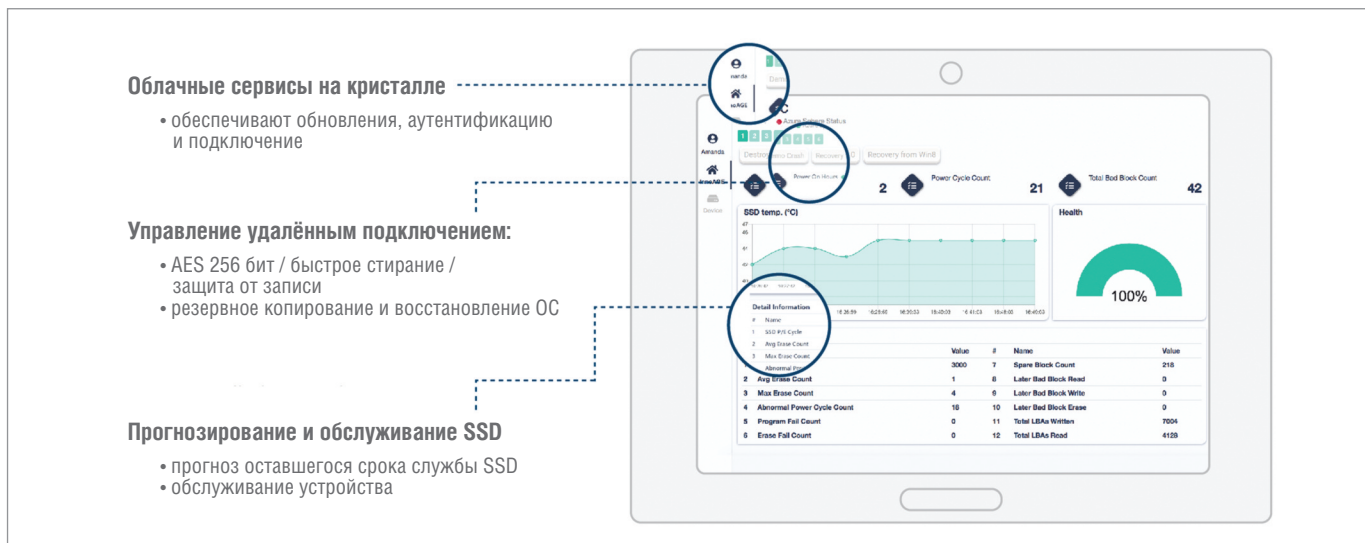


Рис. 3. Скриншот платформы управления InnoAGE SSD

1. Корень доверия на основе оборудования.

Это гарантия того, что на устройстве работает только подлинное актуальное программное обеспечение. Лишь в таком случае устройство сможет подключиться к Интернету.

2. Защита в глубину.

Чем больше уровней защиты, тем сложнее получить доступ к наиболее конфиденциальным секретам устройства. Для более важных областей назначается более высокий уровень защиты.

3. Небольшая доверенная вычислительная база.

Доверенная вычислительная база должна быть по возможности небольшой. Это минимизирует её уязвимость для злоумышленников и снизит вероятность использования ошибок или компонентов для её компрометации.

4. Динамическое обособление.

Границы между компонентами программного обеспечения могут предотвратить распространение нарушения безопасности одного компонента на другие. Динамические границы можно безопасно перемещать и перестраивать.

5. Проверка подлинности на основе сертификата.

Пароли могут быть самым слабым звеном во многих системах безопасности. Проверка подлинности на основе сертификата позволяет управлять устройствами без использования паролей.

6. Отчёты об ошибках.

Раннее обнаружение ошибок, их анализ и реагирование на них крайне важны для устранения угроз до того, как они смогут нанести значительный ущерб.

7. Возобновляемая безопасность.

Возможность развёртывания текущих обновлений программного обеспечения необходима для усиления защиты устройства и устранения уязвимостей.

ОБЪЕДИНЕНИЕ ПРЕИМУЩЕСТВ

Для операторов системы Интернета вещей интеграция всех перечисленных аспектов означает, что у них под рукой будет мощный набор инструментов для решения самых сложных задач. Сделав удалённое обслуживание доступным, подключив интуитивно понятную платформу управления, система IoT становится гораздо более масштабируемой и значительно более лёгкой в поддержке её безотказной работоспособности.

ЗАКЛЮЧЕНИЕ

Твердотельные накопители Innodisk SSD InnoAGE с современным программным обеспечением и встроенным независимым микроконтроллером Microsoft Azure Sphere предоставляют системным интеграторам эффективный способ решения большинства самых серьёзных проблем Интернета вещей. Наличие независимого канала связи может значительно облегчить управление и техническое обслуживание при сохранении безопасности на самом высоком уровне. Результатом является решение, которое обеспечивает надёжную эксплуатацию с постоянным ростом числа устройств в IoT-системах, а также снижение затрат предприятий на обслуживание данных систем.

В скором времени данная концепция построения устойчивых и надёжных решений, по существу, будет являться обязательным требованием при создании систем Интернета вещей. ●

**Автор – сотрудник
фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru**



innodisk

**Новая система хранения данных
Innodisk Fire Shield SSD™ в формате 3,5"**

**Абсолютная сохранность данных при воздействии открытого пламени
при температуре +800°C до 30 минут**

PROSOFT® ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР (495) 234-0636
INFO@PROSOFT.RU WWW.PROSOFT.RU