

# Функции безопасности – важнейший элемент микроконтроллеров для IoT

Рассказывает вице-президент компании Nuvoton П. Ван



Компания Nuvoton Technology, образованная в 2008 году как спин-офф Winbond и унаследовавшая от своей родительской компании множество решений в том числе в области микроконтроллеров, постоянно дополняет ассортимент своей продукции новыми компонентами и решениями, благодаря чему изделия Nuvoton находят широкое применение в вычислительной технике, потребительской, промышленной электронике и других областях. Кроме того, компания обладает собственным кристалльным производством и предлагает услуги фаундри.

Очевидно, компания, одним из ключевых видов продукции которой являются микроконтроллеры, не может оставаться в стороне от такого тренда, как Интернет вещей. Это направление предъявляет свои специфические требования к устройствам в целом и микроконтроллерам в частности. О том, как решения Nuvoton отвечают этим требованиям, а также о перспективах, которые видит для себя компания на российском рынке, на выставке electronica 2018, прошедшей в Мюнхене в ноябре прошлого года, нам рассказал Патрик Ван (Patrick Wang), вице-президент компании Nuvoton.

## Господин Ван, какие новые решения появились у вашей компании в 2018 году?

Для нашей компании 2018 год стал очень важной вехой, поскольку в этом году мы создали новое поколение наших микроконтроллеров общего применения на различных ядрах от 8051 до Cortex-M0, M4, M23 и ARM9, а также микроконтроллер на базе ядра Cortex-M4 с сигнальным процессором для цифровой обработки звука, который позволяет строить на своей основе системы с распознаванием голосовых команд из определенного небольшого набора. При этом распознавание может быть как независимым от голоса конкретного человека, так и с привязкой к индивидуальным особенностям говорящего. Во втором случае обеспечивается персонализация и определенная защищенность системы, поскольку

будут исполняться команды только того человека, который эту систему обучал.

Наша компания уделяет большое внимание безопасности, и мы являемся одним из немногих производителей микроконтроллеров, которые способны объединить в своих изделиях и решения для обеспечения безопасности, и средства аудиообработки. Такая комбинация открывает дополнительные возможности для разработчиков изделий в различных областях, в частности тех, где требуется человеко-машинный интерфейс с управлением голосом.

Мы ожидаем, что эти микроконтроллеры нового поколения будут одним из основных драйверов роста бизнеса нашей компании в течение последующих пяти лет. Полностью линейка нового поколения будет представлена

рынку в 2019 году, а здесь, на выставке electronica 2018 на стенде компании Winbond – родоначальницы Nuvoton, демонстрируется решение на основе нашего нового микроконтроллера NuMicro M2351 – контроллер «умной» двери, замок которой открывается по отпечаткам пальцев. Помимо микроконтроллера M2351, в данном решении применяется защищенная флеш-память W77F32W компании Winbond.

**Судя по обозначению, микроконтроллер NuMicro M2351 основан на ядре Arm Cortex-M23. Это так?**

Да, мы широко используем процессорные ядра и другие IP-блоки Arm и также стараемся приобретать лицензии на использование новейших решений этой компании, чтобы предлагать нашим заказчикам наиболее современные средства. В то же время в наших микроконтроллерах мы применяем и множество собственных IP-решений, ориентированных на удовлетворение потребностей наших клиентов.

Что касается микроконтроллеров серии NuMicro M2351, в их основе – действительно процессорные ядра Arm Cortex-M23. Эти микроконтроллеры способны работать на тактовой частоте до 64 МГц и содержат флеш-память объемом до 512 кБ и память SRAM до 96 кБ.

В данной серии учтены потребности такого быстроразвивающегося направления, как Интернет вещей. Как



Решение для замка «умной» двери на основе микроконтроллера NuMicro M2351, представленное на выставке electronica 2018 на стенде Winbond

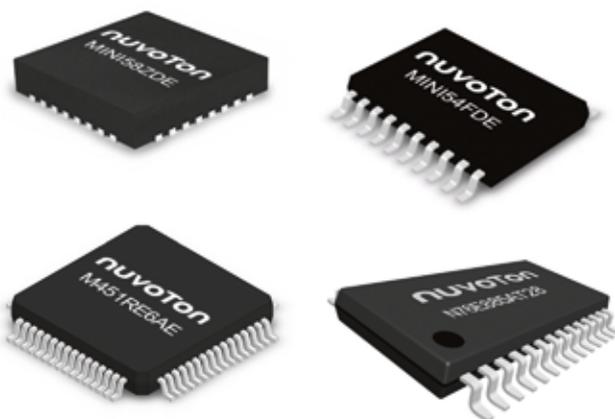
я уже говорил, наша компания уделяет большое внимание вопросу безопасности, защиты данных и протоколов, а для IoT это один из ключевых вопросов: ведь само понятие «Интернет вещей» означает, что устройства объединяются в сеть, общаются между собой, причем для их коммуникации используется множество

**Микроконтроллеры со встроенной аудио обработкой и защитой данных и протоколов**



**Доступные архитектуры**

- ◆ 8051
- ◆ ARM Cortex-M0
- ◆ ARM Cortex-M4
- ◆ ARM Cortex-M23
- ◆ ARM9



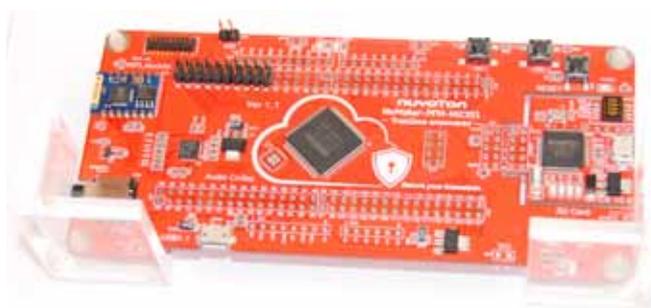
**Закажите образцы:**  
 тел.: (812) 370 60 70 доб. 775  
 e-mail: [memory@macrogroup.ru](mailto:memory@macrogroup.ru)



Официальный партнёр Nuvoton  
 Санкт-Петербург (812) 370 60 70  
 Москва (495) 988 02 72  
 Екатеринбург (343) 385 95 10

e-mail: [memory@macrogroup.ru](mailto:memory@macrogroup.ru)

Ростов-на-Дону (863) 227 03 93  
 Чебоксары (8352) 23 79 55  
 Новосибирск (383) 233 34 87



Макетная плата Nuvoton NuMaker-PFM-M2351 на стенде Winbond на выставке electronica 2018

различных протоколов, как проводных, так и беспроводных. Эти устройства и их «общение» должны быть защищены как от случайных ошибок, так и от злонамеренных действий.

В микроконтроллерах M2351 применяются технология Arm TrustZone для Armv8-M и архитектура безопасности платформы Arm PSA с поддержкой платформы NuSMP (Nuvoton Secure Microcontroller Platform), разработанной нашей компанией. Эта платформа сочетает в себе как аппаратные, так и программные технологии и позволяет обеспечивать выполнение требований по безопасности к микроконтроллерам и общего назначения, и для устройств Интернета вещей. Среди реализуемых с помощью платформы NuSMP задач безопасности – доверенная загрузка (trusted boot), безопасное обновление микропрограммного обеспечения по беспроводным каналам и др.

Упомянутое решение для «умных» дверей, в частности, демонстрирует возможности средств обеспечения безопасности в устройствах на основе серии M2351.

Также стоит отметить, что микроконтроллеры серии M2351 обладают множеством различных встроенных интерфейсов, таких как UART, SPI, I<sup>2</sup>C, USB и интерфейс смарт-карт ISO 7816-3.

#### К основным требованиям к устройствам Интернета вещей также относится обеспечение малого энергопотребления. Как это учитывается в микроконтроллерах Nuvoton?

У нас есть несколько решений и технологий, благодаря которым мы можем достигать малых значений потребляемой мощности как в рабочем режиме, так и в режиме ожидания.

В частности, значение потребляемого микроконтроллерами M2351 тока в обычном режиме работы составляет 97 мкА / МГц в режиме стабилизации с малым падением напряжения (LDO) и 45 мкА / МГц в режиме DC / DC-преобразования, а для экономии энергии в тех случаях, когда микроконтроллер не задействован, предусмотрен не

только режим ожидания с потреблением тока 2,8 мкА, но и режим глубокого энергосбережения (DPD), при котором величина потребляемого тока составляет менее 2 мкА.

#### Предлагаются ли уже средства разработки для новой серии M2351?

Да. Nuvoton предлагает платформы для упрощения разработки изделий на основе различных своих микроконтроллеров. Такая платформа была разработана и на основе микроконтроллера M2351. Ее также можно увидеть на этой выставке на стенде Winbond. Это макетная плата Nuvoton NuMaker-PFM-M2351, на которой имеется программатор Nu-Link-Me; интерфейс, совместимый с Arduino UNO; полноскоростной протокол USB 2.0 с разъемом OTG; слот для карты microSD; безопасная флеш-память с последовательным доступом от Winbond для защищенного хранения данных, в том числе криптографических ключей; аудиокодек с микрофонным входом и выходом для наушников; кнопка сброса и две кнопки, а также два светодиода, назначения которых задаются пользователем; модуль Wi-Fi для беспроводной связи. Иными словами, плата содержит множество возможностей для прототипирования схемотехники и отработки ПО устройств на основе микроконтроллеров M2351, что очень важно для сокращения времени разработки и вывода устройств на рынок.

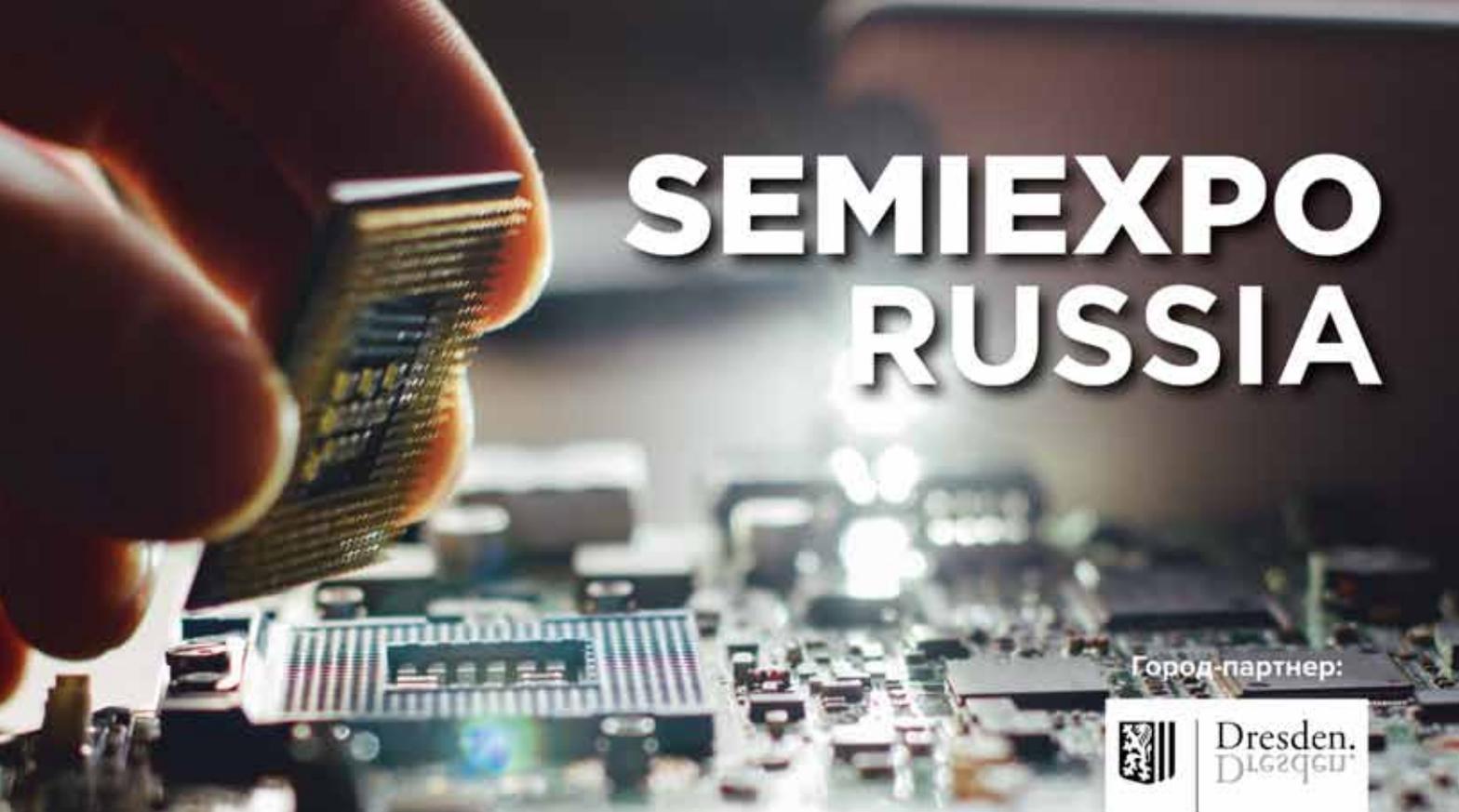
#### В заключение расскажите, пожалуйста, какой потенциал вы видите для вашей компании на российском рынке.

Хотя наш бизнес в России пока небольшой, его динамика очень вдохновляющая: в 2018 году мы наблюдаем рост доходов от российского рынка порядка 64%. Так что, российский рынок обладает большим потенциалом для нас, и продолжать вкладываться в развитие бизнеса в России для нас разумно. В этом нам будут помогать наши партнеры, в том числе компания Макро Групп.

Среди областей, обладающих хорошими возможностями в вашей стране, – аэрокосмическая, оборонная отрасли, а также телекоммуникационная аппаратура, промышленная и автомобильная электроника. Эти области обладают своими специфическими требованиями к применяемым компонентам, и у нас есть решения, которые эти требования способны удовлетворить. Мы выпускаем изделия с расширенным диапазоном рабочих температур, напряжений, с развитыми функциями по обеспечению безопасности. Также у нас есть решения, сертифицированные в соответствии со стандартом AEC-Q100 для применения в автомобильной отрасли.

#### Спасибо за интересный рассказ.

С П. Ваном беседовал Ю. Ковалевский



# SEMIEXPO RUSSIA

Город-партнер:



Dresden.  
Dresdener

ОТРАСЛЕВЫЕ ОБЗОРЫ СОТРУДНИЧЕСТВО БИЗНЕС ИННОВАЦИИ

**ВЫСТАВКА И КОНФЕРЕНЦИЯ  
ПО ТЕХНОЛОГИЯМ, МАТЕРИАЛАМ,  
СТАНДАРТАМ И ОБОРУДОВАНИЮ  
В ОБЛАСТИ МИКРОЭЛЕКТРОНИКИ**

МОСКВА ЦВК «ЭКСПОЦЕНТР» 14-15 МАЯ 2019 SEMIEXPO.RU