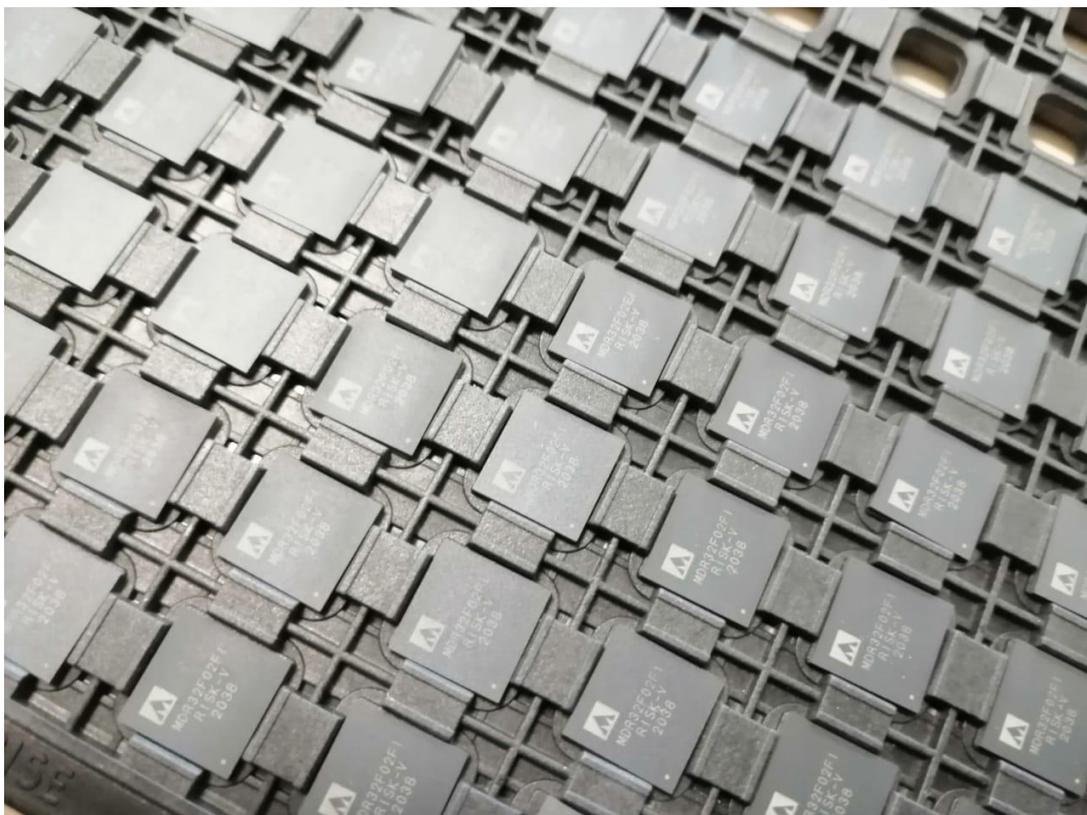


Отечественный микроконтроллер K1986BK025 на базе процессорного ядра RISC-V для приборов учета электроэнергии

Добро пожаловать в эпоху RISC-V!

Решения на базе открытого стандарта системы команд RISC-V всё чаще появляются на рынке. Уже в серийном производстве микроконтроллеры от китайских коллег, интересные решения предлагает Microchip с FPGA на борту. Растет экосистема ПО и средств разработки для данной архитектуры. Кажущиеся ранее непоколебимыми лидеры все чаще встречаются в объявлениях о перепродаже, а молодые стартапы привлекают многомиллионные инвестиции. Компания Миландр так же ввязалась в эту гонку и сегодня начала поставку заинтересованным предприятиям инженерных образцов своего нового микроконтроллера K1986BK025 на базе процессорного ядра RISC-V для приборов учета электроэнергии. В общем картинки, характеристики и прочая информация, а так же немного хайпа под катом.



Что такое RISC-V? Слава великому Хабру и его пользователям, которые уже написали много статей по данной теме, и избавили меня от этой участи. Посмотрите [RISC-V с нуля](#). Так же можно ознакомиться с уже серийными изделиями от [GigaDevice](#). А так же с критикой и описанием [недостатков RISC-](#)

У архитектуры со стороны сотрудников ARM.

Микроконтроллер K1986BK025 на базе ядра RISC-V это второе поколение Миландровских микроконтроллеров для счетчиков электроэнергии. Первое поколение — микросхемы K1986BK2x разработаны на базе процессорного ядра ARM Cortex-M0 и выпускаются уже более 5 лет. На их основе сейчас выпускаются счетчики Милур.

Но время не стоит на месте и новые правила рынка диктуют новые требования к микросхемам. Нужно сделать больше функций — новые требования по минимальному функционалу приборов учета. Нужно попасть в требуемую цену, так как конкурировать придется с монстрами типа TI и NXP. Так же, если вы следите за этим направлением, то знаете, что новые «интеллектуальные» счетчики электроэнергии могут ~~отключать электричество~~ ограничивать потребление электроэнергии. А это значит новая система должна обеспечивать и информационную безопасность, чтобы злоумышленники не могли отключить или наоборот включить электричество по своему усмотрению. Все это привело к появлению новой микросхемы K1986BK025, о которой сейчас и расскажем.

1. Основные характеристики K1986BK025

Процессорное ядро — RISC-V (BM-310S CloudBEAR)

Тактовая частота — 60 МГц

Напряжение питания (основное) 2,2...3,6В

Напряжение питания (АЦП) 3,0...3,6В

Напряжение питание (батареиное) 1,8...3,6В

Объем памяти программ Flash — 256+8 Кбайт

Объем памяти ОЗУ — 112 Кбайт

Объем однократно-программируемой ПЗУ — 16 Кбайт

Метрологический измерительный АЦП — сигма-дельта 24 бита, 7 каналов

Аппаратный блок вычисления показаний потребляемой энергии

Инструментальный АЦП — 10 бит с датчиком температуры

Интерфейсы — 5xUART, 3xSPI, 1xI2C

Число пользовательских выводов — 55

Батарейный домен объемом 512 байт с часами реального времени и детектором фиксации проникновения

4 блока 32-разрядных таймеров с 4 каналами захвата событий и ШИМ

Сторожевой таймер

Блок подсчета CRC с изменяемым полиномом

Блок поддержки вычисления симметричных криптографических алгоритмов

Блок генератора случайных чисел

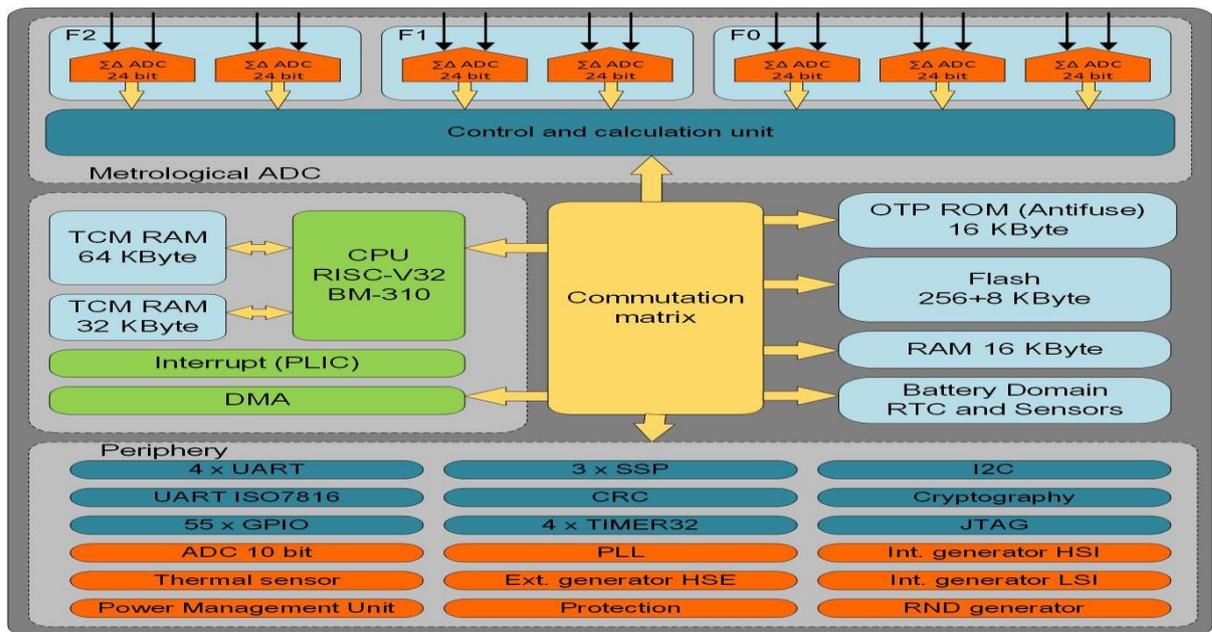
Блок детектора изменения тактовой частоты

Блок детектора изменения напряжения питания (основного и батарейного)

Блок оптического детектора

Блок генерации шума в цепи питания
 Защитная экранная сетка
 Интерфейс отладки — JTAG
 Тип корпуса — QFN88 (10 x 10 мм)
 Рабочая температура от минус 50С до +85С

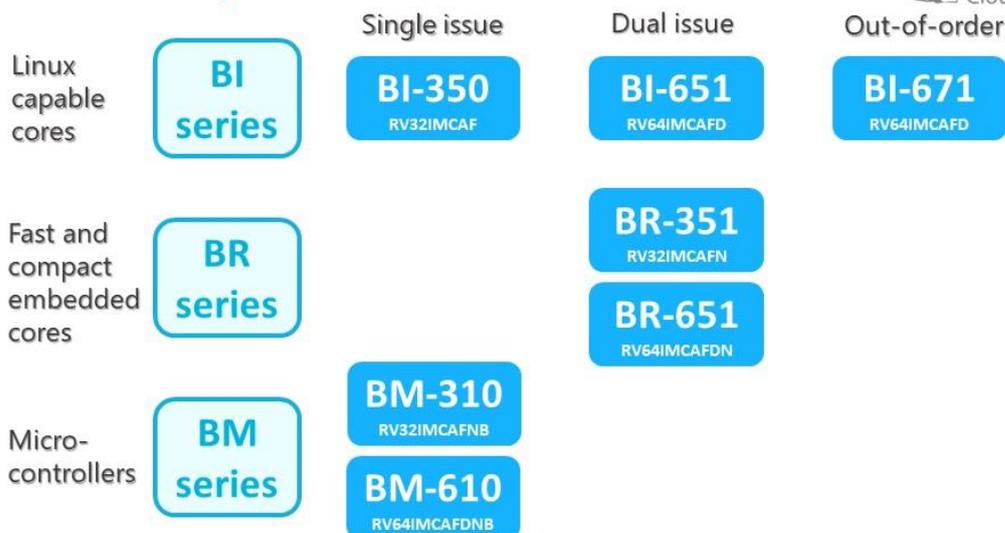
Структурная схема:



2. Процессорное ядро

Как уже было отмечено, сердцем микросхемы является 32 битное процессорное ядро RISC-V (в конфигурации RV32IMC) с обозначением BM-310, которое было разработано нашими хорошими друзьями из компании [CloudBEAR](#). Это не единственное их процессорное ядро. Ребята предлагают целую линейку ядер, начиная от небольших микроконтроллерных ядер и заканчивая высокопроизводительными 64 битными многопроцессорными кластерами.

RISC-V 32/64-bit cores

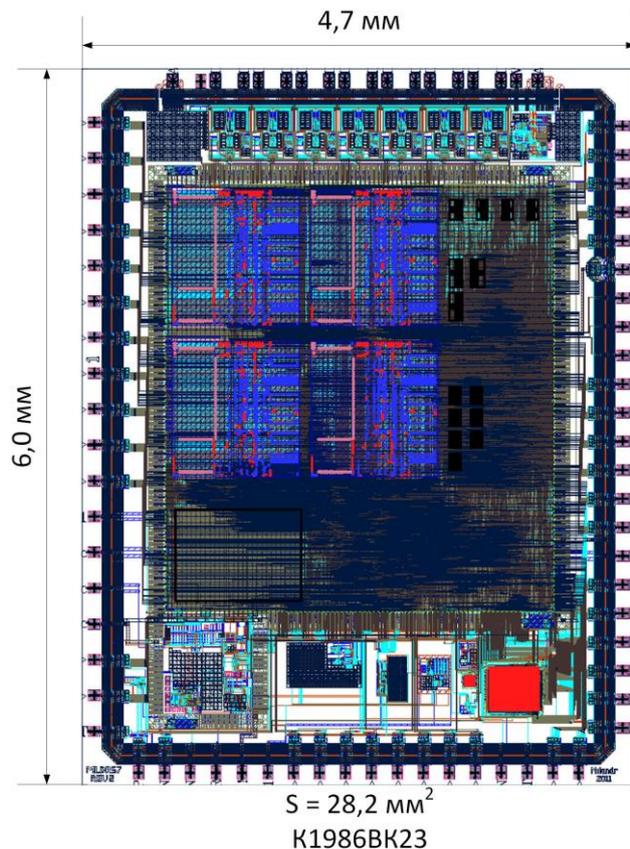
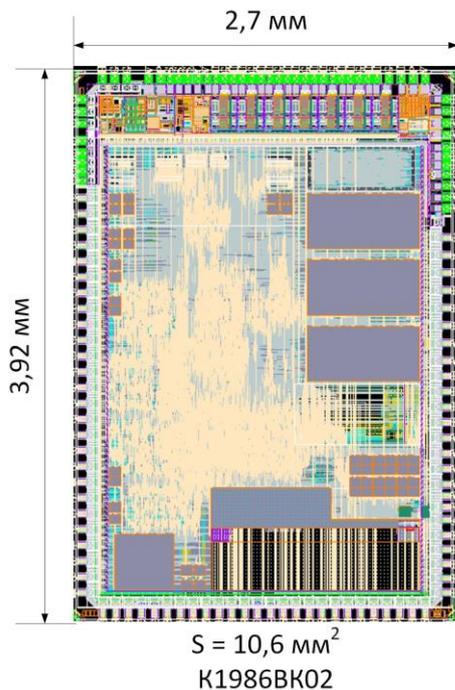


Компания Миландр ведет разработку новых продуктов на базе ядер из всех весовых категорий портфолио CloudBEAR. В кремнии сейчас доступны только K1986BK025 на базе ядра BM-310. Но и другие продукты, в том числе на базе 64 битных ядер скоро увидят свет. Ядро BM-310 это 32 битное RISC-V ядро с трехстадийным конвейером, с возможностью выполнения операции умножения за два такта. Поддержка операций с плавающей запятой в данной версии микросхемы не была реализована (хотя ядро позволяет это реализовать). Производительность ядра BM-310 на тесте CoreMark составляет 3,0 CoreMark/МГц. Таким образом его можно сравнить с ARM Cortex-M3. При этом ядро в новой микросхеме занимает всего 0,3 мм². А с учетом того, что большинство задач по вычислению параметров потребления электроэнергии выполняются аппаратно контроллером метрологического АЦП, то основная вычислительная мощность ядра может использоваться для коммуникационных задач в приборе учета.

3. Цена

Цена — один из основных критериев для микросхемы. Основной вклад в стоимость микросхемы вносит кристалл. Чем больше его площадь — тем дороже, чем более сложная технология изготовления — тем он тоже дороже. Но при этом, чем более сложная технология, тем на меньшей площади можно реализовать требуемый функционал, а значит будет дешевле. В общем выбор технологии не всегда очевиден. Микросхемы первого поколения K1986BK2x были разработаны на 180 нм. Примерно треть кристалла относилось к аналоговой части (собственно сами сигма-дельта АЦП, питание, IO) и при переходе на более тонкие процессы эта часть практически не уменьшается. Но в соответствии с новыми требованиями, объем функционала должен быть увеличен практически в 4 раза. В новой микросхеме реализовано 256 Кбайт Flash против 64К, ОЗУ 112Кбайт против 16К, 5 блоков UART против 2, 3 блока SPI против 1 и еще криптография... В общем, после

долгих прикидок и расчетов было принято решение, что если уделить особое внимание площади, то на технологии 90 нм можно попасть в требуемый коридор стоимости, на технологиях 65 нм или ниже было бы легче, но большие затраты на разработку в целом сделали бы проект более рискованным по финансам.



В результате мы получили действительно компактный кристалл, который по площади более чем в 2 раза меньше предыдущего. И хотя изначально были и более амбициозные планы уменьшить кристалл до 8 мм^2 , полученный результат тоже очень хорош. Именно из-за амбиций форма кристалла получилась прямоугольной, а не квадратной. Верхняя часть кристалла отдана под аналоговые блоки, и ее топологию прорисовывали отдельно под изначально планируемые размеры, а когда стало понятно, что цифра не влезет, то кристалл стал «расти» в прямоугольник. Та же картина была и с микросхемами первого поколения. Постоянство — признак мастерства.

4. Метрологический АЦП

Если процессорное ядро это сердце микроконтроллера, то метрологический АЦП это его мозг, так как именно он определяет предназначение микросхемы. В микроконтроллере реализован блок из 7 каналов 24 битных $\Sigma\Delta$ АЦП. Все каналы разбиты на три пары F0-F2 (канал напряжения и канал тока) для 3-х фазной сети и еще одного независимого канала тока (отнесен к F0). Каждый из 7 каналов

оцифровывает входной сигнал с выходной частотой отсчетов до 16 кГц. Кроме этого, в каждой паре каналов F0-F2 реализована возможность рассчитывать среднеквадратические значения тока/напряжения, вычислять активную и реактивную мощности, вычислять потребленную активную и реактивную энергию, частоту сигнала в каналах напряжения, превышение пикового значения, падение сигнала ниже установленного уровня. Эти дополнительные блоки позволяют снизить нагрузку на процессор, что в свою очередь снижает потребляемую мощность всего кристалла. Так же каждый АЦП имеет независимый канал DMA, обеспечивая возможность сохранения данных в ОЗУ без участия процессора.

Список основных параметров и возможностей блока сигма-дельта АЦП:

- 7 независимых АЦП с выходной частотой отсчетов 4/8/16 кГц (4 канала тока и 3 канала напряжения). Эти каналы образуют 3 блока для измерения параметров каждой фазы F0-F2.
- В блоке каналов F0 реализуем автоматический выбор канала тока (который имеет максимальное значение) для последующих расчетов мощностных характеристик. Если разница токов превышает 6%, то формируется прерывание. Кроме этой функции в остальных блоках F0-F2 идентичны.
- Все каналы АЦП имеют независимые калибровочные коэффициенты наклона характеристики.
- Каждый канал тока имеет независимый интегратор.
- В каждом блоке АЦП (F0-F2) независимо рассчитывается период сигнала по каналу напряжения. Количество периодов, в течение которого рассчитывается эта величина, можно задавать равным 1/2/4/8/16/32/64/128 периодам.
- В каждом блоке есть проверка на пропадание периодического сигнала в канале напряжения.
- В каждом блоке проверяется «просадка» напряжения ниже заданного уровня, а так же превышения сигнала в каналах тока и напряжения установленного лимита.
- Есть возможность скорректировать фазы сигналов в каналах напряжения с точностью до 0,02%.
- Вычисляются среднеквадратические, квадрат среднеквадратических значений токов и напряжений, а так же их независимая калибровка.
- При вычислении активной и реактивной энергии значение накопленной энергии в течение периода сохраняется в отдельных регистрах (для положительной и отрицательной энергии).
- Вычисляются полная мощность и полная энергия.
- Вычисляется сдвиг фаз по отношению к фазе 0.

Таким образом, основные функции по расчету потребленной энергии выполняются с минимальным участием процессора.

5. Информационная безопасность

Как уже было отмечено ранее новые интеллектуальные счетчики электроэнергии должны уметь отключать потребителя от сети по соответствующей команде. Так же передача показаний потребленной энергии осуществляется автоматически по различным каналам связи. А это значит что вопросы информационной безопасности будут стоять особенно остро. В Постановление Правительства РФ от 19.06.2020 N 890 "[О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии \(мощности\)](#)" ([вместе с «Правилами предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии \(мощности\)»](#)) сформулированы минимальные функциональные требования для приборов учета электроэнергии. Но в части информационной безопасности они пока не сформулированы (ожидаются до конца 2020 года). Поэтому при разработке микросхемы мы опирались на [требования ФСБ к средствам криптографической защиты информации для некорректируемых регистраторов \(СКЗИ ИР\)](#). Реализованный функционал на наш взгляд избыточен, а если где-то и что-то и не предусмотрели, то можно реализовать это программно. Но в любом случае — в части обеспечения специальных требований микросхема находится на уровне карточных и паспортных чипов. Поэтому в данной микросхеме реализуются все требования необходимые для бытовых электросчетчиков как в части собственно задач измерения, так и в части информационной безопасности, она может найти свое применение и в других областях — тахографах, электронных пломбах, идентификации и аутентификации элементов IoT. Всю «спецуху» в микросхеме можно разделить на две части — криптография и инженерная защита.

5.1. Криптография

На микросхеме реализовано всё для защиты информации по ГОСТ Р 58940-2020 (СПОДЭС), в том числе:

- Блоки сопроцессоров для поддержки блочных шифров «Кузнечик», «Магма» и AES;
- Блок генератора случайных чисел;
- Блок вычисления CRC по произвольному полиному;
- Блок специальной энергозависимой памяти ключевой информации с батарейным питанием
- Однократно программируемая ПЗУ первоначального загрузчика, в которой реализуется уникальная идентификация каждой микросхемы.

Симметричная криптография реализуется на базе сопроцессоров, которые ускоряет самые тяжёлые операции. Это позволяет получить скорость шифрования с пиковой производительностью до 10 Мбит/с. При необходимости алгоритмы

асимметричной криптографии реализуется программным путем. В общем про идентификацию, аутентификацию шифрование, обновление прошивок нужно писать отдельную статью, что и сделаем потом.

5.2. Инженерная защита

Для затруднения различных инженерных методов воздействия как на сам счетчик электроэнергии, так и на отдельно микросхему реализованы специальные методы инженерной защиты:

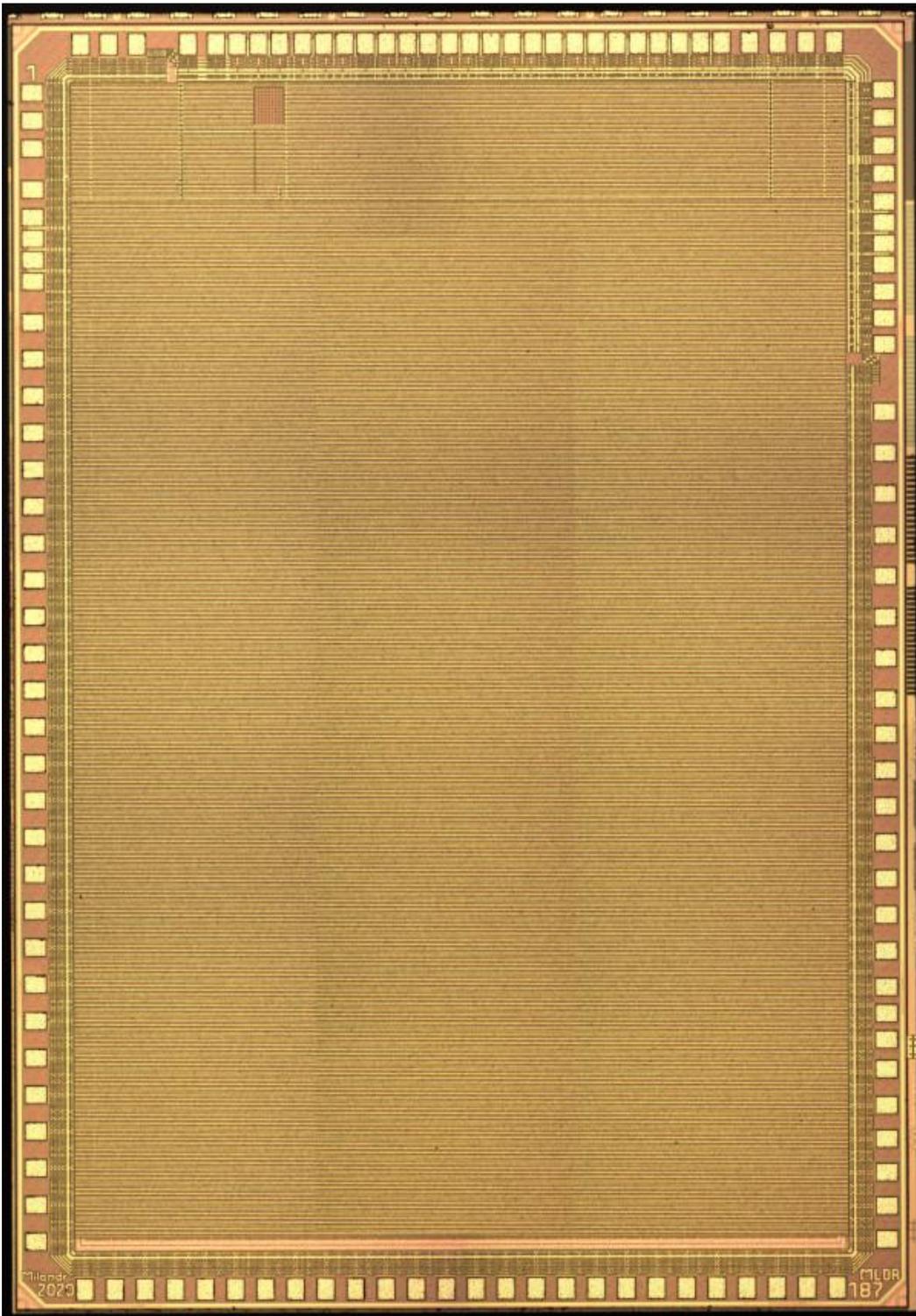
- 3 вывода для детекторов проникновения (электронные пломбы)
- Блок детектора изменения тактовой частоты
- Блок детектора изменения напряжения питания
- Блок оптического детектора
- Блок генерации шума в цепи питания
- Защитная экранная сетка
- Защита от несанкционированного считывания памяти

Выводы для детекторов проникновения — это три отдельных вывода микроконтроллера через которые фиксируются сигналы от внешних электронных пломб, даже в случае отсутствия питания. Таким образом, какие-либо попытки механического воздействия на счетчик будут обнаружены и зафиксированы. Кроме механизмов защиты корпуса прибора реализуется методы защиты уже самой микросхемы от более изощренных атак.

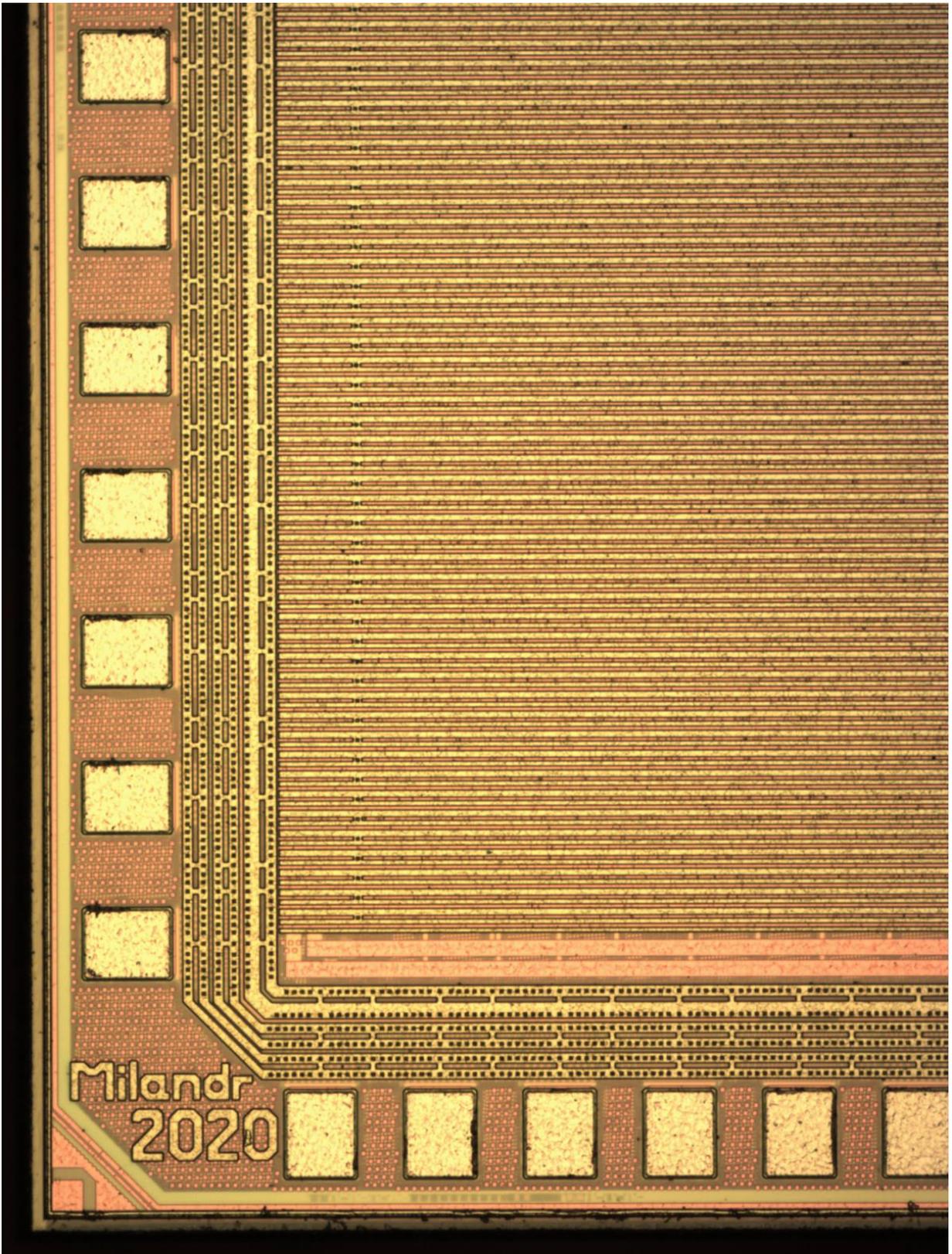
Для исключения ситуации с «разгоном» или наоборот «торможением» тактовой частоты процессора реализован детектор изменения частоты, который непрерывно сравнивает внешний источник тактирования с внутренним RC генератором. И при возникновении отклонений выходящих за заданные границы фиксирует это событие или может переключить микросхему на внутренний (реализован на кристалле) аварийный источник тактирования. «Гличивание» сигнала тактирования парируется системой фильтрации входного сигнала. Для корректного запуска микросхем по включению основного питания, а также обнаружения факта выхода питания из допустимых диапазонов реализован блок детектора напряжения. Так же блок обеспечивает контроль уровня заряда батарейки, на которой работает микросхема при отсутствии основного питания. Таким образом исключаются какие-либо манипуляции или попытки сбить работу микросхемы через питающие напряжения. Для исключения утечки ключевой информации по «паразитным» каналам, например цепям питания (подробнее [можно почитать тут](#)) в микросхеме реализован блок зашумления основного питания с помощью псевдослучайного генератора. Блок формирует случайным образом изменяемое дополнительное потребление, маскируя основной профиль потребления. Для противодействия более серьезным полу-

инвазивным и инвазивным атакам (атака на микросхему когда есть доступ к кристаллу микросхемы или даже отдельным цепям кристалла) реализован оптический детектор. Так как обычно кристалл микросхемы в корпусе, то доступ света к нему невозможен. Если же корпус микросхемы вскрыт и на кристалл попадает свет, то оптический датчик сформирует сигнал тревоги. Если же злоумышленник прошел еще дальше, то для ограничения доступа к внутренним цепям микросхемы в верхних слоях топологии кристалла реализована защитная сетка, в которой перемежаются цепи земли, питания и информационная цепь, по которой передается случайный полином. Кстати именно поэтому в верхних картинках приведен рисунок топологии из САПР, а не реальная фотография кристалла.

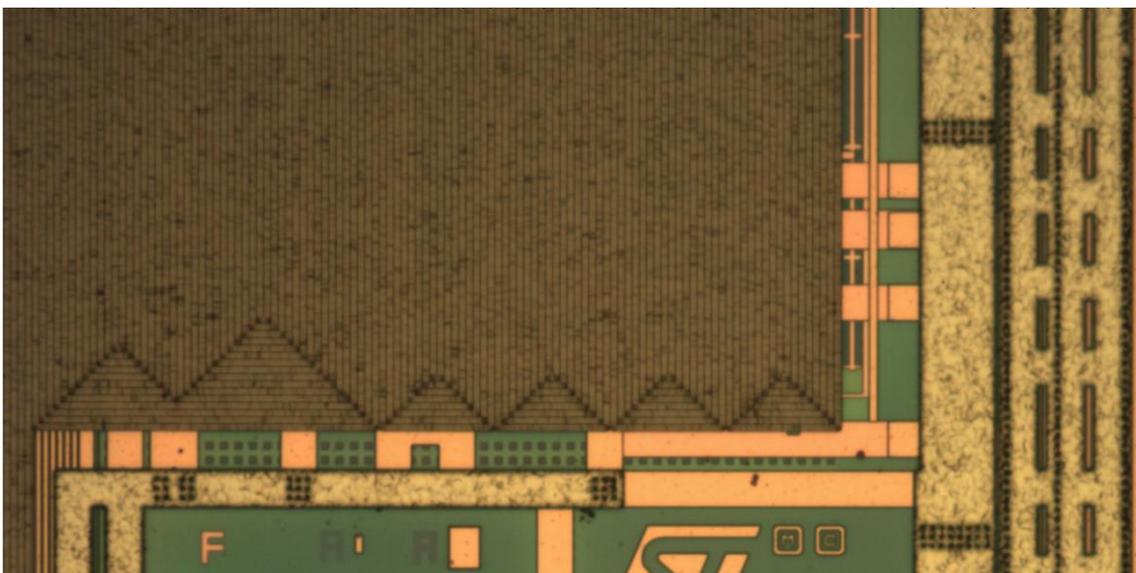
Так как реальная фотография кристалла выглядит вот так.



Или чуть поближе:



Для сравнения как защитная сетка выглядит в чипе для карточек от ST (серия ST23).

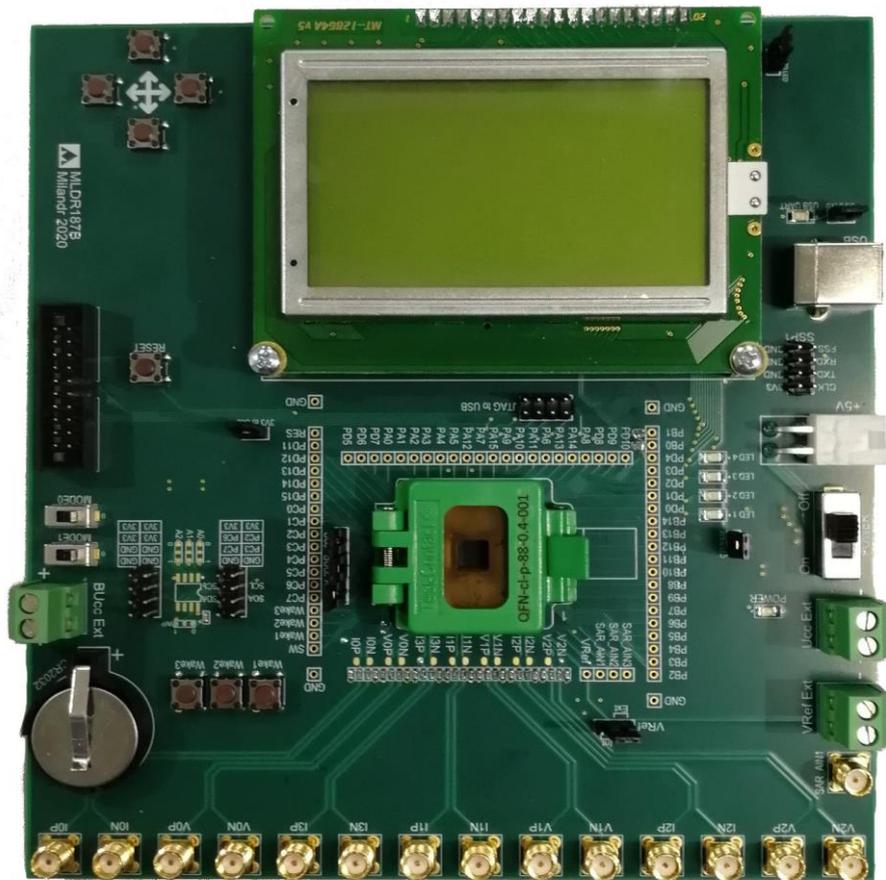


В случае физического нарушения целостности сетки так же формируется сигнал тревоги. Программное обеспечение должно контролировать все сигналы тревоги и в случае их возникновения фиксировать факт атаки. Так же микросхема может быть настроена так, что бы криптографическая ключевая информация была автоматически стерта, при обнаружении фактов атаки. Все это требует обеспечения доверенности ПО. Для пользовательской программы в микросхеме реализовано 16 Кбайт однократно программируемой ПЗУ (по принципу анти-фьюз) и 256+8 Кбайт перепрограммируемой Flash. Запуск микросхемы происходит из встроенной однократно программируемой памяти. Изначально при изготовлении микросхем, данная память чистая, и для серийных изделий загрузка стартового доверенного загрузчика будет происходить при тестировании и отбраковке. Это позволяет обеспечить уникальную идентификацию каждой микросхемы, гарантировать целостность метрологического и криптографического ПО и стартовый загрузчик является корнем доверия для пользовательской программы, исполняемой из Flash. А так же при необходимости обеспечить защиту от считывания пользовательской программы во Flash. На время исследования для инженерных образцов в стартовую память записан типовой загрузчик для серии 1986BE. При необходимости может быть выпущена отдельная партия микросхем со стартовым загрузчиком адаптированным под задачи потребителя.

6. Средства разработки и документация

Предварительный вариант спецификации доступен по [ссылке](#).

Для первоначального знакомства с микроконтроллером разработана демонстрационная плата.



Это плата предназначена для прототипирования приборов учета, большое число ВЧ разъемов предназначено для подключения измерительных трансформаторов. Это позволяет не завязываться на какой-то конкретный их тип, и легко подключить именно те трансформаторы или шунты, которые применяют разработчики приборов учета. Также это позволяет подключить различные измерительные приборы для снятия точностных характеристик АЦП. Кроме того отсутствие высокого напряжения (220В) на плате снимает с нас ответственность, если кого то стукнет. Для более массового продвижения микросхемы ведется разработка миниатюрной тестовой платы в формате arduino uno или mega.

6.1. Eclipse+GCC

Разработка программ может осуществляться в среде на базе Eclipse с компилятором GCC и отладкой через OpenOCD, GDB. Для отладки в среде Eclipse подходят классические отладчики J-Link и их клоны. Так же подходят [отладчики](#) производства компании Миландр.

6.2. IAR

Так же разработку можно осуществлять в более привычной для многих среде IAR

Embedded Workbench, которая включает средства отладки, компиляции и оптимизации. Для отладки используются либо фирменный шнурок I-JET for RISC-V, либо если заказать [Evaluation Kit for RISC-V](#), то вместе с ним вы получите I-jet Lite debug probe (который поддерживает в том числе и ARM), а так же 30 дневную лицензию на саму среду.

Более подробную информацию по настройке и запуску сред IAR и Eclipse для работы с микроконтроллером K1986BK025 можно [найти тут](#).

7. Что нужно для получения образцов

Это посылочки, тем кто ждет эти микросхемы, а так же тем, кто наоборот...



Если вы хотите получить образцы и платы для ознакомления, то необходимо обратиться в отдел маркетинга [Миландра](#). В приоритете, конечно фирмы из электроэнергетического сектора, но в любом случае попытаемся всем помочь. После проведения всего комплекса испытания серийный выпуск микроконтроллеров будет запущен в 21 году, также данная микросхема будет включена в реестр продукции соответствующей [719 Постановлению Правительства](#).

Заключение

Вчерашние смелые идеи уже сегодня воплощаются в технических решениях и становятся нормой жизни. Мир, в котором мы с Вами живем, не позволяет стоять на месте. Появление описанной выше микросхемы имеет огромное значение для всего сообщества RISC-V. Я поздравляю всех, кто причастен к разработке данной микросхемы с ее рождением. А так же, надеюсь, что потребители (разработчики приборов учета) воспримут ее положительно, и невзирая на скепсис по отношению к отечественным микросхемам, я уверен мы можем конкурировать с иностранными компаниями.

Добро пожаловать в эпоху RISC-V!