CloudBEAR

Use cases for RISC-V processor IP
Commercial cores for real life applications

RISC-V 32/64-bit cores product line

CloudBEAR

Small and efficient MCUs

BM series

BM-310
RV32IMCAFNB

BM-610
RV64IMCAFDNB

Fast and compact embedded cores

BR series

BR-351
RV32IMCAFN

BR-651
RV64IMCAFDN

Linux capable application cores

BI series

BI-350
RV32IMCAF

Single issue

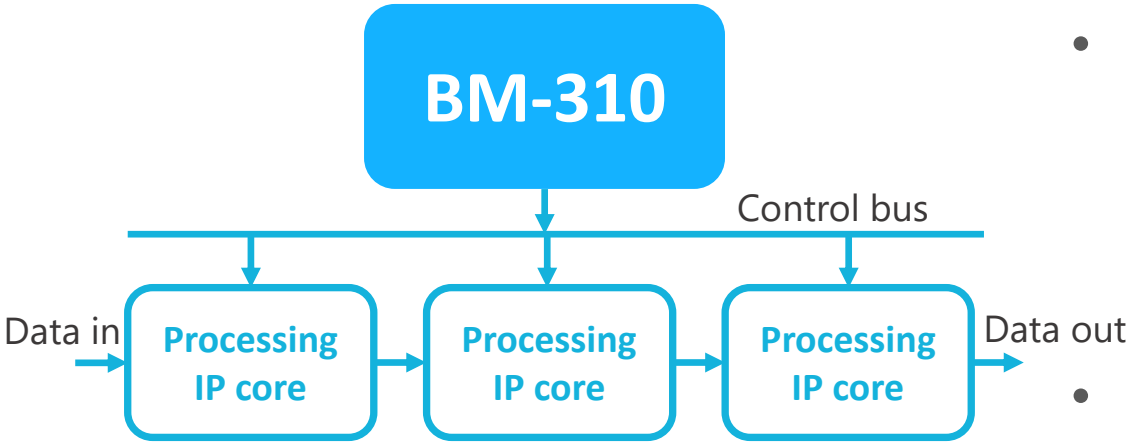
BI-651
RV64IMCAFD

Dual issue

BI-671
RV64IMCAFD

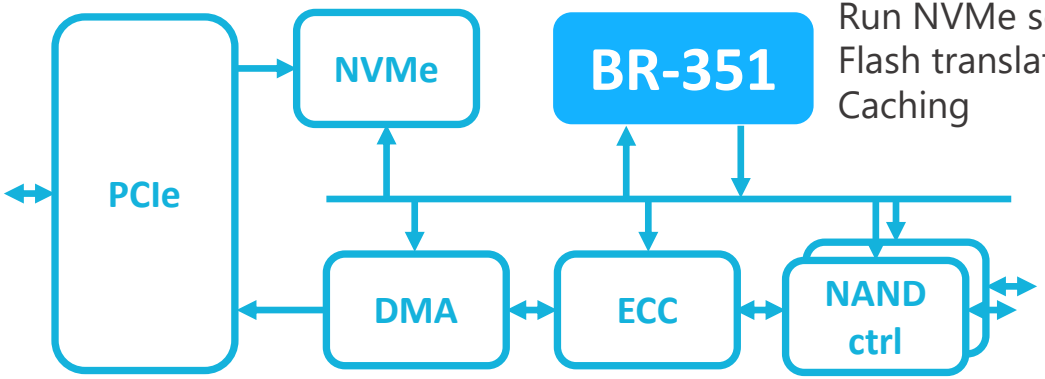
Out-of-order

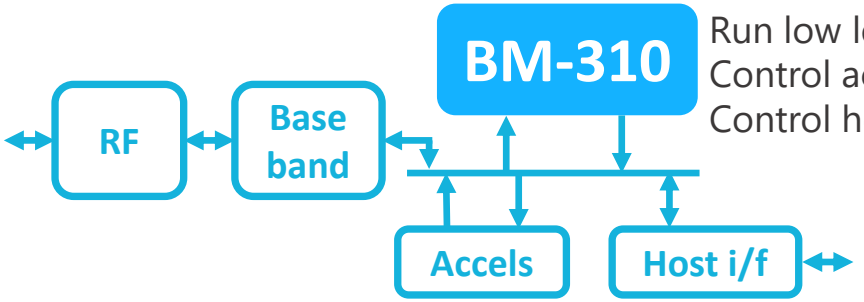
Deeply embedded applications: Control path applications



- Core doesn't touch the data
  Examples:
  - Video processor
  - AI accelerator control
  - Wireless baseband
- RV32IMC, RV32IC configurations are typically enough

Deeply embedded applications: Complex control/management software



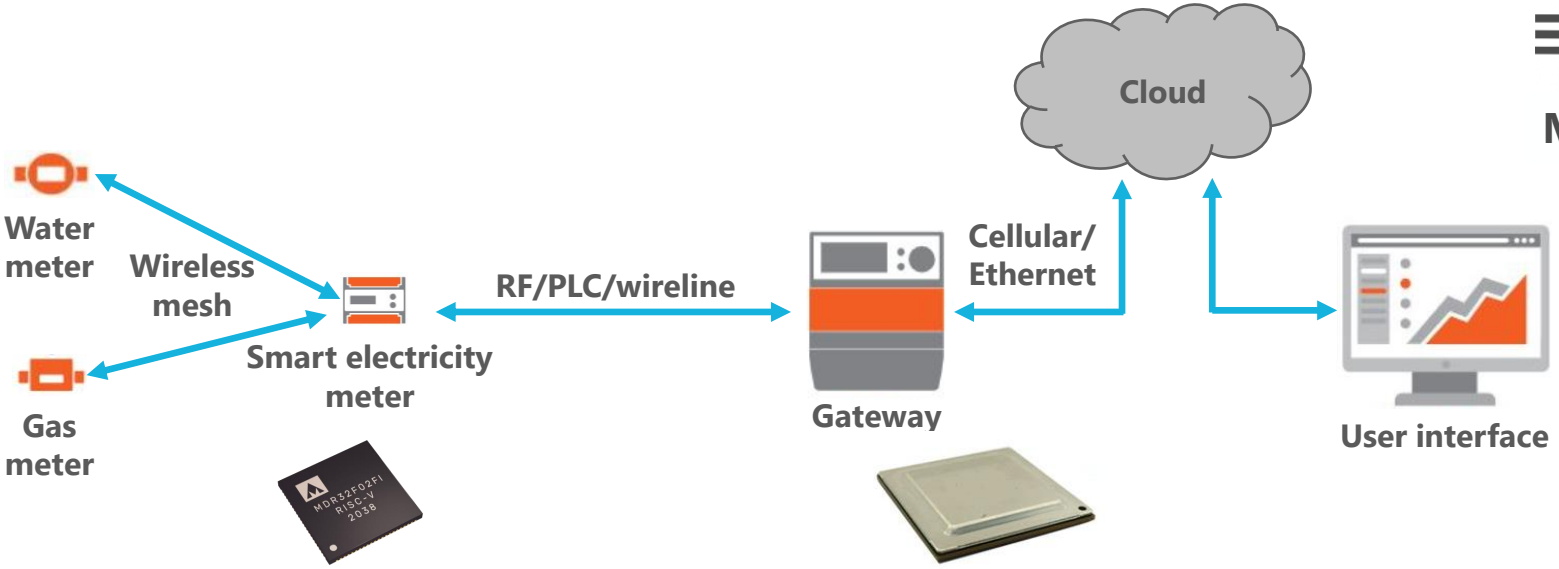


- Control/Data path
- Parsing protocols and control accelerators
  - SSD controller
  - Wireless MAC
- RV32IMCABN + Dynamic BP (optionally) perfectly fits
- B extension 0.92

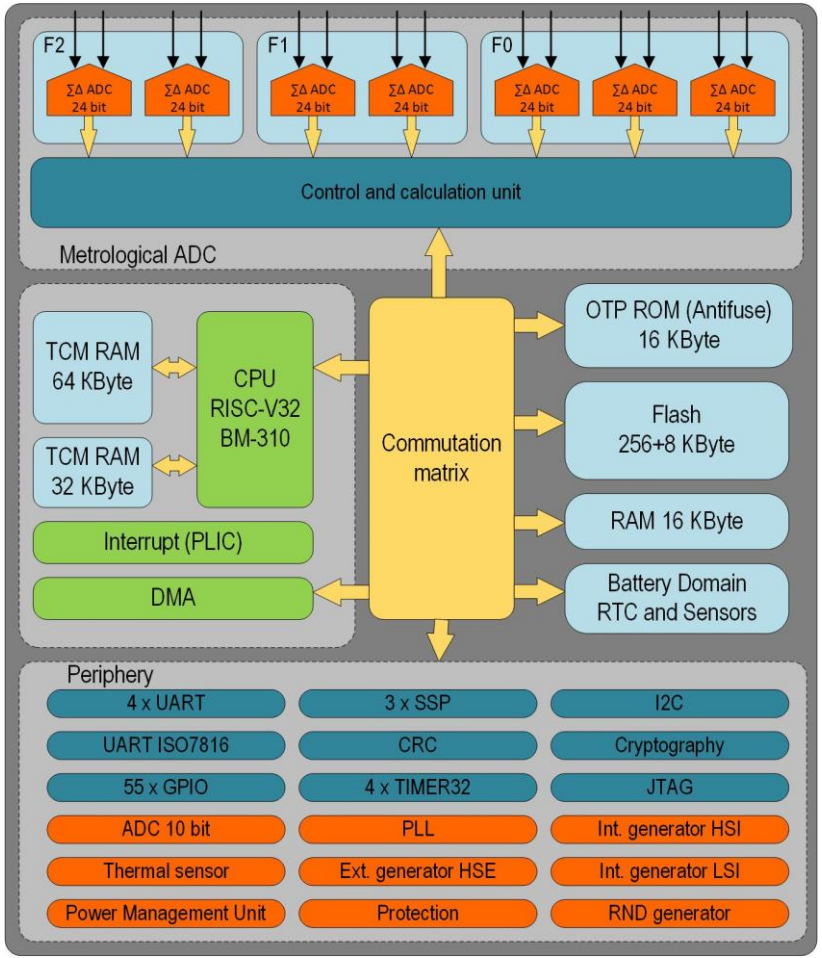
IoT/Smart Metering

CloudBEAR

Milandr



Secure MCU for Smart Metering

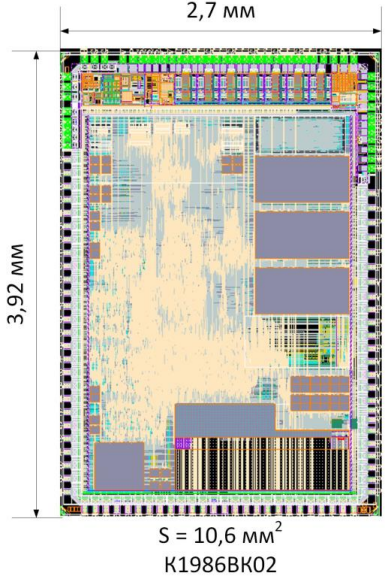


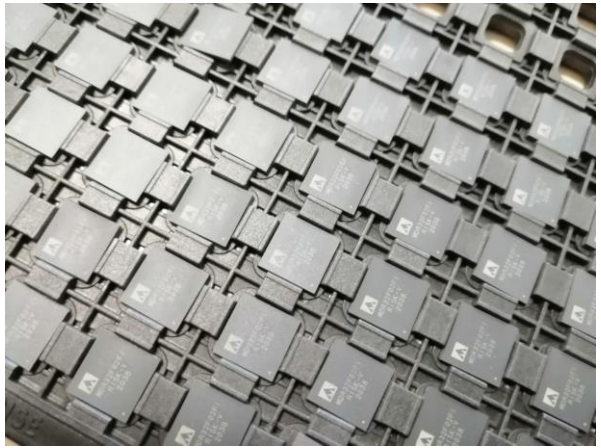
- TSMC 90nm LP
- High volume and low unit price
- Better than Cortex-M4 performance at lower power

CloudBEAR

Milandr

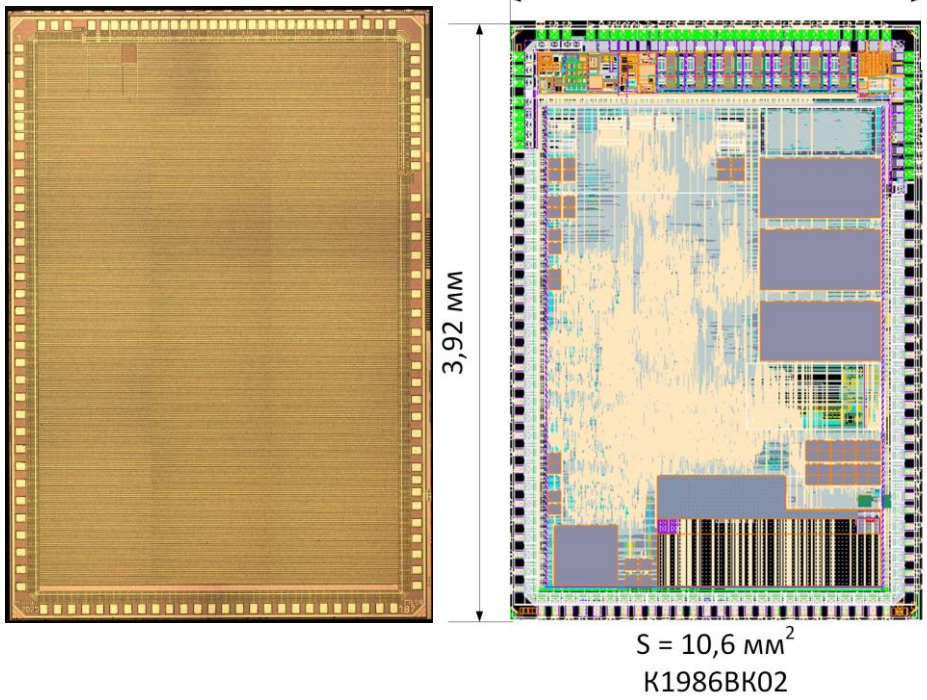
BM-310





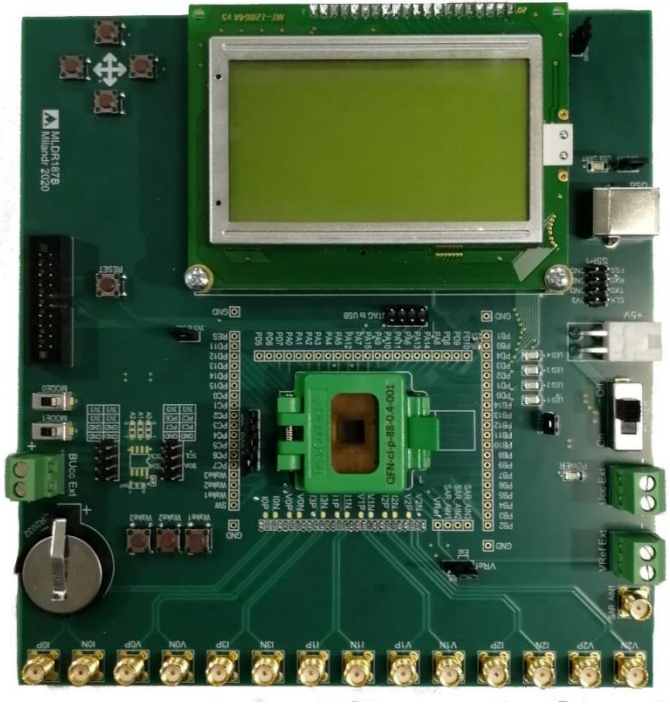
Secure MCU for Smart Metering

- BM-310
  - RV32IMC configuration
  - 3 stage
  - Parallel multiplier
  - Debug + 4 HW triggers
  - PLIC
- <0.3 mm^2@TSMC 90nm LP
- <3% of chip area



- K1985VK025 chip features
  - Specialized ADCs
  - Secure storage (keys)
  - Crypto
  - Tamper detection (optical sensor, shield, battery domain)

Boards



For smart meters developers
Available for early customers

Arduino compatible board
Available for
CloudBEAR's customers for BM-310 eval

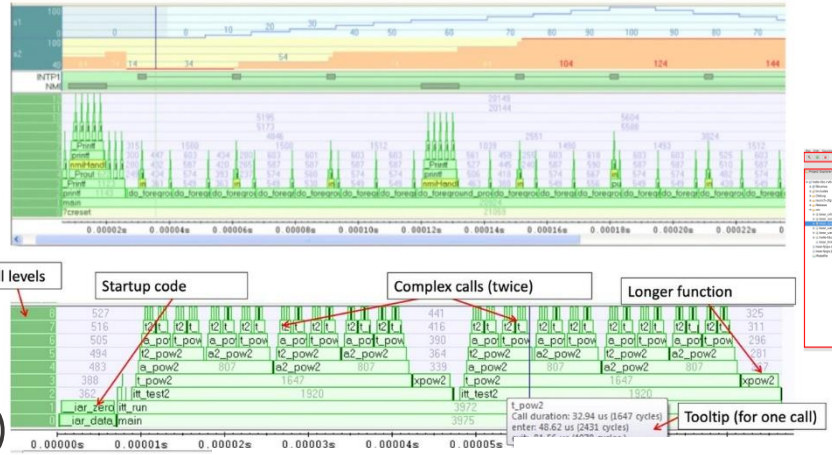
- Arduino Shield
- 2x PMOD
- RGB LED
- Micro SD
- Integrated debug via USB or connector for IAR I-Jet probe

CloudBEAR

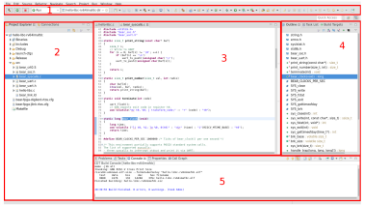
Milandr

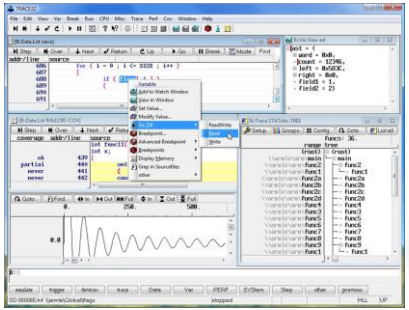
Development tools

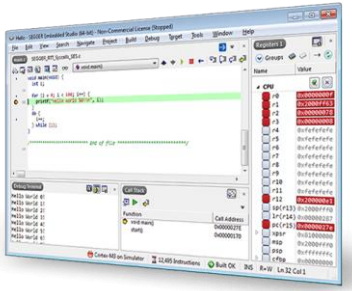
- Third-party ecosystem of development tools
- Interoperability due to Debug spec
- HW triggers for eFlash and ROM breakpoints
- **New:** Nexus trace (Q1 2021)



Eclipse IDE







Digilent JTAG-HS3

IAR SYSTEMS

LAUTERBACH DEVELOPMENT TOOLS

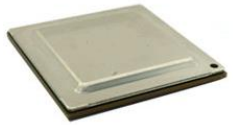
SEGGER

Application processor

- Linux capable processor
- 1 GHz dual core BI-671
- Security and real-time core BR-351
- Temp from -60C to +85C
- DDR, PCIe, Ethernet, eMMC, Camera, USB, UART, SPI, I2S, I2C, NAND, CAN, LCD
- 1.8/3.3V I/O domains

- General purpose CPU
- Secure gateways
- VPNs
- Industrial automation
- Industrial user interfaces

CloudBEAR



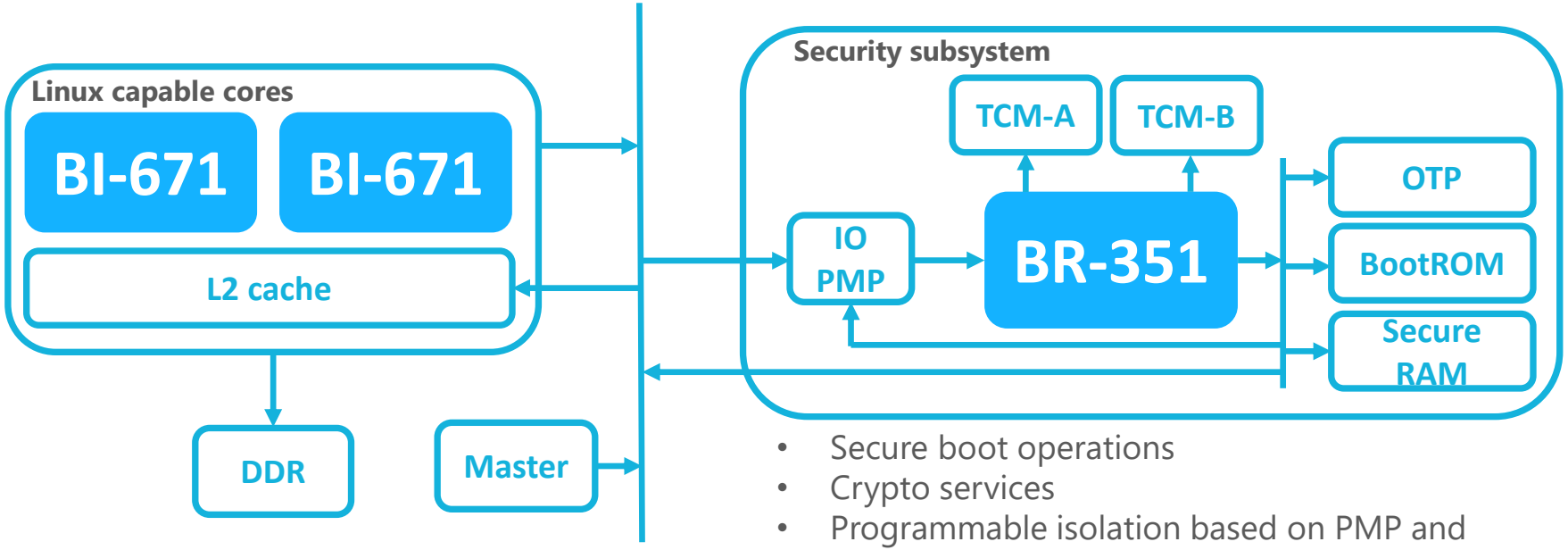
2x **BI-671**

BR-351

Milandr

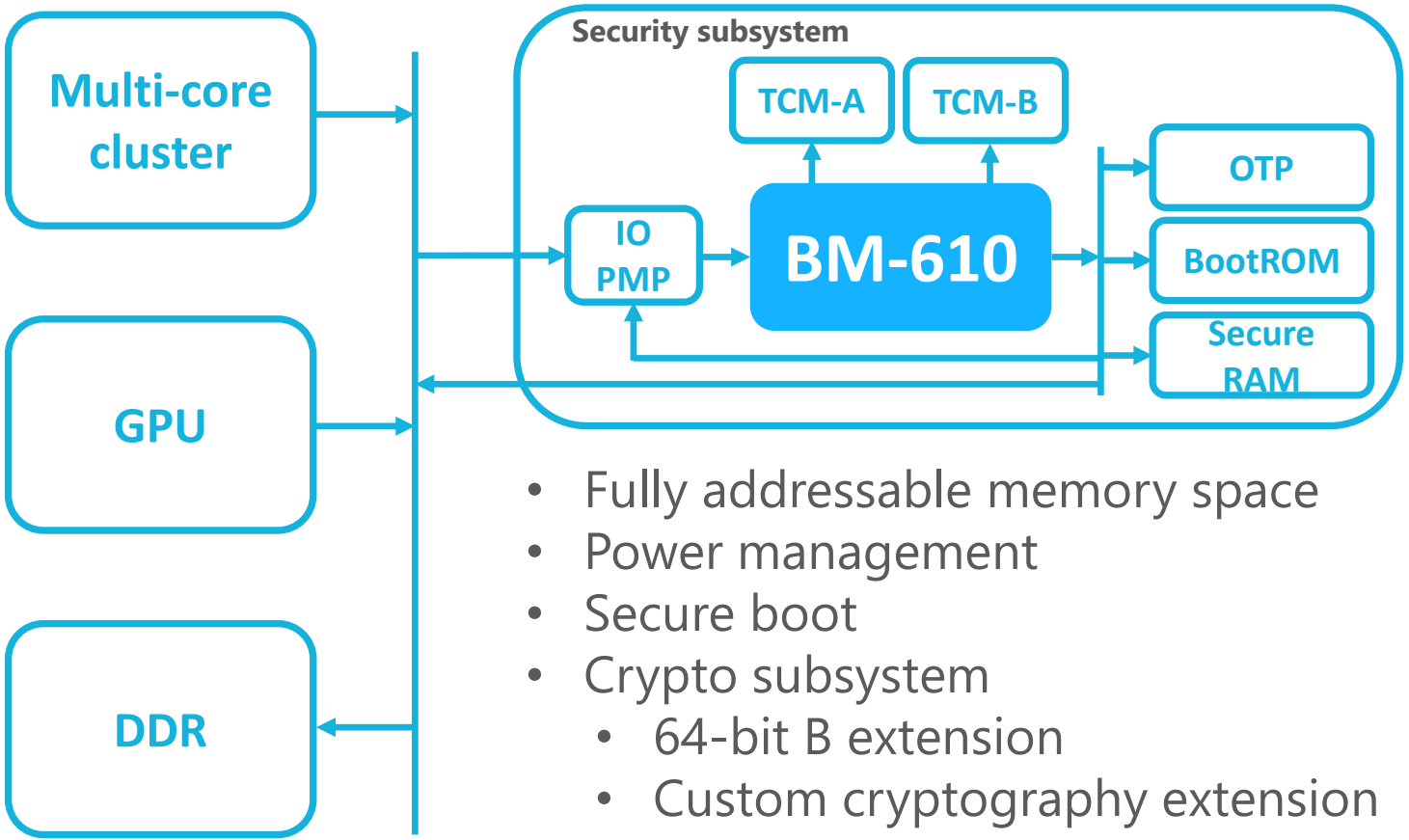
- Last development phase started in Q4 2020
  - SoC infrastructure IP by CloudBEAR
- Engineering samples by end of 2021

Application processor: Security and real-time subsystem



- Secure boot operations
- Crypto services
- Programmable isolation based on PMP and IOPMP which limits access to TCMs for external masters
- Real-time tasks offload from main CPUs
- Easy synchronization between BI-671 and BR-351 using A extension commands in TCMs

BM-610 – 64-bit housekeeper core



- Fully addressable memory space
- Power management
- Secure boot
- Crypto subsystem
  - 64-bit B extension
  - Custom cryptography extension

Custom instructions

CloudBEAR

C code with intrinsics

```
// Encrypt in place 128-bit block using GOST R 34.12-2015 Kuznechik algorithm
// keys is array of round keys 160 bytes (10x 128 bit)
static inline void kuzn_encrypt(uint64_t* text, const uint64_t* keys)
{
    const uint64_t* lastkey = keys + 18;

    int64_t s_lo;
    int64_t s_hi;

    int64_t text_lo = text[0];
    int64_t text_hi = text[1];

    while (keys != lastkey) {
        s_lo = _rv_gost64sb(text_lo ^ keys[0]);
        s_hi = _rv_gost64sb(text_hi ^ keys[1]);

        text_lo = _rv_gost64kul(s_lo, s_hi);
        text_hi = _rv_gost64kuh(s_lo, s_hi);

        keys += 2;
    }

    // Last round
    text[0] = text_lo ^ keys[0];
    text[1] = text_hi ^ keys[1];
}
```

Dissasembly

```
40000f76:   0407472b        gost64sb    a4,a4
40000f7a:   8ebd                xor a3,a3,a5
40000f7c:   0406c6ab        gost64sb    a3,a3
40000f80:   48d747ab        gost64kul   a5,a4,a3
40000f84:   4ad746ab        gost64kuh   a3,a4,a3
40000f88:   6706                ld  a4,64(sp)
40000f8a:   4641                li  a2,16
40000f8c:   858a                mv  a1,sp
40000f8e:   8fb9                xor a5,a5,a4
40000f90:   6726                ld  a4,72(sp)
40000f92:   0407c7ab        gost64sb    a5,a5
40000f96:   0988                addi    a0,sp,208
40000f98:   8eb9                xor a3,a3,a4
40000f9a:   0406c6ab        gost64sb    a3,a3
40000f9e:   48d7c72b        gost64kul   a4,a5,a3
40000fa2:   4ad7c6ab        gost64kuh   a3,a5,a3
40000fa6:   67c6                ld  a5,80(sp)
40000fa8:   0980                addi    s0,sp,208
40000faa:   4d010493        addi    s1,sp,1232
40000fae:   8f3d                xor a4,a4,a5
40000fb0:   67e6                ld  a5,88(sp)
40000fb2:   0407472b        gost64sb    a4,a4
40000fb6:   8ebd                xor a3,a3,a5
40000fb8:   0406c6ab        gost64sb    a3,a3
40000fbc:   48d747ab        gost64kul   a5,a4,a3
40000fc0:   4ad746ab        gost64kuh   a3,a4,a3
```

Crypto Algorithm	Performance @ BM-610, 400 MHz
Kuznyechik (cipher)	780 Mbit/s
Streebog (hash)	72 Mbit/s

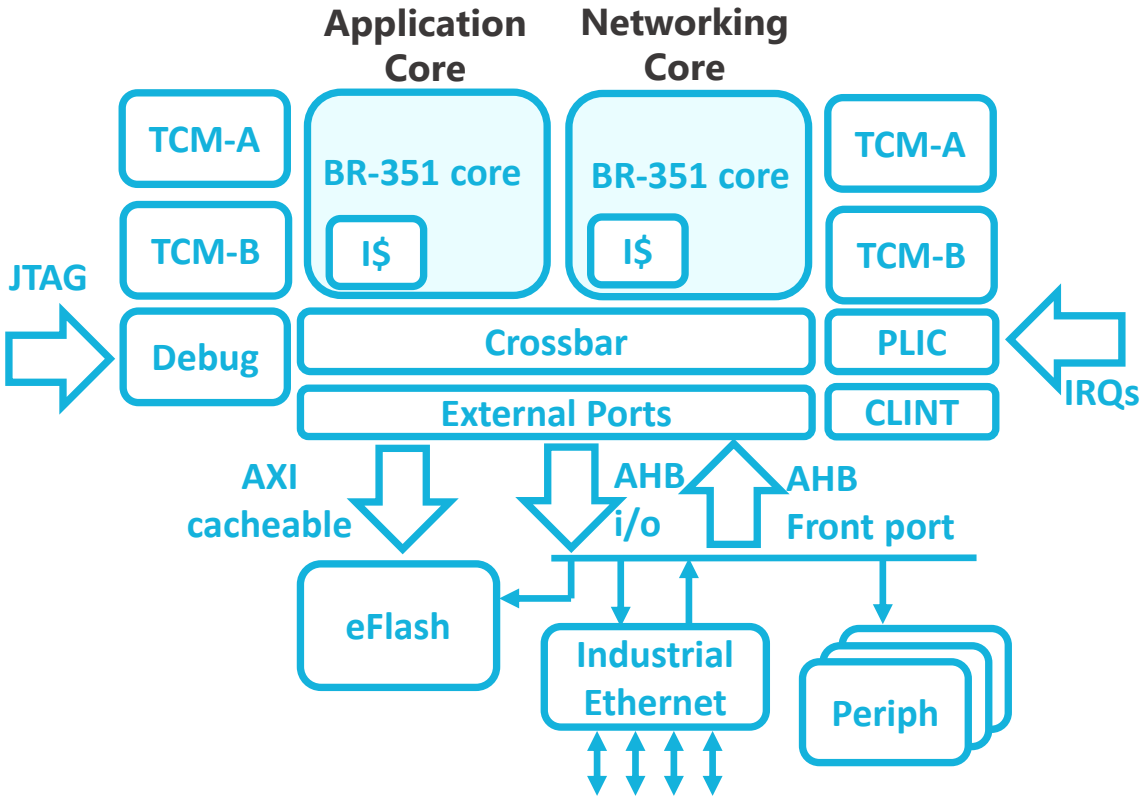
Configuration Core + PLIC + Debug	Area (mm^2) @ 28nm, worst, 400 MHz
BM-610 RV64IMC	0.062
BM-610 RV64IMC + B	0.077
BM-610 RV64IMC + B + Xgost	0.095

More than 100x improvement in encryption and 50x in hashing performance with custom instructions

*** Implementation of "Kuznyechik" cipher using vector instructions (2018)**
MIPT, Milandr, Intel Corporation, Intel Core i5-8250u @ 1.6GHz: 1272 Mbit/s

**** https://github.com/adegtyarev/streebog Intel Core i7-2600 CPU @ 3.40GHz : 968 Mbit/s**

Industrial automation SoC



- Dual core
  - Separate networking core for low latency industrial communication protocols
- PMP for networking/crypto/ application processes isolation
- Low latency
  - N extension
  - Direct access to TCMs from ethernet master
- Execute from the eFlash => I caches with prefetch
- Atomics on buses to support cores sync mechanism

 @CloudBEARInc

www.cloudbear.ru