SVD 200
SECURE IoT EDGE NODE DEVICE

sondrel
Success through partnership

A fast-track edge node device architecture using a proven design for a low-power, secure IoT solution

Lead the market

Buying off the shelf silicon may give you the comfort of a known unit cost, but at what price? There is little chance to customise the design, it's not your chip, your chosen size, your feature set or your roadmap. What is more, you're vulnerable to supplier price changes.

Take charge

Create your own chip and you can differentiate, lead the market, reduce your bill of materials and take charge of the supply chain.

✓ No dead silicon ✓ You're in control
✓ The chip is optimised in terms of size and efficiency.

A truly compelling approach

Sondrel's customisable designs compress the design lifecycle, reducing the cost, time and risk compared with designing from scratch. The core of the design is silicon proven meaning we've flushed out the design challenges and can now offer unparalleled efficiency in the design process.

Fit and forget

Designed for a long time in the field between battery swap outs, this design is for a tiny, 4mm^2 silicon area on the Samsung® 28nm FDSOI process node.

Silicon for emerging markets

Smart home | Smart Metering | Smart City | Smart Factory
Voice Controlled Devices | Sensor fusion | Automotive

SVD-200 is the benchmark reference design for secure IOT edge devices using trusted Arm® IP. Sondrel was the first company to design a chip combining these secure components in a proven architecture that offers ultra-low power consumption properties and robust, Arm® based security features.

Our next generation designs are based on successful client implementations that offer an attractively low NRE and a compelling speed to market for a competitive edge.

A silicon proven, system design kit for a short delivery timeframe

- Based on the Arm® CoreLink SSE-200 subsystem to deliver low power IoT designs quickly

- Each stage of the design optimised for security, low power and connectivity
- Dual Arm® Cortex M-33® processors which are both powerful and low power

Secure designed to work seamlessly across software, hardware and connectivity

- Deploys the highly regarded Arm® Platform Security Architecture utilising Arm® TrustZone™ throughout
- Configurable TrustZone™ protection for memory and peripherals

Interoperable connectivity

- Standards-based low-power (~7mW) wireless IP
- Suitable for One-to-One, One-to-Many and Many-to-Many connectivity
- Bluetooth 5
- IEEE 802.15.4

Power management

- Intelligent power management unit
- Dynamic voltage & frequency scaling

Silicon technology

- Samsung® 28nm FDSOI
- Frequency: 200MHz

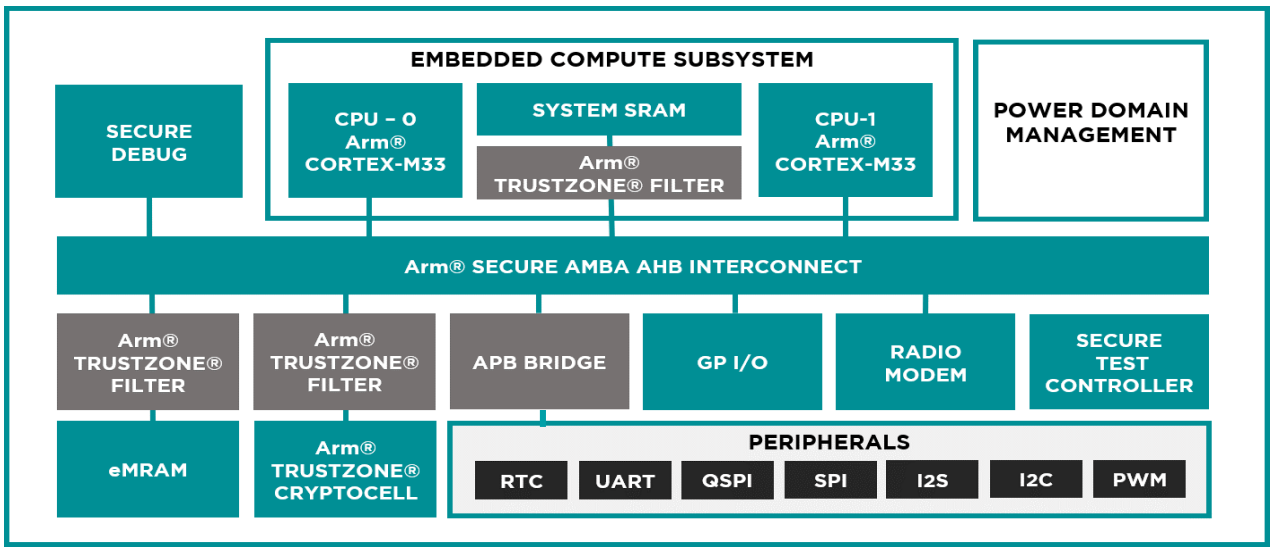
Call us on +44 (0) 118 983 8550 or email sales@sondrel.com

Sondrel Ltd, Sondrel House, Theale Lakes Business Park, Moulden Way, Sulhamstead, Berkshire, RG7 4GB, UK

SVD 200
SECURE IoT EDGE NODE DEVICE

sondrel
Success through partnership

- ✓ Layered security architecture based on the Arm® Platform Security Architecture (PSA).
- ✓ Data to and from the chip interconnect bus protected by the Arm® TrustZone® Filter
- ✓ Root of Trust provided by the Arm® TrustZone® CryptoCell block for security services, lifecycle management, key management and cryptographic acceleration.
- ✓ Secure debug using on-chip authentication
- ✓ Embedded on-chip authentication using an eSIM for secure connectivity over mobile networks
- ✓ Efficient power management backbone using the Arm® PCK600 ensuring dynamic low power
- ✓ Secure Network on Chip functionality provided by the Arm® secure AMBA™ AHB5/APB4 Interconnect which interoperates with the Arm® TrustZone® components
- ✓ Silicon-proven design for optimum data security



Technical Specification

Embedded Compute
- 2 x Arm® Cortex-M33 Arm® 8-M generation for MCU & DSP
- 4KB cache per processor
- Up to 4 x 128KB System SRAM
- 128KB TCM

Security
- Arm® TrustZone® Cryptocell Secure AMBA® interconnect:
  - AHB5 Bus Matrix
  - AHB5 TrustZone® Memory Protection Controller
  - AHB005 TrustZone® Peripheral Protection Controller
  - AHB5 Exclusive Access Monitor
  - AHB5 Access Control Gates
  - AHB5 to APB Bridges
- Expansion AHB5 master and slave buses (two each)
- Implementation Defined Attribution Unit
- Secure Boot
- Secure & non-secure configurable peripheral access
- Secure and non-secure configurable memory access
- OTP (1 x 8Kbit)

Power control
- Power Dependency Control Matrix
- Power Policy units
- Arm® CoreLink™ LPD-500 low power distributor
- Power consumption: 10µA idle, 2W max active

Memory
- 2 x 2MB eMRAM (expandable up to 8Mbytes)

Communications (optional)
- Low power PAN - Bluetooth 5 and IEEE802.15.4
- Arm® NBIoT supporting 5G

Peripheral interfaces
- Real Time Controller (RTC)
- 16 x GPIO
- I2C x 2
- I2S 3 channels
- 1 x QSPI
- 1 x SPI
- 2 x UART
- 9 x PVT
- 8 x PWM

Timers
- 3 x general purpose timers with configurable security
- Arm® Cortex-M System Design Kit dual timer with configurable security
- Boot/power MNG

Debug & Test
- Arm® CoreSight debug
- Configurable secure debug
- JTAG/SWD port shared for debug & test
- Manufacturing test controller (SCAN/MBITS & PLL test)

Physical
- Samsung 28nm FDSOI
- Silicon area 4mm^2
- Frequency 200MHz

PD-SVD 200 190503a