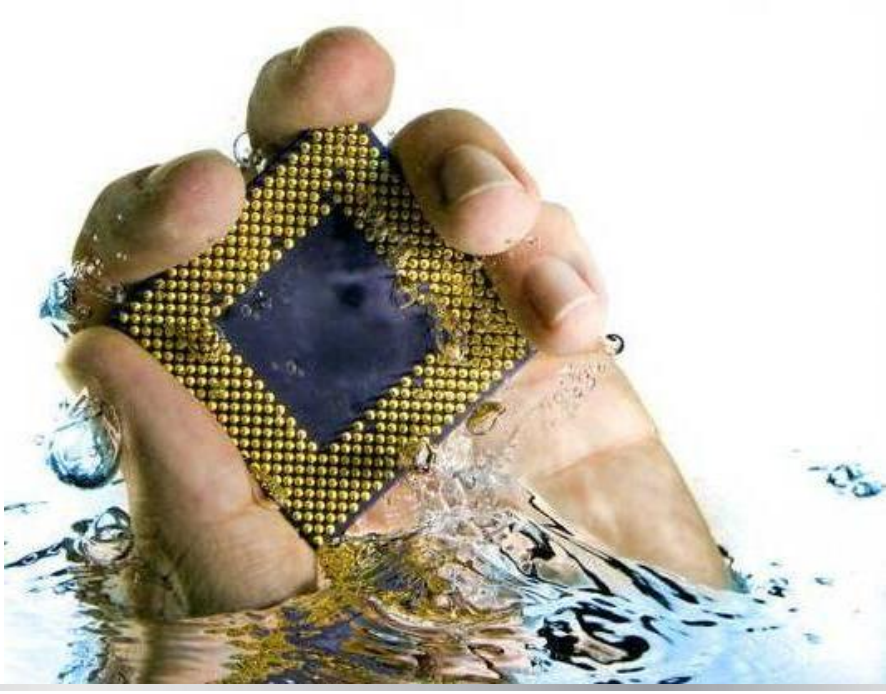
Protection logiciels embarqués

Carl Vincent

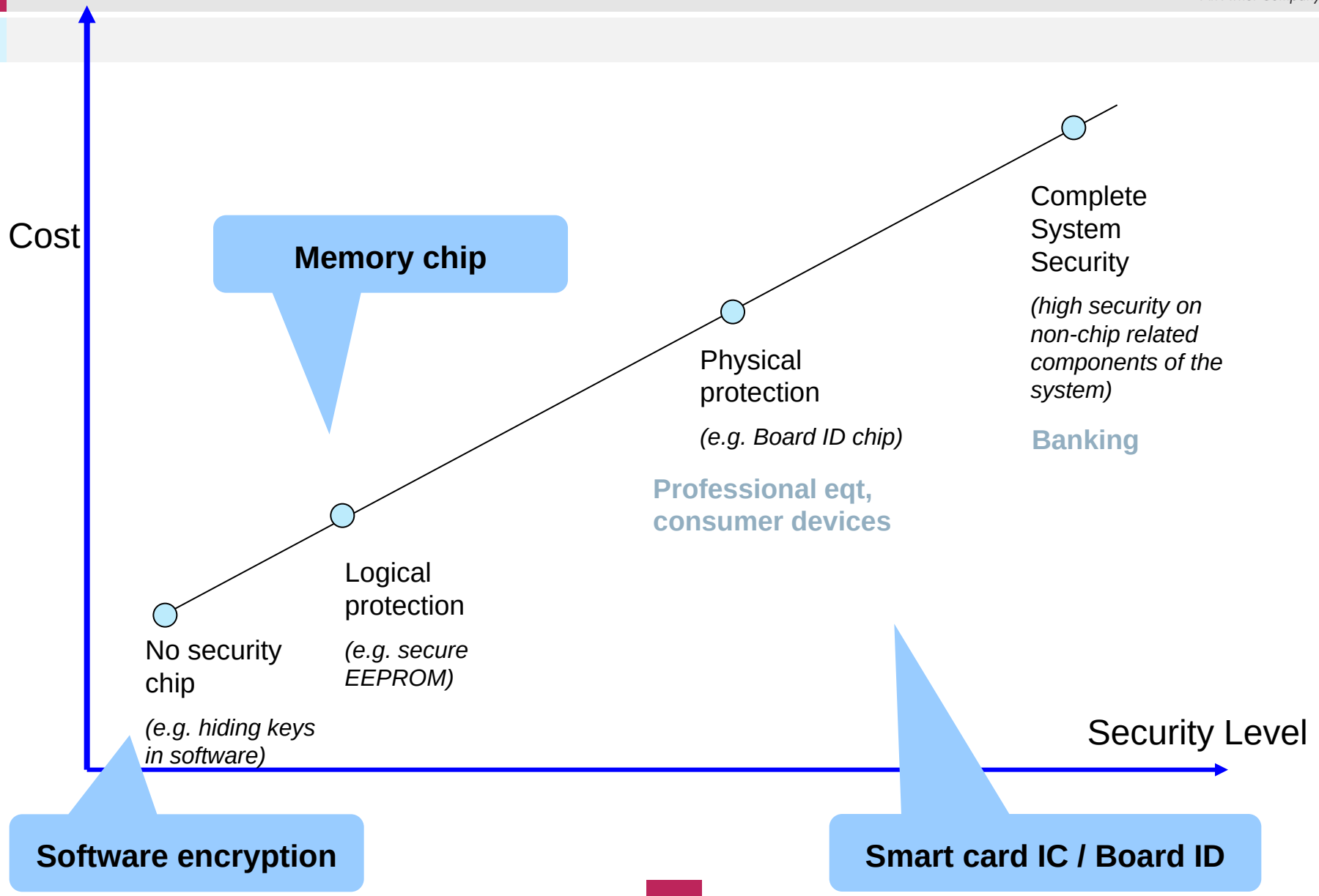
carl.vincent@silica.com

0608729887



SILICA Linecard

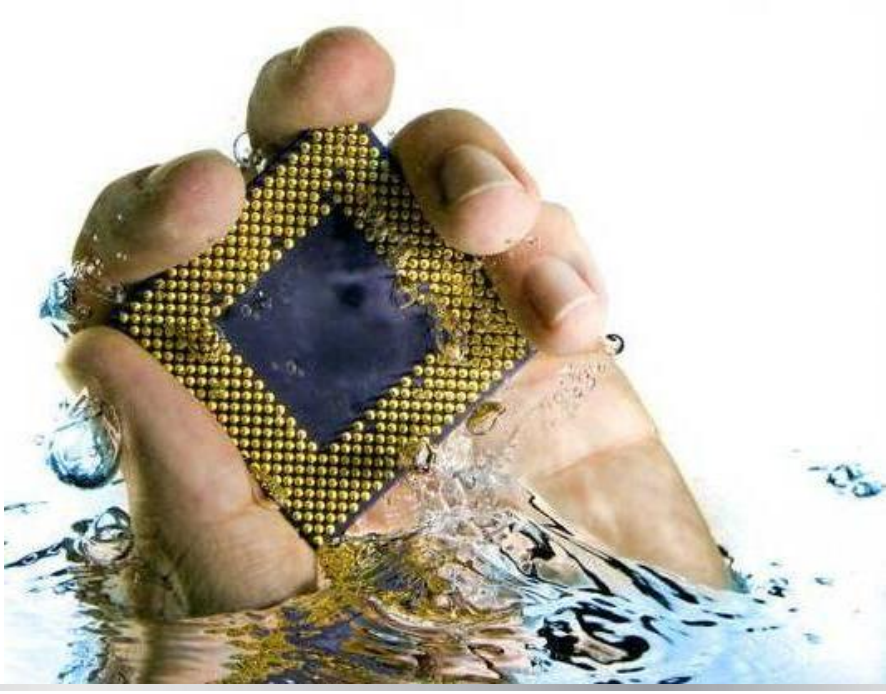
Security Level vs. Cost

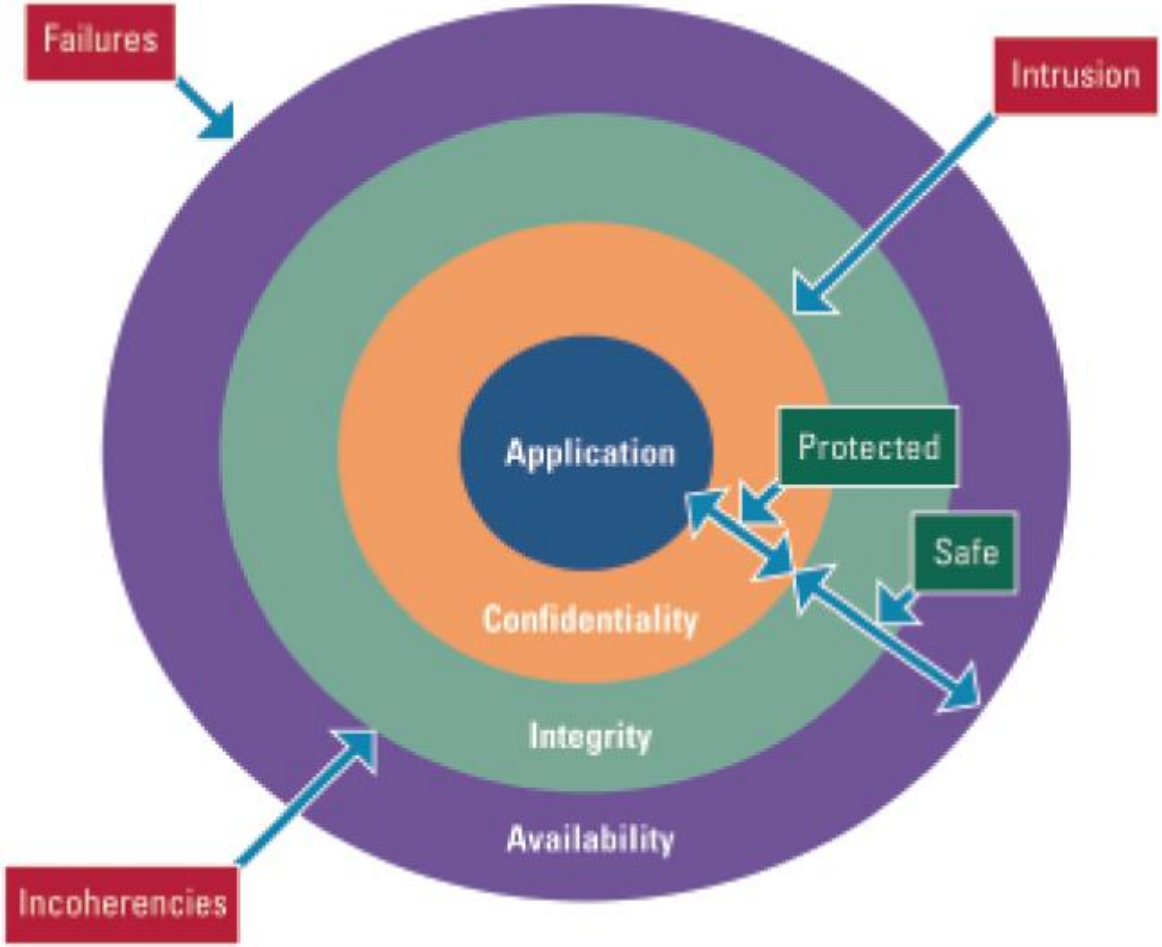


Agenda

- Protection µC
- Communication
- External Protection
  - Maxim
  - Flash Sécurisé
- Protection Renesas

Protection µC





To maintain the availability, the following features are used:

- Programmable voltage detector (part of power voltage supervisor)
- Clock security system
- Emergency stop state (to ensure the failure does not spread)

To maintain the integrity, the following features are used:

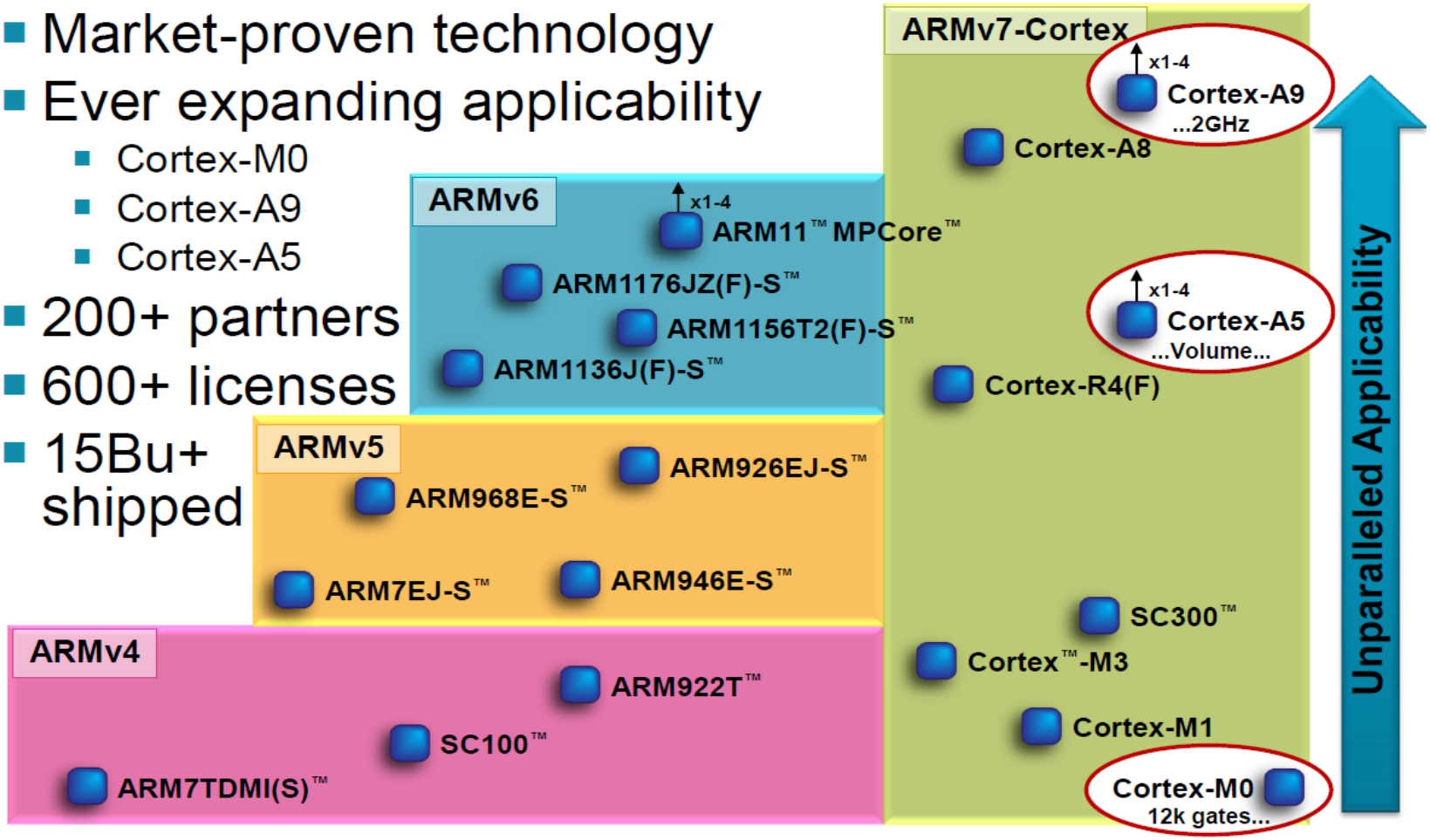
- Power-on reset and power down reset (part of power voltage supervisor)
- Write once registers
- Lockable IOs
- Exception fault handling
- Dual watchdog

To maintain the confidentiality the following features are used:

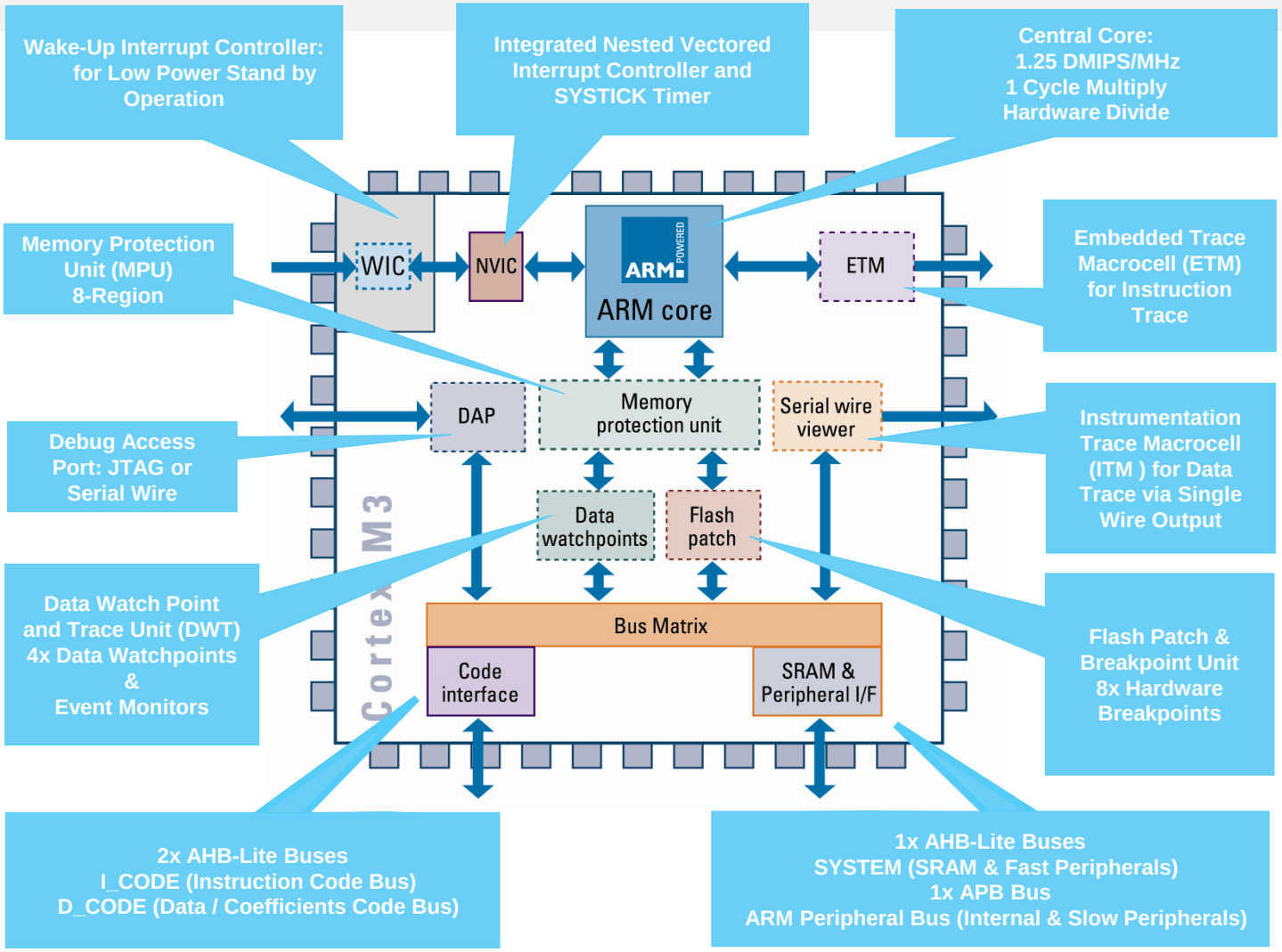
- Flash memory protections (write and read)
- Backup registers and anti-tamper feature

ARM Processor Portfolio

- Market-proven technology
- Ever expanding applicability
  - Cortex-M0
  - Cortex-A9
  - Cortex-A5
- 200+ partners
- 600+ licenses
- 15Bu+ shipped



Cortex-M3 Processor Overview



optional blocks, please consult your silicon manufacturers data sheet

MPU Overview

- **Support for 8 regions and each region can be broken up into 8 sub-regions**
- **MPU provides full support for:**
  - Region protection
  - Overlapping protection regions
  - Access permissions
  - Exporting memory attributes to the system
- **Configuration only in privileged mode**

LPC17XX : code security

Important: Any CRP change becomes effective only after the device has gone through a power cycle.

Table 569. Code Read Protection options

Name	Pattern programmed in 0x000002FC	Description
CRP1	0x12345678	Access to chip via the JTAG pins is disabled. This mode allows partial flash update using the following ISP commands and restrictions: • Write to RAM command can not access RAM below 0x10000200. This is due to use of the RAM by the ISP code, see Section 32–3.2.7. • Read Memory command: disabled. • Copy RAM to Flash command: cannot write to Sector 0. • Go command: disabled. • Erase sector(s) command: can erase any individual sector except sector 0 only, or can erase all sectors at once. • Compare command: disabled This mode is useful when CRP is required and flash field updates are needed but all sectors can not be erased. The compare command is disabled, so in the case of partial flash updates the secondary loader should implement a checksum mechanism to verify the integrity of the flash.
CRP2	0x87654321	This is similar to CRP1 with the following additions: • Write to RAM command: disabled. • Copy RAM to Flash: disabled. • Erase command: only allows erase of all sectors.
CRP3	0x43218765	This is similar to CRP2, but ISP entry by pulling P2.10 LOW is disabled if a valid user code is present in flash sector 0. This mode effectively disables ISP override using the P2.10 pin. It is up to the user's application to provide for flash updates by using IAP calls or by invoking ISP with UART0. **Caution: If CRP3 is selected, no future factory testing can be performed on the device.**

STM32 / Flash protection

- Two kind of protections are available:
  - Write protection to avoid unwanted writings
  - Readout protection to avoid piracy
  - Activated by setting option bytes in the Small Information Block (SIF)

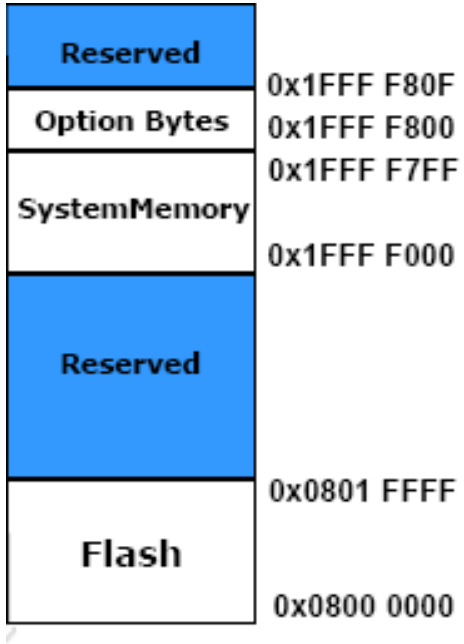
STM32 / information block

- The Information Block consists of:
  - 2 KBytes for SystemMemory : contains Bootloader
  - 16 Bytes for Small Information block (SIF): contains The Option bytes

- **8** option bytes (SIF Block) are available

(+ Their complements = 16 bytes in Total) :

  - 4 for write protection
  - 1 for read protection
  - 1 for Device configuration:
    - IWDG HW/SW mode
    - Reset when entering STANDBY mode
    - Reset when entering STOP mode
  - 2 For User Data (To store Security IDs, etc.)



STM32 / Flash protection / Read (1)

Readout protection

- Once the protection byte has been programmed :
  - Main Flash memory read access is not allowed except for the user code (when booting from main Flash memory with the debug mode not active).
  - Pages 0-3 are automatically write-protected.
  - The rest of the memory can be programmed by the code executed from the main Flash memory (for IAP, constant storage, etc.), but it is protected against write/erase (but not against mass erase) in debug mode or when booting from the embedded SRAM.
  - Flash memory access through data read using JTAG, SWV (serial wire viewer), SWD(serial wire debug), ETM and boundary scan are not allowed.
  - All features linked to loading code into and executing code from the embedded SRAM are still active (JTAG/SWD and boot from embedded SRAM) and this can be used to disable the read protection.

- **Tamper detecion**
  - The STM32 F10x provides 10 16-bit registers which

  can be used to store key data.

  This data will be saved in the registers via the optional backup battery, but it will be erased automatically if a tamper is detected via the anti-tamper pin.

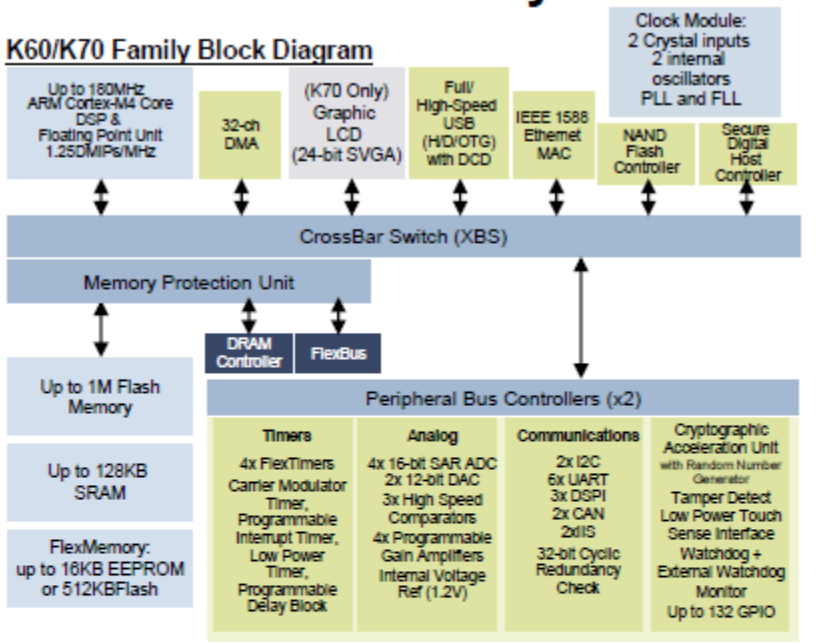
M4 solution

K60/K70 Family Overview

Higher Performance, Security, & Connectivity

- **Real-time Ethernet for precision automation**
  - IEEE 1588 hardware time stamping & clock synchronization enables accurate, deterministic control over Ethernet networks
- **(K70 only) Graphical LCD for advanced user interfaces**
  - Single-chip QVGA support possible, allowing use of lower-cost displays without Chip-on-Glass capability
  - Up to 24-bit SVGA with external memory support
- **Robust system security with tamper detection**
  - Tamper detection with voltage, frequency, and temperature monitoring. External sensor support for physical attack detection
- **Hardware Encryption for secure data transfer & storage**
  - Significantly faster than software implementations while consuming minimal system resources.
  - Supports numerous algorithms with hardware assisted software routines – SSH, SSL, IPSec, etc

256KB Flash in 100 pin package starting at $2.99 for 10K SRP



Enablement Bundle

TOWER development system
Complementary MQX RTOS with TCP/IP & USB Stack
Eclipse-Based CodeWarrior 10.0 IDE
Processor Expert Rapid Application Development Tool
IAR, Keil and Full ARM Ecosystem Support
Graphics LCD and Encryption libraries

Family	Graphics LCD Controller	IEEE 1588 Ethernet / Encryption / Tamper Detect
K60	-	X
K70	X	X

Kinetis Product Family Features

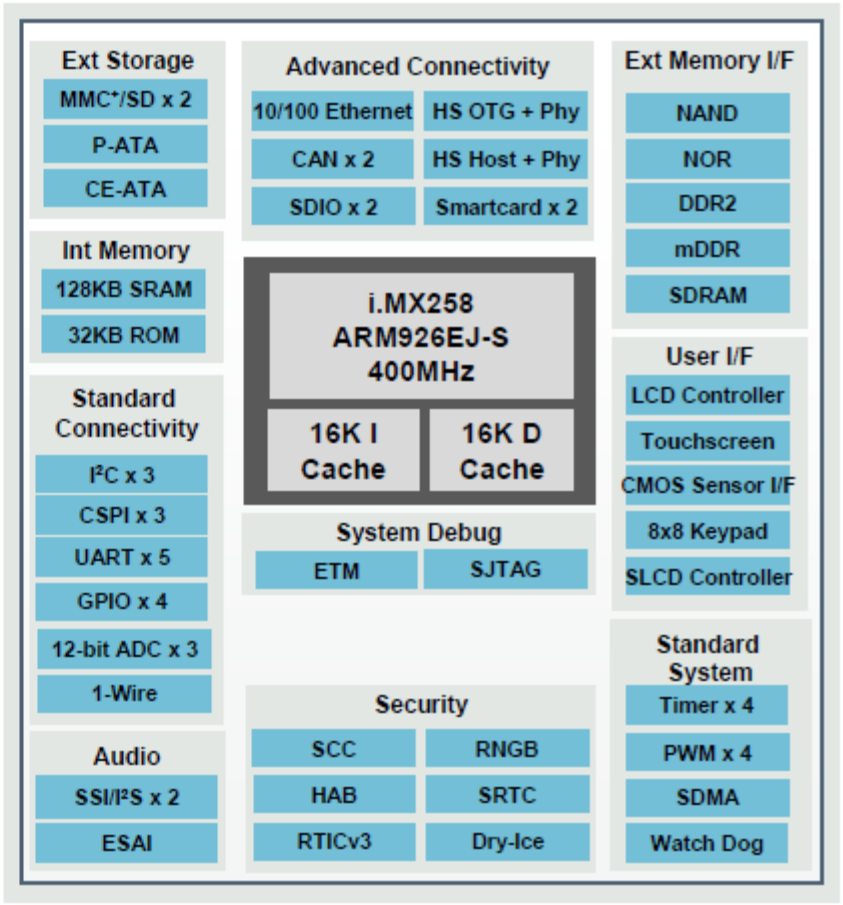
MCU Family	USB OTG (FS & HS)	LCD (Segment/Graphics)	NAND Flash Controller	Floating Point Unit	Ethernet (IEEE 1588)	Encryption (CAU+RNG)	Dual CAN	Hardware Tamper Detect	DRAM Controller
K70 Family 512KB-1MB, 196-256pin	●	●	●	●	●	●	●	●	●
K60 Family 256KB-1MB, 100-256pin	●		●	●	●	●	●	●	●
K50 Family 128-512KB, 64-144pin	●	●			●	●			
K40 Family 64-512KB, 64-144pin	●	●					●		
K30 Family 64-512KB, 64-144pin		●					●		
K20 Family 32KB-1MB, 32-144pin	●		●	●			●		
K10 Family 32KB-1MB, 32-144pin			●	●			●		

Common System IP	Common Analog IP	Common Digital IP	Development Tools
32-bit ARM Cortex-M4 Core w/ DSP Instructions	16-bit ADC	CRC	Bundled IDE w/ Processor Expert
Next Generation Flash Memory High Reliability, Fast Access	Programmable Gain Amplifiers	I^2C	Bundled OS USB, TCP/IP, Security
FlexMemory w/ EEPROM capability	12-bit DAC	SSI (I^2S)	Modular Tower H/ware Development System
SRAM	High-speed Comparators	UART/SPI	Application Software Stacks, Peripheral Drivers & App. Libraries (Motor Control, HMI, USB)
Memory Protection Unit	Low-power Touch Sensing	Programmable Delay Block	Broad 3rd party ecosystem
Low Voltage, Low Power Multiple Operating Modes, Clock Gating (1.71V-3.6V with 5V tolerant I/O)		External Bus Interface	
DMA		Motor Control Timers	
		eSDHC	
		RTC	

ARM9

i.MX25 – Features

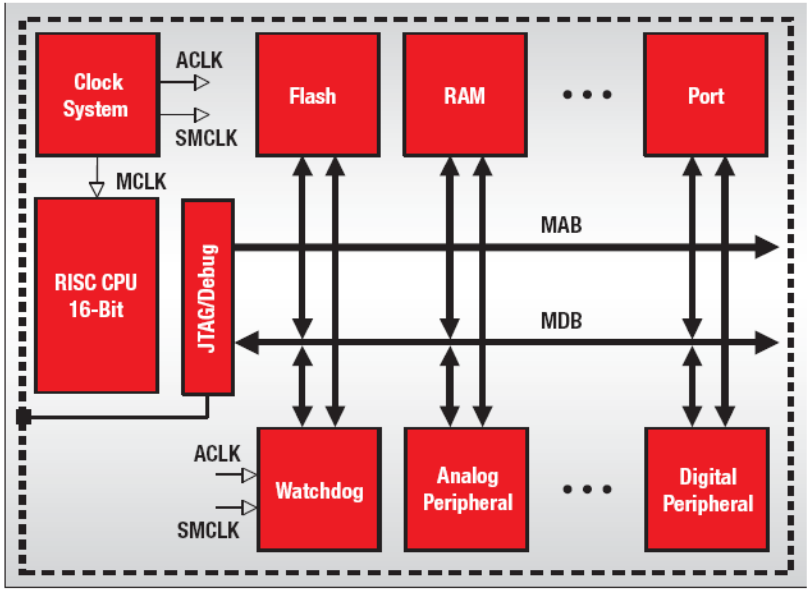
- **Key Features and Advantages**
  - 400MHz ARM926EJ-S™
  - 16KB L1 I-Cache, 16KB L1 D-Cache
  - 128KB on-chip SRAM for low power LCD refresh
  - External memory interface supports DDR2, mDDR, or SDRAM up to 133MHz
  - Supports off-chip NAND or NOR Flash
  - 10/100 Ethernet MAC with RMII support
  - USB 2.0 OTG 480Mbps with high-speed PHY
  - USB 2.0 Host 480Mbps with full-speed PHY or ULPI
  - SVGA (800x600) LCD controller with integrated touchscreen controller
  - CMOS sensor interface
  - Two CAN interfaces
  - Two Smartcard interfaces
  - Enhanced serial audio interface
  - 3 general purpose 12-bit ADC channels
  - UART's, CSPI's, I2C, I2S
  - 3.3V I/O reduces external component count
  - Enhanced security features, including tamper detection for voltage, frequency and temperature
  - High-Assurance Boot (HAB)
- **Available Parts**
  - i.MX251, i.MX255, i.MX253, i.MX257, i.MX258
- **Package and Temperature**
  - 0.8mm, 17x17, 400-pin MAPBGA
  - -40C to +85C, -20C to +70C



MSP430 from TI

Key Features

- **Ultra-low-power** architecture and flexible clock system extends battery life:
  - 0.1-µA RAM retention
  - <1-µA RTC mode
  - <250 µA/MIPS
- **Integrated intelligent peripherals** including wide range of high-performance analog and digital peripherals offload the CPU
- **16-bit RISC CPU architecture** enables new applications with industry leading code density
- **Easy to Get Started:** Complete development tools starting at only $20



MSP430 von-Neumann architecture — all program, data memory and peripherals share a common bus structure. Consistent CPU instructions and addressing modes are used.

MSP430 Flash protection

- **Which MSP430 Programmers can blow the JTAG fuse?**

  The MSP430 JTAG programming tools that can blow the JTAG fuse are

  *** MSP-PRGS430, MSP-GANG430 and the MSP430 Replicator (third-party tool from SoftBaugh).**

  You can not blow the JTAG fuse using the Bootstrap Loader (BSL).

JTAG Fuse (see Note 1)

PARAMETER		TEST CONDITIONS	VCC	MIN	TYP	MAX	UNIT
$V_{CC(FB)}$	Supply voltage during fuse-blow condition	T_A = 25°C		2.5			V
V_{FB}	Voltage level on TEST for fuse-blow			6		7	V
I_{FB}	Supply current into TEST during fuse blow					100	mA
t_{FB}	Time to blow fuse					1	ms

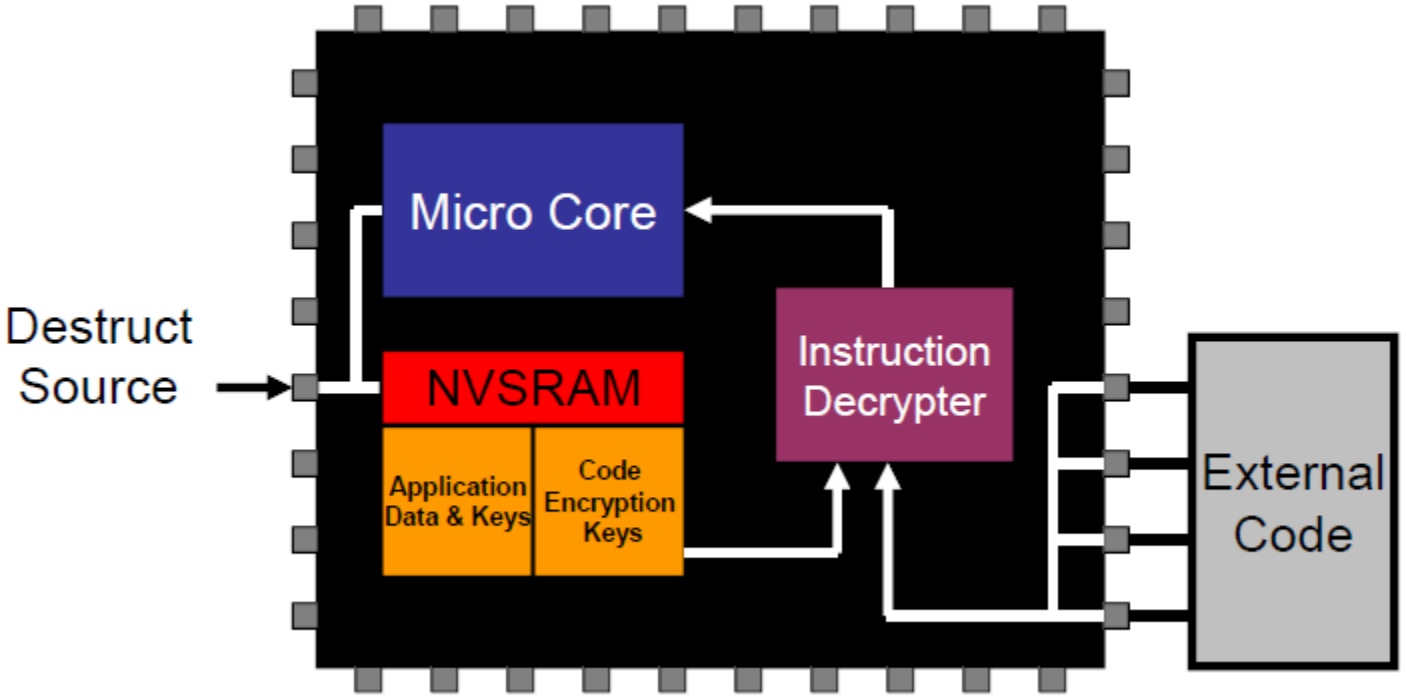
NOTES: 1. Once the fuse is blown, no further access to the JTAG/Test and emulation feature is possible and is switched to bypass mode.

Access to the MSP430 memory via the bootstrap loader is protected against misuse by a user-defined password.

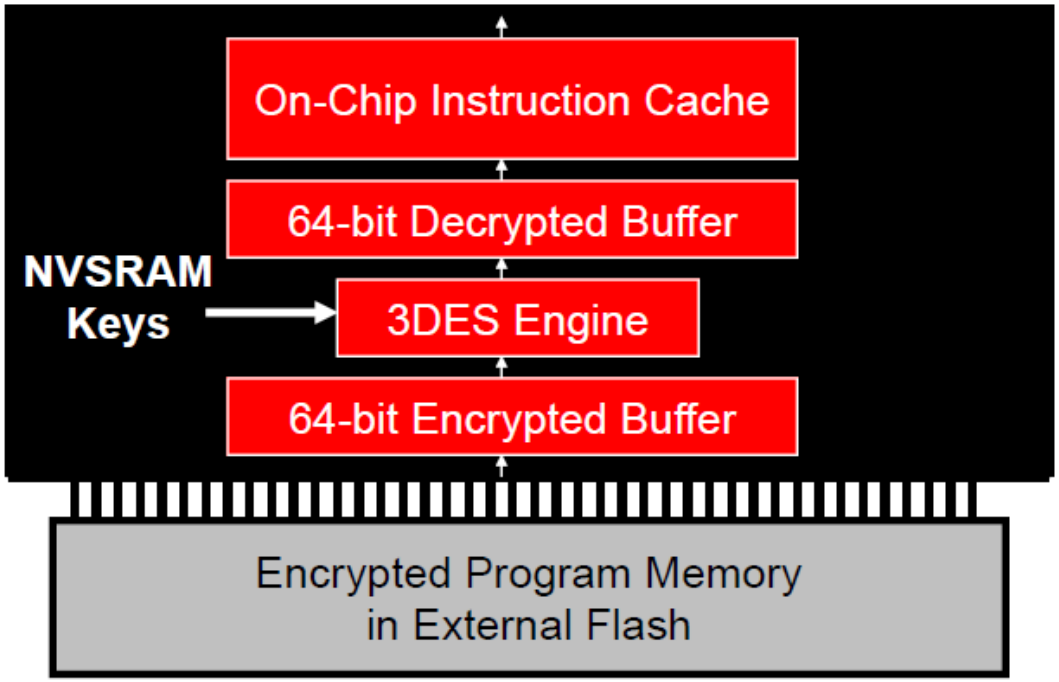
Secure Microcontroller Technology

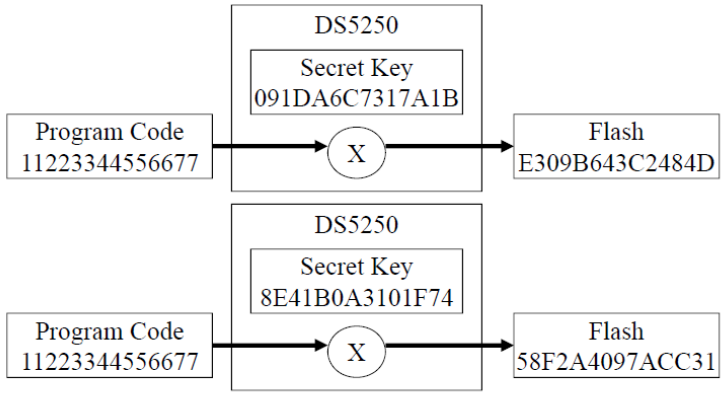
- Trusted for use in:
  - Financial Terminals
  - Medical Equipment
  - U.S. Government Applications
  - Tax Collection Equipment
  - Gaming Equipment

Battery Backed SRAM = STRONGEST Security



Program Code Encryption

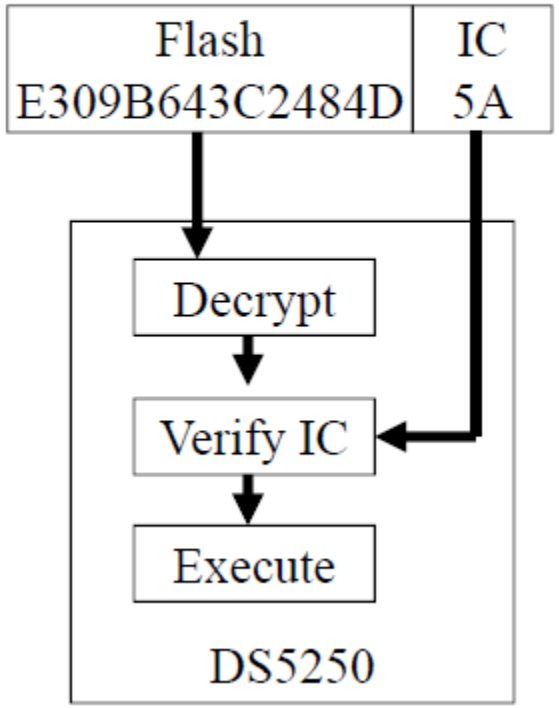




Encryption keys different on every device, so is encrypted flash

No Code Modification Allowed

- Code encryption makes it difficult for attacker to control execution…
- Integrity checking (optional) makes it practically impossible
  - –Integrity check added when code is loaded
  - –While running, if integrity check code wrong, self-destruct

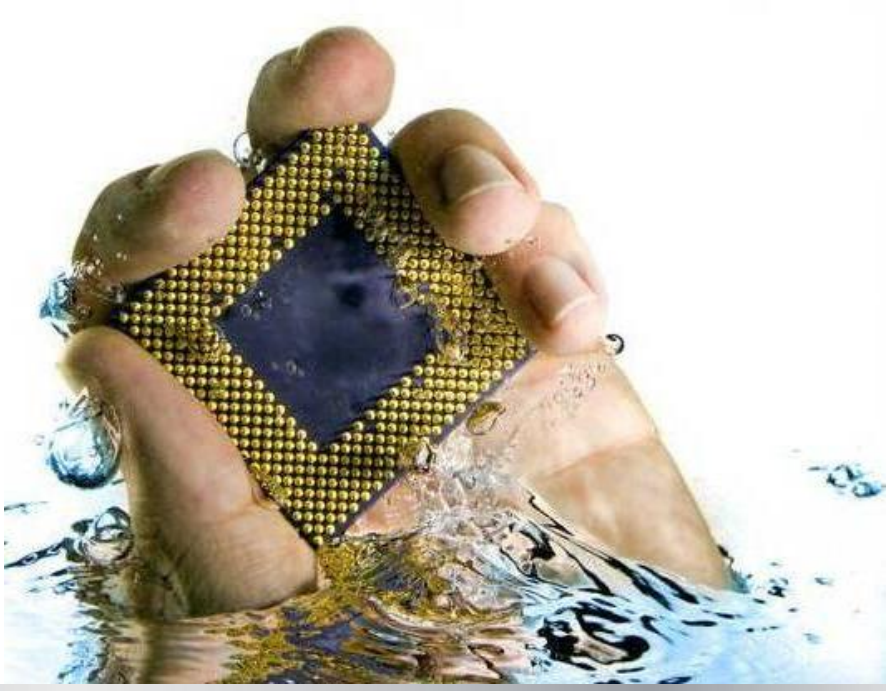


Cryptographic Support

Algorithm	DS5002	DS5250	MAXQ1103	MAXQ1850	MAXQ1004*	MAXQ1010*	USIP	ZA9L0/ZA9L1	Comments
DES	SW	✓	✓	✓	SW	✓	SW	SW	
3DES	SW	✓	✓	✓	SW	✓	SW	SW	Current standard for financial terminals
AES	SW	SW	SW	✓	✓	✓	✓	SW	
SHA-1	SW	SW	✓	✓	SW	SW	SW	✓	Standard one-way hash algorithm.
SHA-2	SW	SW	✓	✓	SW	SW	SW	SW	SHA-224 and SHA-256 in hardware. Others require SW support.
RSA	-	✓	✓	✓	-	-	SW	SW	
DSA	-	✓	✓	✓	-	-	SW	SW	
ECDSA	-	✓	✓	✓	-	-	SW	SW	

- **All crypto accelerators have high resistance to side channel attacks (SPA, DPA)**

Communication



MPC831xE Family

MPC8313E Block Diagram and Features

CPU
e300 processor built on Power Architecture technology, to 400 Mhz rev2.1

DDR2 Memory Controller
16b/32b DDR-333 / DDR2-333

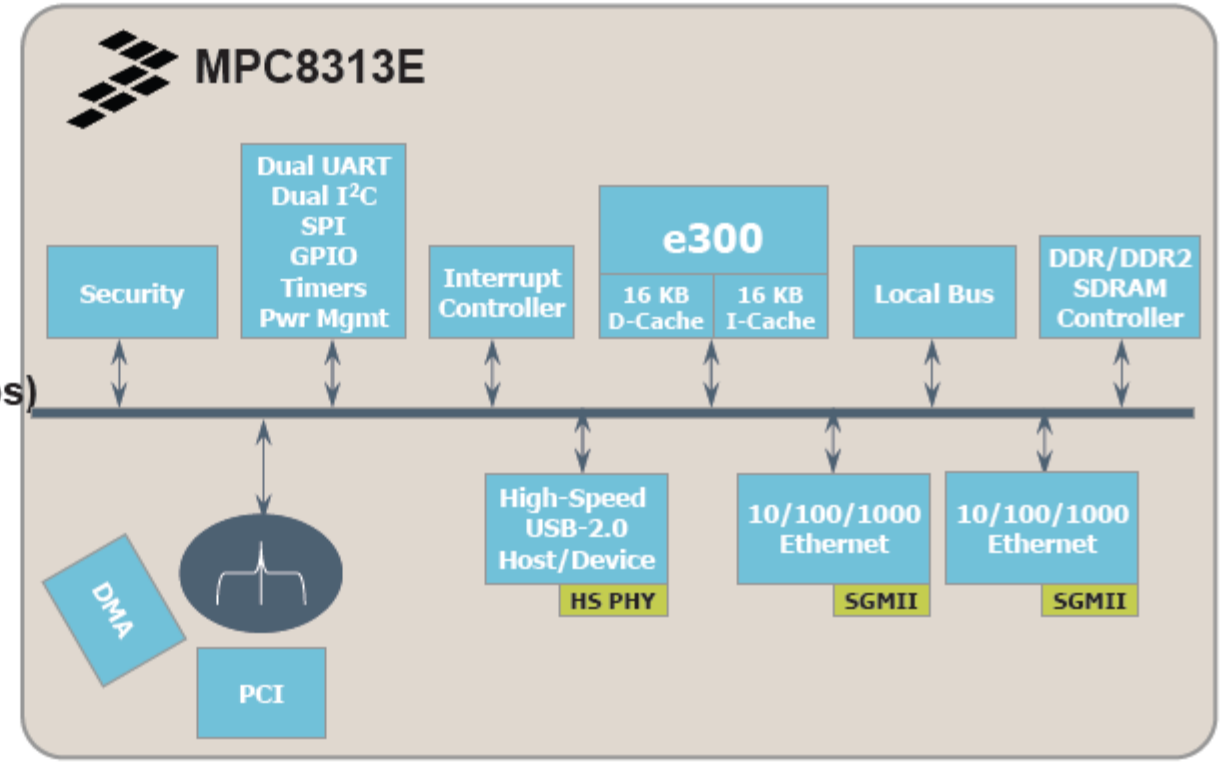
x2 10/100/1000 Ethernet MACs
Dual RGMII/RTBI/MII/RMII/SGMII
IEEE 1588 support VR 2 with rev 2.1

One High-Speed USB 2.0 (480 Mbps)
HS PHY supports host/device

Security (AES, DES, 3DES, SHA-1)

Power Management Controller
Low standby power

Technology and Package
CMOS90G, 1.0V core, 1.8/2.5/3.3V I/O
516 TEPBGAII



CC430F61xx/513x

MSP430+CC1101 RF transceiver Soc

Performance

- 16-bit Orthogonal RISC Microcontroller
- Ultra-Low-Power, Integrated Intelligent Peripherals and Easy-to-Use

Features

- **Power (typical target values at 25°C)**
  - Low Supply Voltage Range 1.8 V to 3.6 V
  - Ultra-low Power Consumption
    - CPU Active Mode: 180 µA / MHz
    - Standby Mode (LPM3 RTC Mode): 1.6 µA
    - Off Mode (LPM4 RAM Retention): 1.0 µA
- Ultrafast Wake-Up from Standby Mode in 5 µs
- **Package**
  - 64-Pin QFN: 9.1mm x 9.1mm (CC430F61xx)
  - 48-Pin QFN: 7.1mm x 7.1 mm (CC430F51xx)

Benefits

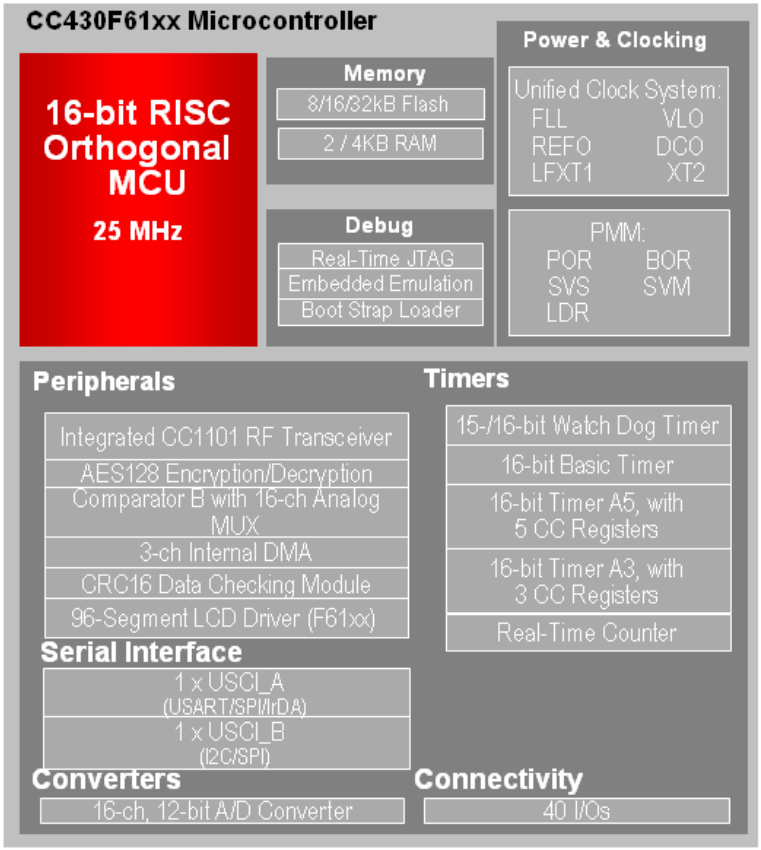
- High sensitivity & excellent blocking performance for reliable RF communication
- Flexible modulation formats and data rates ensure backwards compatibility
- Embedded packet engine and fast startup times reduce power consumption
- Reduces package size by 50%, saving PCB space and enabling smaller RF enabled products
- Integrated AES128 module provides fast, easy encryption/decryption of data for secure communications
- High analog performance ADC, comparator in an RF SoC

Development Board and Programmer

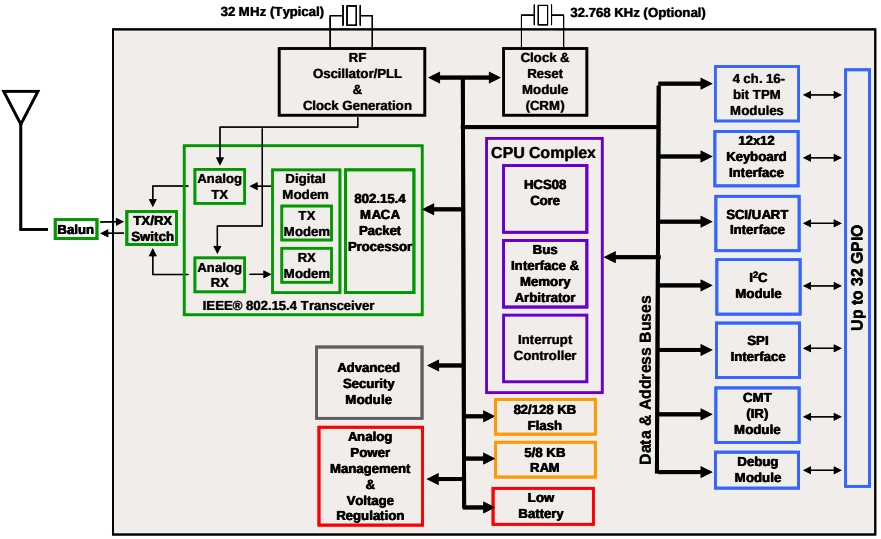
- CC430 EM board kit p/n:
  - EM430F6137RF900 (2EM Boards) - $149 (prelim)
  - FET430F6137RF900 (2 EM Boards + FET) - $199 (prelim)

Applications include:

- Smart remote controls
- Home security and automation
- Wireless sensors
- Sports monitoring equipment
- Energy harvesting industrial monitors



MC1323X Overview



- **Availability**
  - Samples: Q2 2010 (82 KB Flash)
  - Production: Q3 2010 (82 KB Flash)
  - Production: Q4 2010/Q1 2011 (128 KB Flash)

Overview	SoC - Integrated 2.4 GHz 802.15.4 Transceiver with Tx/Rx switch & MCU
	250 Kbps
Network Topo.	Peer-to-Peer, Star and Mesh
Software	SMAC, IEEE 802.15.4, RF4CE, SynkroRF, ZigBee
Sensitivity	<-96 dBm
Power Consumption	27 mA Rx 26 mA Tx (0 dBm)
Power Output	-30 dBm to +3 dBm (S/W selectable)
Memory	82 KB Flash, 5 KB RAM (MC13233C) 128 KB Flash, 8 KB RAM (MC13234C)
Security	AES128
Power Modes	5 low power, 4 run modes
I/O	Up to 32 GPIO, Timer, SPI, SCI, I²C, Up to 12x12 KBI, Carrier Modulated Timer (IR)
Crystals	32 MHz, 32.768 KHz (Optional), 32-bit RTC
Operating Volt.	1.8 to 3.6V with Low Battery Detect
Operating Temp	-40 to +85°C

RFID Security Migration

- Today there is growing concern about security of RFID solution
- Standard Mifare Crypto algorithm is no longer suggested for new design
- Mifare Ultralight C/ Mifare Plus/ Mifare DESFire EV1 provides much higher security based on standard 3DES and AES algorithms
- Silica Seriz provide software libraries support to ease the migration

	Mifare Ultralight	Mifare Ultralight C	Mifare Classic	Mifare Plus	Mifare DESFire EV1
Hw Crypto	-	3DES	crypto1	crypto1, AES	3DES, AES
EEPROM	512 Bits	1500 Bits	320 Bits, 1KB, 4KB	2, 4 KB	2,4,8 KB
Special Features	-	-	-	Mifare Classic compatible	-
Certification	-	-	-	CC EAL 4+	CC EAL 4+
Contactless Interface	ISO 14443 A (13.56 MHz, up to 10cm distance, 106- 848kBaud)				

NFC Application Categories

Card Emulation Mode

Transactions:

Mobile payment, Ticketing, Access control, Transit, Top-ups, Toll-Gate

Peer-to-Peer Communication

Connectivity:

Data transfer: Fast, easy & convenient device association, setup & configuration

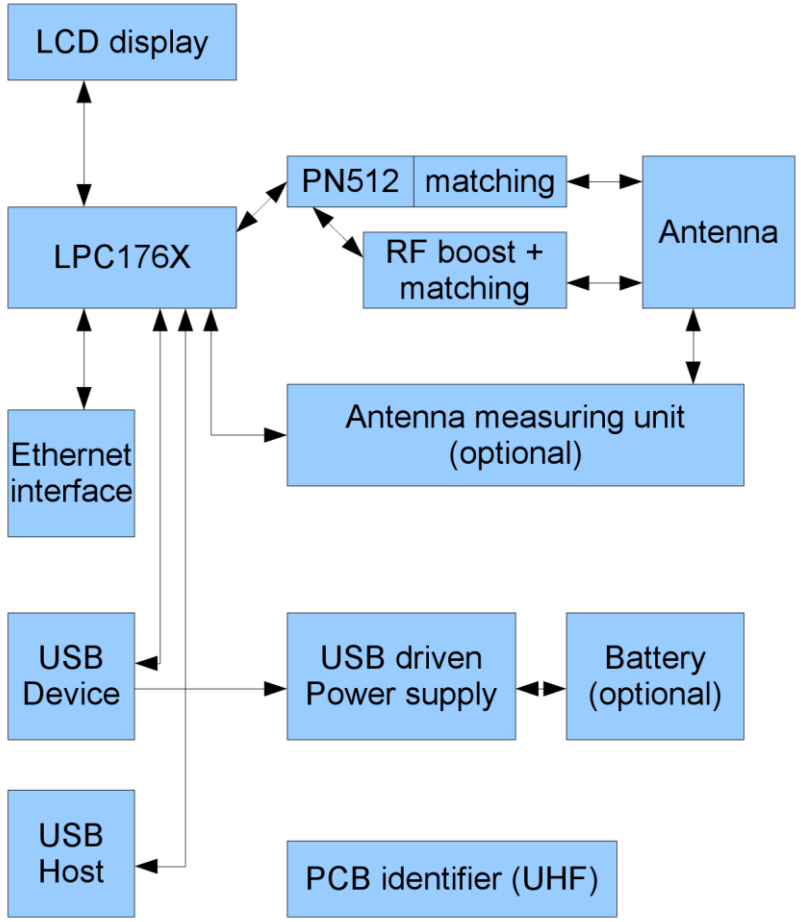
Reader Mode

Service Discovery:

Content distribution, Information access, Smart advertising

Hardware Features

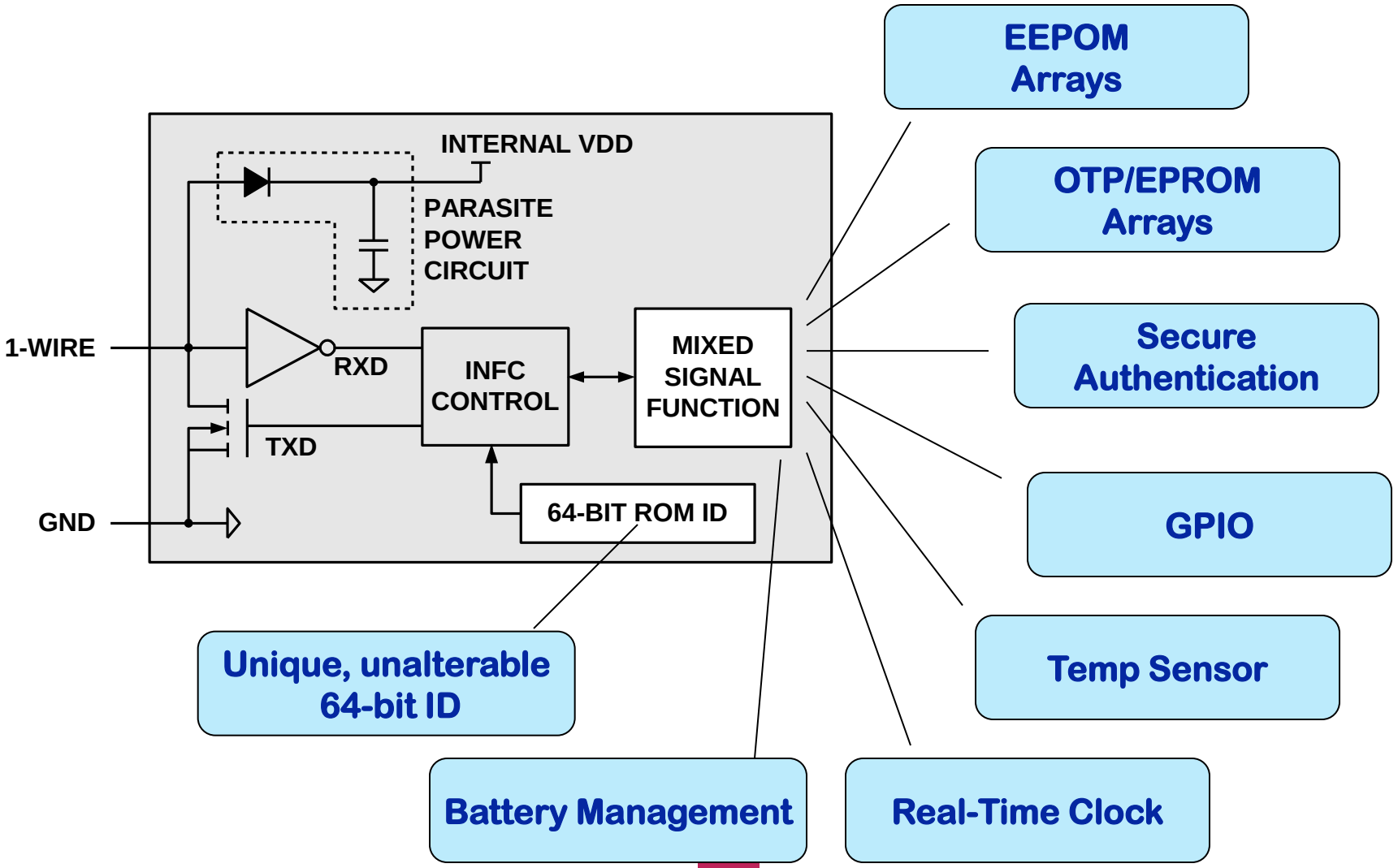
- NXP PN 512 -13.56 Mhz NFC Tranceiver
  - Supporting protocols: ISO 14443a, ISO 14443b, Felica, ISO 18092 (peer to peer)
  - Baudrate 106/212/424 Kbits
  - MIFARE classic security
- TDA 8029 Single card reader for supporting SAMs (Security Access Modules)
- G2XM SOT1122- Passive UHF RFID chip for board tracking identification
- Measuring Circuit for helping antenna matching calculation
- Power Amplifier (for additional reading range)
- NXP Cortex M3 LPC 1766
- USB Input Voltage with rechargeable LI-ION battery
- 2 x 16 LCD Display
- Ethernet Port
- USB Host port
- USB Device port
- JTAG and USB Debug Ports



Protection devices

November 4th, 2009

1-Wire Product Line

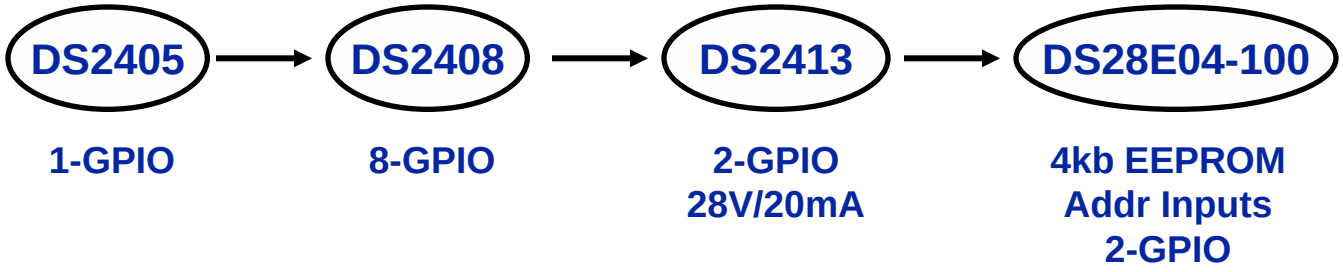


Solution Roadmap

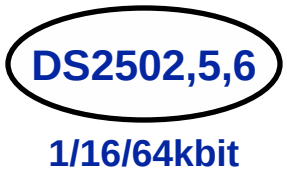
Silicon S/N

Low Density EEPROM

Mem+GPIO

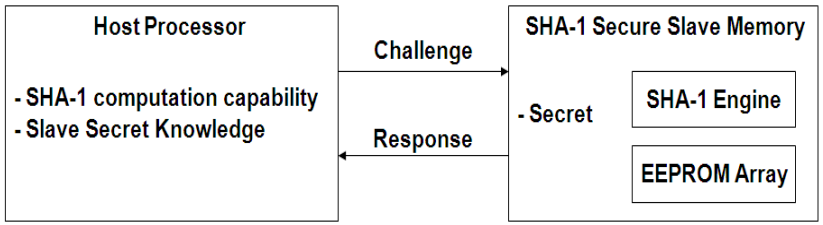


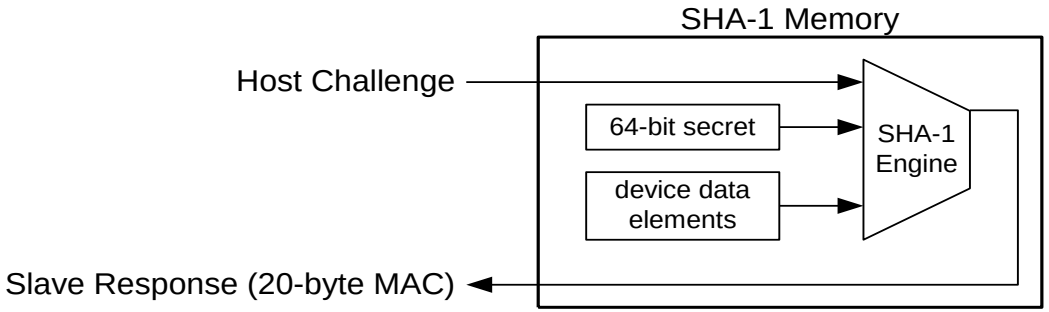
EPROM (OTP)



1-Wire Solutions

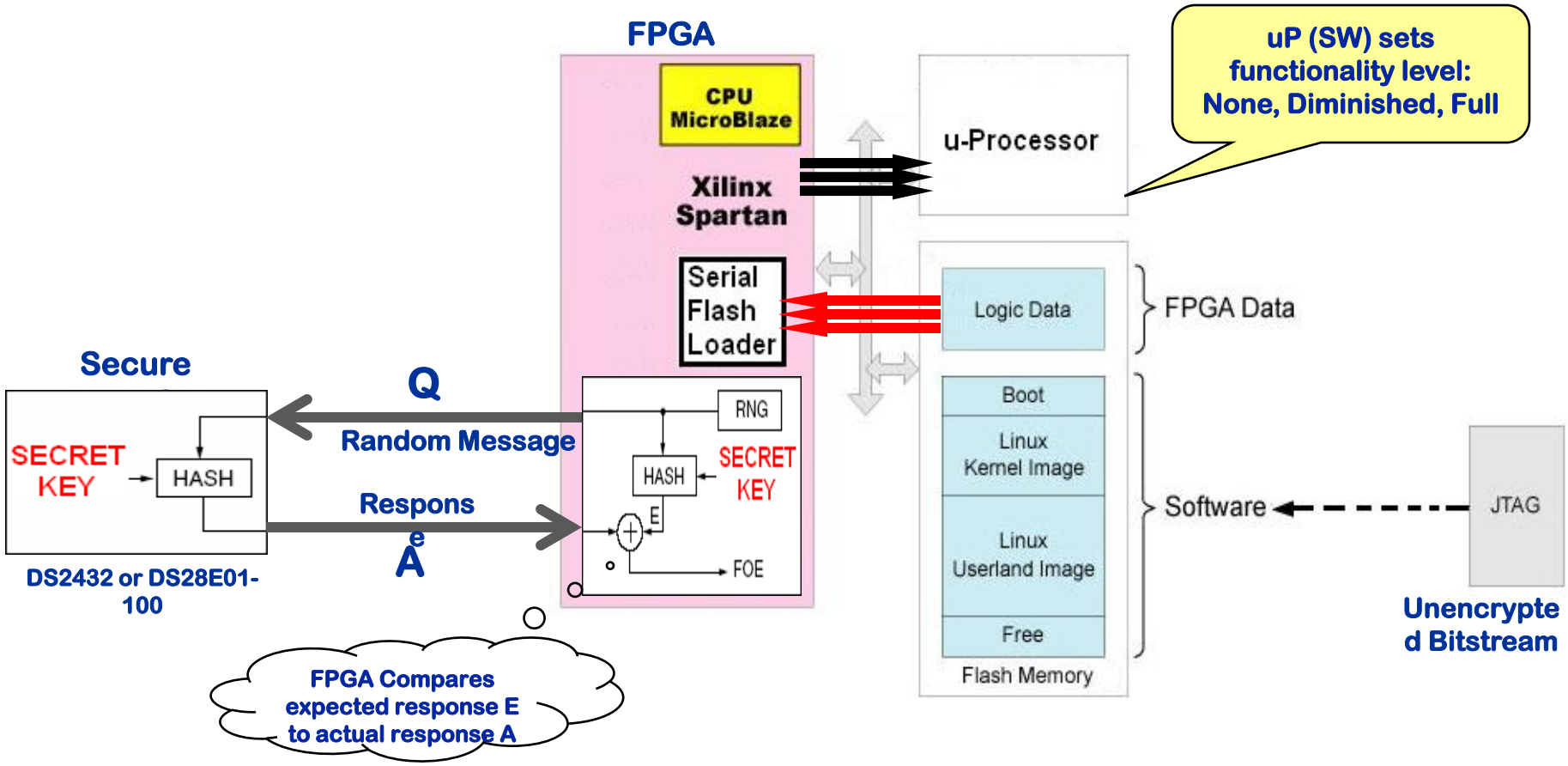
- Crypto-strong bi-directional authentication
- Secured general purpose EEPROM
- Security evaluation/consultation by industry experts
- Custom packaging developed for the consumable application





Device	Description	Security
DS28E01-100	1-Wire SHA-1 1kbit EEPROM	2-way SHA-1 authentication
DS28CN01	I2C/SMBus SHA-1 1kbit EEPROM	2-way SHA-1 authentication
DS28E01-200	1-Wire SHA-1 1kbit EEPROM	1-Way SHA-1 authentication
DS28E10*	1-Wire SHA-1 OTP (small density)	1-Way SHA-1 authentication

Protect FPGA against Cloning



Cost-optimized Copy Protection Scheme – Identification Friend or Foe (IFF)

Host Instrument Solutions

- **ICs, Synthesizable cores, Software, Apps Support**
  - **SHA-1 computation**

Device	Description	Notes
DS1WM	Synthesizable Verilog core: 1-Wire Line Driver	Gate count: 3470
DSSHA1	Synthesizable Verilog core: SHA-1 processor	Xilinx Spartan FPGA implementation: 72 flops, 475 LUTs and 2 block rams (254 slices).
DS2460	IC SHA-1 Co-processor	
DS2482-x00	I2C to 1-Wire line drivers	1 or 8 channel options
Discrete	Discrete 1-Wire line driving references	
SW	SHA-1, 1-Wire driving	

Dual Interface EEPROM : introduction

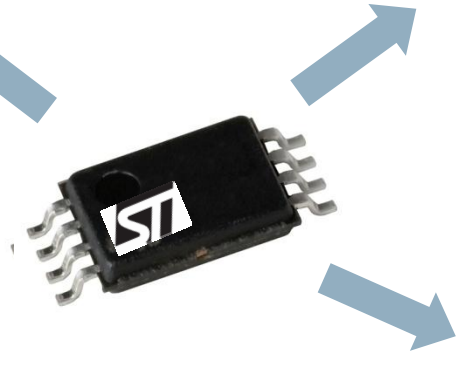
2 worlds now connected

I²C interface	EEPROM	RF interface

Dual Interface EEPROM: Target applications

Industrial, medical

- Calibration
- ID
- Parameter update
- Diagnostics
- Maintenance
- Asset tracking
- Activation



RFID

- ID
- Traceability
- Sensors/cold chain
- Data loggers
- Large RFID memory

Automotive (*)

- Diagnostics
- Maintenance
- ID
- Traceability
- Asset tracking

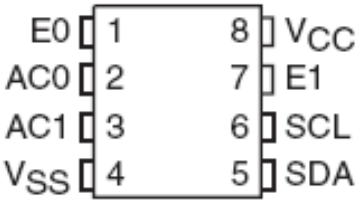
Peripherals, communication and consumer

- Parameter update
- Diagnostics
- Maintenance
- Traceability
- Asset tracking
- Activation

(*) Not an “automotive grade” product

Dual Interface EEPROM: M24LR64 feature set

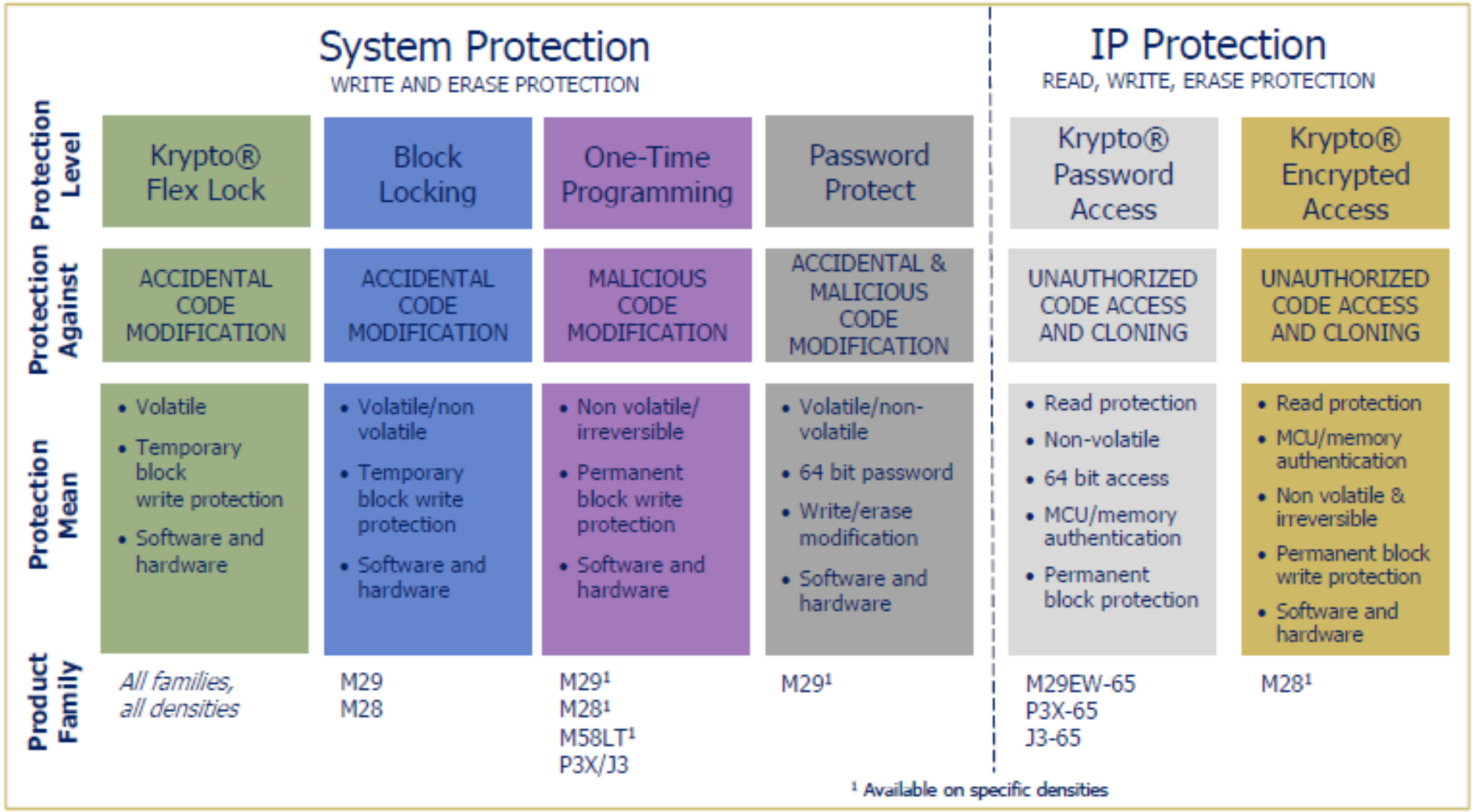
- EEPROM memory
  - 64Kbit **EEPROM memory**
  - **64-bit factory programmed/locked** unique identifier
  - **40 years data retention**
  - **1 million erase/write cycles (I²C)**
  - **100k erase/write cycles (RF)**
  - **32-bit** password **protection (write and/or read)**
- Serial bus access
  - **I²C, 400 kHz, 1.8 V to 5.5 V**
- RF access
  - **ISO 15693 – up to 53kb/s**
- Power supply
  - **Flexible power supply (RF and/or Vcc)**
- Packages
  - **TSSOP8, SO8, MLP8**
  - **Unsawn wafer and bumped dice**



NOR PROTECTION

Security Technology	Security Protection
Krypto® Encrypted Access	Protects blocks from being read or modified by requiring a 64-bit password (Note: this is ST Krypto)
Krypto® Password Access	Enables blocks to be set for OTP, and protect blocks from being read or modified by requiring a 64-bit password
Password Protect	Protects blocks from modification by requiring a 64-bit password
One-Time Programming (OTP)	Permanently protects blocks from modification
Krypto® Flex Lock	Software and hardware method of preventing writes or erases of blocks
Block Locking	Software method of protecting volatile and non-volatile blocks in an array
OTP Registers	User programmable OTP space to store unchangeable information
Hardware Write Protection	Prevents writes or erases of blocks by applying a certain voltage on a pin

NOR PROTECTION

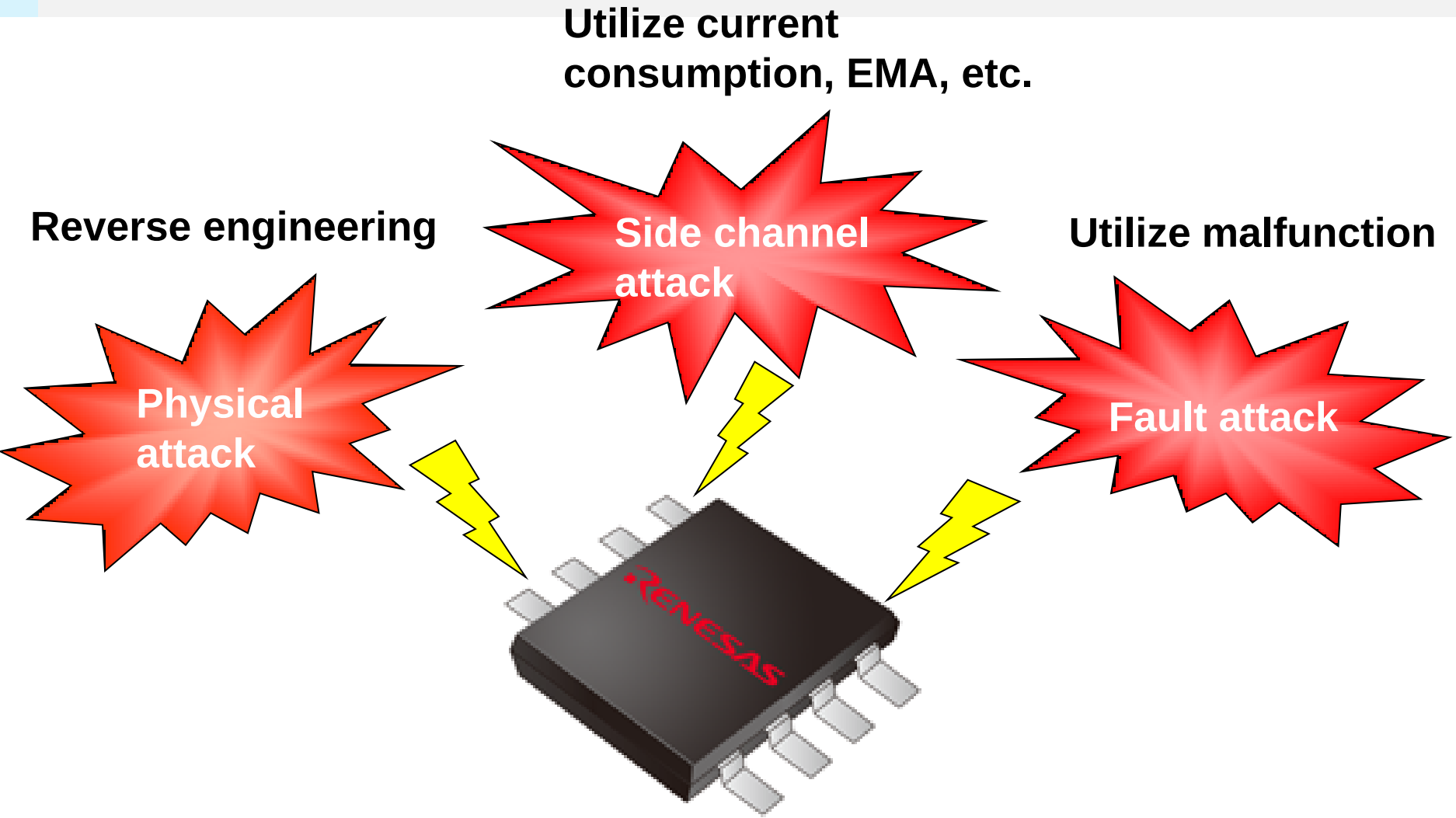


Board ID

Renesas Technology America, Inc.

November 4th, 2009

Attacks on Chip



EMA: Electro Magnetic Analysis

BID Example – Anti-Clone System

Hardware and

software tool

New architecture with Security IC

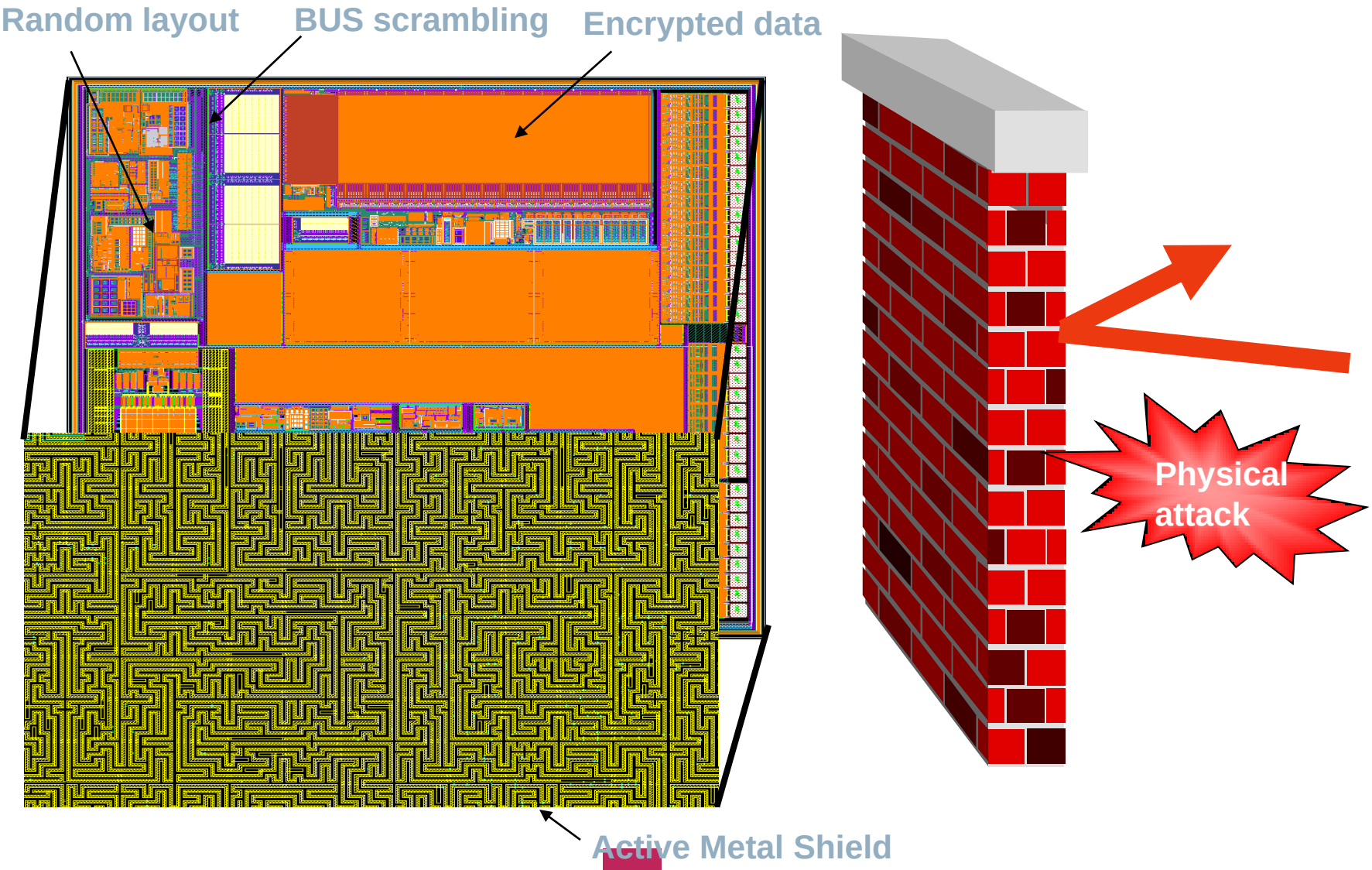
NOK

OK

→ Security IC in the architecture increases barrier to prevent easy cloning

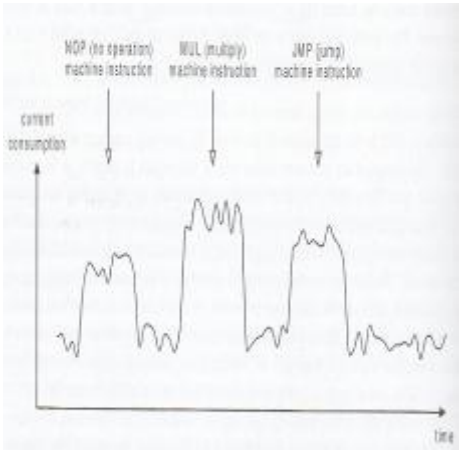
Examples	Use Cases / Business benefits	Key requirements
Communication Module	Anti cloning + IP Protection **Need to perform a very secure authentication to protect the IP of the Hardware / Tool set manufacturer** → Core Biz: Repeat sale of Modules	**Industry standards (Enterprise, IT, Govt.)** **Security strength (PKI)** **Must prevent easy manufacturing of cloned devices** **Long product lifetime**

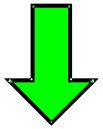
Physical Protection

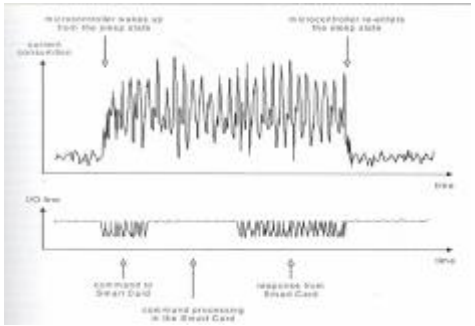


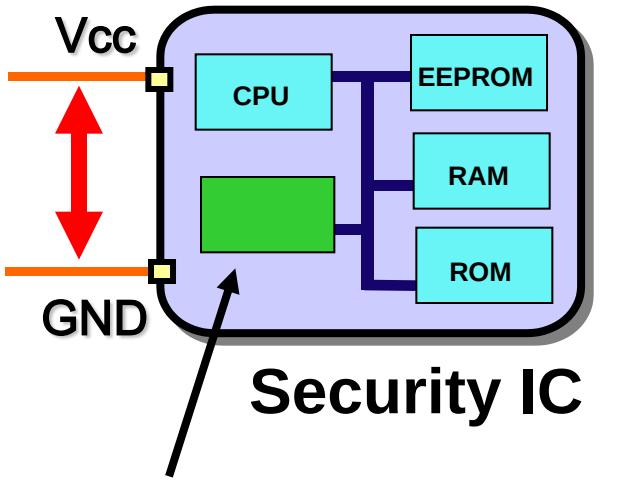
Protection from Power Analysis

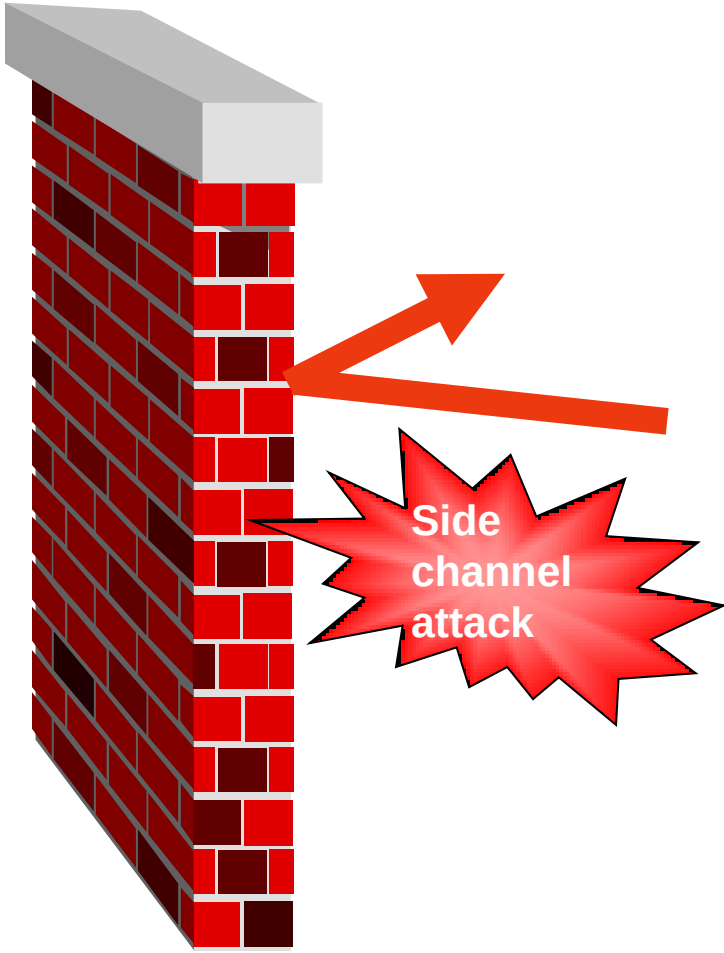
SPA: Simple Power Analysis
DPA: Differential Power Analysis





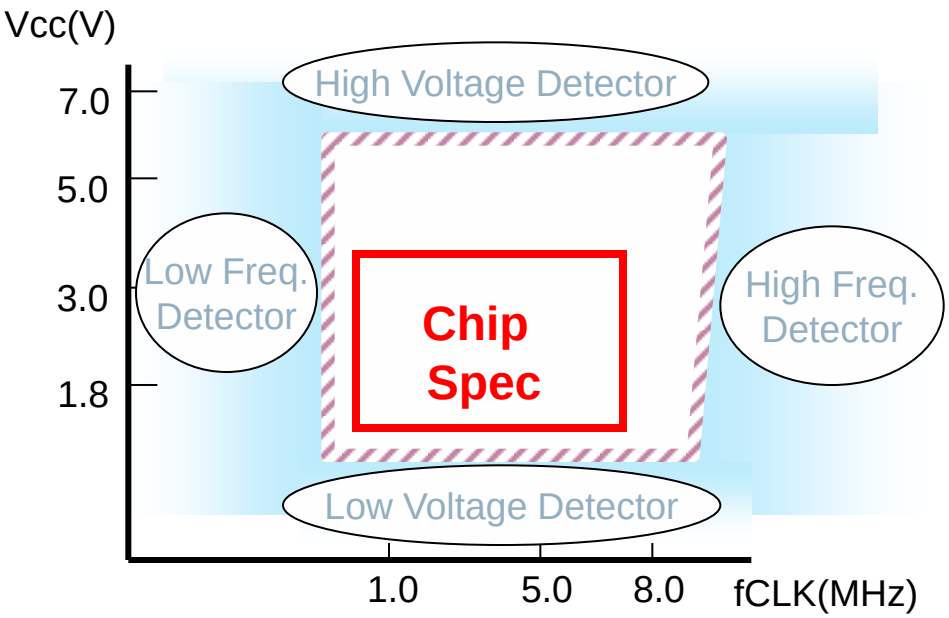




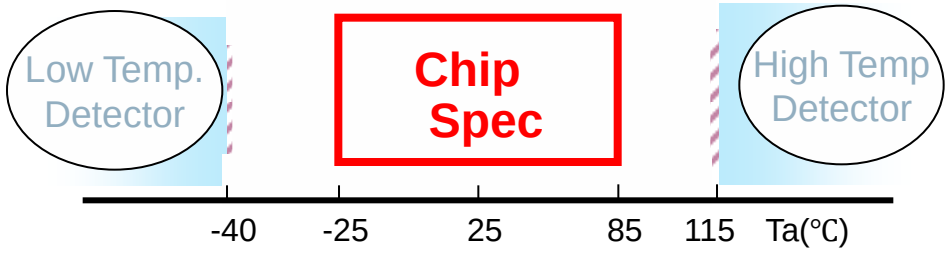


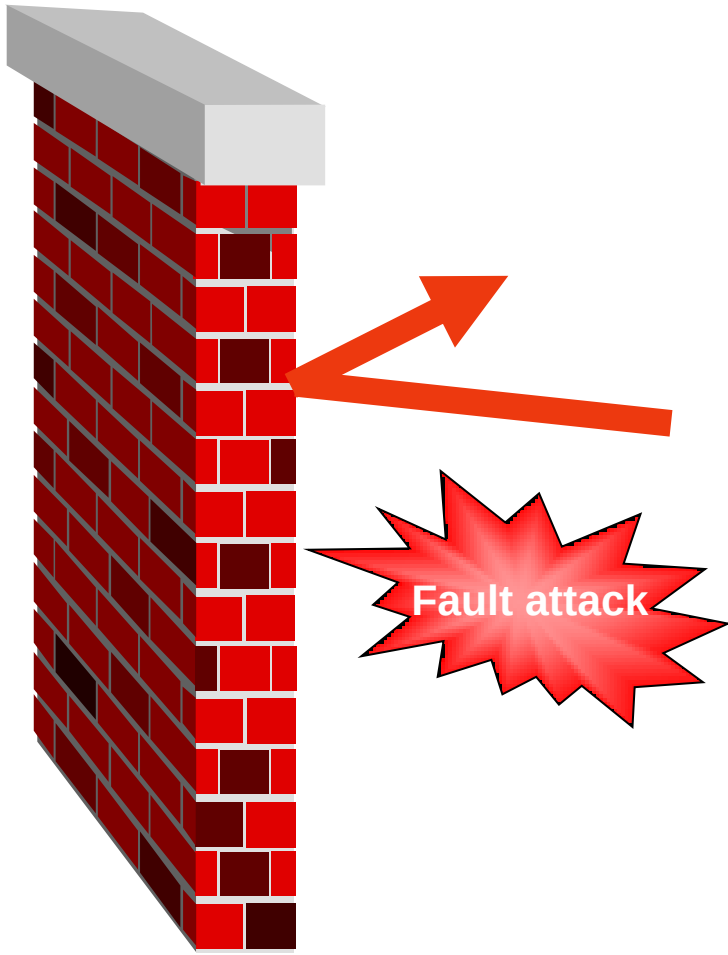
Security Sensors

- Frequency - Voltage characteristic

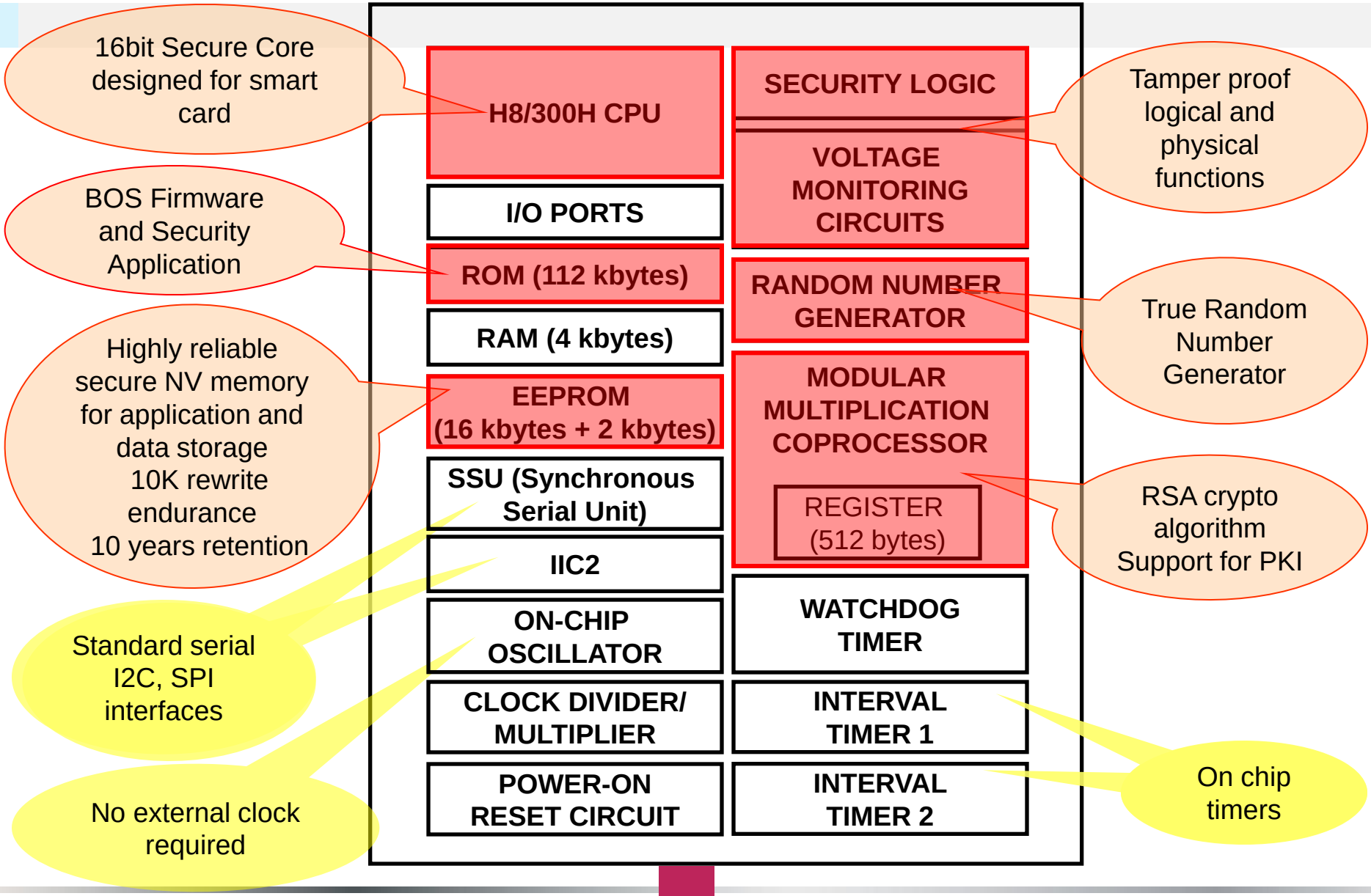


- **Temperature active range**

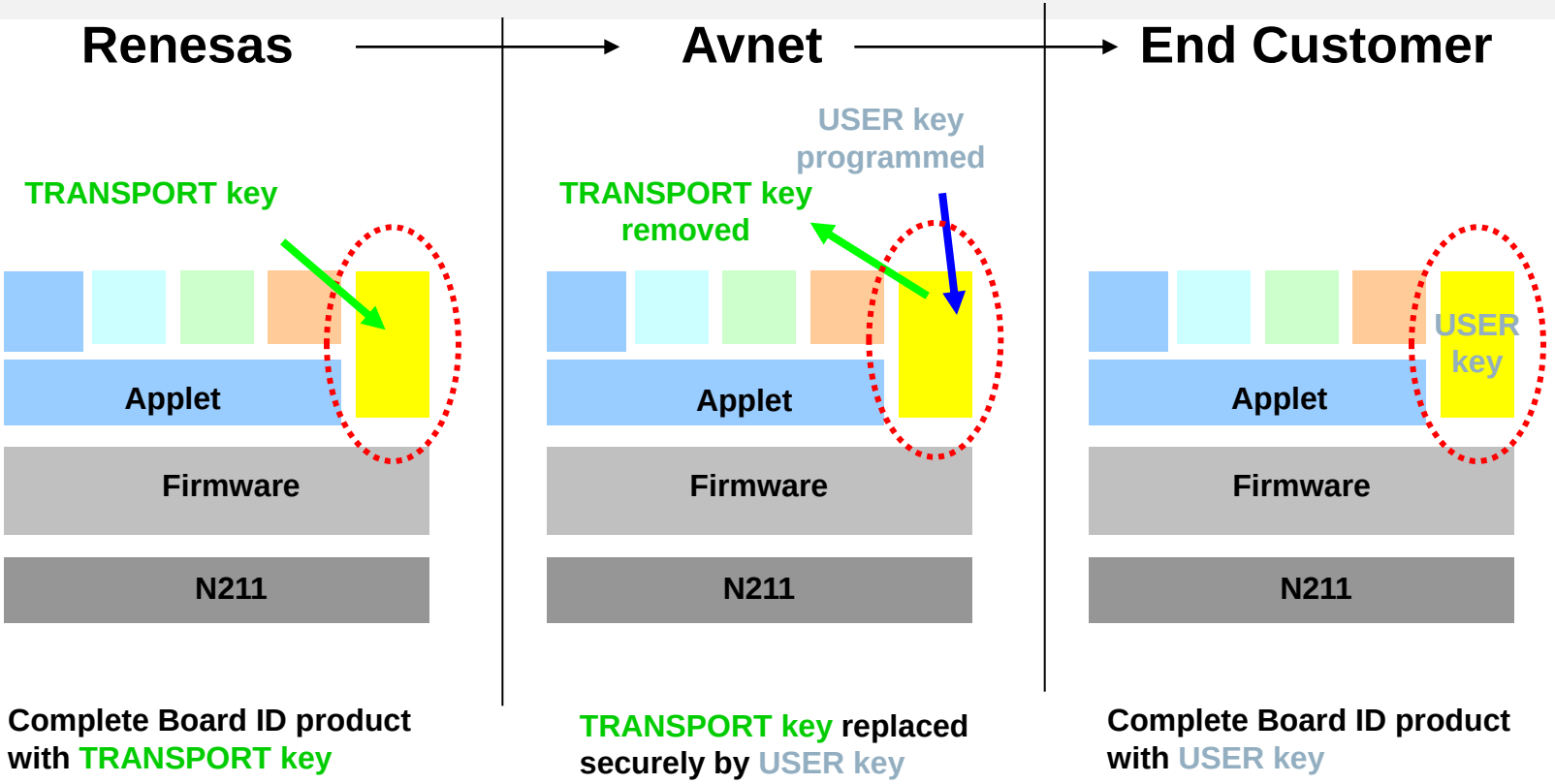




N211 Block Diagram

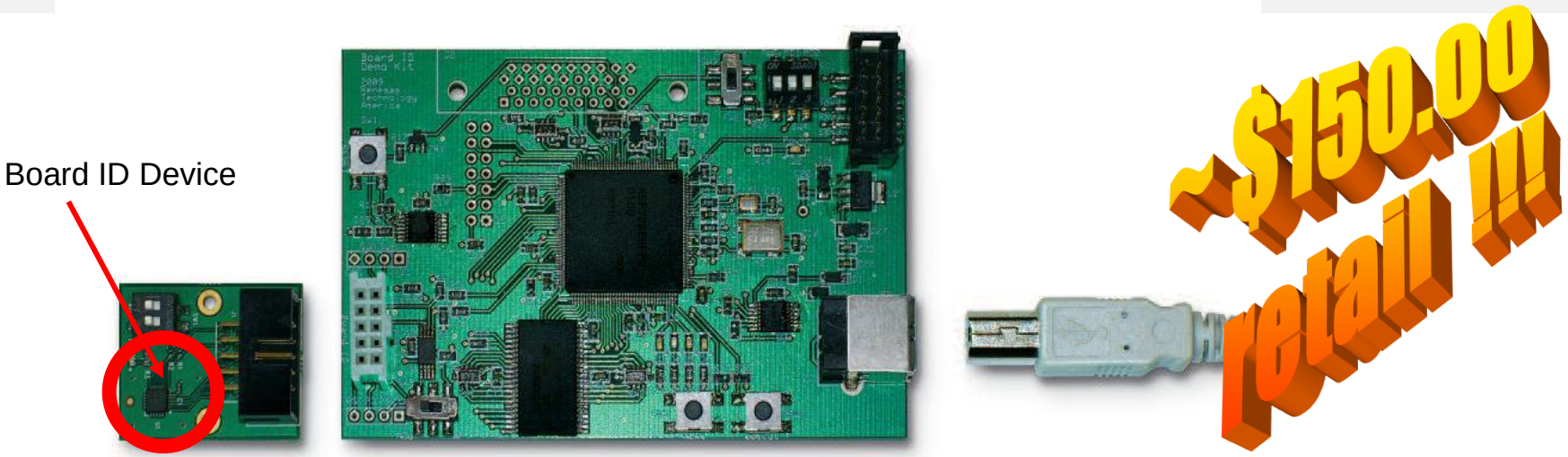


Key programming for Production units



- ***Renesas programs the product with the application in EEPROM and a TRANSPORT key specific to Avnet***
- ***TRANSPORT key is unique to Avnet: only Avnet can inject USER keys***
- ***Without the USER key, the product is unusable (will not respond)***
- ***Avnet is responsible for the production and programming of the USER keys on behalf of the end customers***
- ***Sample units have the same application but are equipped with a 'sample' certificate.***

New demo kit with a MCU (SH-2A) and Board ID



1. Capable to show authentication demo
2. Customers can modify authentication condition w/o coding on device side
3. Authenticator can be MCU, other Board ID device or external server
4. Authenticator software is provided as Board ID Security Stack (BSS)
5. BSS Manager software helps customer to go through authentication steps
6. Anti-Cloning, Usage Control, Secure Tracking and IP Protection use cases
7. Only I2C driver, debug port and NV access need to be ported to the target MCU

- **Thank you !**