NXP（恩智浦） MCU产品线

战略及新产品介绍

APF-INS-T2270

JULY 2016

PUBLIC

SECURE CONNECTIONS
FOR A SMARTER WORLD

A NEW POSITION OF STRENGTH

~45,000 Employees

11,000+ Engineers

35+ Countries

9,000+ Patents

FOCUSING NXP SOLUTIONS ON HIGH GROWTH MARKETS

Secure, **Connected Vehicle**

- ADAS: Radar, V2X, Vision, Fusion, network processor
- Car entertainment
- In-vehicle networking
- Secure car access
- Secure car

End-to-end **Security & Privacy**

- Mobile transactions
- E-Government
- Smart bank cards
- User authentication
- Embedded security
- Cloud & Infrastructure Security

Smart, **Connected Solutions**

Consumer

- Mobile audio
- High-speed Interfaces
- Smartphone RF
- Personal health & fitness
- Healthcare

Industrial

- Smart home & buildings
- Smart cities, smart grid
- M2M, Industry 4.0
- Intelligent logistics
- 4.5G/5G Networks

日程

- NXP’s MCU产品线战略及路标
- Kinetis 5V新产品介绍：KE1X
- Kinetis安全类新产品介绍：K8X及KL8X

恩智浦MCU产品线

为何客户选择我们

- **加入了各种**软件及硬件等生态环境**工具的支持**
- **在客**户支持、质量及长生命周期供货等方面始终处于业界领先地位
- **与众多的合作伙伴共建生**态系统
- 为大众市场提供完善的应用案例，方便中小用户的上手及应用裁剪

Example Customers

BOSCH Invented for life, AVNET, ARROW, Digi-Key, Electrolux, ABB, FLEXTRONICS, GREE, EMERSON Network Power, Haier, GARMIN, Continental, Honeywell, Insulet Corporation, Microsoft, MOUSER ELECTRONICS, SONOS, SONY, LAB126, Schneider Electric, SIEMENS, Whirlpool

Products

Kinetis & LPC 32-bit ARM® Microcontrollers	i.MX ARM® Applications Processors

Applications

Wearable / Healthcare
- Health / Fitness & Wireless Healthcare
- Diabetes & Cardiac Care
- Diagnostics & therapy

Smart Home
- Smart meters & grid
- Integrated wireless connectivity solutions
- Home energy control

Smart Accessories
- Game controllers and consoles
- Wearable computing
- eReaders, tablets, portable navigation

Vehicle Networking & Information
- Infotainment, software define radio
- Navigation systems, E-call

Home Appliances
- Energy efficient refrigerators, dishwashers
- Human-machine interface
- Connected appliances

Factory Automation & Drives
- Machine-to-machine
- Motor control
- Industrial networking

MCU-专业源于专注

ARM技术专家	获得了最多的ARM核的授权：M0、M0+、M3、M4、M7、ARM9、A7, A8、A9…超过1000个基于ARM核的产品
广阔的MCU产品组合	在工业领域的产品线上，从性能、存储、外设资源等方面拥有最丰富的选择
完善的开发工具	将基本的ARM开发工具应用于 Kinetis 及 LPC 系列，并扩展出许多新的特性
领先的生态环境	与业界领先的合作伙伴通力协作，提供从开发板到操作系统，再到多种协议栈的支持，共同助力客户的产品设计
以客户为中心	继续坚持做最好的客户支持模式，向客户提供最好的产品，最优的服务

世界范围及中国MCU的排名Y2015

MCU 全球排名

2015 Rank	Company Name	2015 Revenue($)
1	Renesas Electronics Corp	3,138
2	New NXP	3,017
3	Microchip + Atmel	2,093
4	Infineon Technologies	1,504
5	ST Microelectronics	1,504
6	Texas Instruments	1,206
7	Cypress Semiconductor	675
8	Samsung	376
9	Toshiba	193

通用 MCU 全球排名

2015 Rank	Company Name	2015 Revenue($)
1	Microchp + Atmel	1,763
2	Renasas	1,299
3	New NXP	902
4	ST Microelectronics	796
5	Texas Instruments	713
6	Cypress Semiconductor	486
7	Infineon	190
8	Silicon Labs	151
9	Toshiba	140

* Exclude all ASSP (Auto, etc.)

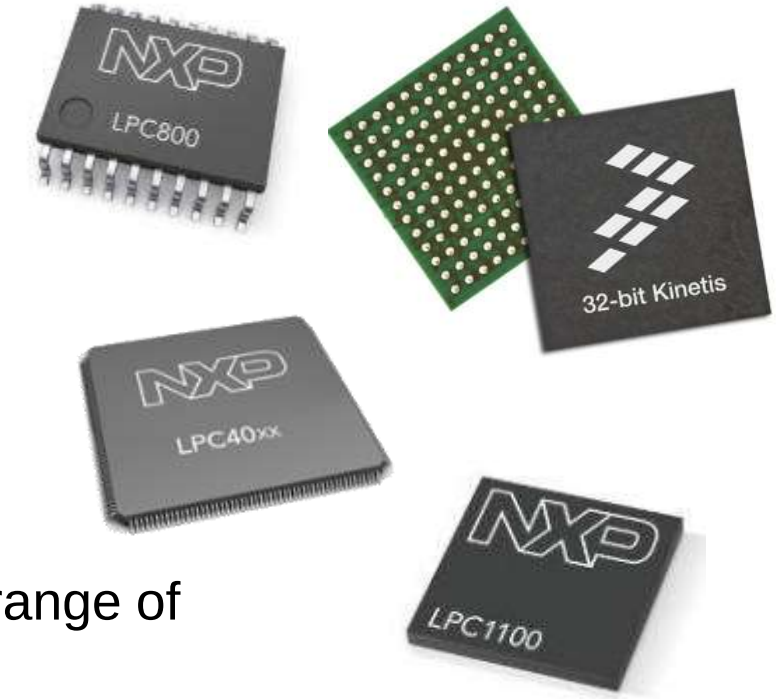
通用 MCU 中国排名

2015 Rank	Company Name	MS%
1	New NXP	37%
2	ST Microelectronics	36%
3	Nuvoton	6%
4	Atmel	4%
5	Silicon Labs	2%
6	Infineon	2%
7	Texas Instruments	2%
8	Spansion	2%
9	Others	8%

* Exclude all ASSP (Auto, etc.)

** Data source: IHS & IHS China*

Strength in Product Longevity
长生命周期支持



- NXP (both NXP LPC and former Freescale) have longstanding records of **providing long-term production support** for our products
- NXP has a **formal product longevity program** for the market segments we serve
  - For the automotive and medical segments, NXP will make a broad range of solutions available for a minimum of **15 years**
  - For all other market segments in which NXP participates, NXP will make a broad range of solutions available for a minimum of **10 years**
  - **Life cycles** begin at the time of launch
  - Includes NXP's standard end-of-life notification policy
- For a complete list of participating products, visit, nxp.com/productlongevity

MCU生态环境支持

操作系统及软件协议栈

NXP Solutions:

Kinetis SDK/LPCOpen
- Drivers
- System Services
- FreeRTOS
- USB
- TCP/IP
- Filesystem

MQX PEG

Kinetis Bootloader

RTOS, Middleware Partners:

freeRTOS Micrium ARM mbed Green Hills SOFTWARE SEGGER www.segger.com wolfSSL expresslogic

Comprehensive frameworks and solutions for low-power, connected, and secure embedded systems

软件开发工具

IDE / Toolchains:

LPCXPRESSO IAR SYSTEMS Kinetis Design Studio freescale ARM KEIL Microcontroller Tools SOMNIUM DRT atollic

Software Configuration:

Kinetis Expert
- Power Estimation
- BSP Tools
- Project Generator
- Power Analyzer

PEG Processor Expert Software freescale

Industry leading IDE support and intuitive software configuration tools to accelerate application development

硬件评估板

Evaluation Kits:

LPC Xpresso

Freedom Development Platform

Tower System

Partner Solutions

SEGGER www.segger.com PE micro 1 SYSTEM LAUTERBACH DEVELOPMENT TOOLS

LPC-Link2

Low cost hardware platforms for evaluation and application development. Partner solutions for hardware debugging solutions

特定应用

HomeKit
- HomeKit SDK
- Motor Control
- Wireless Charging
- Sensor Fusion
- MFi
- PEG GUI
- POS / EMV

Connectivity Solutions

Bluetooth SMART 6LoWPAN EtherNet Wi Fi THREAD GROUP 802.15.4

Software frameworks and development tools for targeted applications and certified connectivity solutions

在线及现场支持服务

Broad Market:
- OOB Walkthroughs
- NXP Community
- Embedded Blogs
- Kinetis Designs
- Kinetis Tutorials
- Application Notes
- Symbols & Footprints

High Touch:
- Professional Support
- Professional Services

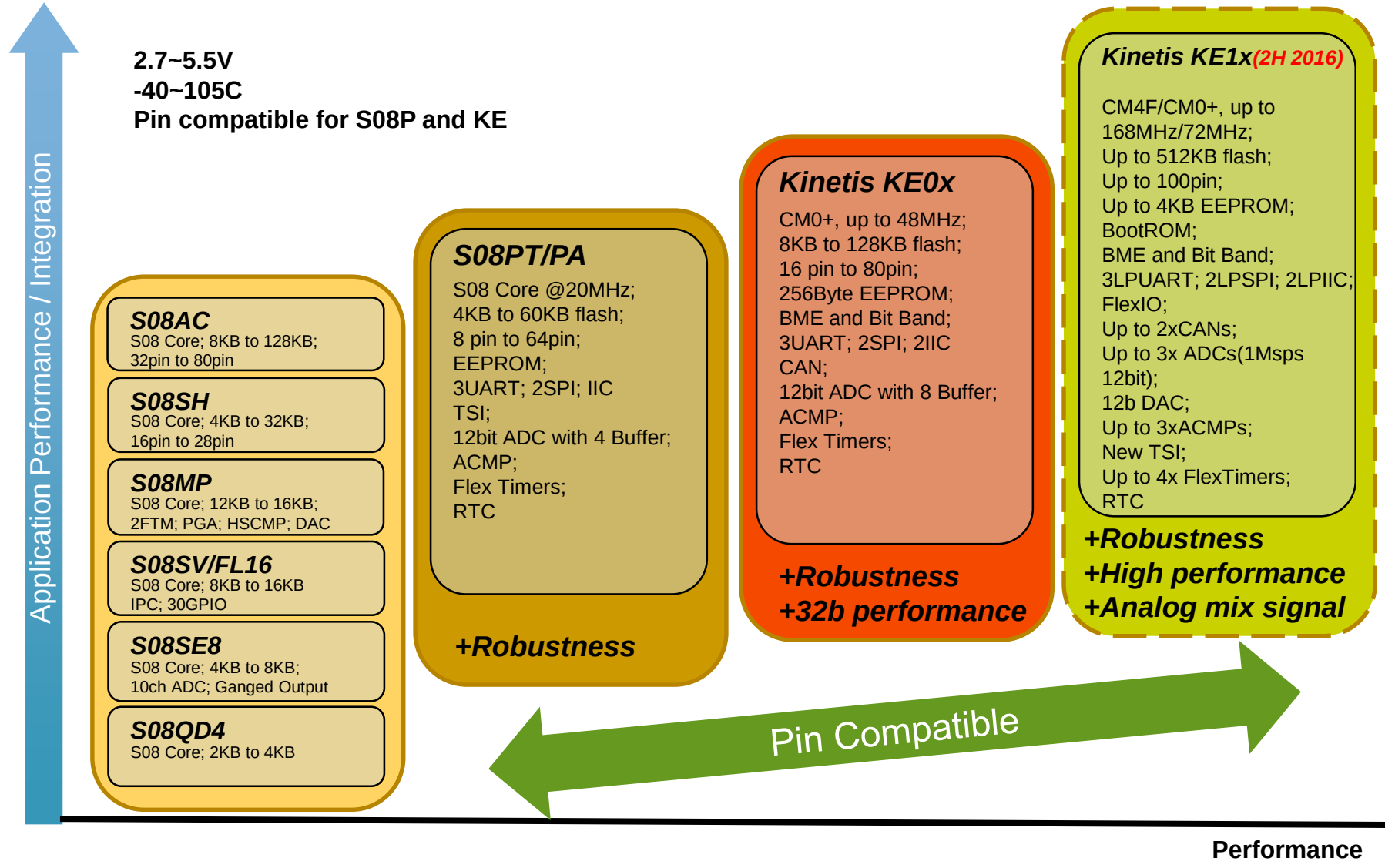
Get started quickly and get the support you need, when you need it

New KE1x Series

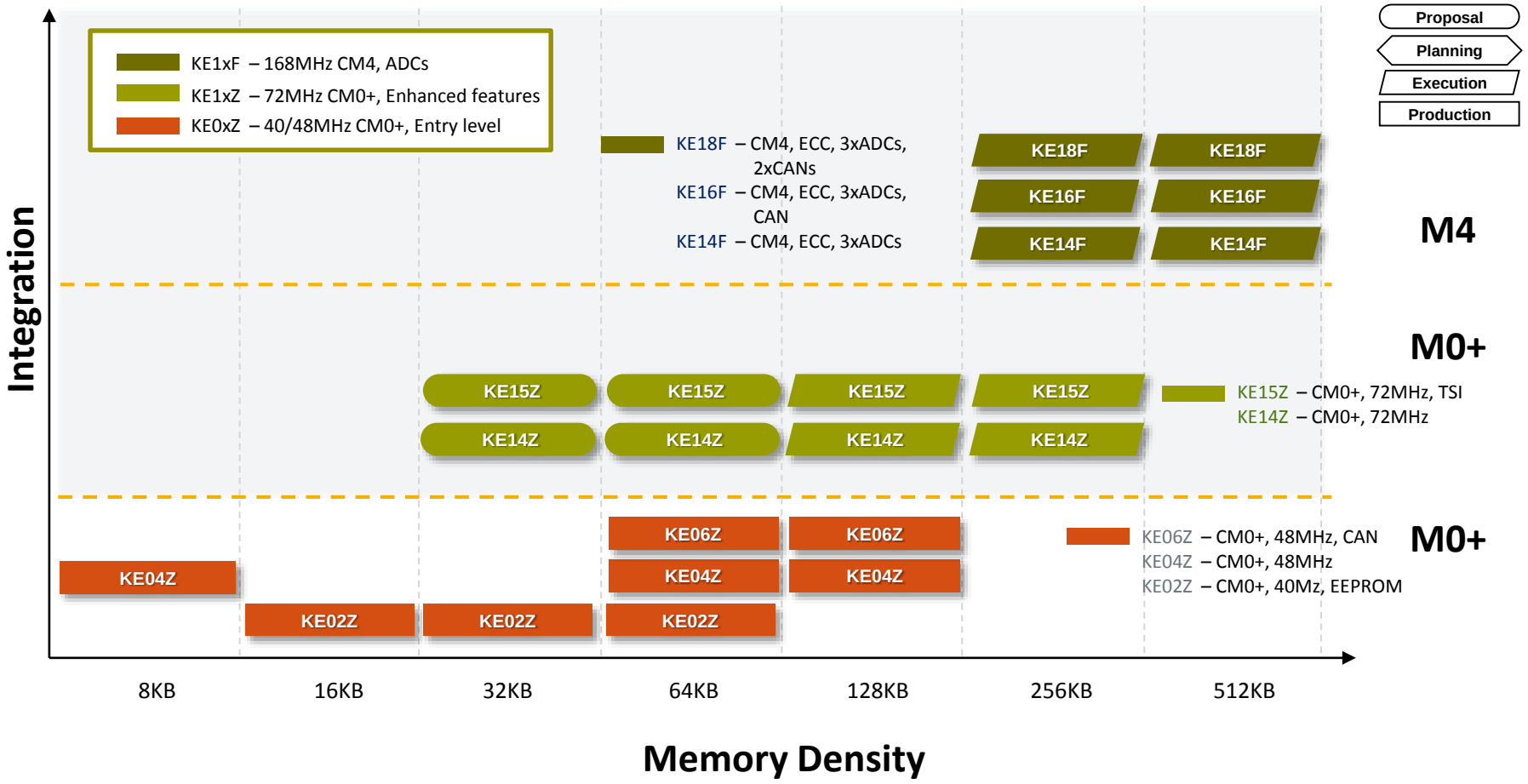
- **提供更多内存**资源，更多外设特性以及更强处理性能的5V Kinetis E系列家族

KINETIS E 路标

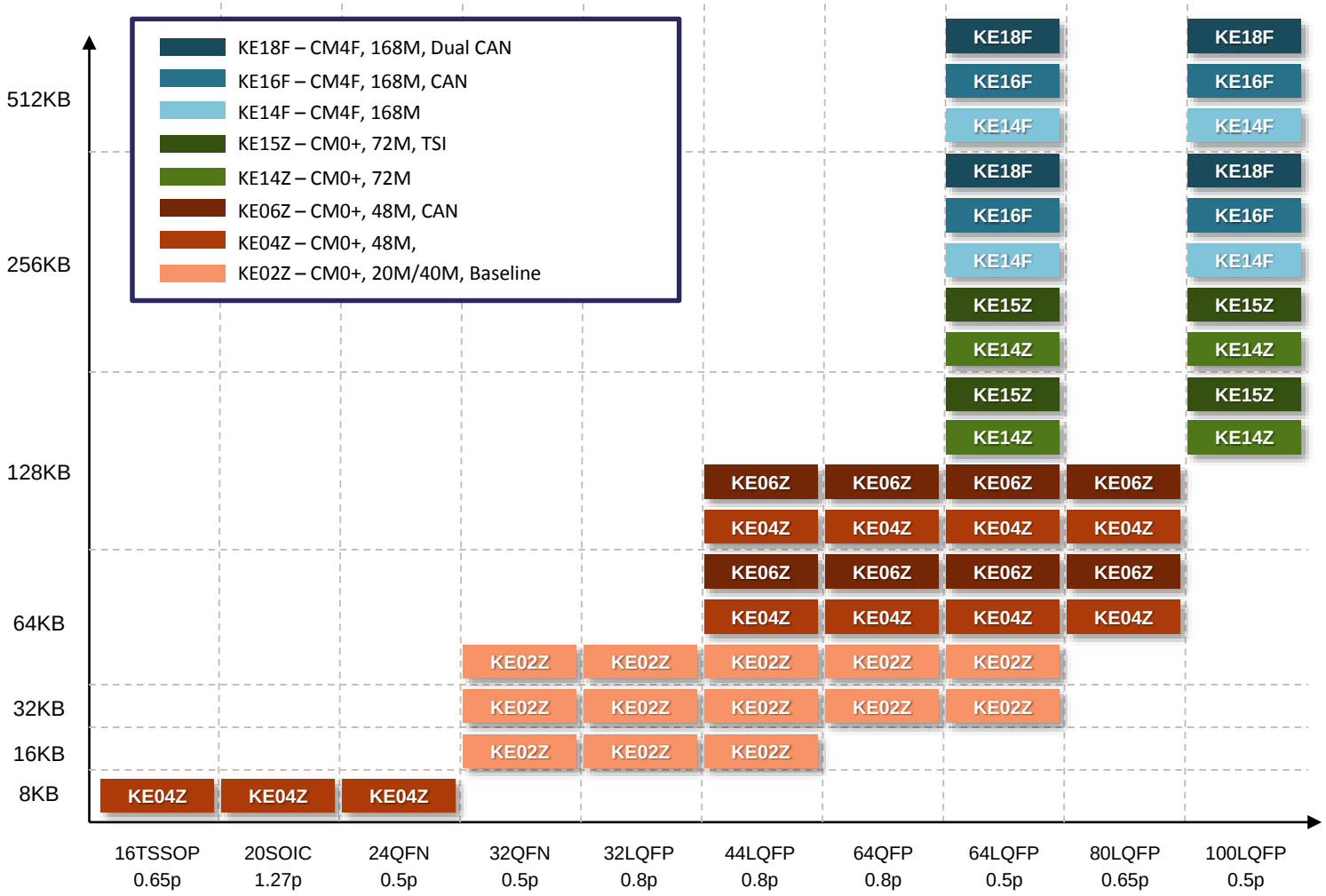
5V产品线的历史及产品更新



Kinetis E 系列的产品家族



基于封装及内存大小分类



- 2.7~5.5V, -40 to +105C
- High EMC/ESD robustness
- Pin compatible within Kinetis E

KE0xZ产品特性

Key Features:

Core/System
• ARM® Cortex® -M0+ up to 48MHz

Memory
• up to 128KB Flash
• up to 16KB SRAM
• up to 256B EEPROM

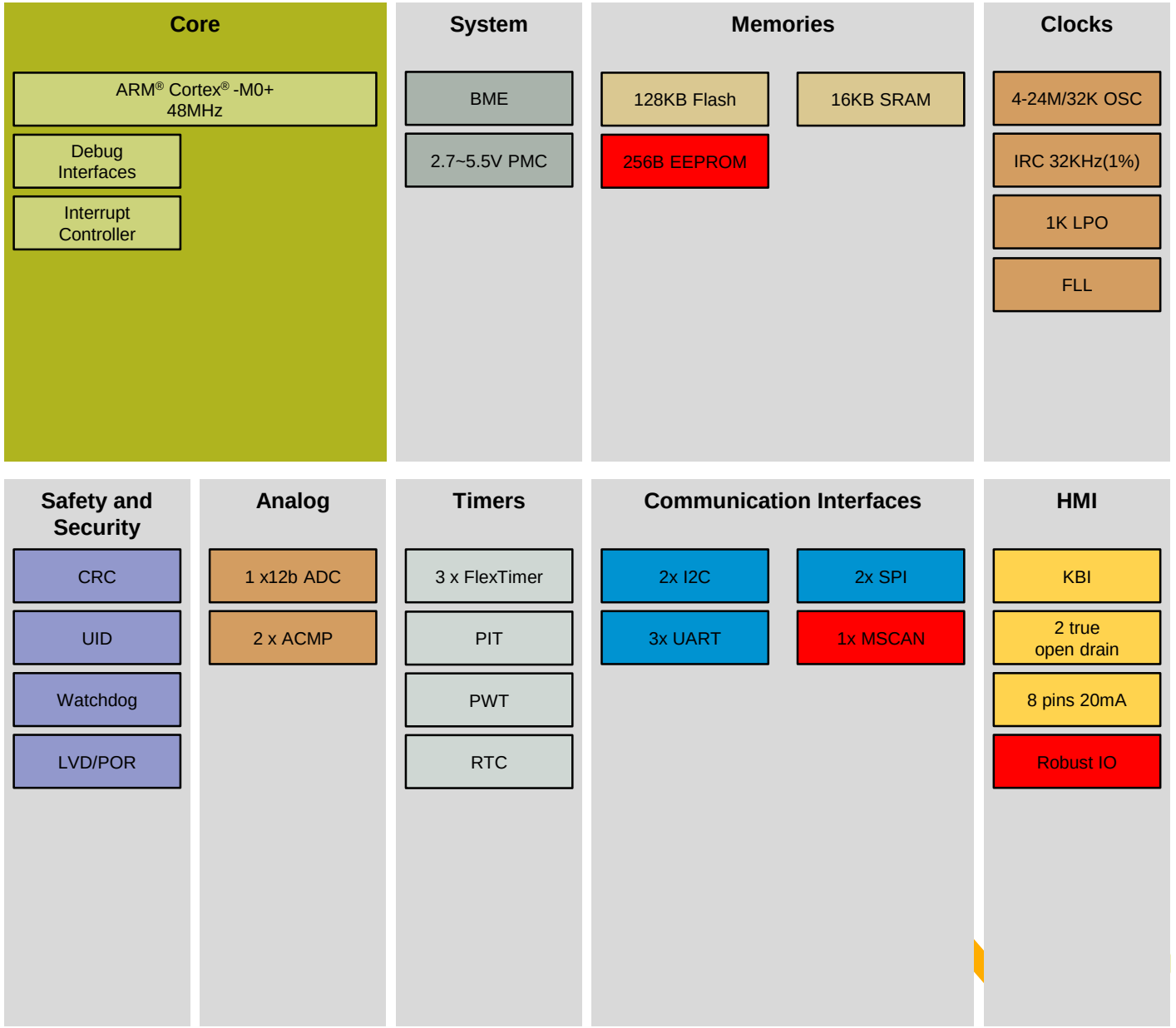
Communications
• 1 x MSCAN
• 3 x UART / 2 x SPI / 2 x I2C

Analog
• 1 x 12b ADC
• 2 x ACMP

Timers
• 1 x 6ch FTM (PWM)
• 2 x 2ch FTM (PWM)
• 1 x PIT / 1 x PWT
• RTC

Others
• Up to 71 I/Os
• 2.7-5.5V, -40 to 105ºC

Packages: 80LQFP(0.65mm pitch)
64LQFP(0.5mm pitch)
64QFP(0.8mm pitch)
44LQFP(0.8mm pitch)
32LQFP(0.8mm pitch)
32QFN(0.5mm pitch)
24QFN(0.5mm pitch)
20SOIC(1.27mm pitch)
16TSSOP(0.65mm pitch)
Pin compatible within KE



KE1xZ产品特性

Key Features:

Core/System
- ARM® Cortex®-M0+ up to 72MHz
- 8ch eDMA
- TRGMUX
- MMDVSQ

Memory
- up to 256KB Flash
- up to 32KB SRAM
- up to 32KB FlexMemory / 2KB EEPROM
- Boot ROM

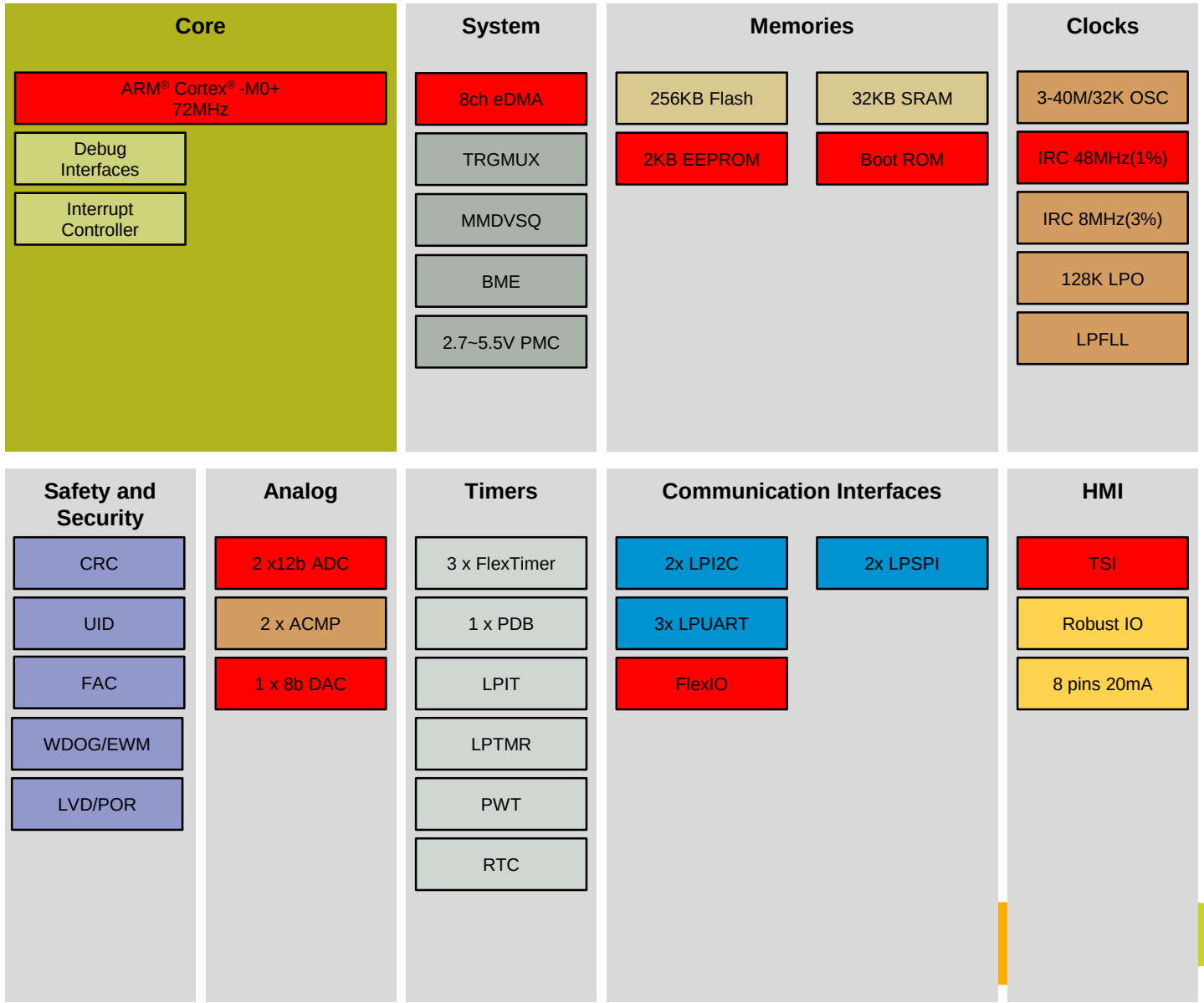
Communications
- 3 x LPUART / 2 x LPSPI / 2 x LPI2C / FlexIO

Analog
- 2 x 12b ADC, 1MSPS
- 2 x ACMP
- 1 x 8b DAC

Timers
- 1 x 8ch FTM (PWM)
- 2 x 4ch FTM (PWM/Quad Dec.)
- 1 x PDB
- 1 x 4ch LPIT / 1 x LPTMR / 1 x PWT
- 1 x RTC

Others
- Up to 36 keys TSI
- Up to 89 GPIO with glitch filter
- 2.7-5.5V, -40 to 105ºC

Packages: 100LQFP(0.5mm pitch)
64LQFP(0.5mm pitch)
Pin compatible within KE



KE1xF 产品特性

Key Features:

Core/System
- ARM® Cortex®-M4F up to 168MHz
- 16ch eDMA
- TRGMUX
- MPU

Memory
- up to 512KB Flash with ECC
- up to 64KB SRAM with ECC
- up to 64K FlexMemory / 4KB EEPROM
- 8KB I/D Cache
- Boot ROM

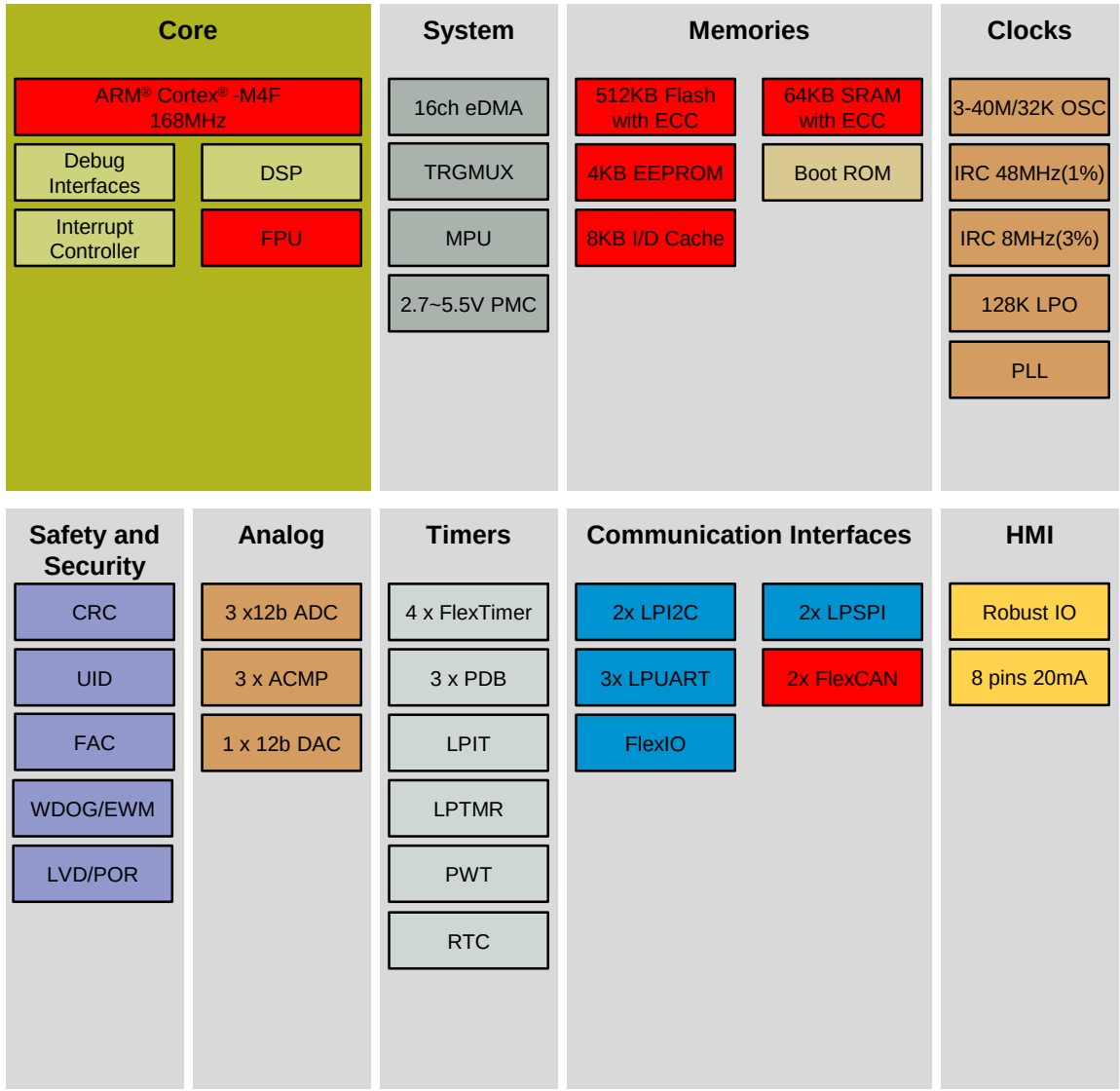
Communications
- 2 x FlexCAN
- 3 x LPUART / 2 x LPSPI / 2 x LPI2C / FlexIO

Analog
- 3 x 12b ADC, 1MSPS
- 3 x ACMP
- 1 x 12b DAC

Timers
- 2 x 8ch FTM (PWM)
- 2 x 8ch FTM (PWM/Quad Dec.)
- 3 x PDB
- 1 x 4ch LPIT / 1 x LPTMR / 1 x PWT
- 1 x RTC

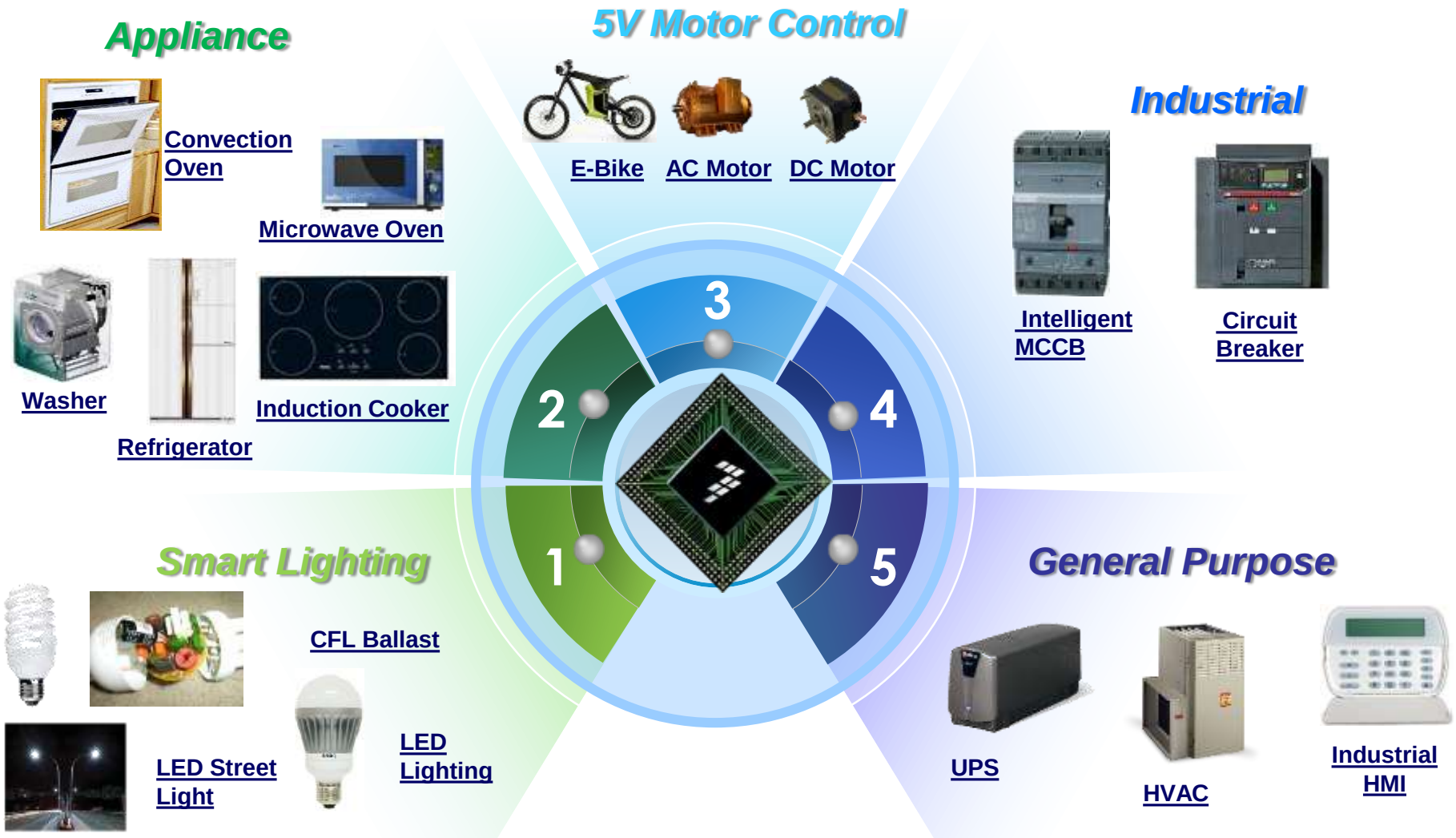
Others
- Up to 89 GPIO with glitch filter
- 2.7-5.5V, -40 to 105ºC

Packages: 100LQFP(0.5mm pitch)
64LQFP(0.5mm pitch)
Pin compatible within KE



KE1X 典型应用

Kinetis E Series 目标市场及典型应用



KE1X 关键特性

强抗干扰、安全特性

Feature category	Description
I/O强抗干扰	I/O支持5V电压输入输出，并带有数字滤波功能
安全运行库	提供自有的符合IEC60730 class B标准的安全库
带有ECC检查的RAM [1]	SRAM拥有ECC错误纠正功能，单bit错校正、双bit错检测
带有ECC检查的Flash [1]	Flash拥有ECC错误纠正功能，单bit错校正、双bit错检测
CRC校验	支持16bit/32bit的基于可编程多项式的CRC校验
片上看门狗	拥有内部看门狗，并支持内部时钟
时钟失锁监视器	片上集成时钟失锁监视器，监视外部时钟是否正常，如果存在失锁现象，将产生中断预警或者复位
内存保护单元	专属的内存保护功能能够防止意外或者非法的内存访问
Flash访问控制	Flash 访问控制单元(FAC) 能够用于保护用户的代码不被窃取，保护软件知识产权
Flash 安全性	Flash安全选项，除了能够屏蔽外部对Flash内容的探测，同时也能防止Flash内容被误擦除。

1: KE1xF only

Robust & Safety – EMC 性能

测试条件

- PKE18F512VLL15
- IH Cooker as the test platform
- System level tests based on
  - IEC 61000-4-4(EFT)
  - IEC 61000-4-2(ESD)

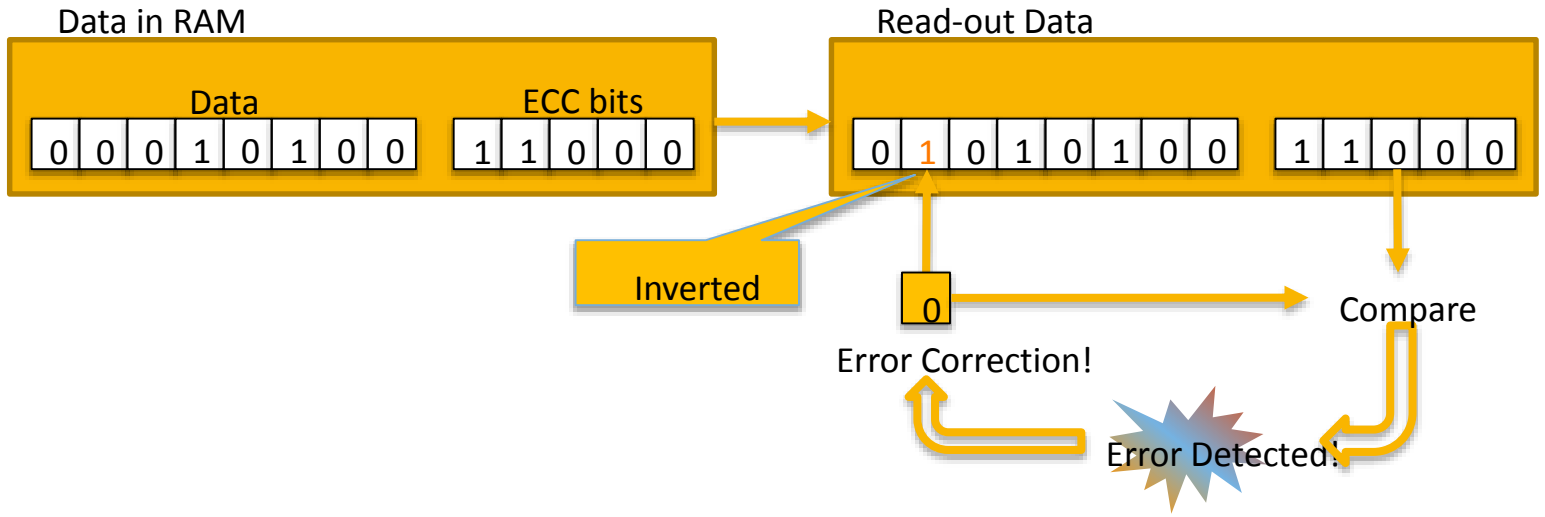
测试结果

- System level
  - IEC 61000-4-4(EFT):+/- 4.5kV*
  - IEC 61000-4-2(ESD): Contact Discharge(at the case) +/- 20kV
  - IEC 61000-4-2(ESD): Air Discharge (at the control panel) +/- 15kV

*Limited by the test equipment max output voltage

Robust & Safety – Error Correction Code[1]

- RAM ECC:
  - 8-bit data with 5-bits ECC
  - detect & correct up to 1-bit error
  - detect out up to 2-bits error support ECC bits self error check
- Flash ECC:
  - 64-bit data with 8-bits ECC
  - detect & correct up to 1-bit error support ECC bits self error check

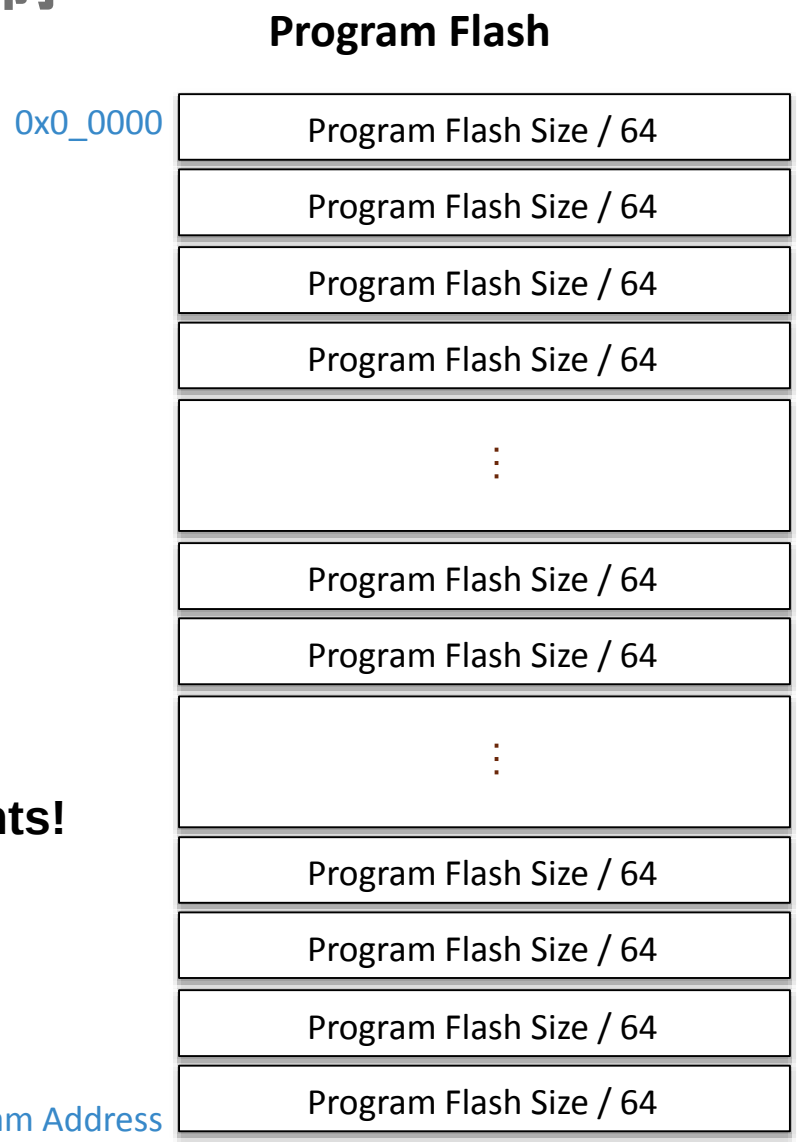


1: KE1xF only

Robust & Safety – FAC- Flash访问控制

- 可编程的将Flash分段，最多64段，可对单独的段设置访问控制
- 多种安全状态:
  - Supervisor/privileged secure state – Execute & Modify
  - Mid-level state – Execute Only
  - Unsecure state – No Access Right
- 用户通过编程Program Once Area使能访问控制

Prevents unauthorized access to selected code segments!
阻止对指定memory区域的未授权的访问



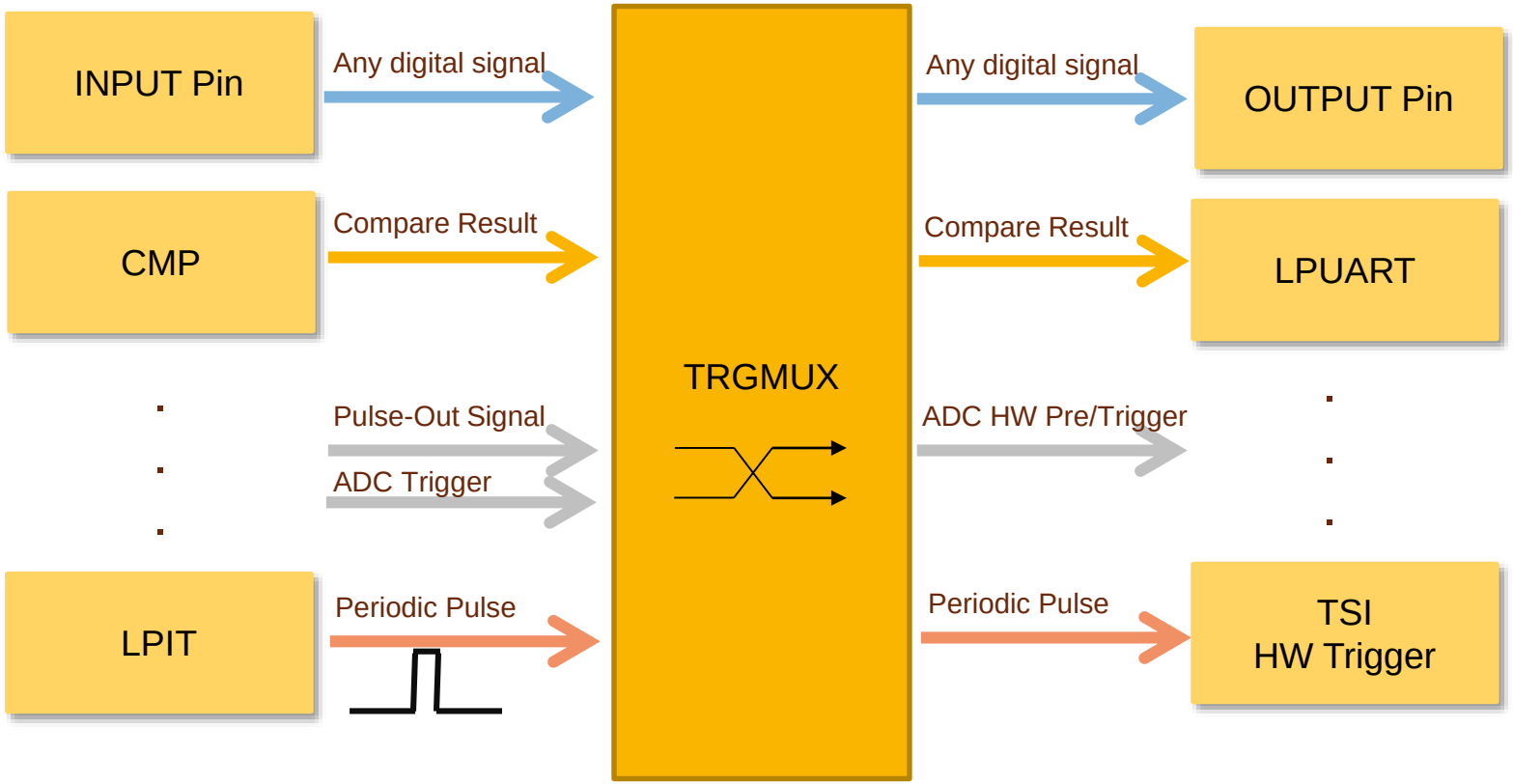
高性能及效率

Feature	Benefit to customer
High frequency CPU core	KE1xF, CM4 core runs up to 168MHz KE1xZ, CM0+ core runs up to 72MHz Improve system performance
8KB I/D Cache[1]	Improving the code and data access efficiency Improve system performance
MMDVSQ [2]	Hardware engine for math operation, reducing CPU workload
TRGMUX	Improve system performance, more flexible for internal connection
eDMA	Improve system performance, reducing power consumption and CPU workload

1: KE1xF only
2: KE1xZ only

Performance and Efficiency – 多路触发TRGMUX

灵活的内部逻辑触发及交互



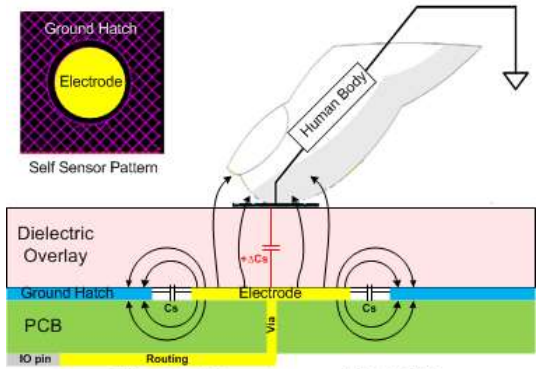
HMI

Feature	Benefit to customer
TSI触摸感应接口[1]	Up to 36 touch keys Pass IEC61000-4-6 test, enhanced EMC/waterproof performance Supports both self-cap and mutual-cap sensing mode
大电流驱动IO	8 high drive pins offer maximum 20mA driver current each
更多的IO数量	More control signal Input/Output More flexible hardware design Up to 89 GPIOs on 100LQFP, 58 GPIOs on 64LQFP

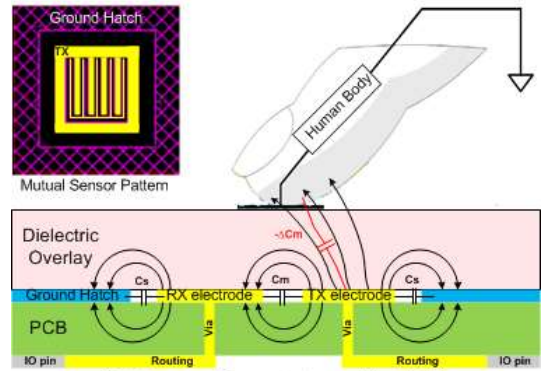
1: KE15Z only

HMI – 触摸感应接口

- **自容感**测 Mode
  - 简单成熟的电极设计
  - **通道**间串扰较少
  - 单**点感**应，可应用于按键、滑条、滚轮等多种外形设计
- **互容感**测 Mode
  - 拥有良好的灵敏度
  - **按**键用于矩阵外形，布线方便
  - **可用于**单点及多点感应
- High Performance in EMC
  - IEC61000-4-6 Certification by GRGTest
  - IEC61000-4-6 Certification by AUDIX



Self-cap Touch Sensor structure and Electric field



Mutual-cap Touch Sensor structure and Electric field

TSI Value Features

- ❑ Two operation modes
  Self-cap: up to 25 keys
  Mutual: up to 36 key
- ❑ Advanced robust in EMC
  Pass IEC61000-4-6 standard test
- ❑ Advanced robust in waterproof
- ❑ High sensitivity and resolution
- ❑ No need for CPU interfere
- ❑ Ease of use
  NXP Touch Library support
  SDK touch APIs support
- ❑ No need for external components

AUDIX
Audix Technology (Shanghai) Co., Ltd.

1. Applicant: Freescale Semiconductor (China) Limited SuZhou Branch
2. Description of Device:

EUT	M/N
KE touch control panel	KE1xF_TSI_EVB

3. Date of Measurement: Sep 30, 2015
4. Test Item:
   Radiated Susceptibility: EN 55024 (IEC 61000-4-6:2006)
5. Measurement Results: Pass
6. Test Data:
   See the additional test data.
   All the test set-up set under the requirement of the customer.
7. Test Photos:
   See the additional test photos.

Vincent Gao
(Vincent Gao / Test Engineer)

For and on behalf of
Audix Technology (Shanghai) Co., Ltd.
Authorized Signature EMC (Sammy Chen / Reviewer)

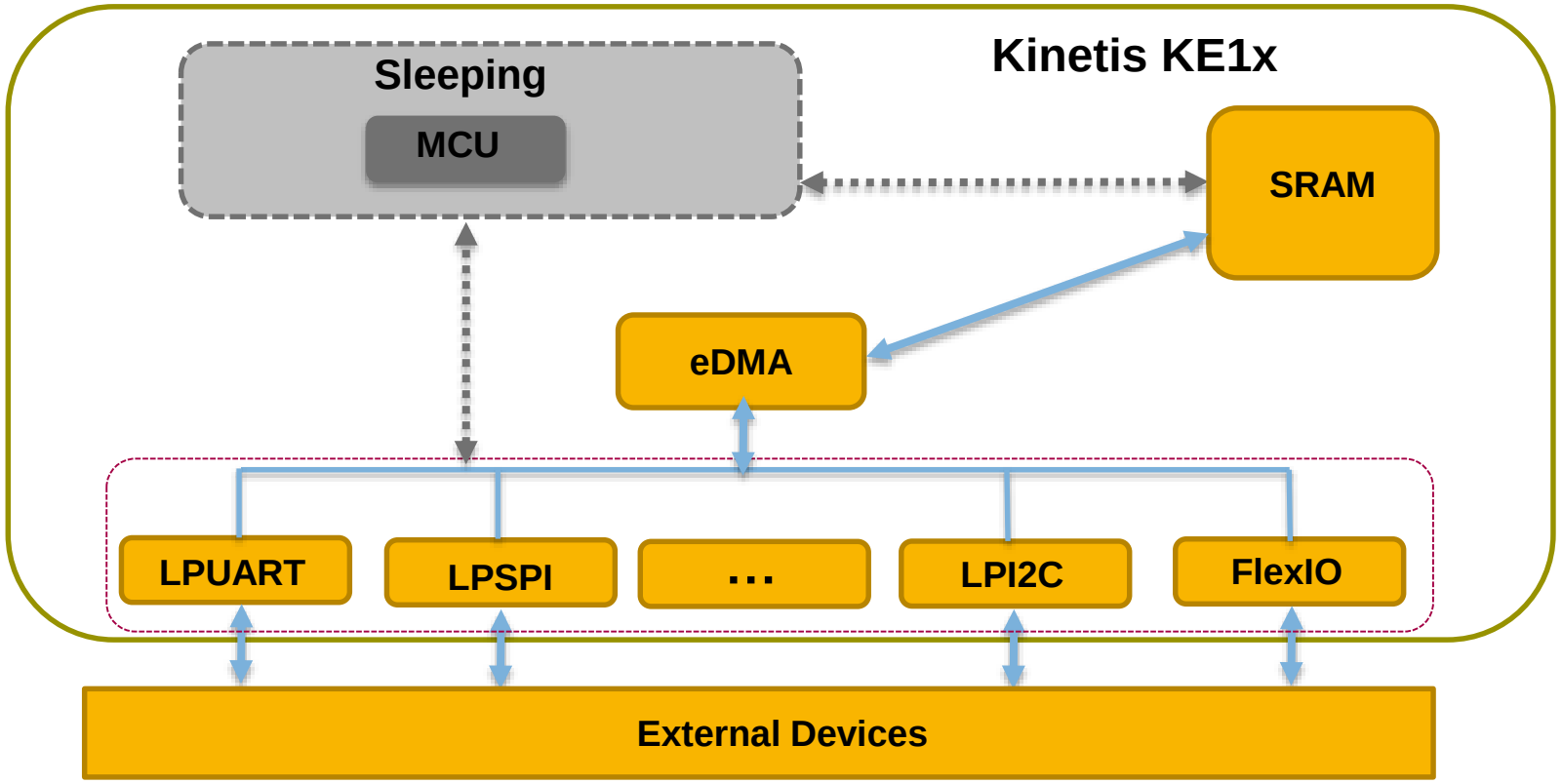
Power Efficiency 高能效

Feature	Benefit to customer
多种功耗模式	Include HSRUN[1], RUN, WAIT, STOP, VLPR, VLPW, VLPS to save power Improve system power efficiency
智能外设	Support working in low power modes Avoid frequently waking CPU and reduce power (TSI[2], LPUART, LPSPI, LPI2C, FlexIO, ADC, eDMA)

1: KE1xF only
2. KE15Z only

高能效 – 智能外设

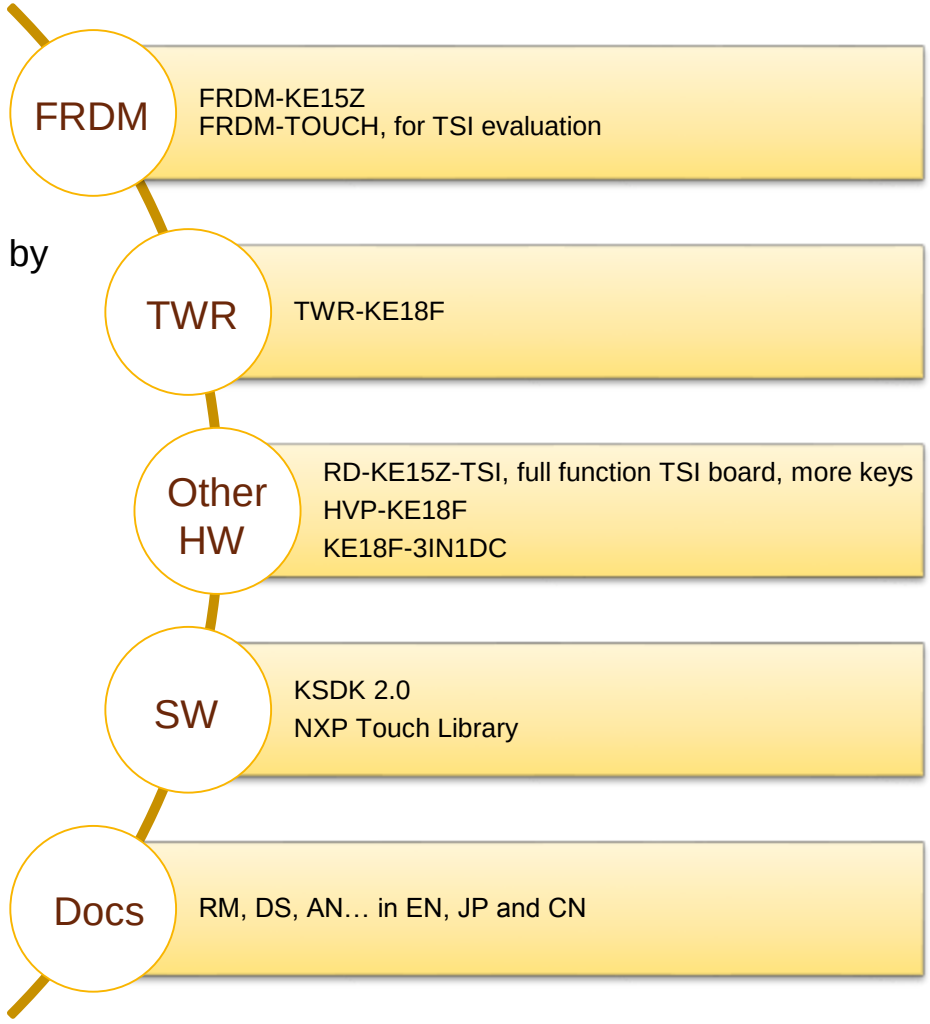
- LPUART, LPSPI, LPI2C, FlexIO 都能在wait及stop模式下工作，并使用eDMA完成数据收发，无需唤醒CPU。



ENABLEMENT

KE1x开发工具

- 软件工具
  - KDS, IAR, KEIL
  - KSDK Kinetis Software Development Kit
  - IEC60730 compliant library (Class B Safety S/W routines certified by VDE)
- 硬件评估平台
  - FRDM
  - TWR
- 参考设计/评估板
  - 3-in-1 motor control, dual motor control and PFC
  - High voltage motor control daughter board
  - Touch sensing in pad, slider and wheel



KE1x Enablement – 已有的硬件开发平台

Freedom Platform

FRDM-KE15Z

- Ultra low -cost/power development platform
- Form factor compatible with Arduino platform
- Compatible with Freedom shield

Freedom Shield

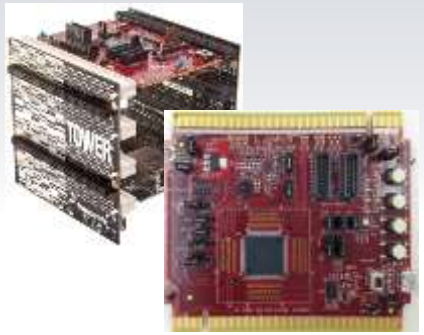
FRDM-TOUCH

- This evaluation board, in a shield form factor, effectively turns a NXP Freedom development board platform into a complete motor control reference design

Tower System

TWR-KE18F

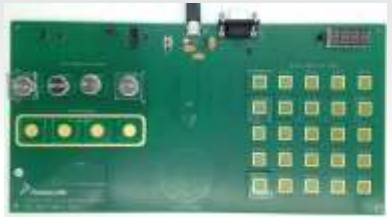
- Richer feature set
- Standard Tower Controller Module
- Compatible with existing Tower System peripherals



TSI Evaluation Board

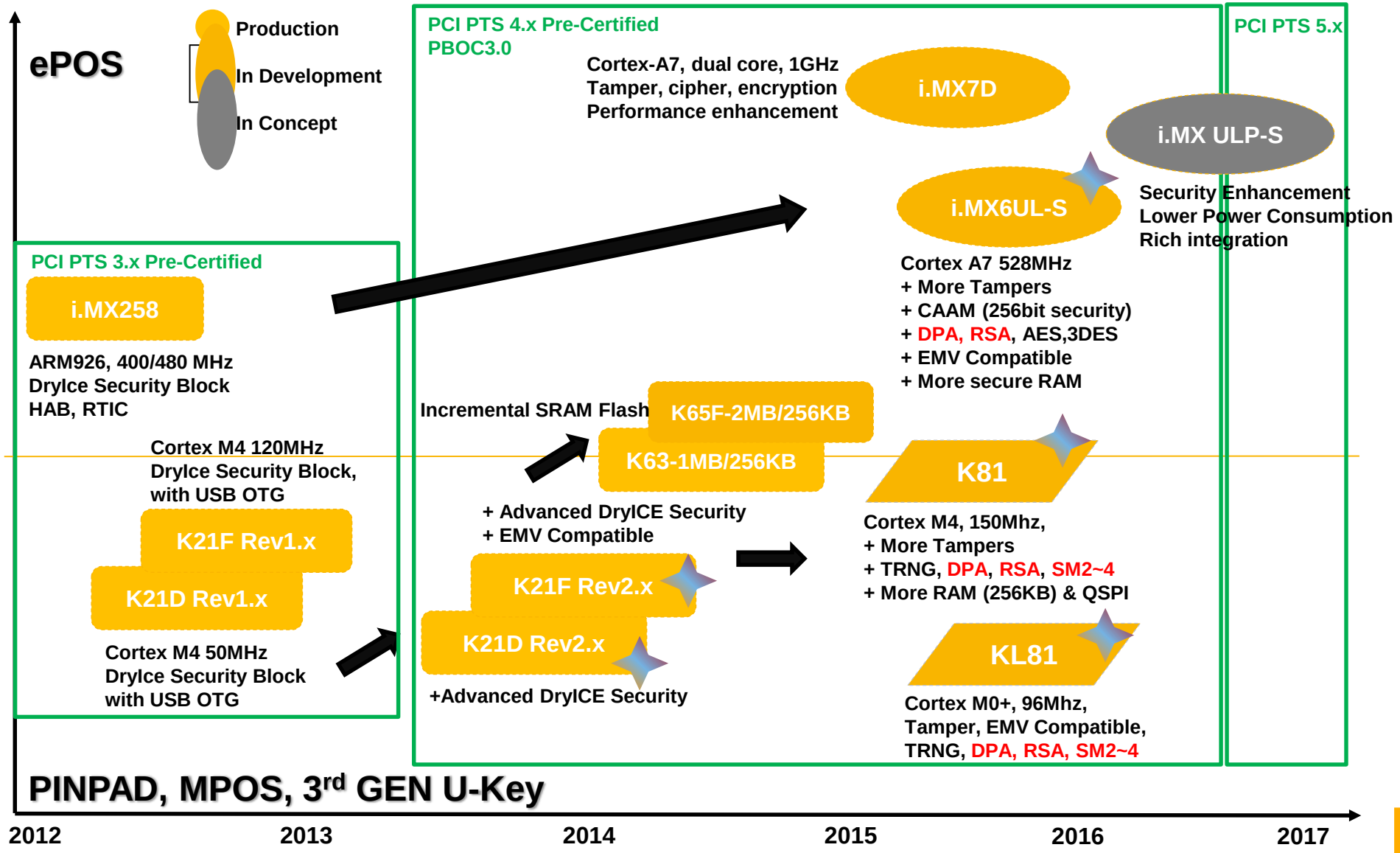
RD-KE15Z-TSI

- Evaluation board for new TSI hardware and software design



面向高安全应用场合的 K8X & KL8X

安全类MCU及面向的金融产品应用



K81 Devices (256KB Flash, 256KB SRAM)

Key Features:

Core/System
- Cortex-M4 with 8KB I/D-Cache
- FPU and MPU , BME

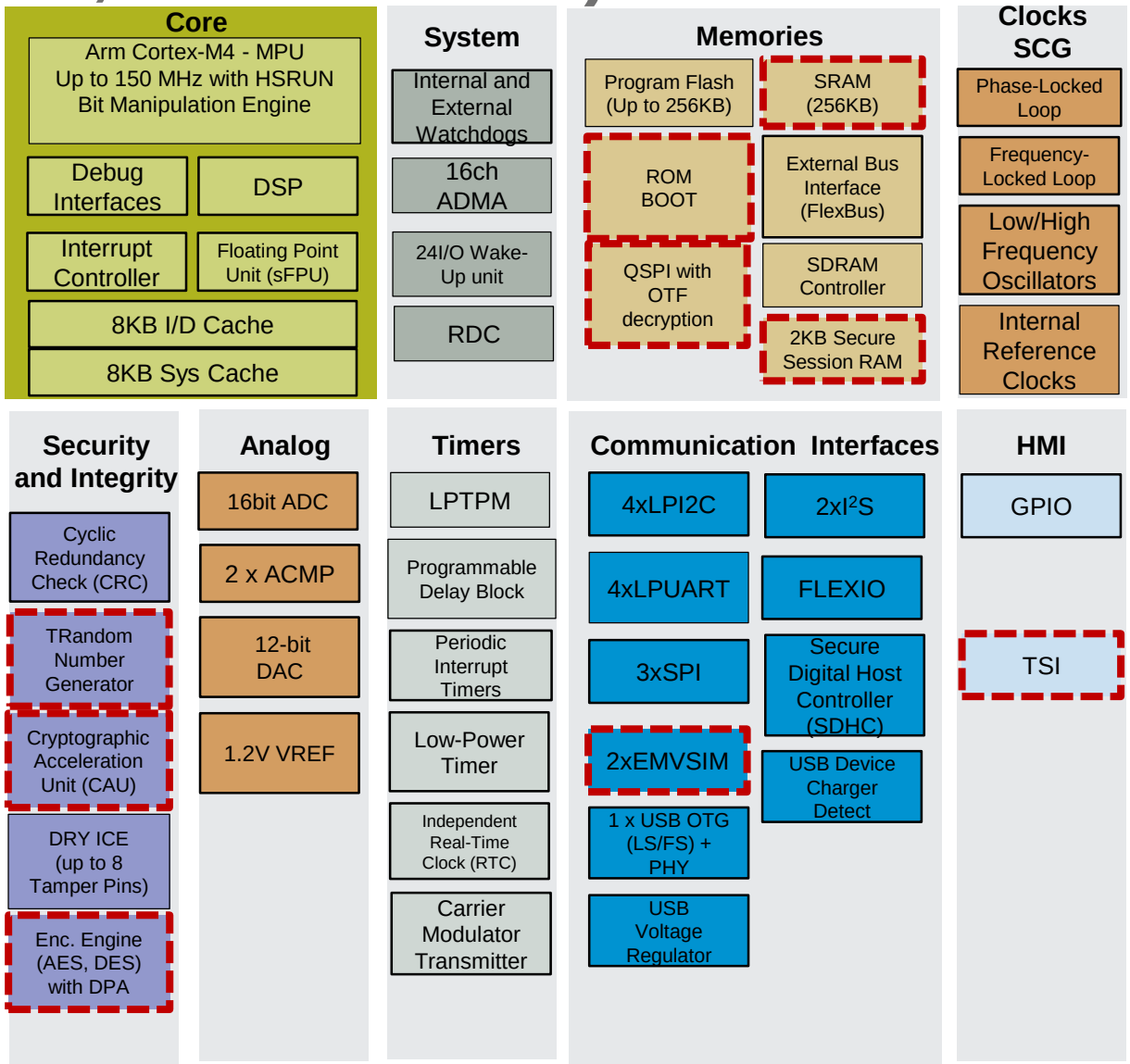
Memory
- up to 256KB Flash,
- up to 256KB SRAM
- QSPI Flash interface with OTF

Security
- **True Random Number Generator**
- Crypto acceleration MMCAU
- **160B(32B+128B) Secure RAM for Key storage**
- **Enc. Engine (DES/3DES/AES/RSA)**
  - RSA2048 support (3 decrypt and 1 encrypt <750ms)
  - ECC: ECDSA and ECDH for up to P256
  - DES/3DES with HW DPA
  - AES256/192/128 with DPA
- Up to **8** Tamper Pins
- RDC: Resource Domain Controller

Timers
- Independent Real-Time Clock (RTC)

Others
- **2x EMV compatible ISO7816-3 interfaces**
- 1.71V-3.6V; -40 to 105ºC
- Up to TBD x I/Os (3V)
- Priority Packages:121MBGA, 100LQFP

Availability
- Samples: Q4 2014
- Qual/Production: Q1 2015



KL81 Devices (128KB Flash, 96KB SRAM)

Key Features:

Core/System
- Cortex-M0+
- MTB
- BME

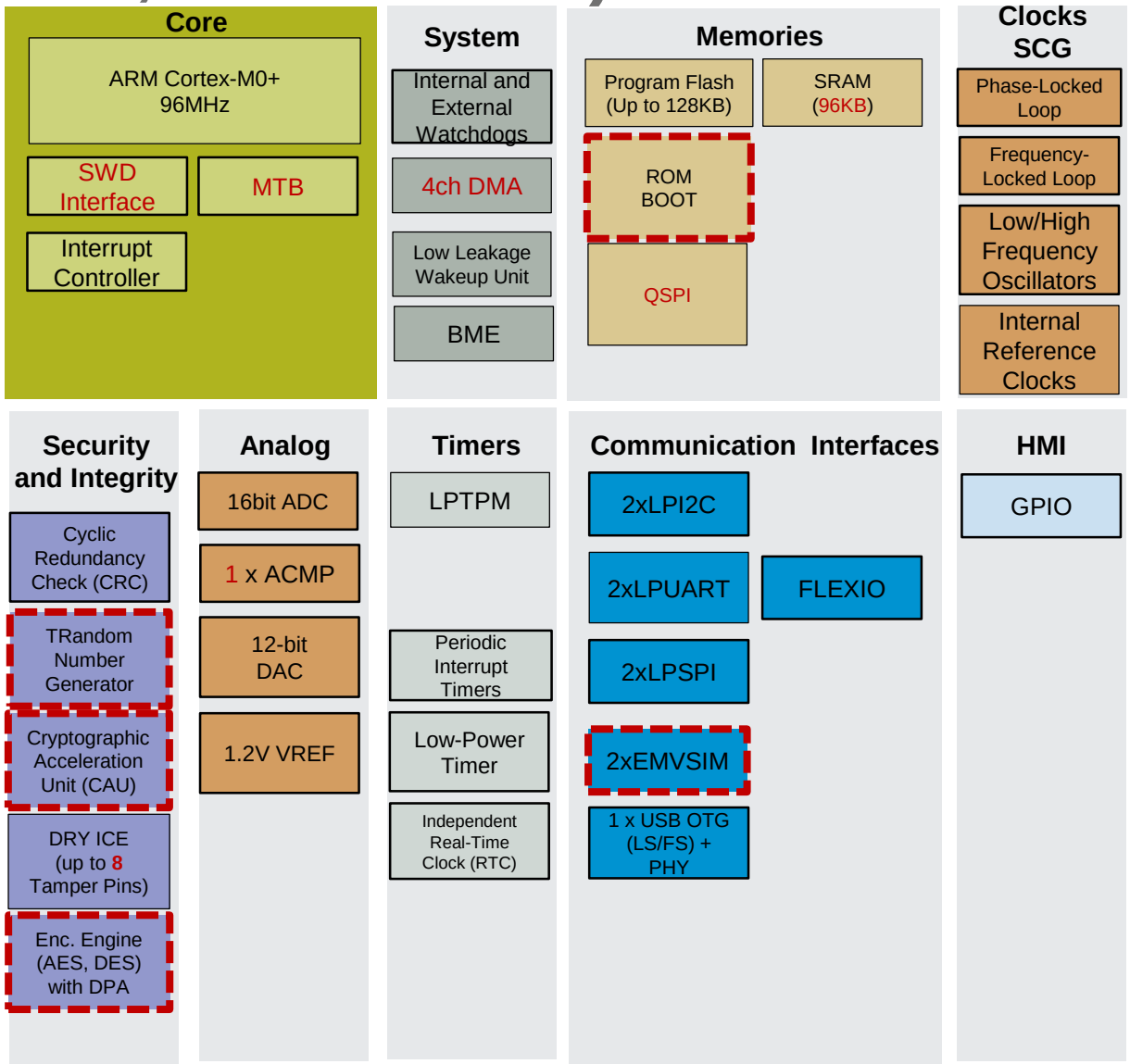
Memory
- up to 128KB Flash,
- up to 96KB SRAM
- QSPI Flash interface

Security
- **True Random Number Generator**
- Crypto acceleration MMCAU
- **160B(32B+128B) Secure RAM for Key storage**
- **Enc. Engine (DES/3DES/AES/RSA)**
  - RSA2048 support (3 decrypt and 1 encrypt <750ms)
  - ECC: ECDSA and ECDH for up to P256
  - DES/3DES with HW DPA
  - AES256/192/128 with DPA
- Up to **8** Tamper Pins
- RDC: Resource Domain Controller

Timers
- Independent Real-Time Clock (RTC)

Others
- **2x EMV compatible ISO7816-3 interfaces**
- 1.71V-3.6V; -40 to 105ºC
- Up to TBD x I/Os (3V)
- Priority Packages:121MAPBGA, 80LQFP, 64LQFP

Availability
- Samples: Q1 2015
- Qual/Production: Q2 2015



日程

Kinetis K81的介绍

- Oveview & Architecture
- Flash Security for Code Protection and Trust Boot
- DryICE for Tamper Detection
- QSPI
- LP Trusted Cryptography (LTC)
- TRNG
- EMVSIM
- SDK

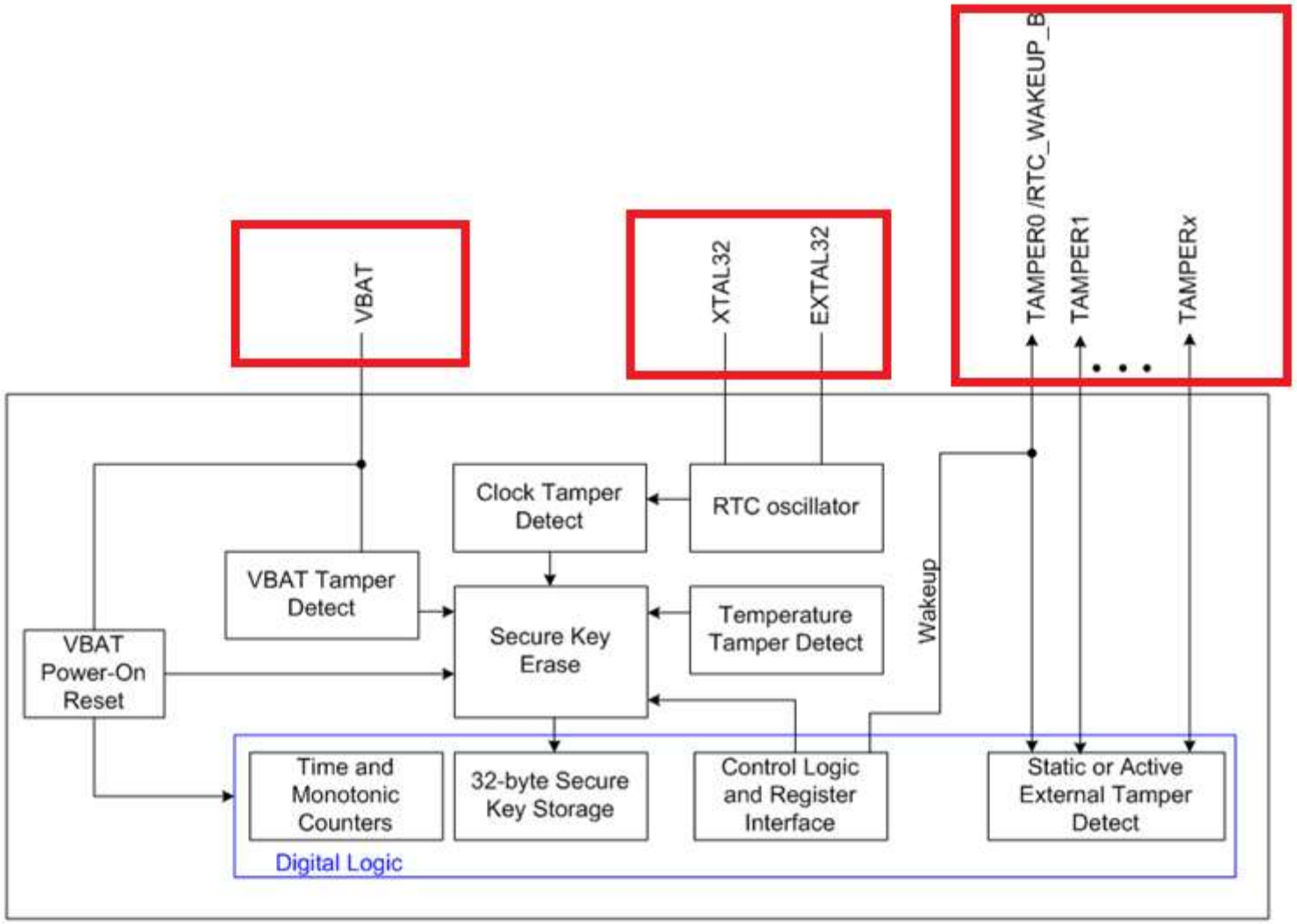
OVERVIEW & ARCHITECTURE

K81 关键特性

- 高性能的150 MHz ARM® Cortex®-M4F MCU with 8KB I/D-Cache
- 最大256 KB program flash 及 256 KB SRAM
- FlexBus 扩展总线接口及SDRAM 控制器接口
- Dual QuadSPI接口， 支持 XIP(eXecute In Place)， 对于加密image支持OTF decryption
- Digital Host Controller (SDHC) 和FlexIO
- 低功耗的电容式触摸感应接口
- 2x EMVSIM 模块，符合EMV Standard v4.3 及ISO 7816-3 接口标准
- 外部侵入侦测 管脚, 2KB 安全SRAM存储用于存放秘钥
- LP Trusted Crypto (LTC) 硬件加速器能够同时执行AES, DES, 3DES, RSA and ECC等运算
- 真随机数发生器
- 同时也支持CAU模块的DES, AES, SHA的硬件加速

用于侵入侦测的DRYICE模块

DryIce/安全的RTC



DryICE 特性

- 独立的VBAT供电系统，32.768kHz的专供时钟源，即使在MCU断电的情况下，保持DryIce模块的正常工作
- 多达8个外部的侵害侦测I/O，同样工作在VBAT供电域，并能够工作于静态或者主动模式
- 这些防侵入I/O能够配置触发的极性及输入滤波
- 用户可以通过配置两个动态侵入移位寄存器，生成16bit的多项式函数，用于在tamper I/O工作于主动模式时的输入输出校验
- 安全存储区域将在侦测到侵入时被擦除.
- 被保护的寄存器能够在VBAT电源域重新上电的过程中被重新使能读写的权限
- 侵入时间寄存器将记录下受到侵入的时间.
- 多种侵入事件，包括温度，电压，时钟等可以单独配置

FLASH访问安全保护及安全启动

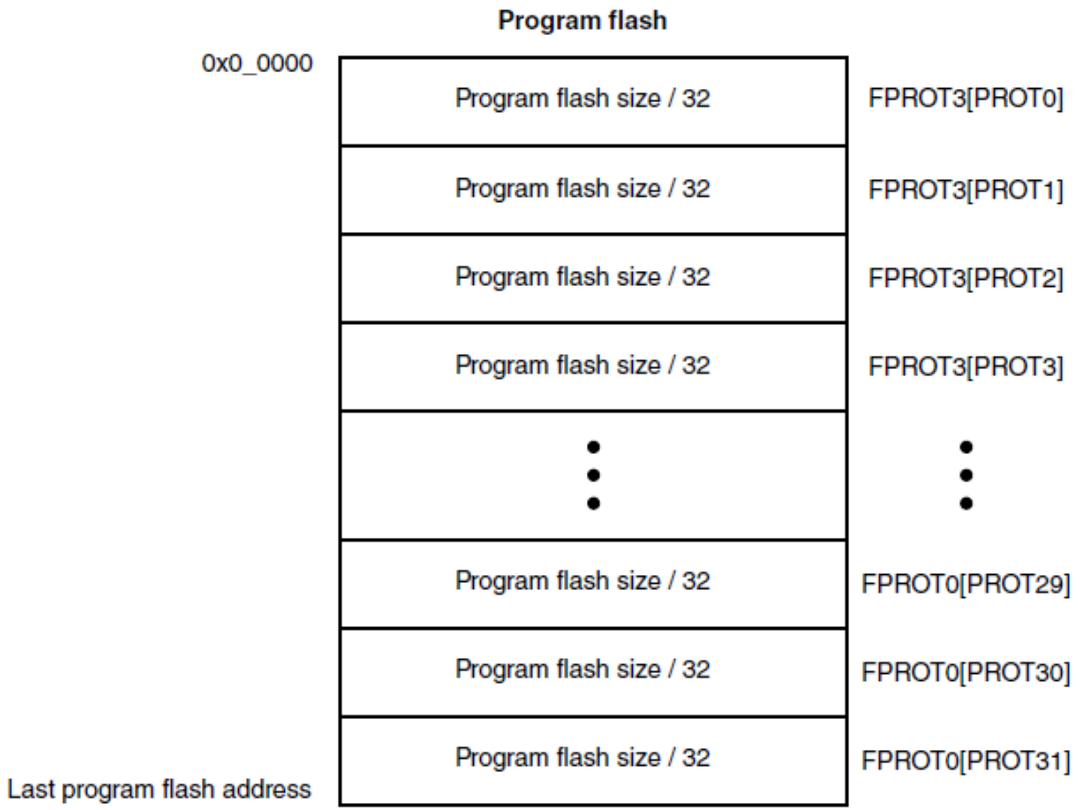
Flash配置域

- 在flash区域的0x400-0x40F区域，包含了16个字节的flash配置字节，这些配置项包括了对flash安全配置的选项。

Flash Configuration Field Byte Address	Size (Bytes)	Field Description
0x0_0400–0x0_0407	8	Backdoor Comparison Key. Refer to Verify Backdoor Access Key Command and Unsecuring the Chip Using Backdoor Key Access.
0x0_0408–0x0_040B	4	Program flash protection bytes. Refer to the description of the Program Flash Protection Registers (FPROT0-3).
0x0_040F	1	Reserved
0x0_040E	1	Reserved
0x0_040D	1	Flash nonvolatile option byte. Refer to the description of the Flash Option Register (FOPT).
0x0_040C	1	Flash security byte. Refer to the description of the Flash Security Register (FSEC).

Flash保护寄存器

- FPROT寄存器定义了受保护的flash区域，受保护的区域将不能被编程及擦除
- FPROT可以将所有flash分成32等分，受保护的区域最小单位即这样一个等分

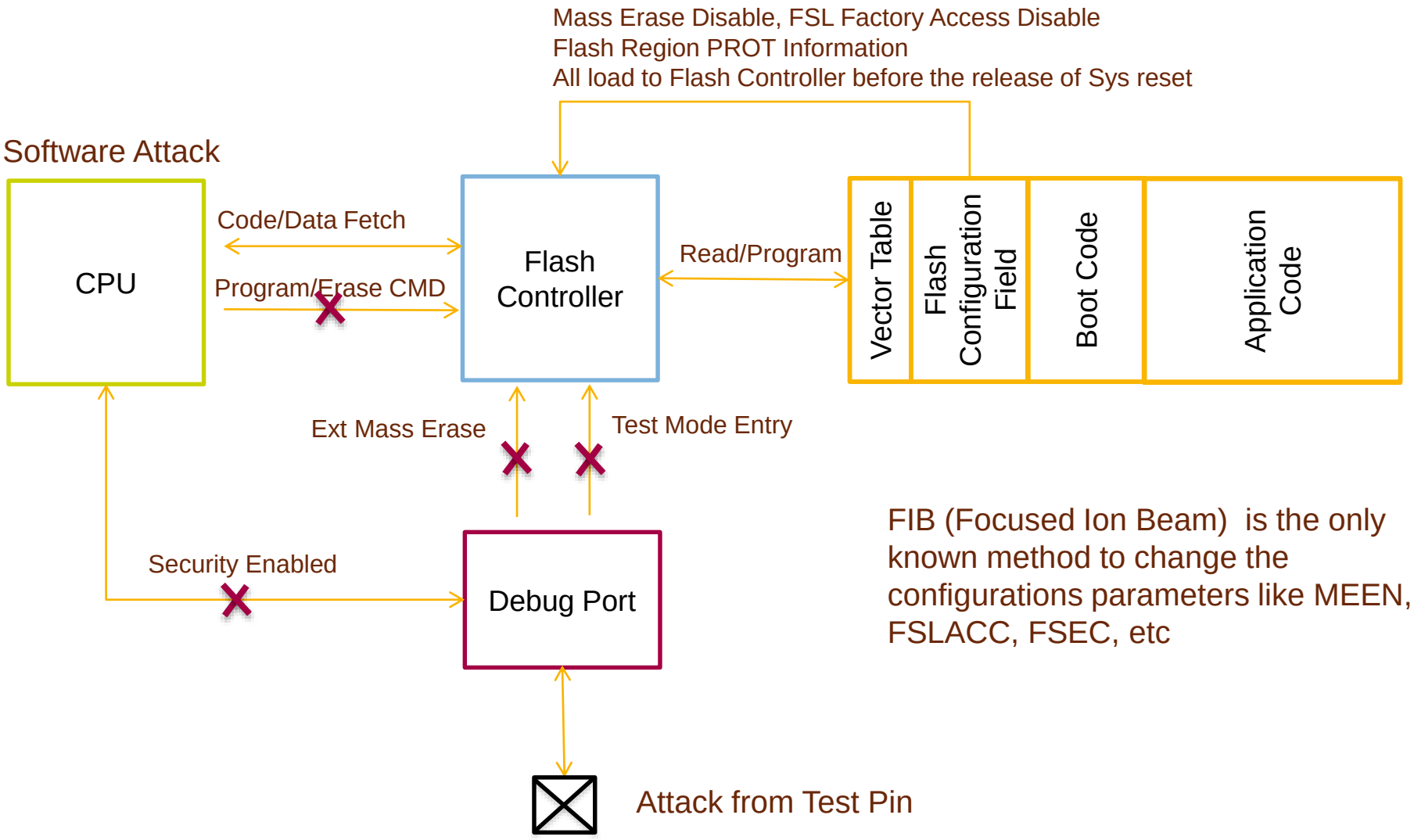


Flash 安全寄存器

FSEC field	Description
KEYEN	Backdoor Key Access
MEEN	Mass Erase Capability
FSLACC	Freescale Factory Access
SEC	MCU security

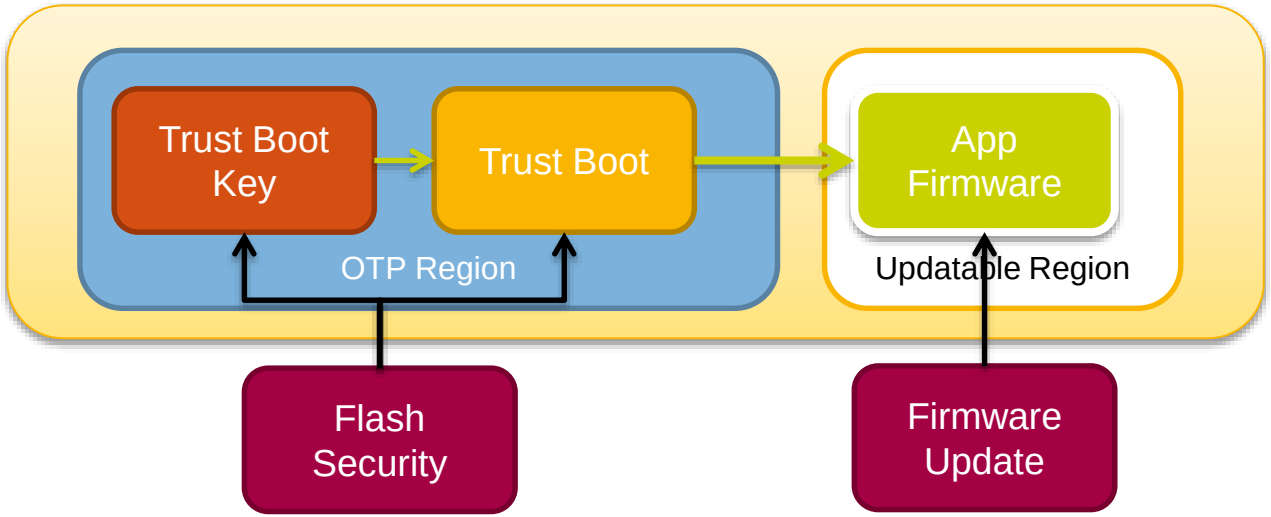
- 如果禁用Mass Erase，任何擦除OTP区域及flash配置域的企图都会失败
- 如果禁用“工厂访问”功能，任何进入测试模式及特殊模式的企图都会失败
- SEC位定义了MCU的安全状态，如果MCU被定义为安全状态，通过Debug口去访问内存区域是不被允许的

安全访问的整体框架



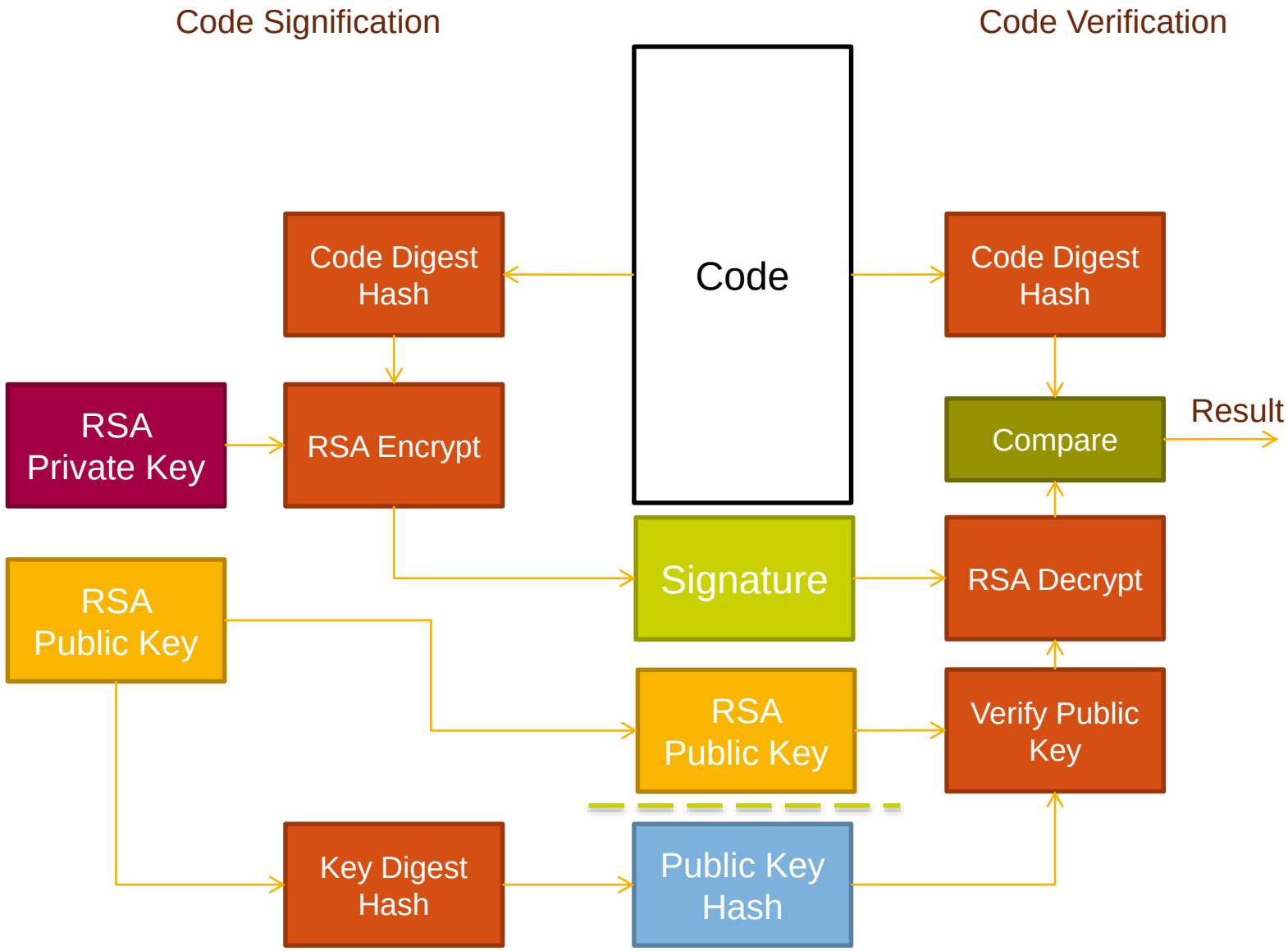
FIB (Focused Ion Beam) is the only known method to change the configurations parameters like MEEN, FSLACC, FSEC, etc

加密代码的安全启动



- **授信启**动区域（Trust Boot region）**用于**鉴别应用代码
- **安全的**bootloader**在跳**转到应用代码之前，会验证基于PKSC(e.g. RSA2048) **的数字**签名
- **授信启**动区域的代码及公钥被编程进OTP**区**间，是不可能被修改的
- 应用代码是能够被随时更新的

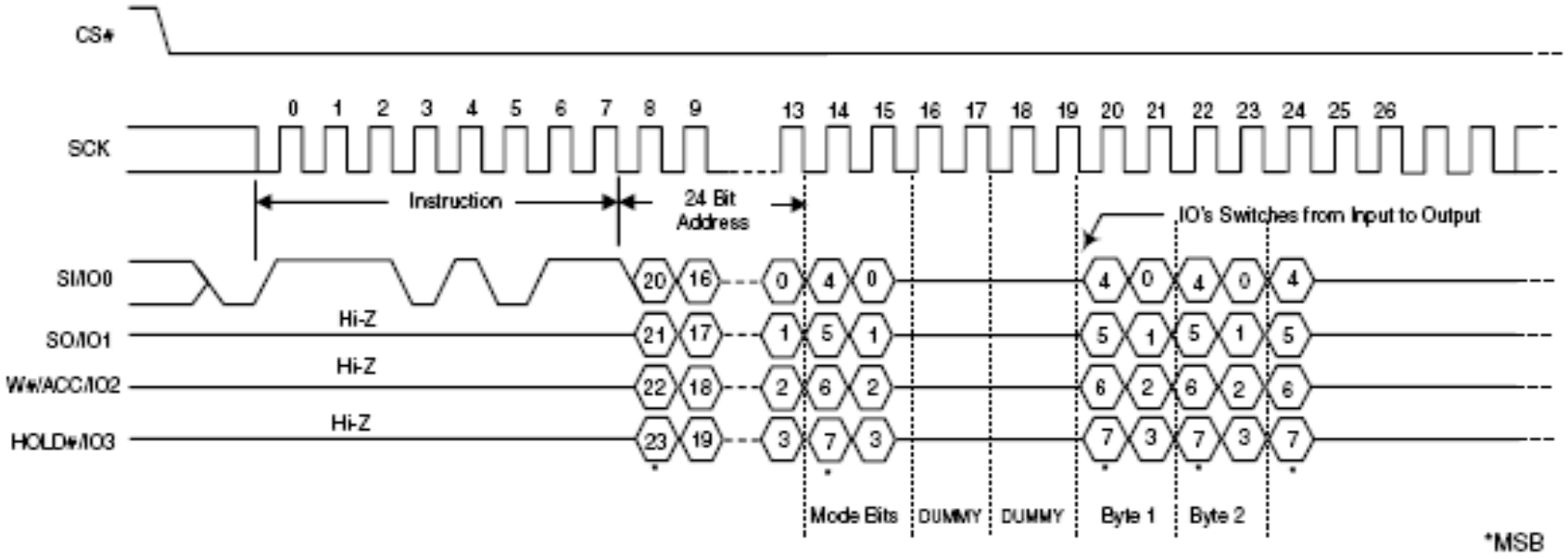
K80授信启动的全流程



QUADSPI

QuadSPI Flash

- 用于接口外部的串行Flash
- 通信接口类似于SPI
- 具有可编程命令时序引擎，能够支持XIP，片上执行代码
- 支持On-The-Fly-Decryption-Engine (OTFAD)
- 支持单，双，4线甚至8线的数据线接口，并能工作于SDR或者DDR模式
- SDR模式最大可以工作于100MHz，DDR最高可以工作于75MHz
- 支持24-bit及32-bit地址寻址



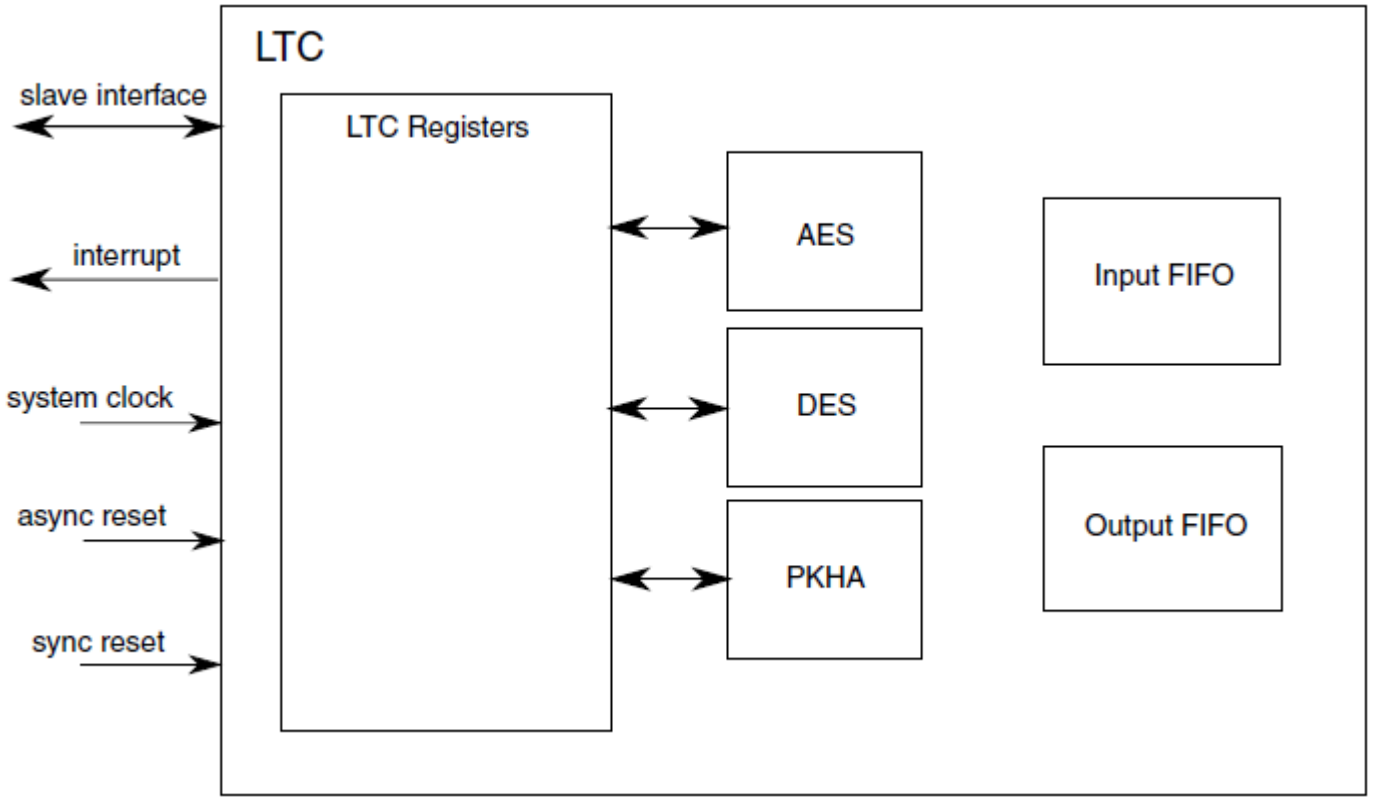
On-the-Fly AES Decryption Module (OTFAD)
运行时AES解密模块

- 使用AES-128秘钥保护存储在外部存储中的应用代码,并在代码执行时使用OTFAD解密
- AES-128 Counter Mode On-the-Fly Decryption
  - 128-bit key and 128-bit data block sizes
  - Adds zero cycles of incremental latency for decryption when used with QuadSPI
  - Receives 64-bit encrypted data from QuadSPI, calculates decrypted data which is sent to AHB RAM buffer and bypassed back to system AHB read data bus
- Hardware support for 4 independent decryption segments, known as memory “contexts”
  - Each context has a unique 128-bit key, 64-bit counter and 64-bit memory region descriptor
- Functionally acts as a slave sub-module to the QuadSPI
  - Logically connected "between" the QuadSPI and its AHB RAM buffer
  - Shares system AHB and IPS (slave peripheral) bus connections
  - Private 64-bit data buses for encrypted (ciphertext) and decrypted (plaintext) data

LP TRUSTED CRYPTOGRAPHY (LTC)

LP Trusted Cryptography (LTC)

- 允许多个硬件加密引擎实例化
- 目前支持 AES, DES, 3DES, RSA and ECC(KL81 加入了SHA)



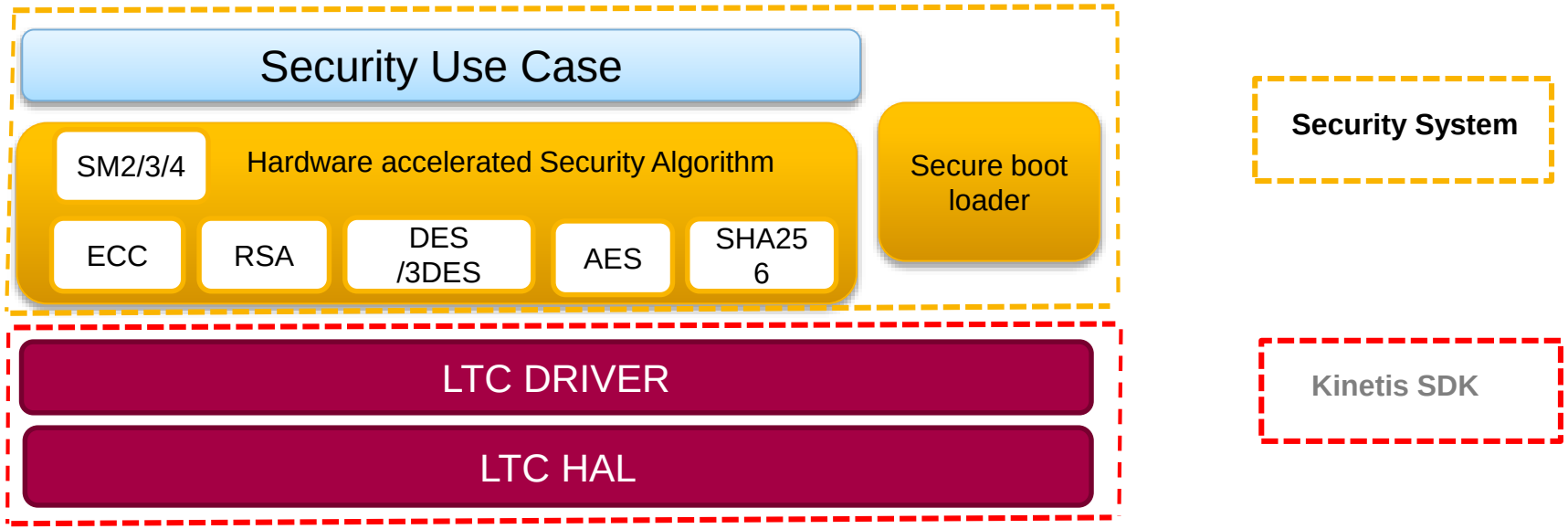
对称加密

- AES with HW DPA
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
  - Output feedback (OFB)
  - 128-bit cipher feedback (CFB128)
  - Counter (CTR)
  - Extended cipher block chaining message authentication code (XCBC-MAC)
  - Cipher-based MAC (CMAC)
  - CTR and CBC-MAC (CCM)
  - Galois/Counter mode (GCM)
  - Combined CBC and CMAC (CBC-CMAC)
  - Combined CTR and CMAC (CTR-CMAC)
- DES (KL81 support HW DPA)
  - Supports both single- and triple-DES functionality
  - ECB, CBC, CFB, and OFB modes

公钥加密

- Public-key hardware accelerator (PKHA) perform a number of different operations used in public-key cryptography
  - Integer MOD arithmetic
    - Addition
    - Subtraction
    - Multiplication
    - Exponentiation
    - Reduction
    - Inversion
  - Elliptic-Curve Mathematics
    - Point math over a prime field (Fp)
    - Point math over a binary field (F2m)
  - RSA up to 2048-bit
  - ECC up to 512-bit

K81/KL81基于SDK的安全类demo



- Implemented key security algorithm based on LTC
- Security use case
  - ✓ Data Encryption/Decryption
  - ✓ Hash function
  - ✓ Digital signature
  - ✓ Key exchange
  - ✓ Message authentication
- Secure boot loader with image authentication and upgrade
- Closed the gap between customer's requirement and LTC driver

TRNG

True Random Number Generator

- **使用硬件加速生成512-bit的**熵
- 熵来源于随机噪声
- **随机噪声源来源于一个**环形振荡器，该振荡器对随机噪声相当敏感，包括温度、电压、串扰等随机噪声
- **随机数很**难被猜测及预测

EMVSIM

Euro/Mastercard/Visa/SIM Serial Interface Module(EMVSIM)

- 支持智能卡标准EMV Standard v4.3 及ISO 7816-3接口
- SIM的时钟（包括收和发）是独立的，相应的寄存器的读写时钟也是独立的
- 当发生奇偶校验错误或者接收缓冲区溢出时自动产生NACK信号
- 具有自动重传机制
- 接收时自动检测NACK
- 具有独立的可调节定时器用于计算“character wait time, block wait time and block guard time”
- 可选择时钟源的计数器
- 支持DMA传输

EMV 认证方案

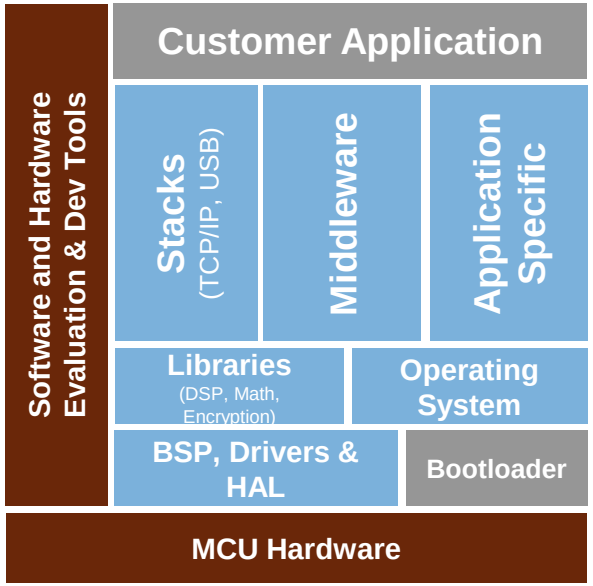
- K81(TWR-K81&POSCard board) 通过了EMV L1 pre-certification
- 提供EMV L1 stack lib and EMVSIM driver
- 标准的EMV L1认证设备 (Microprоss Star3150)

SDK

Kinetis Software Development Kit (SDK)

A complete software framework for developing applications across all Kinetis MCUs

HAL, peripheral drivers, libraries, middleware, utilities, and usage examples; delivered in C source



Open Source Initiative

CMSIS COMPLIANT

Product Features

- Open source Hardware Abstraction Layer (HAL) provides APIs for all Kinetis hardware resources
- BSD-licensed set of peripheral drivers with easy-to-use C-language APIs
- Comprehensive HAL and driver usage examples and sample applications for RTOS and bare-metal.
- CMSIS-CORE compatible startup and drivers plus CMSIS-DSP library and examples
- RTOS Abstraction Layer (OSA) with support for Freescale MQX, FreeRTOS, Micrium uC/OS, bare-metal and more
- Integrates USB and TCP/IP stacks, touch sensing software, encryption and math/DSP libraries, and more
- Support for multiple toolchains including GNU GCC, IAR, Keil, and Kinetis Design Studio
- Integrated with Processor Expert

Kinetis IDE Options

SDK 1.2

Featured IDEs:

Atollic TrueSTUDIO

- Professional ECLIPSE/GNU based IDE with a MISRA-C checker, code complexity analysis and source code review features.
- Advanced RTOS-aware debugger with ETM/ETB/SWV/ITM tracing, live variable watch view and fault analyzer. Dual-core and multi-processor debugging.
- Strong support for software engineering, workflow management, team collaboration and improved software quality.

Green Hills MULTI

- Complete & integrated software and hardware environment with advanced multicore debugger
- Industry first TimeMachine trace debugging & profiler
- EEMBC certified top performing C/C++ compilers

Keil Microcontroller Development Kit

- Specifically designed for microcontroller applications, easy to learn and use, yet powerful enough for the most demanding embedded applications
- ARM C/C++ build toolchain and Execution Profiler and Performance Analyzer enable highly optimized programs
- Complete Code Coverage information about your program's execution

IAR Embedded Workbench

- A powerful and reliable IDE designed for ease of use with outstanding compiler optimizations for size and speed
- The broadest Freescale ARM/Cortex MCU offering with dedicated versions available with functional safety certification
- Support for multi-core, low power debugging, trace, ...

Complimentary Solutions:

Kinetis Design Studio

- Complimentary basic capability integrated development environment (IDE) for Kinetis MCUs
- Eclipse and GCC-based IDE for C/C++ editing, compiling and debugging

mbed Development Platforms

- The fastest way to get started with Kinetis MCUs
- Online project management and build tools – no installation required; option to export to traditional IDEs
- Includes comprehensive set of drivers, stacks and middleware with a large community of developers.

Additional Ecosystem Partners:

Q&A

SECURE CONNECTIONS
FOR A SMARTER WORLD