APLIKAČNÍ PROCESORY I.MX 7

MICHAL SUSEN

SYSTEMS ENGINEER

OCTOBER 2016

SECURE CONNECTIONS
FOR A SMARTER WORLD

i.MX Processor Roadmap

Two New i.MX Platforms Based on 28nm FD SOI Technology

i.MX 6 QuadPlus

↓

i.MX 6 Quad

↓

i.MX 6 DualPlus

↓

i.MX 6 Dual

↓

i.MX 6 DualLite

↓

i.MX 6 Solo

↓

i.MX 6 SoloX

↓

i.MX 6 SoloLite

↓

i.MX 6 UltraLite

ARM® v7-A

i.MX 8 series

Advanced Graphics & Performance

ARM® v8-A

i.MX 7 series

Power Efficiency

ARM® v7-A

I.MX 7 INTRODUCTION

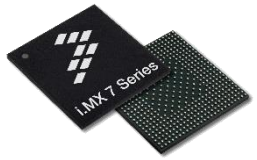
i.MX 7Dual/Solo Family Target Applications

MOBILE DEVICES

LPDDR2/3
Small Package







- Healthcare / Patient Monitoring
- Wearables
- IoT
- Point of Sale
- eReaders

- HMI Control / Security
- Printing
- Home Control
- General Embedded Control

CONNECTED DEVICES

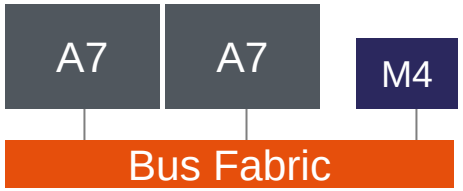
Low Cost DDR3
Larger Pitch Package






Advanced Heterogeneous Architecture

- Up to Dual Cortex-A7 @ 1GHz
- Cortex-M4 @ 200MHz
  - Offload Tasks
  - Optimize Power
  - Increase Security



Unmatched Power Efficiency

- 3x improvement in Power Efficiency vs i.MX 6
- 100 uW/MHz for Cortex-A7
- 70 uW/MHz for Cortex-M4
- One third the power consumed in the Low Power suspend mode (250uW) vs i.MX 6

Energy Efficient Solutions by Freescale

Enabling Flexible High Speed Connectivity

- PCI-e v2.1
- Dual Gbit Ethernet with AVB
- DDR QuadSPI support
- eMMC 5.0

Complete Security Infrastructure

- Secure Boot
- Crypto H/W Acceleration
- Secure JTAG
- Internal and External Tamper Detection
- DPA attack Resistance
- Secure Storage

SECURITY

Common Security Attacks

Common Security Attacks

JTAG Protection
(3 security modes)


Viruses, Trojans

Modifying / Replacing
Device's Image

Version Rollback
Attack

Physical Attacks

Common Security Attacks

JTAG Protection
(3 security modes)


Viruses, Trojans

High Assurance
Boot

Version Rollback
Attack

Physical Attacks

Common Security Attacks

JTAG Protection
(3 security modes)

HW Firewall

High Assurance
Boot

Version Rollback
Attack

Physical Attacks

Common Security Attacks

JTAG Protection
(3 security modes)

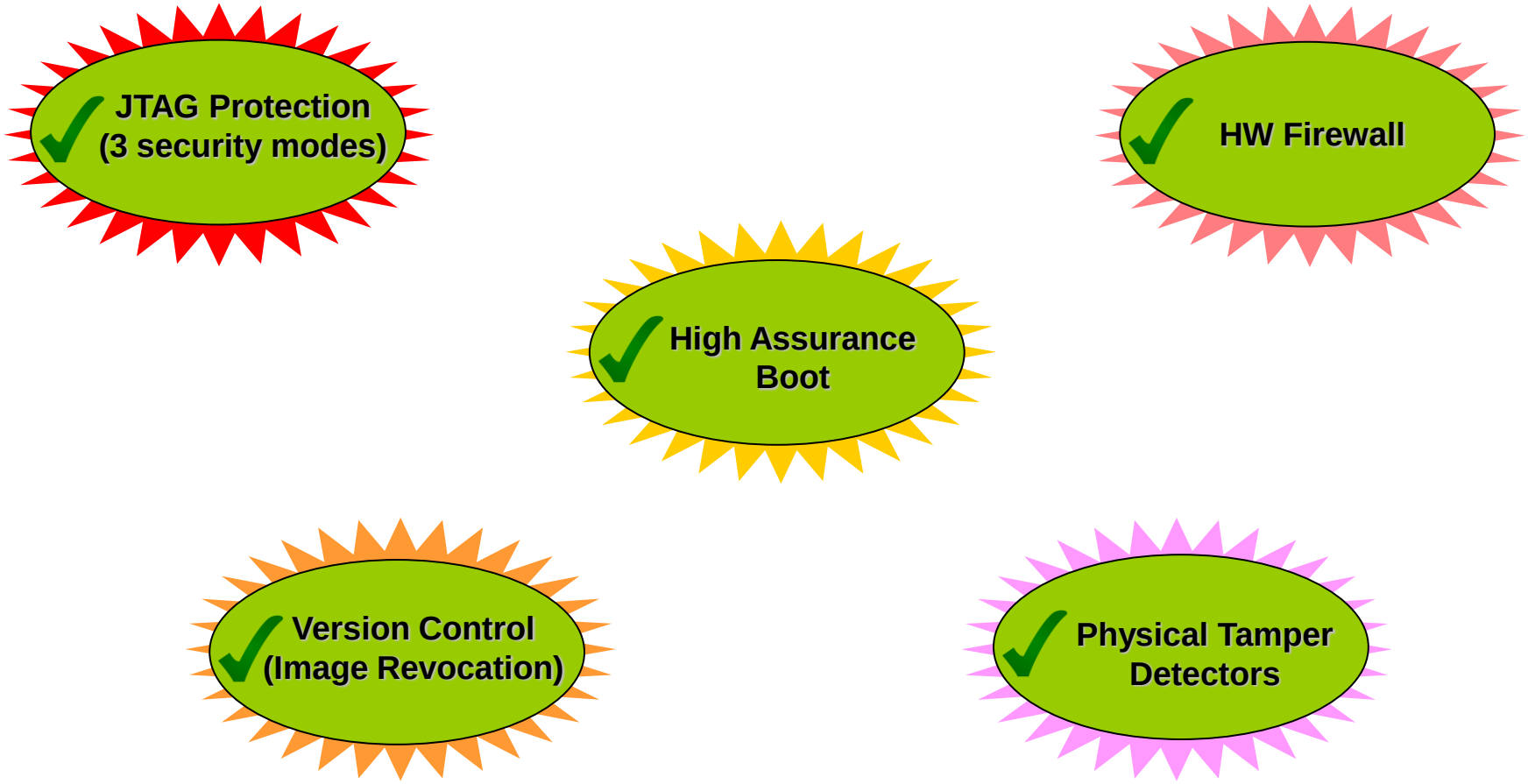
HW Firewall

High Assurance
Boot

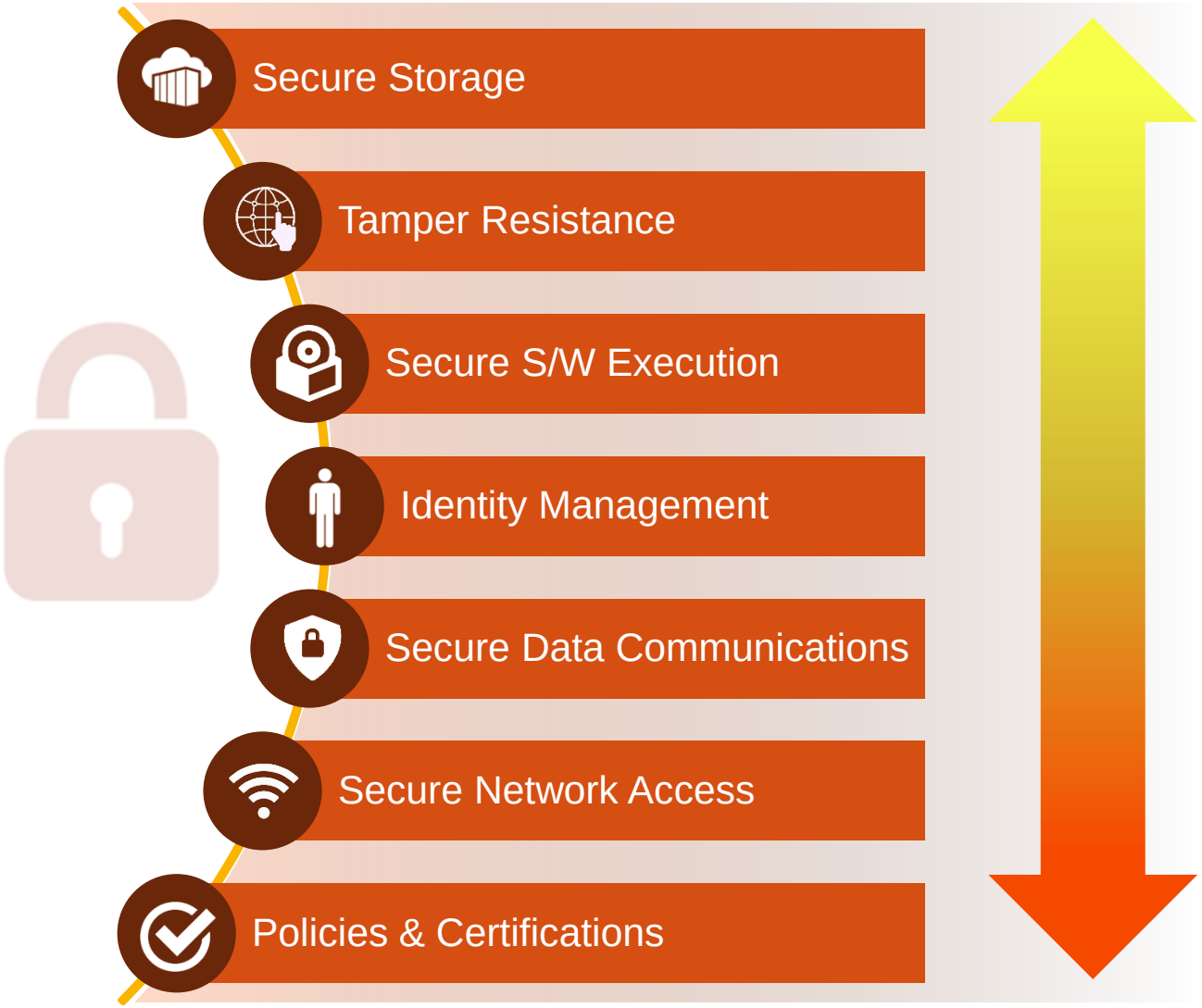
Version Control
(Image Revocation)

Physical Attacks

Common Security Attacks



Security – i.MX Hardware Enablement



In-Line Encryption (Memory)

Manufacturing Protection

Authenticated debug & Field returns

Run-time integrity

Trust Zone

Secure Storage

Zeroizable RAM

Root of trust

Cryptographic Acceleration

Symmetric & Asymmetric accl.

Random Number Generator

Attack Protection

Active Tamper Detection (Physical)

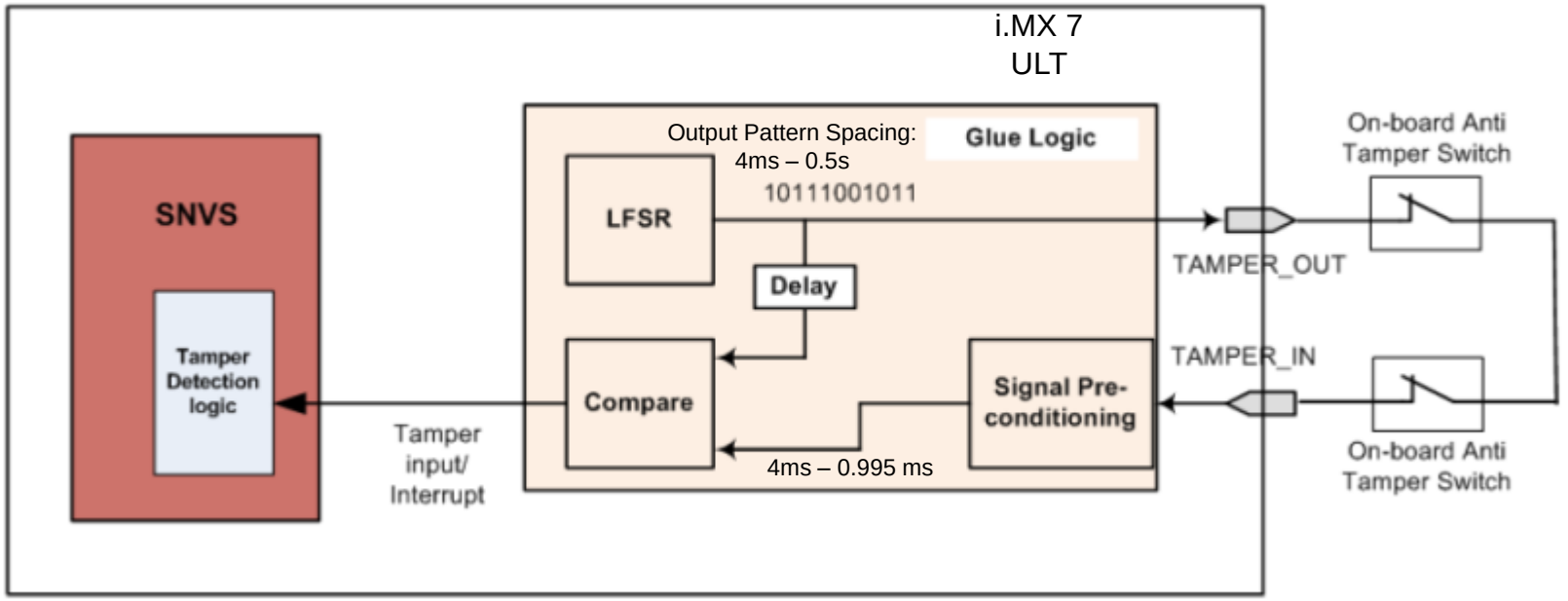
DPA Protection (Side Channel)

Secure S/W Execution

Resource Domain Control

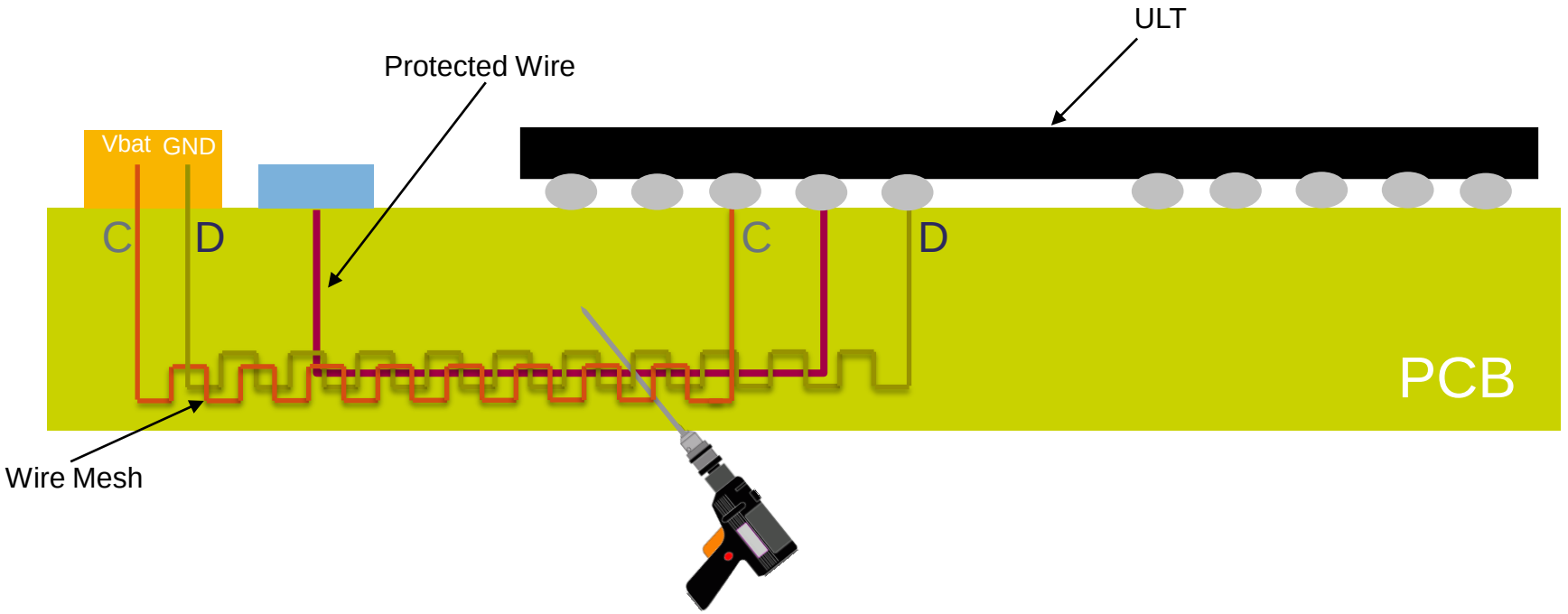
System Memory Protection Unit

External Tamper Detection – PCI4.0 Compliance Targeted



- **10 dedicated pins for active tamper detection**
  - Each pair of pins is used for active wire-mesh outputs/inputs that provides up to 5 active meshes
- **Pattern generated via 16-bit Linear Feedback Shift Register (LFSR)**
- **Glitch filter per active tamper input pin.**
- **LFSR seed randomized by scrambling internal design signals.**

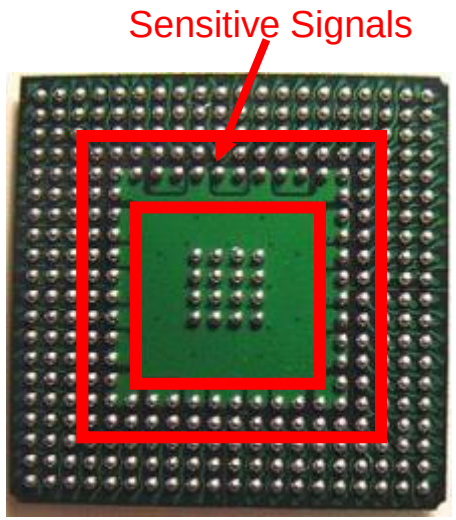
Differential PCB Tamper Detection (Wire Mesh)



- **SNVS module will detect Tamper and initiate key erasure when:**
  - C is disconnected (floating)
  - D is disconnected (floating)
  - C and D are short-circuited

Sensitive Pins

- **Sensitive Pins located at least 3 Row deep within BGA package**
  - Include All passive tamper pins
  - Include All Active tamper pins
  - Include internal
  - Battery Supply
  - Others



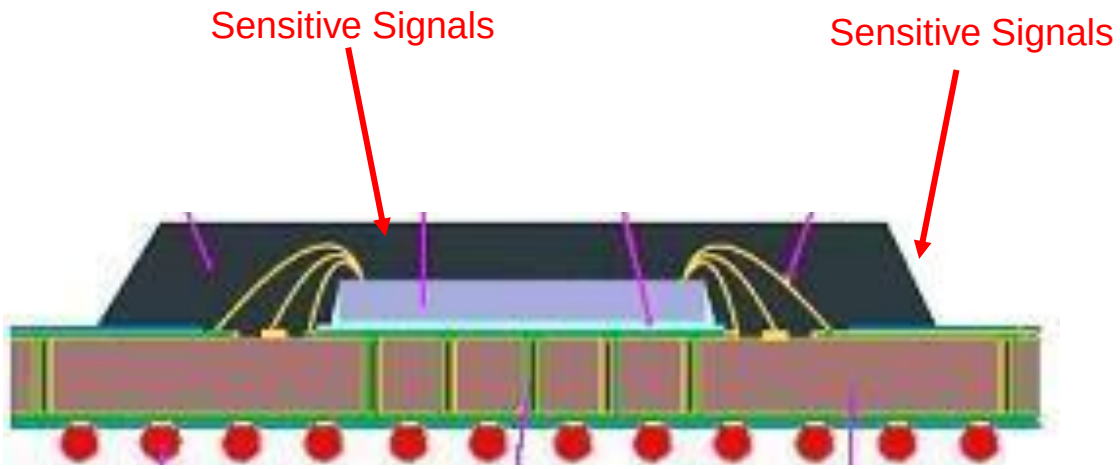
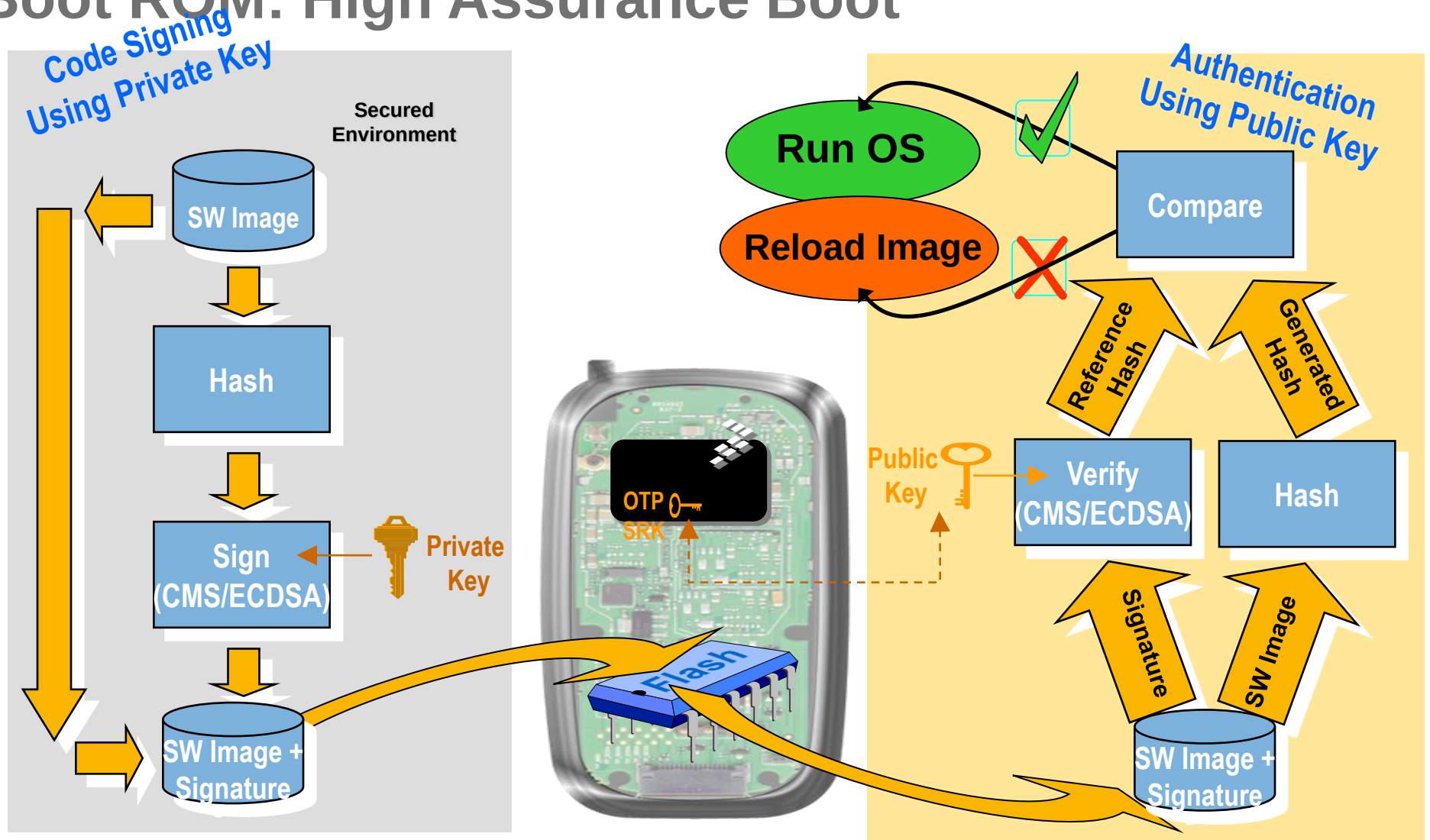


Image does not represent actual i.MX 7 ULT packaging

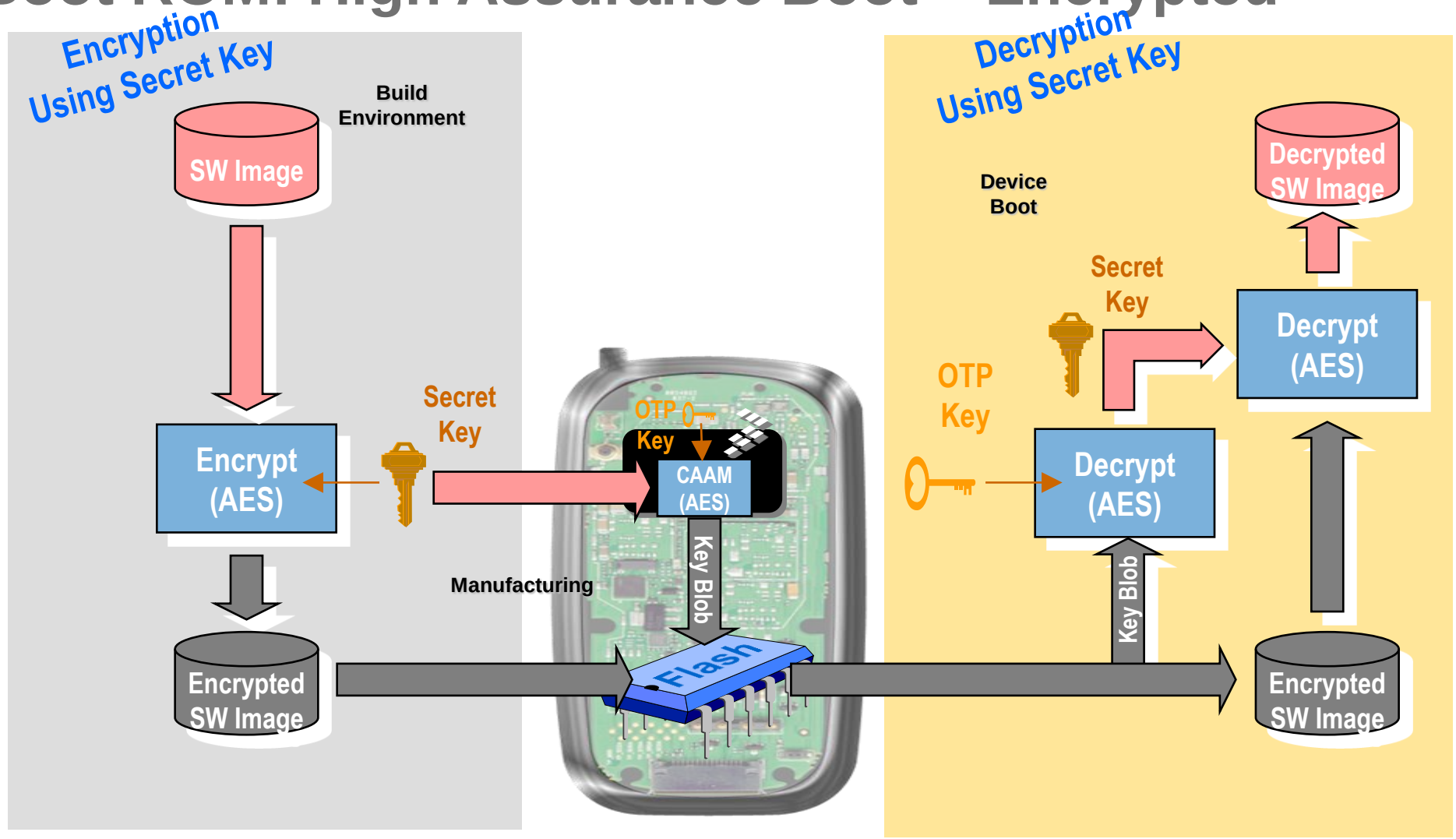
Secure Boot: HAB4.2 Features

Feature	HAB4	Comments
Image authentication	Yes	Yes
Super Root Key	Multiple, revocable	Fused Hash
Public key type	RSA-4096 (max)	256-bit security achieved with RSA-4096
Certificate format	X.509v3	Tools support
CMS (PKCS#1)	CMS (PKCS#1)	Tools support
Hash algorithm	SHA-256	NIST recommended
Image Encryption	Yes	
Wrapped key format	CAAM blob	Secret keys stored in secure RAM partition on i.MX6 Dual/Quad
Secret key type	AES-128/192/256	
Decryption algorithm	AES-CCM	Authenticated decryption
Device configuration commands	▶Write value ▶Set/clear bitmask ▶Wait on bitmask	Provides flexible device configuration
Unlock commands	▶Field Return fuse ▶Revocation fuses ▶Secure JTAG ▶CAAM/SNVS	Secure by default

Boot ROM: High Assurance Boot

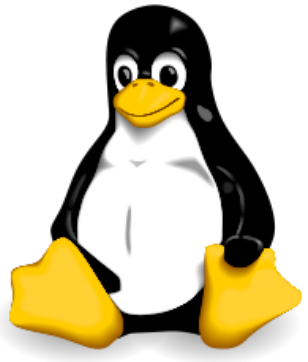


Boot ROM: High Assurance Boot – Encrypted



SOFTWARE

i.MX 7: Software



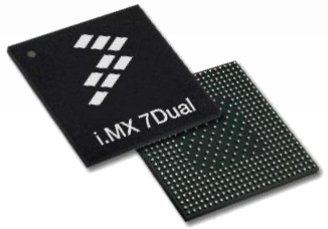
yocto PROJECT

ENABLEMENT

Freescale Full Solutions

i.MX7

- **1 GHz** ARM® Cortex™-A7
  - **NEON™ coprocessor**
- ARM® Cortex™-M4,
- **Electronic Paper Display (EPD)** in addition to LCD.
- Targeting a broad range of applications including many **low power**, **portable** consumer devices



+

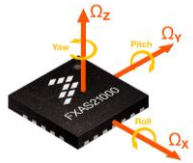
PMIC

- Integration of Freescale's PMIC chip set with i.MX processor for optimization of power efficiency and software/hardware integration
- One-stop customer service and support during development phase to enable the design process

+

Sensors

- MEMS gyroscopes for reliable sensing and measuring
- Magnetometers: measuring the magnitude and direction of magnetic fields
- Pressure Sensing Devices, composed of single silicon, piezoresistive devices



=

i.MX7 SABRE Board

Development platform:

- Single-board evaluation kit
- Linux® and Android™ Board Support Packages are available out of box and updates through Freescale.com

A Single Solution for Streamlined Performance

I.MX7D SABRE

i.MX 7: SABRE Platform Planned Key Features

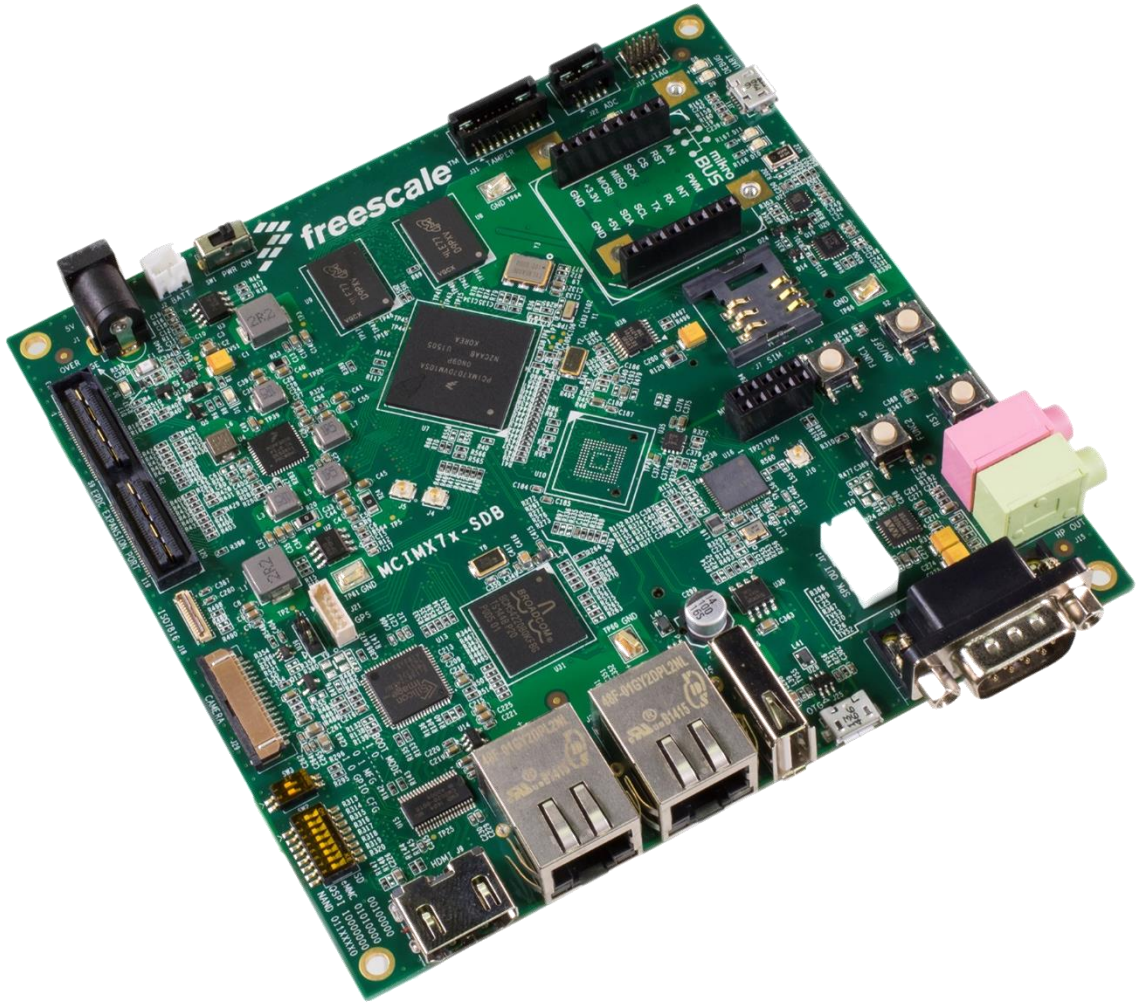
Processor
- Freescale i.MX 7Dual
  - Dual Cortex™-A7 @1GHz
  - 512KB L2$
- Freescale PF3000 PMIC

Memory
- 1 GB DDR3
- eMMC5.0 footprint
- QuadSPI Flash
- SD/MMC socket
- NAND footprint

Display/Camera Connectors
- HDMI
- Parallel LCD
- MIPI-DSI
- Electronic Paper Display
- MIPI-CSI (camera)

Wireless
- Wifi (802.11ac) onboard
- BT4.0 / BLE onboard

Audio
- Audio HP Jack
- External speaker connection



Connectivity
- USB Host connectors
- microUSB OTG connector
- ETH (1Gbit) Receptacle
- ETH (10/100) Receptacle
- Full Mini PCIe socket
- SIM Card slot
- CAN (DB-9)
- GPIO
- MFi Module support
- MikroBus expander

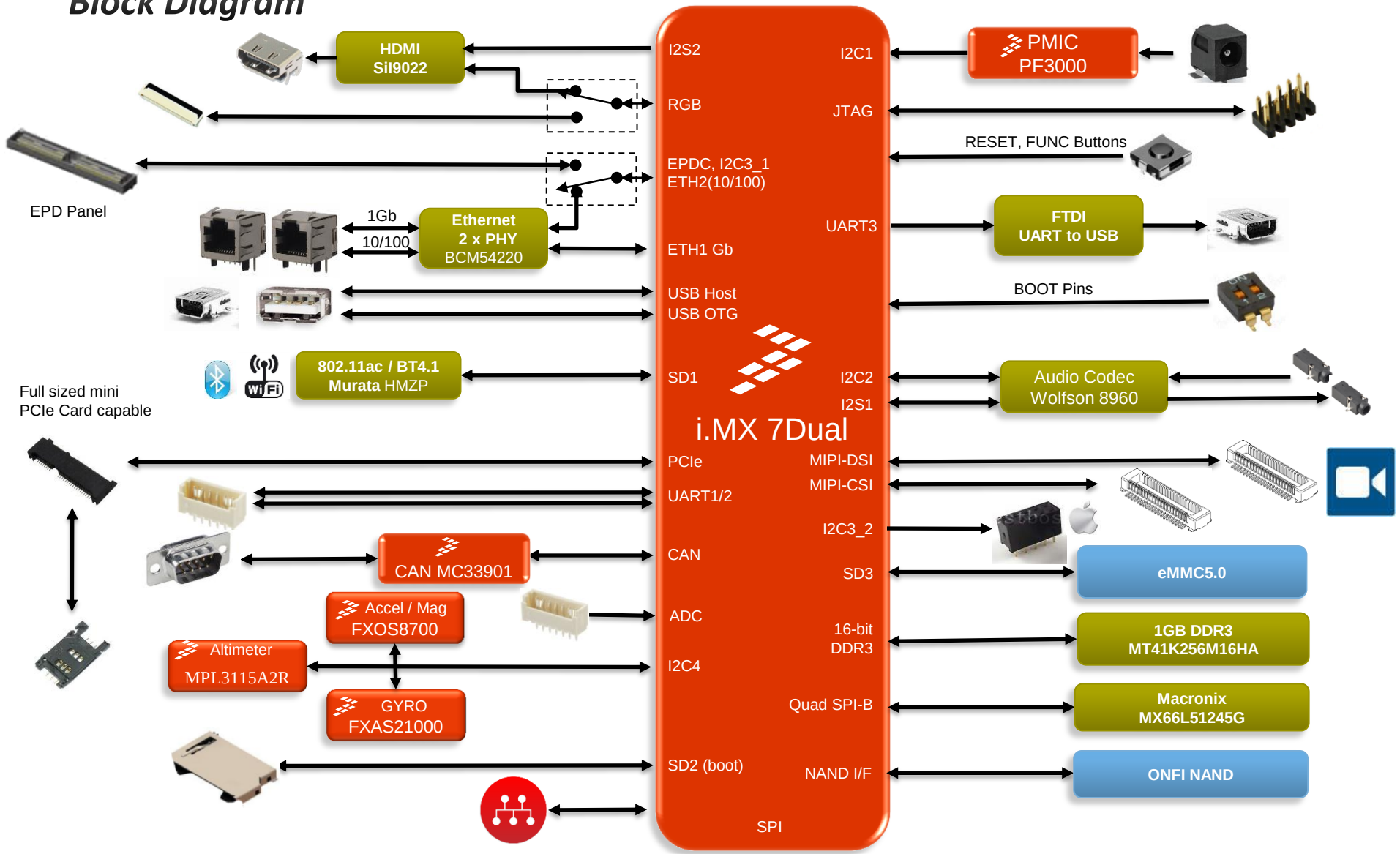
Debug
- JTAG connector
- UART via USB

Sensors
- **FXOS8700** three-axis digital accelerometer/Magnetometer
- **MPL3115A2R** Altimeter/Pressure sensor
- **FXAS21000** three-axis digital Gyroscope

Tools & OS Support
- Linux®
- Android™
- FreeRTOS

i.MX 7 Platform

Block Diagram



SECURE CONNECTIONS
FOR A SMARTER WORLD