SECURITY MODELS FOR APPLICATION PROTECTION AND AGAINST REVERSE ENGINEERING

SECURITY @ KONTRON
PETER MÜLLER, DIRECTOR PRODUCTLINE BOARDS & MODULES

TELEREX

OCTOBER , 2017

AGENDA

01
TECHNOLOGICAL EVOLUTION OF DATA

02
SECURITY LAYERS

03
KONTRONS APPROTECT SOLUTION

04
APPENDIX: KONTRONS COMS BASED ON ARM

TECHNOLOGICAL EVOLUTION

Continuous evolution

1930

- Manual operations required to fulfill services

Today

- Hardware is commodity (servers)
- Software is replacing manual labor

New demand drivers …

Smart applications

Data needs

Connectivity needs

Security needs

… lead to new IoT solutions, related infrastructure, and business models

- Smart applications that use connected devices and cloud software to build IoT solutions
- Device software/middleware is key to enable the needed infrastructure and function

EMBEDDED SOFTWARE SECURITY – SITUATION TODAY

➔ Rapidly growing number of connected devices (IoT)
- 2017 | 8.0 bn devices, 2020 > 20.0 bn devices expected

➔ Computing power of embedded deivces is growing
- High performance CPUs, extended memory, complex software

➔ Embedded devices are implemented in more and more important machinery
- This drives motivation for attacks

OT & IT ENVIRONMENT

Manufacturing

But what if there is a hole in the Firewall?

TRUSTED COMPUTING GROUP

Secure Elemements and SGX

- PLCs and Gate
- Communicate ...nication
  wireless comn ... application
- Control & Data aggregation

Factory Floor / On Premise

Internet

EMBEDDED SOFTWARE SECURITY – MANY DIFFERENT ASPECTS

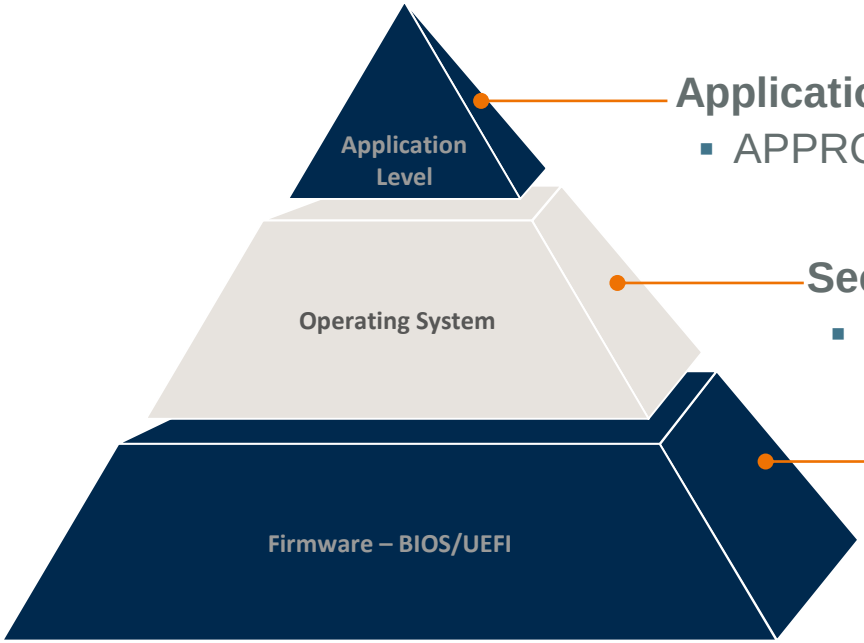
➔ Prevent misusage of device / functionality of device

➔ Secure device data / data protection

➔ Copy Protection / Secure intelectual property (IP)

SECURITY LAYERS

KONTRON SECURITY LAYERS



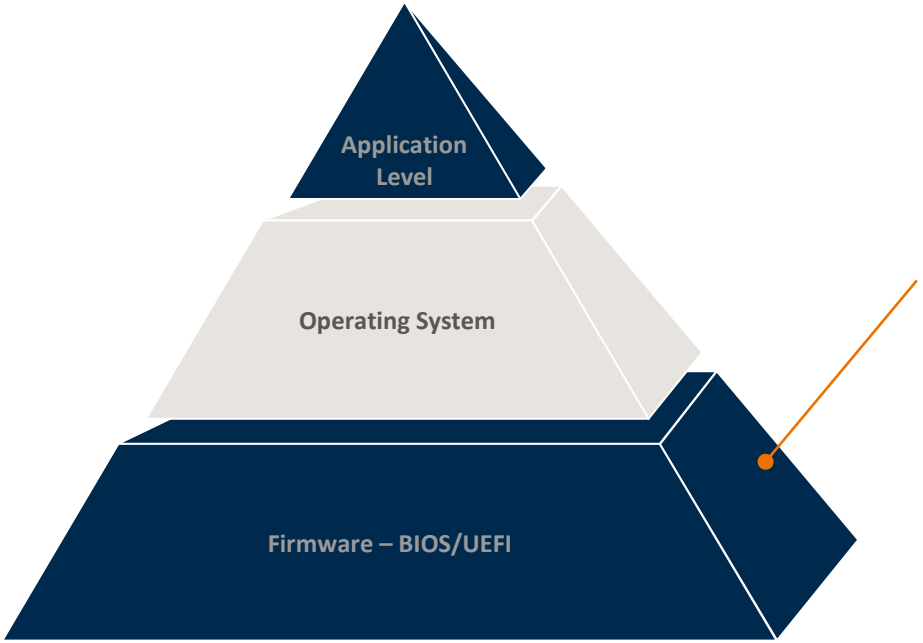
Application Level Security
- APPROTECT

Secure Operating System
- TPM + Bitlocker (WIN10)

Secure/Trusted Boot
- TPM + Kontron BIOS

3 LEVELS OF SECURITY ENSURE HIGHEST LEVEL OF SECURITY FOR EMBEDDED SYSTEMS

SECURITY LAYERS – SECURE & TRUSTED BOOT

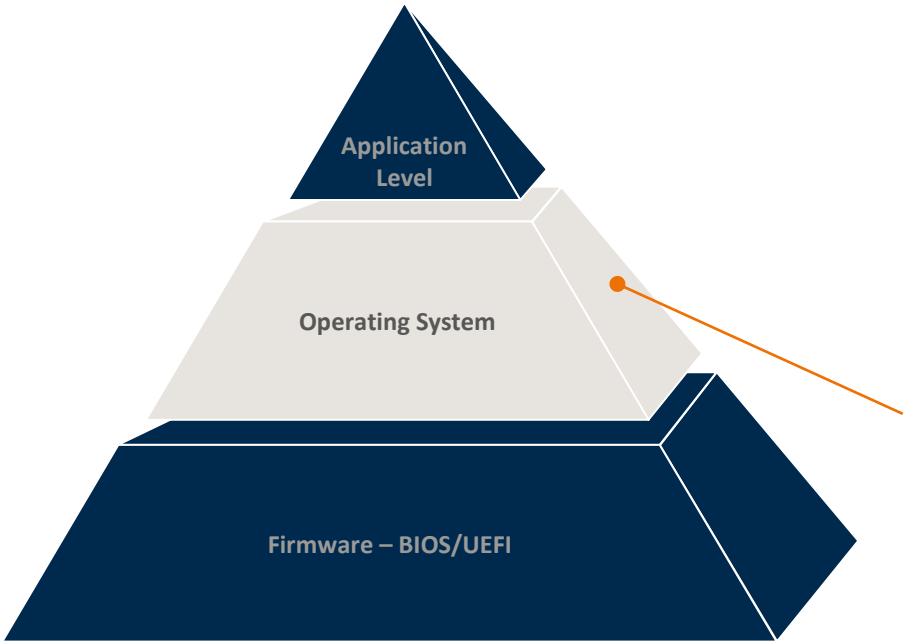


- Built into the BIOS
- BIOS Flash is protected
- OS loader is verified
- Software based

- Make sure the correct BIOS is executed

EVERYTHING STARTS WITH THE BIOS AND PROTECTED STORAGE DEVICE

SECURITY LAYERS – SECURE & TRUSTED OPERATING SYSTEMS

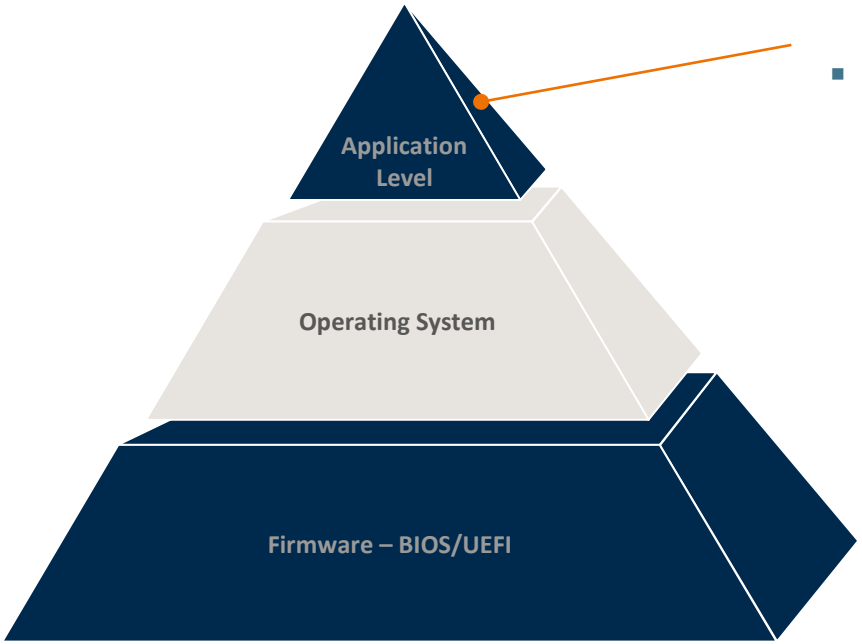


- Windows 10 IoT featuring with TPM 2.0:
  - Trusted Boot Loader
  - Verification of executables
  - Measured boot stores boot history
  - BitLocker
  - Device Guard
- Alternatively Linux

- Remote attestation (external or internal)

MODERN OPERATING SYSTEMS PROVIDE ENCRYPTION, AUTHENTICATION, KEY HANDLING

SECURITY LAYERS – SECURE APPLICATION



- APPROTECT – IP protection, copy/reverse engineering protection
- APPROTECT Licensing – Enabling new business models

HARDWARE SUPPORT TO PROTECT YOUR INTELLECTUAL PROPERTY

SECURITY SOLUTION KONTRON

- **System Boot-Time Security:**
  Offering Secure/Trusted-Boot and Update implementations available for all systems with the latest generation of Intel®'s Core™ and Atom™ CPUs.
- **Secure Operating Systems:**
  Offering attractive bundlings with operating systems like Windows 10 IOT.
- **Application Level Security with APPROTECT powered by WIBU:**
  Offering copy protection and reverse engineering protection with hardware based encryption; on top enabling new business models by restricting runtime or features of any custom application.

TO COVER MARKET NEEDS FOR SECURITY AND DEVICE MANAGEMENT KONTRON OFFERS THE COMPLETE SOFTWARESTACK TO ENABLE SECURE AND TRUSTED PRODUCTS AND ALLOW CUSTOMERS TO ACTIVELY MANAGE THEIR PORTFOLIO

APPROTECT FROM KONTRON

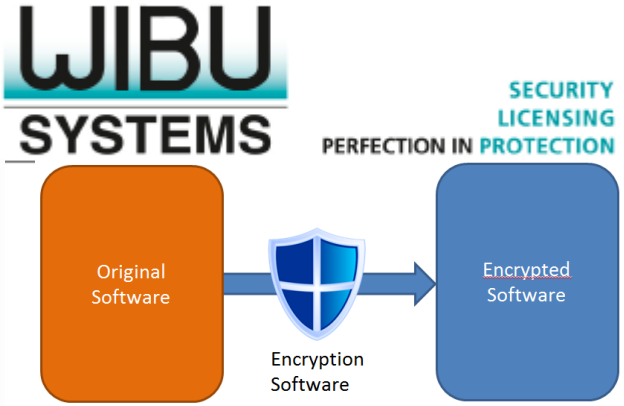
KONTRON APPROTECT

- ‘**APPROTECT**’ allows copy protection of executables
- ‘**APPROTECT Licensing**’ allows various licensing models like
  - Pay per Use
  - Run a certain time, time based license
  - Add / remove features
  - ....

- Hardware versions
  - Security chip on board (COMe/SMARC/Motherboards)
  - Security chip on USB stick or mPCIe card for upgrade kits

SECURITY SOLUTION KONTRON APPROTECT / APPROTECT LICENSING

HW enabled on all new Kontron embedded designs plus SW framework



Kontron APPROTECT

- IP protection
- Copy/reverse engineering protection

Kontron APPROTECT Licensing

- Enabling new business models

ALL NEW DESIGNS OF MODULES/BOARDS/SYSTEMS INCLUDE APPROTECT HARDWARE

COM – PRODUCT LINE

125 x 95 mm

COMe basic

95 x 95 mm

COMe compact

84 x 55mm

COMe mini

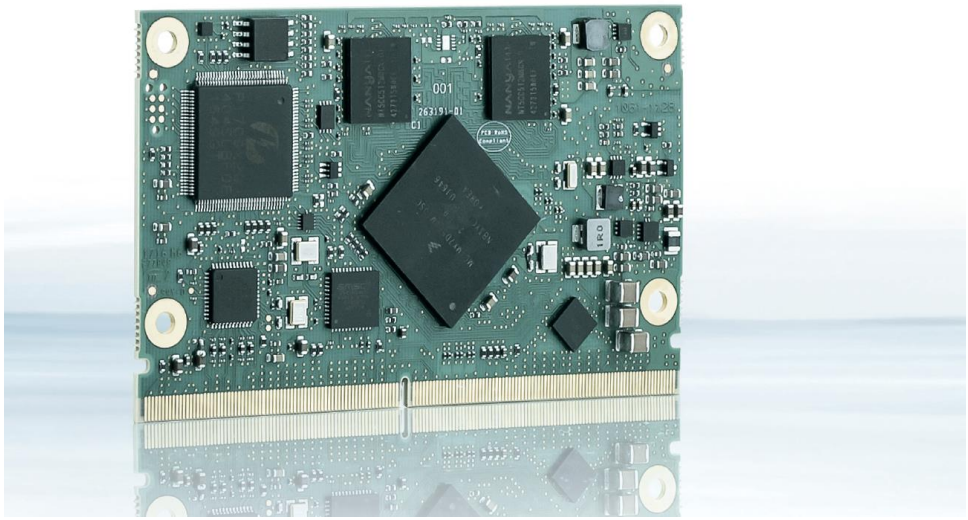
82 x 50 mm

SMARC

PRODUCTS WITH APPROTECT

Product	APPROTECT	APPROTECT Licensing	Secure / Trusted Boot
COMe-bSL6	✓	✓	
COMe-cSL6	✓	✓	
SMARC-sAMX7	✓	✓	
mITX-SKL-S-C236	✓	✓	
FlexATX-SKL-C236	✓	✓	
COMe-mAL10	✓	✓	✓
COMe-bKL6	✓	✓	✓
COMe-cKL6	✓	✓	✓
COMe-cAL6	✓	✓	✓
SMARC-sXAL	✓	✓	✓
mITX-SKL-H	✓	✓	✓
mITX-KBL-H	✓	✓	✓
mITX-KBL-S-C236	✓	✓	✓
FlexATX-KBL-C236	✓	✓	✓
pITX-APL	✓	✓	✓
3.5-APL	✓	✓	✓
Kbox C-102 (COMe-bSL6)	✓	✓	
Other systems (with upgrade kit APPROTECT)	✓	✓	

SMARC 2.0 IMX7



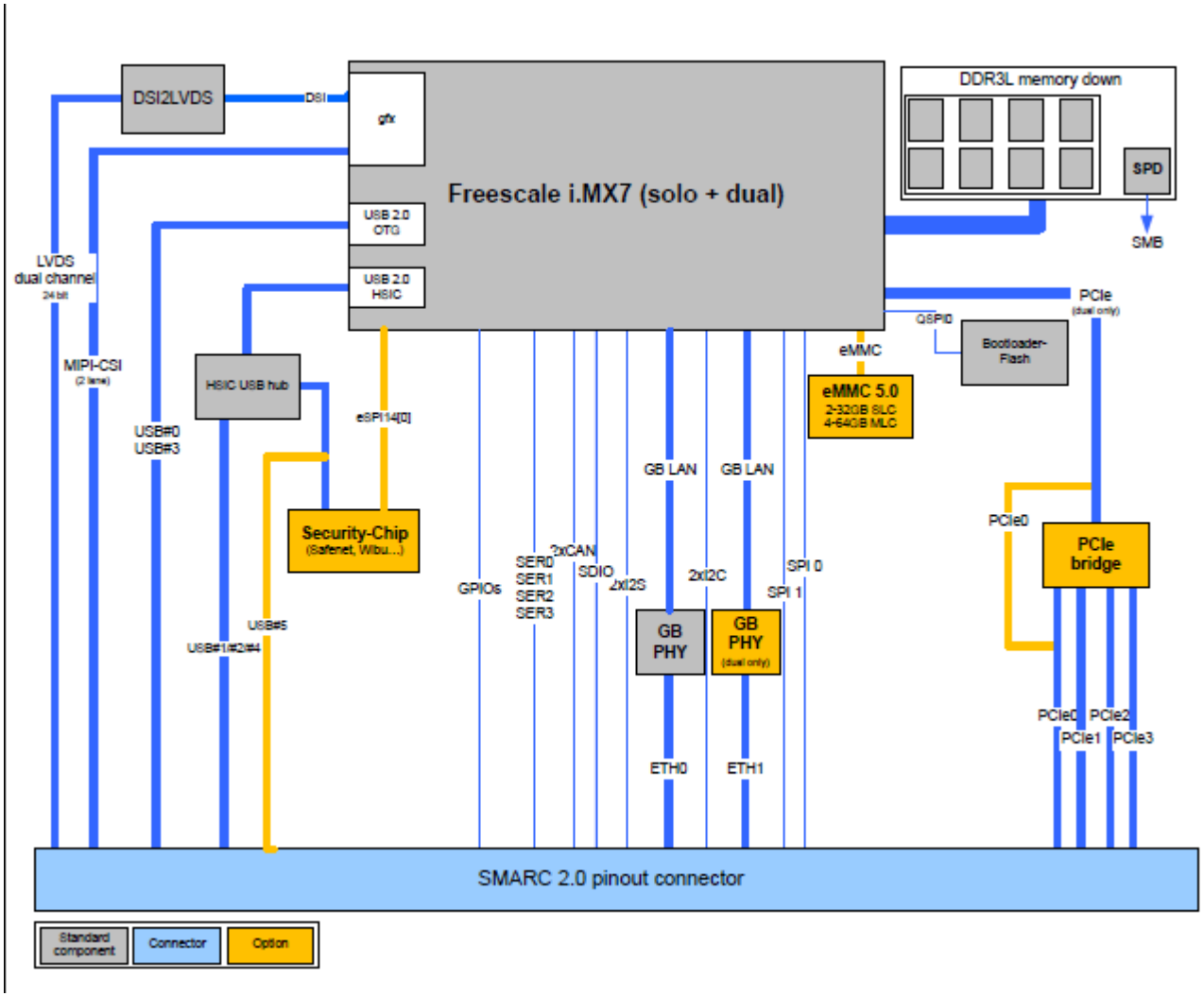
Perfect fit to build up little router or gateway BOX PC

Build in Security Solution already comes along with Hardware

SMARC MODULE WITH EXTREM LOW POWER i.MX7 SERIES PROCESSOR

- Up to 2x 1 GHz Cortex® A7 + 200 MHz M4 processor
- Up to 2 GByte RAM
- Dual channel LVDS interface
- Up to 2x GByte Ethernet, 3x PCIe, 4x USB 2.0
- support of Kontron's Embedded Security Solution (Approtect)

SMARC 2.0 IMX7 MODULE BLOCK DIAGRAM



EMBEDDED SOFTWARE SECURITY – APPLICATION EXAMPLE

- Temper protection (FDA, MPG)
- Quality assurance
- Licensing
- Pay Per Use

sirona
The Dental Company

WIBU SYSTEMS
SECURITY
LICENSING
PERFECTION IN PROTECTION

THANK YOU