

Security / Trusted Execution Environment and Functional Safety with Zynq Ultrascale+ MPSoC / RFSoc

- Sebastian Stiemke, Director Operations, Missing Link Electronics
Andreas Schuler, Director Applications, Missing Link Electronics



1

2/7/19

Agenda

- Definition Safety and Security
- Security Intro
 - Why?
 - General intro
 - Arm TrustZone
 - OP-TEE
- Safety Intro
 - State of the art
 - Xilinx Safety Lounge

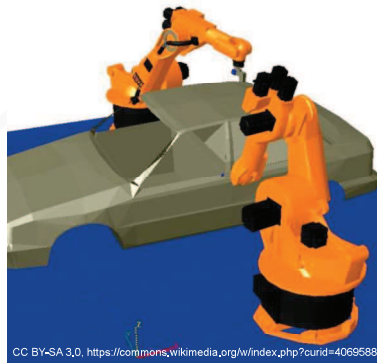
2

2/7/19



Security and Safety (Sicherheit)

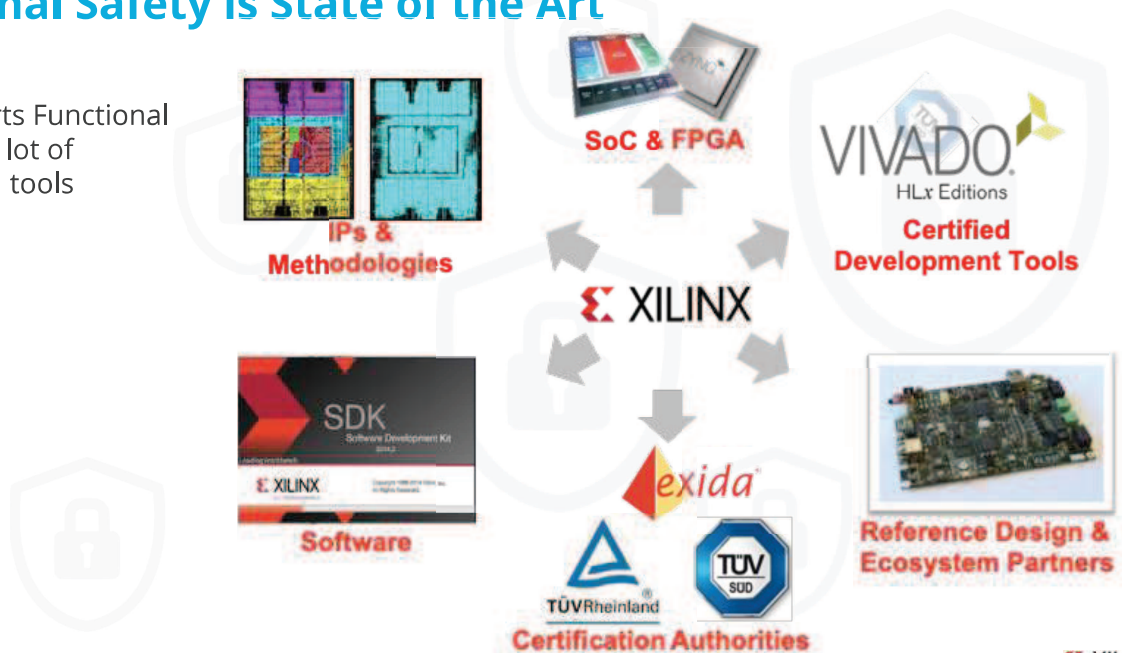
Security:
Protection of the system against unauthorised access



Safety:
Protection of the environment from system effects

Functional Safety is State of the Art

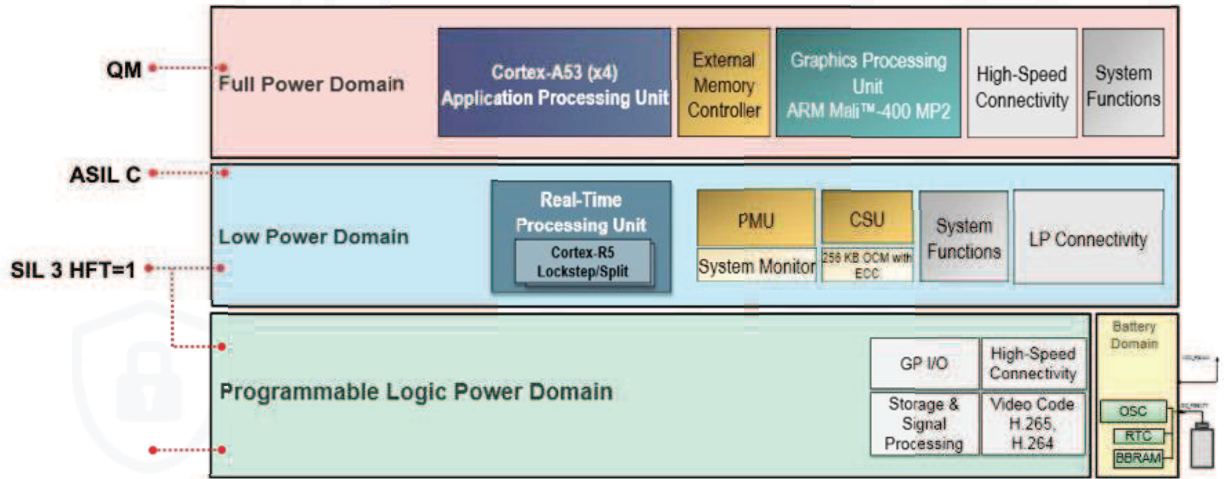
Xilinx supports Functional Safety with a lot of activities and tools



Source: XILINX

Devices are Developed under Functional Safety Aspect

Safety architecture of Zynq UltraScale+



Source: XILINX



5

Vivado Toolchain Certified for Safety Use



Source: XILINX



6

2/7/19

Functional Safety Lounge

For more information visit the Functional Safety Website:
<https://www.xilinx.com/safety>

For Toolchain Certificates, Functional Safety Assessment Reports and much more you can register to the:

Functional Safety Lounge

Functional Safety Lounge

Overview

ISE / Vivado

7-Series

Zynq
UltraScale+

Miscellaneous

Announcements:

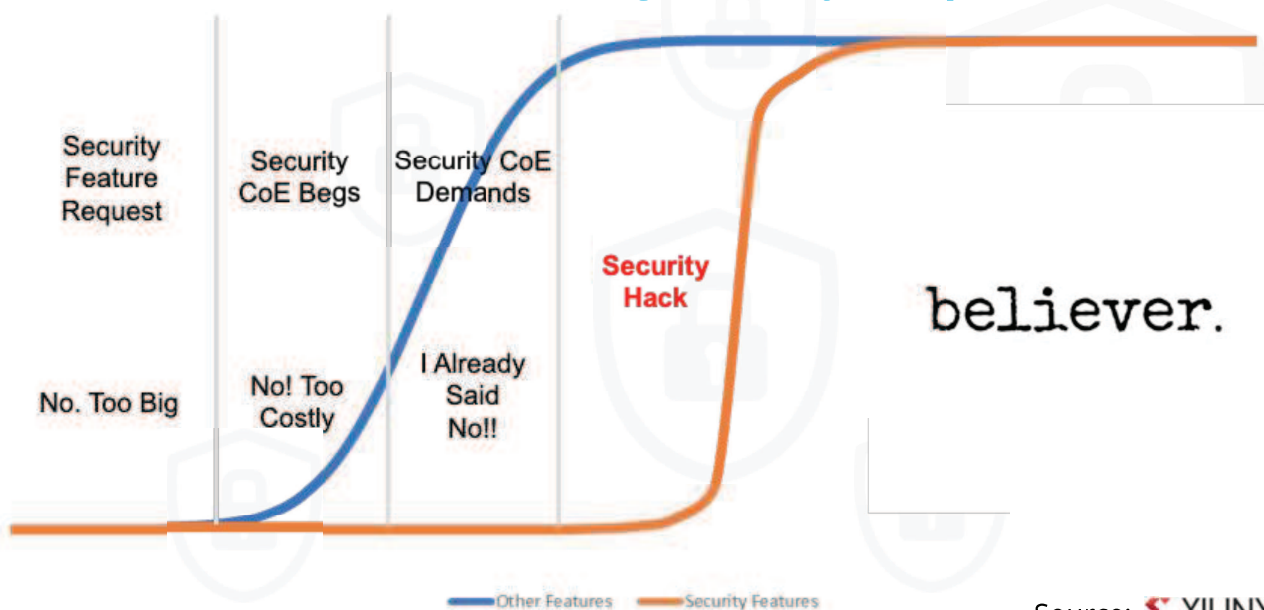
Xilinx has received the Certificate Z10 16 11 84605004 from Tuv SUD for the FPGA Programming Tool Chain of the Vivado Design Suite 2015.2, for Safety Related Development on November 10, 2016.



Certificate
Microblaze
Compiler
Tool Chain
2016.2



The Unfortunate Truth Driving Security Adoption



Source: XILINX
SECURE SOLUTIONS

The Evidence:

New Mirai malware variant targets signage TVs and presentation systems

Security researchers spot new Mirai botnet with an enhanced arsenal of IoT exploits.

Silex Malware: Deadly New Virus Bricks 1000s of IoT Devices

by Michael Schachter on July 2, 2019

Hackers were able to remotely control a moving Tesla Model S

FDA confirms that St. Jude's cardiac devices can be hacked

by Selena Larson @selenal Larson

Source: XILINX SECURE SOLUTIONS



Defining Security

ANTI-TAMPER (AT)
Protecting customers IP (Reverse Engineering, Cloning, etc.)

CYBER SECURITY

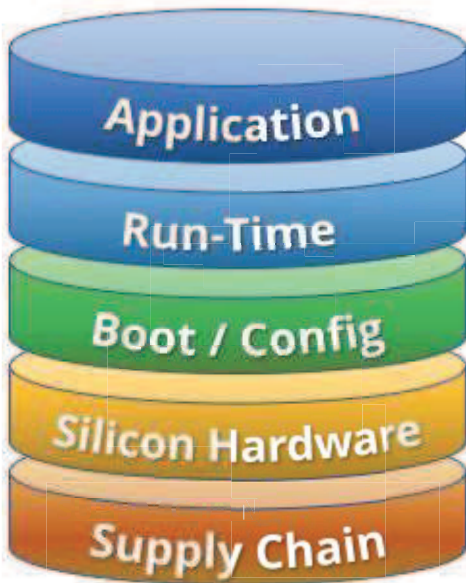
INFORMATION ASSURANCE (IA)
Protecting customers information/data using cryptography and other means

TRUST
Silicon, software, firmware and IP is "trojan-free"

Source: XILINX SECURE SOLUTIONS



Responsibilities



Digital Signatures, User Passwords, Tokens, Biometrics Role-based Accounts, etc.

Customer Responsibility

Hypervisors, Microkernels, TrustZone, Isolation Design, Flow Protections, Security Monitor, etc.

Shared Responsibility

Asymmetric/Symmetric Authentication, AES Crypto, DPA Protections, etc.

Xilinx Responsibility

Security Critical Redundancy, JTAG Protections, Environmental Monitors, Tamper Detection/Penalties, etc.

World Class Best Practices, Authorized Suppliers, Blind Buys, Anti-counterfeit, etc.



Source: XILINX SECURE SOLUTIONS



Security Feature Overview

Active Security Features	Virtex-5 (65nm)	Spartan-6 (45nm)	Virtex-6 (40nm)	7-Series (28nm)	Zynq-7000 (28nm)	UltraScale/+ (20/16nm)	Zynq US+ (16nm)
Internal Configuration Memory R/W Access	✓	✓	✓	✓	✓	✓	✓
Programmable Logic SEU (Health) Checking	✓	✓	✓	✓	✓	✓	✓
Dynamic JTAG Disable/Monitor	✓	✓	✓	✓	✓	✓	✓
Secure Programmable Logic Clock Source	✓	✓	✓	✓	✓	✓	✓
Internal AES Key Clear	✓	✓	✓	✓	✓	+ Verify	+ Verify
Global 3-state/Set-reset (GTS/GSR)	✓	✓	✓	✓	✓	✓	✓
On-chip Temperature/Voltage Monitors & Alarms	✓	x	✓	✓	✓	✓	✓
Unique Identifiers (Device DNA & User eFUSE)	x	x	✓	✓	✓	✓	✓
Permanent JTAG Disable (internally)	x	x	x	x	x	✓	✓
Secure BBRAM Key Agility in the Field	x	x	x	x	x	✓	✓
Non-volatile Tamper/Maintenance Logging	x	x	x	x	x	✓	✓
Permanent Decryptor Disable	x	x	x	x	x	✓	x
User Accessible Crypto Accelerators	x	x	x	x	x	x	✓
Programmable Tamper Responses	x	x	x	x	x	x	✓
Secure External Data Storage (via PUF)	x	x	x	x	x	x	✓
Public Key Revocation/Replay Protection	n/a	n/a	n/a	n/a	x	x	✓
ARM TrustZone	n/a	n/a	n/a	n/a	✓	n/a	✓
ARM v8 Cryptography Extensions	n/a	n/a	n/a	n/a	x	n/a	✓
Memory/Peripheral Protection Units (XMPU/XPPU)	n/a	n/a	n/a	n/a	x	n/a	✓
AXI/APB Isolation Block (AIB)	n/a	n/a	n/a	n/a	x	n/a	✓
System Memory Management Unit (SMMU)	n/a	n/a	n/a	n/a	x	n/a	✓

ACTIVE FEATURES

Source: XILINX SECURE SOLUTIONS



Security Feature Overview

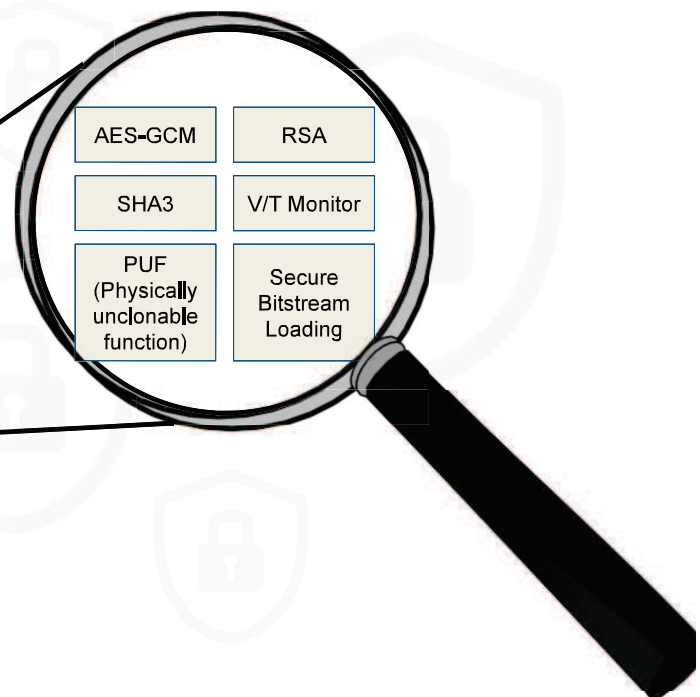
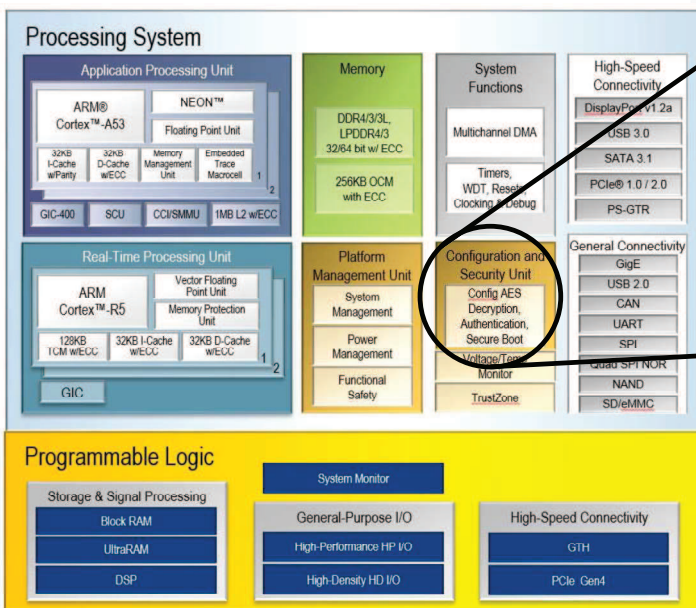
Passive Security Features	Virtex-5 (65nm)	Spartan-6 (45nm)	Virtex-6 (40nm)	7-Series (28nm)	Zynq-7000 (28nm)	UltraScale+ (20/16nm)	Zynq US+ (16nm)
Confidentiality w/ AES-256	✓ CBC Mode	✓ CBC Mode	✓ CBC Mode	✓ CBC Mode	✓ CBC Mode	✓ GCM Mode	✓ GCM Mode
Secure AES Key Storage (BBRAM/eFUSE)	✓ BBRAM Only	✓	✓	✓	✓	✓	✓
Readback Disable	✓	✓	✓	✓	✓	✓	✓
Symmetric Authentication	✗	✗	✓ HMAC	✓ HMAC	✓ HMAC	✓ AES-GCM	✓ AES-GCM
Asymmetric Authentication	✗	✗	✗	✗	✓ RSA-2048	✓ RSA-2048	✓ RSA-4096
Permanent JTAG Disable	✗	✗	✗	✗	✓	✓	✓
DPA Resistance	✗	✗	✗	✗	✗	✓	✓
Permanent DFT Disable	✗	✗	✗	✗	✗	✓	✓
Obfuscated Key Storage	✗	✗	✗	✗	✗	✓	✓
Encrypted (black) Key Storage (via PUF)	✗	✗	✗	✗	✗	✗	✓
Secure Boot/Configuration Clock Source	✗	✗	✗	✗	✗	✗	✓

PASSIVE FEATURES

Source: XILINX SECURE SOLUTIONS



Zynq Ultrascale+ Architecture



Arm TrustZone – Hardware Enforced Isolation



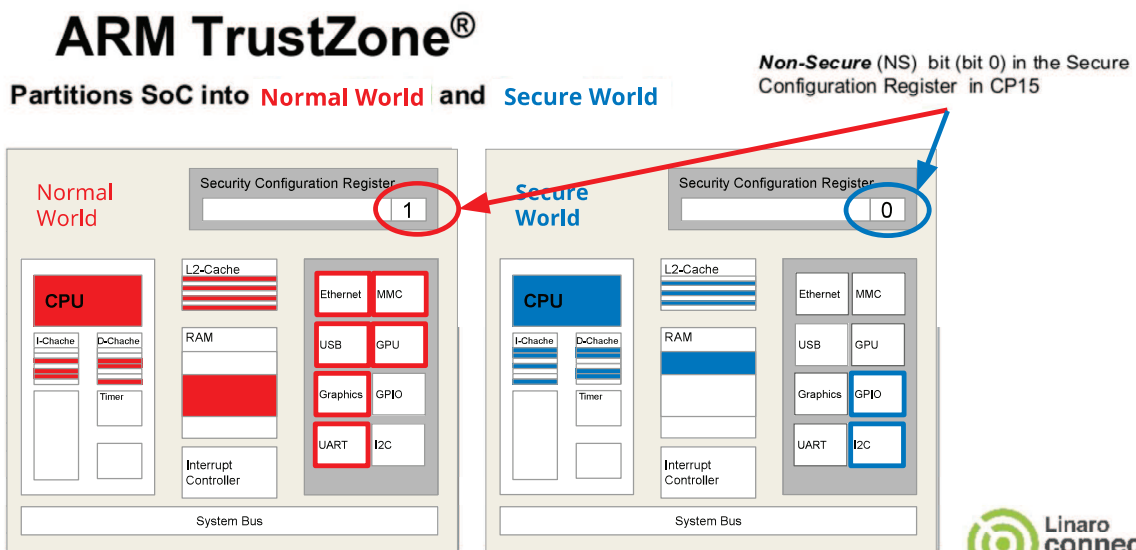
- ▶ Secures the AXI bus for read and write transactions
- ▶ AxPROT[1] – AXI Read or Write
 - ▶ '0' – Clear for secure transactions
 - ▶ '1' – Set for non-secure transactions
- ▶ Propagated from the Application Processing Unit (APU) to the Programmable Logic (PL)
- ▶ Applicable Xilinx Labs
 - ▶ Functional and Physical Isolation Within the Programmable Logic (PL) of the Zynq UltraScale+ MPSoC
 - ▶ Functional and Physical Isolation Within the Processing Subsystem (PS) of the Zynq UltraScale+ MPSoC

15

2/7/19

mle
missing link electronics

Arm TrustZone – Hardware Enforced Isolation



Source: <https://www.slideshare.net/linaroorg/bkk16110-a-gentle-introduction-to-trusted-execution-and-optee>

16

2/7/19

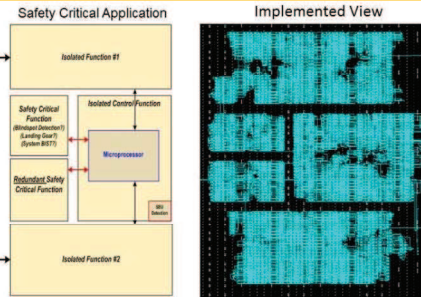
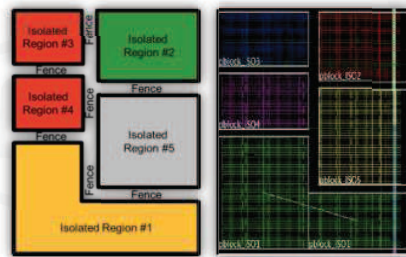
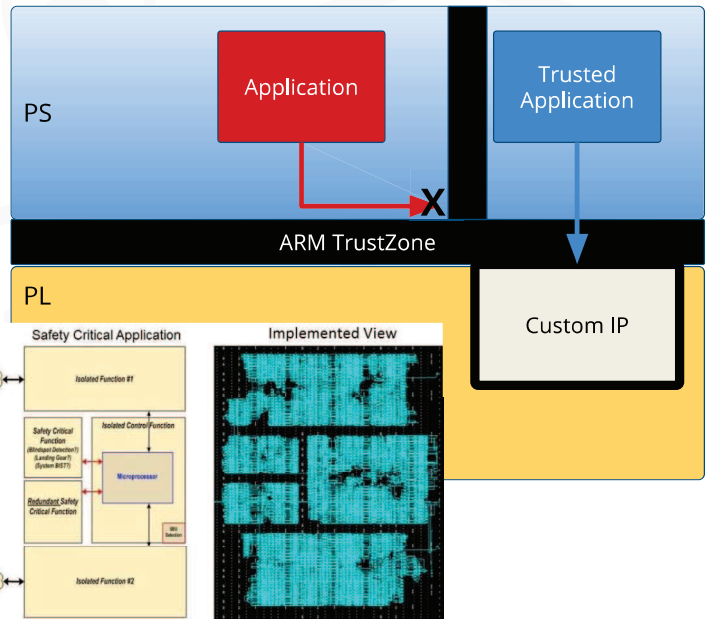
Linaro connect
Bangkok 2016

mle
missing link electronics

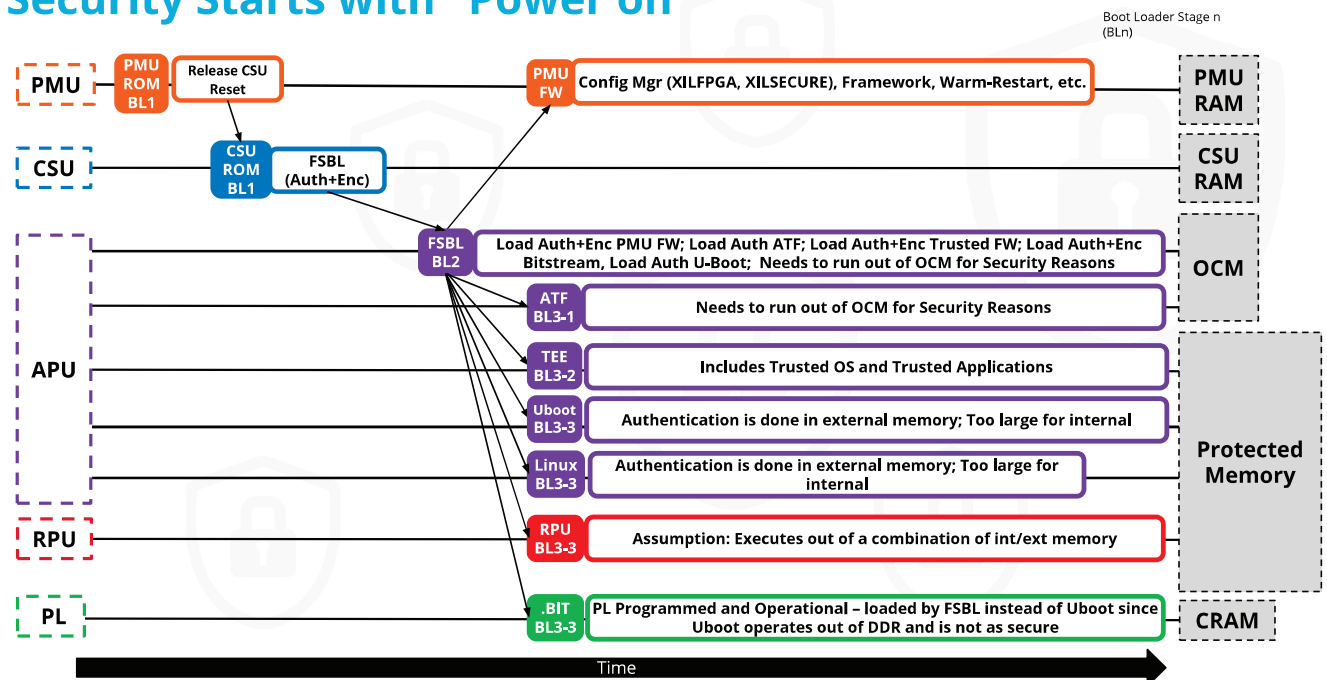
Arm TrustZone – Hardware Enforced Isolation extended in PL

The secure functions can be extended into the Programmable Logic:

- ▶ The Arm TrustZone regulates the access to this resource by checking if the request comes from a trusted or untrusted source
- ▶ Xilinx Isolation Design Flow (XIDF) ensures the function is physically isolated and can not be tempered by closely IP cores



Security Starts with "Power on"

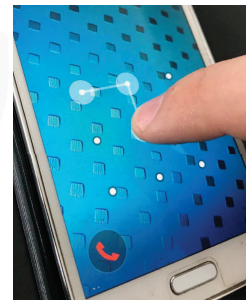


OP-TEE

- ▶ What is OP-TEE?
 - ▶ OP-TEE is a Open Platform Trusted Execution Environment
 - ▶ Utilizes arm TrustZone to isolate Hardware
 - ▶ Utilizes Exception Levels to isolate Software
- ▶ Why OP-TEE or why Software Isolation?
 - ▶ To minimize attackable surface
 - ▶ Add another Layer of security between the adversary and your keys

Real World Application

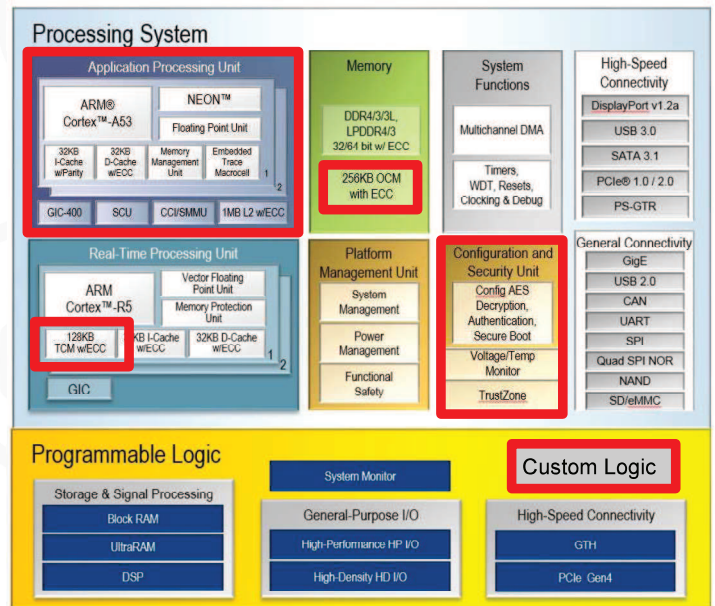
- ▶ Trusted Touch Screen
 - ▶ Touch screen get elevated to secure HW
 - ▶ Data processed in secure world
- ▶ Secure Storage
 - ▶ Encrypt/Decrypt algorithms run in trusted world
 - ▶ Encrypted data stored in untrusted world
- ▶ Secure Communications
 - ▶ Data comes in from an untrusted source that gets authenticated in the trusted world



Quick Look at Zynq Ultrascale+ Architecture

OP-TEE utilizes following parts of a Xilinx Zynq Ultrascale+ device:

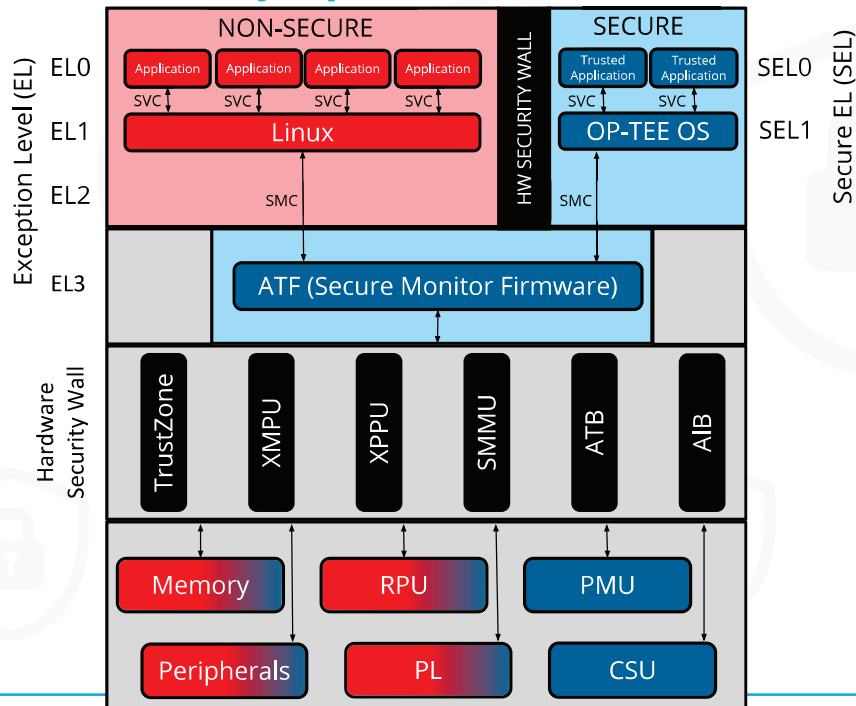
- ▶ ARM Cortex A53 , ArmV8
- ▶ Internal Memory (OCM / TCM)
- ▶ Configuration and Security Unit
- ▶ Indirectly PMU for ATF



TEE Software Components

- ▶ Secure Monitor – ATF
 - ▶ Handles switching from the non-secure state to the secure state and vice versa
 - ▶ Called via a Secure Monitor Call (SMC) exception
 - ▶ Operates at EL3
- ▶ Trusted Operating System
 - ▶ Handles secure device drivers
 - ▶ Loads trusted applications and schedules their operation
 - ▶ Operates at secure exception level 1 (SEL1)
- ▶ Trusted Applications
 - ▶ Runs in the trusted OS to safely deliver trusted services to untrusted applications
 - ▶ Called via a TEE driver running in the non-secure kernel or hypervisor
 - ▶ Operates at SEL0

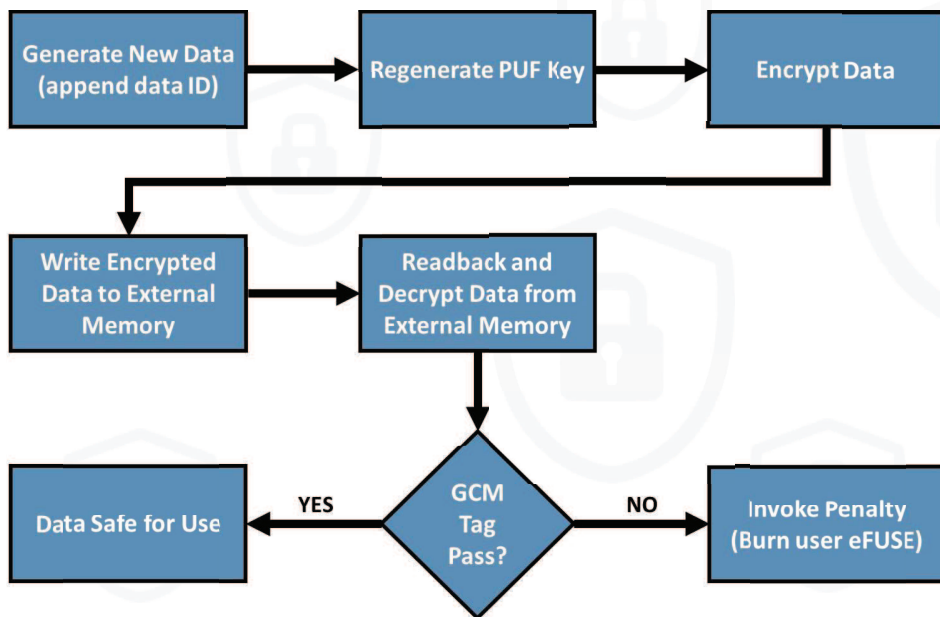
Enhancing the TEE on Zynq UltraScale+



23

2/7/19

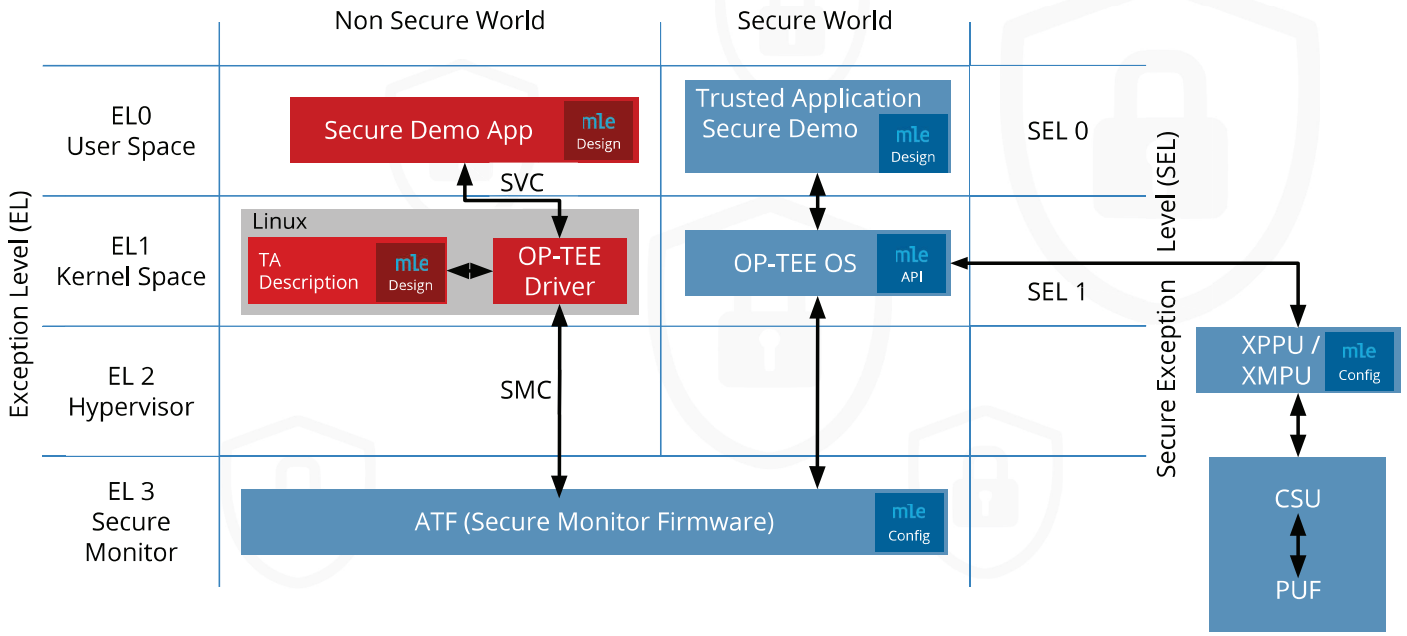
Joint Xilinx/ MLE Demo: Secure Storage



24

2/7/19

Secure Storage Demo



25 2/7/19

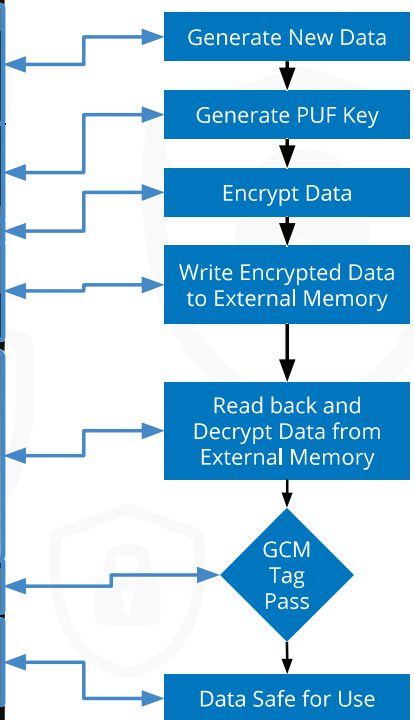


```

root@opteedemo:/# notes example secure storage puf
Prepare session with the TA
Create and load blob in the TA secure storage
Unencrypted blob:
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
Invoke command WRITE_RAW
E/TC:0 create_raw_object:60 *** Entering secure world ***
E/TC:0 create_raw_object:83 Configure PUF configuration 0 and configure the shutter
E/TC:0 create_raw_object:92 Spin up the PUF and connect the key to the AES engine
E/TC:0 create_raw_object:97 Wait for the PUF regeneration to complete
E/TC:0 create_raw_object:102 Initialize & configure the DMA
E/TC:0 create_raw_object:118 Initialize AES engine
E/TC:0 create_raw_object:141 Request to encrypt the blob using PUF Key
E/TC:0 create_raw_object:145 00000000ffe0ffd0 54 5b f4 b5 79 63 2f ae 5f 2f da d9 1f ec 2f f2
E/TC:0 create_raw_object:145 00000000ffe0ffe0 46 b0 8e be c0 72 fd 9d 97 53 26 e2 1a 26 9c 51
E/TC:0 create_raw_object:145 00000000ffe0fff0 7d ae cb 4e 6d f0 e9 65 7b 61 8c 79 76 8c 71 46
E/TC:0 create_raw_object:145 00000000ffe10000 4a d7 b0 8d 6c e1 a3 9b 19 3a 3c f0 a1 8b 56 e1
E/TC:0 create_raw_object:148 Clear the PUF key
E/TC:0 create_raw_object:158 *** Exiting secure world ***

Read back the blob
Invoke command READ_RAW
E/TC:0 read_raw_object:181 *** Entering secure world ***
E/TC:0 read_raw_object:191 Configure PUF configuration 0 and configure the shutter
E/TC:0 read_raw_object:199 Spin up the PUF and connect the key to the AES engine
E/TC:0 read_raw_object:203 Wait for the PUF regeneration to complete
E/TC:0 read_raw_object:207 Initialize & configure the DMA
E/TC:0 read_raw_object:216 Initialize AES engine
E/TC:0 read_raw_object:241 Peek into encrypted blob:
E/TC:0 read_raw_object:242 00000000ffe0ffd0 54 5b f4 b5 79 63 2f ae 5f 2f da d9 1f ec 2f f2
E/TC:0 read_raw_object:242 00000000ffe0ffe0 46 b0 8e be c0 72 fd 9d 97 53 26 e2 1a 26 9c 51
E/TC:0 read_raw_object:242 00000000ffe0fff0 7d ae cb 4e 6d f0 e9 65 7b 61 8c 79 76 8c 71 46
E/TC:0 read_raw_object:242 00000000ffe10000 4a d7 b0 8d 6c e1 a3 9b 19 3a 3c f0 a1 8b 56 e1
E/TC:0 read_raw_object:245 Request to decrypt the blob using PUF Key
E/TC:0 read_raw_object:251 GCM Tag Match!
E/TC:0 read_raw_object:255 Clear the PUF key
E/TC:0 read_raw_object:266 *** Exiting secure world ***

Blob read back:
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1 | .....
Blob read back matches unencrypted blob!
We're done, close and release TEE resources
root@opteedemo:/#
    
```



26 2/7/19



OP-TEE Functionality

Functionality	OP-TEE free	OP-TEE by MLE
OP-TEE Basic functionality	x	x
Trusted Applications	x	x
Secure Paging	x	x
Testsuite	x	x
AES-GCM (hardware accelerated)	-	x
RSA (hardware accelerated)	-	x
SHA3 (hardware accelerated)	-	x
Physical Unclonable Function (PUF)	-	x
eFuse programming	-	x
Secure Bitstream Loading	-	x
Performance Measurement	-	x
Custom PL Functions	-	x

27

2/7/19

mle
missing link electronics

Evaluation/Test Hardware



Ultra96 V2 (~\$250)

Production



Special Order Code to ensure entropy of PUF

28

2/7/19

mle
missing link electronics

Documents

Security Guidance for Zynq UltraScale+:

- XAPP1323 Developing Tamper Resistant Designs with Zynq UltraScale+

Automotive Standards:

- Auto-ISAC (Information Sharing & Analysis Center)
- ISO 21434 (Draft): Road vehicles – Cybersecurity engineering
- SAE J3101 – Requirements for Hardware-Protected Security for Ground Vehicle Applications
- SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

Security and Safety landing pages from Xilinx:

www.xilinx.com/security
www.xilinx.com/safety

Contact Information

Missing Link Electronics GmbH
Neu-Ulm, Germany
Phone DE: +49 (731) 141149-0

Missing Link Electronics
Web: <http://www.MLEcorp.com/security>
Email: sales-web@mlcorp.com

