力旺電子Briefing

ememory

IPR
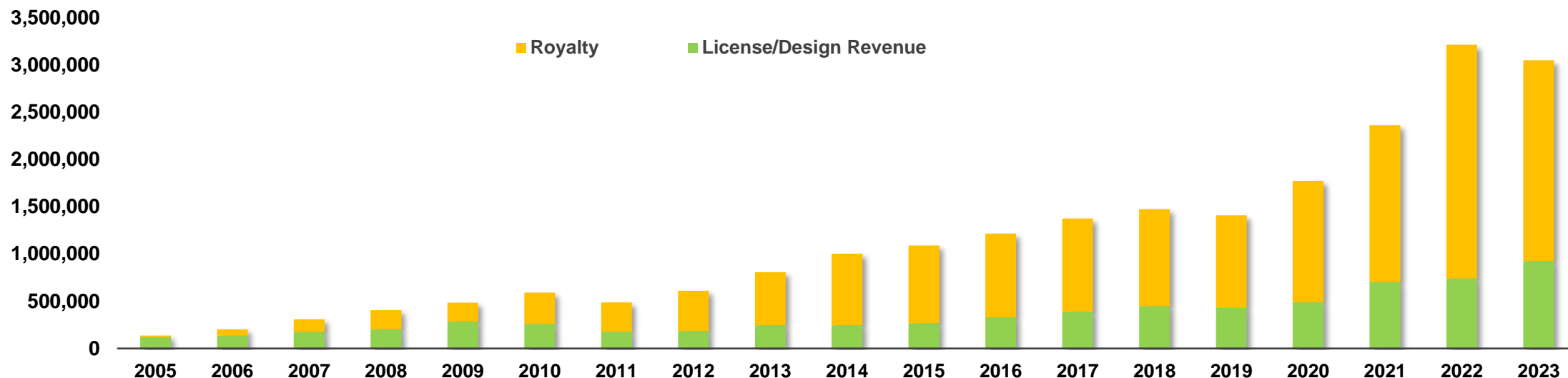# Notice ■

- eMemory is the global leader of embedded non-volatile memory IP

Revenue Trend
(Unit: NT$ 1,000)

■ Royalty   ■ License/Design Revenue

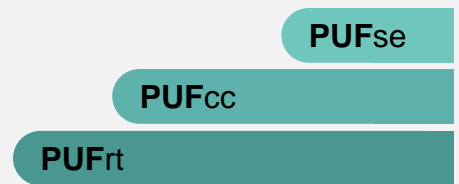|		
Founded	**1240+**	**Best IP Partner**
In 2000	**Patents Issued**	**With TSMC**
Based in Hsinchu, Taiwan. IPO in 2011. Over 62M wafers shipped.	200 pending patents. 357 employees with 68% R&D personnel.	TSMC Best IP Partner Award since 2010.

With access to eMemory's widely verified IP process platform, PUFsecurity is uniquely positioned to provide **OTP and PUF-based** Security IP Solutions with **extensive availability** across various foundries and process nodes.

PUFsecurity
PUF-based Security IP Design & Service

| | PUFse |
| PUFcc |
| PUFrt |

ememory
Technology Provider + IP Design & Service

NeoPUF (PUF)

NeoFuse (OTP)

NeoEE (MTP)

NeoFlash

NeoMTP (MTP)

NeoBit (OTP)

| 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
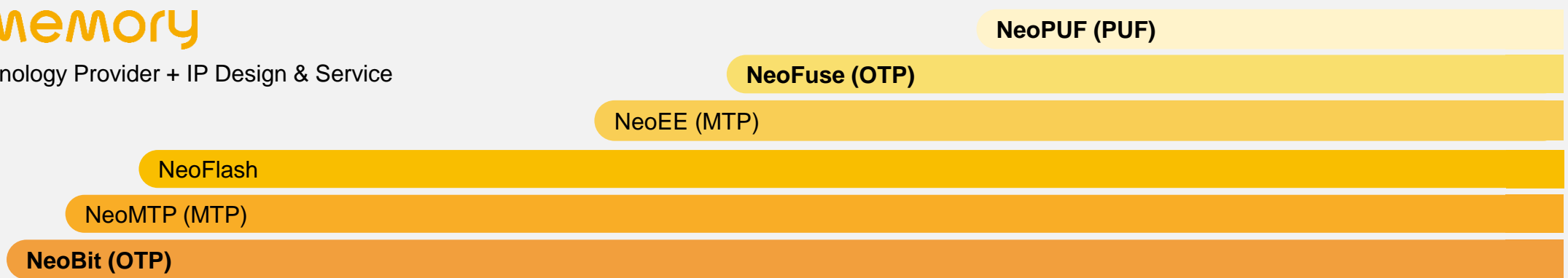
Registered IPs at TSMC

Registered IP > 750
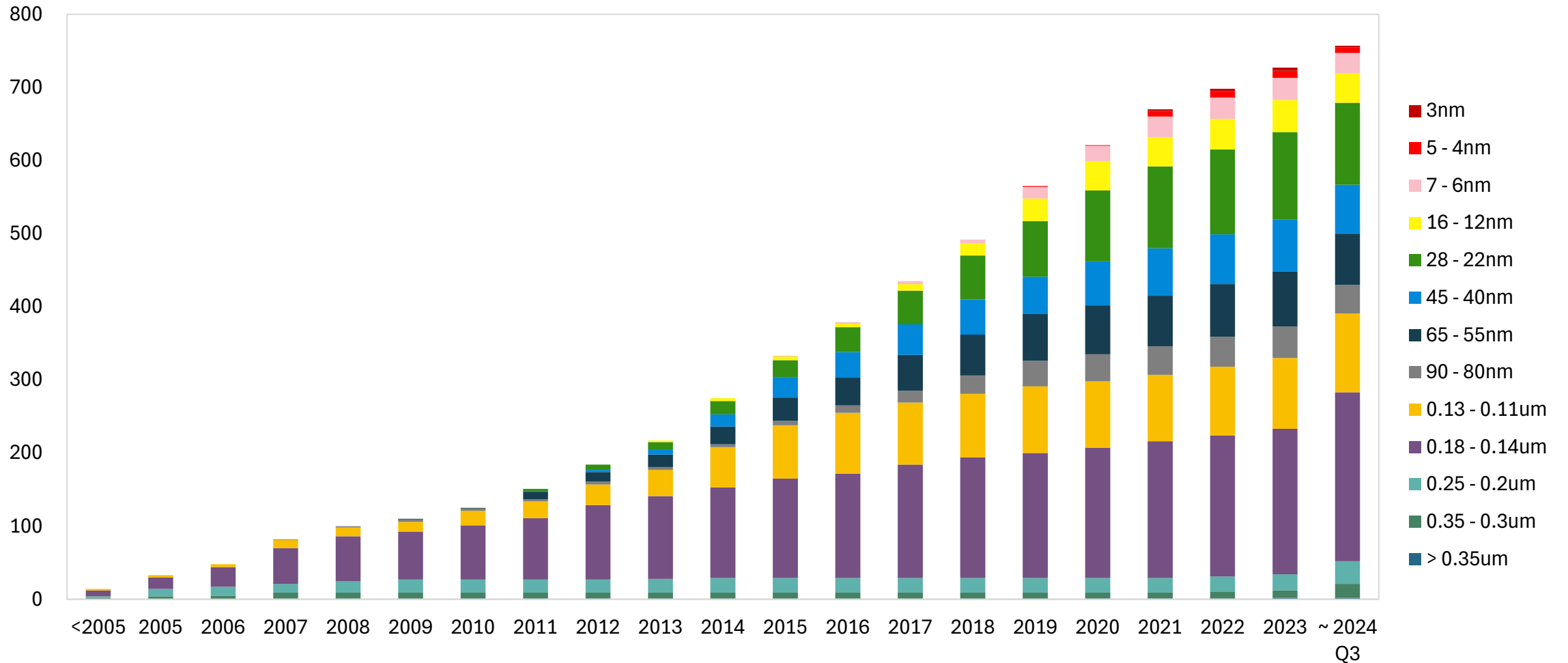
New Tape Out Contribution > 2300

Wafer Contribution at TSMC

8" Wafer Contribution > 25M

Revenue and Tape-out by Technology

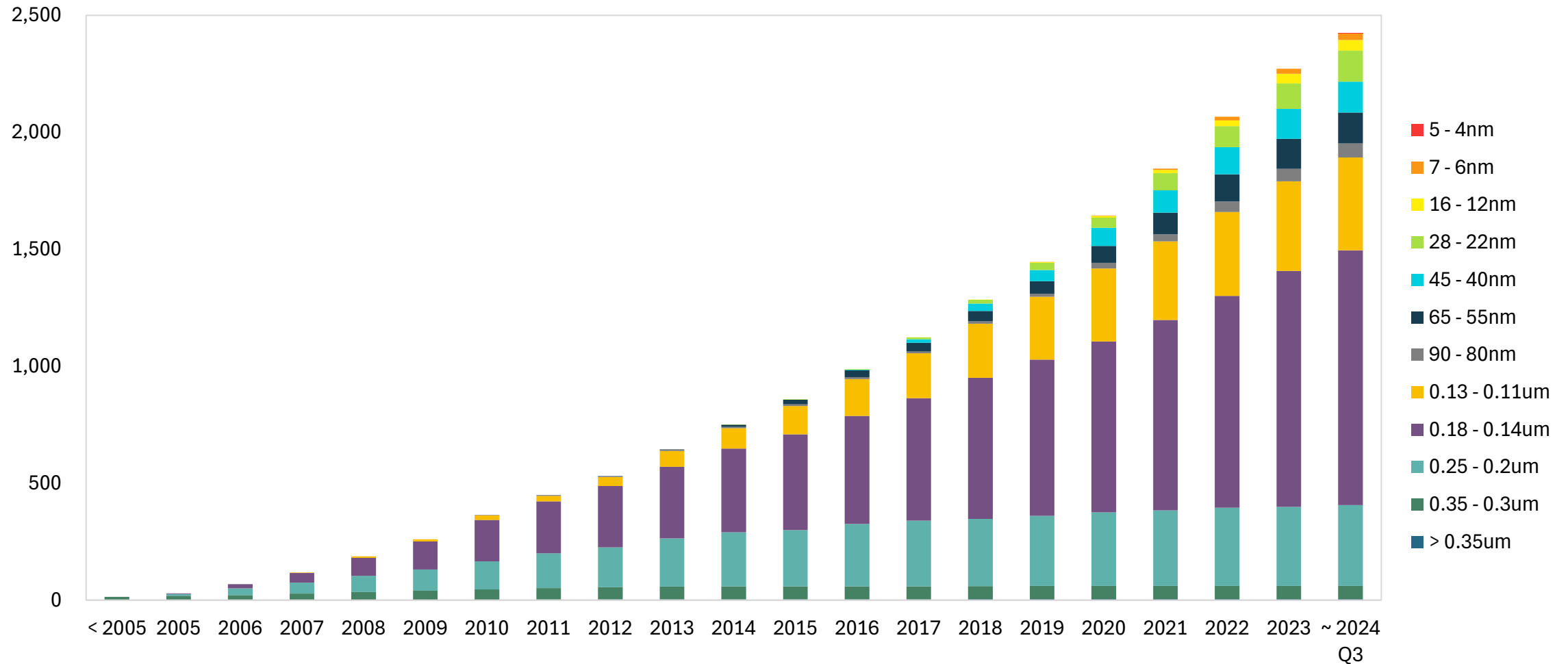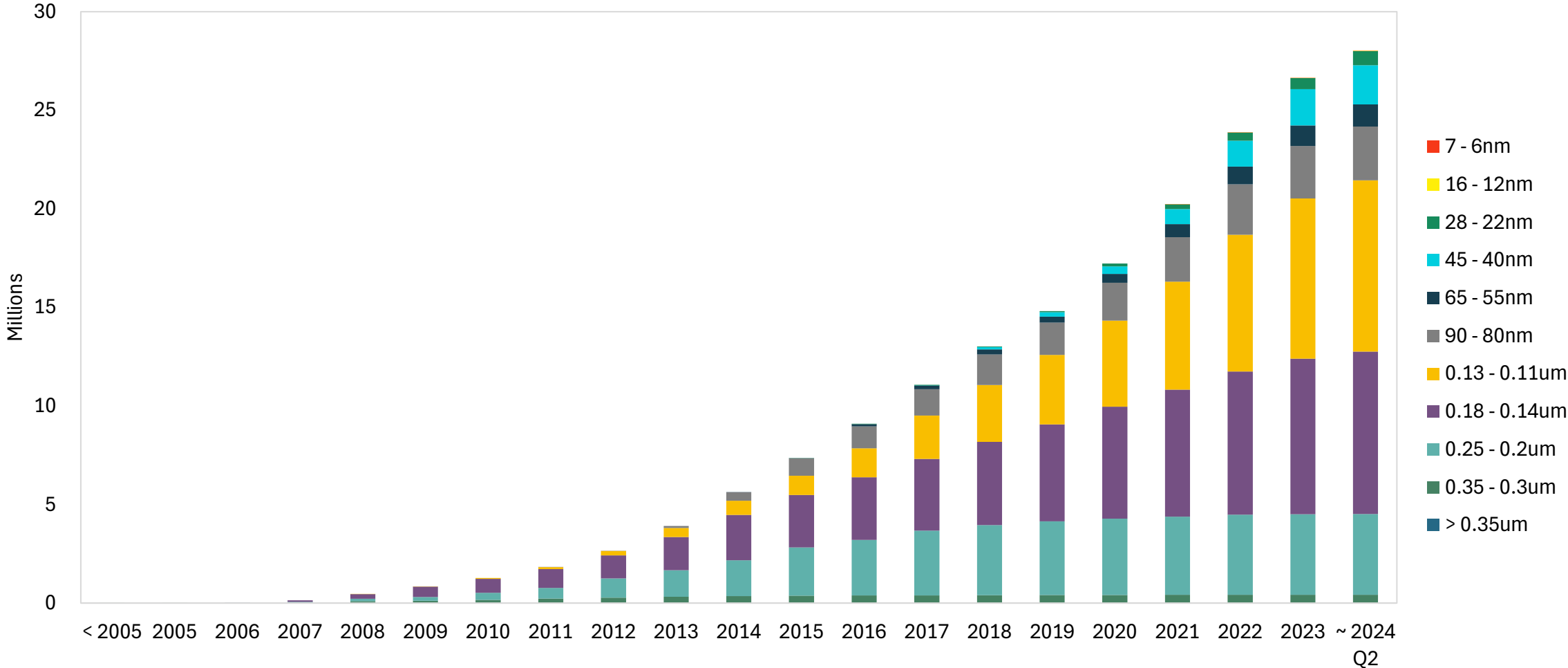| Year	NTO		Revenue (USD)		
	NeoBit	**NeoFuse**	**NeoBit**	**NeoFuse**	**PUF-based**
2002	3				
2003	29				
2004	40				
2005	68		$ 4,217,380		
2006	133		$ 6,202,270		
2007	220		$ 9,402,479		
2008	253		$ 12,896,211		
2009	268		$ 11,695,587		
2010	284		$ 15,873,331		
2011	254		$ 15,399,098		
2012	270		$ 19,620,768		
2013	363	1	$ 25,436,669	$ 382,084	
2014	371	3	$ 31,831,985	$ 328,787	
2015	311	11	$ 30,943,426	$ 1,080,373	
2016	270	28	$ 30,247,340	$ 3,636,142	
2017	257	61	$ 34,619,653	$ 5,238,351	
2018	253	86	$ 31,834,860	$ 10,773,223	$ 85,000
2019	226	109	$ 27,602,332	$ 14,466,279	$ 195,000
2020	248	182	$ 30,378,346	$ 26,437,660	$ 434,998
2021	252	259	$ 32,367,560	$ 44,011,223	$ 1,160,702
2022	264	231	$ 35,327,060	$ 63,762,480	$ 4,207,209
2023	226	241	$ 23,251,721	$ 64,276,058	$ 4,375,409
Total	**4,863**	**1,212**	**$ 429,148,077**	**$ 234,392,660**	**$ 10,458,318**

*NTO stands for **New Tape-Out**   * Revenue includes both **licensing** and **royalty**

PUF-based Security Solutions

- Based on OTP Technologies, many different security functions IPs have evolved
- Regulations, such as TPM 2.0, now require Hardware Root of Trust
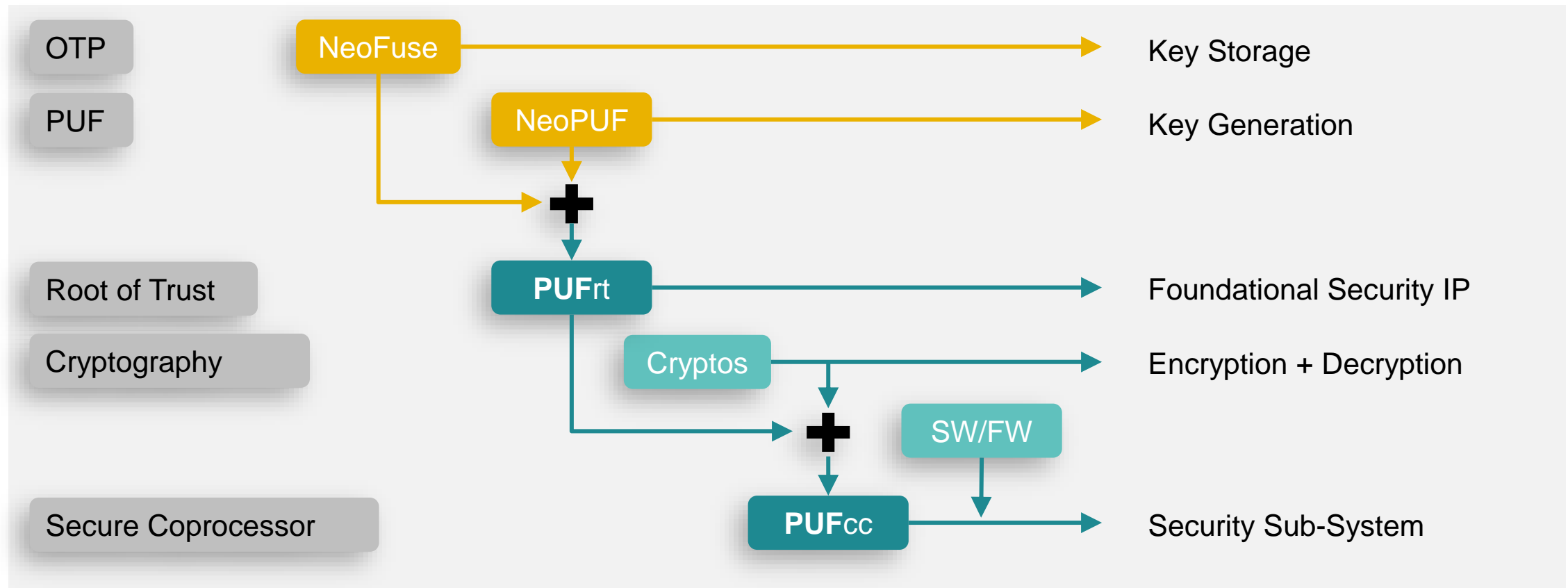
Standards Drive Hardware-Based Security .

Driving an open standard for silicon root of trust

Using asymmetric public/private key encryption technology and device ID to achieve fast and secure access to the network

PUFrt

Data Center

PUFcc

IoT

Security Business Development .

■ As eMemory is an established IP company, there are different **platforms** that we can leverage for sales in security IPs and sub-systems

Foundry Platforms
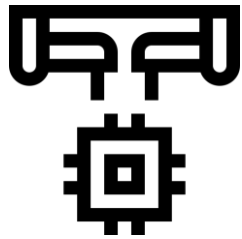
TSMC, Intel, UMC, GF, etc.

- Licensed our security technology to major foundries
- Co-promotional activities

CPU Partners
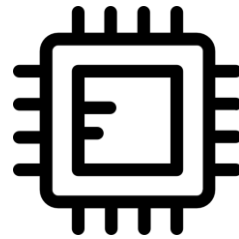
Arm, RISC-V, Cadence, etc.

- SoC customers looking for both CPU and security subsystems

CSP
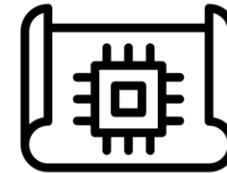
More to come

- Work with CSP and system companies for embedded security on a chip level

Market **Application** ▪

▪ Customers with many different applications will begin to adopt **PUF-based Security Solutions**

CPU	AI	SSD
DPU	DTV/STB	Wi-Fi
FPGA	ISP	And More.

eMemory

Next Computing: **Confidential Computing**

CPU Cores — Core 1 (Tag 1), Core 2 (Tag 2), Core 3 (Tag 3), ... Core N (Tag N)

PUFcc Generated Tags

Virtual Memory — Tag 1 / Realm 1, Tag 2 / Realm 2, Tag 3 / Realm 3, ... Tag N / Realm N

Virtual Boundaries
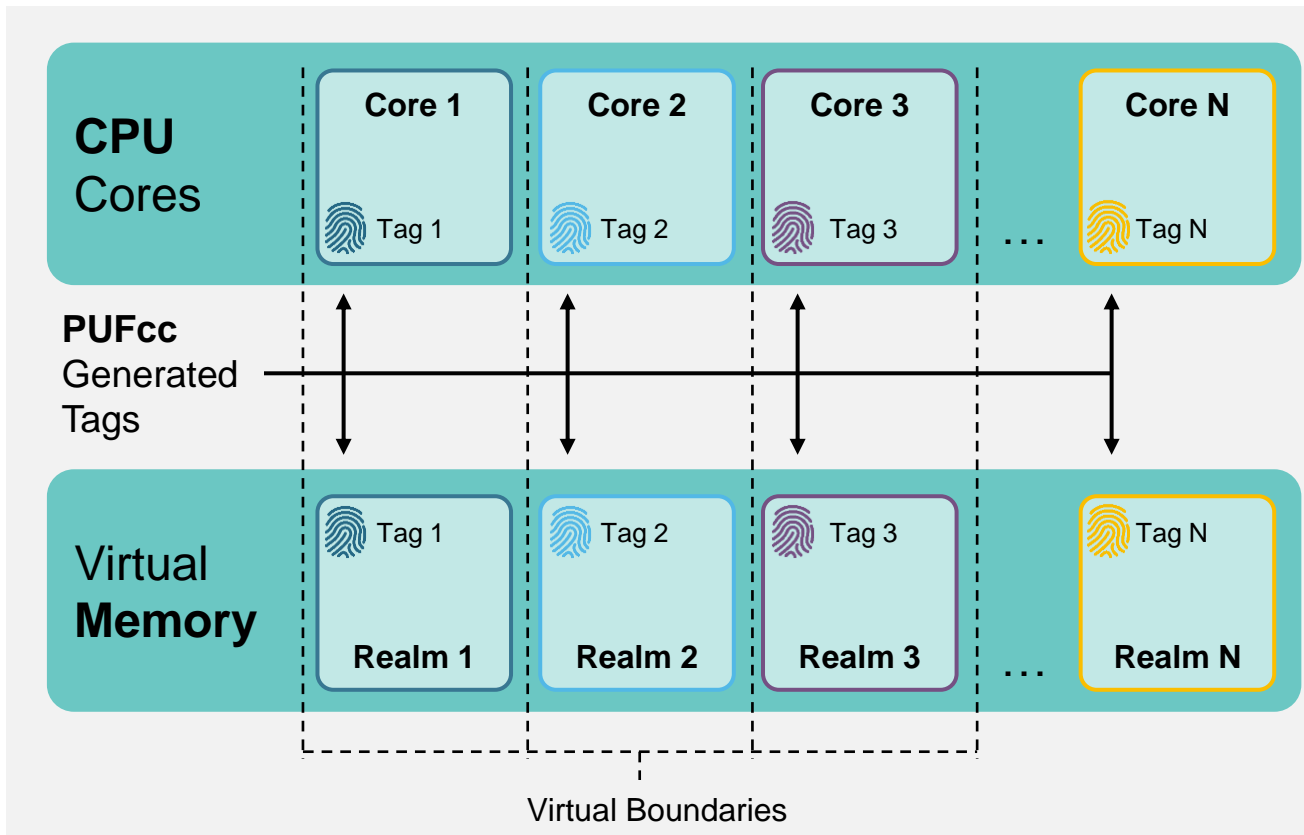
- **Protect data** in the Virtual Memory of Multi-Core CPUs

- CPU Cores and Virtual Memory have unique corresponding **tag numbers**

- Tag numbers are internally **randomly generated** by **PUFcc** (Crypto Coprocessor IP)

One Time Programable (OTP) memory is a SoC-wide resource

- RSS supports OTP as field-programmable to store confidential code and data

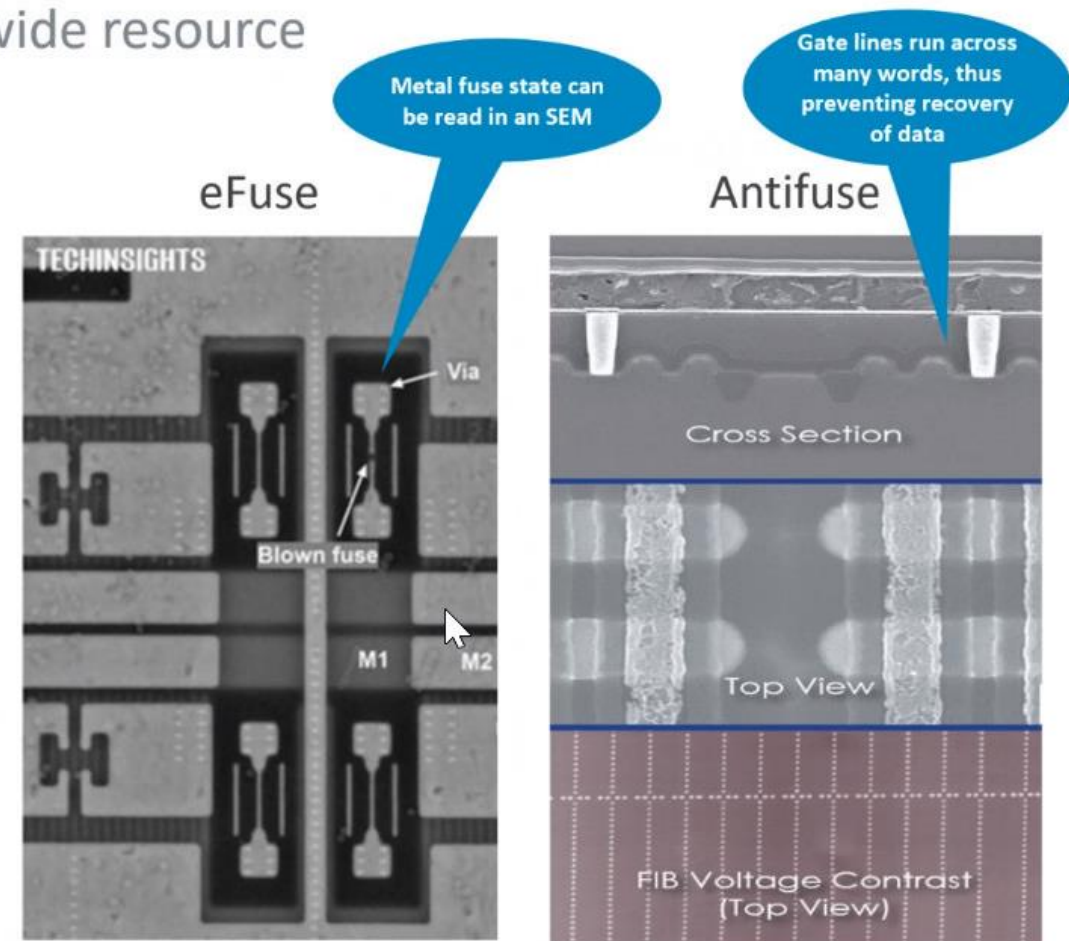- eFuse:
  - Area efficient for smaller arrays
  - Typically not field programmable
  - Can be easily read by delayering SoC (a few $k cost)
    - The secure channel key can be compromised
    - The device can then be cloned

- Antifuse OTP:
  - Cannot be read using a scanning electron microscope
  - Dense bit cells, efficient for large arrays
    - Macro periphery is large versus eFuse
  - Integrated charge pump enables field programming
  - PUF can be included for a small additional area
    - ~0.04mm2 on 7nm for 128x32 bit PUF

eFuse

Antifuse

Metal fuse state can be read in an SEM

Gate lines run across many words, thus preventing recovery of data

https://semiengineering.com/the-benefits-of-antifuse-otp/

arm

Example: **eMemory** Helps Memory .

- eMemory's security IP and OTP/MTP IP 1) ensure data security and 2) improve yield for SRAM and DRAM.

SRAM

DRAM
(e.g. DDR5)

CXL Memory

Storage (SSD/HDD)

Highly required in AI/HPC

AI Accelerator

Embedded memory repair function to improve yield

DIMM

Standalone memory repair function to improve yield

CXL Memory Controller

PUF-based solutions for secure data transmission

SSD Controller

PUF-based solutions for secure data storage
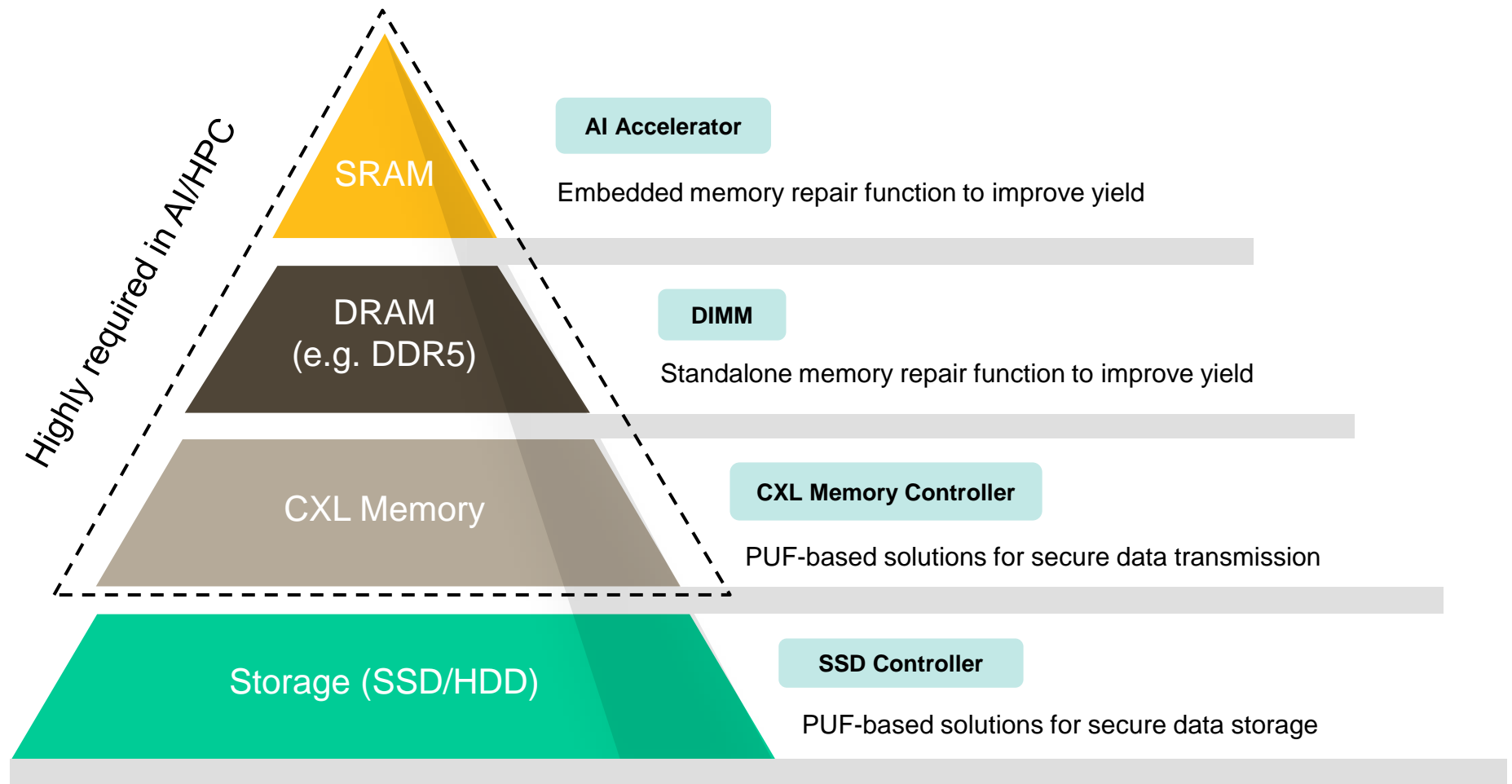
eMemory for **AI Servers** and **Edge Devices**
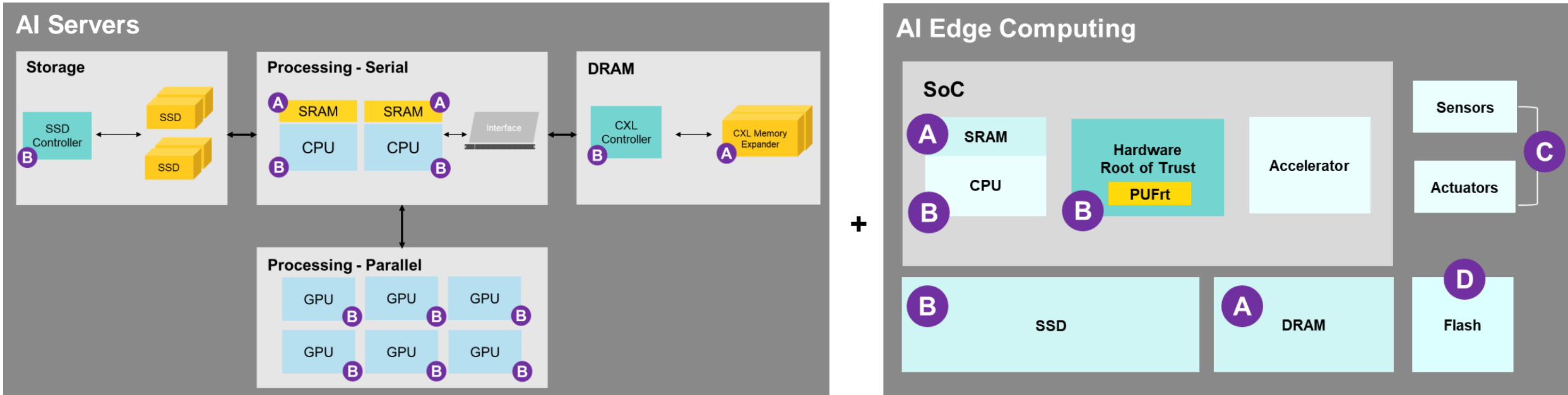
A **Memory Repair**

B **Root of Trust** provides:
1. Key storage/generation
2. Cryptographic processing to protect AI models, input data and output results
3. Confidential Computing

C **OTP** needed for trimming analog circuits in Sensors and Actuators
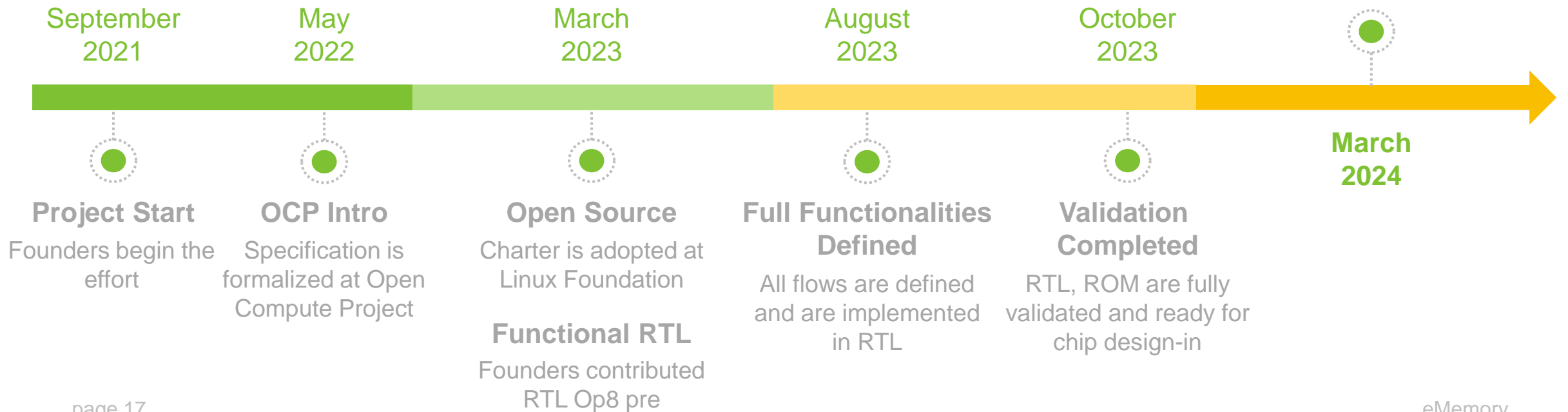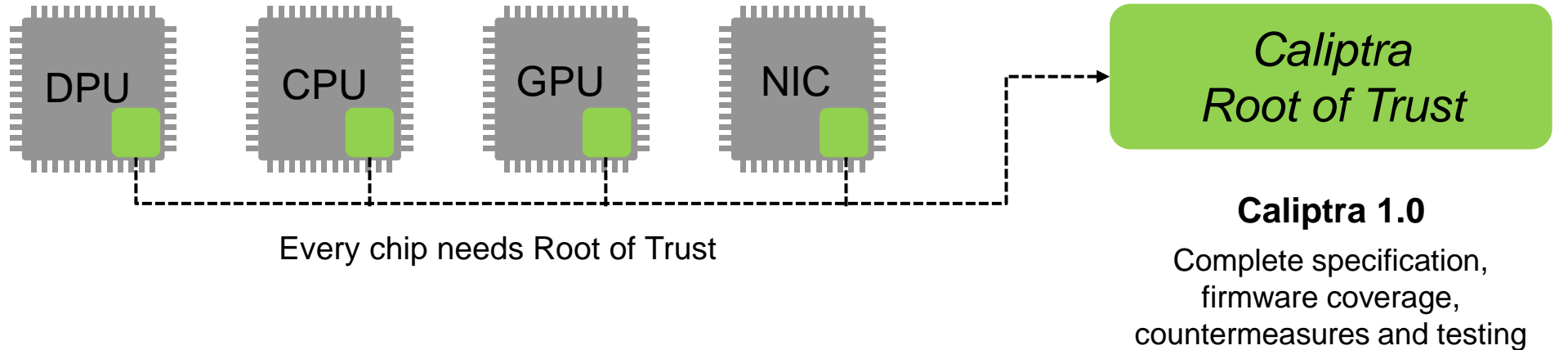
D **NeoFlash** to replace conventional eFlash for a much lower cost

Why is **Caliptra** so Important?

Datacenter Chips

DPU   CPU   GPU   NIC

Every chip needs Root of Trust

Caliptra Root of Trust

Caliptra 1.0

Complete specification, firmware coverage, countermeasures and testing

September 2021	May 2022	March 2023	August 2023	October 2023	

March 2024

Project Start

Founders begin the effort

OCP Intro

Specification is formalized at Open Compute Project

Open Source

Charter is adopted at Linux Foundation

Functional RTL

Founders contributed RTL Op8 pre

Full Functionalities Defined

All flows are defined and are implemented in RTL

Validation Completed

RTL, ROM are fully validated and ready for chip design-in

eMemory

What is the Important Role of **eMemory** in **Caliptra?**

- eMemory's root of trust IP is ready to meet Caliptra's requirements.

Datacenters

Caliptra Silicon RoT

ememory IP Portfolio

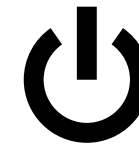| OTP	PUF	TRNG	Crypto Engine
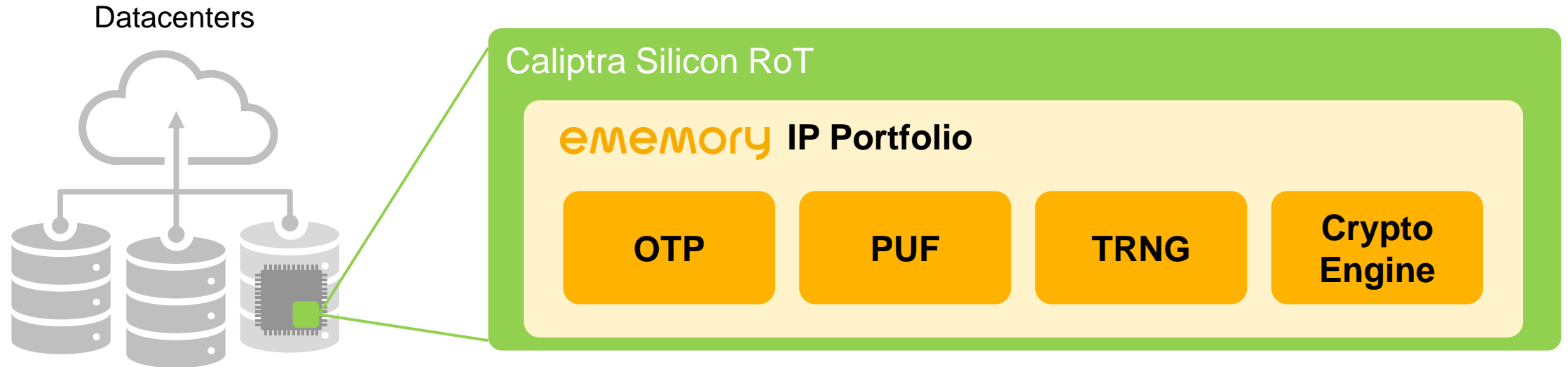
Unique Chip Identity

Chip Fingerprint

Secure Attestation

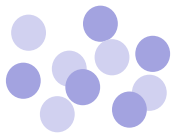Device Certificate

Secure Boot

Boot into Trusted Operating System

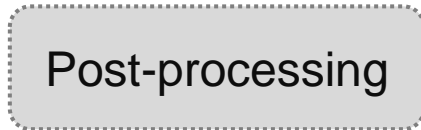# PUFtrng: 100 Times Faster than Conventional TRNG

- PUF-based conditioning algorithm provides high-throughput and high entropy quality

Similar to…

Conventional TRNG

Dynamic Entropy
(ROSC)

Post-processing

Conventional TRNG

Slower

Classic Cars

PUFtrng

Static Entropy
PUF
(Chip Fingerprint)

+

Entropy Refine Engine

PUFtrng

100x Faster

New Energy Cars

Why is **High-Density SRAM** needed in **AI?**

- To increase the speed of AI accelerators, **high-density SRAM** is needed for use in:

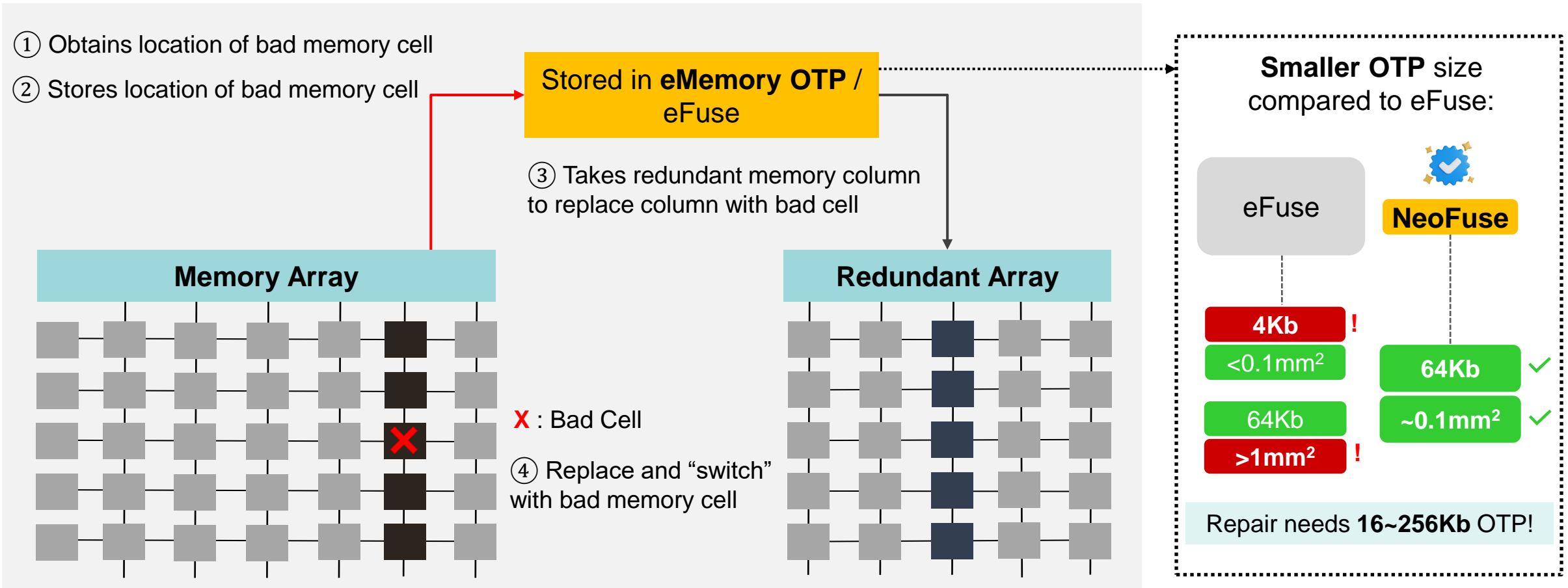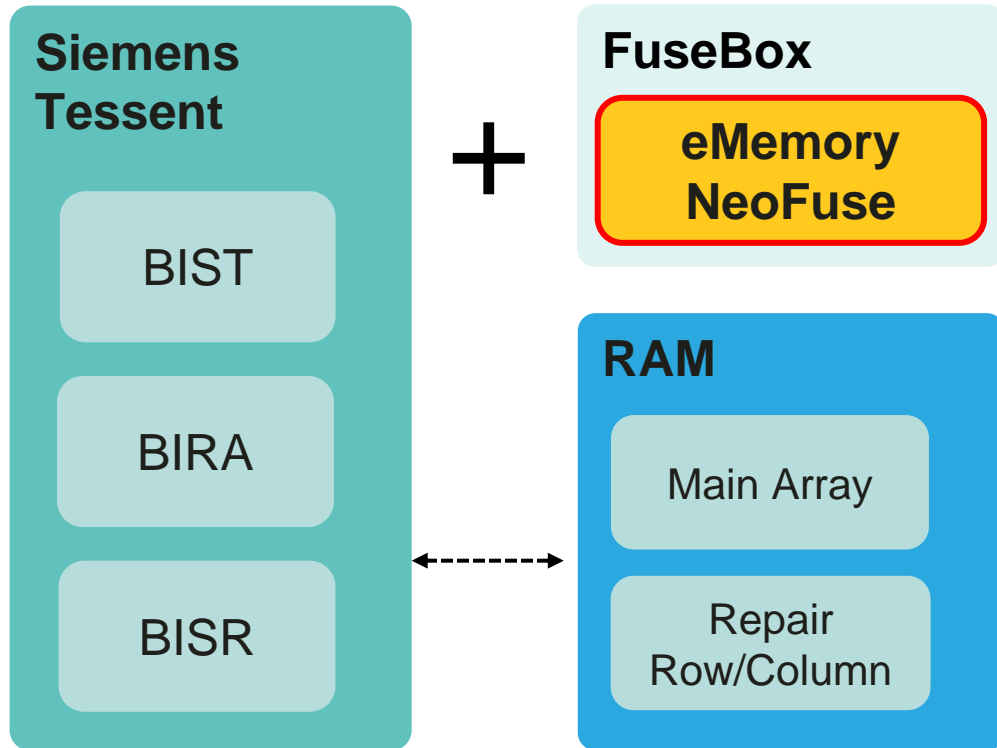| Buffer Memory	AI Model Training	Computing in Memory (CIM) for Inference
• High-density SRAM helps improve data transfer speed and reduce energy costs by acting as a fast **intermediate storage** between different processing stages.	• High-density SRAM helps **store** vast amounts of data for AI accelerators to access quickly to speed up training.	• High-density SRAM enables **in-memory computation** by storing large datasets and performing computations on them without transferring data to separate processors.

eMemory enables **High-Yielding** SRAM

- SRAM yield decreases as technology is scaled due to smaller dimensions. To **increase yield**, **eMemory's OTP** is required.

① Obtains location of bad memory cell

② Stores location of bad memory cell

Stored in eMemory OTP / eFuse

③ Takes redundant memory column to replace column with bad cell

Memory Array

Redundant Array

X : Bad Cell

④ Replace and "switch" with bad memory cell

Smaller OTP size compared to eFuse:

eFuse

NeoFuse

4Kb	!
<0.1mm^2	
64Kb	
>1mm^2	!

| 64Kb | ✓ |
| ~0.1mm^2 | ✓ |

Repair needs **16~256Kb** OTP!

Partnering for Success: **eMemory and Siemens** ■

Siemens Tessent

- BIST
- BIRA
- BISR

+

FuseBox

> **eMemory NeoFuse**

RAM

- Main Array
- Repair Row/Column

BIST = Built-in Self Test
BIRA = Built-In Redundancy Analysis
BISR = Memory Built-in Self Repair

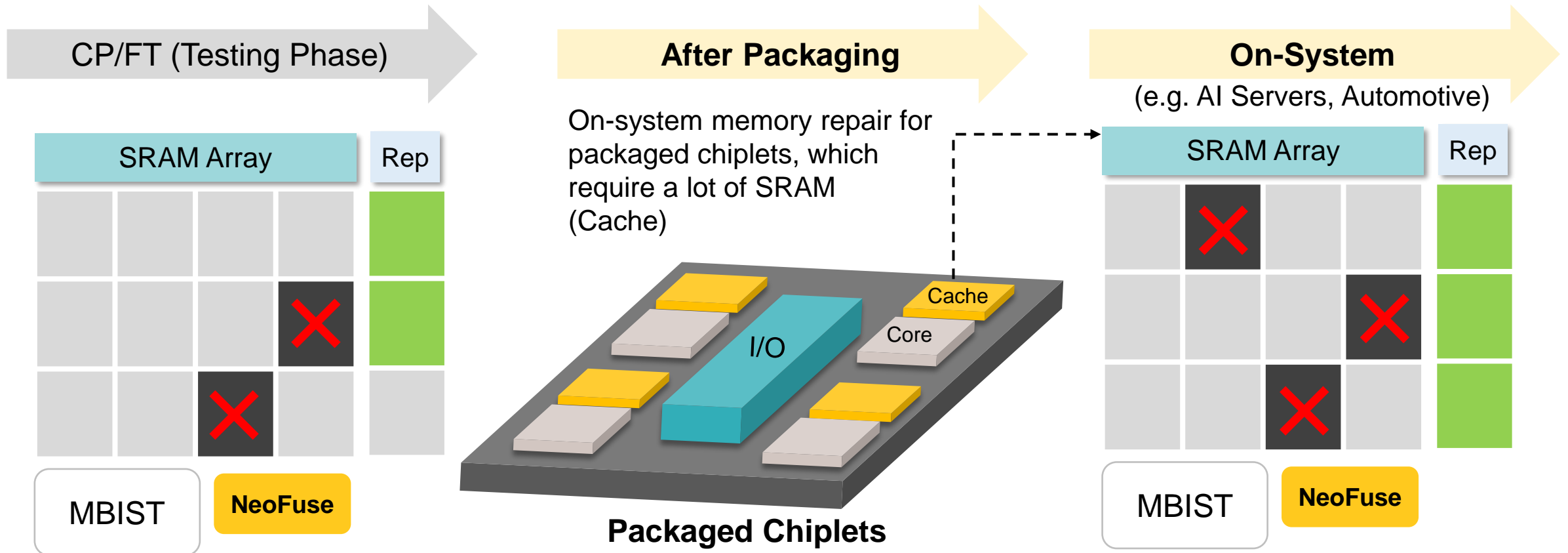eMemory provides OTP with interface for Siemens MBIST:

- **Tessent** provides memory BISR functions with BIST and BIRA

- **NeoFuse OTP** provides defect-free OTP using BIRA, BISR and adapter to Tessent

- **New MBISR**: Tessent MBISR + NeoFuse, scanning defective SRAM by word/column and logging to the OTP

1. **Compact**
2. **Flexible**
3. **Robust**

On-System Repair for AI Accelerators

■ Memory Built-in Self-Test (MBIST) offers **on-system repair** capabilities, which are essential for high-speed high-reliability applications and chiplet **architecture** or **after system** packaging.
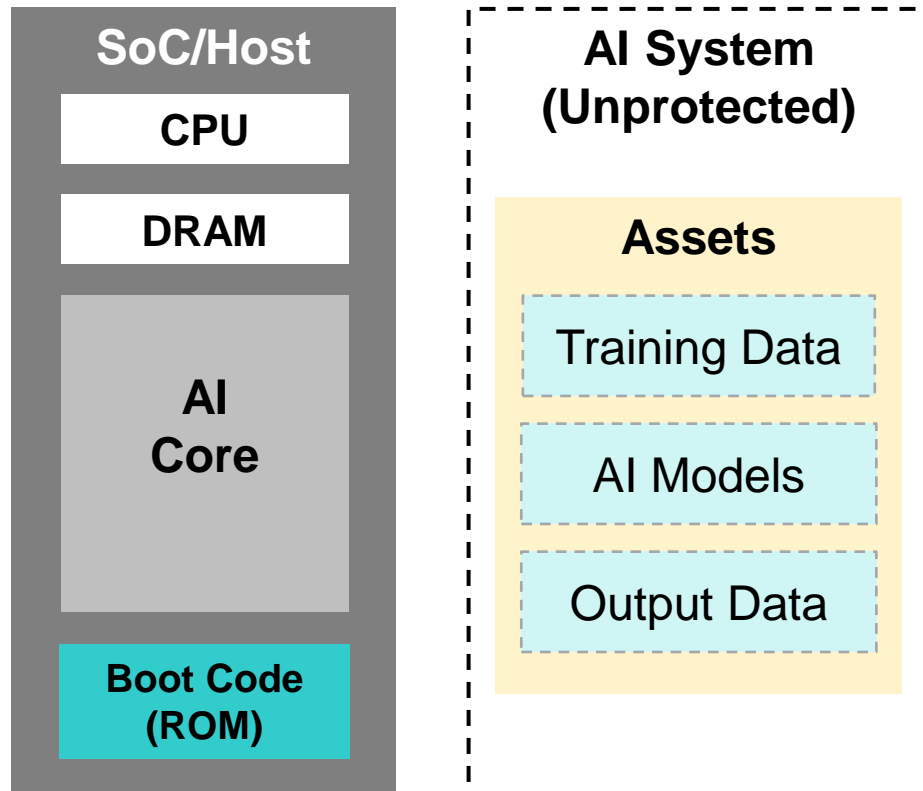
CP/FT (Testing Phase)

After Packaging

On-System
(e.g. AI Servers, Automotive)

On-system memory repair for packaged chiplets, which require a lot of SRAM (Cache)

SRAM Array | Rep

MBIST | NeoFuse

Packaged Chiplets

Cache
Core
I/O

SRAM Array | Rep

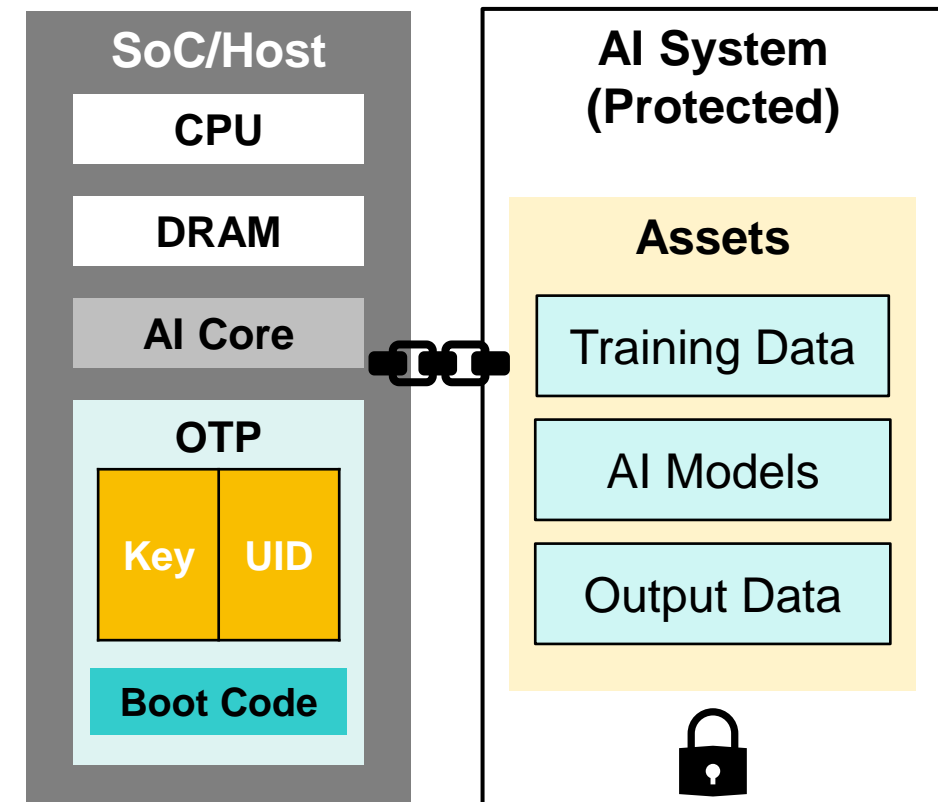MBIST | NeoFuse

Made possible with MBIST

eMemory enables HPC in **AI Applications**

- **eMemory's OTPs** can also **store boot codes**, **root key** and **unique ID** for the root of trust in **AI systems**.

Without eMemory OTP

SoC/Host
CPU
DRAM
AI Core
Boot Code (ROM)

AI System (Unprotected)

Assets
- Training Data
- AI Models
- Output Data

With eMemory OTP

SoC/Host
CPU
DRAM
AI Core
OTP — Key	UID
Boot Code

AI System (Protected)

Assets
- Training Data
- AI Models
- Output Data

Thank You for your time .

For more information, please visit:
eMemory Website: https://www.ememory.com.tw/
PUFsecurity Website: https://www.pufsecurity.com/

ememory