MACRONIX

Challenges to Failure Analysis for Secure Flash Memory Chip

John Grogan, Warren Chen, Ron Chang, Roger Chen

AEC Reliability Workshop 2026 in Detroit, April 1, 2026

Outline

- Flash Memory Security, Trends and Methods
- How Flash memory is secured—the building blocks
- Cooperation Needed for FA
- Test Mode Essential tool for FA
- Physical Barriers Limiting FA
- Non-destructive Analysis Are Available for FA
- FA Comparison with traditional Flash
- Enhancing FA Capabilities for Secure Flash
- Summary

Why Flash Memory Needs Security

Flash memory is essential in security embedded systems because flash memory chip stores firmware, device unique ID, and keys of electronics system.

Store and forward use cases are growing across all industries

Availability of large scale data management providers

(e.g. Amazon AWS, Microsoft Azure, Google Cloud)

Affordability of high performance compute and sensor technology

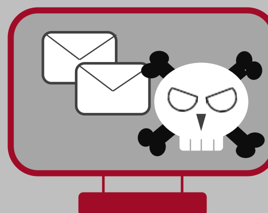
Communication networks driving availability of Internet connectivity (e.g. 5G)

Need to secure data as a national security requirement

Increase in remote content availability & need to protect against unauthorized use

Increasing requirements to meet privacy regulations

(e.g. GDPR)



Thwart Internet Attacks

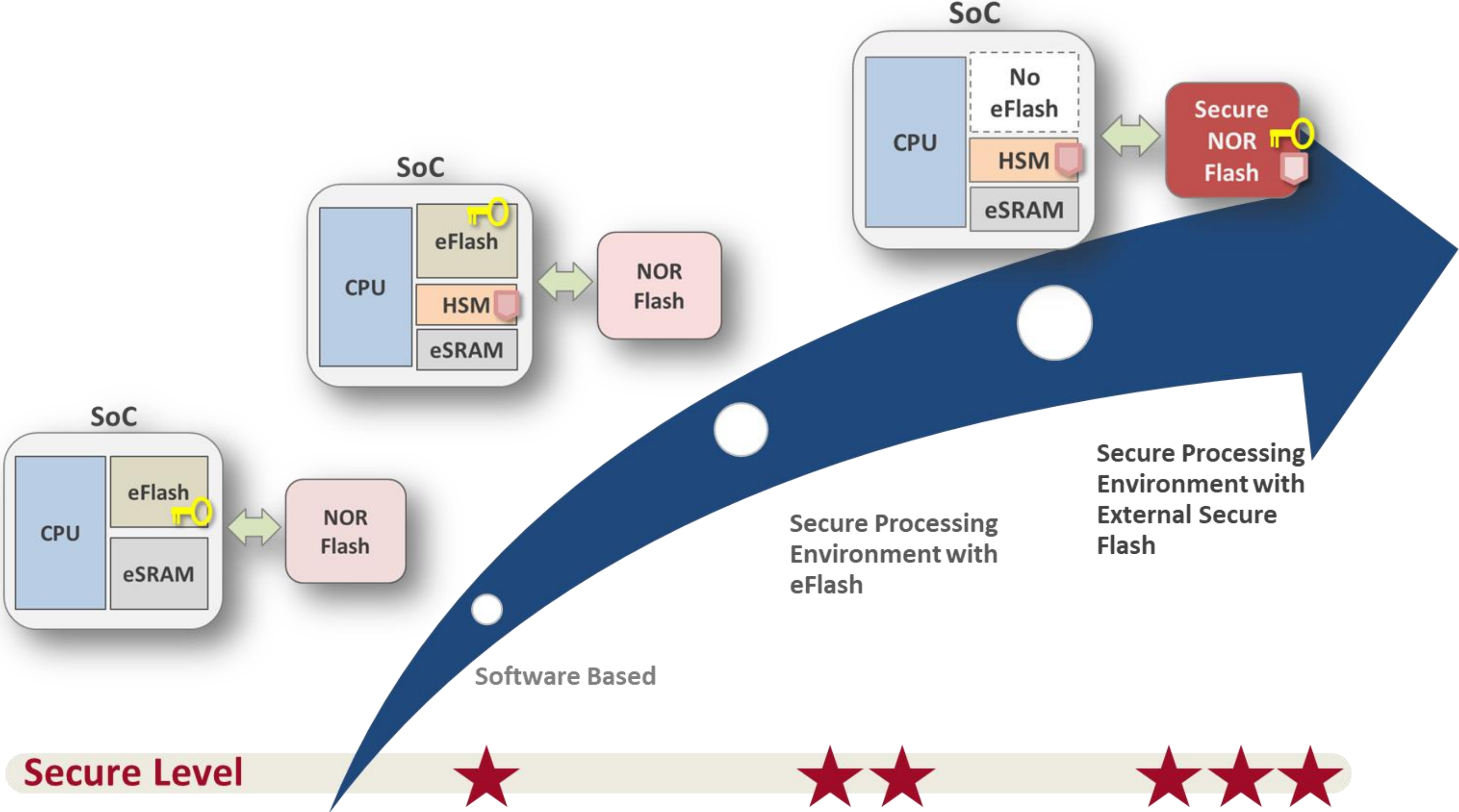
e.g. botnets carrying out Distributed Denial of Service programs

Growth of buildings' biometric keys for authorized entry & monitoring for unauthorized entry

The Trend from eFlash to Secure Flash

Traditional embedded flash densities are increasingly becoming inadequate to store all this data

And, embedded flash is more difficult for more advanced logic process technologies (below 28nm)

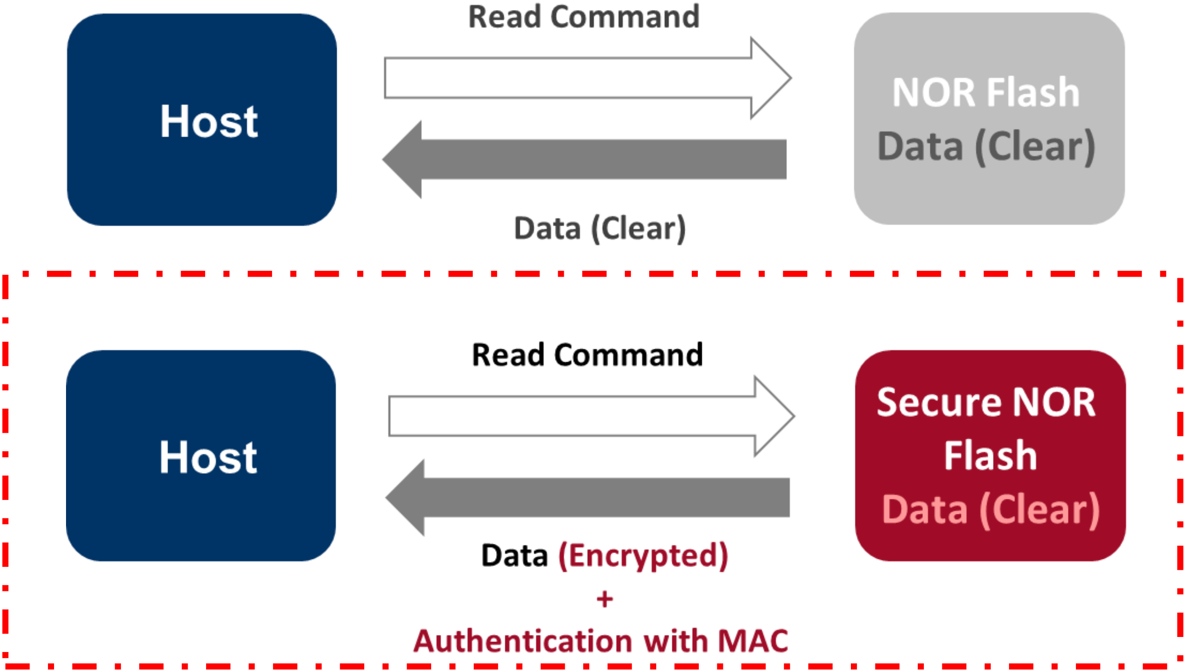


Importance of Secure Flash Memory Chip to Cyber Security

Flash memory stores essential firmware, device unique ID, and keys of electronic systems

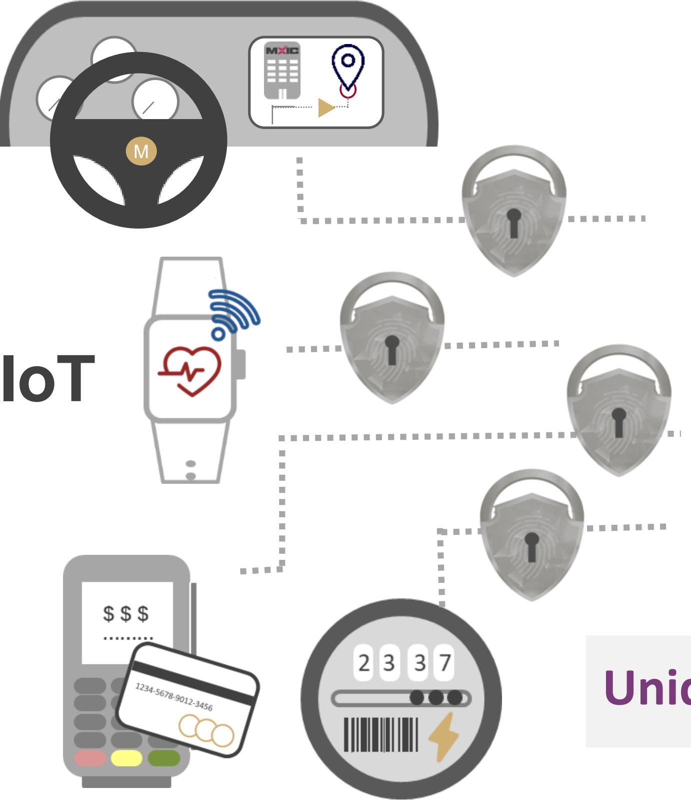
If attacked by side-channel analysis or illegal firmware update the data is compromised

Solution is to build security onto serial NOR flash by providing a secure ID, authentication, and an encrypted link protecting valuable data



Key Methods of securing Flash Memory

A highly secure data-storage solution ensures data confidentiality, integrity, and availability, offering high levels of security with features like:



- ECC & CRC
- Non-volatile Monotonic Counter
- Hardware Crypto Engines
- Authentication
- Data Encryption
- Key Storage & Measurement
- True Random Number Generator (TRNG)
- Unique ID & Extra Serial Number Storage
- Non-volatile PUF (Immutable Unique ID)
- Anti-Tamper

How Flash memory is secured—the building blocks

1. Top-layer fill-in during IC manufacturing and anti-tamper designs
2. Eliminating backdoor—fusing test mode before shipment
3. Customer provisioning (infrastructure)
   initialize secure bootloaders
   establish secure connectivity credentials
   generate root key(s)—
4. Lock down applicable DataZones access with root key(s)

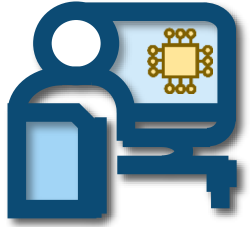
Support Security Function

32Mb	2Mb	15
	2Mb	14
	2Mb	13
	2Mb	12
	2Mb	11
	2Mb	10
	2Mb	9
	2Mb	8
	2Mb	7
	2Mb	6
	2Mb	5
	2Mb	4
	2Mb	3
	2Mb	2
	2Mb	1
	2Mb	0

Flash memory is secured—what about FA?

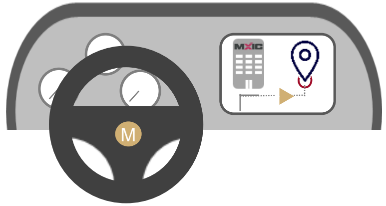
- ❖ Secured DataZones not accessible after lock down
- ❖ Customer has the root key to the locked Host/Memory system
- ❖ Supplier cannot access test modes for the detailed analysis
- ❖ Physical FA restricted due to top-layer fill in and anti-tamper designs

Cooperation Needed for FA



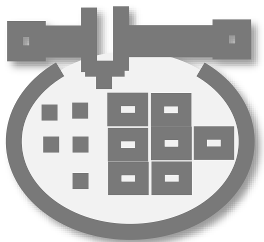
Core Chip Vendor

Provides the key acquiring function to Tier 1 System Provider



Tier 1 System Provider

Generates cryptographic script based on key acquiring function



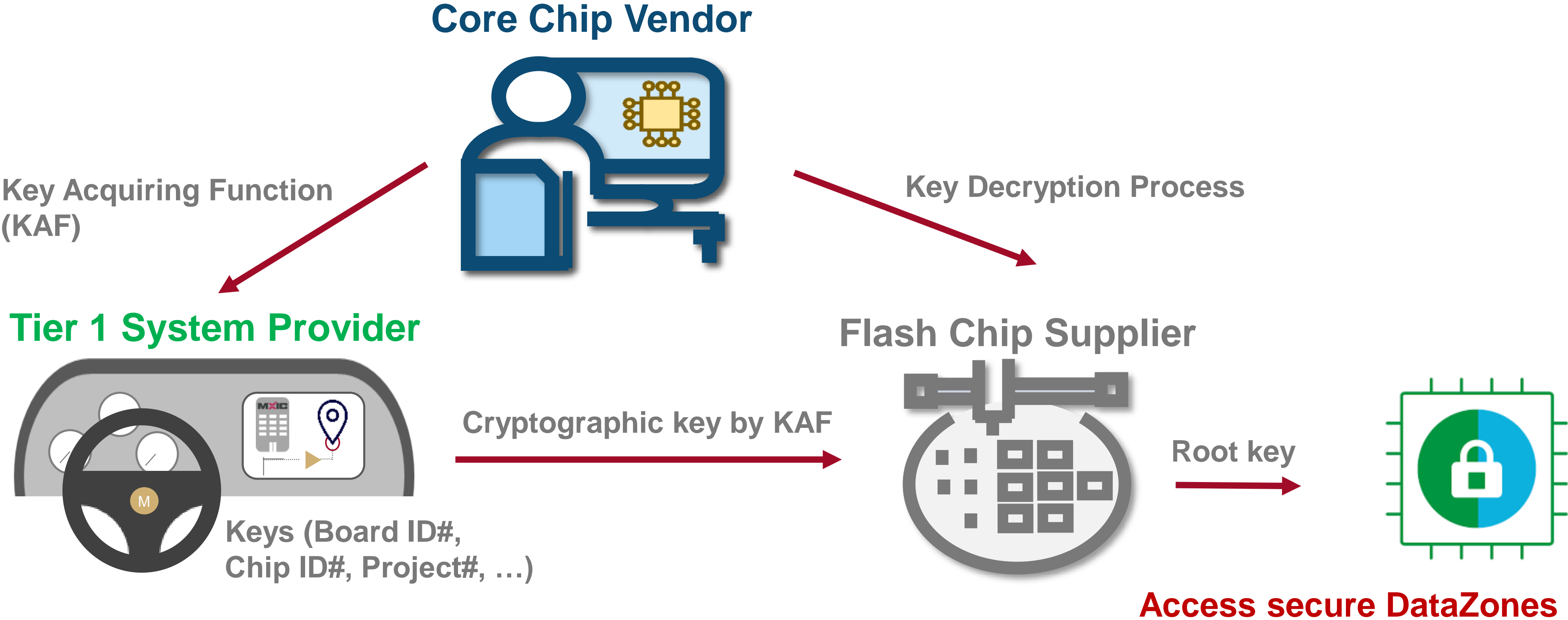
Flash Chip Supplier

Needs support from Tier 1 and Core Chip Vendor to provide decryption process

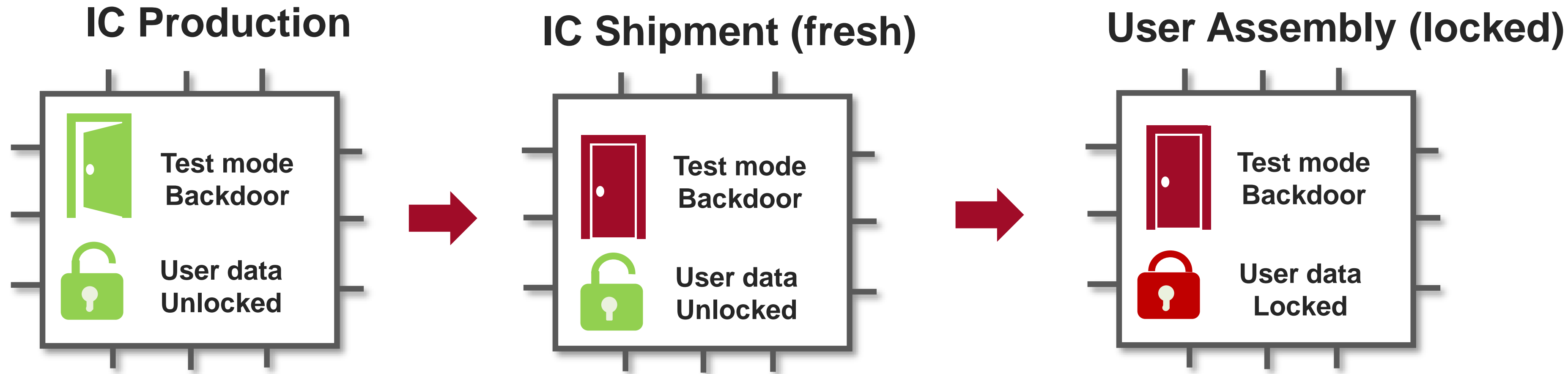
Triangle for Unlocking Secure Chips

The root key generation requires cybersecurity knowledge and cooperation across all 3 parties

The communication can be complicated with gaps of knowledge and skill



Test Mode Essential tool for FA



Supplier cannot access test modes (cf., slide 7)

Supplier test mode function is a key debug tool for reading the Vt of memory bit-cells

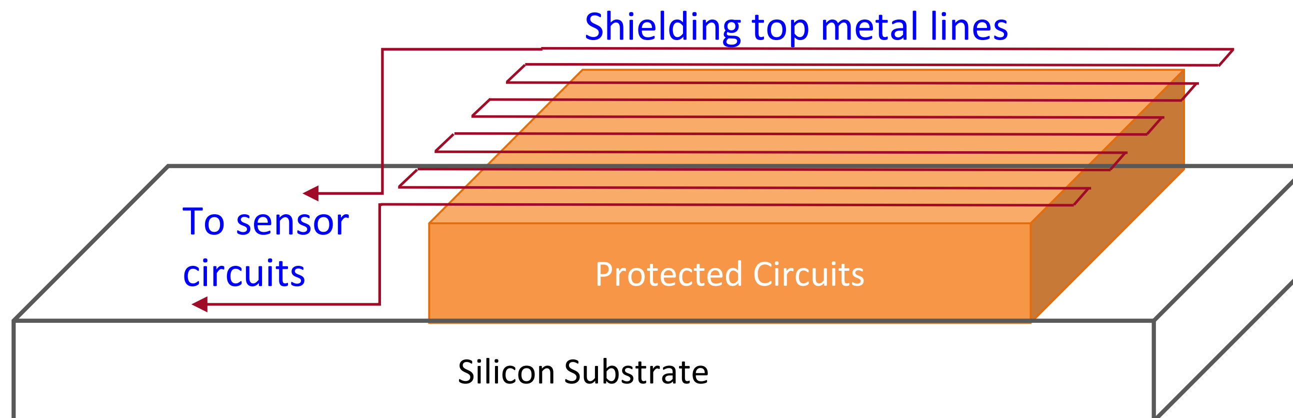
Fusion of these test modes prior to shipping limits electrical failure analysis for root cause identification

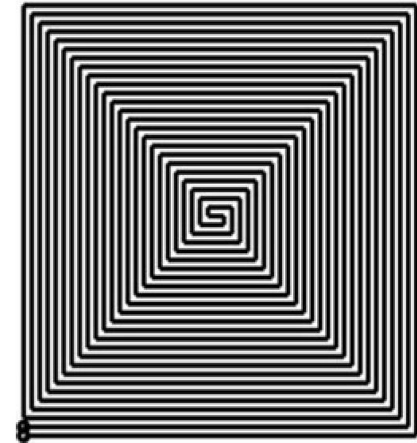
Locked User data (Datazones) is reversible using Root Key

Supplier test mode disabled is irreversible

Top Metal Layer Fill-in Limits FA

To prevent on-chip probing attacks, a fill-in structure is deposited on the top metal layer of peripheral logic circuit area (security engine, state machine, high voltage generator, etc.) of secure flash.





Source: Gao etal, "An Active Shielding Layout Design based on Smart Chip", 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)

The fill-in structure creates two complications for failure analysis of peripheral circuits

- Neither micro-probing (signal probe or bias measurement) nor circuit modification by FIB (Focused Ion Beam) are possible due to the dense top metal layer. Attempts to edit circuitry by FIB can cause malfunction of the chip
- The fill-in structure blocks the light emitted from defective MOSFET/layers during front side Infrared emission or Laser based microscopy. Hot Spot cannot be identified

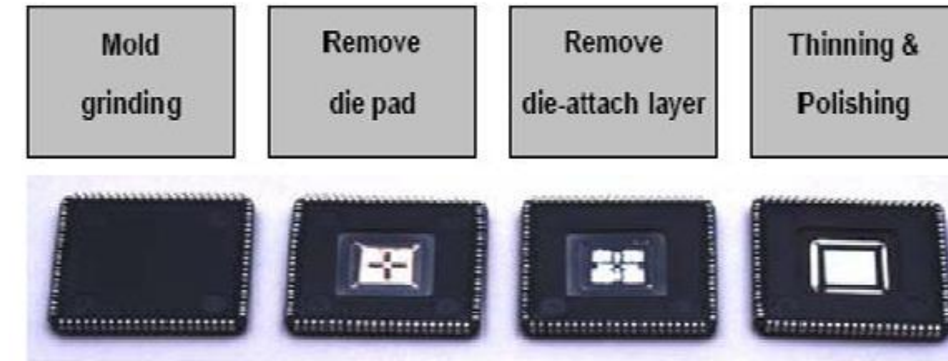
Front-side Microscopy is not possible for FA

Microscopes tools (EMMI, OBIRCH, InGaAs, and InSb) used for locating defects are blocked by the dense top metal fill-in layer covering the peripheral/secure logic area of a secure flash

Heavy reliance on Back-side emission for Failure Analysis

Requiring extra sample preparation such as:

- molded package grinding/de-capsulation
- die pad/attach removal
- backside thinning and polishing
- wire-to-wire bonding to a new package carrier (for BGA package)



Result is—increasing FA time and cost and root cause not guaranteed

Source of figure: Tao etal, Backside IR Photon Emission Microscopy (IR-PEM) Observation in Failure Analysis of the Packaged Devices, 2008, IEEE, DOI: 10.1109/ICEPT.2007.4441539

Non-destructive Analysis Are Available for FA

Non-destructive inspections are still available for checking package configuration or damage

- 2D/3D X-ray inspection for checking package internal wire-bonding interconnect
- SAT (Scanning Acoustic Tomography) for looking at package internal delamination

Non-destructive DC electrical test/analysis to detect open, shorts, excessive leakage currents, or standby/powerdown current failures is available.

- Applying DC voltage/current can identify abnormal behavior e.g., device exceeds specification limits
- Checking power supply current and time-mode waveform during power-up and at specific functions can verify if the device has abnormal leakage or malfunctions

DC analysis along with Emission Microscopy (EMMI) or Optical Beam Induced Resistance Change (OBIRCH), can pinpoint hotspots (abnormal points) for precise localization of defects before physical destructive analysis.

FA Comparison with traditional Flash

Analysis type	Failure analysis item	Standard NOR flash	Secure NOR flash
Non-destructive:	**X-ray** inspection	**Yes**	**Yes**
	Acoustic tomography CSAM inspection	**Yes**	**Yes**
	DC electrical test/measurement (pin open/short/leak, standby current, deep power-down current)	**Yes**	**Yes**
	Traceability: Die ID (lot#, wafer#, die location x/y) readout	**Yes**	**Yes**
	Non security functions: Read device ID, HW and SW Reset, Write enable	**Yes**	**Yes**
	NOR flash operational functions: Program / Erase / Read	**Yes**	**No, without root key**
	Test mode function: Vth (threshold voltage) read or distribution	**Yes**	**No**
Destructive	**Front side** Emission Microscopy	**Yes**	**No**
	Back side Emission Microscopy	**Yes**	**Yes**
	FIB circuit edition or probing pad on secure circuits with shielding	**Yes**	**No**

…without Test Mode access only symptoms can be highlighted during FA for Secure Flash

Enhancing FA Capabilities for Secure Flash

Initialize (reset) data zone protection —partial

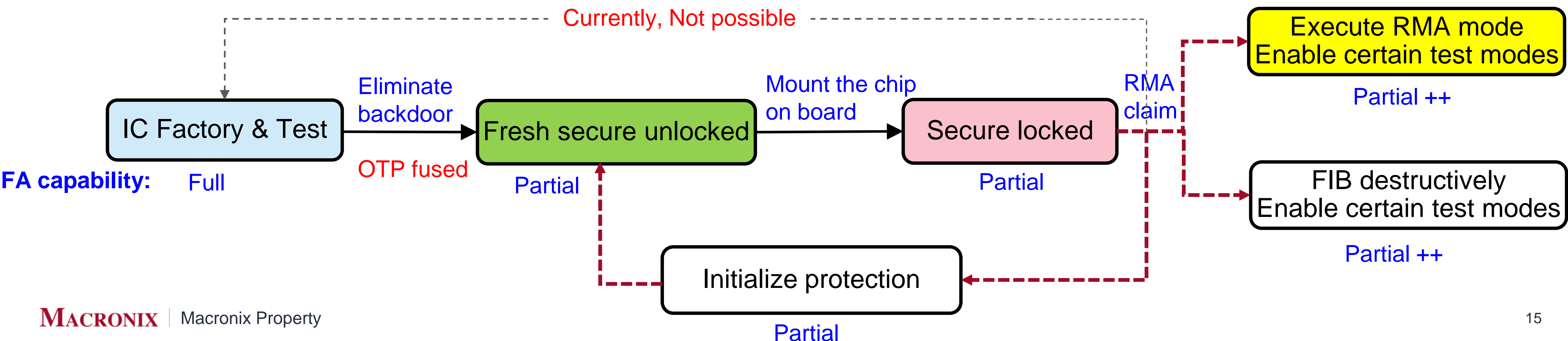
- With root key from customers, erase cryptographic keys and credentials

Trending is the idea of executing RMA mode before sending back RMA samples for analysis enable certain test modes for failure analysis—partial ++

- Enable certain test modes for failure analysis, because this change won't impact security of embedded systems
- Being evaluated by the industry

Other ideas—utilize FIB destructively to re-enable test modes—partial ++

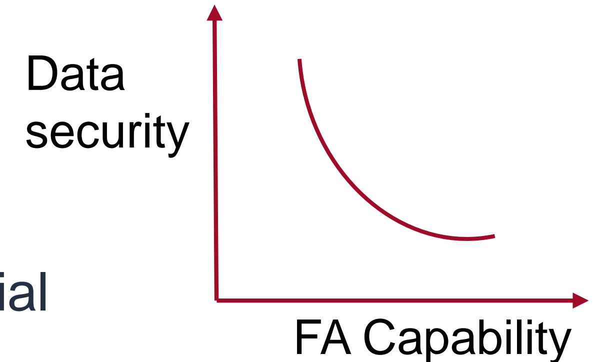
- Needs more time to develop and evaluate (reconnect disabled test mode lines, bypass security fuses,…)



Summary

Secure Features restrict what failure analysis can be performed on the device

Trade-off between security, ease of FA and operational complexity



Communication across Core Chip Vendor, Tier 1 and Flash supplier is essential

Increase in analysis time and cost (Ex., decap, die pickup, re-bonding on PCB for backside EMMI)

Only partial diagnosis—failure symptoms but not root cause

Enhancing FA capabilities for secure chip is evolving

THANKS FOR YOUR ATTENTION