SNIA DEVELOPER CONFERENCE
SDC 25
By Developers FOR Developers

Hyatt Regency Santa Clara, CA
September 15-17, 2025

Emerging Trends in Data Security for Data Centers and Automotive Fabrics

Bill Gervasi, Principal Memory Solutions Architect
Junjian Zhao, Sr. Manager, Technical Marketing
Monolithic Power Systems

www.sniadeveloper.org

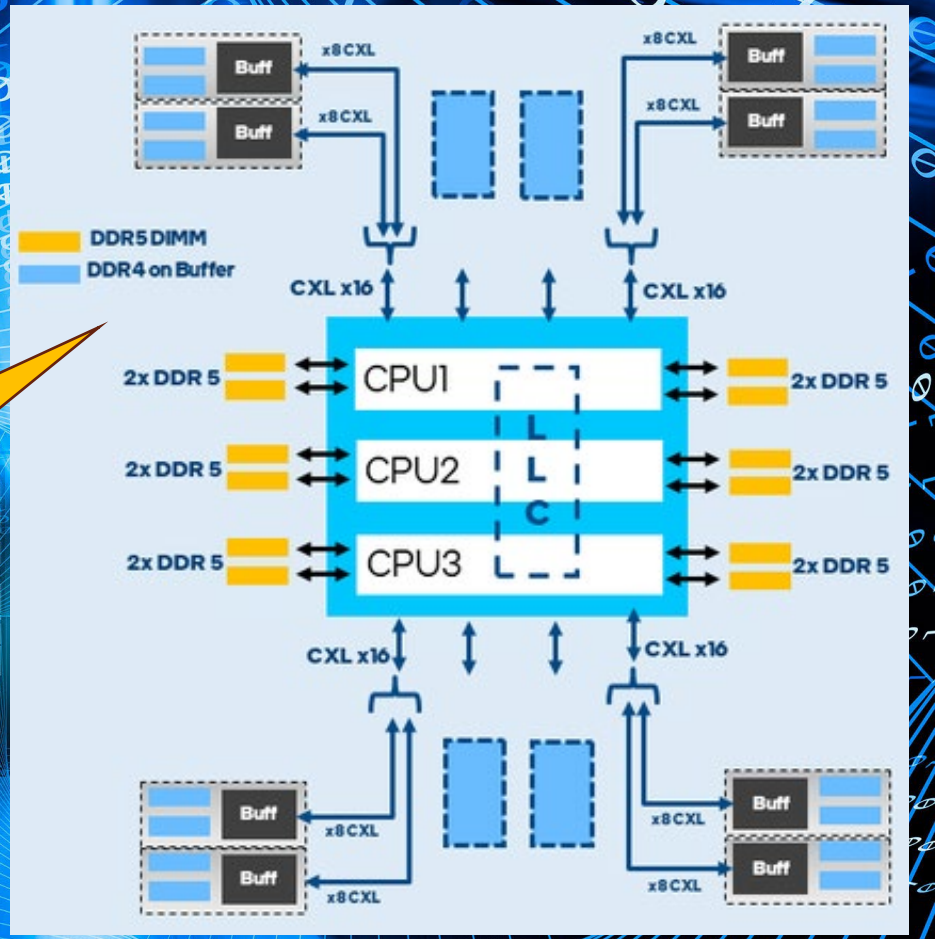
Emerging Trends in Data Center Security

Security Concerns in the next generation

So many attack points in fabric architectures

…and the sophistication of the attackers is increasing…

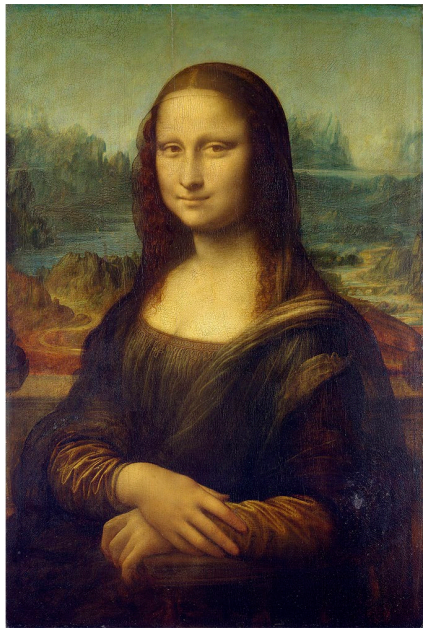
Growing variety of memory and storage options creates new challenges

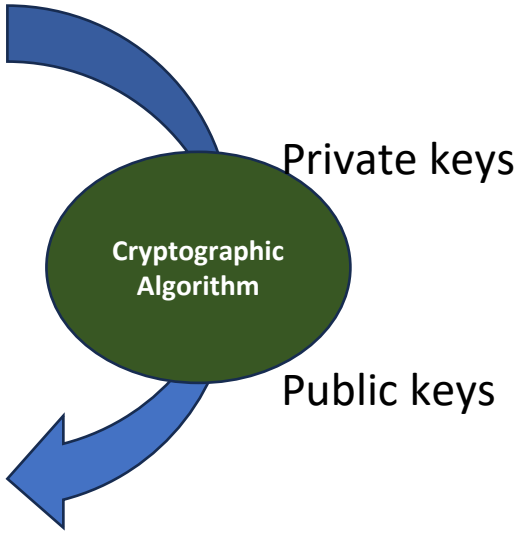


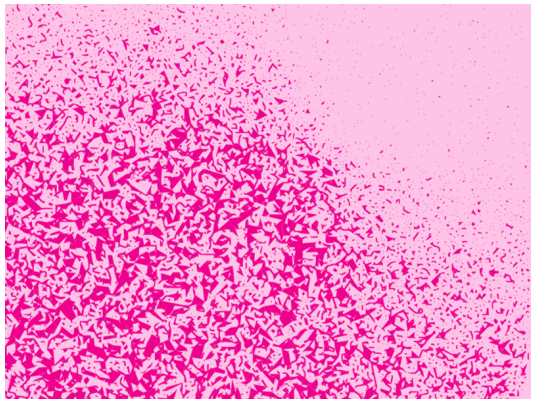
Detection & mitigation need support

Hardware		Software
Malware	Virus-style programs, Denial of Service attacks	Insecure Agency
Man-in-the-middle	Mimic trusted device, Intercept data in flight	Insecure Plugin Design
Spy chips	Devices planted in system Malicious data corruption	Insecure Output Handling

Not even close to a comprehensive list… illustrative only!







Security regimes include verifying a root of trust

Combination of keys and hashing algorithms allow data security

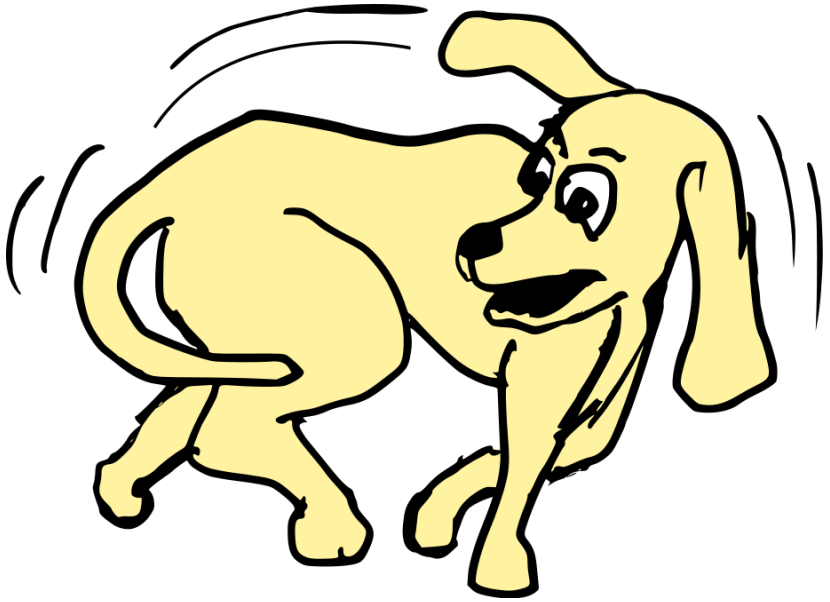
Algorithms assume thousands of years are needed to decode the information

The larger the data set, the more difficult to decode

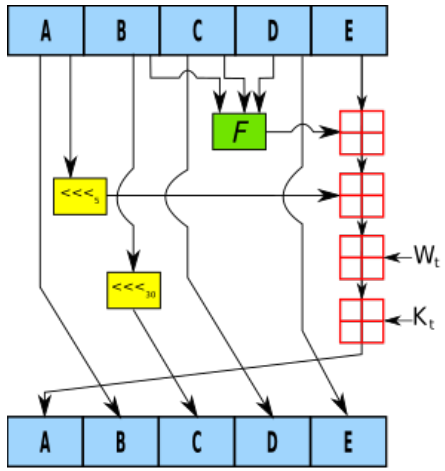
Security is a treadmill

Algorithm complexity increases as computers get better

1993: SHA-0 160-bit hash
1995: SHA-1 improved algorithm
2001: SHA-2 256 & 512-bit hashes
2015: SHA-3 improved algorithm



e.g., During Auto SSD standard development, NIST deprecated 256-bit in favor of 384-bit… so we changed the proposal



Security requirements will undoubtably change during the life of the next generation memory and storage

We need to be flexible in how we keep up

Hardware + firmware likely necessary… but where?

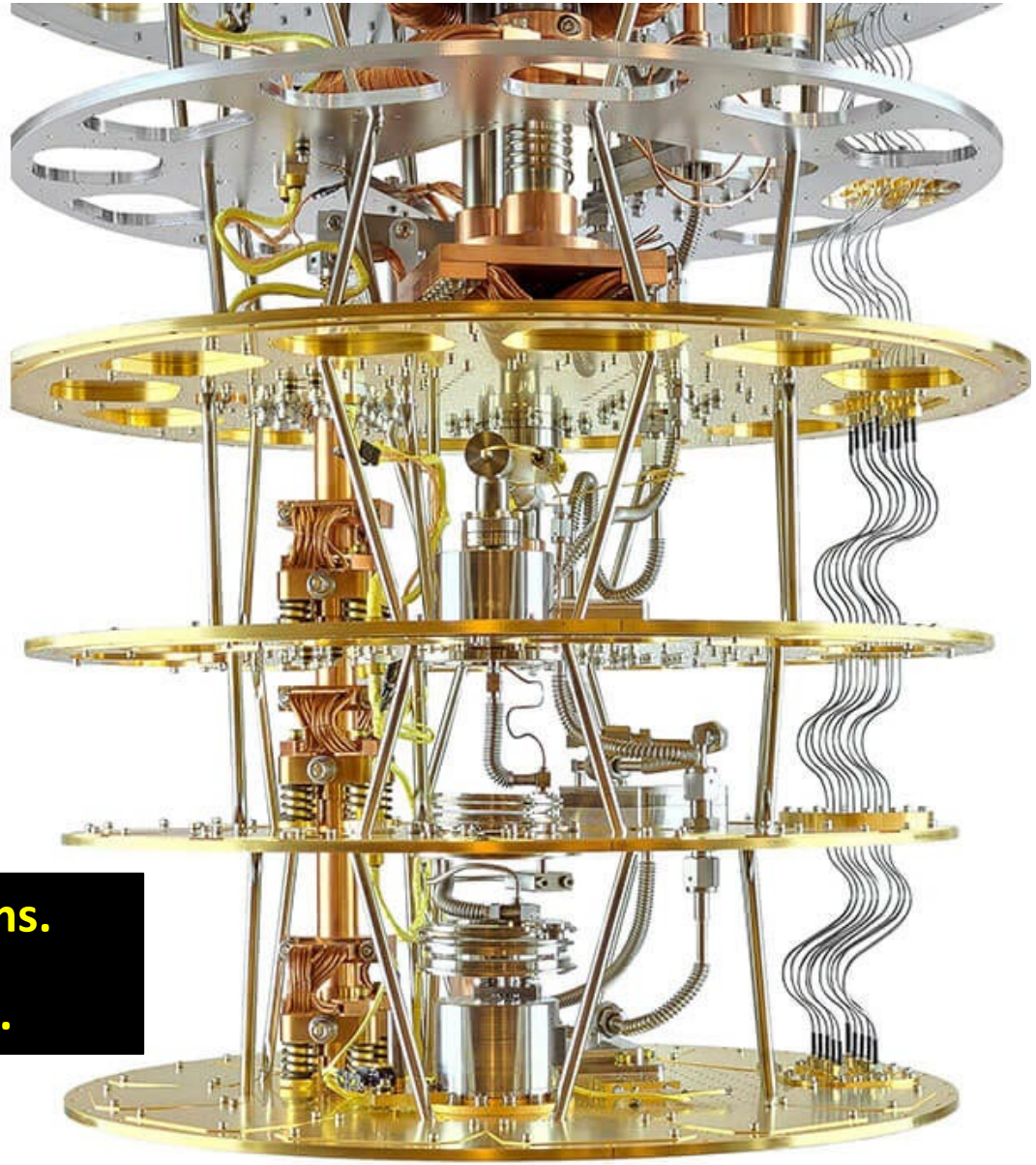
Enter Quantum Computers

Quantum computers process data exponentially faster than traditional computers

Need for newer security algorithms emerge

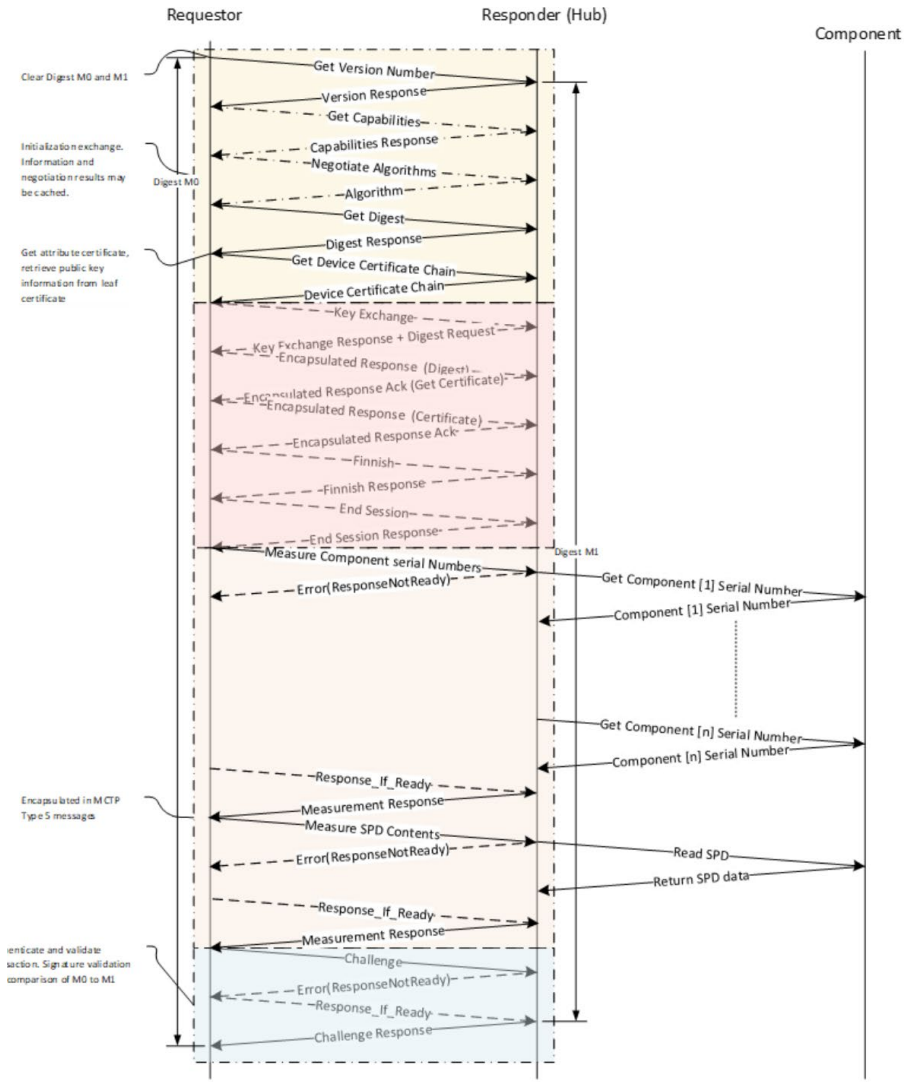
The NIST treadmill is alive and well

2024: First three PQCs: FIPS 203, FIPS 204, FIPS 205
2025: HQC joins the list



•2030: NIST plans to deprecate RSA-2048 and ECC-256 algorithms.

•2035: NIST plans to disallow RSA-2048 and ECC-256 algorithms.



Security handshake to establish root of trust is fairly complex

Requires certificates that are multiple KB in size

Taking this complexity all the way to every active component would be

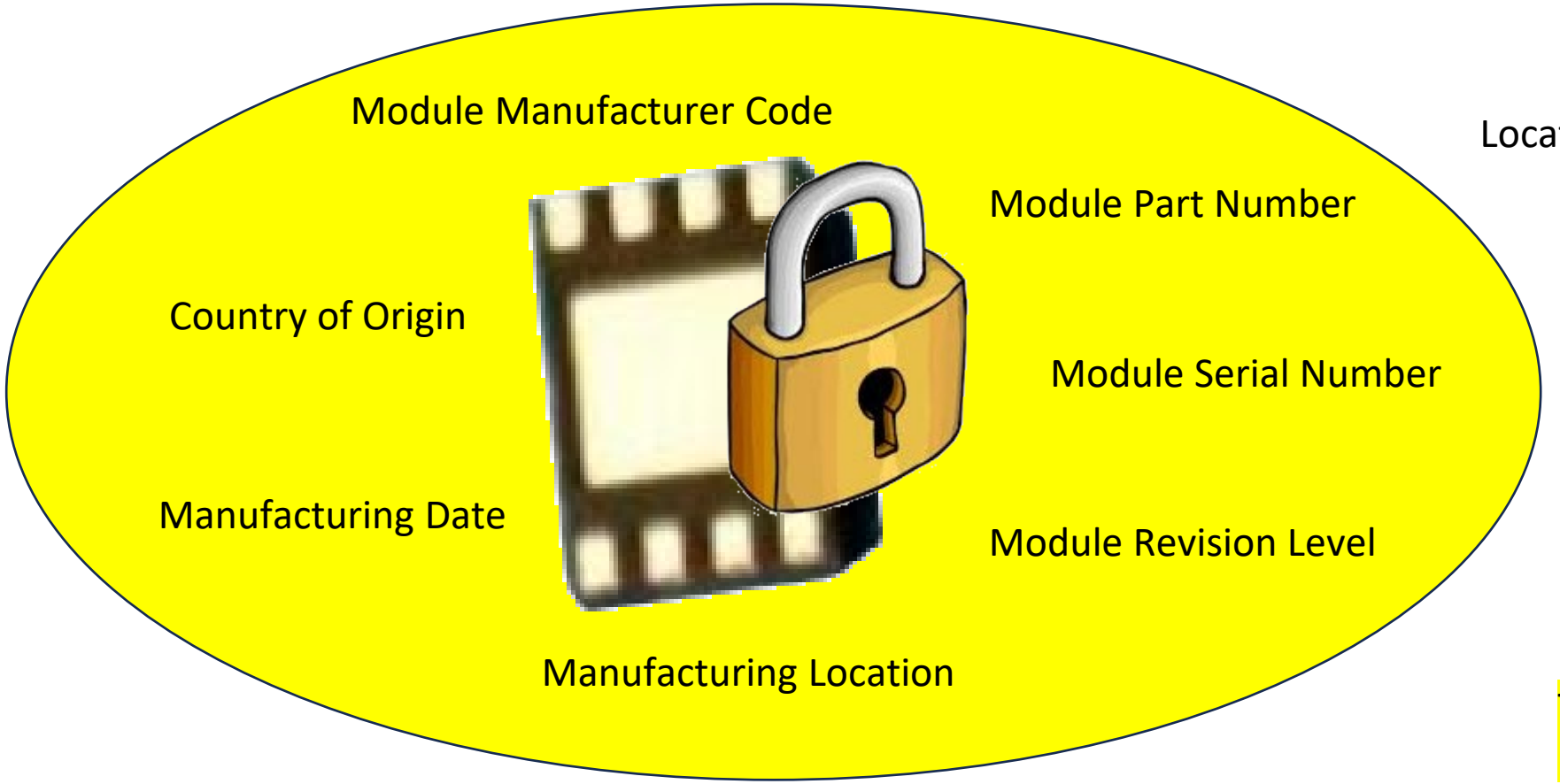
- Too costly (tens of thousands of gates)
- Introducing new security risks and attack points

Having a system management hub proxy the module leaves it open to spoofing with non-secured components

However, end users do want to add bill-of-materials tracing to memory modules to increase trust levels

Bill of Materials

Hardware identifiers programmed into a secured (immutable) configuration ROM



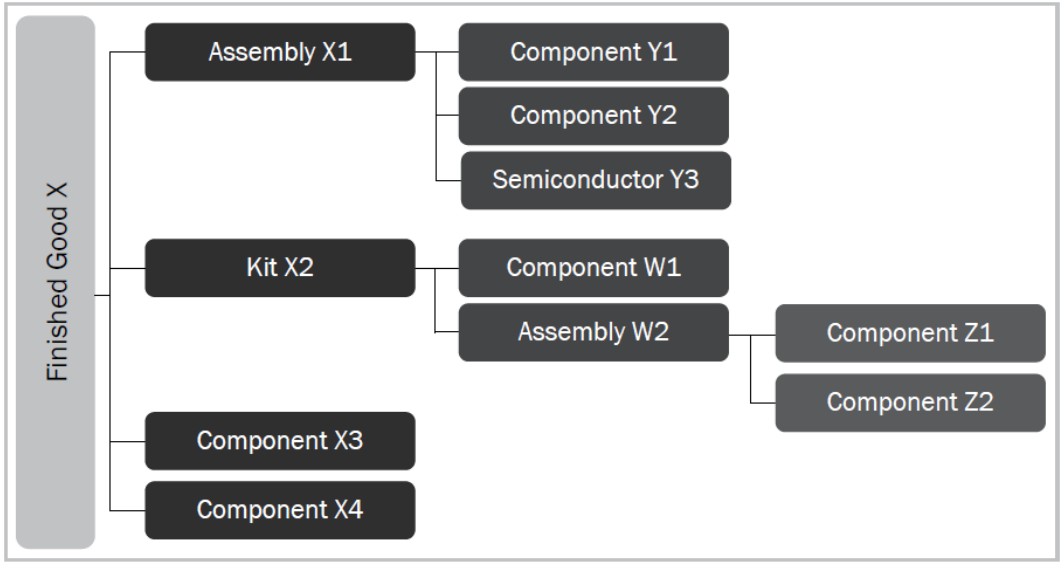
Located on a system management bus

Read by baseboard manager or host CPU

This information may be spoofed!
Next level verification still needed

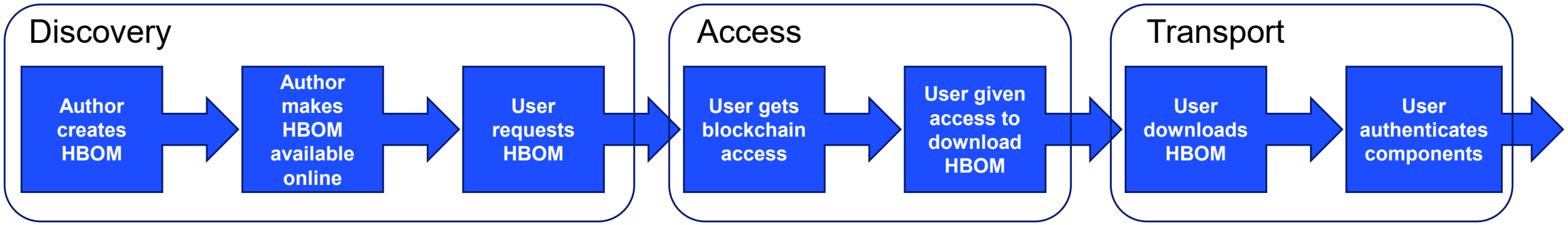
HBOM Framework

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE



- Provide a framework for identifying hardware installed in systems
- Covers nearly everything in the data center wish list
- May need some additional information

https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management
https://www.dmtf.org/sites/default/files/standards/documents/DSP0289_1.0.0WIP80.pdf
https://csrc.nist.gov/pubs/ir/8536/2pd



Establish a trust between end user and supplier

1. Supplier creates an HBOM (Hardware Bill of Materials) describing product
2. Customer establishes blockchain encrypted access to HBOM from supplier
3. HBOM may include nested links to key (e.g., smart) components

CISA HBOM Schema

C.1. Field Category: HBOM Header Information

These fields express information about the HBOM document itself, such as when the HBOM file was created.

C.1.1. FIELD NAME: HBOM_STD_VERSION
C.1.2. FIELD NAME: HBOM_CREATION_DATE
C.1.3. FIELD NAME: HBOM_MODIFY_DATE
C.1.4. FIELD NAME: HBOM_AUTHOR
C.1.5. FIELD NAME: FGA_SUPPLIER
C.1.6. FIELD NAME: FGA_NUM
C.1.7. FIELD NAME: FGA_DESCRIPTION

C.2. Field Category: Finished Good Product Details
C.2.1. FIELD NAME: FGA_TYPE
C.2.2. FIELD NAME: FGA_VERSION

C.3. Field Category: Entity Name
C.3.1. FIELD NAME: FGA_HASH
C.3.2. FIELD NAME: FGA_MAIN_MANUFACTURER
C.3.3. FIELD NAME: FGA_ALT_MANUFACTURER
C.3.4. FIELD NAME: COMP_SUPPLIER
C.3.5. FIELD NAME: COMP_MANUFACTURER

Some examples of the data

encapsulated in a standard HBOM

C.4. Field Category: Entity Location
…
C.5. Field Category: Component Part Information
…
C.6. Field Category: Component Part Details
…
C.7. Field Category: Production Details

A Personal Criticism…

“This is great, but where is the serial number?”

I’ll be researching how to add this to the schema

Security breaches will still occur

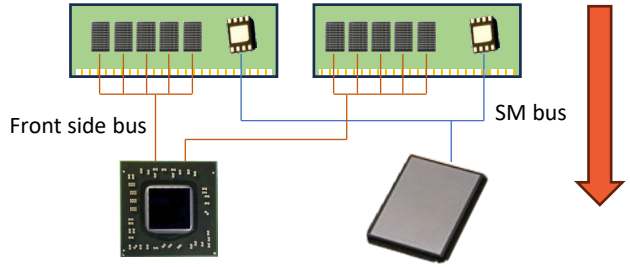
When they are caught, what action is taken?

Adding security numbers to the schema would allow building Exclusion Lists for known threats

Without serial number, users would have to disallow all parts from a supplier built in a specific factory in a specific week

Downside: suppliers’ databases get larger

Data Center Example Using DRAM Module



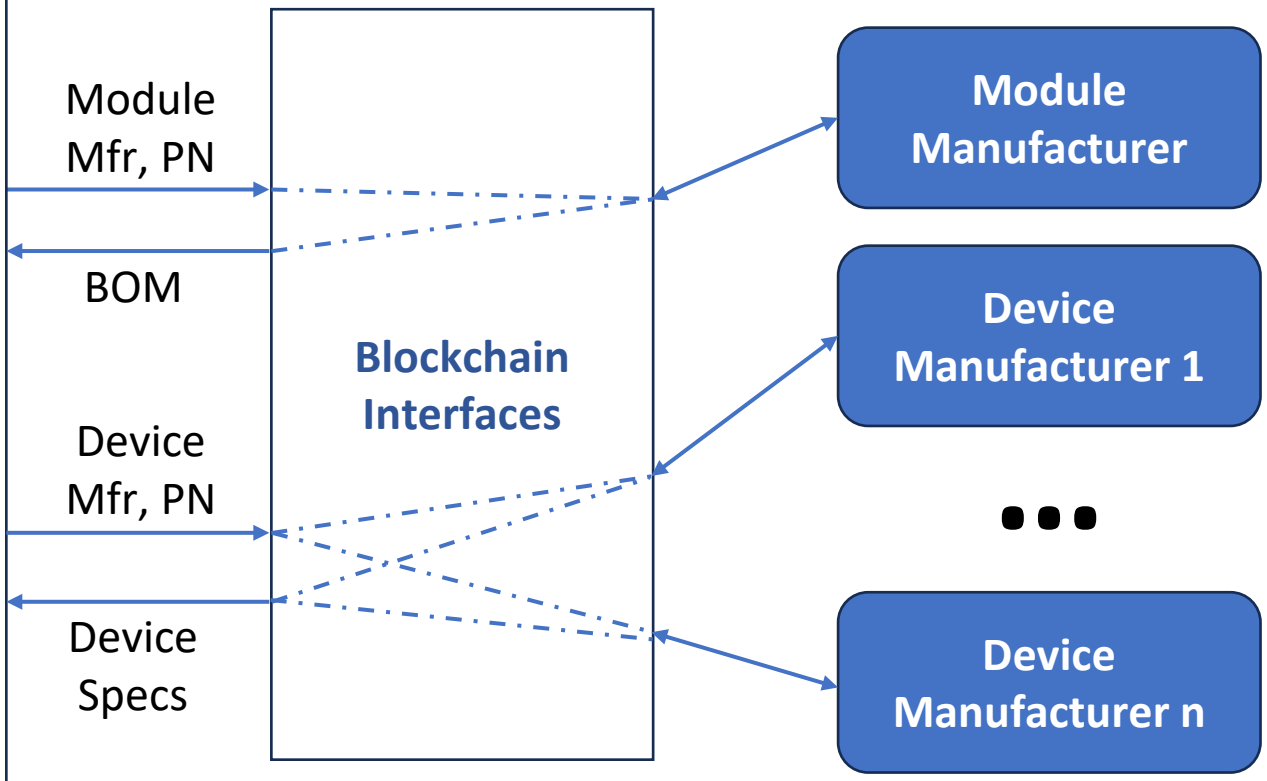
Software BOM read from configuration ROM
Manufacturer codes: Module, DRAM, etc.
Serial numbers from memory components
Serial numbers from support chips

Security check performed by host

BMC/CPU gets supplier data from ROM

Uses blockchain access to module vendor to read full BOM

Any specific devices can be looked up as BOM contains supplier info as well



Spoofing resilience requires additional tracking

- Destination of module
- Known violators reported and identified
- Full SPDM hash verification could be added using device serial numbers if added to schema

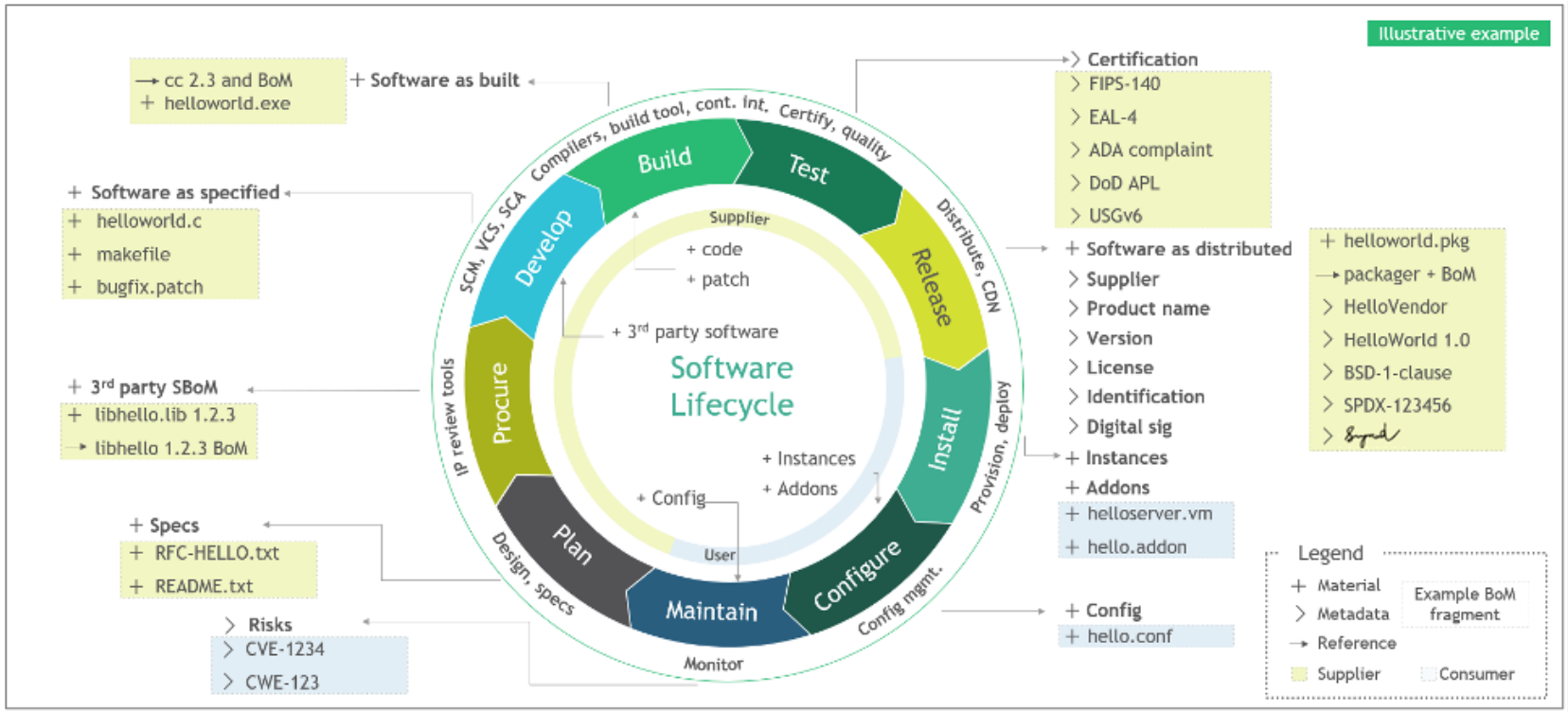
SBOM: Software Validation

Software needs even deeper security

Includes apps, firmware, BIOSes

Authentication required before any updates executed

Rollback in case updates cause issues



https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1
https://www.cisa.gov/sbom
https://spdx.dev/

BOM Tracking is a Start…

Data center BOM tracking builds trust in components

Requires suppliers and users cooperate with electronic links

Additional levels of security checks may be added (e.g., SPDM)

Security proxies, system authentication, encryption are beyond the scope of this talk

Security isn’t free – this takes time and adds cost…

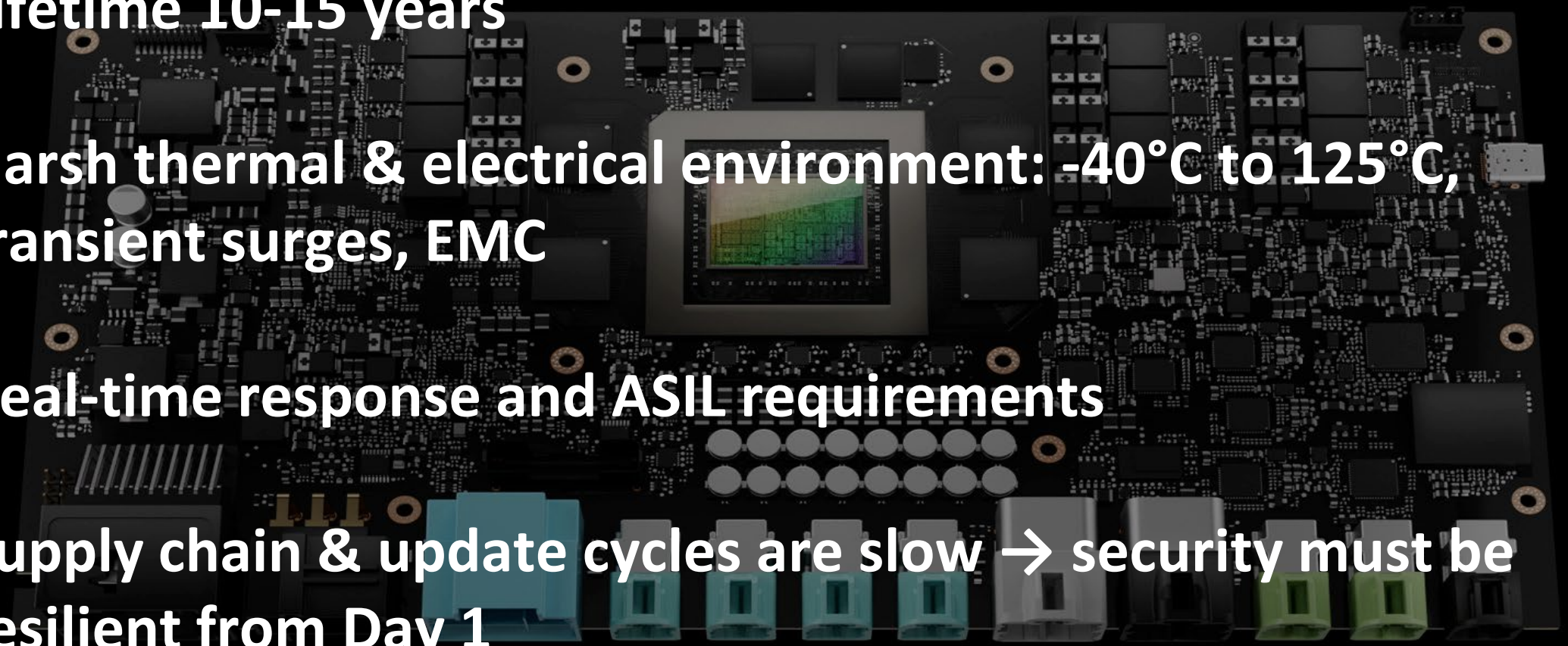
…but detecting an attack before it happens

is cheaper than fixing the problem after it happens

Emerging Trends in Automotive Fabrics and Data Security

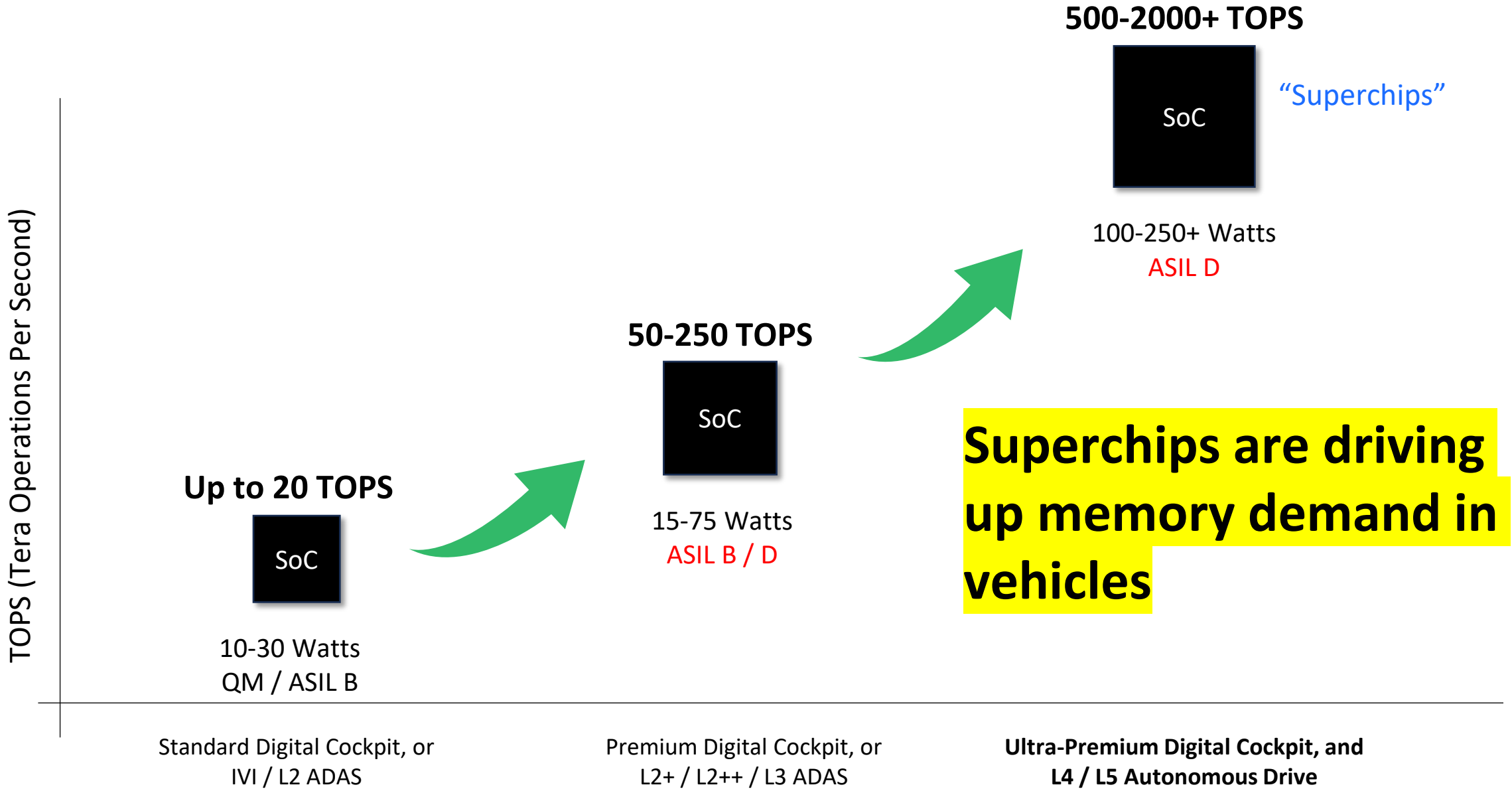
What's Different When Memory Goes Into Cars?

- Lifetime 10-15 years
- Harsh thermal & electrical environment: -40°C to 125°C, transient surges, EMC
- Real-time response and ASIL requirements
- Supply chain & update cycles are slow → security must be resilient from Day 1



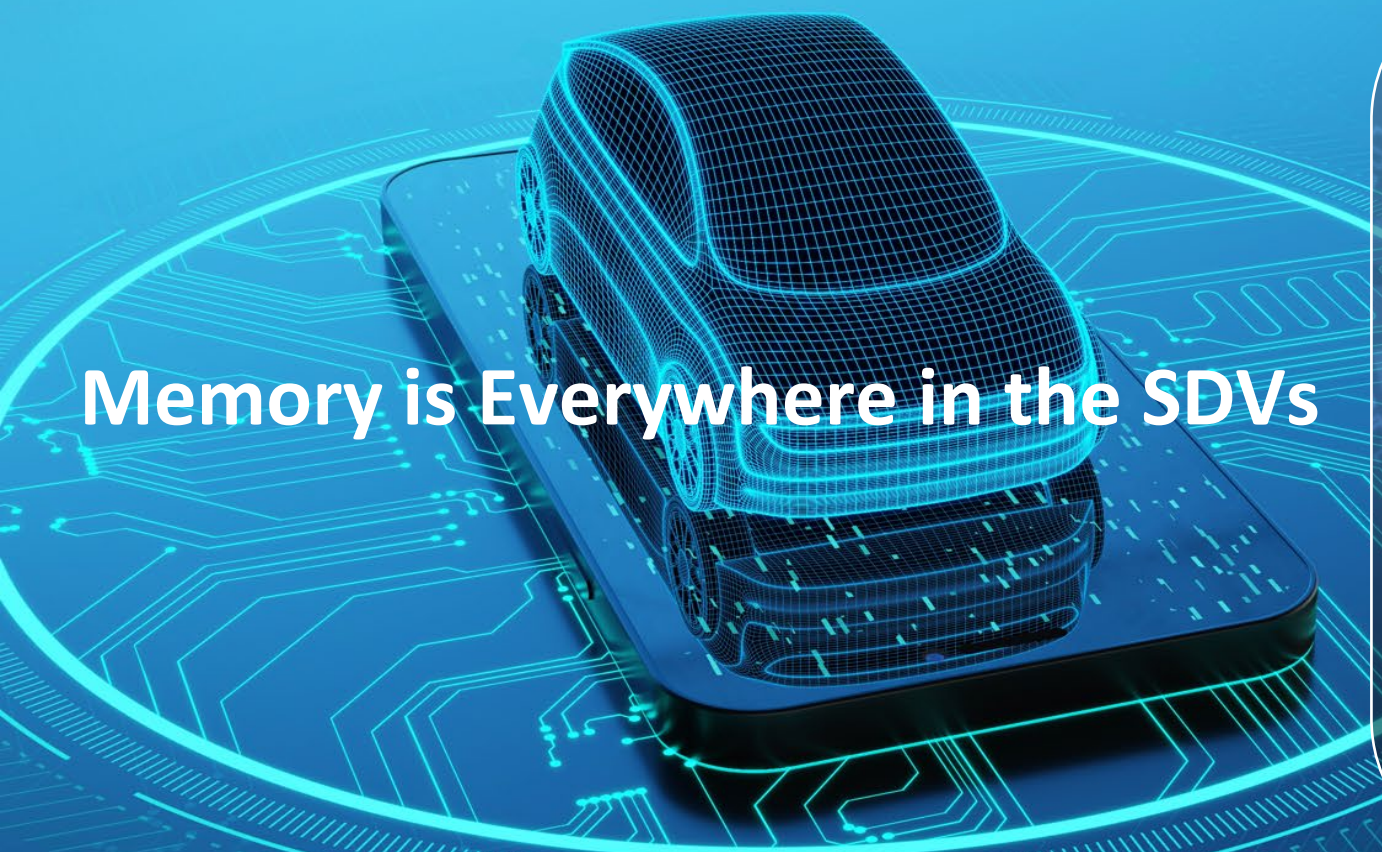
NVIDIA DRIVE Thor – publicly announced late 2022

High Performance Computing Puts Memory at the Heart of the Car



Superchips are driving up memory demand in vehicles

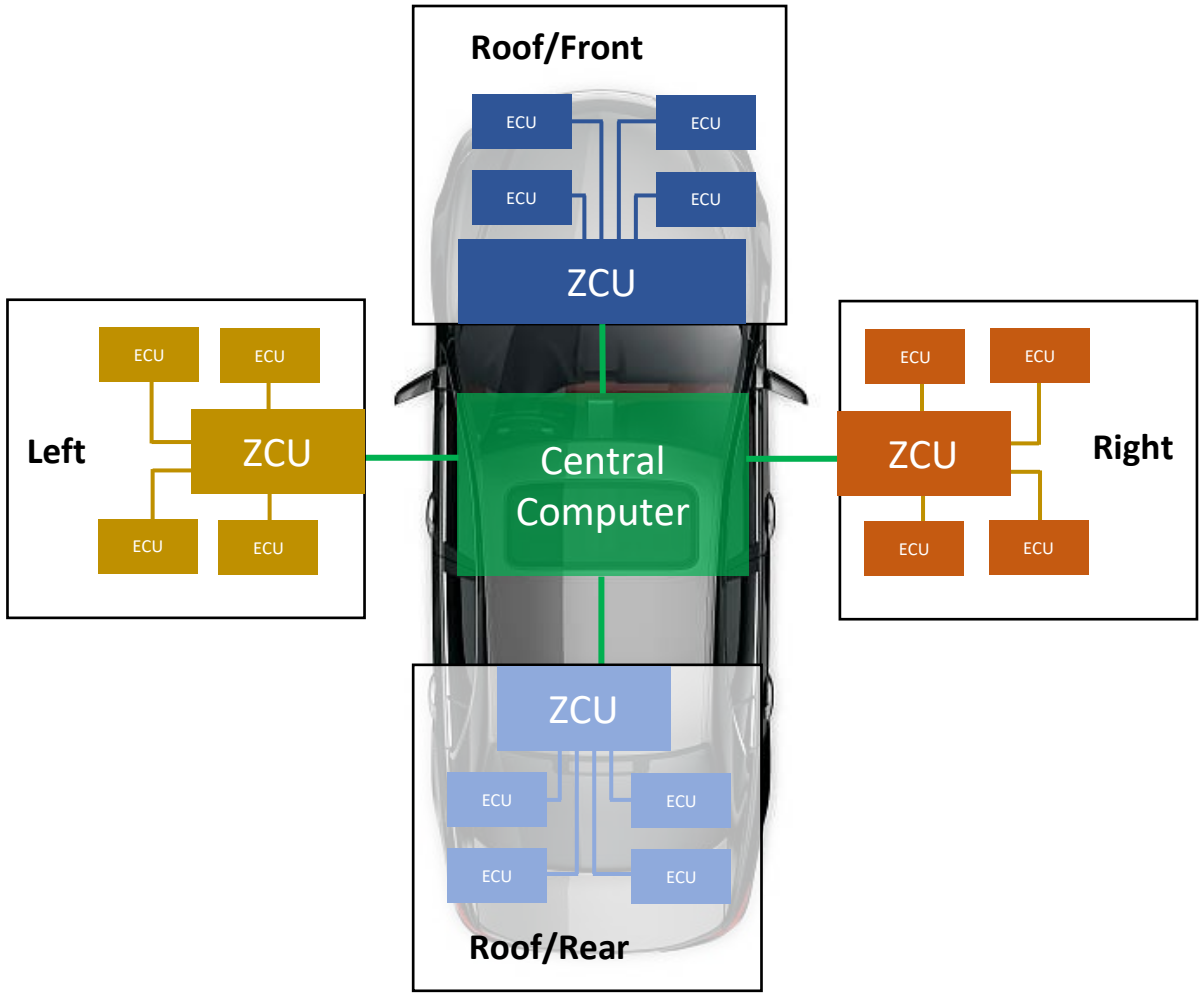
Transforming into Software-Defined Vehicle (SDV)



Memory is Everywhere in the SDVs

- Flexibility
- OTA Upgradability
- HW & SW Ecosystem
- Ubiquitous Connectivity
- SaaS / App Marketplace
- Big Data
- Faster SW Development

The Emerging Attack Surface in SDVs

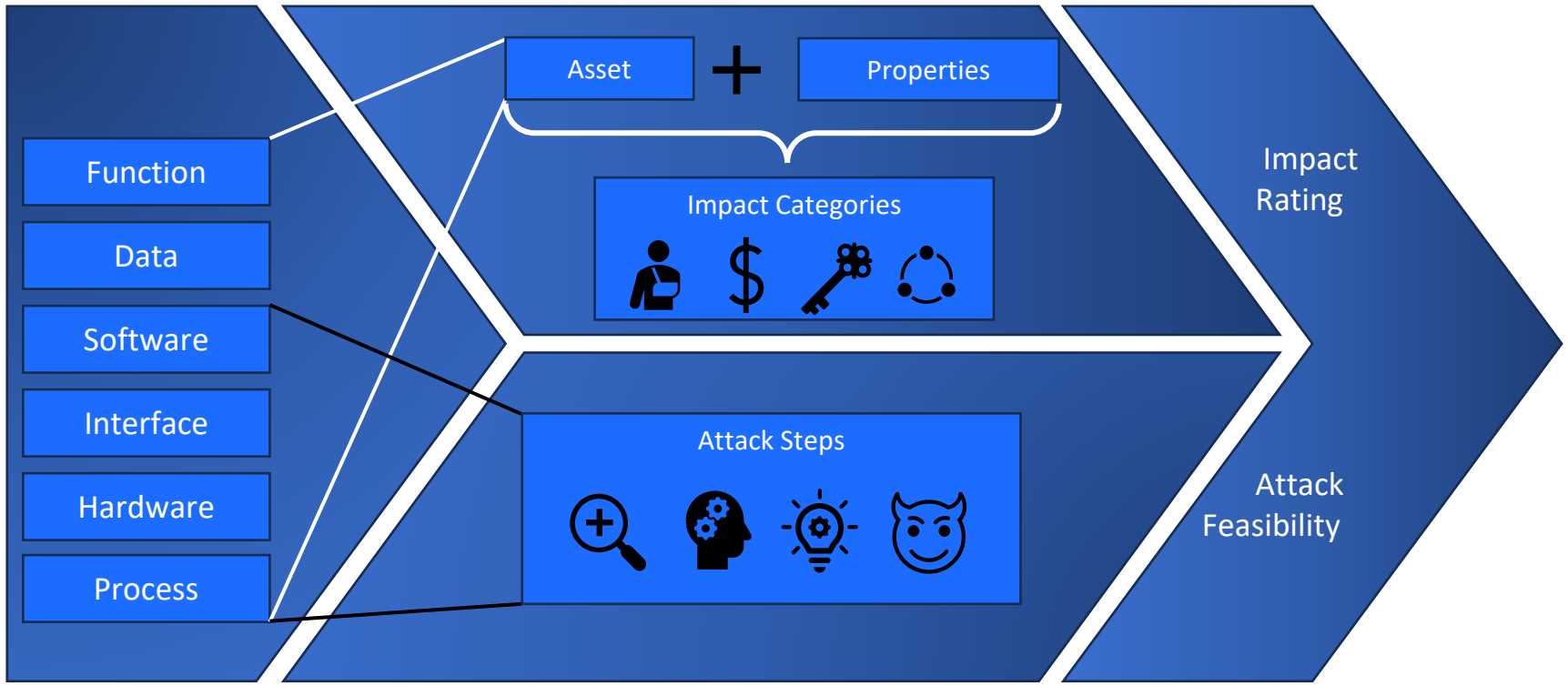


Zonal architecture

- Zonal architecture and Centralizes compute, making memory central to vehicle operation
- More memory usage → more potential attack surfaces
- SDVs mean OTA updates, frequent reconfigurations → DDR must maintain security long-term

Memory Security Gaps

- Spoofing
- Row hammer
- Unauthorized access
- Man-in-the-middle



SPDM: A Good Start, but Not Sufficient

- SPDM = Platform Security Protocol (used for auth & secure messaging)
- Works well in servers, but still spoofable in some cases (e.g., cloned serials)
- Requires frequent updates → **requalification headache in automotive**

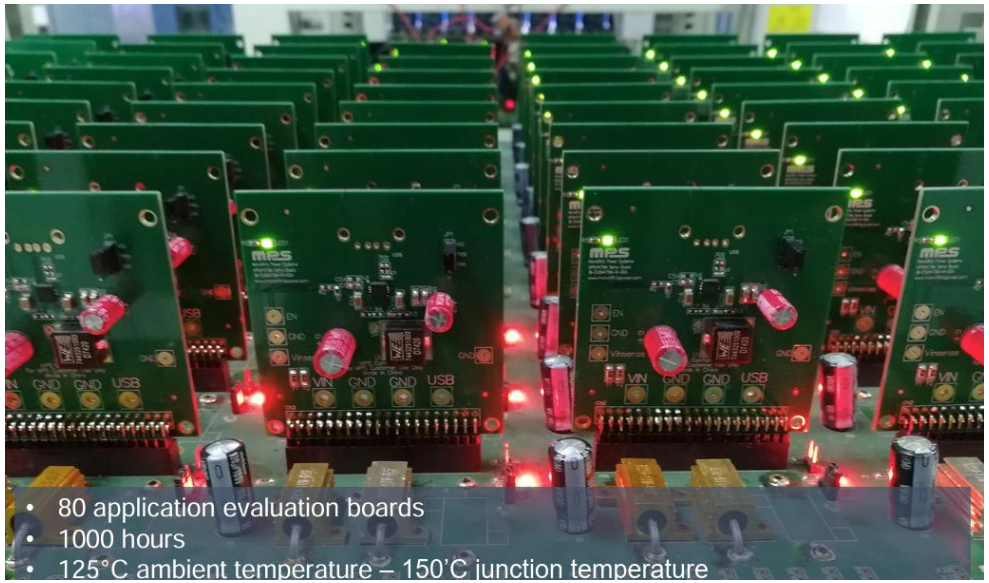
Table 2 Test #	A2	A3	A4	A5	A6	B1	B2	B3	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4	D5	E2	E3	E4	E5	E7	E9	E10	E11	E12	G1-	G4	G5	G6	G7	G8
Test Abbreviation	THB	AC	TC	PTC	HTSL	HTOL	ELFR	EDR	WBS	WBP	SD	PD	SBS	LI	EM	TDDB	HCI	NBTI	SM	HBM	CDM	LU	ED	CHAR	EMC	SC	SER	LF	MECH	DROP	LT	DS	IWV
DESIGN																																		
Active Element Design		●	●	M		●	●	DJ							D	D	D	D	D	●	●	●	●	●	●	●	●			F			
Circuit Rerouting			A	M																●	●	●	●	●	●	●							
Wafer Dimension / Thickness			E	M		●	●		E	E								●		E	E	E	●											
WAFER FAB																																		
Lithography	●		●	M		●	G		●	●								●					●											
Die Shrink	●	●		M		●	●	DJ							●	●	●	●	●	●	●	●	●	●	●	●	●							
Diffusion/Doping				M		●	G											●		●	●	●	●	●										
Polysilicon			●	M		●		DJ										●		●	●	●	●	●										
Metallization / Vias / Contacts	●	●	●	M		●			●	●					●				●				●	●		●								
Passivation / Oxide / Interlevel Dielectric	K	K	●	M		●	GN	DJ	K	●						●	●	●	●	●	●	●	●	●										
Backside Operation			●	M		●														M	M	●		●					H				H	
FAB Site Transfer	●	●	●	M		●	●	J	●	●					●	●	●	●	●	●	●	●							H				H	
ASSEMBLY																																		
Die Overcoat / Underfill	●	●	●	M	●	●																					●							H
Leadframe Plating	●	●	●	M	●					C	●			●														L				H		
Bump Material / Metal System	●	●	●	M	●	●						●	●														●	L						
Leadframe Material		●	●	M	●					●	●	●		●												●		L	H			H		
Leadframe Dimension		●	●	M							●	●		●												●		L	H					
Wire Bonding	●	●	●	Q	●				●	●													M			●			H					
Die Scribe/Separate	●	●	●	M																														
Die Preparation / Clean	●	●		M		●			●	●																						H		
Package Marking											B																							
Die Attach	●	●	●	M		●																	●			●		L	H			H	H	
Molding Compound	●	●	●	M	●	●	●				●	●		●													●	L						
Molding Process	●	●	●	M	●	●					●	●		●														L						
Hermetic Sealing		H	H		H							H		H															H		H		H	
New Package	●	●	●	M	●	●	●		●	●	●	●	T	●						●	●		●			●		L	H			H	H	
Substrate / Interposer	●	●	●	M	●	●			●	●			T															L	H			H	H	
Assembly Site Transfer	●	●	●	M		●	●		●	●	●	●	T	●									●					L	H			H	H	

- Highly Recommended

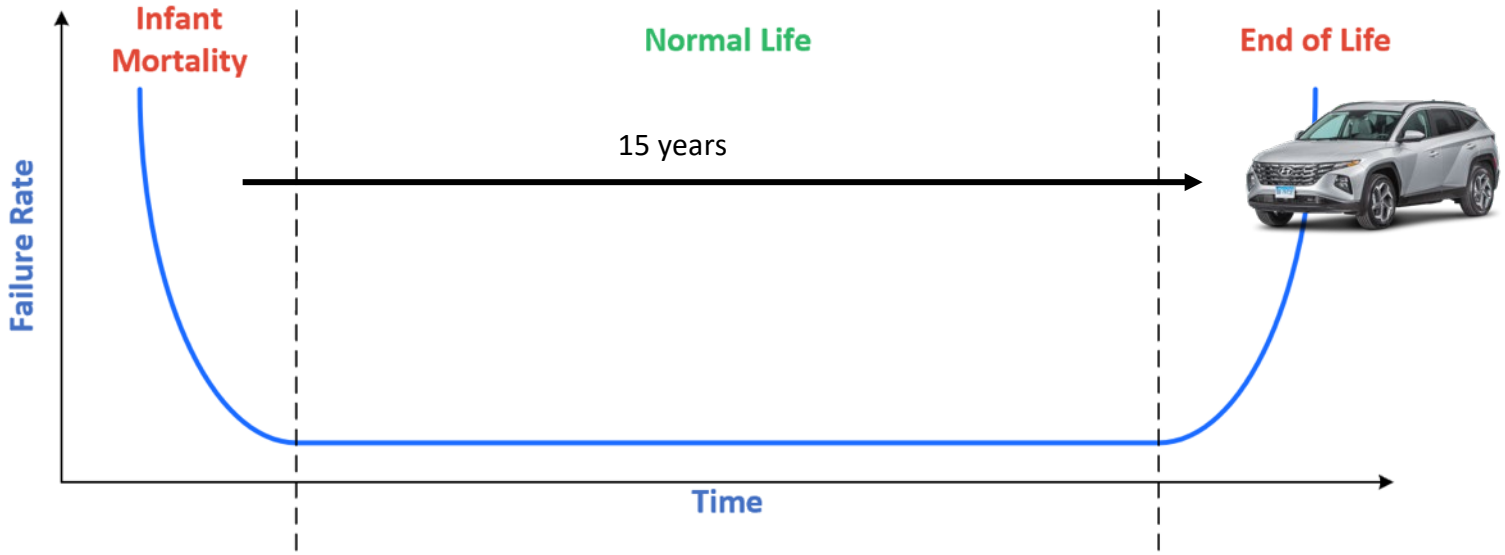
A Only for peripheral routing
B For symbol rework, new cure time, temp
C If bond to leadfinger
D Design rule change
E Thickness only

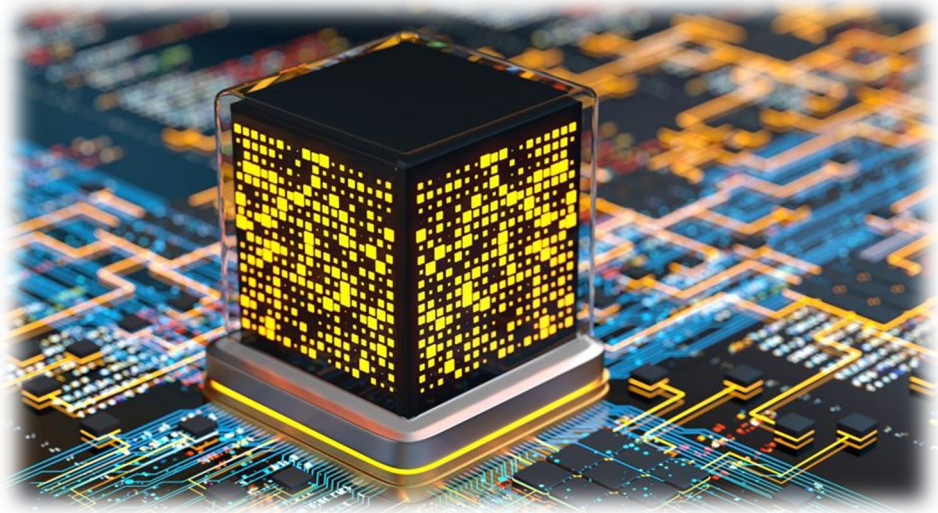
F MEMS element only
G Only from non-100% burned-in parts
H Hermetic only
J EPROM or E^2PROM
K Passivation only

L For Pb-free devices only
M For devices requiring PTC
N Passivation and gate oxide
Q Wire diameter decrease
T For Solder Ball SMD only



Post-Quantum Threats: Why Automotive Might Be First





- Cars shipping in 2025 may still be on the road in 2040
- PQC-ready hardware for memory encryption and secure boot will likely appear in robotaxi first
- Memory vendors need to consider future-proofing hardware-level encryption/latency tradeoffs

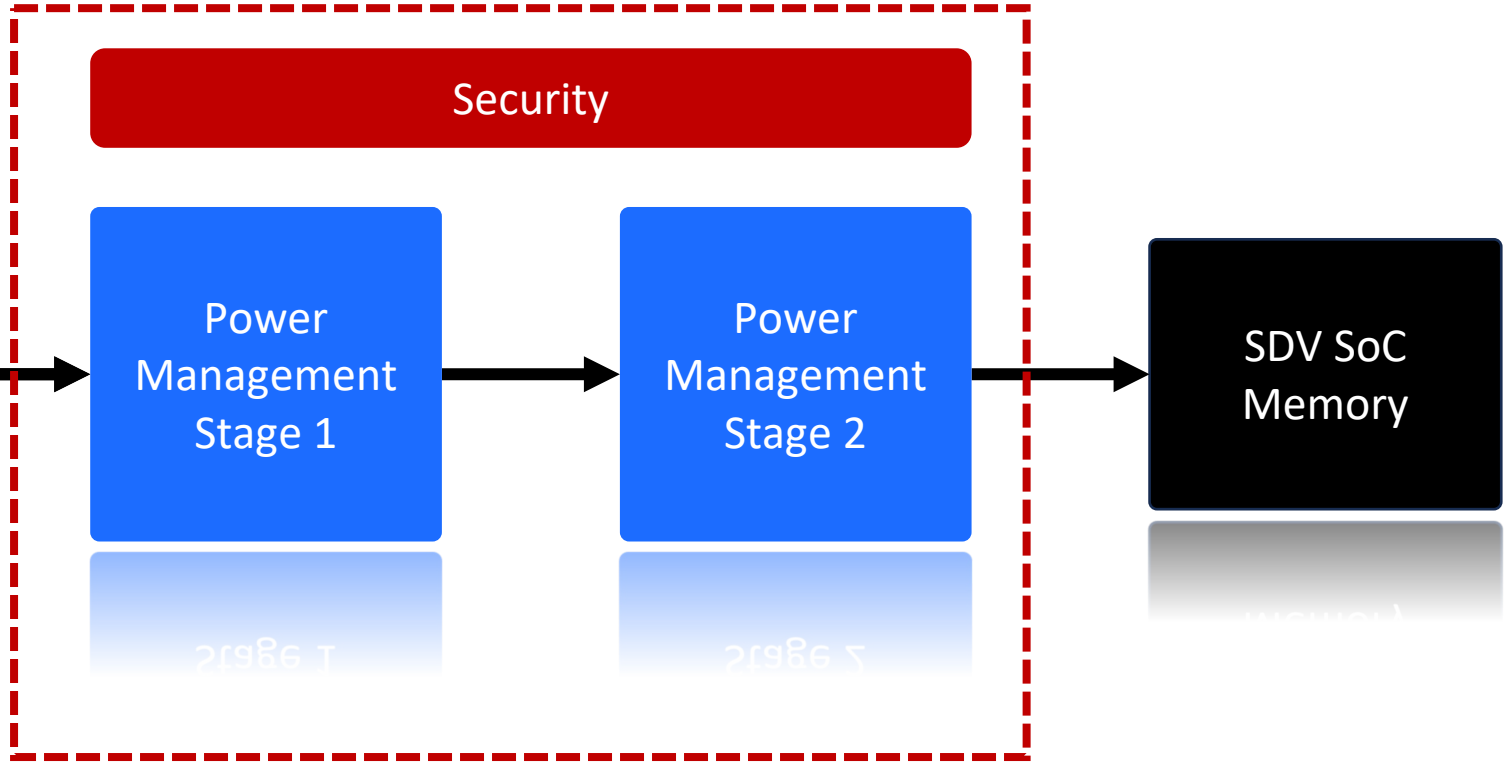
The Missing Link Between SoC and Memory

- Today, Memory has no strong identity verification at boot
- If compromised, SoC can’t distinguish genuine vs. spoofed memory
- Need a new trust anchor—closer to the physical connection

Power, Once an Afterthought, Can Make Data Security

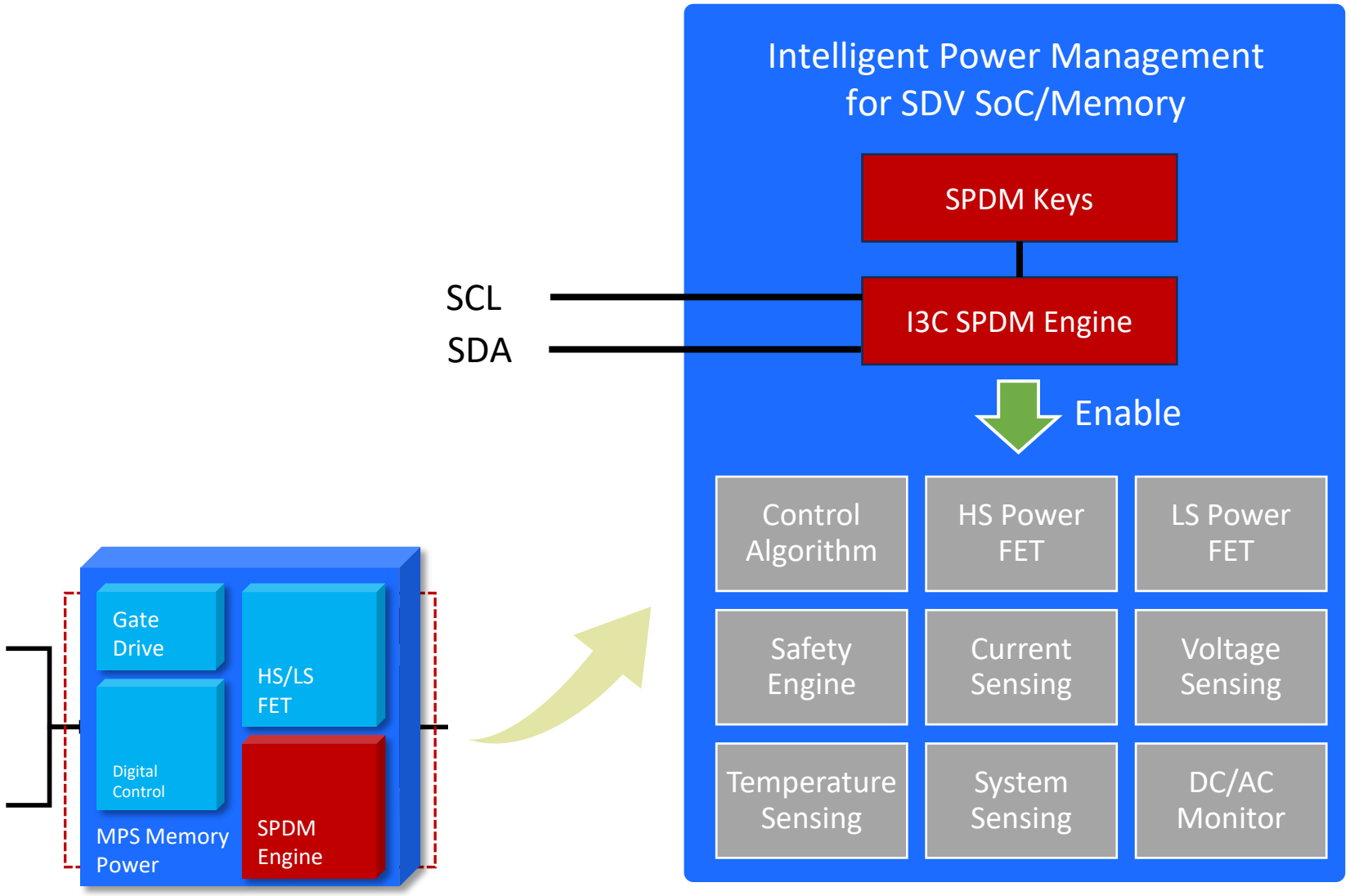
12V/48V Battery

EV Battery



- PMICs already sequence memory power, control I3C
- Natural location to enforce security policies before memory is accessible
- Low-level access = strong control point

PMIC with Embedded SPDM + PQC



- PMIC performs SPDM handshake with host and memory
- Can store certified hash keys, implement PQC algorithms
- Allows memory access **only after authentication passes**

Benefits for Memory/Storage Vendors

- Offloads SPDM/PQC complexity from memory module
- No need to requalify DIMMs or SSDs every security cycle
- Security can be upgraded via PMIC firmware, not hardware redesign
- Enables modular design for automotive and edge

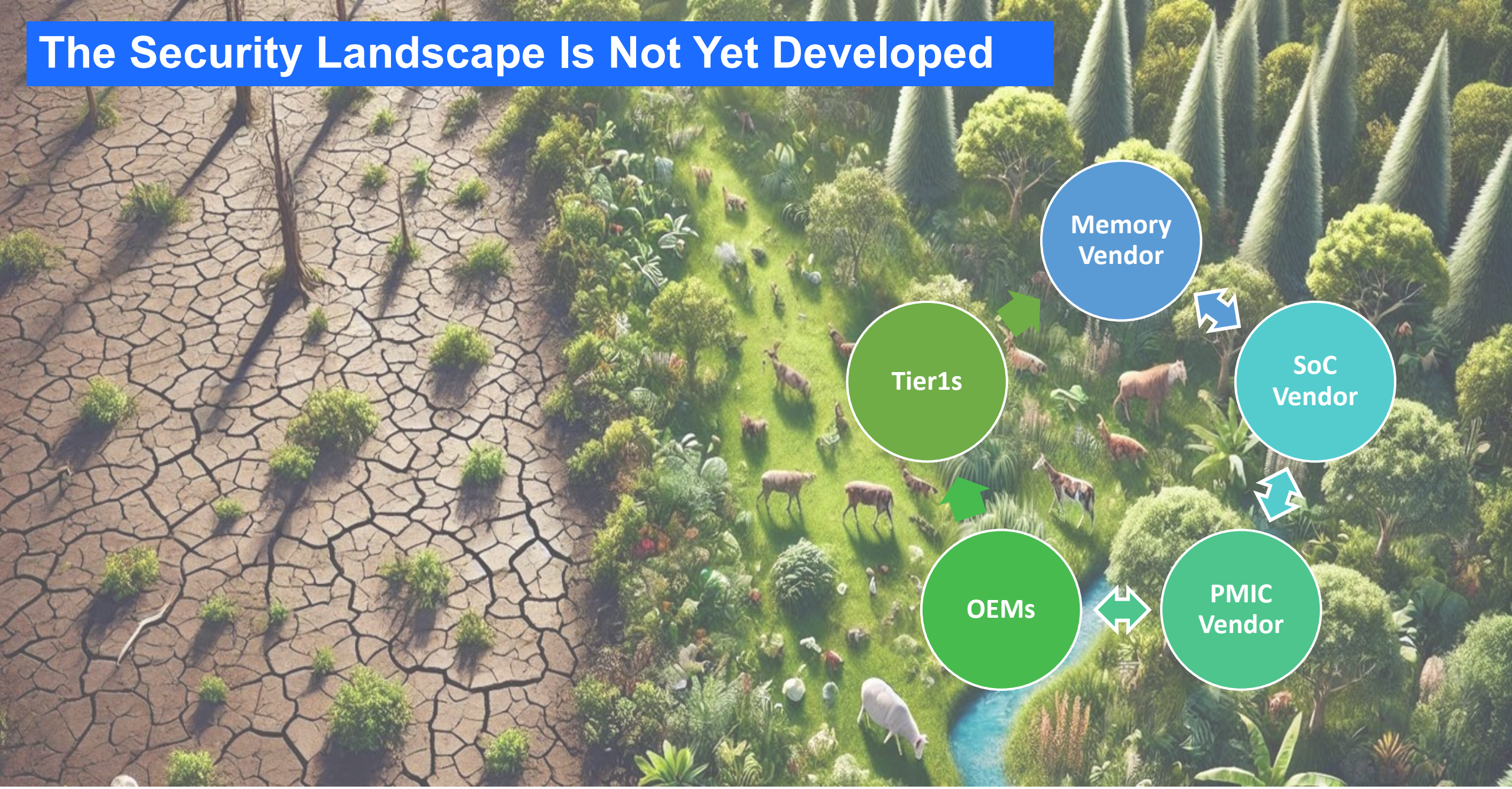
Shield from malicious breach
cyberattacks

Where This Applies First

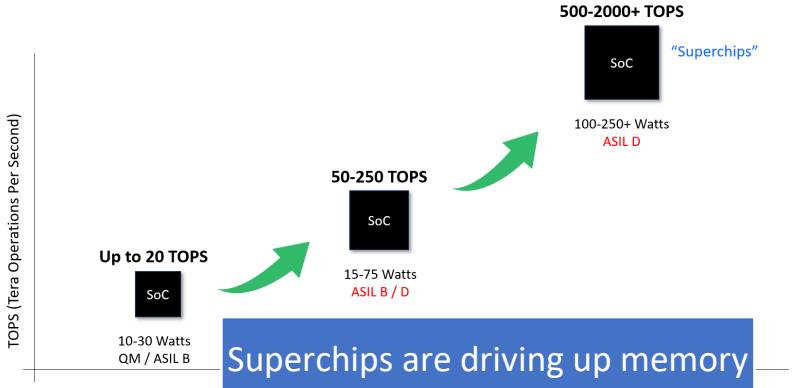
SSDs for automotive: high requalification cost → prime market

DDR5/LPDDR for SDV SoCs: high-speed + security need

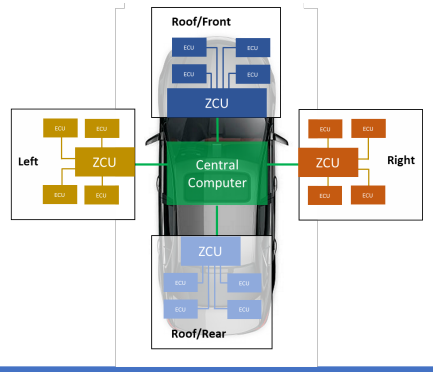
The Security Landscape Is Not Yet Developed



Recap



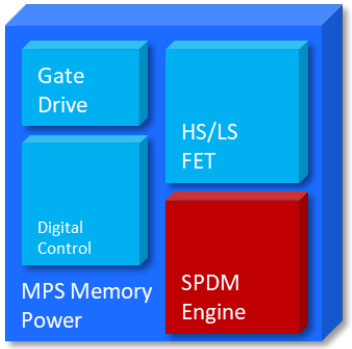
Superchips are driving up memory demand in cars



More memory usage in SDV → more potential attack surfaces

AECQ requalification headache in automotive

Post-Quantum Threats - Automotive Might Be First

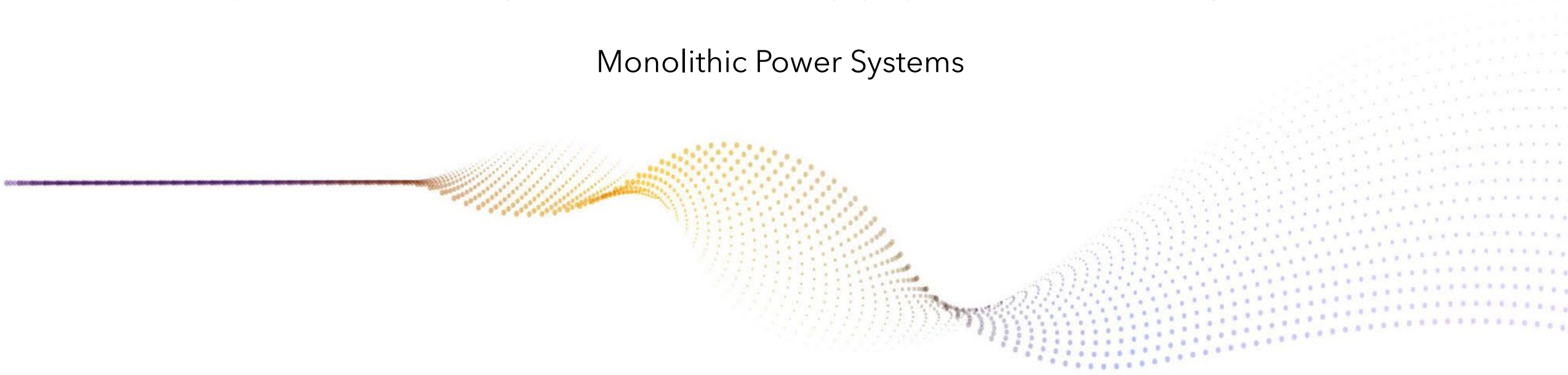


PMIC with Embedded SPDM + PQC

Collaboration for a future-ready, secure memory for automotive

Bill Gervasi, Principal Memory Solutions Architect (bill.gervasi@monolithicpower.com)
Junjian Zhao, Sr. Manager, Technical Marketing (junjian.zhao@monolithicpower.com)

Monolithic Power Systems



Thank you for attending!

Please remember to rate this session. You get access the presentations at
http://sniadeveloper.org/conference

