

Government Investment in Heterogeneous Integration

Jeff Demmin Sr. Lead Scientist Booz Allen Hamilton

September 11, 2019 demmin_jeffrey@bah.com

Image courtesy of Athena Group

🖉 Innovate Forward

Booz | Allen | Hamilton

Past

- -Background and history
- -DAHI (Diverse Accessible Heterogeneous Integration)
- Present
 - -CHIPS (Common Heterogeneous Integration and IP Reuse Strategies)
 - -ERI (Electronics Resurgence Initiative)

Future

- -Security and Trust Issues
- -MINSEC (Microelectronics Innovation for National Security and Economic Competitiveness)
- -SHIP (State of the art Heterogeneous Integrated Packaging)



Past



DARPA No "Perfect" Material

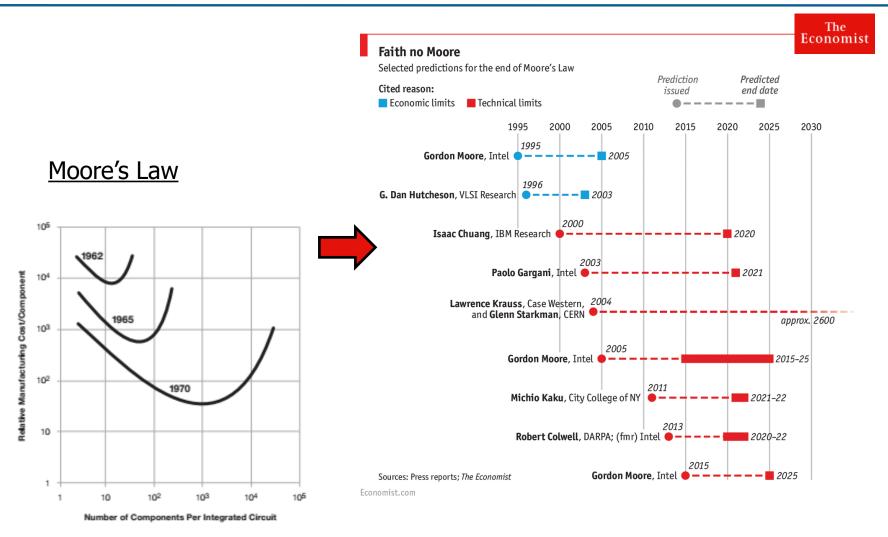
			←──	device r	materials	→	integration
Parameter	Why?	Unit	Si	GaAs	InP ¹	GaN ²	COSMOS / DAHI
Electron Mobility	Carrier velocity	10 ³ cm ² /V·s	1.4	8.5	12	<1	InP
V_{peak}	Transit time	10 ⁷ cm/s	1	2	2.5	2.5	InP / GaN
Е _{вк}	Voltage swing	10 ⁵ V/cm	5.7	6.4	4	40	GaN
Eg	Charge density	eV	1.12	1.42	0.74	3.4	GaN
к	Heat removal	W/cm·K	1.3	0.5	0.05	2.9	GaN / Si
Maturity	Circuit complexity		Excellent	Good	ок	Limited	Si + GaN + InP (heterogeneous)
DARPA Investment			~ \$100M	~\$600M	~\$200M	~\$300M	~\$180M
Programs			Portions of GRATE, ADRT, LPE, and TEAM	MIMIC	SWIFT, TFAST, THz Electronics, SMART	GaN Title III, WBGS- RF, NEXT, MPC, NJTT	COSMOS, DAHI

Materials and device parameters favor a diversity of semiconductors

- InGaAs channel 1.
- SiC substrate 2.



DARPA End of Moore's Law?



Changes in silicon industry will be felt by compound semiconductors

Source: Electronics Magazine, Economist.com



It may prove to be more economical to build large systems out of smaller functions, which are separately packaged and interconnected. The availability of large functions, combined with functional design and construction, should allow the manufacturer of large systems to design and construct a considerable variety of equipment both rapidly and economically.

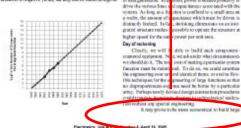
equivalent picce of sensiondar up in the equivalent outcase containing more components. But as components are adden



a two-mill square care also contain several hildness of resis- is economically justified taka or a few dieder. This allows at least 500 components - the thermocheanic rand when a molteration that offers test per linux lich or a quarter utilizes per square liefs. Thus, spetch in chemical rese, one, it is not even recession to do (5,000 component) and coupy only about one-fourth a may fundamental rescords or to replace present processes. igner: with On the allows water parents used, usual b as lock or

station pitters upstied by distoint films. Auch a density of components can be achieved by messed optical techniques and does not explore the none exacts techniques, and as effective hours operations, which are being tracked to sake over realize threchever.

increasing the yield.



The experts look ahead

Cramming more components onto integrated circuits

With unit cost failing as the number of components per circuit rises, by 1975 economics may dictate aqueezing as many as 65,000 components on a single silicon chip

By Gordon E. Moore Director: Research and Development Laboratories, Pair-Still Rentineedants ribial set of Patienhild Carriers and Instrument Corp.

The follow of integrated electronics, is the larger of electronits itself. The advantages of integration will bring should proliferation of electronics, pushing this selence into many HOW WIDE. Integrated circatio will lead to such worders to here: compaters-or at loss trematisally switted at a second com-

-automatic controls for parametrizes, and personal metable communication conference. The electronic writewards needs only a doplay to be liasible today. But the biggest potential lies in the production of lines.

term. In telephone communications, imagined clicult in digital fibers will asparate charate is on makipies aquipment. Energiated circuits will also awitch wisphone circuits and perform data proceeding.

Computers will be receiptiverful, and will be regarded in completely diffusion ways. For example, managing hait of integrated electronics may be distributed throughout the

The other The antibiot Dr. Conton F. Morea is none of the new town of machines, engineers, addressing of machines, internets of software share the descentes in twenting from the descentes of twenting from the descentes of twenting for the machine of the twenting for a descen-tes of the software of the descentes of twenting of the twenting of the dest Barriers are have assaulty have the divertor of the second hand

machine insign) of being concentrated in a q addition, the improved reliability made possible citatis will allow the construction of largers.

Machines shellar to these in existence today lower costs and with lister tem-around Present and Makes By integrated di tonics, I near all the authority which are referred to as microeleen

well as any additional error that result is a butions narolied to the user as bridgeble units. refugies were first investigated in the late 19. lest was to ministurize electronics e arises mi mutingly complex electronic functions in Inminimum weight. Several sportsches evelmicrossenthly techniques for individual con

(Tim structures and semiconductor magnitude) Each approach evolved rapidly and coneach borrowed includence from another. Many

ballane the way of the finance to be a combination our approaches. The advocates of services ductor integral already using the improved characteristics of it tion by applying such films directly to accertise tor substants. These advantating a technology films are developing applications discharges, meet of active presidential are devices to the p Both approaches have wavked well

in equipment to by

Electronics, Volume 35, Humber 8, April 18, 1915



G. E. Moore is one of the new breed of electronic engineers schooled in the physical sciences rather than in electronics. He earned a B.S. degree in chemistry from the University of California and a Ph.D. degree in physical chemistry from the California Institute of Technology. He was one of the founders of Fairchild Semiconductor and has been Director of the research and development laboratories since 1959

The establishment be serviced of a strategiestic destruction of the strategiest of the s almost mandatory for rervealitary systems, since the re-

hald fity, size and weight required by some of them is address. able only with integration. Such programs as Aprille, for manual more flight, have demonstrated the reliability of laregressed electronics by showing that complete classic fine-tions are as free from failure as the best individual maske-Milercompative in the commercial company field have

stachines in design or in early production employing im-grated abschurcks. These machines cost less and perform batter than these which are "conventional" electronics. instruments of variant sorts, especially the topicly inmaning sambers corploying digital tachs agon, are starting are integration because it can see to both manufacture and design

The use of linear integrated circadey is still restricted. primarily to the military. Such imagrated functions are nopersive and net available in the variety required to assistly a major function of linear electronics. But the first applications are bugineding to appear in construction electronics, par-ticularly in equipment, which useds have desparency simplifyen of level loop.

Rationality counts

In almost every case, integrated a sectorate, has denote strated high reliability. Door at the present level of production -- leve compared to that of discrete components -- it offor reduced systemic clot, and in many systemic improved performance has been realized.

Integrated electronics will make electronic techniques more generally available throughout all of society, performing course theoreticous that present is any done intellegisately by other techniques or not done at a l. The principal advantages will be lower unvis and greatly simplified design-payoffs from a much supply of low-cost functional packages Torrace applications, we conductor integrated circuits.

will predominate. Semiconductor devices are the only reacouble candidates presently in avidence for the active ele-ments of traggrand circuits. Pour te senicorductor elements look attractive too, because of their potential for low-past and high reflectifies, but they can be used only if propinion is not a price would be Silicon is likely to remain the basis material, although

afters will be of me in specific applications. For chargele, pillium amenide will be important in integrated crick Encilors. But silicon will predominate it lower treasencies because of the technology which has already evolved around it and its oracle, and because it is an abundant and relationly interpretation starting material.

Costs and curves

Reduced cost is one of the big stituctors of integrated electronics, and the unit advantage continues to increase or the technology evolves toward the production of larger and l'fonctions on a single services du lor substation larger classi For single a sould, the cost per commonset is usually invested. propertional to the merilest of components, the musit of the

Electronics, Velores 39, Number 5, April 10, 1983

Daily He organization of a transmission of the series desired regarded an an more in diameter, deve to apple some for such a structure of conversely loss the even such repeative. Today ordinary to to components can be closely picked within space wisked. I toprated circuits are must with yields comparable with those In terminate the enderso. The terminate since effects is unitated for indicated even valuate cleaners. The same where a level of complexity above the presents available pattern will make large mus communed, if other bunned mergered crimits are stready underway using multilator - analises make such area - Gavinable Plast problem Will here reasolities move the here generated by tem of thousands of comparents in a single all servicing? If we could strick to volume of a standard high-speed digital compare to that experted for the components themsalves, no would apport the glow bright is with present perver There is no functioneral clusted to advecting density jublic of 100%. At present, packaging cents to far exceed Since imaginized clusters are two dimensional. The exist of the sense output or devices it of that here is not they have a sufficienced. It is for costing does to such order is costing to improve yields, but they can be main it a high as the fraction prover is model priority to

No berier exists comparable to

ingmind area ins. when yields were

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

10

-

decreased yields more than compensate for the in

complexity, tending to mise the cost per comp-

there is a minimum cost at any given time in the s the instructory. At present, it is reached when I

rents are used per circuit. But the annianam is ro

while the estimated or reaction in the property look sheed five years, a plot of costs suggests the

recent doubt new component reliably he exceeded in a

about 1,000 components per circuit (providing o fauctions can be employed in residents must due.

the manufacturing cost per component can be ex-

The complexity for minimum comprised a

counsed at a usic of rangity a Gatar of two per

graph on west page). Cartainly over the shorttee

can be expected to continue, if set to increase

former term, the taxe of increase is a bit more tax

though there is no issues to believe it is ill not rea-

constant for at least 10 years. Their researchy 1977

her of composents per mergrated circuit lise many

I believe that such a large cleased survive bailt

With the dimensional tubescore sites dy being

can be built on content two thermaniths of an inch of

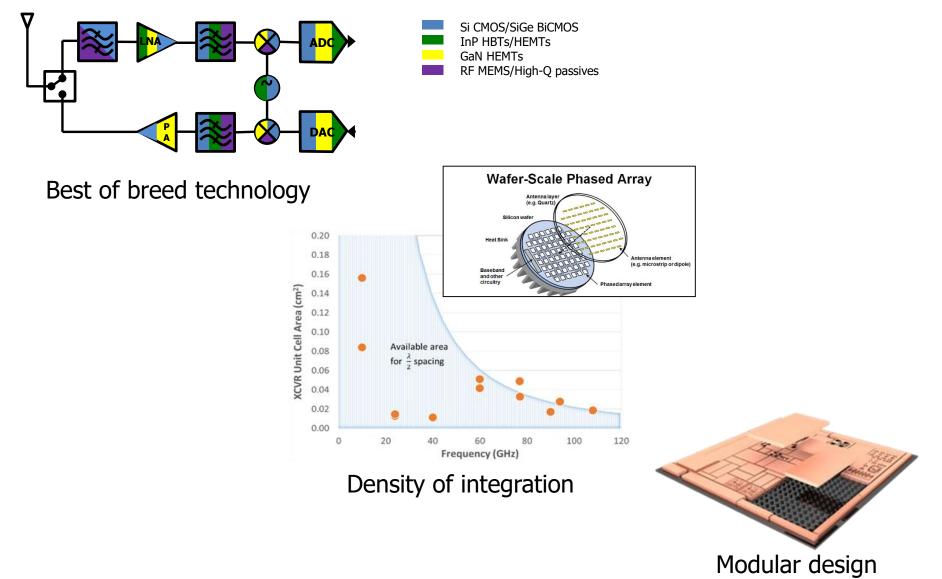
rangestand circuits, in slatted high-partie

carls a tanih of the present and,

101210-05-000

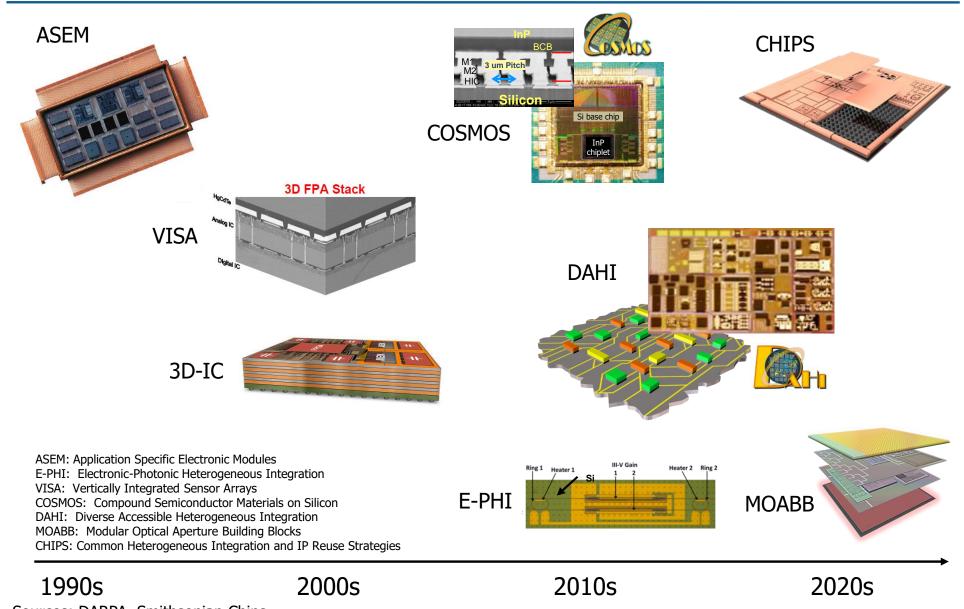


Why Heterogeneous Integration?





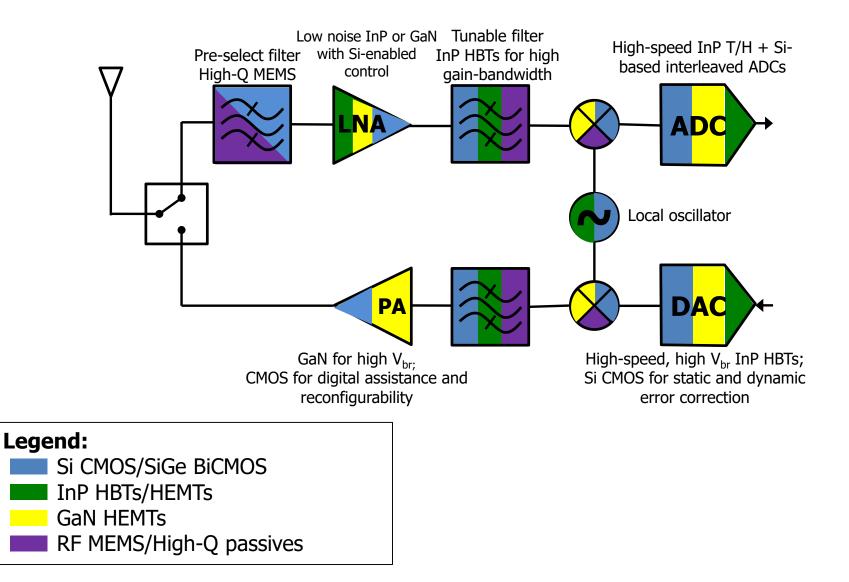
DARPA's long history of innovation in integration



Sources: DARPA, Smithsonian Chips Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

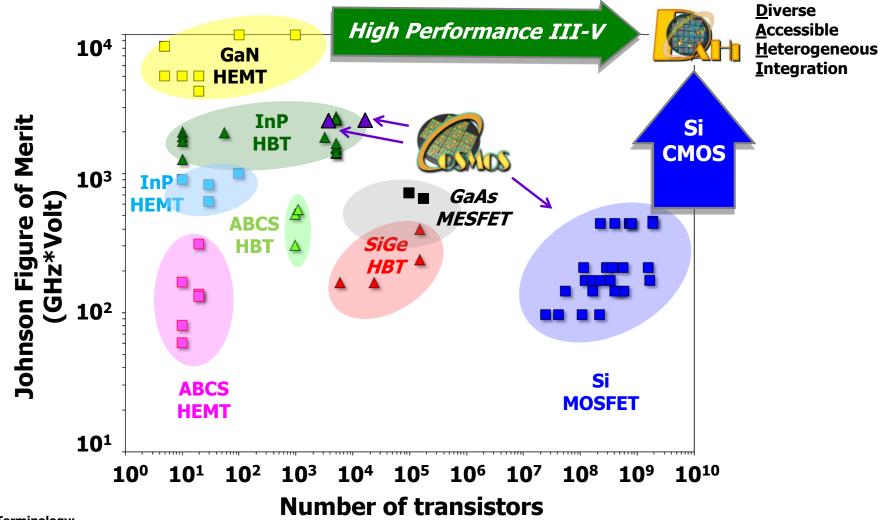


Vision for Representative Transceiver: 4+ Device Technologies





Heterogeneous Integration: DAHI Broadens the Device Material Options

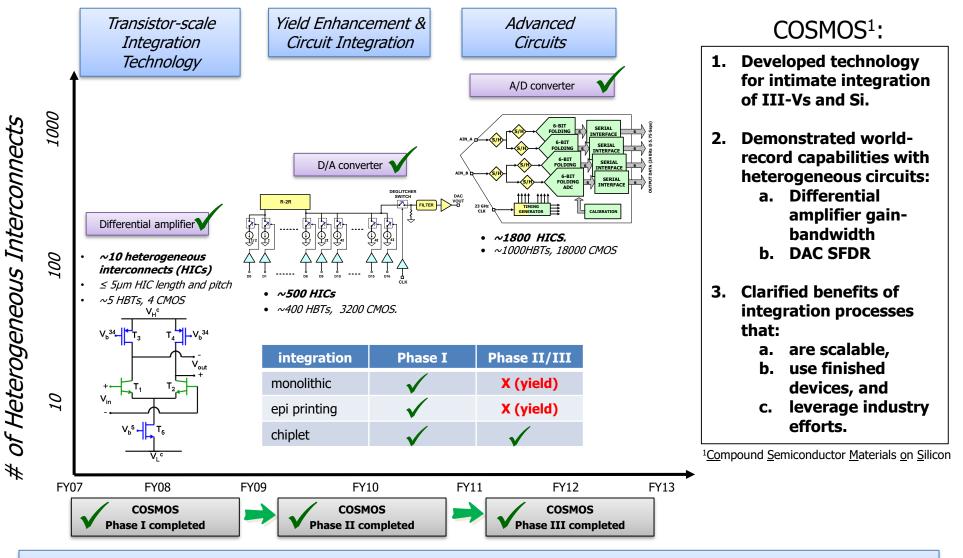


Terminology:

InP = indium phosphide, GaN = gallium nitride, SiGe = silicon germanium, ABCS = antimonide-based compound semiconductor HBT = heterojunction bipolar transistor, HEMT = high electron mobility transistor, CMOS = complementary metal oxide semiconductor COSMOS = Compound Semiconductor Materials on Silicon



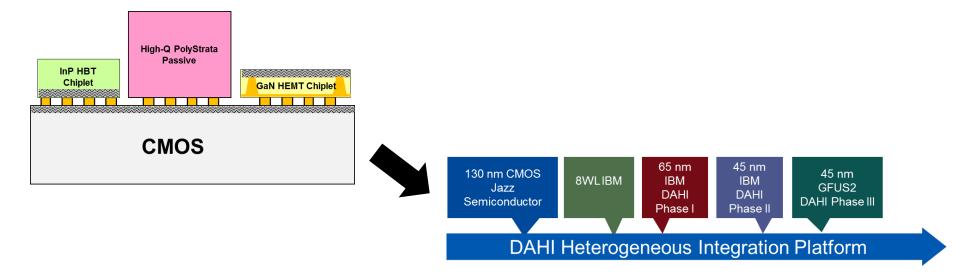
COSMOS Program Showed the Promise of Heterogeneous Integration

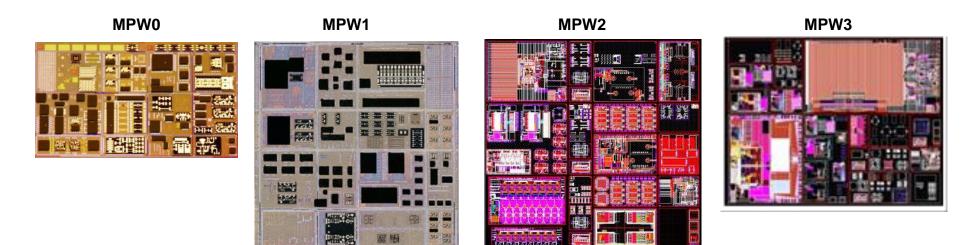


Phase II/III: Demonstrated benefits of integration of completed devices.



DARPA's DAHI program: Silicon CMOS as integration platform





Sources: DARPA, Northrop Grumman



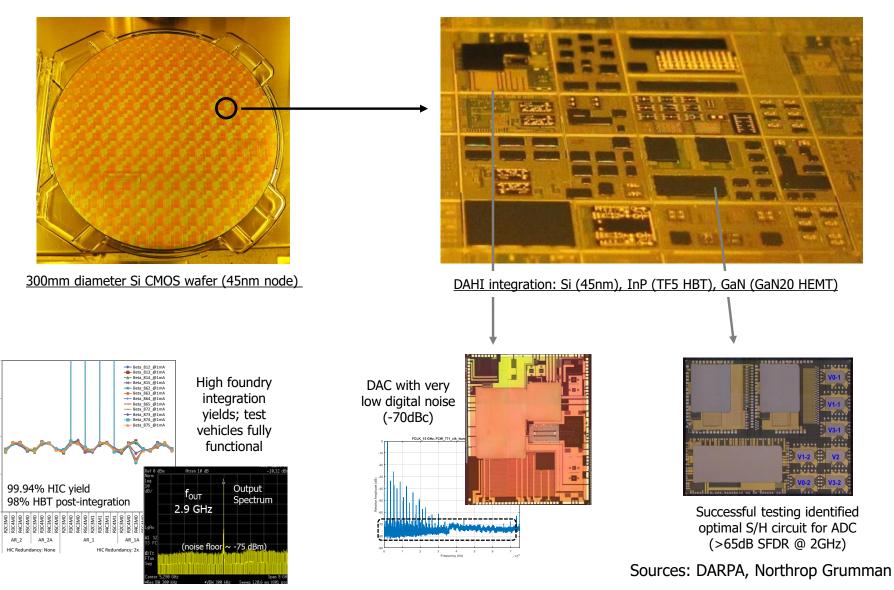
60

HBT Array - Beta at 1mA 6

20

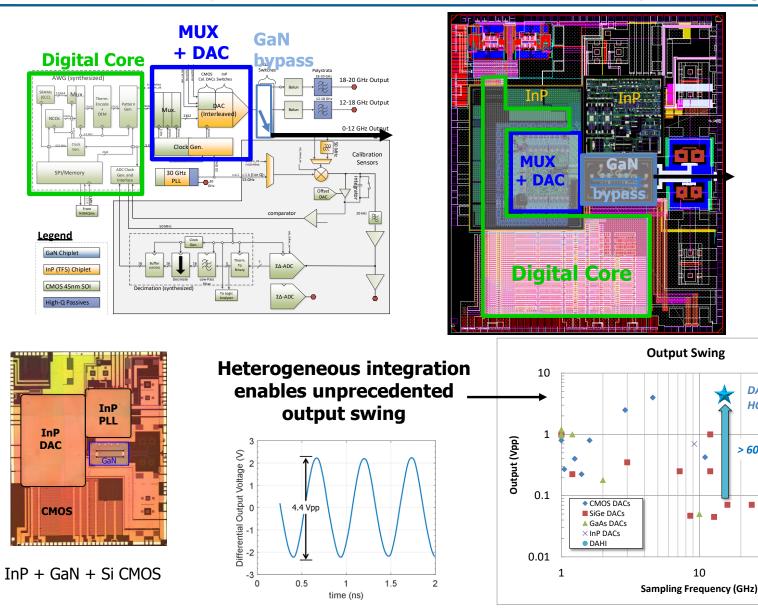
DAHI snapshot: Excellent yield, demonstrated RF performance







DAHI MPW1: Arbitrary Waveform Generator Enabled by Heterogeneity



Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

100

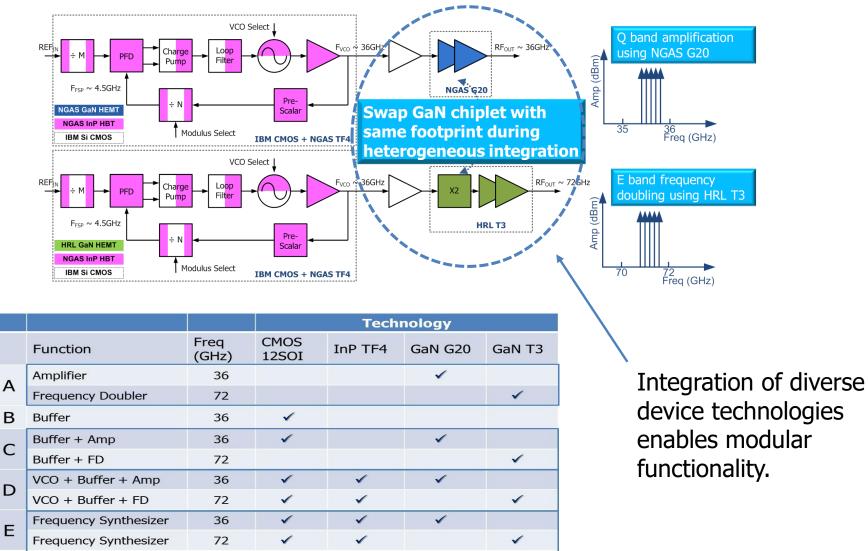
DAHI HOTSOS

> 60X

10



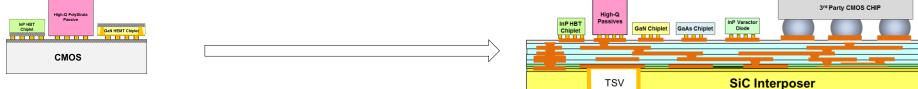
MPW1 Q/E Dual Band Frequency Synthesizer (36 and 72 GHz)





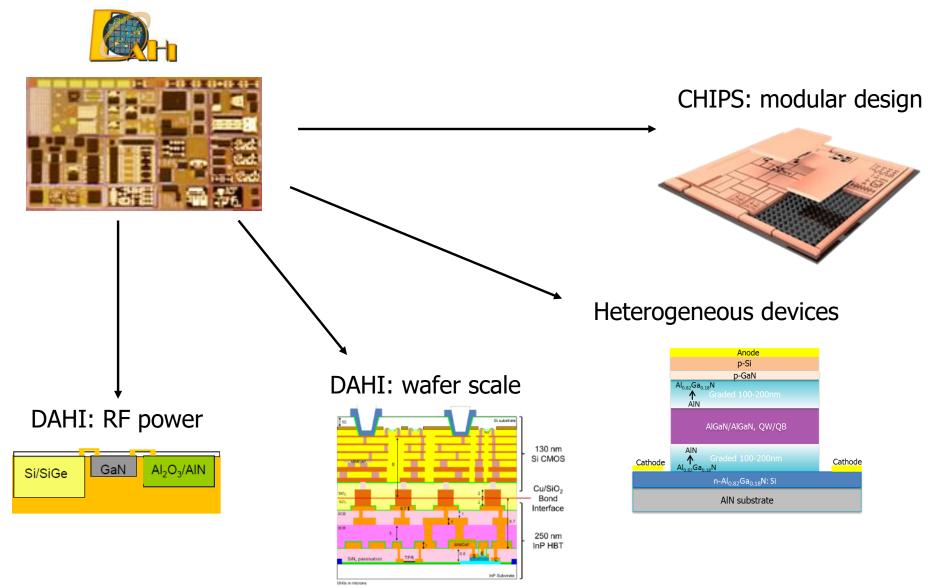
DARPA DAHI simplicity enables rapid evolution

GF 45 nm TF4 (4 metals) TF5 (4 metals) GaN20 T3 (HRL) P3K6	GF 45 nm TF4 (4 metals) TF5 (4 metals) AD1 GaN20 T3 (HRL) P3K6
TF5 (4 metals) GaN20 T3 (HRL)	TF5 (4 metals) AD1 GaN20 T3 (HRL)
GaN20 T3 (HRL)	AD1 GaN20 T3 (HRL)
T3 (HRL)	GaN20 T3 (HRL)
T3 (HRL)	T3 (HRL)
. ,	
P3K6	D21/6
	PSKU
PolyStrata (Nuvotronics)	PolyStrata (Nuvotronics)
CMOS	CMOS
SiC (IWP5)	SiC (IWP5)
	(in design)



Sources: DARPA, Northrop Grumman

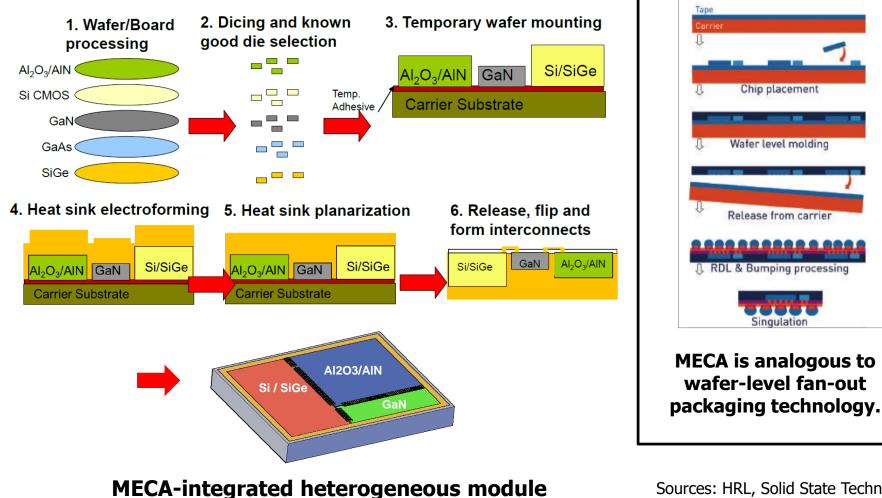




Source: DARPA



MECA enables heterogeneous integration with a metal interconnect platform for high-power requirements.



Sources: HRL, Solid State Technology

Singulation

SIMPLE FAN-OUT WLP PROCESS FLOW Chips are embedded in a mold compound

Chip placement



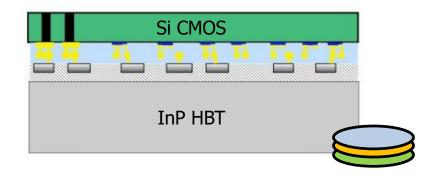
Heterogeneous integration for mm-wave: **Phased array beamformers**

- Can maintain $\lambda/2$ channel spacing as frequencies increase
- CMOS control circuitry closely integrated with RF chain •
- Improved channel performance and efficiency with addition of III-V devices
- Fully integrated beamformer channels demonstrated with integrated InP devices and Si control electronics

Integration schematic

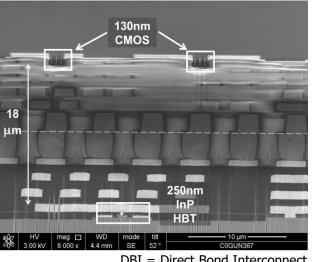
>100mW Pout Tx channel, 4.5 dB NF Rx

Wafer-level heterogeneous integration



Si substrate 130 nm Si CMOS Cu/SiO₂ Bond Interface 250 nm InP HBT TER SiN, passivation InP Substrate

InP/CMOS with DBI Process

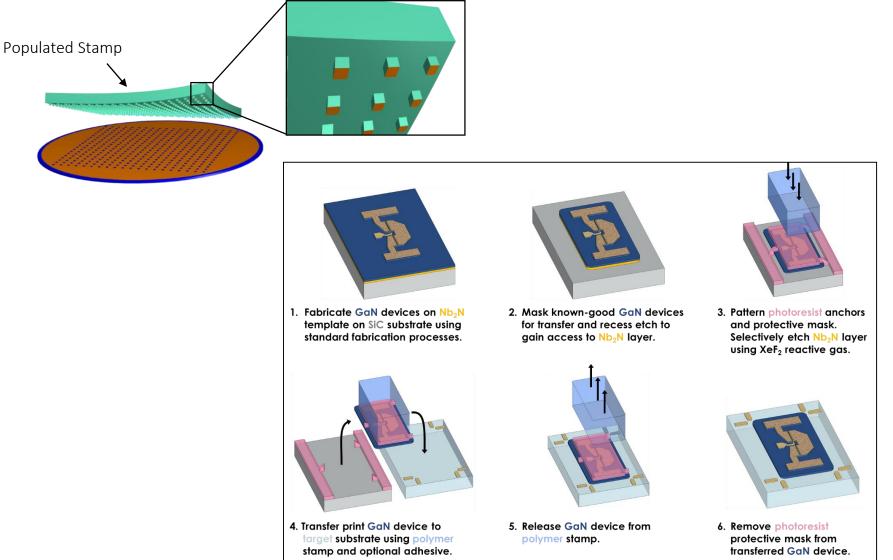


DBI = Direct Bond Interconnect

Units in microns



Microtransfer Printing



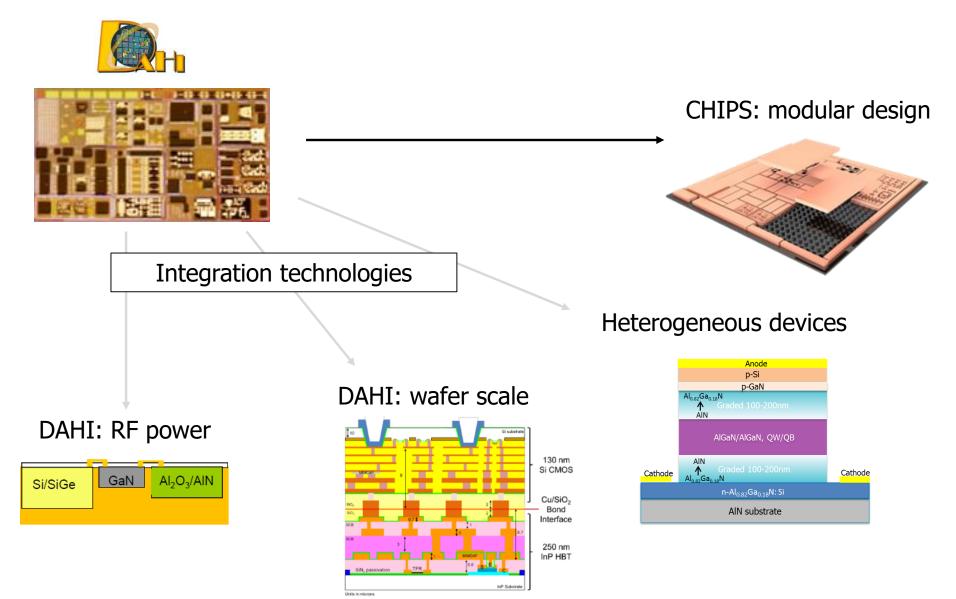
Source: Naval Research Laboratory Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)



Present



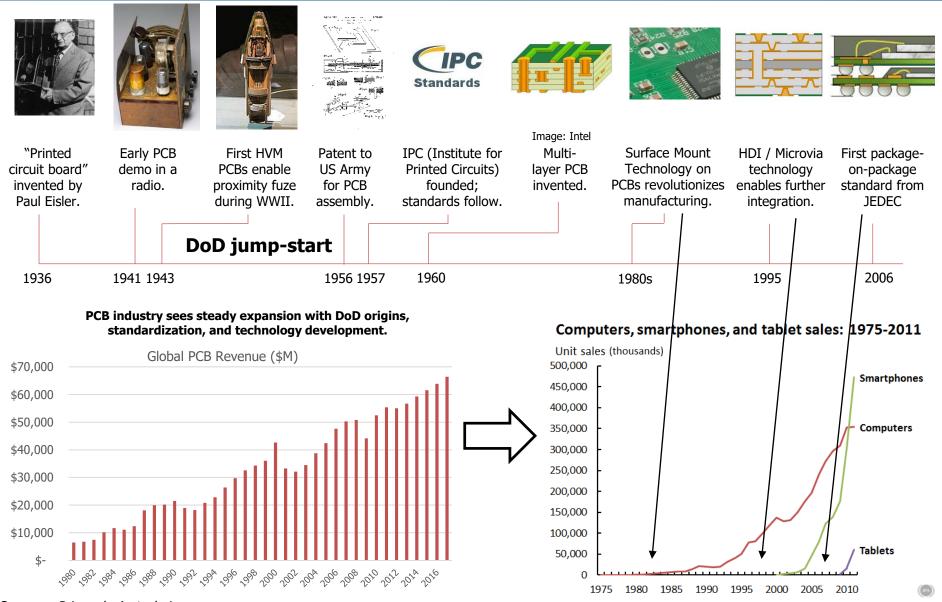
Common Heterogeneous Integration and IP Reuse Strategies: CHIPS as the next step in heterogeneous integration



Source: DARPA



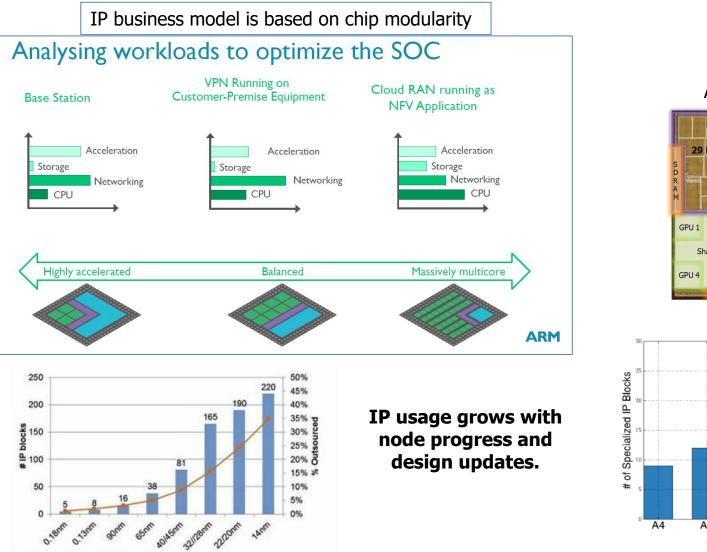
Integration impact driven by **Standards** and **Modularity**



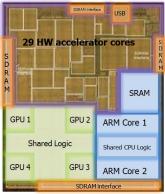
Sources: Prismark, Arstechnica, USPTO, Wikipedia, IPC, SMTA

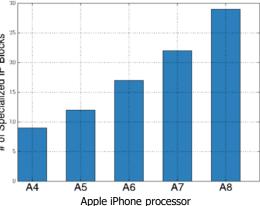


Modularity Already in Place at Monolithic Level



Apple A8





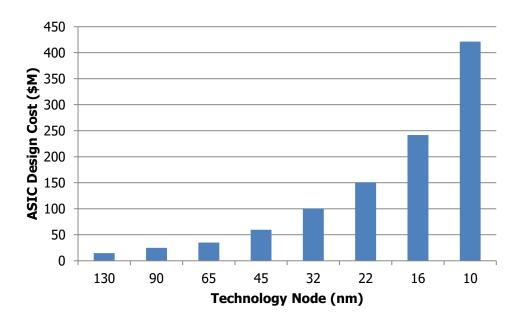
Modular semiconductor IP reduces chip design effort (time AND cost)

Sources: Cadence; ARM, Chipworks, Harvard



Expensive to design at advanced nodes ...

... which some commercial products can support ...





 $\ensuremath{\textcircled{}}$ apple.com

Fab cost for commercial electronics amortized over **one day's** worth of iPhones

... but DoD cannot.

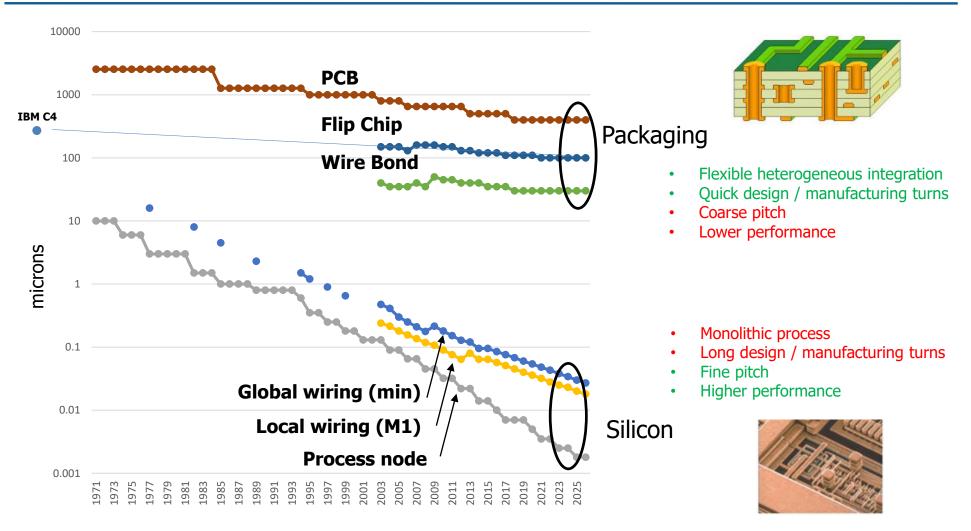


Fab cost for a DoD IC amortized over **entire 29 year** acquisition of JSF

Source: "Cashing in with Chips" AlixPartners Semiconductor R&D outlook report, 2014.



Conventional Assembly Has Attractive Features Too ... But Isn't Keeping Up on Pitch and Performance

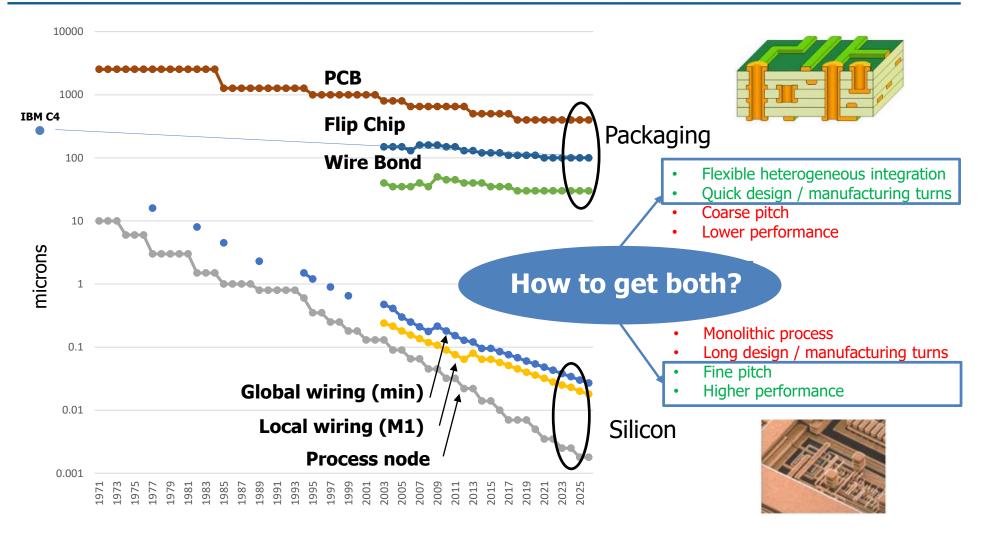


Need to combine speed and flexibility of packaging with pitch and performance of advanced heterogeneous device technology.

Source: 2003-13 ITRS, Wikipedia Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)



Conventional Assembly Has Attractive Features Too ... But Isn't Keeping Up on Pitch and Performance



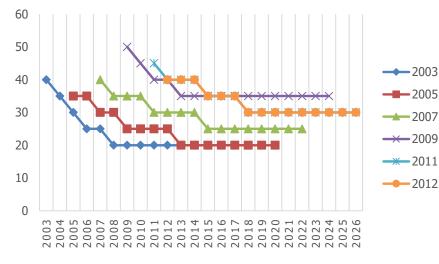
Need to combine speed and flexibility of packaging with pitch and performance of advanced heterogeneous device technology.

Source: 2003-13 ITRS, Wikipedia Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

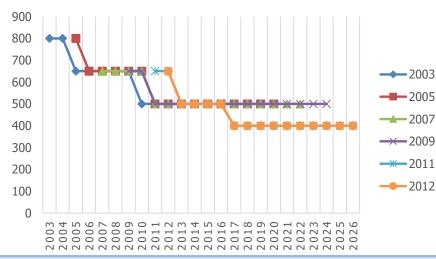


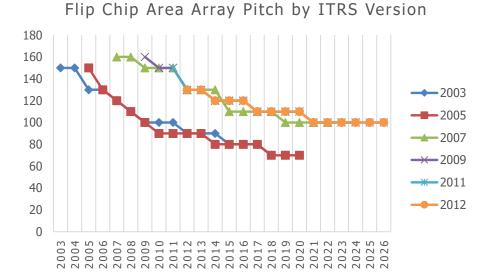
Interconnect Pitch Progress Has Lagged Projections

Wire Bond Pitch by ITRS Version



PCB Solder Ball Pitch by ITRS Version





Notes:

- 1. Dimensions in microns.
- 2. Wire bonding:
 - a. Discontinuity in 2009 due to shift to Cu as mainstream wire material.
 - b. Data is for "single in-line." Multi-tier first appeared in 2005 roadmap.

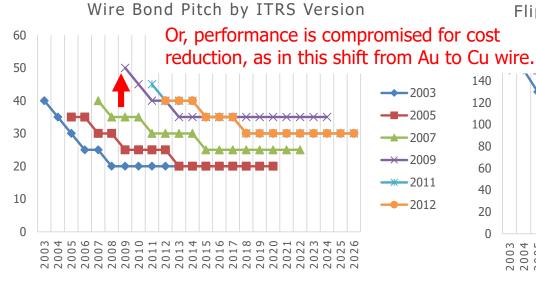
3. Flip chip:

- a. Discontinuities due to shifting ITRS product/application categories.
- b. Data is for "GPU/CPU/Chipset" in 2007, "high-performance" in 2009, and "cost-performance" in 2011-12.
- 4. PCB:a. Data is for "cost-performance" category.
 - b. Data is for "conventional system board" application starting in 2007.

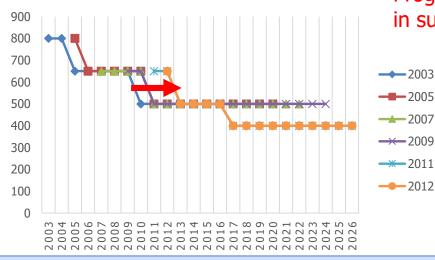
Can address the growing interconnect gap with standardized, fine pitch interconnects.

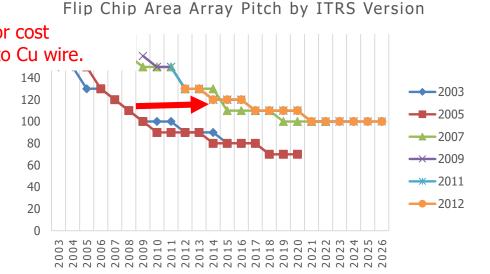


Interconnect Pitch Progress Has Lagged Projections



PCB Solder Ball Pitch by ITRS Version





Progress is typically pushed out in subsequent roadmap updates.

- Notes:

 Dimensions in microns.
 Wire bonding:

 Discontinuity in 2009 due to shift to Cu as mainstream wire material.
 Data is for "single in-line." Multi-tier first appeared in 2005 roadmap.

 Flip chip:

 Discontinuities due to shifting ITRS product/application categories.
 Data is for "GPU/CPU/Chipset" in 2007, "high-performance" in 2009, and "cost-performance" in 2011-12.

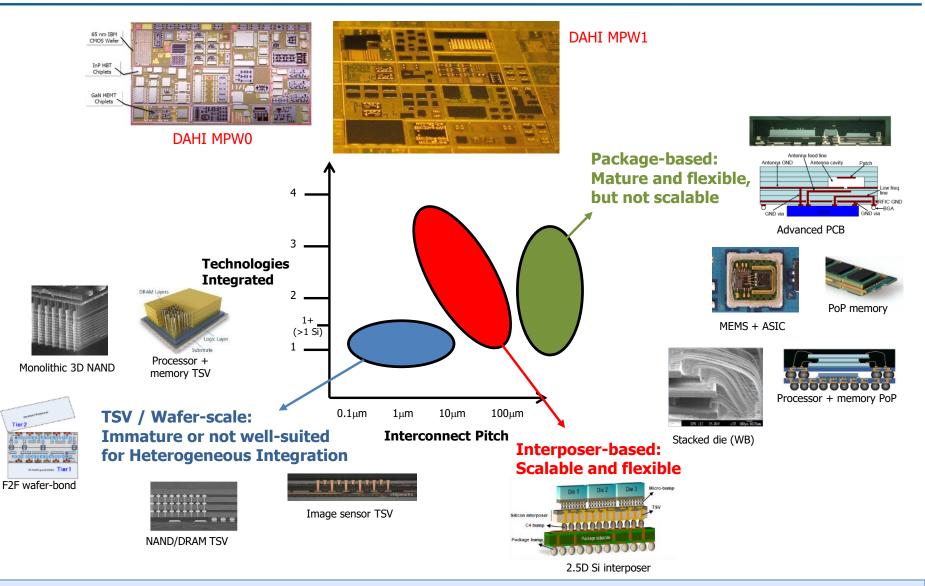
 PCB:

 Data is for "cost-performance" category.
 - b. Data is for "conventional system board" application starting in 2007.

Can address the growing interconnect gap with standardized, fine pitch interconnects.



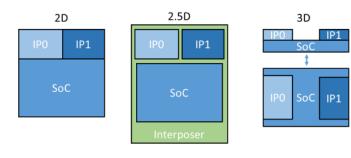
Heterogeneous Integration: Bridging the Gap



DAHI creates integration capabilities beyond current advanced interconnect technologies.



Case Study Scenario



Die size

Power

Many factors affect optimal integration approach:

- size of IP blocks
- % IP reuse
- licensing cost
- die size

2.5D is the best

option for high

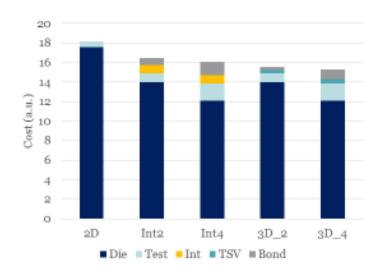
power density

designs

Die size

Die size

- process yield / maturity
- relative cost of nodes
- power / cooling options
- gate count



The die cost dominates, independent of integration approach, so chip cost reduction via IP reuse is beneficial in all scenarios.

2.5D is typically the best option for high power, high complexity designs.

Cost

2D is the best

option for small designs

(<100mm²)

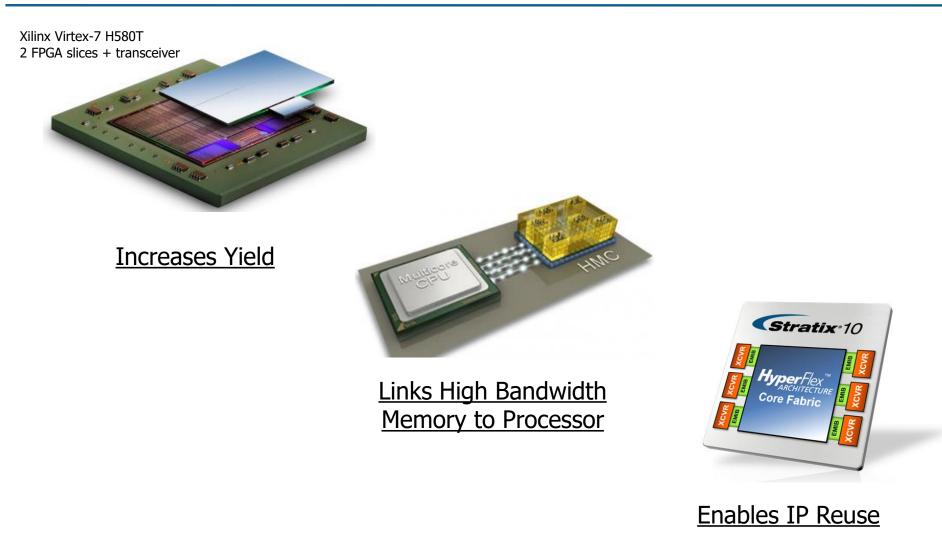
3D

Die size

2D

2.5D





But everything is a point solution!

Sources: EETimes / Xilinx, Extremetech / HMC, Altera/Intel

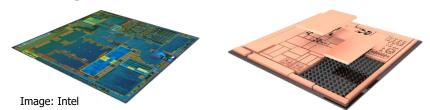


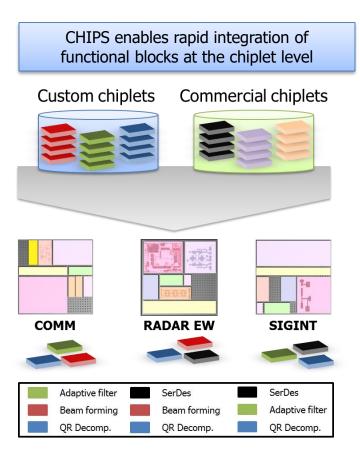
What is CHIPS?

CHIPS will develop design tools, integration standards, and IP blocks required to demonstrate modular electronic systems that can leverage the best of DoD and commercial designs and technology.

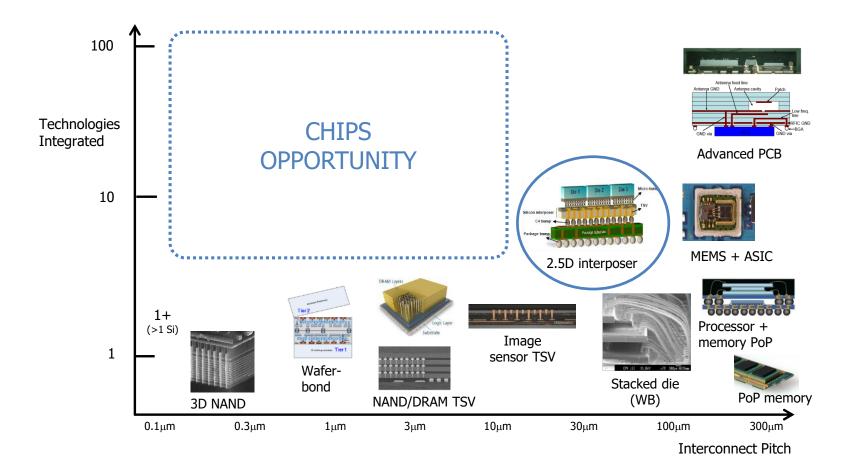


Today – Monolithic Tomorrow – Modular

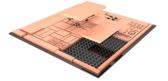


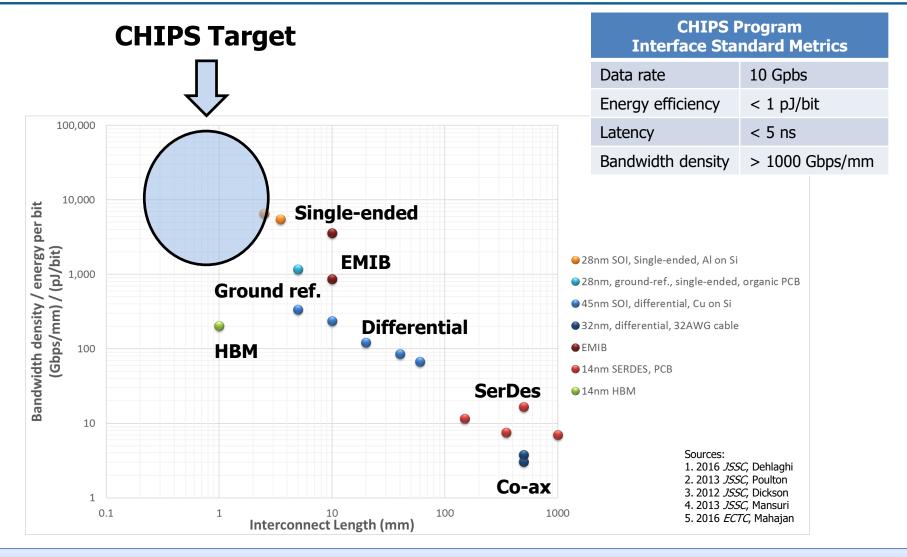








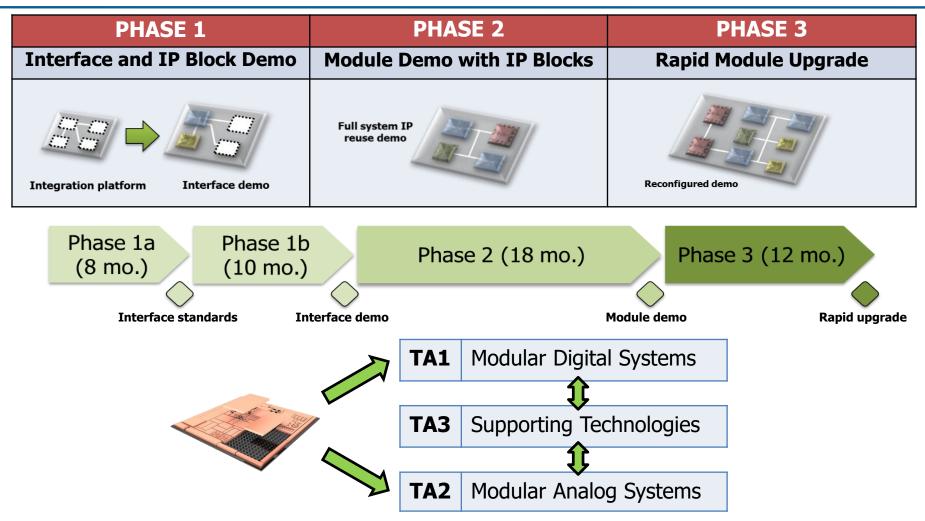




CHIPS interface is one of many possible routes for efficient interdie communications



CHIPS program: structure and timing



Seeking CHIPS collaboration to help drive a common interface

Source: DARPA

DARPA CHIPS: August 2017 Kickoff



CHIPS Team

- Boeing
- Intel

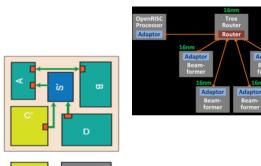
Designs

Chiplets

Tools

- Lockheed Martin
- Northrop Grumman
- Univ. of Michigan
- Intrinsix
- Jariet
- Micron
- North Carolina State
- Synopsys
- Cadence
- Georgia Tech

CHIPS Approach Modularity Standards



Substrate with EMIB Option

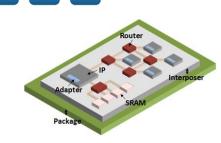
Stratix 10 FPGA die 14nm









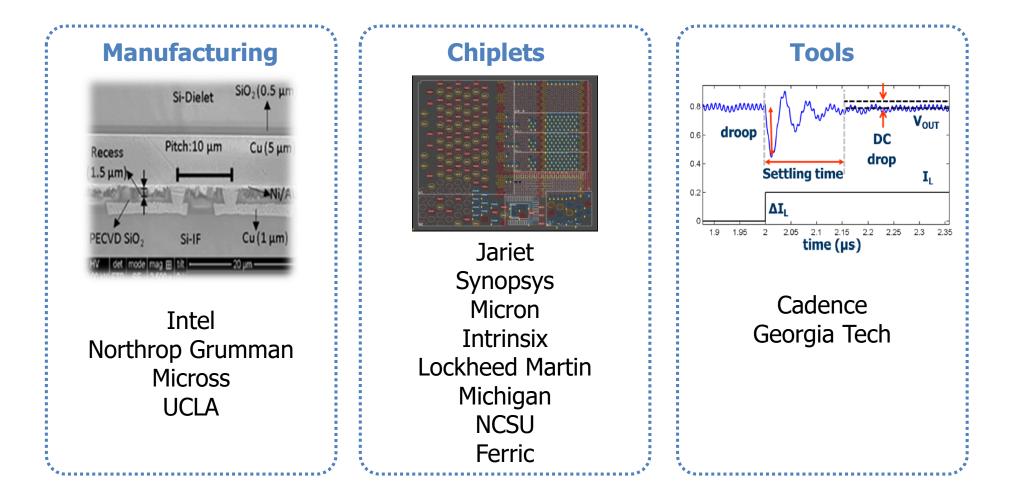


Images sources: Lockheed Martin, Boeing, Intel, Intrinsix, Univ. of Michigan, 3GPP.org

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)



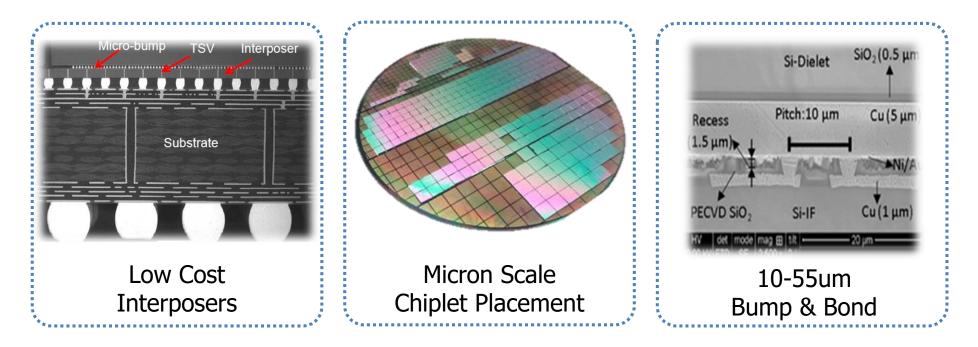
DARPA CHIPS Performer Summary





Current Focus of CHIPS: Interface Standard and Manufacturing

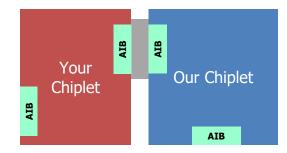




CHIPS is targeting solutions suitable for low volume (<100K units) trusted manufacturing needed for national security requirements.



- AIB (Advanced Interface Bus) is a PHY-level interface standard for high bandwidth, low power die-to-die communication
 - AIB is a clock-forwarded parallel data transfer like DDR DRAM
 - High density with 2.5D interposer (e.g., CoWoS, EMIB) for multi-chip packaging
 - AIB is PHY level (OSI Layer 1)
 - Can build protocols like AXI-4 or PCI Express on top of AIB
- **AIB Promoters** agreed to promote AIB as a die-todie interface standard
- Public information available from Intel at: <u>https://intel.ly/2LISZcr</u>



ADC/DAC Machine Learning Memory Processors Adjacent IP Etc. ...







- **Modularity**: A ubiquitous chiplet interface standard "Ethernet for chiplets"
- **Speed**: Board manufacturing time scales (days) possible with a library of hundreds of COTS chiplets
- **Performance**: 1pJ/bit and 1Tbit/mm WILL disrupt the computing landscape
- **Security**: CHIPS disaggregation offers a pathway to high assurance electronics



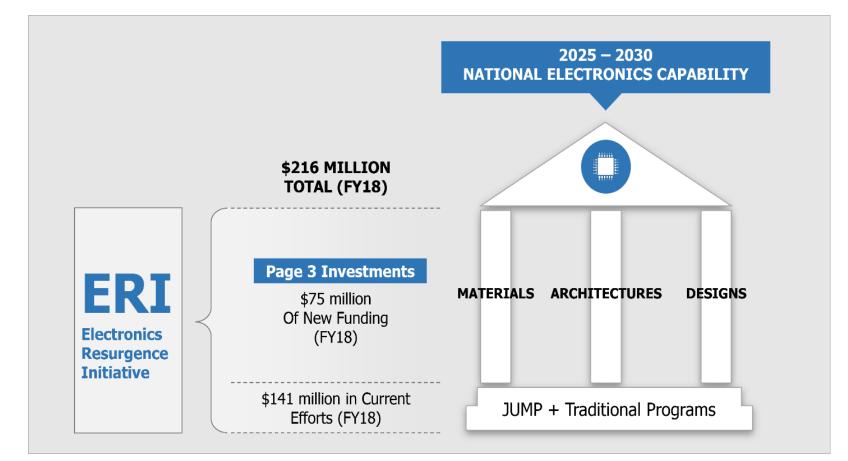


DARPA MTO Electronics Resurgence Initiative

Most presentations from the July 2018 and July 2019 ERI Summits are available as links from the agenda pages: http://www.eri-summit.com



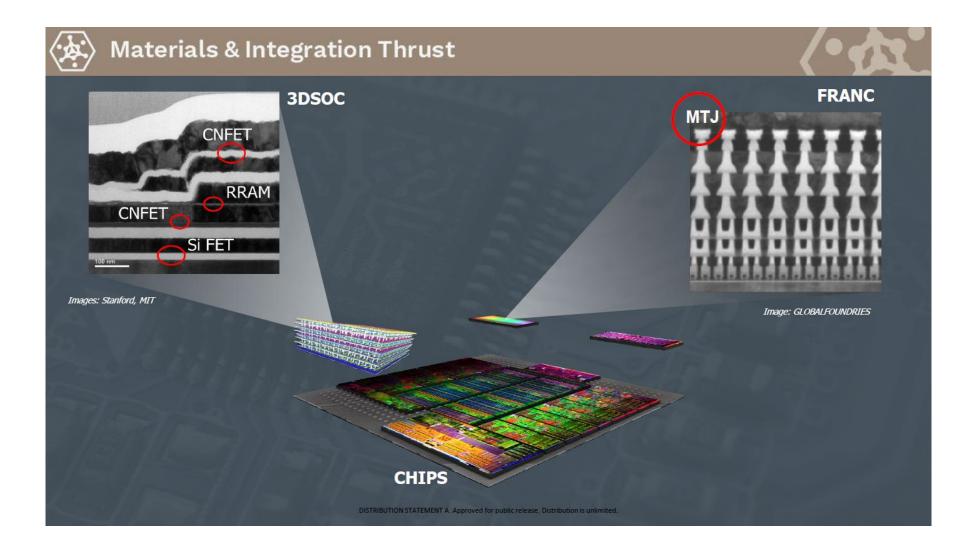
- ERI—creating an electronics capability that will provide a foundational contribution to national security
- Three thrust areas: Materials and Integration, Architectures, Designs





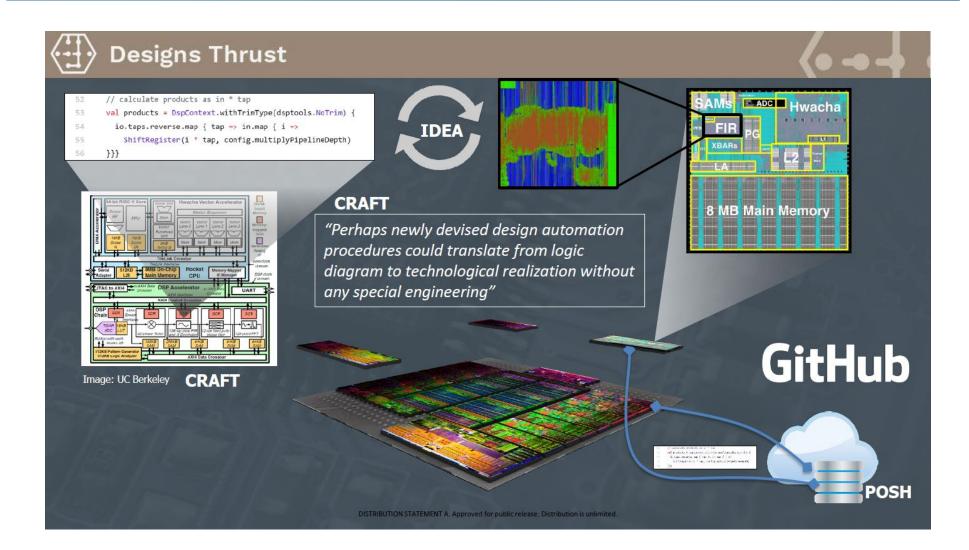
172 THE FUTURE OF COMPUTING PREDICTION	AMINUM C	VIII. DAY OF RECKONING
<page-header><text><figure><figure><figure><figure><figure><figure><text><text><text><text><text><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></figure></figure></figure></figure></figure></figure></text></page-header>	ents	Clearly, we will be able to build such component- crammed equipment. Next, we ask under what circumstances we should do it. The total cost of making a particular system function must be minimized. To do so, we could amortize the engineering over coveral identical items, or evelve flexible te evolve flexible techniques for the engineering of large functions in the total cost of the expense need be borne by a particular array. Dechaos evelved design automation procedures could translate from logic diagram to technological realization special engineering. It may prove to be more economical to build large systems out of smaller functions, which are separately packaged for combined with functional design and construction, should allow the manufacturer of large systems to design and construct a considerable variety of equipment both rapidly and economically.
Architecture Maximizing specialized functions	Design Quickly enabling specialization	Materials & Integration Adding separately packaged novel materials and using integration to provide specialized computing





Bill Chappell, DARPA ERI Summit, July 2018



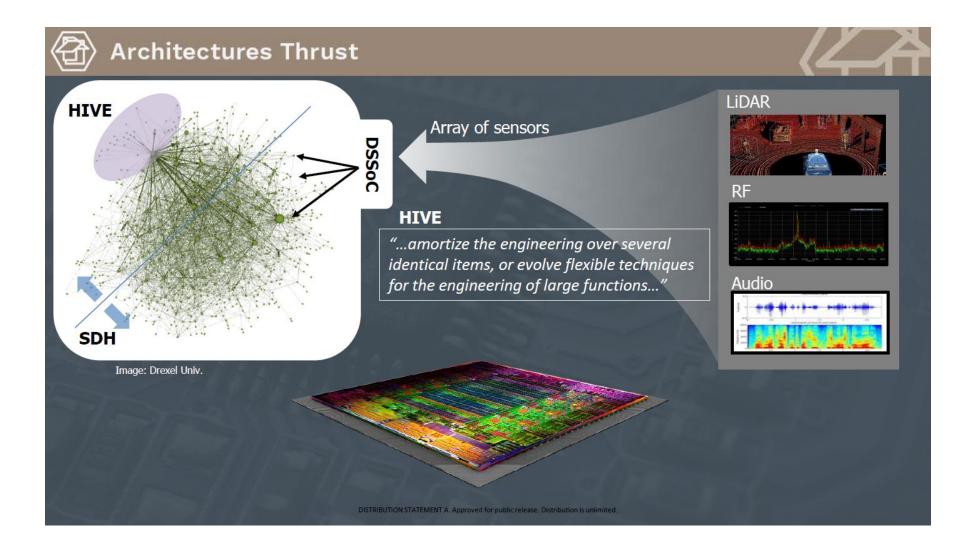


Bill Chappell, DARPA ERI Summit, July 2018

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

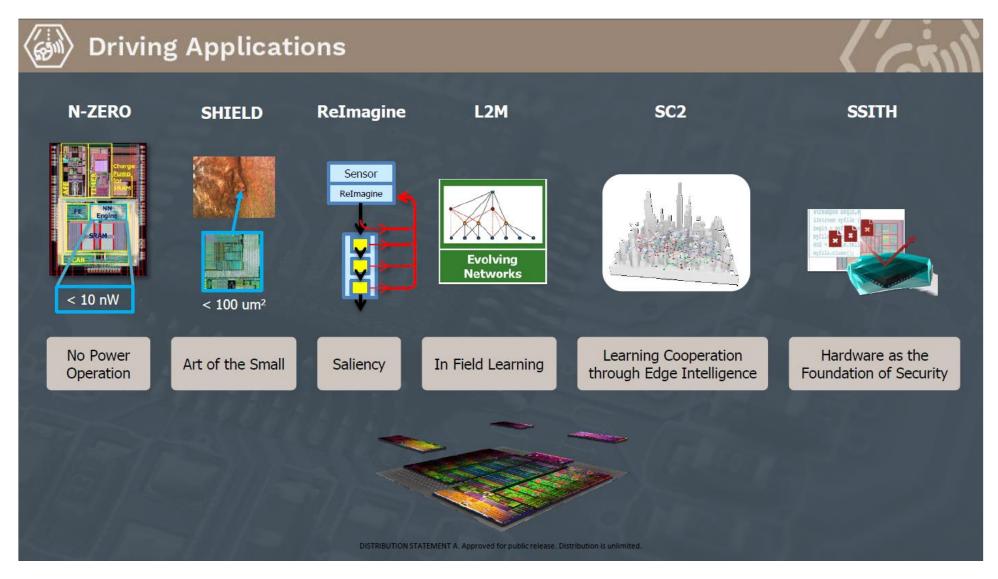


DARPA ERI Architectures



Bill Chappell, DARPA ERI Summit, July 2018





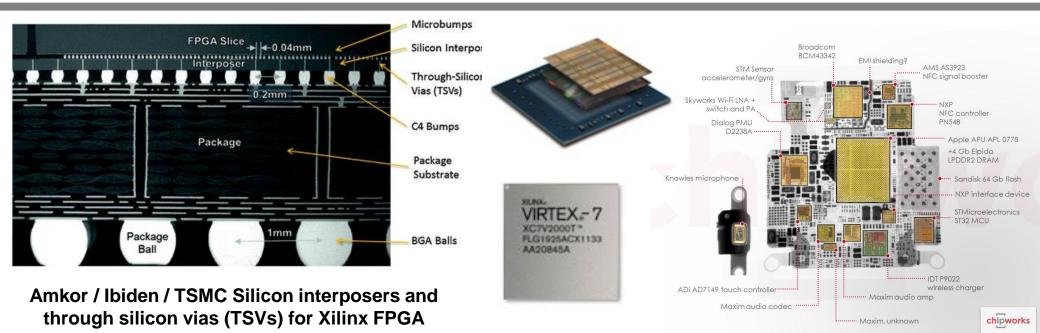
Bill Chappell, DARPA ERI Summit, July 2018

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)



Future

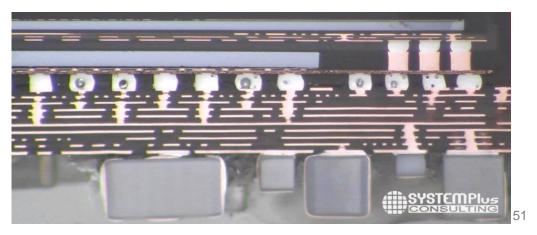
Semiconductor Packaging Landscape: Examples of leading edge capabilities available at commercial scales



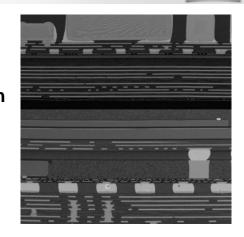
•

0

TSMC Integrated fan-out (InFO) packaging of A10 processor in iPhone7

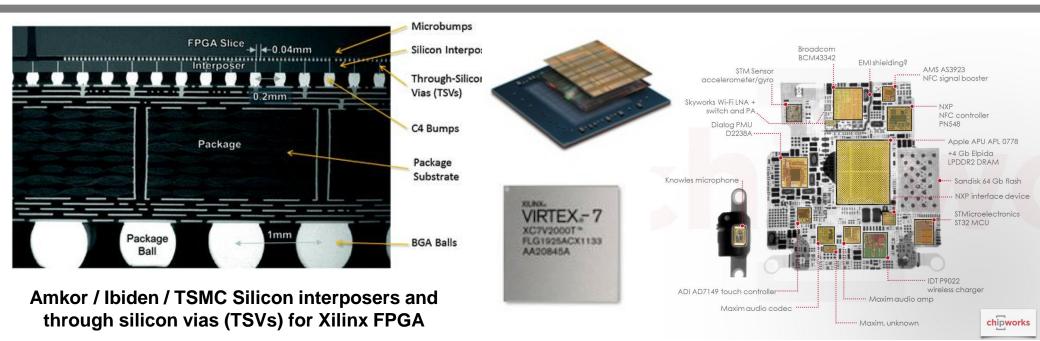


ASE System-in-Package in Apple Watch



Booz | Allen | Hamilton

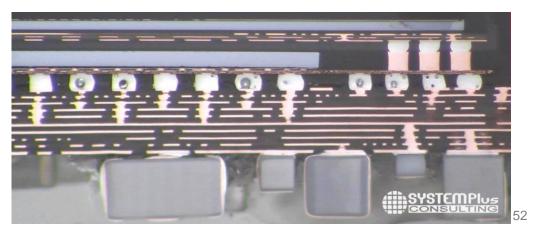
Semiconductor Packaging Landscape: Examples of leading edge capabilities not available to the DoD



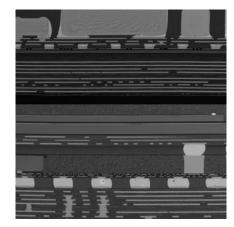
•

0

TSMC Integrated fan-out (InFO) packaging of A10 processor in iPhone7

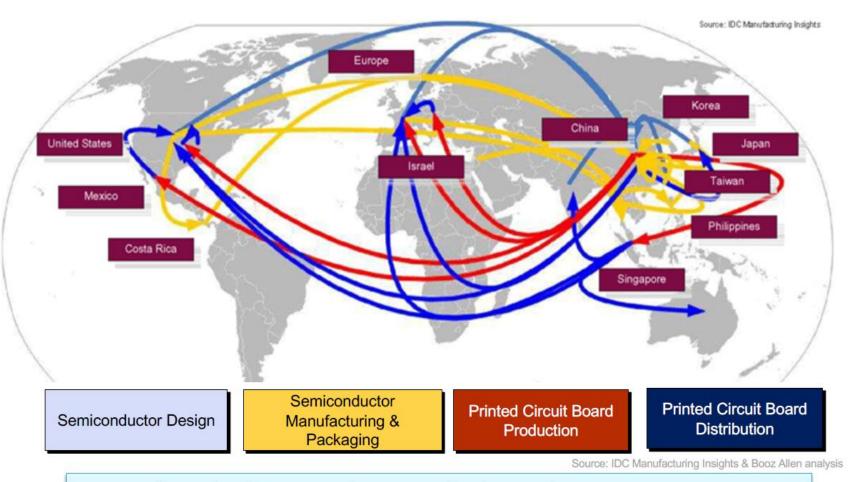


ASE System-in-Package in Apple Watch



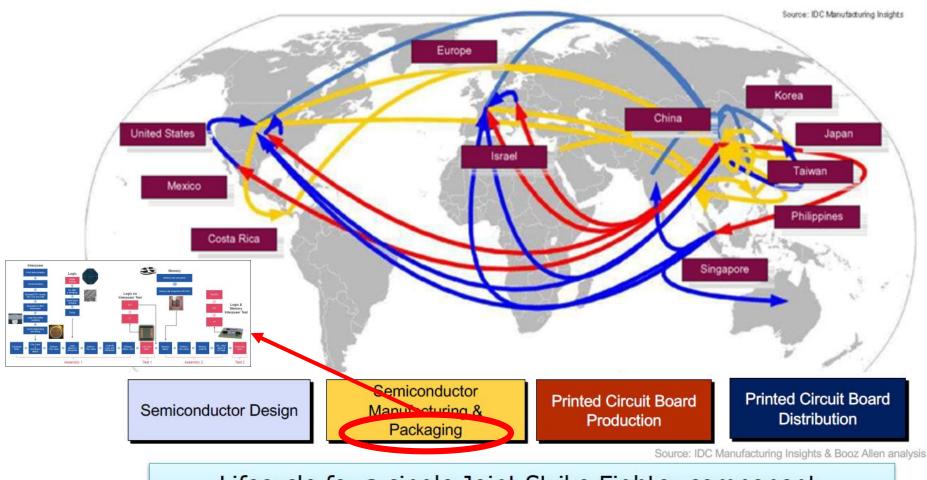
Booz | Allen | Hamilton

Electronic Manufacturing Supply Chain: Unavoidably international, even for DoD



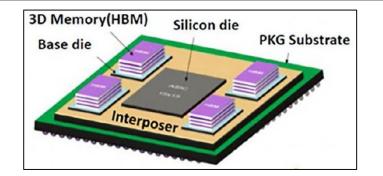
Lifecycle for a single Joint Strike Fighter component, which changes hands 15 times before final installation

Electronic Manufacturing Supply Chain: Unavoidably international, even for DoD

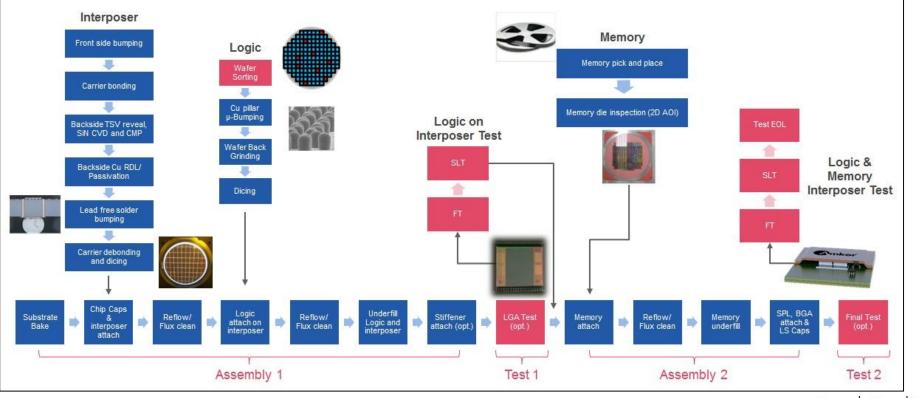


Lifecycle for a single Joint Strike Fighter component, which changes hands 15 times before final installation

Semiconductor Assembly Example (2.5D HBM)



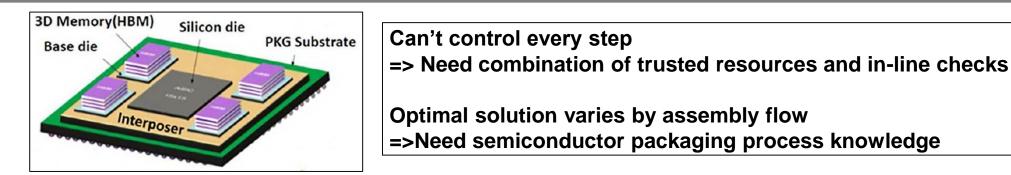
How many people have access throughout the supply chain?

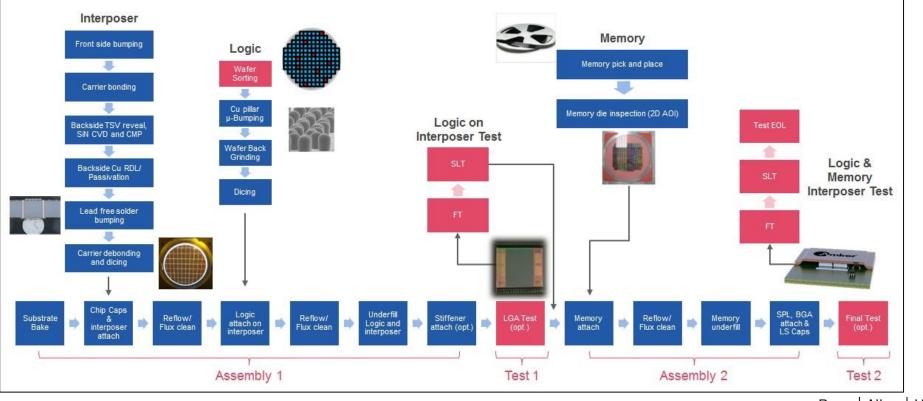


55

Source: "Start Your HBM/2.5D Design Today," SK Hynix, Amkor, eSilicon, Northwest Logic, Avery Design, 2016.

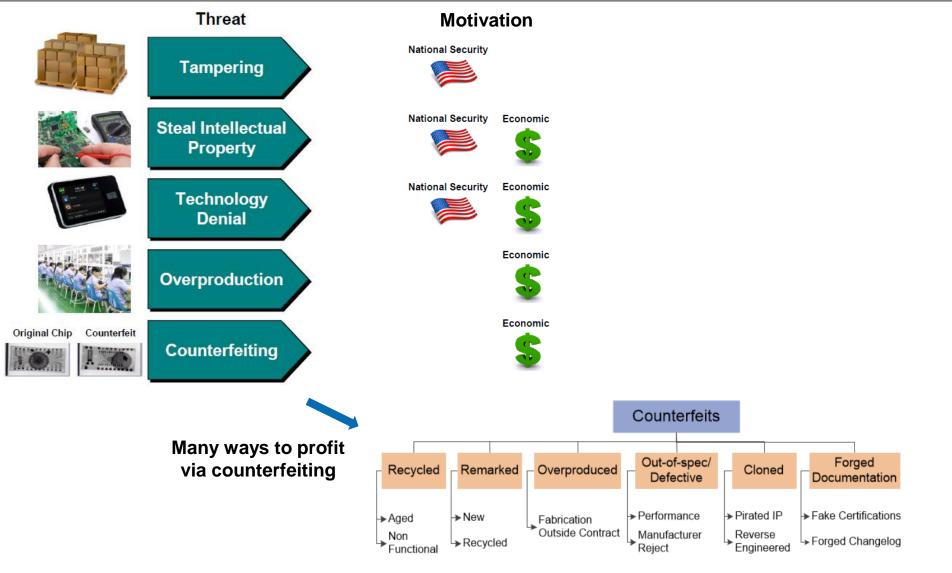
Semiconductor Assembly Example (2.5D HBM): How many people have access throughout the supply chain?





Source: "Start Your HBM/2.5D Design Today," SK Hynix, Amkor, eSilicon, Northwest Logic, Avery Design, 2016.

Semiconductor Security Vulnerabilities: Many types of threats, motivated by financial and malicious interests

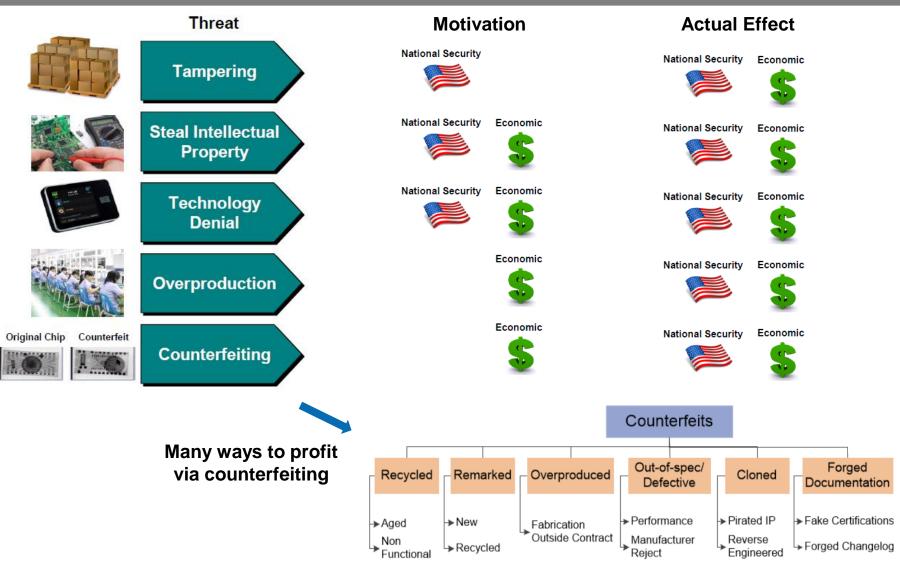


57

Source: Mark Tehranipoor, "Counterfeit Detection and Avoidance," April 2018. Source: "Supply Chain Hardware Integrity for Electronics Defense (SHIELD)," Serge Leef, Software and Supply Chain Assurance Winter Forum, Dec. 2018

Booz | Allen | Hamilton

Semiconductor Security Vulnerabilities: Many types of threats, motivated by financial and malicious interests



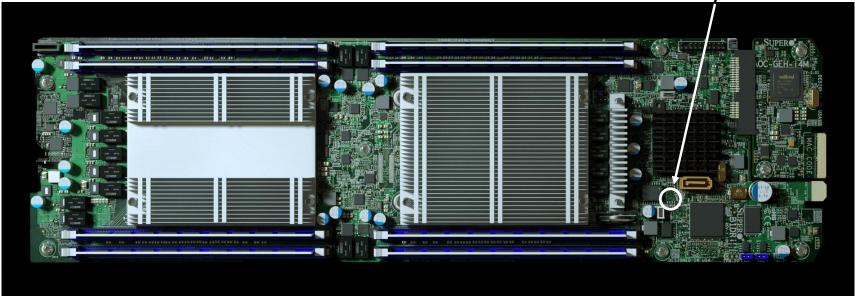
Source: Mark Tehranipoor, "Counterfeit Detection and Avoidance," April 2018. Source: "Supply Chain Hardware Integrity for Electronics Defense (SHIELD)," Serge Leef, Software and Supply Chain Assurance Winter Forum, Dec. 2018

Booz | Allen | Hamilton

Supply Chain Vulnerability: Headline-worthy hacking – full story still TBD, but illustrates the risk

- Recent reports of malicious interdiction in Supermicro server boards assembled in China
- Very broadly used in commercial and government systems (Amazon, Apple, CIA, etc.)
- High functionality components miniaturized, hidden, and disguised as other components
- Enable third party to control hardware, apparently done in parallel with SW/FW attacks





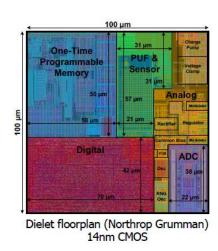
Government Focus on Semiconductor Packaging Security

DARPA Microsystems Technology Office (MTO) PMs: Areas of interest => significant interest in security / packaging

						Are	as of	Inte	erest	(htt	ps://	/ww\	<i>w</i> .da	rpa.i	mil/a	bou	t-us/	′peo	ple)					
		Adaptibility	Automation	Communications	Cyber	Decentralization	Electronics	EW	Imagery	Integration	ISR	Leadership	Manufacturing	Materials	Microstructure	Microsystems	Photonics	PNT	Processing	Quantum	Security	Sensors	Spectrum	DARPA
MTO PM	Joined	2	2	2	2	1	8	3	2	3	1	1	3	5	1	5	3	2	1	1	2	5	7	Packaging Interests
Griffin, Ben	Oct-18						1							1								1	1	extreme environments
Rebello, Keith	Oct-18				1		1							1		1								
Burke, John	Aug-18							1		1							1	1		1		1		
Leef, Serge	Aug-18						1						1			1					1			Supply Chain, Security
Trimberger, Steve	Aug-18		1				1									1					1			Security
Mason, Whitney	Nov-17								1													1	1	
Chen, YK	Sep-17													1		1	1					1		Heterogeneous integration, materials
Keeler, Gordon	Aug-17						1			1						1	1							Photonics
Polcawich, Ron	Aug-17			1										1	1			1						MEMS
Olofsson, Andreas	Jan-17		1				1						1						1					HI, standards, automation, manufacturing
Hancock, Tim	Sep-16					1	1	1															1	Heterogeneous integration
Rondeau, Tom	May-16	1		1																			1	
Plaks, Ken	Jan-15				1			1						1										Security
Tilghman, Paul	Dec-14										1												1	
Lewis, Jay (DD)	Nov-14								1													1	1	
Salmon, Linton	Sep-14						1						1											Manufacturing, foundries
Chappell, Bill (OD)	Jun-14	1								1		1											1	

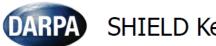
Another Approach to Trust: SHIELD uses advanced assembly technology to verify a full assembly

Challenge and response to verify presence of trusted SHIELD dielet within



Key SHIELD Specifications

- Unique Key Storage
- Full 256-bit AES encryption engine
- Unpowered, passive intrusion sensors
- RF power and communication
- Transfer fragility
- 100μm x 100μm
- 50 µW Total Power
- Operating temp < 120°C
- Cost < \$0.01 per dielet



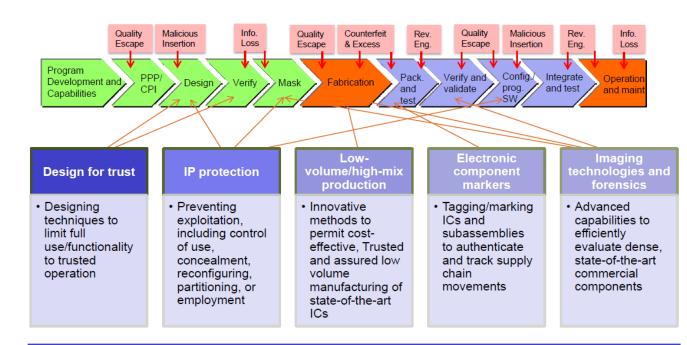
SHIELD Key Components

Γ	Dielet	Reader	Remote Server
m In pa · · ·	ogrammed on-reticle after anufacture stalled on or within host IC ackage Embedded within package Custom package Epoxy to surface o impact to host IC erformance or reliability	Transmits at 5.8GHz to power dielet; 3.6GHz for data transfer USB connection to smartphone, tablet or computer Can be configured for high- volume interrogation (transaction time < 1 sec)	Communicates with reader via Internet connection; performers using Amazon and Microsoft web services Maintains a record for each IC • Manufacture date • Part/package information • Interrogation history

Microelectronics Innovation for National Security and Economic Competitiveness (MINSEC): Packaging is critical part of security

T&AM New Trust and Assurance Approaches





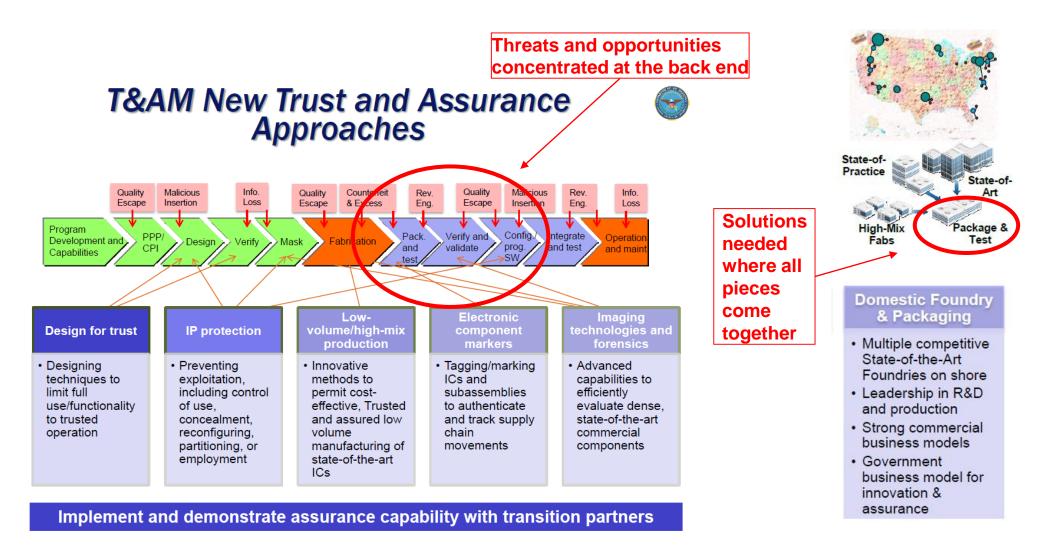
Implement and demonstrate assurance capability with transition partners



Domestic Foundry & Packaging

- Multiple competitive State-of-the-Art Foundries on shore
- Leadership in R&D and production
- Strong commercial business models
- Government business model for innovation & assurance

Microelectronics Innovation for National Security and Economic Competitiveness (MINSEC): Packaging is critical part of security



Source: "Long-Term Strategy for DoD Assured Microelectronics Needs and Innovation for National Economic Competitiveness," K. Baldwin, NDIA, Oct. 2018 Booz | Allen | Hamilton

Office of the Secretary of Defense, July 2019



Competitive Opportunities



Opportunity	Open Date	End Date	Reference
State of the Art (SOTA) Heterogeneous Integrated Packaging (SHIP) Prototype	3 Jul 2019	6 Aug 2019	https://s2marts.org/ Contact: S2MARTS@nstxl.org
Rapid Assured Microelectronics Prototypes using Commercial Design & Intellectual Property	4th Qtr FY19		https://s2marts.org/ Contact: S2MARTS@nstxl.org
Microelectronics Innovation for Next- generation System Advancement and Validation (MINSAV) Advanced Research Announcement			
Advanced Technology Center (ATC) for Data Processing	4th Qtr FY19		https://www.cto.mil/work-with-us/
Assured and Trusted Microelectronics Solutions (ATMS) Broad Agency Announcement (BAA)	Jan 2017	Nov 2022	FedBizOps Solicitation Number: FA8650-18-S-1201
Rapid Innovation Fund (RIF) Broad Agency Announcement (BAA)	4th Qtr FY19		https://www.cto.mil/work- with-us/

Distribution Statement A: Approved for public release. Distribution is unlimited.

State of the art Heterogeneous Integrated Packaging (SHIP)

This Request for Solutions is anticipated to result in two awards, with each award respectively related to the focus areas below:

1) <u>SHIP Digital</u>: State of the Art Digital Design Center and Integrated Packaging and Assembly Test Center; and,

2) <u>SHIP RF</u>: State of the Art RF Design Center and Integrated Packaging and Assembly Test Center.

Item No.	Item/Deliverable	Quantity / Frequency	Deliverable Due Date
1	 Phase 1 SHIP Report Comprised of Technical & Business Plans discussing the phases below: <u>Phase 2</u>: Advanced Prototype Capability Development and Initial Design Activities; <u>Phase 3</u>: Install and Qualification of Processes; <u>Phase 4</u>: Operate and Maintain Advanced Prototype Capability 	1 / Once	<u>No Later Than</u> six (6) months from project award.

State of the art Heterogeneous Integrated Packaging (SHIP)

This Request for Solutions is anticipated to result in two awards, with each award respectively related to the focus areas below:

1) <u>SHIP Digital</u>: State of the Art Digital Design Center and Integrated Packaging and Assembly Test Center; and,

\$25M for a six-month paper study!

2) <u>SHIP RF</u>: State of the Art RF Design Center and Integrated Packaging and Assembly Test Center.

Item No.	Item/Deliverable	Quantity / Frequency	Deliverable Due Date	
1	Phase 1 SHIP Report	1 / Once	No Later Than six	

Current Project Budget: \$25,000,000 is budgeted and available for the Phase 1 awards, while subsequent Phases will be funded upon successful completion of the previous Phase.

 <u>Phase 3</u>: Install and Qualification of Processes; <u>Phase 4</u>: Operate and Maintain Advanced Prototype Capability 	 <u>Phase 2</u>: Advanced Prototype Capability Development and Initial Design Activities; 	
	• <u>Phase 3</u> : Install and Qualification of	

SHIP Advanced Prototype Capability Concept

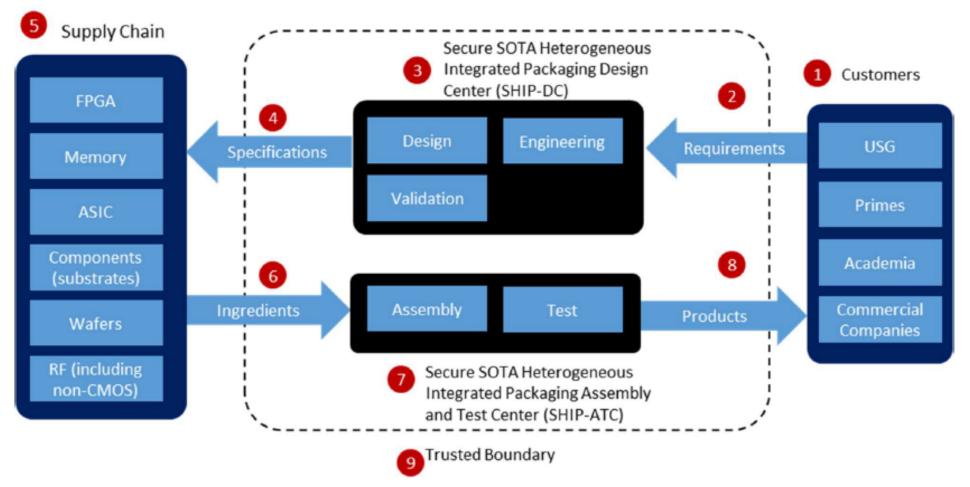


Figure 1 Notional design and prototype manufacturing flow

SHIP Capabilities

Table 3 General Capacity and Capability for the SHIP-ATC

Category	IOC	FOC	Scale
Capacity: Volume	1k+	10k+	100k/mo+
Silicon interposer	Required	Required	Required
Organic interposer	Preferred	Required	Required
Utilize SOTA COTS FPGA ¹ and programmable devices	Required	Required	Required
Structured ASIC	Preferred	Preferred	Required
Security	Trust	ITAR	Classified
Number of Chips/Package ²	4	8	12+
Supply Chain target	>50% US	>75% US	>90% US
Can process singulated die	Required	Required	Required
Can process up to 300mm wafers	Preferred	Required	Required
Can process 200mm die	Preferred	Preferred	Required

¹Must include ability to integrate and test SOTA FPGA (<14nm), not required for RF centric applications

² Could include, but not limited to, memory, ADC/DAC, transceivers, optical couplers, ASIC, structured ASICs, etc.

Table 4 Silicon Interposer Foundry Specifications

		IOC	Final State
Size	Interposer Area	26x33mm	(26x33mm) X 2 with stitching (1)
Front-side	Wiring Density	1000-1600 IO/mm	1600 IO/mm (2)
	Metal Layers	(0.4/1.08/4.0) μm (1.08/1.08/4.0) μm	(0.4/1.08/4.0) μm (1.08/1.08/1.08/4.0)
	Bump Pitch	50µm	μm 36μm
Middle	TSV Pitch	55µm Min	45µm Min
Back-side	Bump Pitch	55µm Min	45µm Min

SHIP Assembly Specs (sample)

Table 6 Advanced Microelectronics Assembly Specifications

		IOC	Final State		
		IOC	FOC		
Chip on Chip	Silicon Interposer Sizes	(22 x 33) mm	(22 x 33) mm		
	Top Chip Process	All leading process	es from 180nm to 7nm		
	Chip Size Range	(2 x 2) mm to (21 x	(1 x 1) mm to (21 x 32)		
		32) mm	mm		
	Chips Placed Per	20			
	Interposer				
	Chip Spacing	100 µm	100 µm		
	Chip Bump Pitch	50 µm	36 µm		
	Total Connections				
	Number of chips in 3D stack	21 (estimate only)	> 21 (estimate only)		
Chip on Substrate	Max Organic Substrate Sizes	(76 x 74) mm	(100 x 100) mm		
	Substrate C4 Bump Pitch	55 µm	45 μm		
	Chips Placed Per Substrate	7	12		
	Chip Spacing	100 µm	100 µm		
Packaging	Features	• High performance	polymer and solder		
		thermal interface materials integrated with			
		Cu heat spreaders for improved thermal			
		performance			
		 Package substrates 	s that are optimized for		
		low loss high spee	-		

Booz | Allen | Hamilton



DARPA Future of heterogeneous integration



Requires a lot of pieces coming together!

Source: DARPA