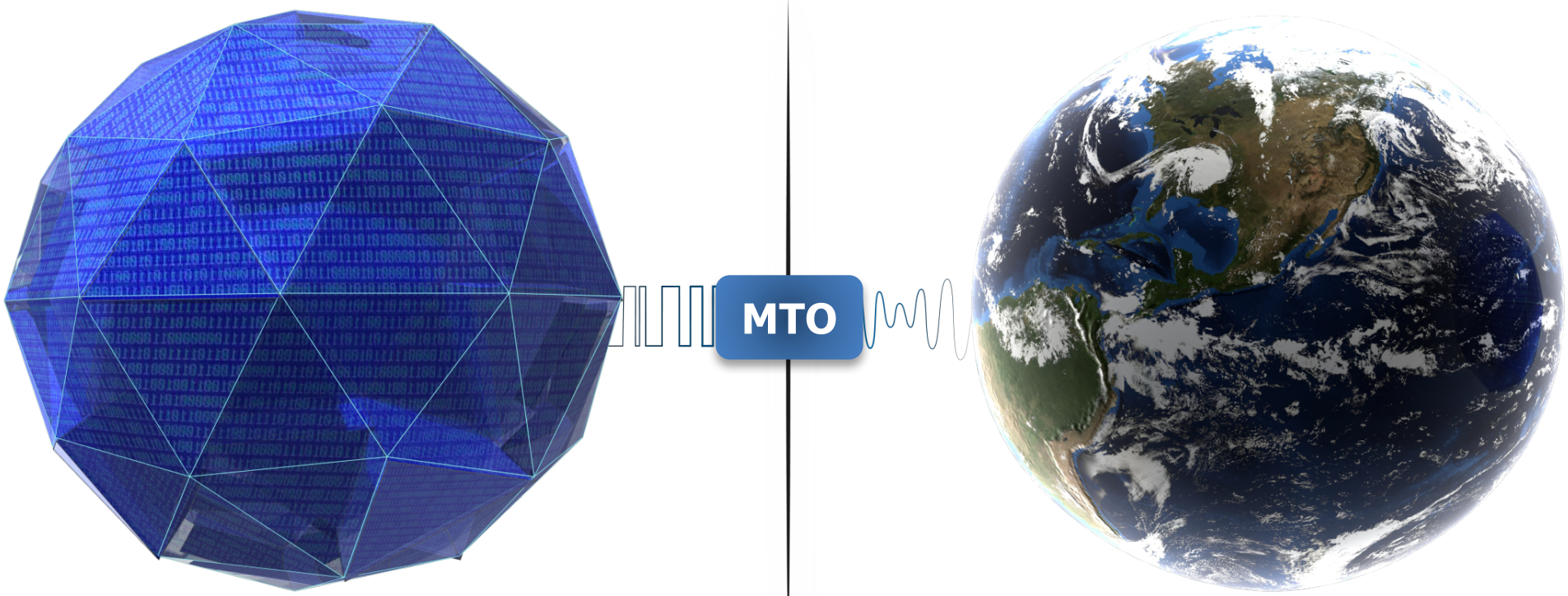
A TECHNOLOGY-ENABLED NEW TRUST APPROACH

Dr. William Chappell
Director, DARPA Microsystems Technology Office (MTO)

NDIA Trusted Microelectronics Workshop

August 17, 2016



Artist's concept

Role of DARPA MTO

Tactical Information Extraction

Develop processing architectures for next generation machine learning

Processing	*Learning*	*Application*
UPSIDE	Cortical Processor	ARC
PERFECT		SC2

Globalization

Move from fear to exploiting a new technology approach

Speed	*Leveraging*	*Security*
CRAFT	DAHI	VAPR
CHIPS	ICECool	SHIELD
	SPADE	IRIS
	STARnet	

Spectrum & Physics Interfaces

Expand our lead in the physical realm

RF	*Optics*	*Sensors*
ART	Endurance	N-ZERO
ACT	FLASH	microPNT
MPC	DODOS	PRIGM
ELASTx	MOABB	ACES
HERMES	WIRED	
SPAR	LOTS	
M3IC	LUSTER	
HAVOC		
TROPHY		

DoD faces unique security challenges in protecting its microelectronics against advanced nation-states

Fabrication & Assembly

Potential Attacks

Malicious insertion

Fraudulent products

Loss of CPI

Poor quality

Reliability failures

Loss of access

Courtesy: extremetech.com

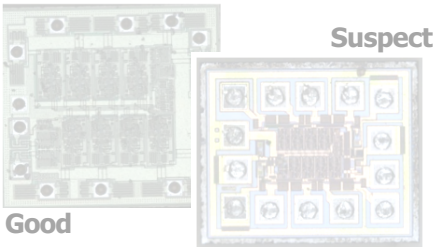
Overproduction & Test Fails

Courtesy: NSWC CRANE

Counterfeiting

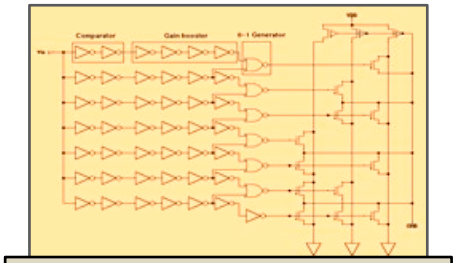
Courtesy: Daily Mail, Shutterstock

Hardware or IP theft



Courtesy: NSWC CRANE

Cloning



Courtesy: cse.psu.edu

Design Compromise

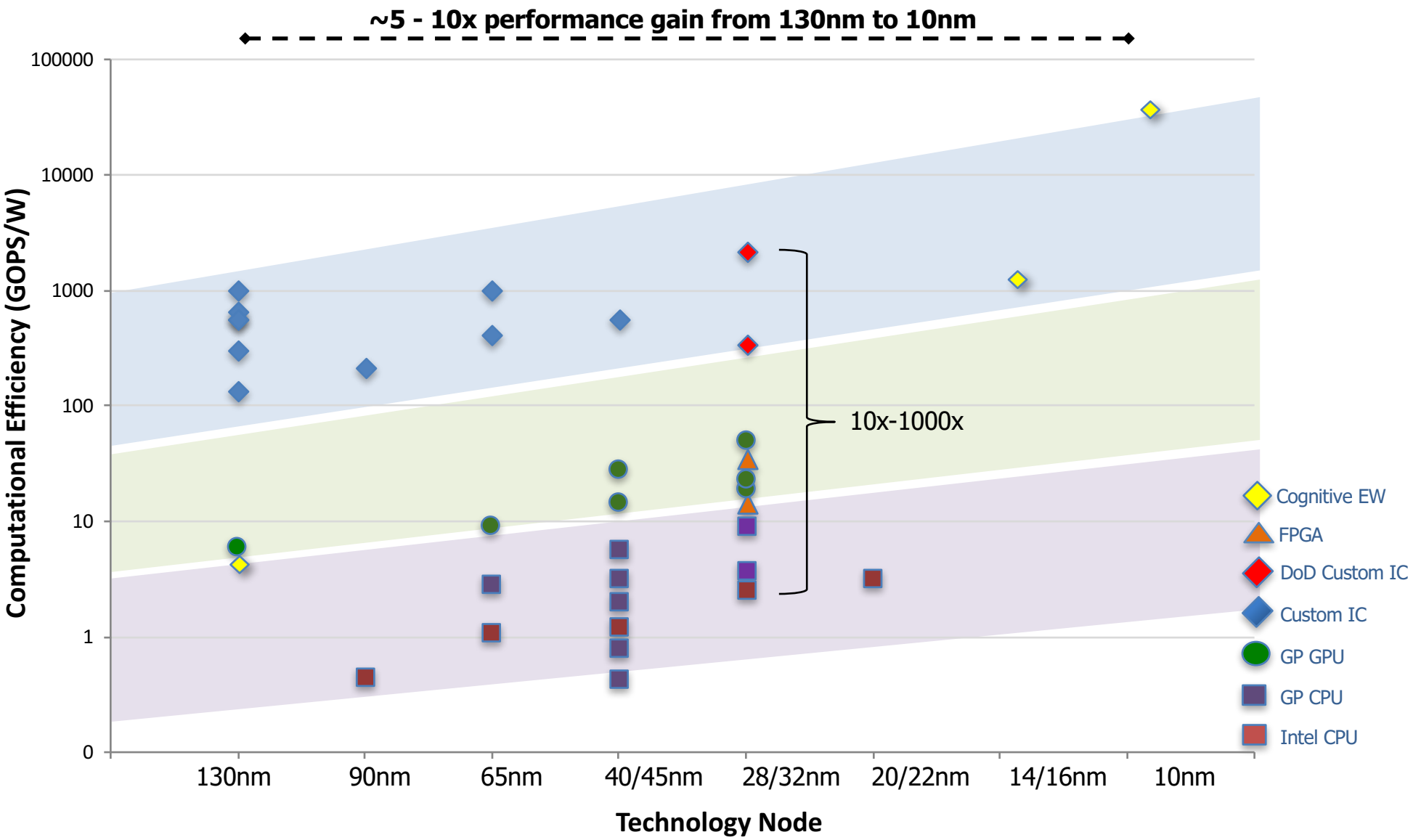
Courtesy: IEEE Spectrum

Reliability Compromise

Courtesy: IDC Manufacturing Insights and Booz Allen analysis

Supply Chain Risk

Leading-edge microelectronics offer specific, military-relevant advantages to DoD

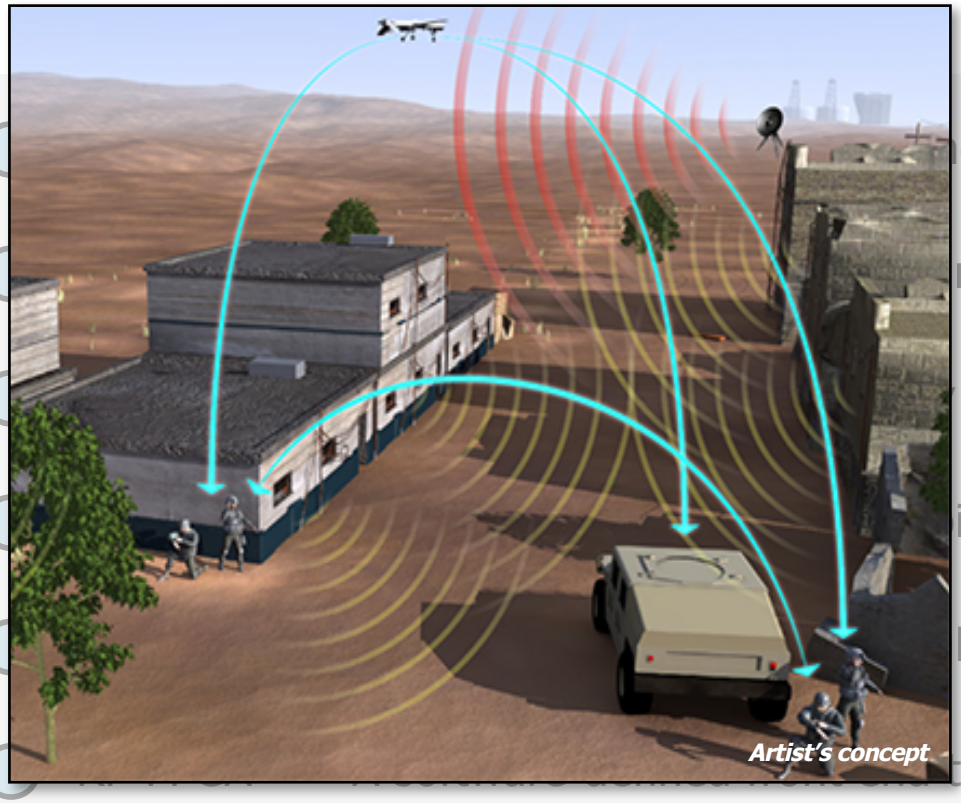


Data from ISSCC papers 2010 – 2013
and "Energy Efficient Computing on Embedded and Mobile Devices" on nVidia.com

Example ASICs under development could deliver revolutionary capabilities to the warfighter

ACT	Capture unprecedented volumes of RF data at 64Gs/sec for next-gen arrays
CLASIC	Distinguish and classify RF signals for 180 hours on a cellphone battery
CLASS	Disguise and dynamically vary signals for inexpensive LPI/LPD comms
DAHI	10x higher dynamic range arbitrary waveform generator for EW solutions
ReImagine	Collect different data in a single camera frame with a reconfigurable ROIC
RF-FPGA	A software-defined front end that works for 20GHz or below
SHIELD	Verify the authenticity of components at every point in the supply chain
SPADE	Build trusted circuits through 3D integration
UPSIDE	Enable real-time machine learning for object recognition on UAV

Example ASICs under development could deliver revolutionary capabilities to the warfighter

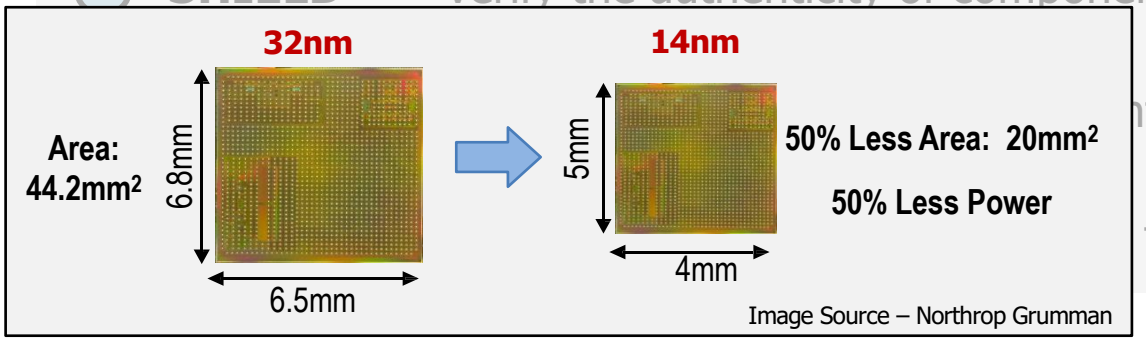


ACT

- Capture unprecedented volumes of RF data at 64Gs/sec for next-gen arrays
- Leverage the world's best digital beamforming system

32nm SOI vs. 14nm FinFet

SHIELD Verify the authenticity of components at every point in the supply chain



ACT – Arrays at Commercial Timescales

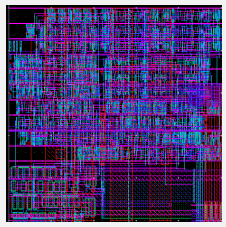
Example ASICs under development could deliver revolutionary capabilities to the warfighter

ReImagine

- Achieve full battlespace awareness with a single reconfigurable ROIC
- Simultaneously collect diverse data types from multiple regions of interest

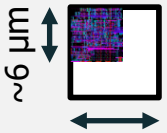
14nm CMOS

SHIELD Verify the authenticity of components at every point in the supply chain



SOA digital ROIC pixel layout using 65 nm CMOS

25 µm

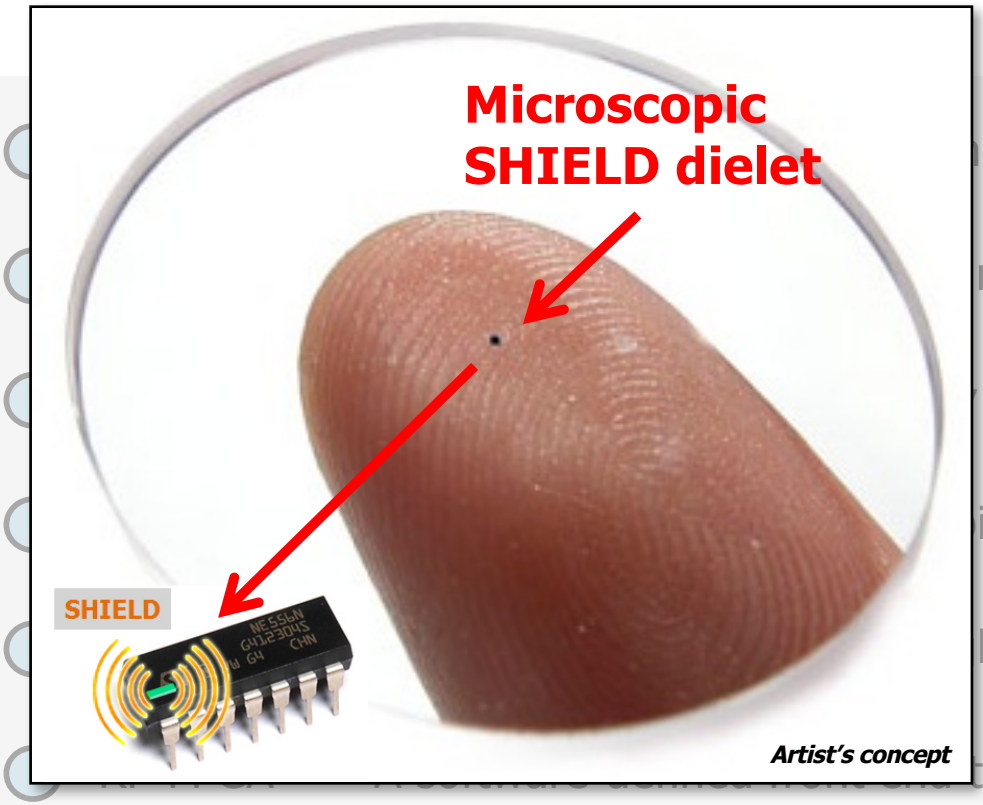


14 nm CMOS pixel with computation

Images courtesy: MIT Lincoln Laboratory

Source: Realistic infrared sequence generation by physics-based infrared target modeling for infrared search and track Sungho Kim ; Yukyung Yang ; Byungin Choi Opt. Eng. 49(11), 116401 (November 22, 2010). doi:10.1117/1.3509363

Example ASICs under development could deliver revolutionary capabilities to the warfighter

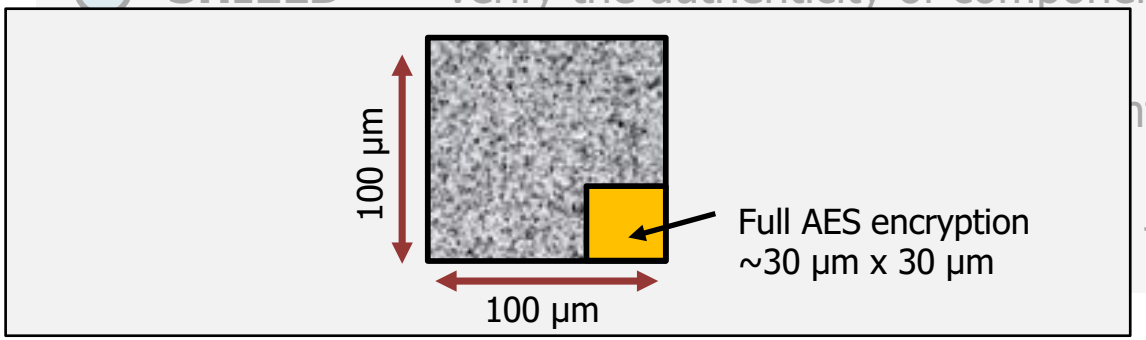


SHIELD

- Ensure the authenticity of genuine military electronic components
- Tag electronics at low cost with an encrypted 100µm x 100µm ASIC

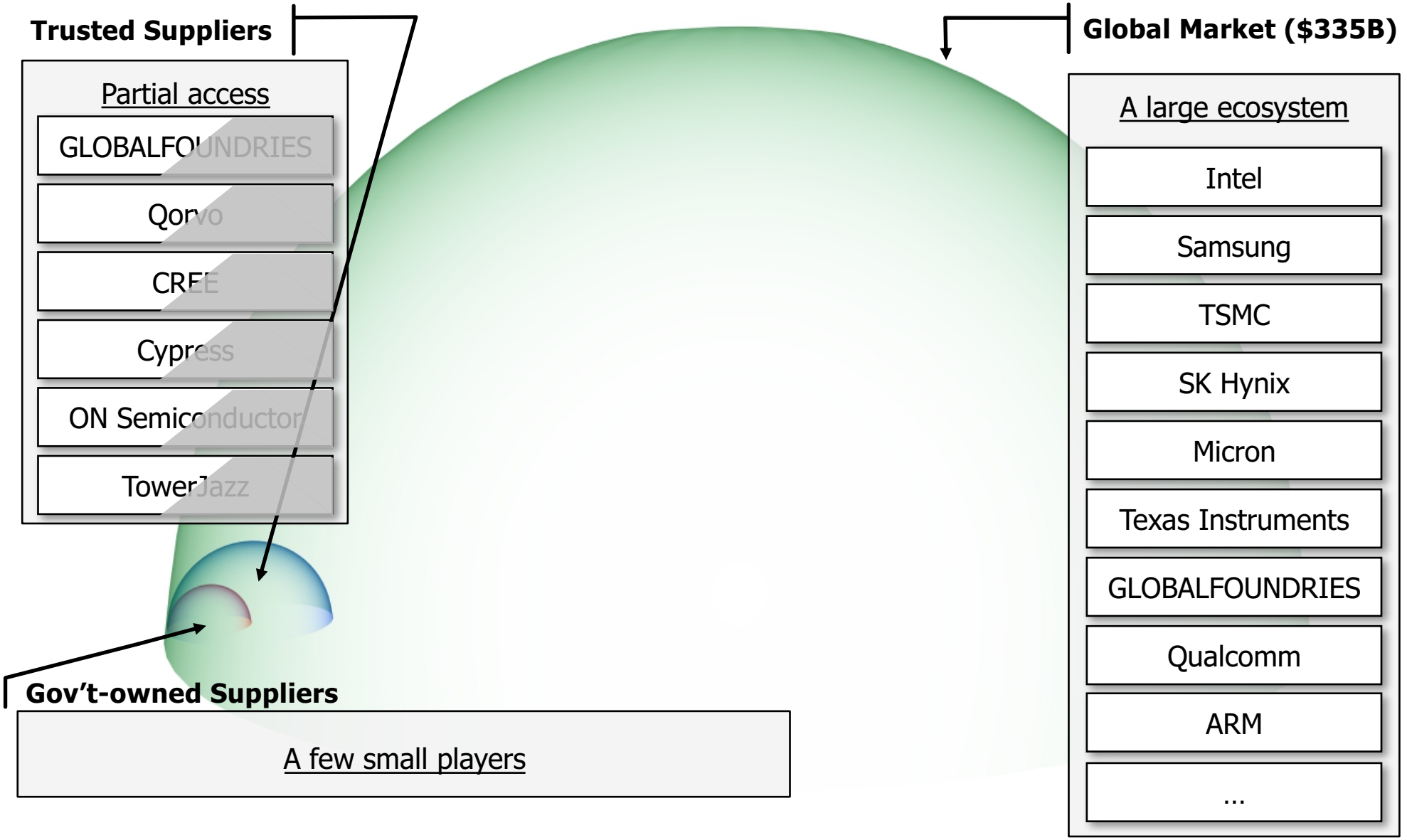
14nm CMOS

SHIELD Verify the authenticity of components at every point in the supply chain

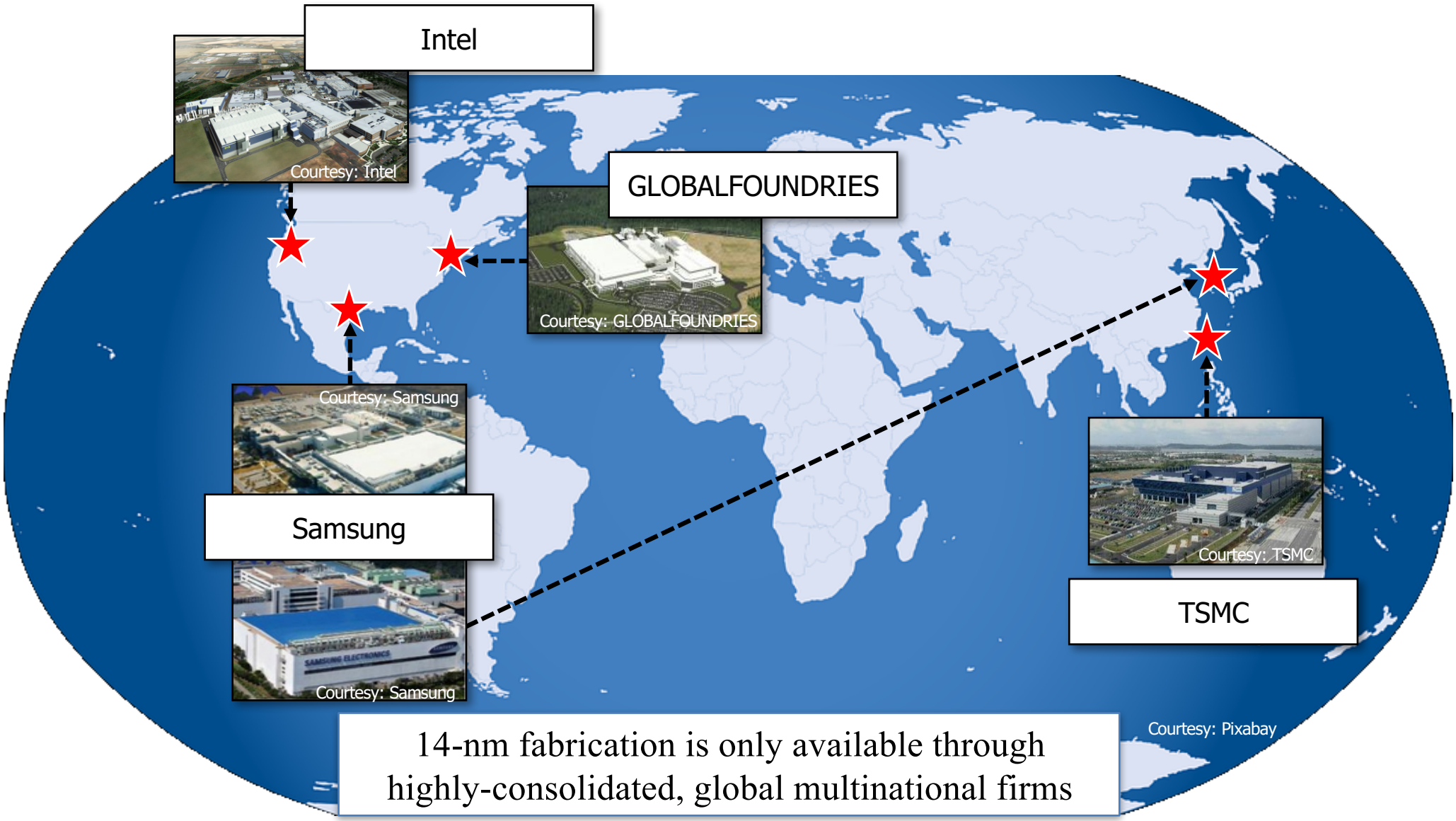


SHIELD - Supply Chain Hardware Integrity for Electronics Defense

The semiconductor market sustains a large ecosystem, with many leading-edge firms operating within the United States

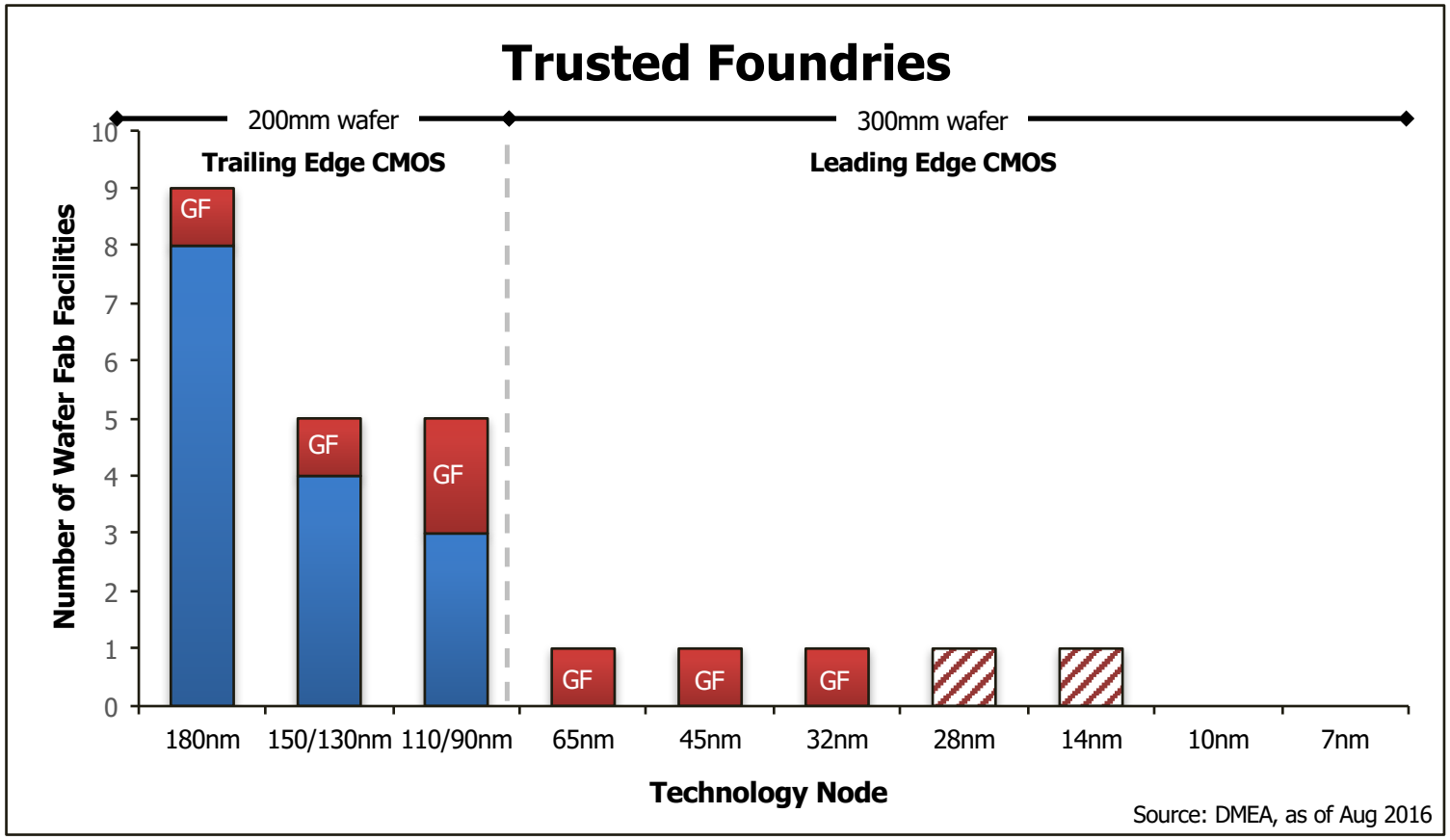


DoD will have to collaborate with the multinational semiconductor firms with leading-edge capabilities



14-nm fabrication is only available through highly-consolidated, global multinational firms

Reliance on trusted suppliers can limit potential partners, yielding few options for trusted access to leading-edge CMOS

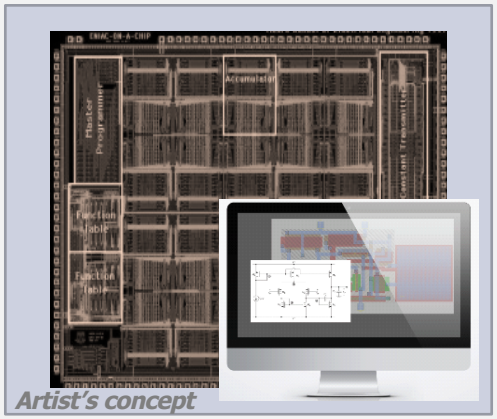


	Foundry Choices	Process node for leading-edge products	Design-to-chip turnaround time
Commercial	Multiple global options	14nm – 10nm	9-10 months (400 engineers)
DoD	One strategic partner	65nm – 32nm	2-3 years (10 engineers)

It is the right time for DoD to reflect on its strategy

Today: DoD relies on a single, sole-source supplier for leading-edge microelectronics

Tomorrow: Technology-driven security techniques can enable new DoD options for acquiring state-of-the-art, commercial microelectronics



Trusted Design

Sole-source Fabrication below 90nm

Trusted DoD Electronics

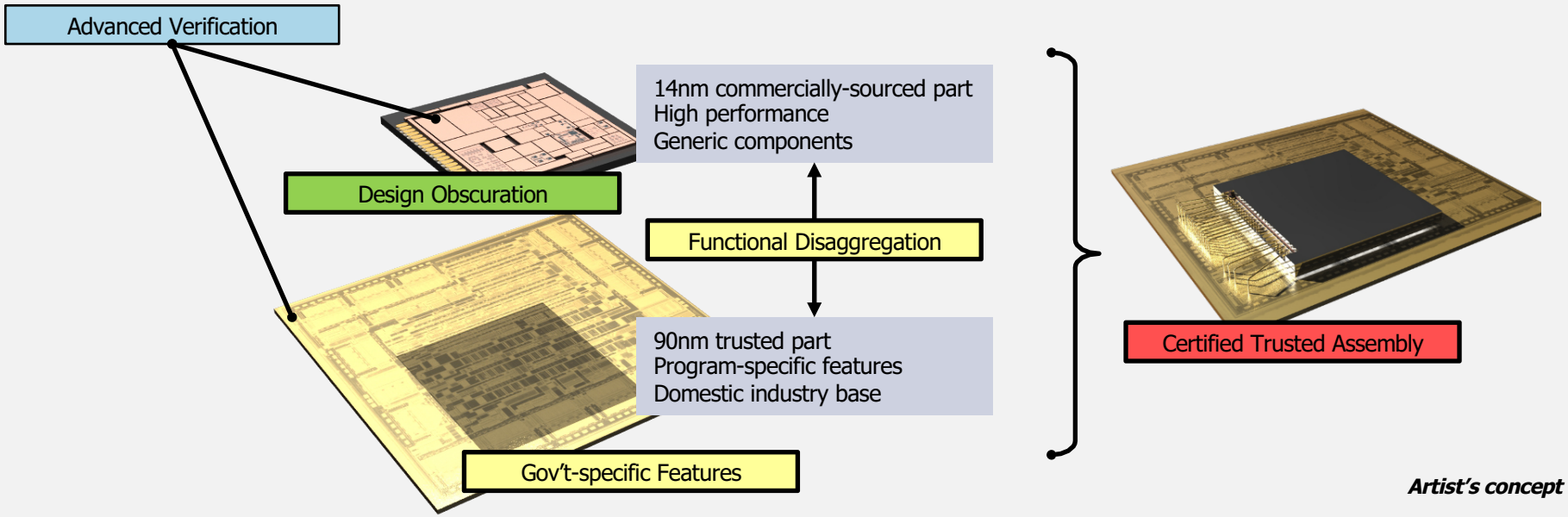
Commercial Fabrication

GLOBALFOUNDRIES	TSMC
Samsung	Intel

Selective application of countermeasures can demonstrate "trust through technology" for a representative device

IRIS / TRUST	CRAFT (eFuses) / SHIELD	CHIPS / DAHI	IARPA TIC / VAPR	Trusted Foundries / Classified Tech
Verification and Validation	Obscuration and Marking	Functional Disaggregation	Fine Disaggregation and Transience	Government-proprietary Techniques

High Commercial Sponsorship → **High Government Intervention**



To ensure security and to leverage the globalized supply chain, DARPA and other agencies are developing a technology-enabled portfolio of protections.

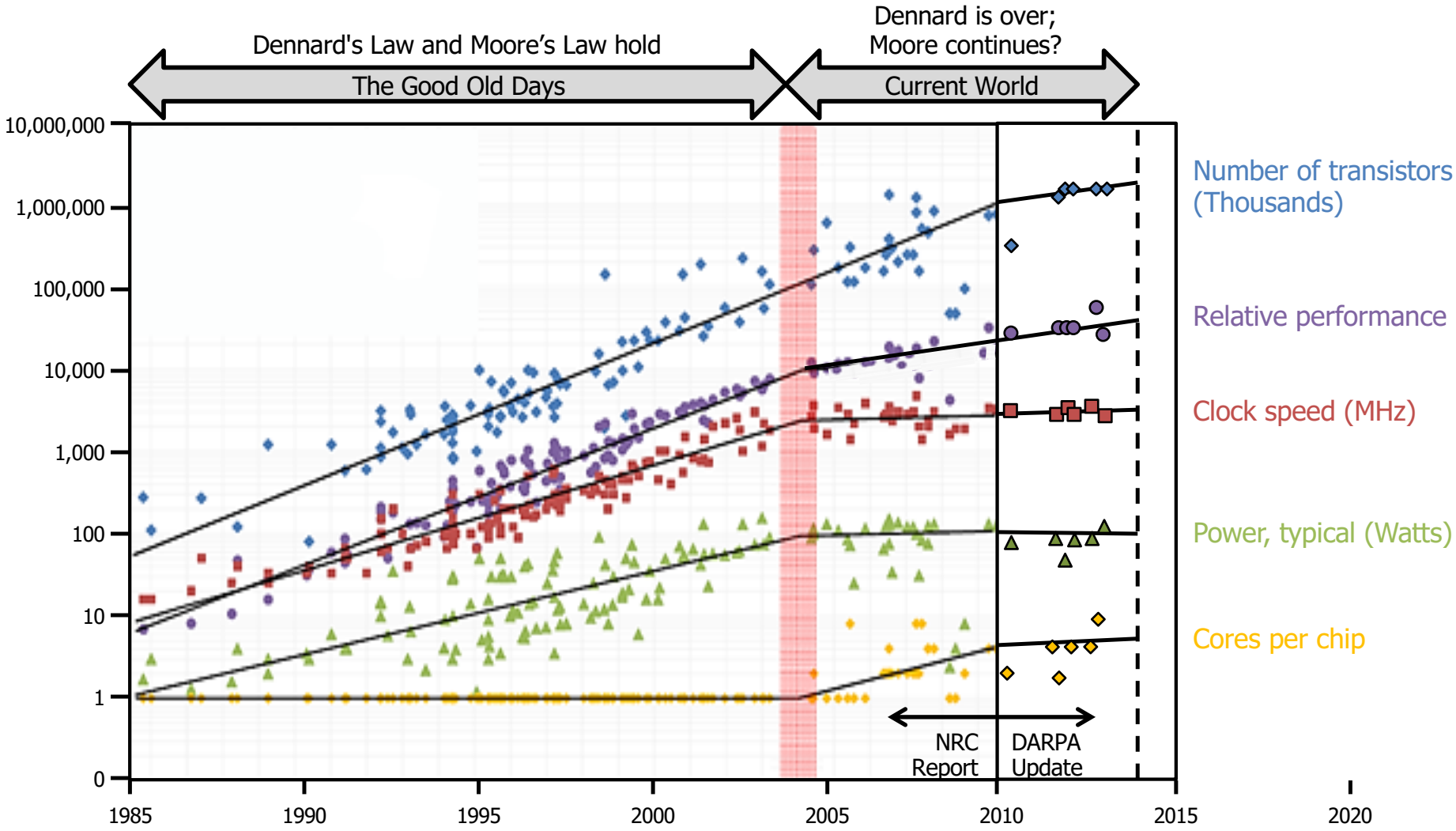
The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need

		Microelectronics Security Threats				
Protection	*Program*	Loss of information	Fraudulent products	Loss of access	Malicious insertion	Quality and reliability
Government-proprietary	Other	●				
Fine Disaggregation and Transience	TIC (IARPA)	●	●	○	○	
	VAPR	●				
Functional Disaggregation	SPADE	●			●	●
	DAHI	●		○	●	
	CHIPS	○		○	●	●
Obscuration and Marking	CRAFT			●		●
	eFuses	●			●	
	SHIELD	○	●			
Verification and Validation	IRIS		●		●	●
	TRUST		○		●	

High Government Intervention ↑ ↓ High Commercial Sponsorship

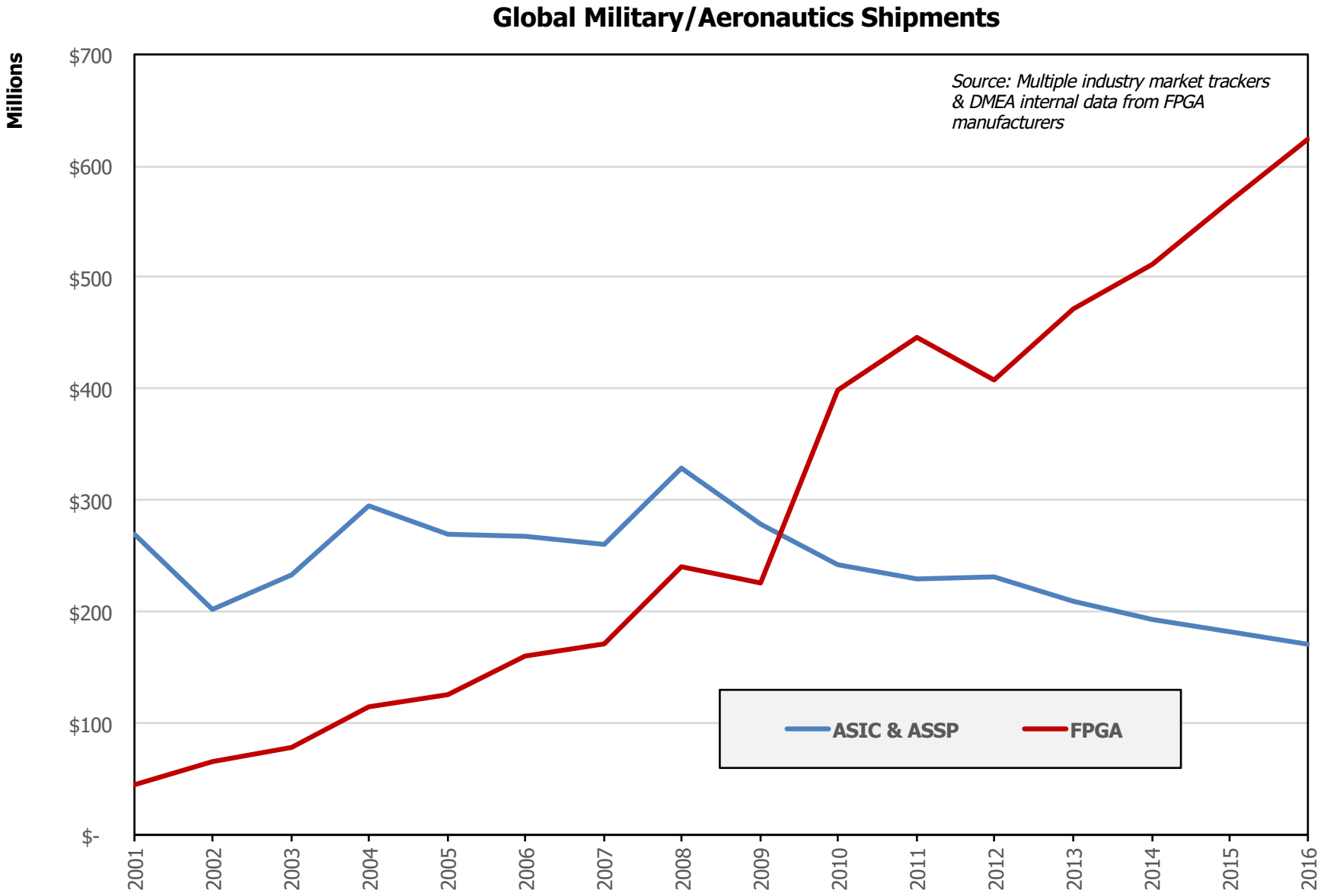
● Primary Impact ○ Secondary Impact

We've adapted to the end of Dennard's Law but are at an inflection point



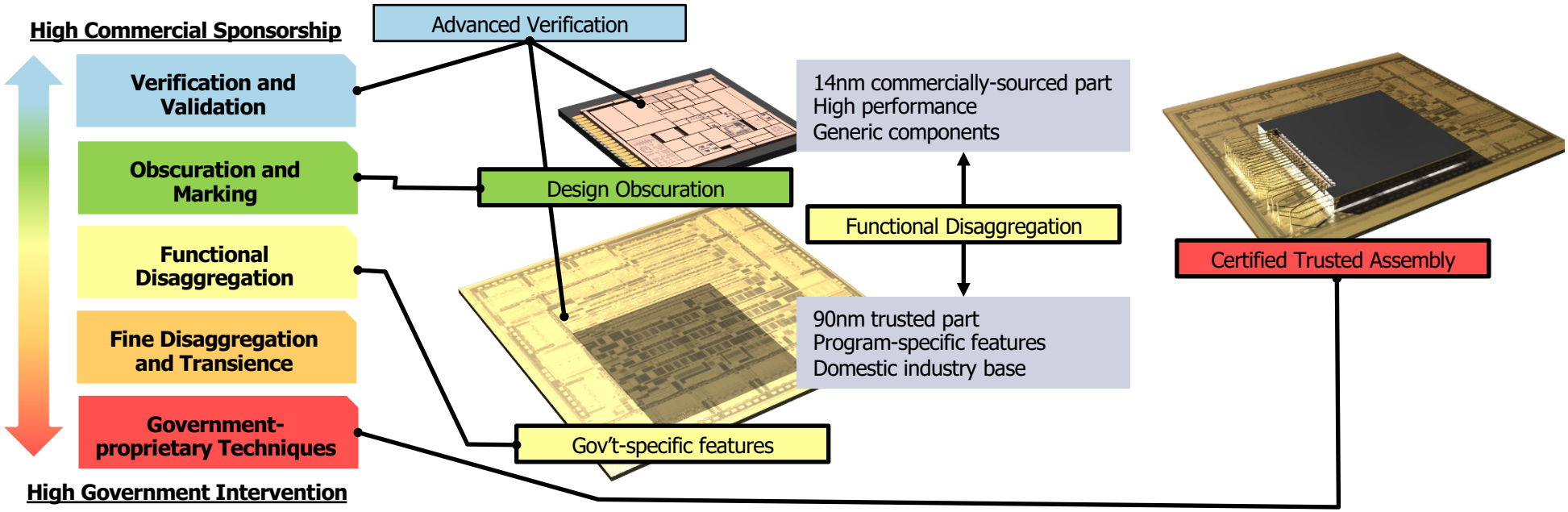
Post-Dennard, we lose the free exponential improvements in computing cost, speed, and power from improvements in fabrication technology.

Moore's Law has allowed the military to increasingly depend on FPGAs



The end of Moore's Law is leveling the playing field, meaning now is the time to focus on ASIC access and specialization

Trust through technology



Artist's concept

Acquisition personnel can selectively apply protections based on a component's criticality, the risks faced, and the need to access leading-edge technologies.

www.darpa.mil