

# **(Un)Intended Communications**

---

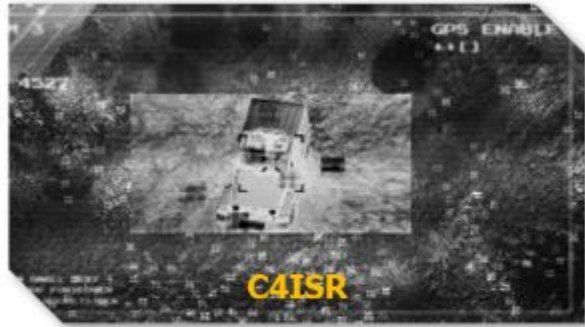
James Wilson, PhD  
DARPA MTO Program Manager

2022-10-17





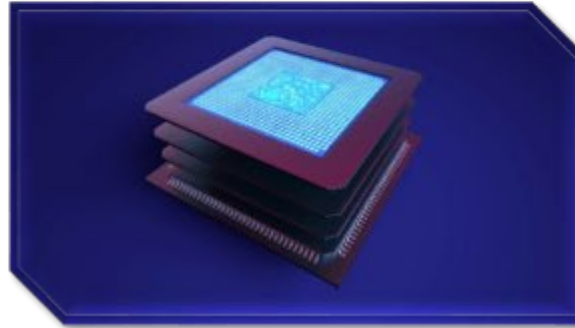
## High-performance, intelligent microsystems and next-generation components



### Disruptive Microsystems



**Local Processing**



**Microsystems Manufacture**



**Spectrum Dominance**



# Key challenges

## Reducing SWaP-C of front-end elements



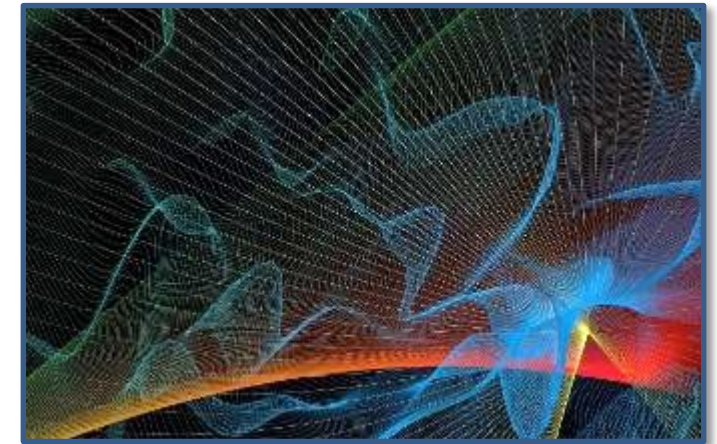
Bulky electronics and optics undermine ability to miniaturize sensors and systems

## Increasing tactical range



Range of EW, DE, and C4ISR is limited by inherent properties of current materials and devices

## Enabling robust operation in congested spectrum



Source: Adobe Stock

RF components are insufficiently adaptable or robust to operate in increasingly congested spectrum

C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance  
DE: Directed Energy  
EW: Electronic Warfare  
SWaP-C: Size, weight, power, and cost



# Key challenges

## Securing communications



Ensuring network availability and security

## Overcoming security threats across the entire hardware lifecycle



Persistent hardware threats limit the ability to access and utilize advanced electronics technology

## Reducing latency in EW



Adaptive threats challenge ability to detect and counter

## Delivering accurate position and timing without GPS



Source: Adobe Stock

Low SWaP-C solutions required for GPS-denied environments





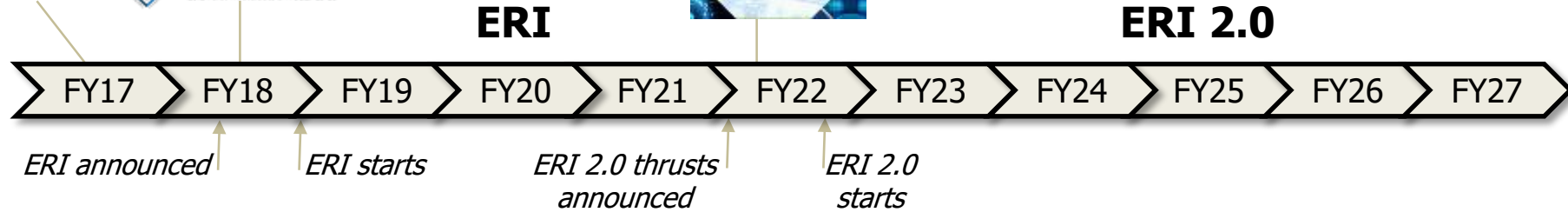
# Electronics Resurgence Initiative (ERI)

*A convergence of the commercial and defense electronics communities driven by common trends and threats*

PCAST Report on Semiconductor Leadership



ERI ELECTRONICS RESURGENCE INITIATIVE SUMMIT



**Overcoming security threats across the entire hardware lifecycle**

**Optimizing design and test for complex circuits and prototypes**

**Securing communications**

**Manufacturing complex 3D microsystems**

**Realizing heterogeneous 3D electronics**

**Accelerating innovation in artificial intelligence hardware to make decisions at the edge faster**

**Increasing information processing density and efficiency**

**ERI / ERI 2.0 thrusts**

Source: Advanced Technology Services, Inc. **Developing electronics for extreme environments**



Source: Adobe Stock

2D: Two Dimensional  
3D: Three Dimensional  
AI: Artificial Intelligence



## Local Processing

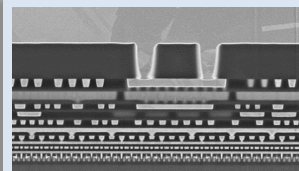
---

- **Increasing information processing density and efficiency**
- **Accelerating innovation in artificial intelligence hardware to make decisions at the edge faster**
- **Reducing the glut of digitized sensor data**



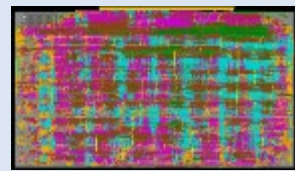
**HIVE**

Fast, small, random, global memory access across a flat, low-latency network



**FRANC**

New materials for compute-in-memory



**SDH**

Reconfigurable HW architectures and supporting SW development



**DPRIVE**

Accelerators to enable fully homomorphic encryption



**LTLT**

Cryogenic operation to enable HPC at reduced power



**SAHARA**

Structured ASICs w/ reconfigurability and near-ASIC performance



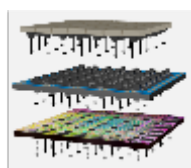
**DSSoC**

Power and cost efficient domain-specific architectures



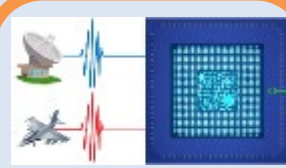
**ReImagine**

Processing layer to enable reconfigurable focal-plane arrays



**FENCE**

Processing of IR data within sensor to minimize power and latency



**MAX**

Power efficient correlators for signal processing



**ShELL**

AI that shares lifelong learning



**IP2**

Applying bio-inspired AI at the pixel level



**QuICC**

Computational approaches to minimize energy



**SPiNN**

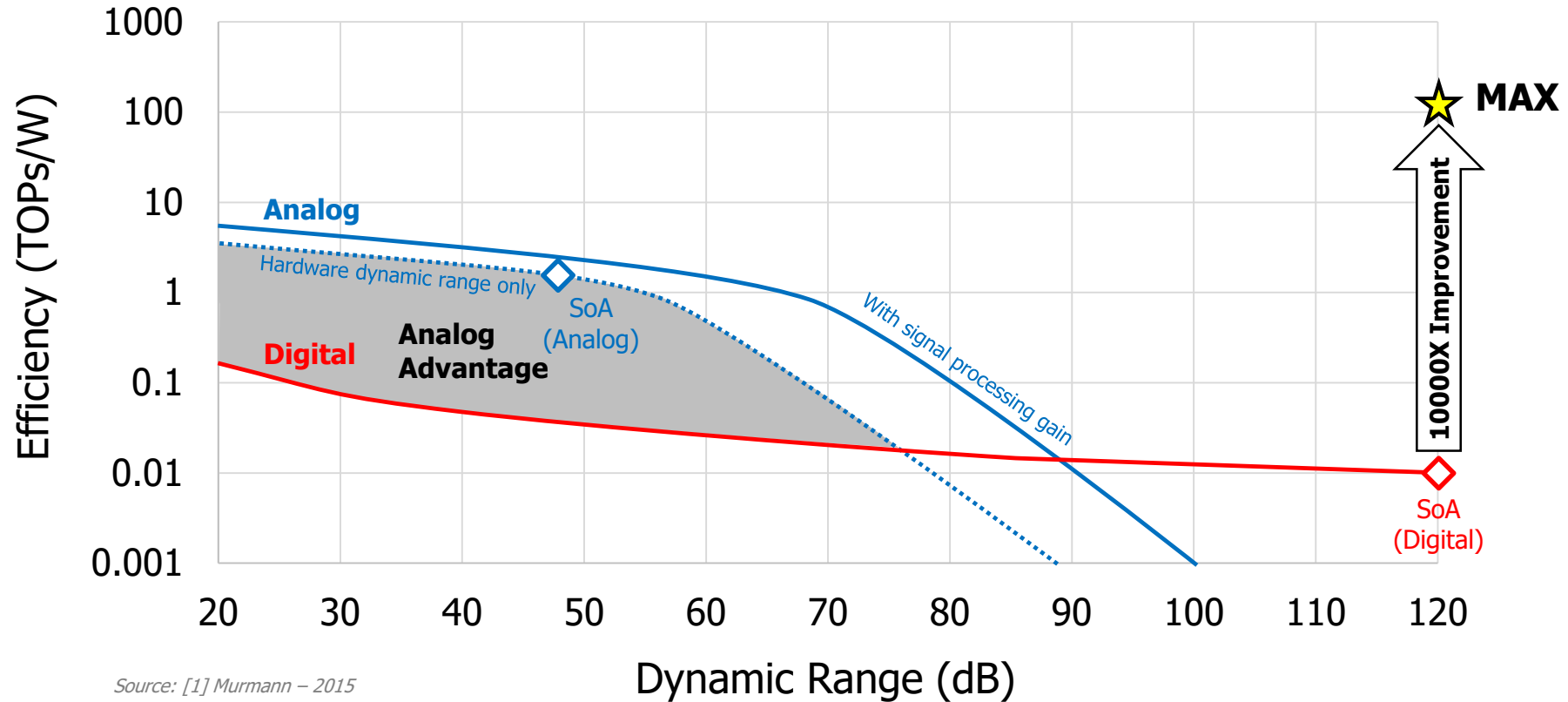
Model-based kernels with GAN-evolved transform layer for signal processing

AI: Artificial Intelligence  
 ASIC: Application specific integrated circuit  
 GAN: Generative adversarial networks  
 HPC: High performance computing  
 HW: Hardware  
 IR: Infrared  
 SW: Software



# MAX will achieve a breakthrough in correlator performance

### Correlator Dynamic Range vs Power Efficiency



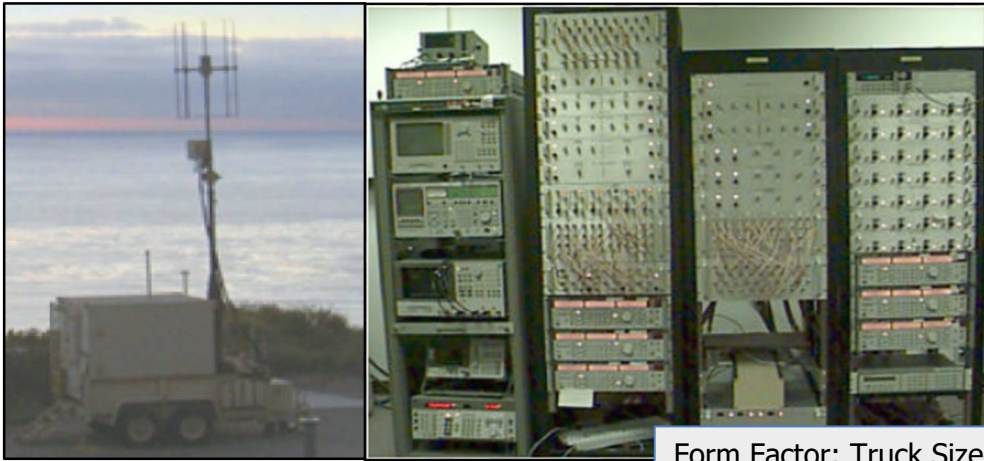
Source: [1] Murmann - 2015

MAX will increase today's analog efficiency advantage to 100 TOPs/W at 120 dB dynamic range



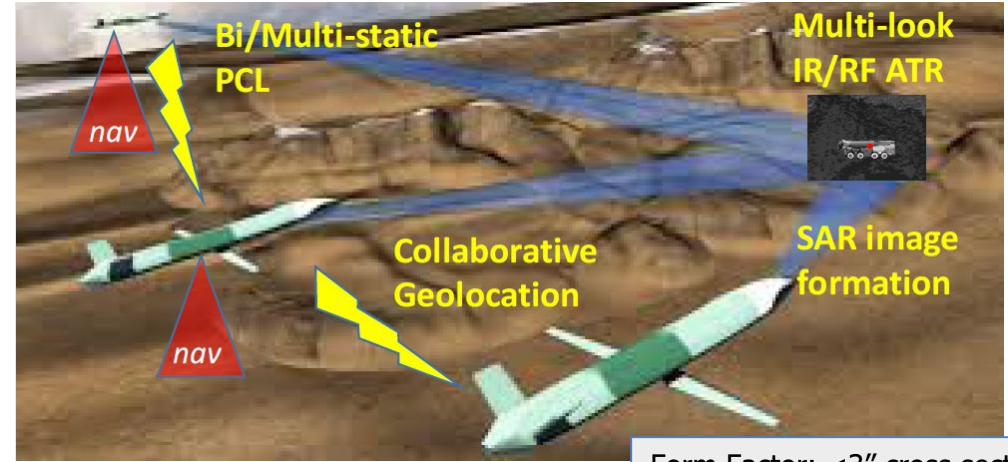


# MAX will enable multi-role missions on small platforms



Lockheed Martin Silent Sentry 3

Form Factor: Truck Sized  
Power: >10 kW



Form Factor: <3" cross section  
Power: <10 W available

	MAX	PCL	Real-time SAR Image Formation	Onboard SAR Image Classification
System Dynamic Range (dB)	<b>120</b>	96	<b>120</b>	72
Sample Rate (MSps)	<b>5,000</b>	<b>5,000</b>	250	250
Power Efficiency (TOPs/W)	<b>100</b>	<b>100</b>	<b>100</b>	3
Correlator Length (Samples)	<b>65,536</b>	1,024 - 4,096	<b>65,536</b>	≥16

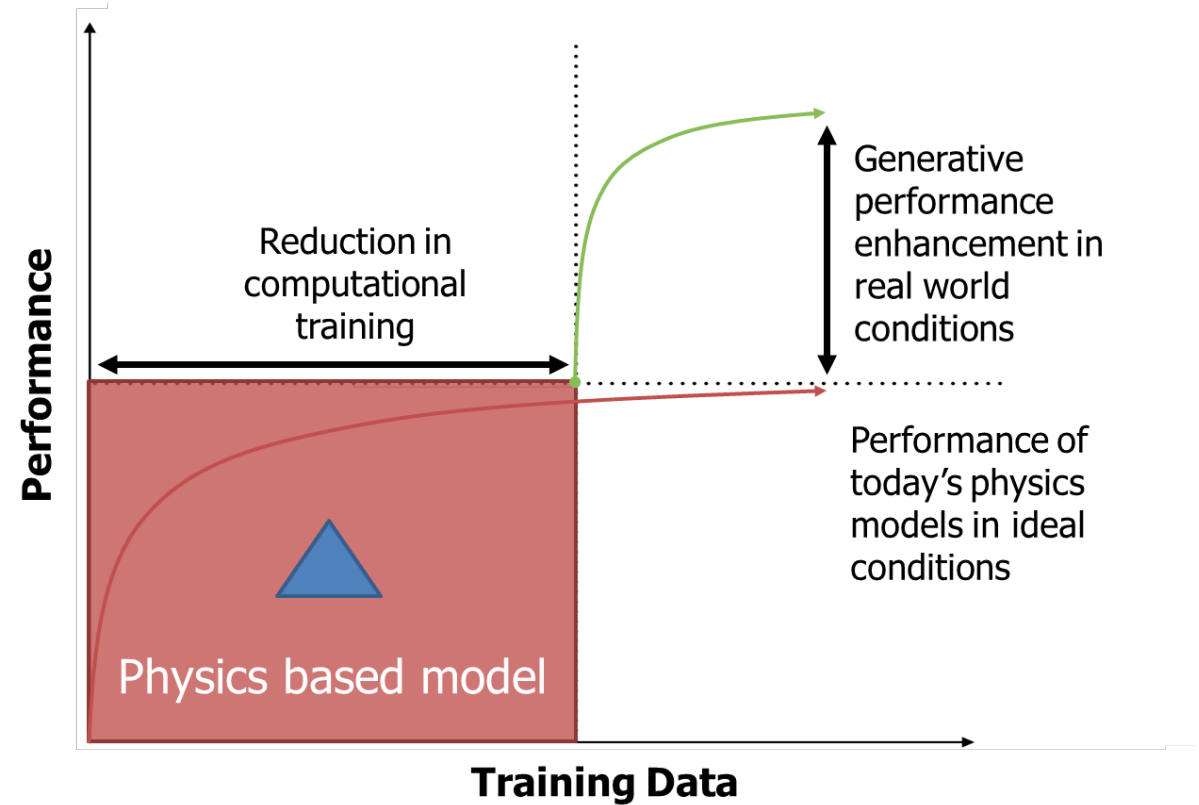
MAX will enable new mission capabilities



# SPiNN – Learning from Sparse Data

**Problem:** Static model and statistical learning approaches to signal processing are not effective at maximizing data transfer in a non-stationary nonideal channel.

**Approach:** Develop physics-based machine learning kernels with an additional adaptive transformer that can learn physics of the channel in real-time and produce optimal parameter adaptation with fallback reliability.



Physics-based machine learning for efficient training, learning, and adaptation from sparse data

References:

"Neural Network-based OFDM Receiver for Resource Constrained IoT Devices"  
<https://arxiv.org/pdf/2205.06159.pdf>

A. Bhatia, J. Robinson, J. Carmack and S. Kuzdeba, "FPGA Implementation of Radio Frequency Neural Networks," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022, pp. 0613-0618, doi: 10.1109/CCWC54503.2022.9720784.



## Disruptive Microsystems

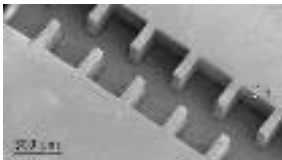




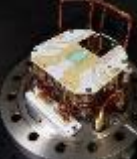

---

- **Securing communications**
- **Generating / directing high power radiation**
- **Reducing latency in electronic warfare**
- **Delivering accurate position and timing without GPS**

C4ISR: Command, Control, Communications, Computers,  
Intelligence, Surveillance, and Reconnaissance

PNT: Positioning, Navigation, and Timing

GPS: Global Positioning System

 <p><b>WARDEN</b> Technologies to defeat electronics using high power microwave energy</p>	 <p><b>MIDAS</b> Element-level millimeter wave, multi-beam digital phased arrays</p>	 <p><b>DRBE</b> Large-scale, cross-connected RF environment emulator</p>	 <p><b>WiSPER</b> Secure comms through agile and adaptive wireless interface</p>
 <p><b>PRIGM</b> Integrate improved MEMS and electronics for inertial guidance</p>	 <p><b>A-Phi</b> Photonic integrated chips technology for atomic clocks and gyroscopes</p>	 <p><b>MELT</b> Compact, modular, and efficient high energy laser sources</p>	

**Cross-cutting**



**JUMP**  
Pathfinding research in new computing and communication technologies



**JUMP 2.0**  
Fundamental research for next-generation microelectronics

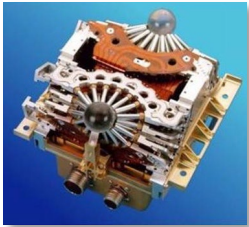
EW: Electronic Warfare  
MEMS: Micro electromechanical systems  
RF: Radio Frequency





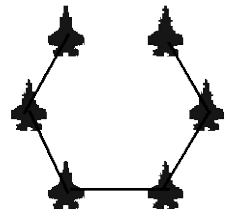
# Millimeter Wave Digital Arrays (MIDAS)

**Problem:** Today's analog antenna arrays have limited performance and functionality



F-22 and F-35 millimeter wave systems

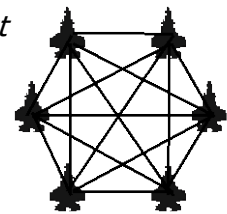
Line Topology



Network Throughput

10-100x

Multi-Beam Mesh Topology



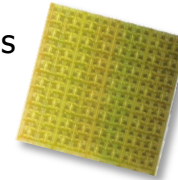
Digital arrays enable adaptive beamforming, multi-link secure communications

**Goal/Metrics:** Millimeter wave element-level digital phased arrays (18-50 GHz)

**Approach:** Prototype element-level millimeter wave digital phased arrays using state-of-the-art CMOS and 3D heterogeneous integration

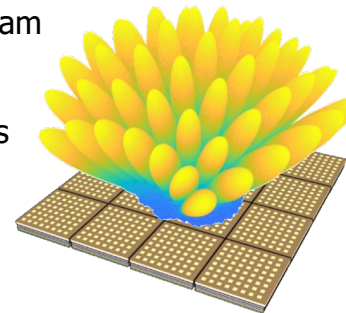
Digital Beam Forming Integrated Circuits in 12LP CMOS

- 32 Integrated Transmit/Receive channels
- Low power consumption
- Wideband 18-50 GHz, 2 GHz bandwidth

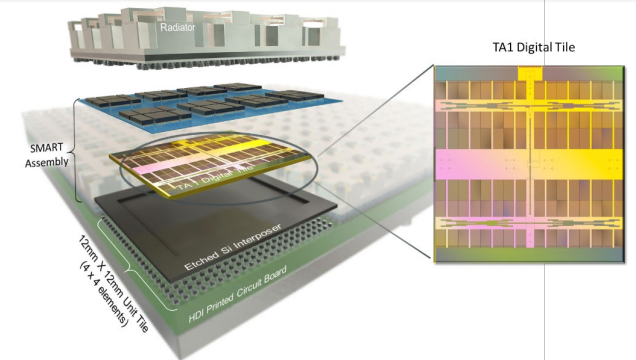


Wideband Millimeter Wave Arrays

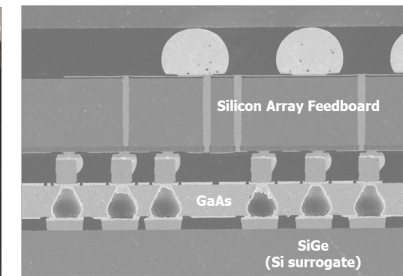
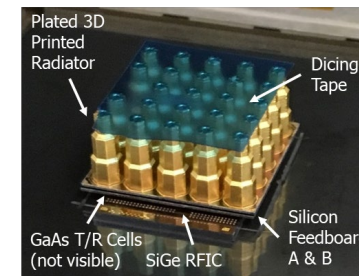
- Scalable 16 element tile for 256-element array by the end of the program
- Dual polarization
- Transmit/Receive components
- Low power consumption
- Heterogeneous packaging



**Accomplishment:** Achieved Phase 1 key metrics; Phase 2 CMOS designs are complete with array development and manufacturing underway



Raytheon 16 element, dual polarized 18-50 GHz scalable tile building block



Heterogeneous integration of compound semiconductors and 3D printed notch antenna array (left) cross-section of array stack (right) by Northrop Grumman

Element-level digital millimeter arrays for multi-beam full spatial coverage of mobile platforms

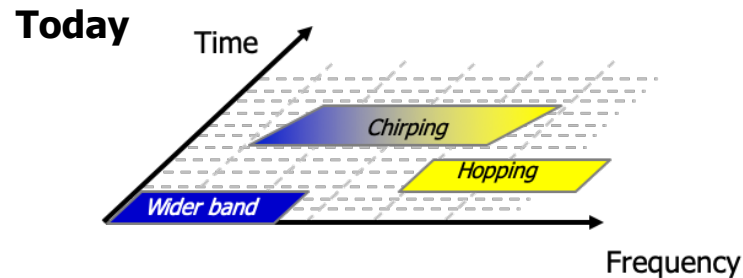


# Wideband Secure and Protected Emitter and Receiver (WiSPER)

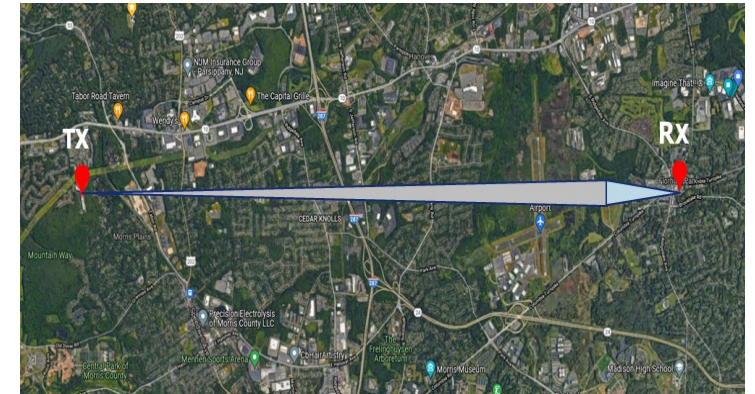
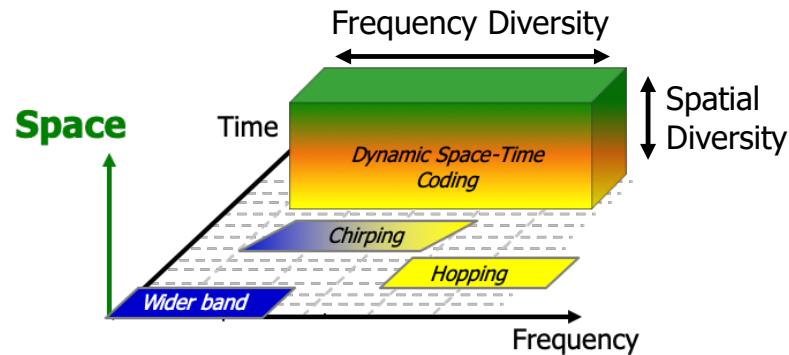
**Problem:** Spread spectrum radio signals are susceptible to detection by temporal and spatial integration

**Approach:** Increase signal diversity and complexity to avoid detection

**Accomplishment:** Worlds first measurements of wideband channel properties necessary to enable secure long range transmission

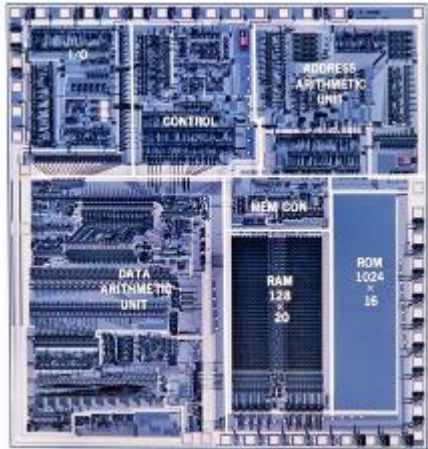


## WiSPER LPX



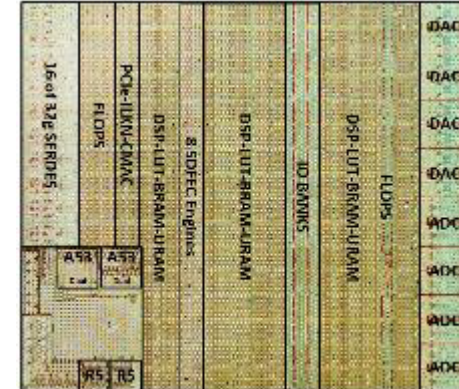
Long range point-to-point transceiver air interface to enable secure communication links

## ASIC

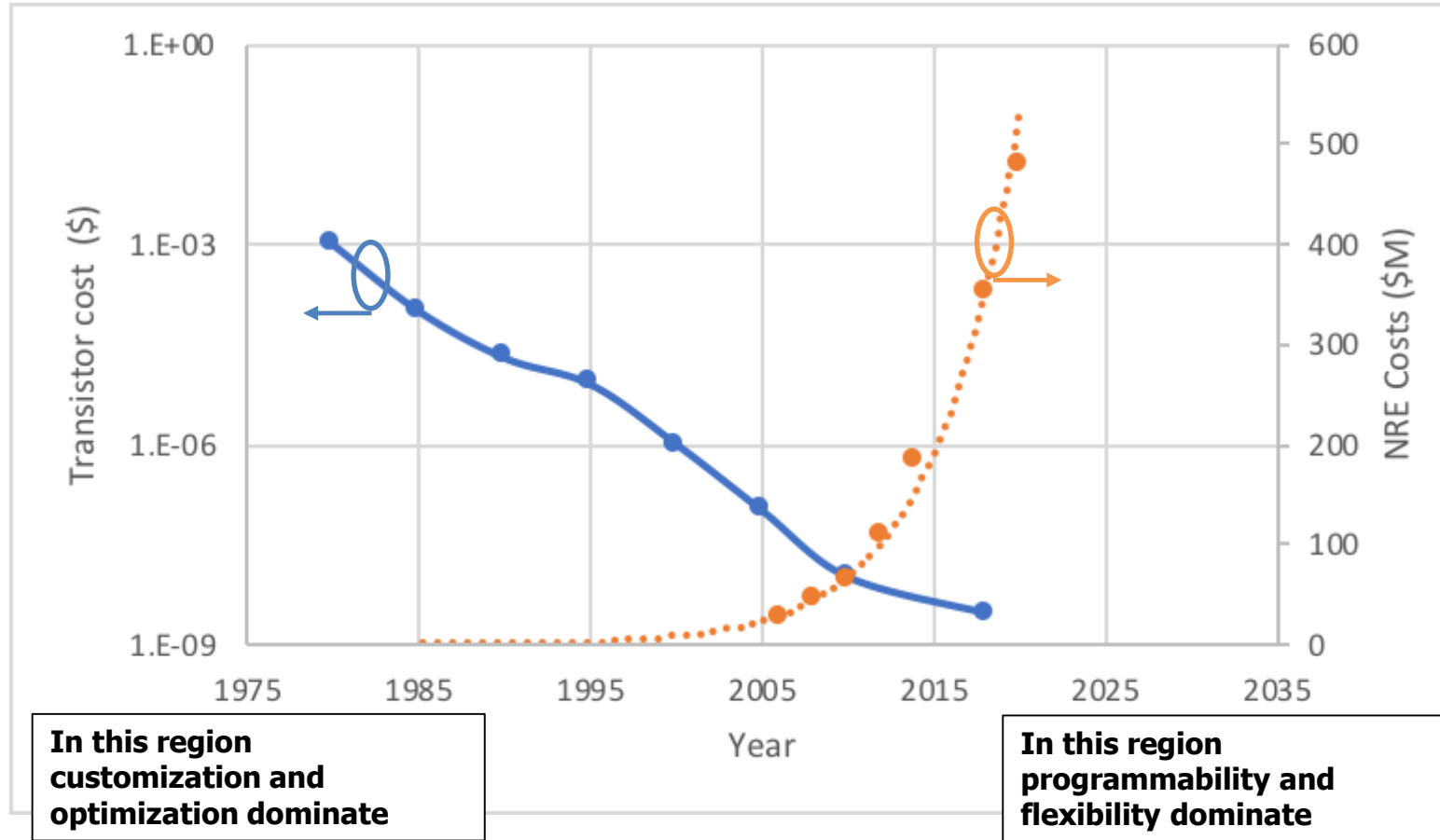


1979 Bell Labs DSP-1  
1K ROM

## PLD



2018 Xilinx RFSOC  
6 CPU, 4270 DSP, 38M  
BRAM, 22M URAM, 425k  
LUTS



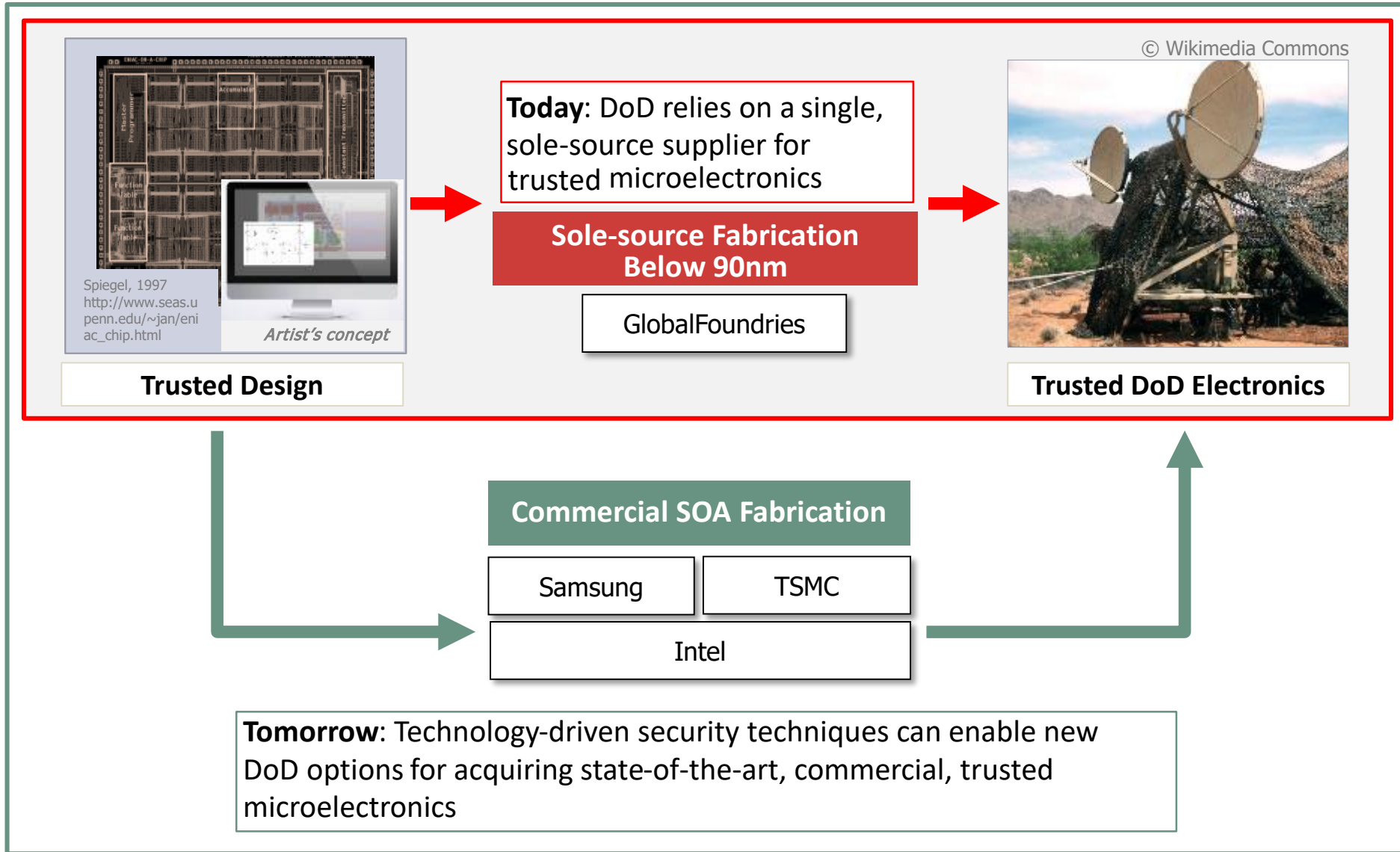
In this region  
customization and  
optimization dominate

In this region  
programmability and  
flexibility dominate

Modern SOCs are far more like PLDs than the ASICs of yore

Sources: IBS; A. Olofsson, "Silicon Compilers - Version 2.0", keynote, Proc. ISPD, 2018

# It Is the Right Time for DoD to Reflect on its Strategy

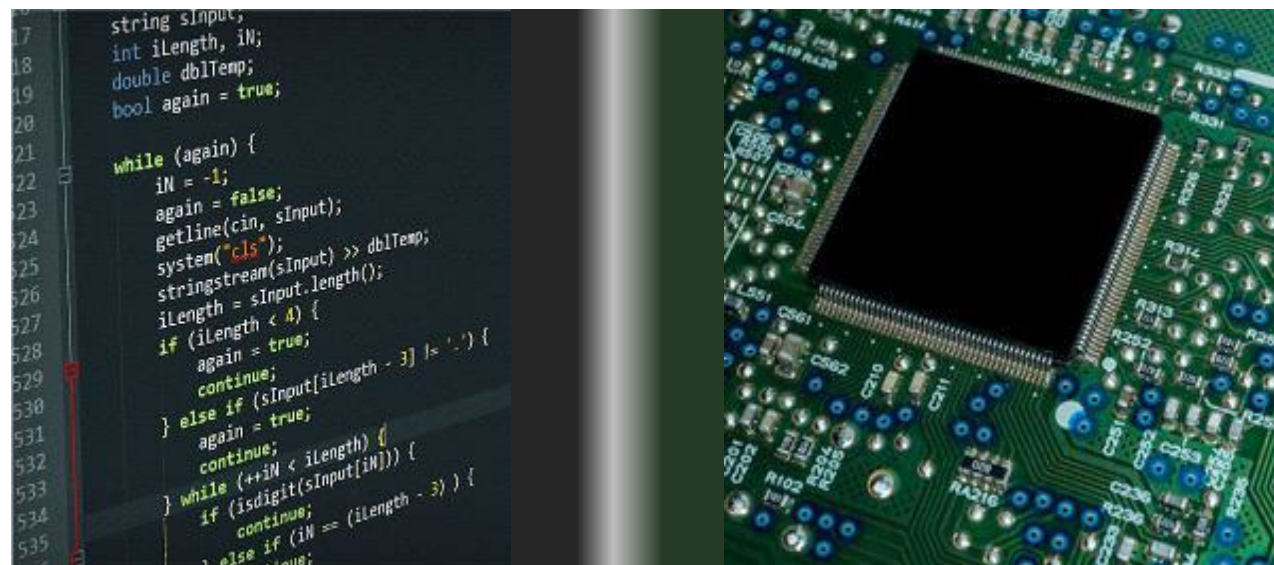






# More than Just a Military Opportunity

**Today:** Software and OS are viewed as vulnerable, hardware is treated as a trusted system level.



**Tomorrow:** Technology-driven hardware security techniques can restore trust, improve performance for cryptographic applications, and offer unique countermeasures to cyber threats.



## Commercial and **military** have common needs

- In globalized industries, how do we protect IP and **CPI**?
- How do we guard against overproduction and ensure compliance with **ITAR**?

## Some unique concerns for **military**

- Beyond commercial threats, military is uniquely concerned about **trojan** insertion
- This is a full lifecycle consideration, with efforts at design, manufacturing, distribution, and use stages

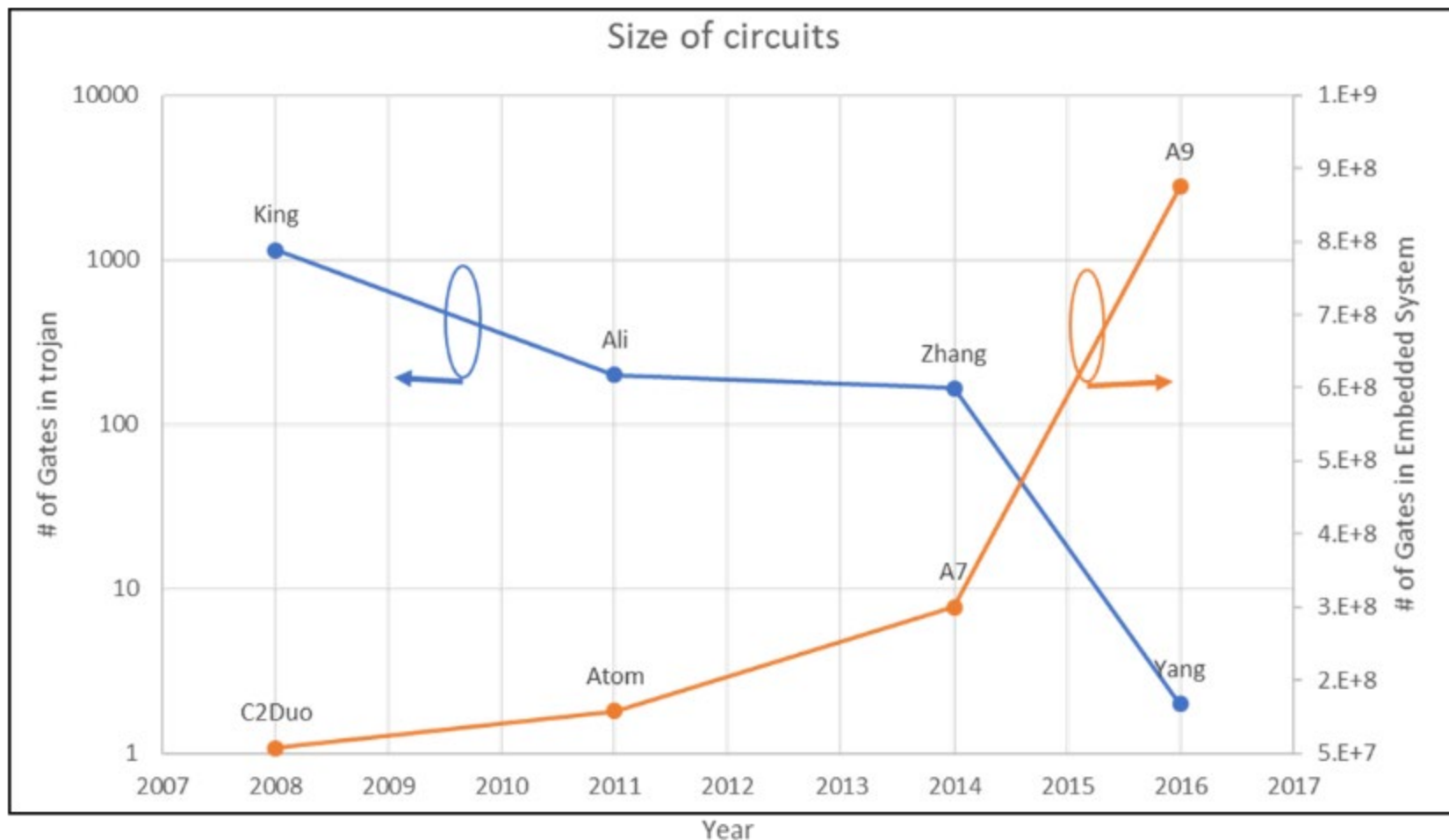
## Trust Through Technology

How can we leverage and enhance commercial practices to restore state-of-the-art electronics to our warfighters?



## Another scaling law...

- Seeking novel technology to...
- Make threat insertion and activation more difficult and easily detected
- Make reverse engineering intractable
- Minimize window of opportunity for design, placement, and testing of threats

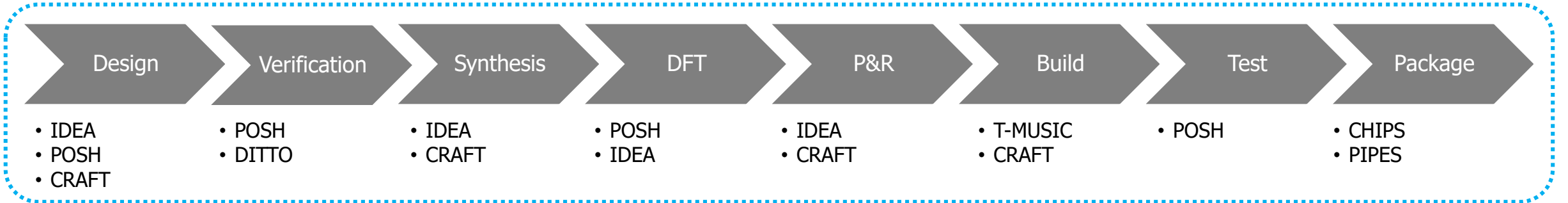


Bigger haystacks, smaller needles

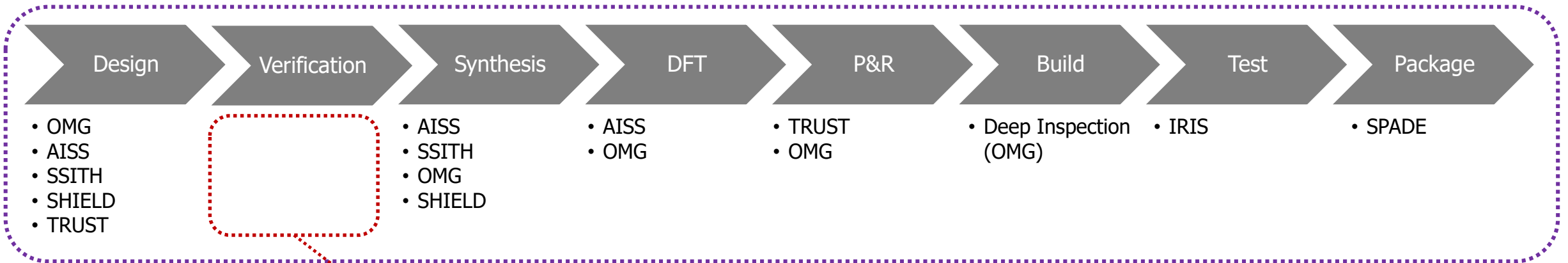


# What are we trying to do?

## Implementation Programs:



## Security Programs:

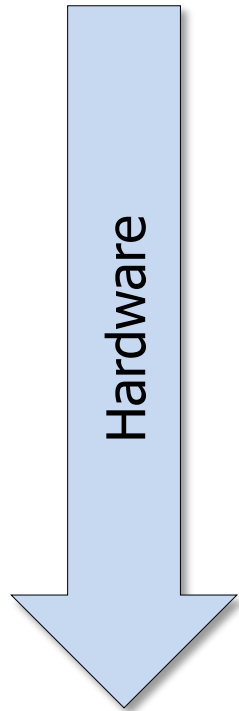
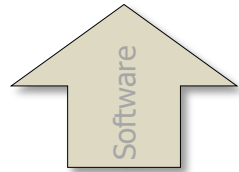


Pre-Silicon Security Signoff: The Missing Piece of the Puzzle





# Attack Surface Based Reference Model



## Moving Target (I20)

- Substantial efforts are on-going in the software community

- Alteration of system behavior based on software-accessible points of illicit entry that exist due to hardware design weaknesses or architectural flaws (SSITH)

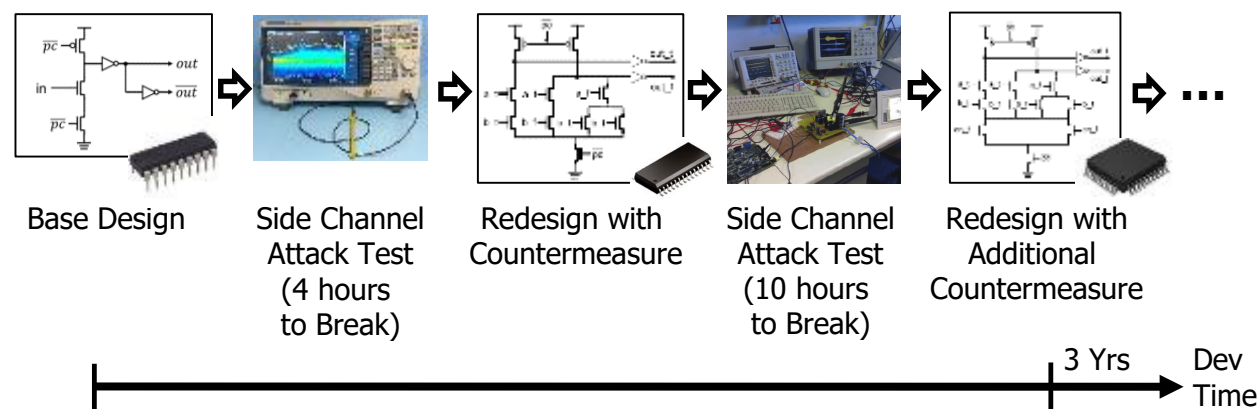
## Focus Areas

- **Side Channel** – extraction of secrets through physical communication channels other than intended (assumption: attackers are able to “listen” to emissions)
- **Reverse Engineering** – extraction of algorithms from an illegally obtained design representation (assumption: attackers have access to design files) (OMG, Deep Inspection, TRUST, IRIS)
- **Supply Chain** – Cloning, counterfeit, recycled or re-marked chips represented as genuine (assumption: attackers can manufacture perfect clones) (SHIELD)
- **Malicious Hardware** – insertion of secretly triggered hidden disruptive functionality (assumption: attackers successfully inserted malicious function(s) into the design) (AISS)

Side channels potentially exist at all levels of the design stack

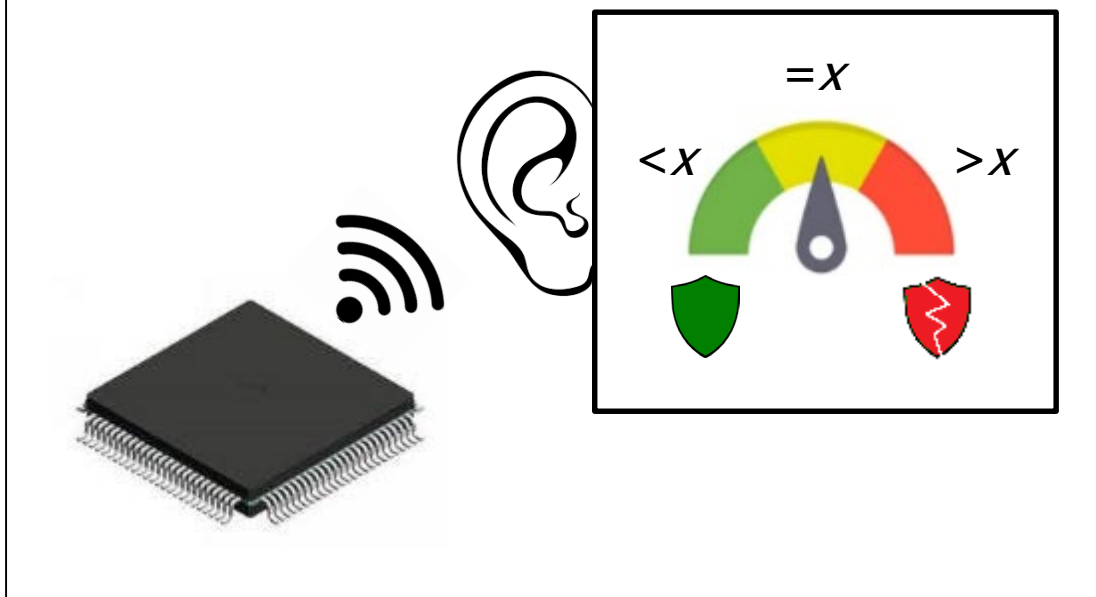
- **Application:** cryptanalysis of app data
- **Software:** control-flow side channels
- **Memory:** memory access side channels
- **Architecture:** timing side channels
- **Circuits:** physical measurement channels

Here's how we deal with them today:



- To achieve non-iterative design for security, we need pre-silicon security verification.
  - For this, two things are required:

1. Agreed-upon measurable definitions of side-channel security built around basic statements about the unintended emissions and their nature.



2. A simulation environment to measure these unintended emissions at a post-layout and software-in-the-loop stage, since emissions are linked with physical form *and* order of execution.





[www.darpa.mil](http://www.darpa.mil)