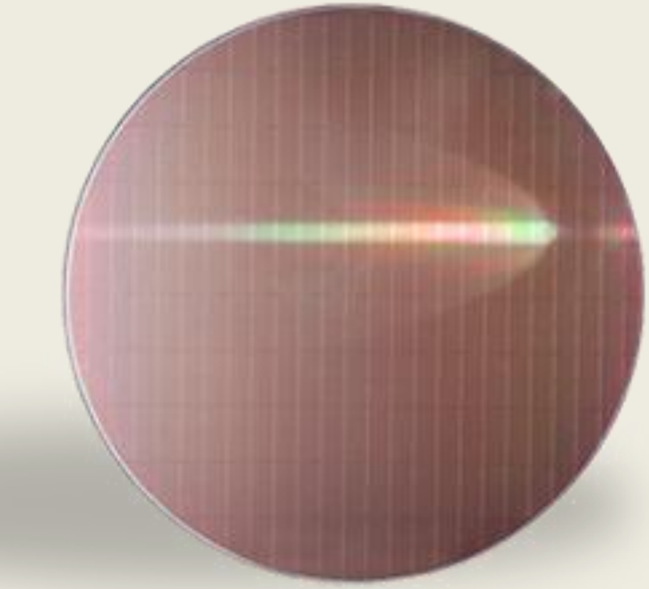


DMEA Trusted Foundry Program

NDIA Systems Engineering Meeting

December 7, 2016

Catherine Ortiz

on behalf of the DMEA Trusted Foundry Program

Today's Talk

Microelectronics in defense systems

Current situation

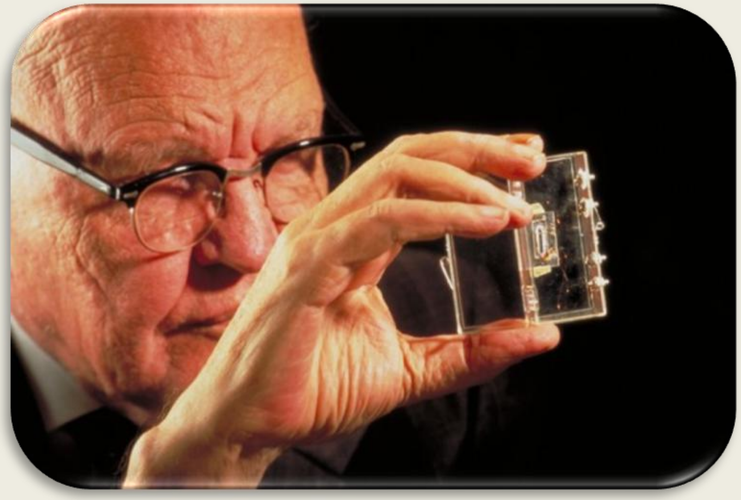
DMEA Trusted Foundry Program

Trusted Microelectronics priorities

NDIA Trusted Microelectronics
Joint Working Group

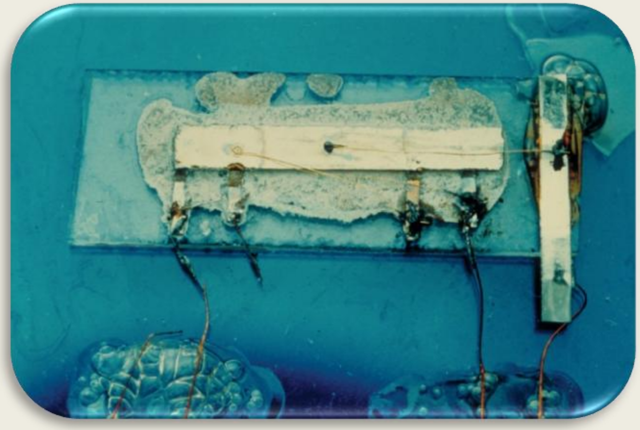
Distribution Statement A: Approved for public release: distribution unlimited.

Early Microelectronics



Nobel Laureate Jack Kilby at Texas Instruments

Kilby's original integrated circuit patented in 1959



Fairchild Semiconductor founders, 1960

Department of Defense and NASA were the primary research sponsors and key customers

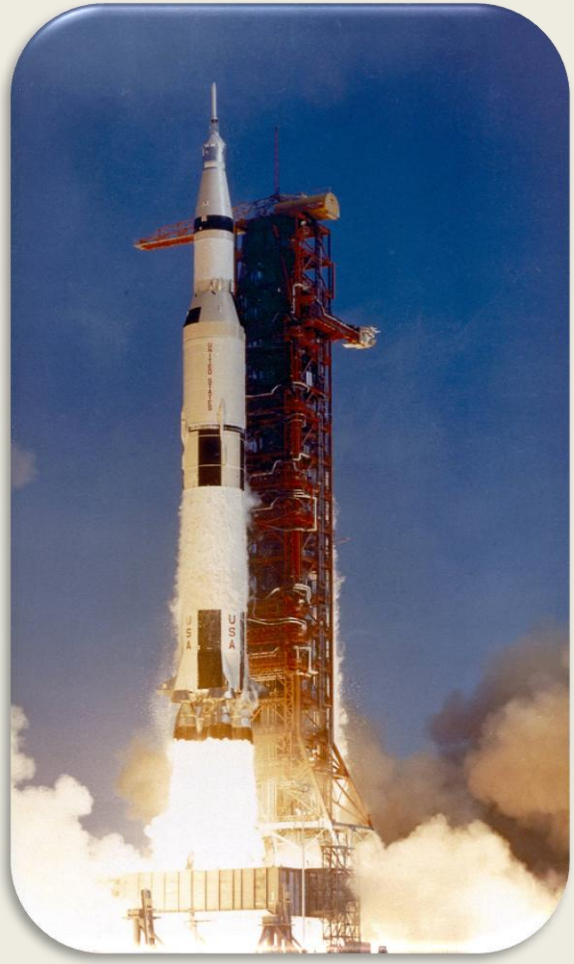
Design and manufacturing by small, self-contained teams

Performance key focus

Security not a consideration

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

Microelectronics Provide Technology Advantage



Apollo Program
First Integrated Circuits
1960s

MK 50 Torpedo Barracuda
Very High Speed Integrated Circuits
1990s

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

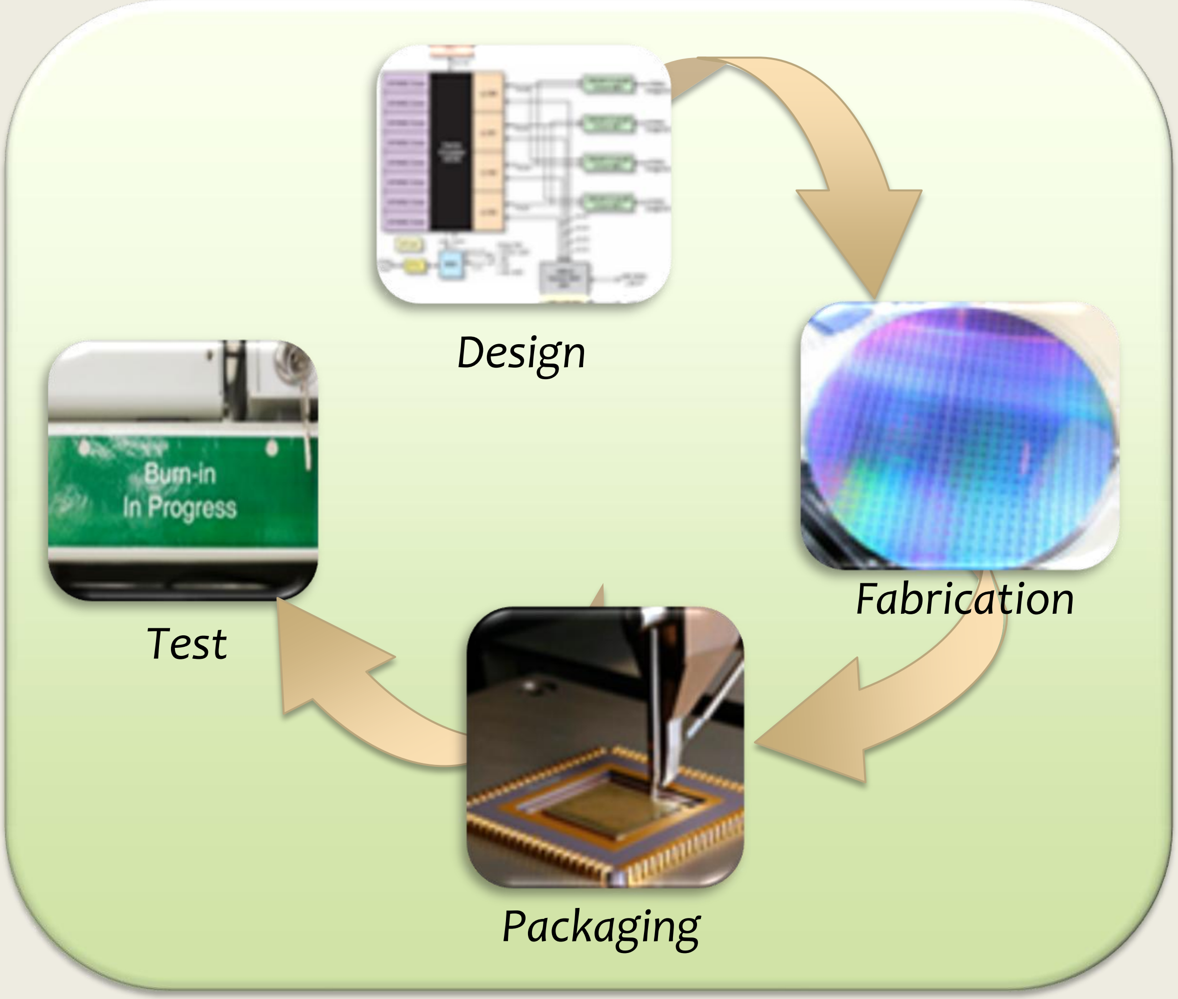
Microelectronics Provide Technology Advantage

F-22 Raptor
Digital Electronic Warfare
2000s

AH-64E Apache Guardian
Real-Time Secure Data Transfer
2010s

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

Multiple Threats in Semiconductor Production Cycle



Risks to DoD:

Lack of trustable designs

Lack of supply chain security

Tampering potential

Reverse engineering and IP siphoning

Lack of chain of custody

Unauthorized copies

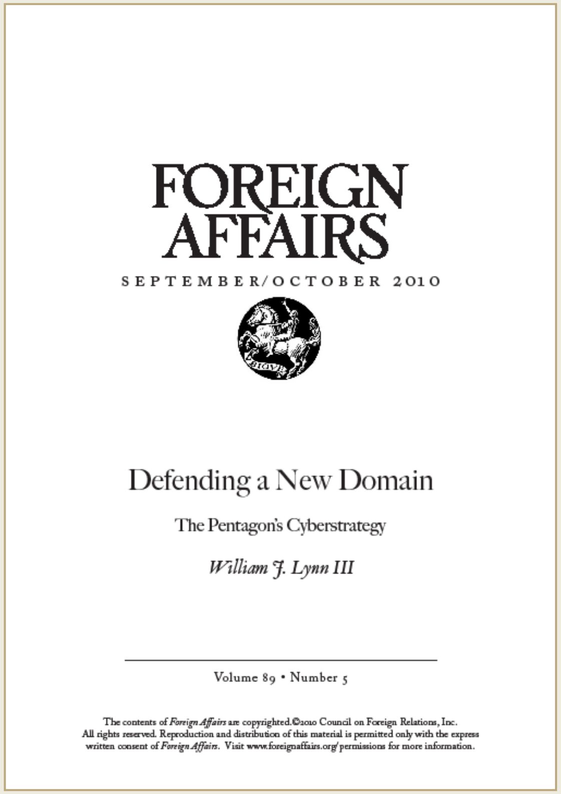
Remarking and counterfeiting

Scrap diversion

Cybersecurity hardware vulnerabilities

"The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat . . . Tampering is almost impossible to detect and even harder to eradicate . . . Remotely operated 'kill switches' and hidden 'backdoors' can be written into the computer chips . . . allowing outside actors to manipulate the systems from afar." -- Deputy Secretary of Defense William Lynn III

http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain



FOREIGN AFFAIRS

SEPTEMBER/OCTOBER 2010

Defending a New Domain

The Pentagon's Cyberstrategy

William J. Lynn III

Volume 89 • Number 5

Much of early cybersecurity discussion focused on threats from software and process vulnerabilities . . . the semiconductors may present even greater risks

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

German Missiles “Hacked By Foreign Source”

A German missile system stationed on the Turkish-Syrian border was reportedly hacked by a "foreign source" and carried out "unexplained commands".

The Patriot missiles, stationed on the Turkish side of the border under the NATO pact, were briefly taken over by an unidentified hacker, according to German civil service magazine *Behörden Spiegel.*

The magazine does not give details about what these orders were or when they were carried out, ***but suggests hackers may have gained access to the missile system through a computer chip which guides the missiles***, or through a real-time information exchange which allows the missiles to communicate with their control system.

Experts say that such a hack could lead to the battery failing to intercept incoming missiles or even firing at an unauthorized target.

Germany's President Joachim Gauck and his partner Daniela Schadt listen to commander of German troops in Turkey Colonel Stefan Drexter as they visit Patriot missile batteries in Kahramanmaras April 27, 2014.Osman Orsal/Reuters

Newsweek, July 8, 2015

Ewan Lawson, a cybersecurity expert at defense think tank RUSI, says that hacks of military missile systems may be more common than realized but go unreported for security reasons. He says that only nation-states would have the capacity to hack such a system.

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

Trusted Foundry Program Created to Mitigate Risks

- The Trusted Foundry Program (TFP) was established as a joint effort between Department of Defense and National Security Agency . . . *in response to Deputy Secretary of Defense Paul Wolfowitz's 2003 Defense Trusted IC Strategy memo*

- By the end of **FY2016, DoD has invested >$800M** for leading-edge microelectronics access and services including manufacturing for a wide array of weapon systems devices with feature sizes down to 14nm on 300 mm wafers

Program provides national security and defense programs with access to semiconductor integrated circuits from secure sources

A full range of Trusted Suppliers are available

- Trusted Foundry Program was originally implemented as a long term arrangement with IBM to secure access to leading-edge foundry technology
  - In 2007, the program was broadened to include other microelectronics suppliers to ***increase competition and ensure the entire supply chain could be trusted***
- Trusted supplier accreditation plan expanded the ranks of suppliers capable of providing trusted services ***for leading-edge, state-of-the-practice and legacy parts*** by certifying that suppliers meet a comprehensive set of security and operations criteria

Today, 76 suppliers are accredited to provide services ranging from:
design - - fab - - mask manufacturing - - packaging & testing

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

Trusted Access Program Office

- Trusted Access Program Office (TAPO) transferred from NSA to DMEA in FY2016
- TAPO contract with GLOBALFOUNDRIES US2 (GFUS2)
  - April 2016 contract awarded by DMEA provides USG and contractors access to all commercially available GFUS2 processes
    - Fab 9 (Burlington, VT) – Cat 1A Trusted Foundry
    - Fab 10 (East Fishkill, NY) – Cat 1A Trusted Foundry
  - Advanced access to other leading edge technologies
    - New: 14LPP at Fab 8 (Malta, NY)
  - Offerings
    - Foundry services: Multi-project wafer and dedicated runs
    - ASIC services
    - Handling: Cat 1A Trusted, ITAR, commercial
  - Extensive array of enterprise design IP licenses
  - **Overall period of performance through March 2023**
  - Further information: http://www.dmea.osd.mil/tapo.html

Uninterrupted access to state-of-the-art technologies

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

Trusted Suppliers Products and Services Offered

- Trusted packaging design, test and assembly
- MEMS
- Trusted product evaluations such as failure analysis, counterfeit design evaluation, environmental testing, trade studies, non-destructive testing . . .
- RAD HARD microcircuit design and fabrication

- Trusted microcircuit emulation
- Anti-cloning protection
- Trusted photomask development and parsing
- Military-grade cryptography Type 1 enabled IP cores
- Trusted ASIC and FPGA design and broker services
- Post-processing, such as wafer bumping

Trusted sources are available for a full range of microelectronics design, production, and test for leading-edge, state-of-the-practice, & legacy microelectronics

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

How to Obtain Trust

- Request trusted services via the designated point of contact at each supplier (POCs are on the accredited supplier list)
  - Ensures trusted flow will be employed
  - Ensures confidentiality of customer information

- If a Trusted device is needed, Trusted services are required at each part of the supply chain

- A Trusted service (just like ITAR) is an option
  - Commercial (untrusted) services are also available at trusted suppliers
  - Trusted services are not automatic

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

DMEA TFP FY2017 Goals – from President's Budget Request

- Continue the development inspection and analysis of application-specific integrated circuits (ASICs) and continuously refine the utilized methods for efficiency, accuracy, and applicability to multiple processes.
- Enhance the cadre of trusted suppliers for the critical trusted components and services needed for appropriate defense systems.
- Enhance Trusted Foundry products to include newly available leading edge technologies and other key specialty processes required by DoD programs.
- Expand a line of trusted catalog components, possibly including FPGAs that can be purchased by Defense contractors.
- Continue activities that ensure the DoD has Trusted Access to leading edge semiconductor technologies.
- Fully assume responsibilities and administration of the Trusted Access Program Office that was previously operated by NSA, including contractual support for state-of-the-art integrated circuit supply.

NDIA Trusted Microelectronics Joint Working Group

Launched in May 2016

- Developed in conjunction with participants from February NDIA Trusted Microelectronics Workshop
- Study teams formed to explore feasible solutions to defense systems microelectronics challenges
  - Team 1: Determining future requirements . . . *what will be needed to maintain military technology advantages?*
  - Team 2: Maintaining access to required technologies . . . *how can we counter shifts in market dynamics that may impact supply?*
  - Team 3: Trustable microelectronics standard products. . . *how can we employ standards and best practices to provide trustworthiness?*
  - Team 4: New methods to instill trust in semiconductor fabrication . . . *where will the technology solutions be available?*

Lots of Experience and Talent Focused on Core Issues

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

NDIA Trusted Microelectronics Joint Working Group

Teams: Leaders and Members

Team	Topic	Members	Leader
1	Future requirements	13	Charley Adams Northrop Grumman
2	Trustable leading edge technology access	21	Ezra Hall GLOBALFOUNDRIES U.S. 2
3	Trustable microelectronics standard products	12	Ken Lebo JACOBS Engineering
4	New methods to instill trust in semiconductor fabrication	25	Pat Hays Boeing

A Support & Integration Team Provides Assistance As Needed

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

Future Trusted Microelectronics Activities

- **NDIA Trusted Microelectronics Workshop**
  - February 2nd, 2017
    - Lockheed Martin Global Vision Center, Arlington, VA
- **NDIA Trusted FPGA Workshop**
  - Planning for FPGA workshop open to Industry and Academia that will highlight Government FPGA Working Group's progress
- **Trusted Supplier Steering Group Industry Day at GOMACTech 2017**
  - March 20th, 2017
    - Reno, NV

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

Summary

- Uninterrupted access to microelectronics technology is critical for military advantage
- Trusted Foundry Program agreement with GFUS2 through 2023
- The Trusted Accredited Supplier provides deep portfolio of products and services with 76 suppliers accredited
- Broad recognition of need for new approaches to retain trustable, leading-edge capabilities
  - NDIA Trusted Microelectronics Joint Working Group is actively pursuing technology and business-oriented access solutions
  - Government FPGA Working Group planning workshop with Industry and Academia

Trusted Foundry Program is Evolving to Meet Today's Government Microelectronics Requirements

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

- DMEA – DoD Program Management & Accreditation
  - (916) 568-4057
  - tapo@dmea.osd.mil

- DBS – Outreach (contractor)
  - (202) 683-2021
  - cjortiz@definedbusiness.com