SAND2011-3550C

Trusted Foundry

A User's Perspective

23 May 2011

Robert Lovejoy, SMTS,
Mixed Signal ASIC/SoC Products, 1735

Sandia National Laboratories
Albuquerque, New Mexico

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2009-0357P

Sandia National Laboratories

Outline

- **Sandia and the Trusted Foundry**
- **The Need for Trust**
- **Trusted Access Program Office**
  - IBM Trusted Foundry
- **User's Perspective**

Sandia and the Trusted Foundry

Sandia National Laboratories

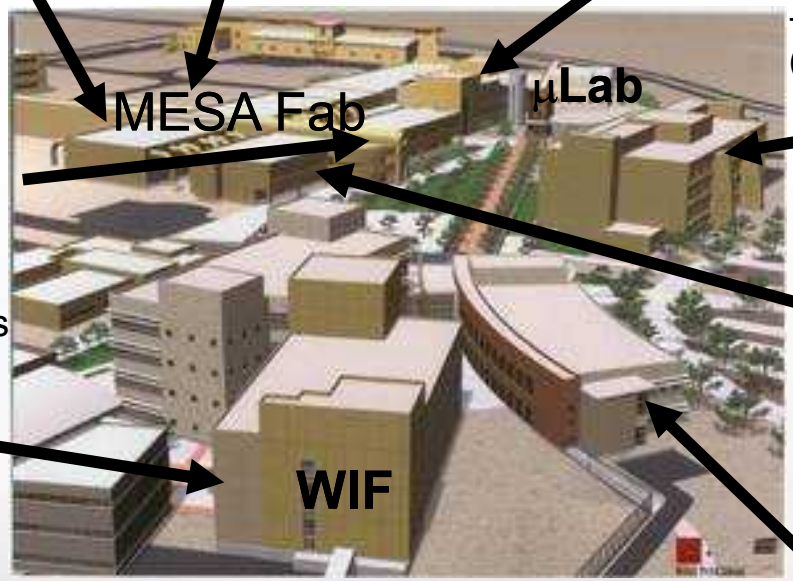
MESA is a 400,000 Sq-ft Complex with over 650 employees

Silicon Fab: *Microelectronics*
Unique custom and rad-hard process technologies
- Trusted Foundry status
- Strategically rad-hard devices and circuits unavailable from other potential providers

Trusted Design:
Expertise in custom design of integrated circuits
- Secure microcontrollers
- Analog/Digital/RF
- IBM Trusted Foundry
- Tamper Resistant Features

Packaging & Qualification:
Custom packaging & COTS qualification
- Advanced packaging
- Custom components (cables, connectors, capacitors, frequency devices, magnetics)

Silicon Fab: *Micromachining*
Deposition, patterning reactive ion etching for micromachines.
- Surety components
- Embedded surveillance including communication



MicroLab:
World's most extensive growth and processing of III-V semiconductor devices
- Neutron-immune Heterojunction Bipolar Transistors
-Rad-hard optical links
-Solid-state radio-frequency devices (radar and communications)

Nanotechnology:
Advanced sensors
Options for novel devices

Failure Analysis:
Microsystems reliability & failure analysis expertise
- Vulnerability analysis in NW systems

Design, Modeling,& Simulation:
3-D system analysis

Sandia has Class 1A certification for both Trusted Design and Trusted Foundry

- In response to the decline of the US IC manufacturing industry, the DoD established a Trusted Foundry and Supplier network
- "Trust" involves assuring the people, processes, and material used to design, manufacture, and distribute national security critical components
- Sandia is a member of this network for both foundry (IC manufacturing) and design services
- Critical Government systems need trusted components

ACCREDITATION OF TRUST

Microelectronics Trusted Source
CATEGORY 1A

By these presents the undersigned expresses the confidence of the Department of Defense, Defense Microelectronics Activity (DMEA) in the ability of the organization known as

Sandia National Laboratories
Microsystems, Science, Technology and Components

to deliver trusted foundry microelectronic goods and services to end users within the United States Government that correspond to Trusted Category 1A which meets Mission Assurance Category 1 as defined by Instruction 8500.2 of the Department of Defense Directives, effective this date.

042	14213	3 Aug 2009	7 Jan 2011
Site Accreditation Number	Cage Code	Effective Date	Renewal Date

Ted Blum
Director, Defense Microelectronics Activity

SCOPE OF ACCREDITATION

Sandia National Laboratories
Microsystems, Science, Technology and Components

IS ACCREDITED FOR TRUST IN THE FOLLOWING FIELD(S):

CATEGORY	FIELD
1A	Design Services
1A	Foundry Services

042	14213	3 Aug 2009	7 Jan 2011
Site Accreditation Number	Cage Code	Effective Date	Renewal Date

Successfully designed in our internal trusted foundry and the IBM trusted foundry

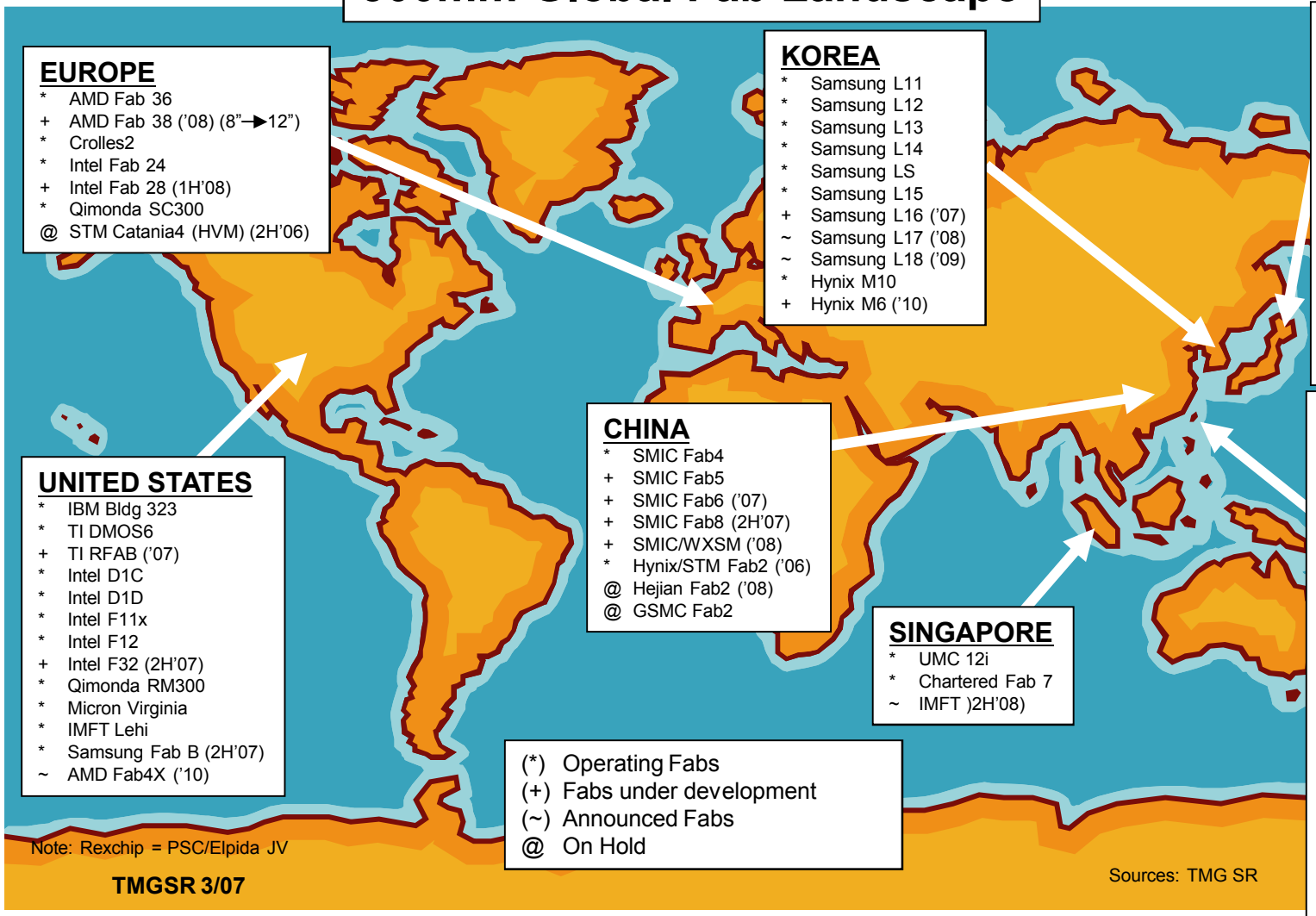
- **Sandia has delivered several thousand custom components to the US Government through our internal trusted foundry (350nm, 3.3v technology)**
  - NW Programs
  - Satellite Programs
- **We were one of the 1st users of the IBM trusted foundry and have worked with our customers to design a diverse set of ICs at several process nodes**
  - FY07 (and earlier) Designs
    - 5 at IBM CMOS8RF, 130nm technology
    - 1 at IBM CMOS9LP, 90nm technology
  - FY08 Designs
    - 6 at IBM CMOS8RF, 130nm technology
    - 1 at IBM CMOS9LP, 90nm technology
  - FY09 Designs
    - 4 at IBM CMOS8RF, 130nm technology
    - 4 at IBM CMOS9LP/SF, 90nm technology
    - 1 at IBM CMOS10SF, 65nm technology
  - FY10 Designs
    - 3 at IBM CMOS8RF, 130nm technology
    - 1 at IBM CMOS9LP/SF, 90nm technology
    - 1 at IBM CMOS10SF, 65nm technology
    - 3 at IBM CMOS12SOI, 45nm technology
  - FY11 Projected Designs (so far)
    - 2 at IBM CMOS9LP/SF, 90nm technology
    - 1 at IBM CMOS12SOI, 45nm technology

The Need for Trust

Sandia National Laboratories

US Microelectronics manufacturing capability continues to move off-shore

300mm Global Fab Landscape



EUROPE
- * AMD Fab 36
- + AMD Fab 38 ('08) (8"→12")
- * Crolles2
- * Intel Fab 24
- + Intel Fab 28 (1H'08)
- * Qimonda SC300
- @ STM Catania4 (HVM) (2H'06)

KOREA
- * Samsung L11
- * Samsung L12
- * Samsung L13
- * Samsung L14
- * Samsung LS
- * Samsung L15
- + Samsung L16 ('07)
- ~ Samsung L17 ('08)
- ~ Samsung L18 ('09)
- * Hynix M10
- + Hynix M6 ('10)

JAPAN
- * Matsushita Uozu
- * Renesas Fab2
- * Renesas Fab3
- * Sony Kyushu (CCD)
- * Sony Fab2 Nagasaki
- * Toshiba Oita
- * Toshiba Fab3
- + Toshiba Fab4 ('07)
- @ Toshiba Fab5
- * Elpida E300
- + Elpida E200 (8"→12")
- * NEC Yamagata
- * Fujitsu Fab No.1
- + Fujitsu Fab No.2
- + Spansion SP1 (2H'07)

UNITED STATES
- * IBM Bldg 323
- * TI DMOS6
- + TI RFAB ('07)
- * Intel D1C
- * Intel D1D
- * Intel F11x
- * Intel F12
- + Intel F32 (2H'07)
- * Qimonda RM300
- * Micron Virginia
- * IMFT Lehi
- * Samsung Fab B (2H'07)
- ~ AMD Fab4X ('10)

CHINA
- * SMIC Fab4
- + SMIC Fab5
- + SMIC Fab6 ('07)
- + SMIC Fab8 (2H'07)
- + SMIC/WXSM ('08)
- * Hynix/STM Fab2 ('06)
- @ Hejian Fab2 ('08)
- @ GSMC Fab2

SINGAPORE
- * UMC 12i
- * Chartered Fab 7
- ~ IMFT)2H'08)

TAIWAN
- + VisEra Fab 1 ('07)
- * Inotera Fab1
- + Inotera Fab2 ('07)
- ~ Inotera Fab3
- + Nanya Fab3
- * Powerchip Fab 12A
- * Powerchip Fab 12B
- * Powerchip Fab12M
- + Rexchip R1 ('07)
- + Rexchip R2 ('09)
- ~ Rexchip R3
- ~ Rexchip R4
- + ProMOS Fab 1 (8'→12")
- * ProMOS Fab 2
- * ProMOS Fab 3
- + ProMOS Fab 4 ('07)
- * TSMC Fab 12
- * TSMC Fab 14
- ~ TSMC Fab 15
- * UMC Fab 12A
- * UMC Fab 12B
- * Winbond FabA
- + Winbond Fab B ('07)

(*) Operating Fabs
(+) Fabs under development
(~) Announced Fabs
@ On Hold

Note: Rexchip = PSC/Elpida JV

TMGSR 3/07

Sources: TMG SR

Most of the world's accessible and leading-edge foundry capacity is in Asia

Recent Examples: Possible design manipulation to provide backdoor access

DANGER ROOM WHAT'S NEXT

HOME | SUBSCRIBE » | SECTIONS » | BLOGS » | READ MAGAZINE | Search

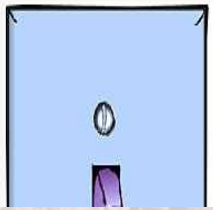
« Army: Make Us a Mini-Drone Swarm (Updated) | Main | Pentagon's Project Minerva Sparks New Anthro Concerns »

Pentagon Looks for 'Killer Switch'

By Sharon Weinberger | May 01, 2008 | 2:48:00 AM | Categories: DarpaWatch

Imagine if the F-35 Joint Strike Fighter could be effectively shut down by a foreign adversary with the flip of a switch? That's, in part, the the concern behind the Defense Advanced Research Project Agency's Trust in Integrated Circuits program, reports *IEEE Spectrum*, in a fascinating article that explores the underbelly of national security and globalization:

Last September, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of a Syrian radar—supposedly state-of-the-art—to warn the Syrian military of the incoming assault. It wasn't long before military and technology bloggers concluded that this was an incident of electronic warfare—and not just



InfoWorld Home / Security Central / News / Malicious microprocessor opens new doors for...

APRIL 15, 2008

Malicious microprocessor opens new doors for attack

Researchers have found a difficult but viable method for hacking a PC's microprocessor -- an attack that would be devastating and virtually undetectable

By Robert McMillan | IDGNS

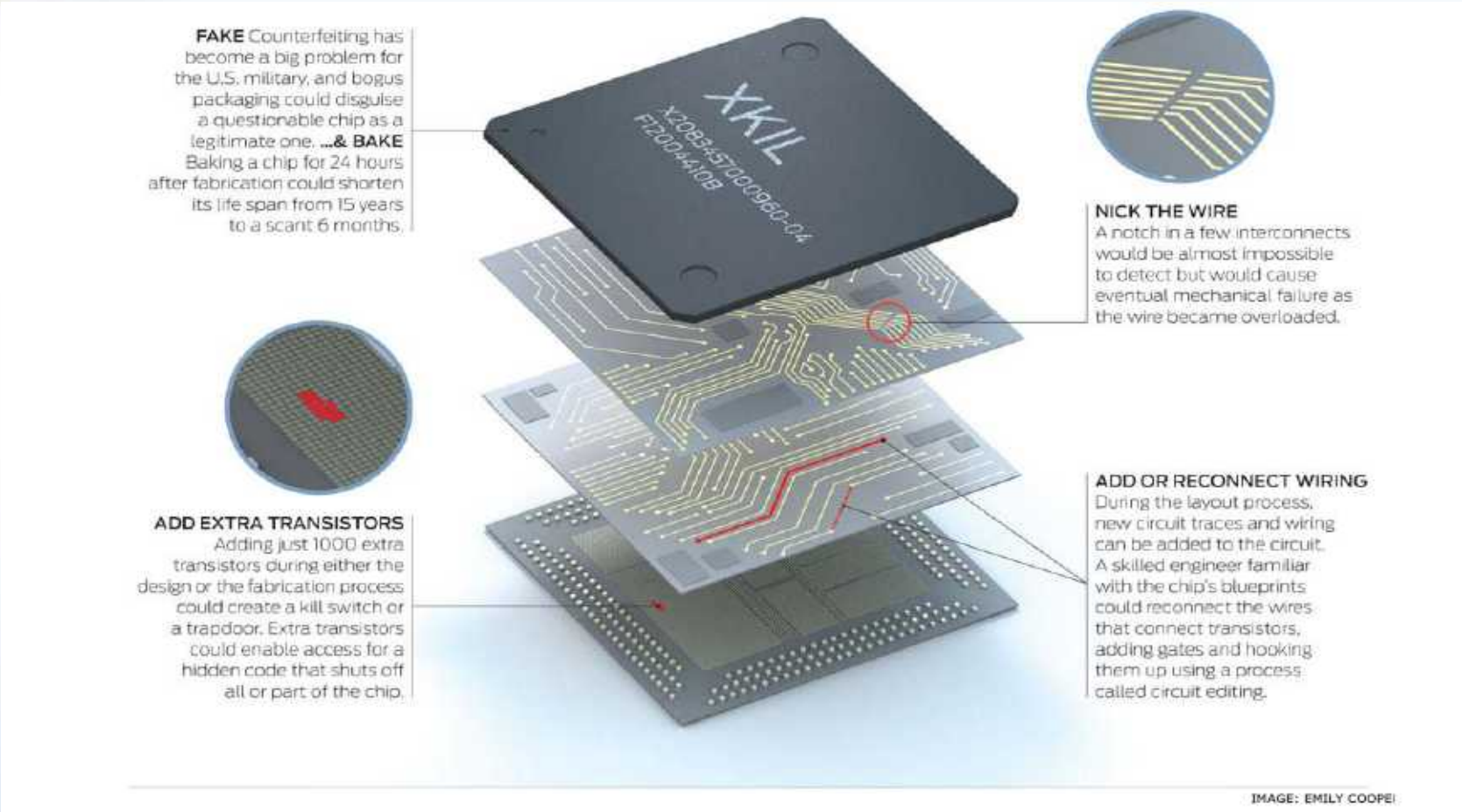
| Print | Add a comment | ★ Recommend This

For years, hackers have focused on finding bugs in computer software that give them unauthorized access to computer systems, but now there's another way to break in: Hack the microprocessor.

On Tuesday, researchers at the University of Illinois at Urbana-Champaign demonstrated how they altered a computer chip to grant attackers backdoor access to a computer. It would take a lot of work to make this attack succeed in the real world, but it would be virtually undetectable.

To launch its attack, the team used a special programmable processor running the Linux operating system. The chip was programmed to inject malicious firmware into the chip's memory, which then allows an attacker to log into the machine as if he were a legitimate user. To

IEEE Spectrum Article



At each step of the hardware design process, a saboteur could make a particular part of the circuit fail. A typical microprocessor can have up to eight layers and any layer on a microchip can be targeted. **Ref: IEEE Spectrum, 5/02/08**

Trusted Access Program Office
& Trusted Foundry

Sandia National Laboratories

Trust Definition and Source Responsibility

The Meaning

Trust is defined as "the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components."
Michael Wynne Acting USD AT&L (27 January 2004)

Trusted Source Responsibility

Trusted source provides custody and control that must be maintained throughout ALL phases of IC Design Cycle

- Assure "**Chain of Custody**" (People, Facilities, Data, Artifacts) AT ALL TIMES for both classified and unclassified ICs
- Ensure that there will not be any reasonable threats related to **disruption of supply**
- Prevent **intentional or unintentional modifications** or tampering of ICs
- Protect ICs from unauthorized attempts at **reverse engineering**, exposure of functionality or evaluation of their possible vulnerabilities

Michael Wynne Acting USD AT&L (27 January 2004)

Trusted Access Program Office

- **Established to provide path for DoD and Intelligence Community Guaranteed Access to Trusted Microelectronics Technologies**
  - Guaranteed Access to Trusted Foundry Suppliers (on-shore)
  - Ability to Fabricate Classified Designs
  - Leaded Edge Technologies (Low Volume)
  - Quick Turnaround for Prototyping and Production
  - Technology Support through Industry Partnership
  - Access to Intellectual Property
  - Facilities Upgrade Cost Avoidance
- **Access is Limited to Government Only**

TAPO Key Players

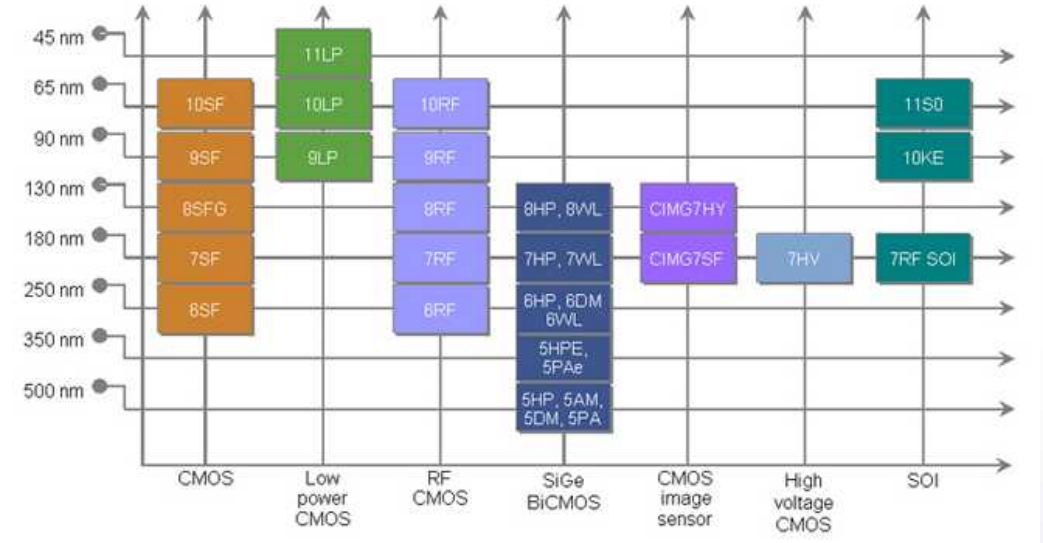
- **Trusted Access Program Office**
  - Contract Management
  - Engagement Path
  - Customer Service
- **IBM Corporation**
  - Foundry Access
  - Design, Test, and Packaging
  - Access to IBM ASIC Flow
- **Kansas City Plant**
  - Multi-Project Wafer Management
- **Abraxas Corporation**
  - Intellectual Property Management
- **Defense Microelectronics Activity**
  - Accreditation Services

IBM Trusted Foundry

- **IBM Trusted Foundry**
  - 7th Year of 10 Year Contract
    - Contract Extensions in Progress
  - $80M Annual Cost for Trusted Access
    - Leading-Edge Foundry Access
    - Capacity Reservations
    - On-Shore
    - Intellectual Property
    - Access to Commercial Technologies

IBM Trusted Foundry

- **Variety of Foundry Options**
  - CMOS
  - Low Power
  - RF CMOS
  - SiGe
  - High Voltage
  - SOI
- **Advanced Access Down to 32nm**
- **Subsidized MPW Runs Available Through KCP**
- **Developed Design Kits**
- **Variety of IP**
  - IBM
  - ARM
  - Virage
  - Aragio

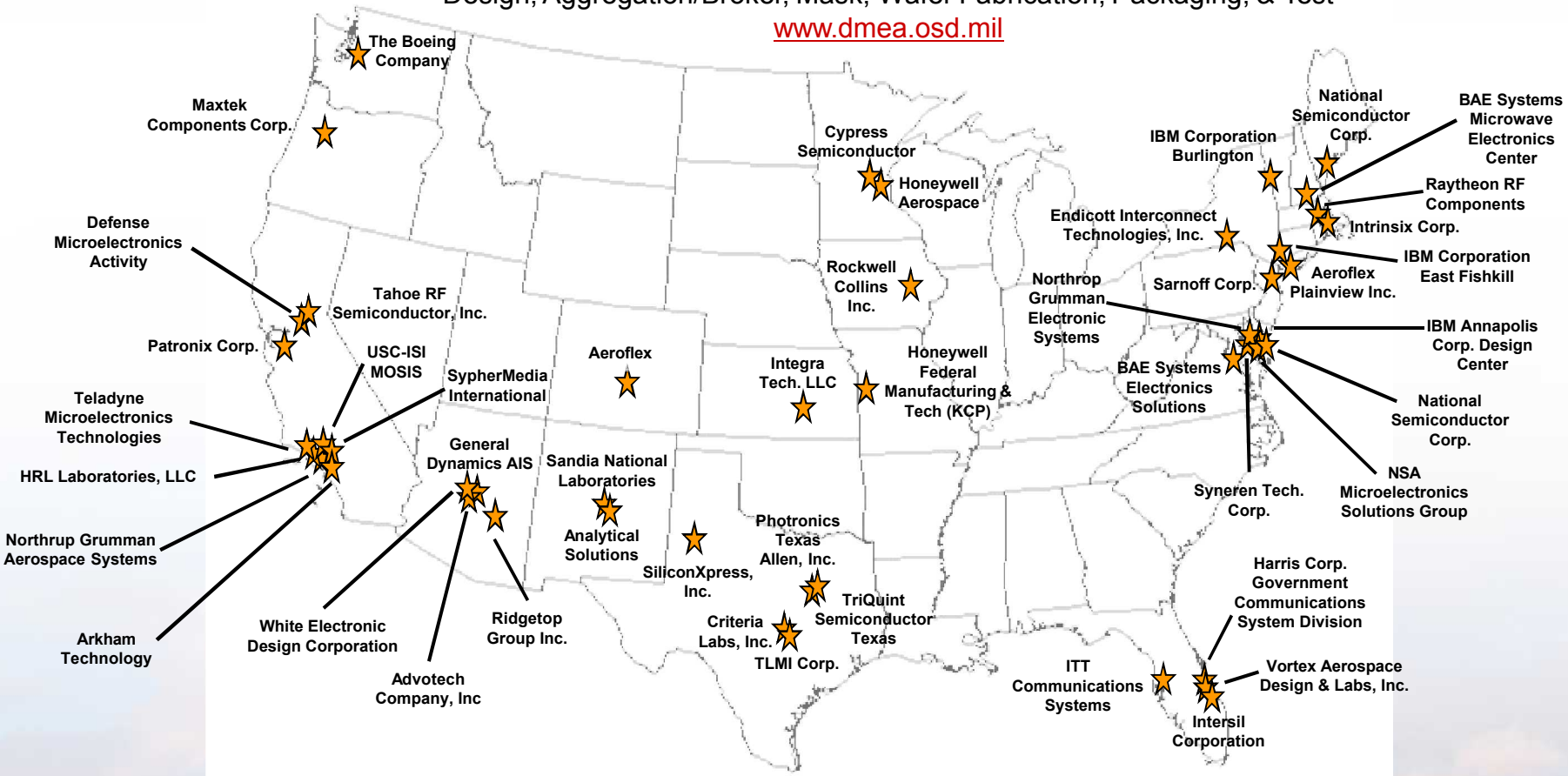


Trusted Suppliers

48 Accredited Suppliers

Design, Aggregation/Broker, Mask, Wafer Fabrication, Packaging, & Test

www.dmea.osd.mil



Sandia National Laboratories

User's Perspective

Sandia National Laboratories

The Good and The Not So Good

- **The Good**
  - Government Access to Leading-Edge On-Shore Microelectronics Fabrication (down to 32nm)
  - Government Subsidized MPW Runs at the IBM Trusted Foundry at several process nodes
    - Supports Low Volume
    - Supports Research and Development Prototyping
    - Advanced nodes heavily subsidized for affordable access
  - Government Purchased Intellectual Property available for use

- **The Not so Good**
  - Eggs in One Basket – IBM
  - Trusted Suppliers (other than IBM) not Seeing Trusted Business Case
  - No Trusted IP Supplier or Path for Trusted IP

Trusted References

- www.tapoffice.org
- http://www.dmea.osd.mil/trustedic.html
- http://www.nsa.gov/business/programs/tapo.shtml
- http://www.trustedfoundryprogram.org/
- www.ibm.com
- http://www.sandia.gov/mstc/trusted/microsystems.html