TRUST,
A Proposed Plan for Trusted Integrated Circuits

Dean. R. Collins
Deputy Director Microsystems Technology Office
Defense Advance Research Projects Agency
Microsystems Technology Office
3701 N. Fairfax Drive
Arlington, VA, US, 22203-1714
Dean.collins@darpa.mil

Summary: This paper outlines a DARPA's Plan for Producing Trusted, Low Volume, Affordable, Fast Cycle Time, RADHard IC's. While the plan is still in the formulation stage it is based on solid military needs and has significant technical challenges. An initial estimate of a number of hard problems has been documented and plans are outlined to scope solutions to these problems. The program is being formulated to get maximum exposure from out-of-box thinking while still protecting a U.S. advantage and maintaining the ability to interact with classified U.S. government programs.

Introduction and Background

The Defense Science Board Report of February 2005 on High Performance Microchip Supply [1] makes the following points:

For the DoD's strategy of information superiority to remain viable, the Department requires trusted, affordable, timely supply of integrated circuits (ICs) as a continued stream of exponential improvements in the processing capacity of microchips and new approaches to extracting military value from information. Technical aspects of trusted circuits involve all aspects of Design, IC fabrication & IC packaging.

A small number of special circuit IC components are essential for the nation's defense. Many have no commercial demand, such as radiation hardening, high power microwave, mm-wave and sensors.

Global economic pressures are driving IC design and manufacturing to foreign soil and out of U.S. control to ensure trust and availability. Taiwan, PRC, Singapore, Korea, and Japan are where modern chip fabrication plants are presently being built. The cost for building a 300-mm wafer, 65-nm chip fabrication plant is approaching $3 billion.

The above facts create significant future vulnerability for critical systems because trust cannot be added to circuits after fabrication. The reverse engineering cannot be relied upon to detect undesired IC alterations, and "Trusted Foundry Program" provides an interim measure for Trusted high performance ICs –on a "take or pay" basis.

The DSB Report covers a wide range of suggestions to reverse these trends; the DARPA TRUST effort responds to a number of these suggestions which are of a technical nature. The DARPA TRUST effort is not synonymous with RADHard, affordable, low volume and fast cycle time, but many customers for trusted parts also desire these other attributes. Trustworthy computing is a much broader issue than just having trusted ICs; however trustworthy computers cannot exist until we have Trustworthy hardware to build them on.

Military Concerns

The old model where the U.S. had complete control of the design and fabrication of IC's is no longer a reality. What is being more and more prevalent is the model where the process is increasingly more vulnerable to potential attack.

Many weapon systems prime contractors do not know the origin of the integrated circuits in their systems, and leave the practice of supply chain management up to their subcontractors. Most U.S. weapon systems under development contain a significant fraction of their integrated circuit electronics from overseas, mainly Asia.

In most state-of-the-art IC development there is a close coupling between fabrication and design. As IC fabrication moves off-shore, design is following it. There are many opportunities for the introduction of unwanted features into the integrated circuit during the design cycle.

In order to formulate an effective TRUST effort it is necessary to define the nature of a potential adversary. For the purposes of the TRUST effort, is assumed that the adversary is a nation/state with modern semiconductor capability that has the motivation, opportunity, talent, manpower & time/patience to do significant harm to the US. It is furthermore assumed that the adversary has the same or better offensive technology than the U.S.

Anti-Tamper

Anti-tampering is a concern for the U.S. Government sales of weapon and communication systems to second parties. Unintentional or combat loss of weapon systems is also a concern. Anti-tamper is concerned with both hardware and software attacks. All DoD systems must now have a critical program information plan, which is the system PM's responsibility. This critical program

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
20 MAR 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
TRUST, A Proposed Plan for Trusted Integrated Circuits	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Advance Research Projects Agency Microsystems Technology Office 3701 N. Fairfax Drive Arlington, VA, US, 22203-1714**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202011, GOMACTech-06 Government Microcircuit Applications and Critical Technology Conference Held in San Diego, California on March 20-23, 2006.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**2**	

information plan must include anti-tamper implementation. Many of the aspects of the trusted effort are of interest to the anti-tamper community.

Commercial Sector Concerns

The commercial sector also has concerns relating to the protection of intellectual property stored and used on IC's. Smart Cards/Smart Keys, Cell Phones and Set Top Boxes are all examples of items where the content of the IC has value. These devices have been subjected to both reverse engineering and side channel attacks. Commercial reverse engineering services are available. There are also documented cases of IC mislabeling and IC counterfeiting that has occurred. The commercial sector has developed many techniques and procedures to protect intellectual property, and the government can benefit from commercial practices.

Hard Problems

DARPA's initial look at the issue of TRUST has resulted in a list of hard problems, such as:

- How do you Trust the design cycle to faithfully generate only the microelectronics desired?

- How do you Trust microelectronics chips when they are manufactured in a non-Trusted facility, such that they will faithfully perform only the function they are designed for?

- How do you Trust that the testing on the microelectronic chips will faithfully determine that the chip will operate only as designed. (no more–no less)?

- How do you know that the packaging of the chip does not introduce features into or misidentify the chip? How do you determine that the packaged chip has not been tampered with after installation, and how do you communicate the fact of tampering?

Existing DARPA efforts

DARPA has had a number of efforts underway that address various aspects the issue of trusted ICs. Examples are radiation hardness by process, radiation hardness by design, asynchronous logic, macroelectronics, reconfigurable chip, radioactive power source and 3D integrated circuits.

Metrics for Evaluating TRUST

At present, no metrics for TRUST exist, nor do any metrics exist even for anti-tamper. Previous approaches to this issue have not proved fruitful according to well recognized experts [2]. Any significant program in the TRUST area will depend on metrics to measure progress. It is recognized that TRUST will not come for free. In addition to TRUST metrics, every proposed TRUST approach must quantify the effect of the technique on Length of Design time, Performance (speed), Power, Cycle time, Chip size, Reliability, Circuits types (e.g. FPGA) & Cost.

DARPA/MTO initiated a seedling effort to define metrics for potential TRUST contractors. The type of metrics desired would be analogous to a cost and schedule quote from a commercial reverse engineering firm.

[1]http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf

[2]James R. Gosler, (*The Digital Dimension*, p. 106. in "Transforming US Intelligence", Edited by Jennifer E. Sims/Borton Gerber, Georgetown University Press 2005)