

**DARPA Tech, DARPA's 25th Systems and Technology Symposium
August 7, 2007
Anaheim, California
Teleprompter Script for Dr. Dean Collins, Deputy Director,
Microsystems Technology Office**

TRUST, but Verify

» **DEAN COLLINS:**

Over the years the US has enjoyed military systems superiority in part because our warfighters had access to systems containing the most advanced integrated circuits - ***provided by American manufacturers.***

But a lot of things have changed since the invention of the integrated circuit.

The time has come for us to reexamine and increase our confidence in the **integrity** of the **integrated circuits** on which the military ultimately depends.

Good afternoon.

I am Dean Collins,
Deputy Director of MTO and the program manager for a new MTO initiative called -- **Trusted IC's.**

Our goal is to ensure that integrated circuits used in DoD systems contain exactly what is specified by the systems designer.

“NOTHING MORE AND NOTHING LESS.”

We have initiated this effort in response to the changing landscape of the IC industry and its impact on DoD systems.

First, let's get some perspective.

The modern electronics industry was born with inventions of the transistor in 1947... and the IC in 1959, in the US.

Major US companies such as Fairchild Semiconductor, RCA, Texas Instruments, Motorola and Intel were world leaders in IC manufacturing and dominated the market.

In the early days, the US military was a major player in IC development largely as a result of the circuits used in the Minuteman ICBM program.

This led to the US military being the dominant consumer of integrated circuits in the 1960s and 1970s.

The worldwide market for IC's has expanded dramatically over the past 50 years to an industry valued at over 200 Billion dollars in 2007.

The majority of this market results from manufacturing and sales of commercial products throughout the world.

As a result of this globalization, IC production is rapidly moving off-shore to Taiwan, Singapore, the European Union, Japan, and Peoples Republic of China.

Intel has announced that it will be installing a leading edge IC production facility, and expanding its joint research programs for its multi-core processor usage, in the People's Republic of China.

Cypress Semiconductor and LSI Logic have recently announced that they are going fab-less.

Texas Instruments is now discontinuing its on-shore technology development and is engaged in 32 nanometer and smaller geometry development off-shore.

Freescale, formally Motorola Semiconductor, has their most modern production facility in the EU.

All of this comes on top of the loss of captive IC fabrication facilities to supply custom IC's to critical US systems.

This, then, is the changing IC landscape.

And it is fraught with obvious implications.

A recent Defense Science Board report expressed concerns about the U.S.

military's use of ICs that are produced off-shore.

These concerns range from the possibility of malicious circuits being inserted into the IC's that are made overseas, to reverse ITAR restrictions being imposed on IC exports to the United States.

Malicious circuits -- that is, "something more" than what is defined by the system designer, can be inserted during the design of the IC's, during the fabrication of ICs or during the packaging of ICs.

In the case of Field Programmable Gate Arrays (FPGAs), malicious circuits could be installed through software changes even when the devices are in the field.

The majority of the ICs used in complex modern military systems are made off-shore.

FPGA's are the dominate IC used in modern weapons systems, and all FPGA's are made off shore.

Because the U.S.

military now consumes only about 1% of the total IC production in the world, the military supply requirement is no longer a dominant market factor that can influence IC production.

DARPA'S Program, "TRUST in ICs", seeks technical approaches to addressing the assessment of Trust in ICs from all sources.

The central idea is

"Trust but Verify," a policy which has worked well for this country in the past.

In the Trust in IC's program, we accept that the world is shifting.

This means that the US will continue to be buying a significant fraction of its ICs used in military systems from overseas suppliers.

Therefore we have to see what we can do to live with the situation and still have high performance ICs which we trust.

In the past, classified ICs were produced by using procedures to insure trust.

These procedures included ensuring security clearances for the staff, building a secure facility and doing all the work in house, including the design work.

Of course these procedures still left open the vulnerability to an insider threat.

In the DARPA TRUST in ICs program we will not rely on procedures but only trust things that we can measure.

Another radical departure of the DARPA Program is basing the degree of trust assigned to an IC on metrics.

Neither metrics for trust nor the testing methods to quantify trust have ever been done before.

We need to validate the design software, the external intellectual property used in the design, and the device fabrication.

We also need to validate device authentication techniques and techniques to prevent devices in the field from being modified.

Finally we need to keep the testing methods confidential.

We have a very challenging metrics problem.

We are pursuing a metrics path that is formulated in terms of probability of detection vs. probability of false alarms.

Moreover we are departing from the traditional malicious circuit or Trojan Horse definition of the signal, to a more basic measurement where any change in the IC -- such as an interconnect or a transistor -- is considered the signal.

We have focused on the finite number of physical changes as opposed to the unbounded unmanageable case of considering the Trojan Horses to be the signal.

Our approach provides a defined basis around which we can construct metrics.

We hope to provide standards and technologies that are useful for both offshore procurement of ICs and also for trusted foundry efforts here in the US.

The technical challenges facing the program are formidable.

We need help in quickly analyzing complex ICs to determine their functionality.

Drastic changes in functionality can occur with only a few changes in transistors or interconnects.

Modern transistors are small.

We can fit 1 million transistors on the head of a pin!

And not only are the transistors small, but they are made up of as many as twenty layers, with many of the layers being only several atomic layers thick.

Imagine an IC consisting of 100 million transistors.

Now imagine looking for changes in a 100 of those 100 million transistors!

One part in a million!

It is like looking for
100 extra straws
in a haystack!

We are particularly interested in non-destructive methods to detect changes.

We need sensitive probes to measure such small changes.

Inserting malicious circuits can also be accomplished during the design cycle.

Opportunities for insertion exist at many points during the design flow and methods for maintaining design integrity are sorely needed.

Most of the present commercial design tools are focused on assuring functionality, but few check for unspecified additional features which could be malicious.

This is truly a DARPA-hard problem
and I would like to hear your ideas on how to enhance trust in ICs!

But of course TRUST is only one of the many exciting MTO topics you have heard about today.

John Zolper described the office vision aimed at breaking fundamental

barriers in component performance which are presently limiting the performance of military systems.

The breakthroughs described in RF, Photonics, and Nanomechanics, coupled with novel concepts for extending Moore's Law are truly exciting.

But you have not heard nearly the expanse of all the things that MTO is doing.

Come talk to us about the 70 different projects that MTO is pursuing right now!

For example, there are a multitude of laser programs, to develop everything from high power fiber lasers to lasers emitting in the ultra violet.

We are even working on a laser whose physical dimensions are smaller than the wavelength of the emitted light.

Imaging sensors including 3D and multispectral imagers form another key office thrust.

These sensors span the spectrum from ultraviolet, visible, near infrared, mid-range IR, long wavelength IR... to millimeter waves and X-rays.

Very, very important research ideas.

We would like to talk to you about those... and get your ideas and have you understand what we are doing.

Therefore I would like to invite you to come to our display area and see all the advanced component technology MTO is pursuing.

Finally, if you are excited by what you have heard today from MTO, and you would like to be part of it and really drive where MTO is going, let's talk about it...

because, who knows, maybe you will end up joining us in MTO to become a program manager at DARPA.

Now, let's meet some of the current MTO Program Managers.