NDIA

Trusted Microelectronics

Joint Working Group

Team 4 Summary

New Methods to Instill Trust in Commercial Semiconductor Fabrication

July 2017

DISCLAIMER: The ideas and findings in this report should not be construed to be official positions of any of the organizations listed as contributing members of this Joint Working Group or the membership of NDIA. It is published in the interest of information exchange between Government and Industry, pursuant to the mission of NDIA.

Team 4 - New Methods to Instill Trust in Commercial Semiconductor Fabrication

Team 4 evaluated new technical methods to instill trust in semiconductor fabrication with the goal of determining if these methods can instill sufficient trust in commercial fabrication to meet the requirements of sensitive DoD programs. Unlike prior surveys, Team 4 evaluated which methods which can be readily and pragmatically applied. For this purpose, 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."

This report recommends development of a new review process to enable approval of trusted access to commercial fabrication for selected military end use semiconductors. The Defense Microelectronics Activity (DMEA), under the Office of the Secretary of Defense, is the program manager for the Trusted Foundry Program and, as such, is the clear candidate to implement this report’s recommendations.

DoD semiconductors require trust throughout the development process starting with electronic design automation (EDA) tools and 3rd party intellectual property; however, Team 4 focused on trust in the fabrication phase because traditional means, using DMEA-accredited Trusted Foundries to achieve trust in semiconductor fabrication, are not available at advanced process nodes, potentially precipitating a crisis for DoD. Unmitigated, this crisis could disadvantage DoD with asymmetric semiconductor capabilities and/or undermine DoDI 5200.44 with increasingly frequent waivers of its Trusted Foundry requirements.

Summary of Findings and Recommendations

Although the primary goal of Team 4 has been to open trusted access to commercial semiconductor fabrication, it is important to note that the same methods can be applied to increase the security of semiconductor fabrication within the current Trusted Foundry program, while extending the program’s offerings.

The new methods discussed in the team’s paper have the potential to instill Confidentiality and Integrity in semiconductor fabs which are outside the DMEA Trusted Foundry program. Whether the risks can be sufficiently mitigated to enable commercial fabrication will depend on the specific IC design as well as the developer’s skill in applying the appropriate methods. As Team 4 concluded, one size does not fit all. Nevertheless, under DoDI 5200.44 today, only one option is available: “In applicable systems, integrated circuit-related products… shall be procured from a trusted supplier… ”. To exploit the new methods as reviewed by Team 4 it is recommended that:

- *Three (3) Trust Levels be defined. The Trust Level definitions should be independent of specific implementation and instead derived from a two-dimensional "risk cube", depending on Criticality of Compromise (CoC) and the end use Threat environment;*
- *The USG program responsible for the "specific DoD military end use" should determine the required Trust Level for the ASIC;*
- *A "Technical Implementation Guide (TIG) for Trusted ASICs" be developed and maintained. This document should outline practical requirements for achieving each Trust Level, incorporating the new methods examined by Team 4 as appropriate, as well as providing developer examples;*
- *The contractor for each military end use ASIC be required to submit a Trust Plan for review and approval at PDR.*

--END--