A DARPA Approach to Trusted Microelectronics

Verify the functions
Verification and validation countermeasures provide assurance that components function as specified. These countermeasures, which can include various commercially available techniques, protect against quality and reliability issues, malicious insertions, and fraudulent products.

Application
Verification and validation may be most appropriate for protecting highly reprogrammable electronic devices that, due to their lack of inherent CPI, are less likely to face reverse engineering threats. These countermeasures can implement protections against threats during fabrication and assembly by:

- Detecting intentional compromise of a microelectronics design or manufactured part
- Detecting accidental compromise of a microelectronics design or manufactured part
- Detecting unreliable, unauthorized, or counterfeit products

Verification and validation protections should also help DoD prevent certain malicious insertion threats. By limiting DoD involvement in the ASIC lifecycle, verification and validation countermeasures can help expand the number of potential ASIC suppliers, making it more difficult for malicious actors to identify and attack the supply chain for military microelectronics.

Current approach and emerging gaps
As currently applied, such as in the destructive physical analysis of an individual IC or comparing suspect ICs to authorized versions, verification and validation can prove both costly and time consuming.¹ Alternatively, less intensive methods such as visually inspecting ICs have limited efficacy against sophisticated counterfeits and cannot detect malicious insertion threats. Design-for-trust techniques that increase IC inspection speed and efficacy reduce susceptibility to these threats. DARPA efforts are meant to enhance or complement current protection approaches.

Proposed technology: commercial options
Commercial firms implement a range of security mechanisms intended to identify failures within IC design and manufacture. Many of these are applicable to verifying the function and reliability of DoD microelectronics and to checking the operation of IC manufacturing lines without exposing a vendor’s proprietary data. DoD could request greater access to information commonly requested by commercial customers, including quality reports, wafer acceptance reports, and extended reliability testing data. DoD could also leverage commercial tools—such as instrumented reliability ovens and systems that simulate IC aging—to verify component reliability. Finally, DoD could repurpose commercial inspection tools to check the fidelity of manufactured wafer patterns against design expectations and therefore detect malicious hardware insertions.

Proposed technology: DARPA’s TRUST and IRIS programs
Two DARPA programs aim to significantly reduce the time and cost required to establish that an IC functions as specified. The Trusted Integrated Circuits (TRUST) and Integrity and Reliability of Integrated Circuits (IRIS) programs represent a comprehensive effort to protect the electronics supply chain from counterfeits, clones, and malicious hardware insertions.

DARPA’s completed TRUST program produced reverse engineering tools to verify that ICs matched design specifications via destructive physical analysis. DMEA and the Air Force Research Laboratory (AFRL) have adopted the resulting FPGA and ASIC functional logic verification tools and IP verification tools, respectively.

Reverse engineering techniques developed under IRIS aim to derive an IC’s functionality using non-destructive imaging, even when IC design specifications are unavailable. IRIS performer Raytheon demonstrated the technology on military hardware with 99.4% accuracy. IRIS technologies have also reduced reverse engineering timelines from 3 months to 3 weeks.

To facilitate rapid assessment of quality failures, IRIS developed enhanced device models for simulating circuit performance and account for device aging. This capability will enable the detection of ICs that have been stressed in order to promote premature failure or of counterfeits that have been reintroduced into the supply chain after disposal. IRIS can therefore help detect fraudulent products and reliability issues. IRIS transitioned a scanning-optical-microscope to the Naval Surface Warfare Center (NSWC)-Crane for use in counterfeit detection.