SAND2015-4348C

Exceptional service in the national interest

Sandia National Laboratories

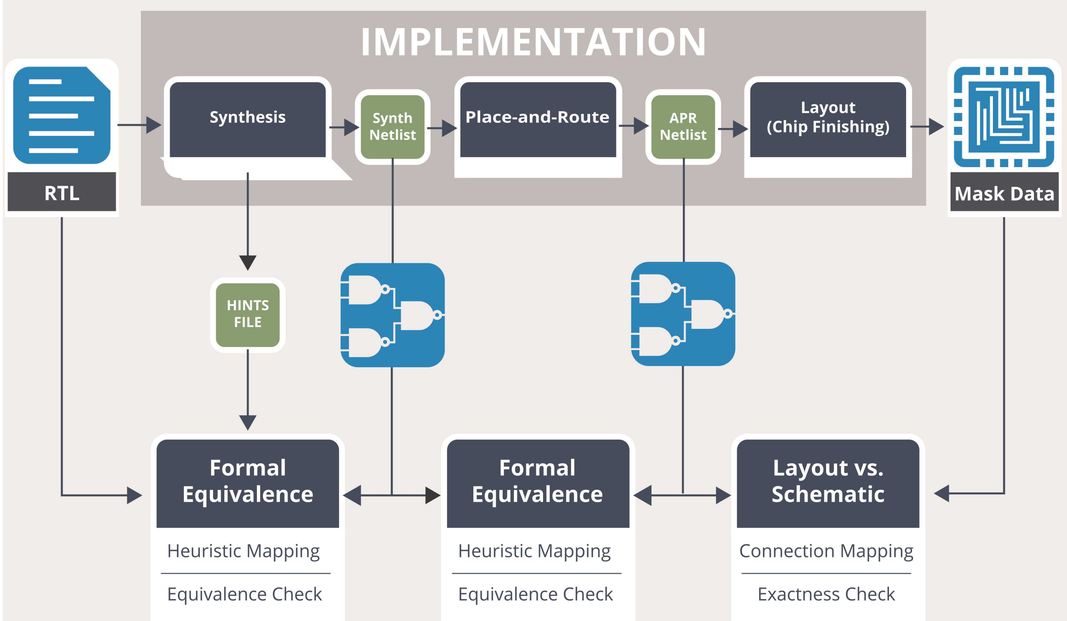
ASSURED TRUST THROUGH RTL-TO-GDS FORMAL EQUIVALENCE

Tom J. Mannos, Jason Michnovicz, Matthew Land, Brandon K. Eames, Joshua R. Templin, Robert C. Armstrong, Jackson Mayo

Ensure no unauthorized changes across the ASIC development flow …for assured trust in defense and safety critical ASICs

TRADITIONAL EQUIVALENCE FLOW

Independently checking each output for assured trust is cumbersome and error-prone.

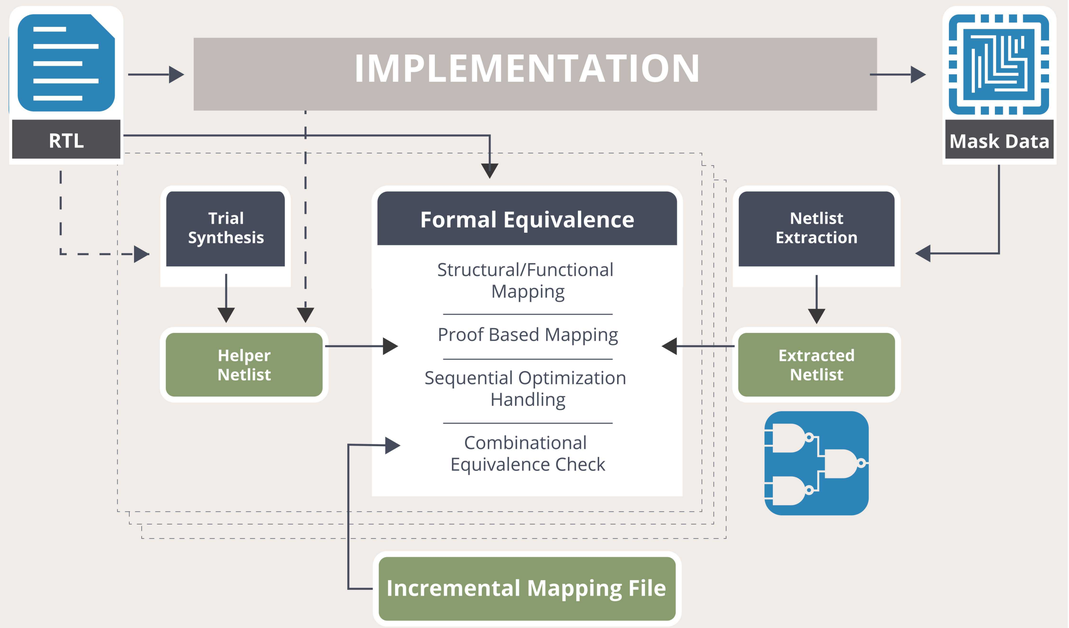


In the traditional equivalence flow, the implementation outputs are verified incrementally.

- Formal Equivalence relies on a "hints" file to identify sequential synthesis optimizations and to map sequential elements to RTL registers.
- Layout Versus Schematic (LVS) verifies the physical GDSII contains the same number of transistors and connections between them as the final APR netlist.

NEW BLACK-BOX EQUIVALENCE FLOW

The mask data (GDS or MEBES) is the only output that needs to be checked for assured trust.

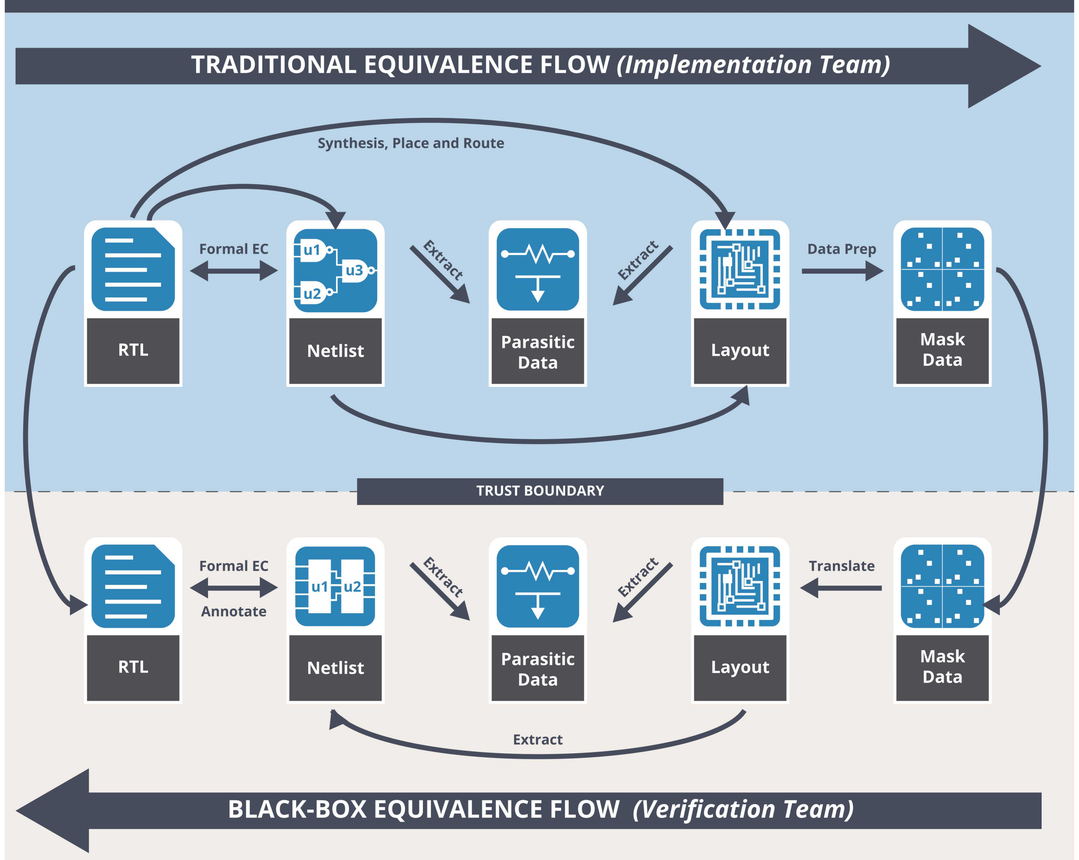


The black-box flow compares RTL directly to a netlist extracted from the mask data (GDS or MEBES).

- During the mapping step, the equivalence checker maps sequential elements of this anonymous netlist to registers in the RTL based on structural and functional similarities.
- During the verification step, The equivalence checker identifies and accounts for a variety of sequential optimizations and fills in mappings not identified during the mapping step.
- An optional "helper netlist" aids the initial mapping process, and the process repeats until mapping and verification are complete.

INTEGRATED FLOW

The integrated flow combines the traditional flow with the black-box flow for increased trust through independence and diversity.



TEST RESULTS

TEST DESIGN	NETLIST SOURCE	FORMAL EC TOOL A	FORMAL EC TOOL B	ONESPIN EC-ASIC
Research Test Chip 3087 registers, custom 32nm library.	Extracted from GDS.	Converged with no additional processing. **Verification succeeded.**	Did not converge. **Failed sanity check.**	Converged with no additional processing. **Verification succeeded.**
Academic Design 547 registers, generic library.	Obfuscated to simulate extraction from GDS.	Converged with help from trial netlist. **Verification failed.**	Did not converge. **Failed sanity check.**	Converged with no additional processing. **Verification succeeded.**
Commercial Processor 2325 registers, commercial 90nm library.	Obfuscated to simulate extraction from GDS.	Did not converge. **Verification failed.**	Did not converge. **Failed sanity check.**	Converged with help from APR netlist. **Verification succeeded.**
Production ASIC 8627 registers + 40k SRAM, 350nm structured ASIC.	Obfuscated to simulate extraction from GDS.	Did not converge. **Verification failed.**	**Not attempted.**	Converged with no helper netlist after 3 iterations. **Verification succeeded.**

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Supported by the Laboratory Directed Research and Development program at Sandia National Laboratories, a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND No. 2011-XXXXP