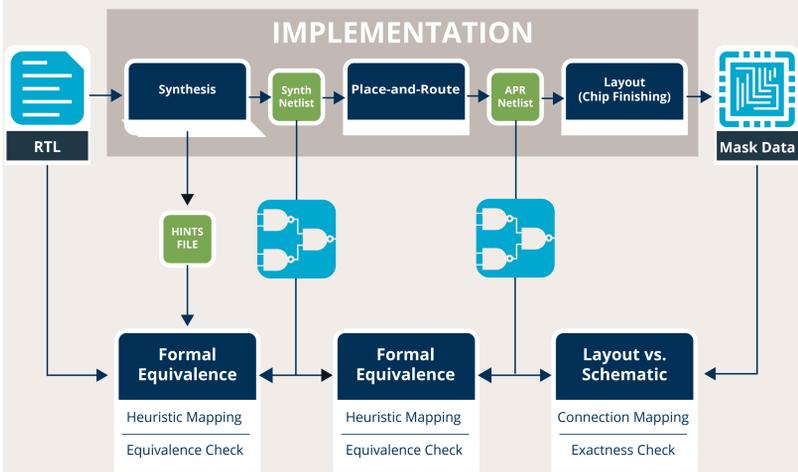


# ASSURED TRUST THROUGH RTL-TO-GDS FORMAL EQUIVALENCE

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

## TRADITIONAL EQUIVALENCE FLOW

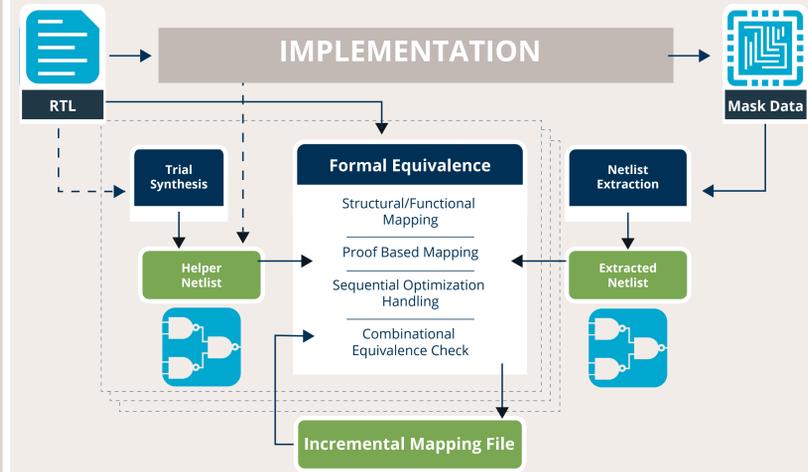


In the traditional equivalence flow, the implementation outputs are verified in stages.

- 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.

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

## NEW BLACK-BOX EQUIVALENCE FLOW

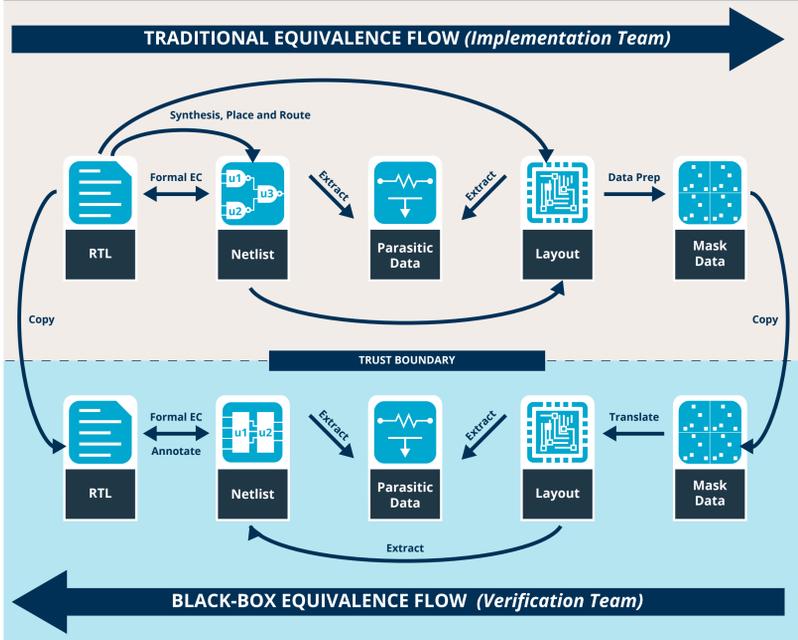


The black-box flow compares RTL directly to a netlist extracted from the mask data (GDS or MEBES).

- 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.

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

## 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	FORMAL EC TOOL C
Research Test Chip 3087 registers, custom 32nm library.	Extracted from GDS.	Converged with no additional processing. <b>Verification succeeded.</b>	Did not converge. <b>Failed sanity check.</b>	Converged with no additional processing. <b>Verification succeeded.</b>
CSAW2009 UART, 547 registers, Isi_10k Library.	Obfuscated to simulate extraction from GDS.	Converged with help from trial netlist. <b>Verification failed.</b>	Did not converge. <b>Failed sanity check.</b>	Converged with no additional processing. <b>Verification succeeded.</b>
Commercial Processor 2325 registers, commercial 90nm library.	Obfuscated to simulate extraction from GDS.	Did not converge. <b>Verification failed.</b>	Did not converge. <b>Failed sanity check.</b>	Converged with help from APR netlist. <b>Verification succeeded.</b>
Production ASIC 8627 registers + 40k SRAM, 350nm structured ASIC.	Obfuscated to simulate extraction from GDS.	Did not converge. <b>Verification failed.</b>	<b>Not attempted.</b>	Converged with no helper netlist after 3 iterations. <b>Verification succeeded.</b>

*Based on preliminary results, we believe this approach to be scalable to larger, more complex designs.*

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

