SYNOPSYS®
Silicon to Software™

Closing Thoughts on the CAD4Security Workshop

DAC 59

San Francisco

Mike Borza, Synopsys Scientist

July 10, 2022

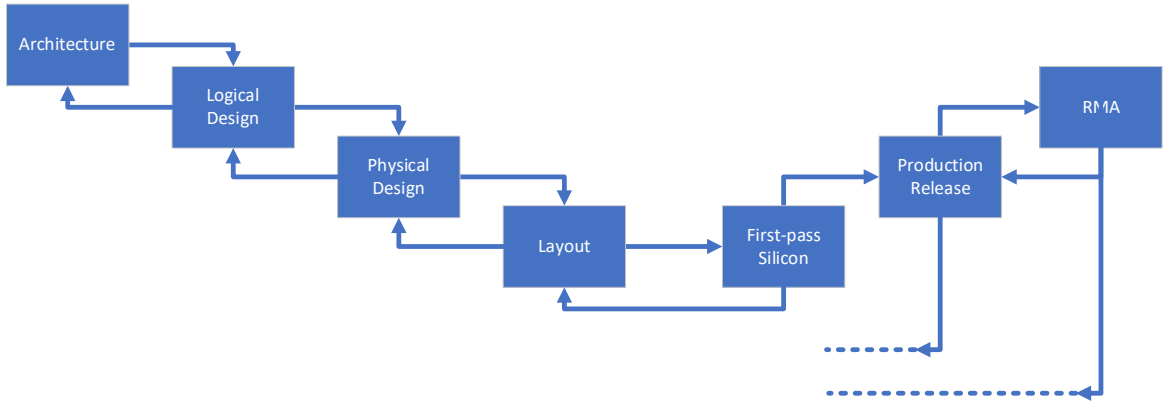
What Progress Have We Made Recently?

From my “CAD for Security” talk at ITC 2019

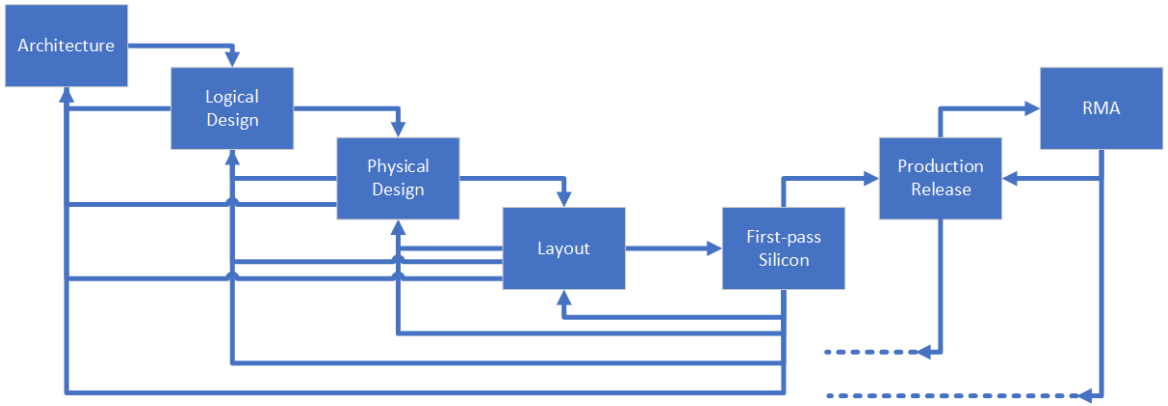
- IC manufacturers were resistant, but starting to understand there are problems
  - Primary focus still to optimize within the PPA envelope – security comes after, if at all
  - Areas of concern
    - Ideal chips: minimum cost (area), maximum functional performance in a minimal power footprint
    - Maximize market opportunity by minimizing time-to-market
  - A “head in the sand” do-nothing approach was viable for many
- Implications of that for security solutions
  - Minimize impact and disruption to existing design & manufacturing flows and practices to ease adoption
  - Raise the recognition of security as a first-class design concern with PPA
  - Admit that this does not come for free and justify that the cost is worthwhile
  - Automate to reduce reliance on scarce expertise and increase probability of success
- Have we moved the needle?
  - We’re starting to – in the third inning of a nine-inning game

How Would We Do This in an Organized Way?

- Traditional waterfall model is not sufficient to incorporate security flow
  - Particularly when side channels are important

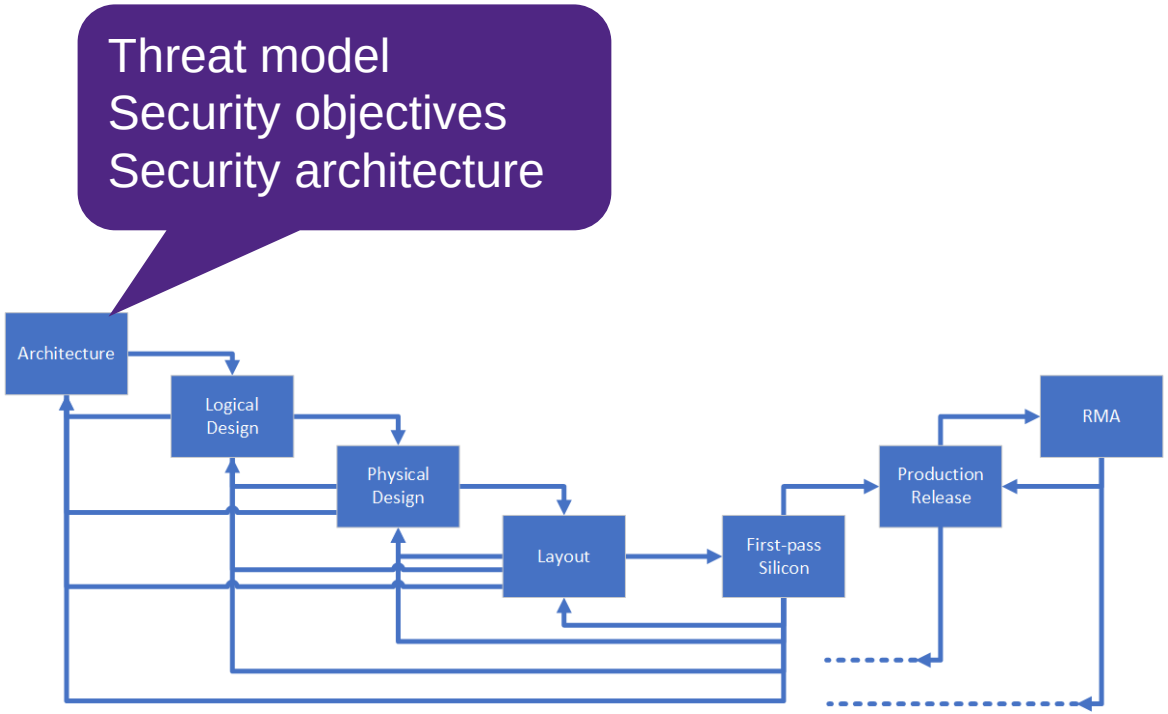


How Would We Do This in an Organized Way?



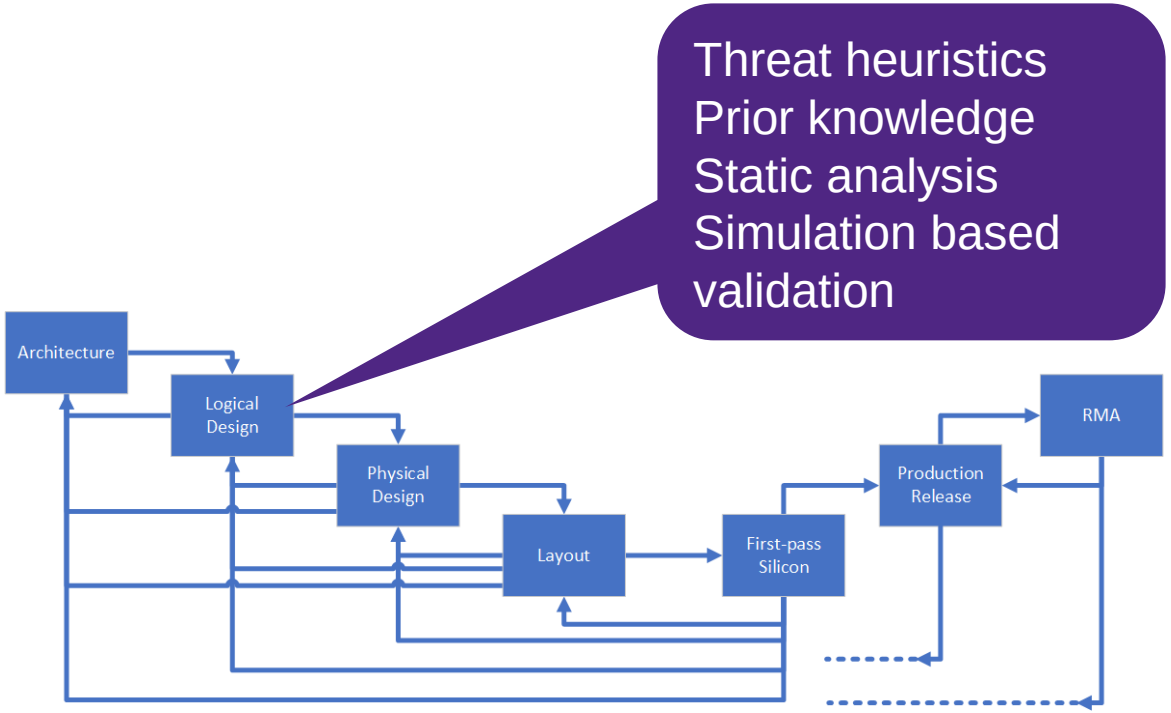
- Traditional waterfall model is not sufficient to incorporate security flow
  - Particularly when side channels are important
- Feedback from phase at which vulnerabilities are detected to the phase best suited to resolve the problem is ideal
  - Identify weaknesses as early as possible ad mitigate locally
  - Recognize that this is not always feasible

How Would We Do This in an Organized Way?



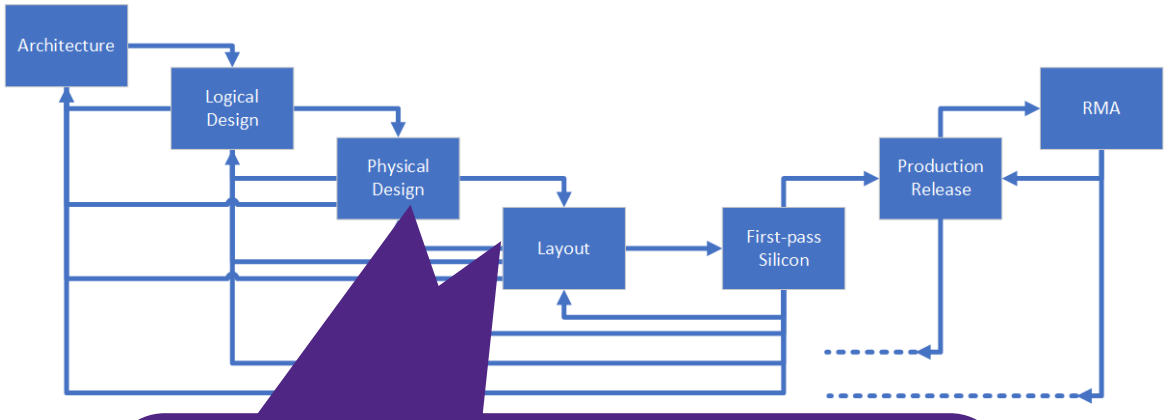
- Traditional waterfall model is not sufficient to incorporate security flow
  - Particularly when side channels are important
- Feedback from phase at which vulnerabilities are detected to the phase best suited to resolve the problem is ideal
  - Identify weaknesses as early as possible ad mitigate locally
  - Recognize that this is not always feasible
- Ideally, spell out at every phase the security concerns, gaps, mitigations
  - Develop plans to close unmitigated gaps
  - While heuristics are necessary, they're less satisfying than rigorous proofs

How Would We Do This in an Organized Way?



- Traditional waterfall model is not sufficient to incorporate security flow
  - Particularly when side channels are important
- Feedback from phase at which vulnerabilities are detected to the phase best suited to resolve the problem is ideal
  - Identify weaknesses as early as possible ad mitigate locally
  - Recognize that this is not always feasible
- Ideally, spell out at every phase the security concerns, gaps, mitigations
  - Develop plans to close unmitigated gaps
  - While heuristics are necessary, they're less satisfying than rigorous proofs

How Would We Do This in an Organized Way?

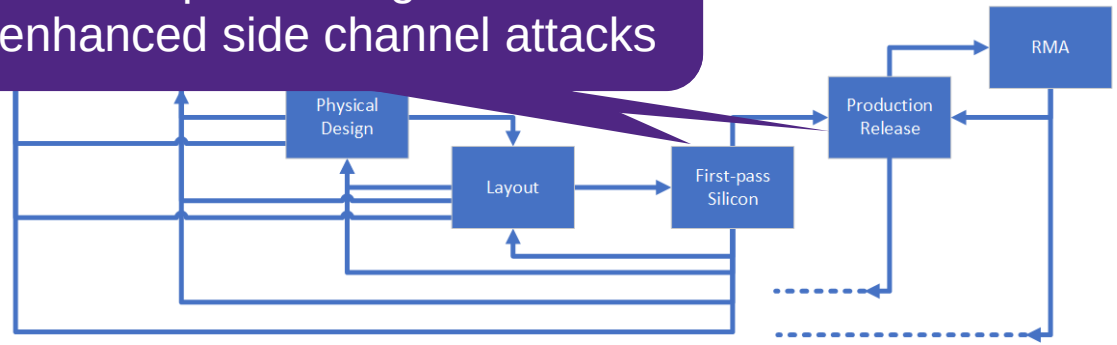


Physics simulation to validate prior mitigations – power, timing, RF emissions, thermal, etc.
Emulation to provide high performance simulation & fault modeling

- Traditional waterfall model is not sufficient to incorporate security flow
  - Particularly when side channels are important
- Feedback from phase at which vulnerabilities are detected to the phase best suited to resolve the problem is ideal
  - Identify weaknesses as early as possible ad mitigate locally
  - Recognize that this is not always feasible
- Ideally, spell out at every phase the security concerns, gaps, mitigations
  - Develop plans to close unmitigated gaps
  - While heuristics are necessary, they're less satisfying than rigorous proofs

How Would We Do This in an Organized Way?

Red teaming
Automated pen testing
AI-enhanced side channel attacks



- Traditional waterfall model is not sufficient to incorporate security flow
  - Particularly when side channels are important
- Feedback from phase at which vulnerabilities are detected to the phase best suited to resolve the problem is ideal
  - Identify weaknesses as early as possible ad mitigate locally
  - Recognize that this is not always feasible
- Ideally, spell out at every phase the security concerns, gaps, mitigations
  - Develop plans to close unmitigated gaps
  - While heuristics are necessary, they're less satisfying than rigorous proofs

How Are We Doing This in Practice?

- Ad hoc point-solutions based on specific research are the low-hanging fruit
  - "Easy" extensions to existing design and verification tools and methodologies, e.g.
    - Security checkers looking for violations of threat heuristics – lint-like tools in the synthesis flow
    - Coverage tools can recognize potential threats such as trojans or other undisclosed functionality
    - Address specific threats in the logic – incompletely specified state machines flagged
    - Analysis of back-annotated results of downstream design elaboration
- Automated fulfillment of design paradigms
  - Insertion and connectivity for security functions in the scan chain, e.g.
    - Logic locks, obfuscation keys, watermark authentication
    - Back channels for bus firewalls, system activity monitors, SLM
    - Access controls on critical resources – secure memories, critical registers, debugging and scanchain access
- Side-files and proprietary extension languages to specify security attributes
  - Annotations to flag asset modification and propagation
  - SA-EDI (Security Annotation for Electronic Design Interchange) is an emerging standard

Signs of Hope

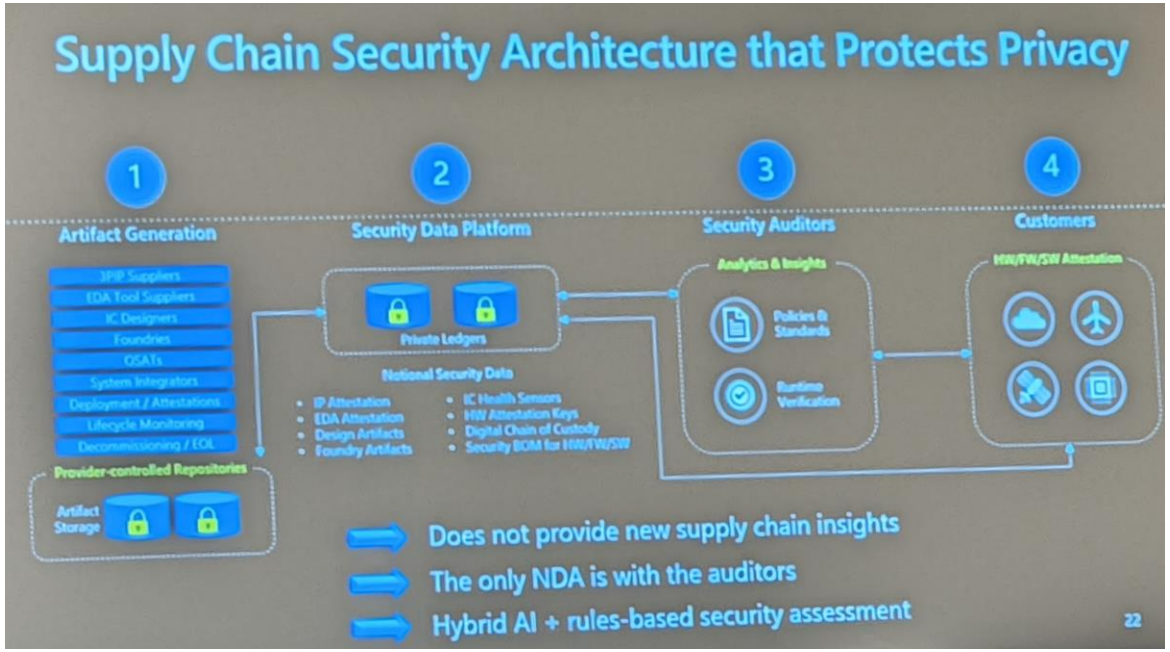
- Right now, as an industry we're responding in a fairly scattershot way
  - Agreement on the issues for concern in cross-vendor forums (mostly)
  - Diverse solution space with a large number of suppliers
    - That's OK – this is still a rapidly evolving space
  - Still parts of the problem space that aren't being addressed
    - Corollary: some darling problems attract an overabundance of solutions
- Industry interest groups are starting to recognize the need to bring order and common understanding
  - Industry segments leading the way: A&D, automotive, industrial IOT, cloud datacenter
  - DARPA, US funded labs, EU are providing guidance and direction, seeding action
  - NDIA, Mitre CWE and work around it, SAE G32, GSA TIES
  - Chips Act(s) have brought the strategic nature of microelectronics supply chains to the fore
- The importance of securing the chip as a means to secure the downstream applications of it is starting to be a common understanding

Where Do the Future Opportunities Lie? #1

- Authenticating the development flow from idea through production
- To succeed, measuring and attesting authenticity needs to respect a multi-vendor workflow defined by the users of the flow (the IC suppliers)
  - Trying to enforce a single workflow has been tried before, and will also certainly fail again
- This is the IC suppliers' portion of a supply chain assurance strategy
  - What assets are going into my chip? Who is putting them there? How and why are they transformed on the way to final silicon?
  - Are the chips that were built the chips that were designed? And only what was designed?

Where Do the Future Opportunities Lie? #2

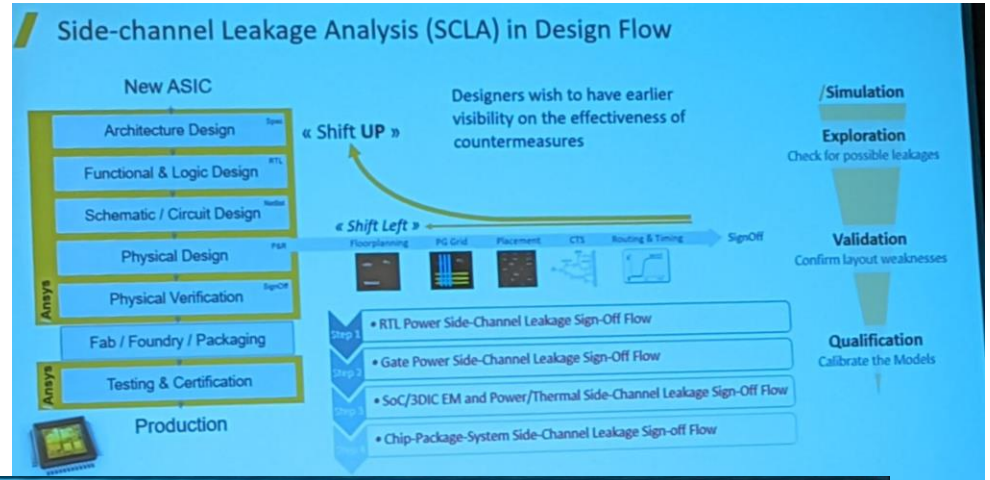
- Supply chain security via MQA
  - Huge opportunity for security applications developed on Silicon Lifecycle Management
  - Data-driven, distributed, access controlled
  - Cloud collection and analysis of data in real-time
  - Challenges
    - Massive datasets need great analytics and visualization
    - Commercial and security sensitivities around data collected and analysed – multi-vendor, different domains of interest

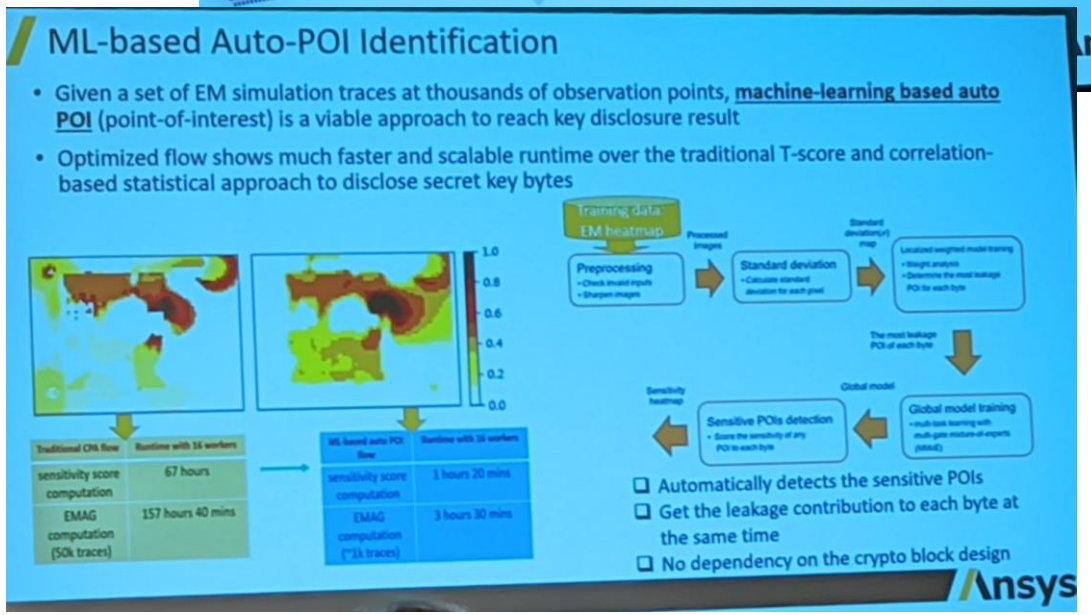


Jay Lewis: Microsoft

Where Do the Future Opportunities Lie? #3

- AI/ML in the small, and in the large
- AI in the small applies to tools focused on a single problem, e.g. power SCA
  - Current solutions focus on the analysis problem
  - Next generation solutions should extend that to point to features of interest (leakage sources)
  - The next logical leap is to help design the mitigations (Jay's Monster Bowl of Soup Knitted out of Wool)
- AI/ML in the large applies to sifting volumes of measurement data to look for evolving attacks and their sources
  - Often inferring attack behaviour from indirect measurements such as local power or thermal data





Norman Chang: Ansys

SYNOPSYS®
Silicon to Software™

Thank You


SYNOPSYS®
Silicon to Software™