SAWBLADE TECHNOLOGY DETAIL

A quick and casual review of Sawblade's approach might tempt the average engineer to wonder why one might need Sawblade's products. The "we do that all the time" psychology might lead some to think they might be able to replicate Sawblade capabilities given enough time, effort and funding.

Apart from the significant investment needed to create the products, the inevitable struggle to "work out the bugs" on the home brewed approach and the resulting risk foisted upon the firm who decides the "not invented here" attitude justifies launching off on a fool-hardy scheme to "roll your own" tools and components, there is an even more compelling reason to not attempt a do-it-yourself job.

One fundamental reason to use Sawblade's unique tools and intellectual properties has to do with design formalism. Task formality is the basis for the choice of tools real craftsmen make when considering a professional job. Tool segregation dictates no professional worker would use a wrench to bang a nail into fine furniture or use a hammer to tighten a bolt on an expensive engine. Such compliance with formal methods means no engineering manager would allow refining and proofing work to be done with the risk of polluting a long fought for project with the same tools used to create the project.

In the validation and qualification disciplines, tool choice is a predicate for proper chain of workflow. In the case of semiconductor circuit design, EDA tools used to build and synthesize the result of an engineering specification have done their job when the specified requirements for the pre-fabricated chip have been completed. To pick up the same set of tools and proceed to build whatever desired security, defense or protection architected for the Host circuit, pollutes the entire legacy of the design. It places in question where the Host circuit left off and where the Defense circuitry begins.

Sawblade tools and intellectual property components were developed specifically for sophisticated monitoring and manipulating of Host circuitry by Dr. Miron Abramovici, a preeminent authority on the science of test circuitry. No engineering manager would think to let the circuit design team also create the formal testing circuitry as the conflict of interest, the risk of task blindness to error and the violation of the predicate rules of compliance in validation and qualification would result in glaringly obvious error. At the same time, the design team should have access to tools capable of informing them as to ad hoc issues the specified circuit might have before a formal delivery for pre-production validation. Given Sawblade technology use throughout the life of the chip, these formal predicates follow into post-production and at-speed operations; an even greater reason for formal tool segregation.

The specifically invented and patented methods used to most effectively create segregated domains of monitor/manipulate behavior targeting parts of the Host are at the center of reliable overwatch and hyper-supervision of legacy or new Host circuits. This ensures the Host is not remodeled while installing granular monitor/manipulate engines to signal sets. These automated methods are baked into the existing tools and components represented by the Sawblade ClearBlue products and are available to automation systems as Tcl (Tool Command Language) statements as well as the more human-manageable GUI suites.

The ability to verify/validate circuit operation at-speed throughout the chip's operating life means the operating domain can be secured. The ability to modify/manipulate circuit operation on-the-fly throughout the chip's overwatch life means the operating domain can be defended.

Perhaps the following narrative may flesh out any nagging doubts a defense team assigned to create a circuit facility that overwatches, reports on and interdicts improper Host circuit operations might have in thinking this kind of job can be handled by existing EDA design tools.

Integrated Hardware

ClearBlue EDA formally installs transparent (**Hidden Embed**) granular monitors and manipulators as an operating fabric into legacy and new designs.

Granular circuits speak to each other through on-chip networks (**Networked Fabric**) carrying commands and data throughout the chip and to the outside world.

These methods create a hardware-based means of monitoring and manipulating resources within the Host (**Host Circuit Overwatch**). This means of servicing Host signals allow designers to build in-chip security and defense operations untouched by outside methods.

Distributed Engines

ClearBlue ReDI (Reconfigurable Digital Instrumentation) reconfigurable engines are designed to retrace wiring within the Host chip and between the Sawblade fabric components (**Reconfigurable Logic**) on-the-fly.

Engines and configurable memory resources monitor and capture designer selected net signals (**Capture and Stimulate**) which may be trapped by assertion based events.

These captured results inform triggering engines which drive gated operations (**Assertion Based Response**). Assertions are configured from outside the chip during real-time circuit operations allowing for adaptation and evolution based on learned patterns.

Seamless Integration

ClearBlue creates a merged netlist consisting of the Host HDL and Sawblade components (**Next Generation Top**) generated and inserted by ClearBlue automation.

Granular component placement allows design freedom (**Flexible Granular EDA**) to choose any signal traces and functions to be instrumented in the Host.

The resulting defended design consists of HDL injected into any legacy or new Host netlist **(Flow to Legacy or New**). This means the smallest or largest designs may be outfitted with unmatched information security and defense augmentation.

Anti-Counterfeit

ClearBlue EDA creates spare trace capacity to allow ReDI engines to reconfigure net connections with within the Host and between Sawblade components (**Retrace Host Circuitry**).

Reconfigurable traces reroute signal flow (**Reconfigure Signal Flow**) within the Host and among the Sawblade components at any time without impacting Host functionality unless desired.

This method creates a hardware-based means to change signal wiring within an operating hardware circuit (**Repair/Repurpose Traces**). Host and instrument functions may then be repaired and/or repurposed at any time throughout the life of the chip.

Anti-Tamper

ClearBlue manipulators may be designed to inject obfuscating signals (**Calculated Noise**) into the Host circuit's electrical signature to mitigate against power analysis and glitching hacks.

Formal EDA and Tcl based operations create beneficial parasites salted into the Host body (**Parasitic Automation**) for automation of security, defense and safety operations.

These facilities provide for 24/7 on-the-fly reconfiguring capabilities (**On-the-fly Personality**) within the Host. Such resources allow the chip to apply reconfiguration of the Host capabilities at any time during operation. Reconfiguration can be used to mitigate new threats.

24/7 Counter-Measures

Sawblade ClearBlue installed monitors in conjunction with transaction and performance engines allow continuous watch processes able to stream internal circuit operations via the on-chip networks (**Watch and Report**).

Sawblade's Capture/Stimulate/Report/Reconfigure formal methods may use such watch/report designs to pro-actively apply an overwatch function able to interdict assertion-based events (**Monitor and Obfuscate**).

These EDA generated and controlled methods and network capabilities may work during attack modes and probing to detect wanted/unwanted behavior, defend against discovered threat and apply counter-measures to resolve the threat (**Detect – Defend – Destroy**). Resolution may include destruction of the circuit or chip for highly sensitive resources.

Contact: Keith Guidry – CTO – Sawblade Ventures, LLC at keith@sawbladeventures.com

Sawblade Ventures, LLC
6001 W. William Cannon Dr. ste. 203A
Austin, Texas 78749