



DAFCA Peter L Levin

ON-CHIP INSTRUMENTS track malicious RTL

DAFCA's founders take a new approach and discover the company's technology can fill an unexpected market need.

DAFCA
TECHNOLOGY
IS NOT
JUST ABOUT
MAKING SURE
NOTHING BAD
HAPPENS;
IT'S ALSO ABOUT
ENSURING
THAT THE
RIGHT THING
HAPPENS.

INNOVATION often depends on looking for new applications for current products and technologies. Peter L Levin, founder, president, and chief executive officer of DAFCA, used that approach in focusing the company's silicon-validation technology on the task of sniffing out semiconductors contaminated by malicious RTL (register-transfer-level) logic. DAFCA's founders didn't originally envision RTL-logic criminology as part of the company's mission. "DAFCA's mission is to deliver a framework for on-chip, at-speed, in-system validation with a combination of on-chip dynamically programmable instruments and off-chip software-analysis tools," he says. "We were blissfully unaware ... of malicious RTL [logic]." But the interactions with colleagues in industry, academia, government, and the venture-capital community that led to the founding of DAFCA also led to Levin's realization that DAFCA technology could help uncover malicious RTL logic.

A 2005 US Department of Defense report outlines the potential problems malicious code can cause (**Reference 1**). The path that led Levin to awareness of the malicious-RTL-logic problem began at Carnegie Mellon University. There, although he concentrated on applied math, he became interested in EDA and semiconductor design and became close to Rob A. Rutenbar, a Carnegie Mellon professor. Levin and Rutenbar would again cross paths when Rutenbar co-founded Neoliner.

After graduation, Levin served as a professor in the electrical- and computer-engineering department of Worcester Polytechnic Institute (Worcester, MA) and then became research dean in Boston University's College of Engineering. Levin was a White House Fellow and presidential appointee during the Clinton Administration. He also received a Humboldt Research Fellowship, which allowed him to study at the University of Darmstadt (Germany). That affiliation and his fluency in German led Levin to approach Munich-based venture-capital-firm TVM, where he again encountered Rutenbar and, working with TVM general partner Hans G Schreck, helped launch Carnegie Mellon spin-off Neoliner. Cadence Design Systems subsequently acquired Neoliner.

Levin was interested in starting his own company, and toward that end, on a visit to Carnegie Mellon after finishing his White House Fellowship, he got in touch with Miron Abramovici, co-author of a leading text and reference in digital-systems testing and testable design (**Reference 2**). Abramovici brought 22 years of

experience at AT&T Bell Labs, Lucent Technologies, and Agere Systems and now serves as chief technology officer of DAFCA. Abramovici worked with Levin in 2003 to raise \$8 million in first-round venture financing of DAFCA. Today, the venture investors include ABS Ventures, 3i US, Bay Partners, New Venture Partners, Vista Ventures, and Individuals Venture Fund.

The start-up garnered some media attention, which brought Abramovici's name to the atten-

tion of a DARPA (Defense Advanced Research Projects Agency) program manager with whom Abramovici had previously worked. That connection led to DAFCA's making several presentations to other government agencies and to companies that were working on government projects.

"We were beginning to gain traction on the commercial side," Levin says, in which DAFCA technology was detecting accidental problems people had inserted into designs. The DARPA introduction opened the door to an "enormous unexpected market need for the detection and potential remediation of malicious RTL [logic] that was deliberately inserted."

Levin provides a brief outline of how DAFCA can detect erroneous code: "To detect that somebody has inserted a Trojan [horse], that Trojan has to activate and do something that the chip wasn't designed to do or force the chip to behave in a way that lies outside the domain of authorized authentic behaviors," he says. "We insert very small, compact, reconfigurable instruments that you can think of as reconfigurable monitors in the RTL [logic], and your enemy may or may not even know that we are there. ... I don't know and I don't care whether this was an accidental mistake or a deliberate intrusion; you are going to use DAFCA to examine the behavior of your device on-chip, at-speed, in-system. From our perspective, it's the same problem."

Levin is careful to distinguish DAFCA from traditional DFT (design-for-test) and BIST (built-in-self-test)

DAFCA page 32 >

