Achronix® Data Acceleration

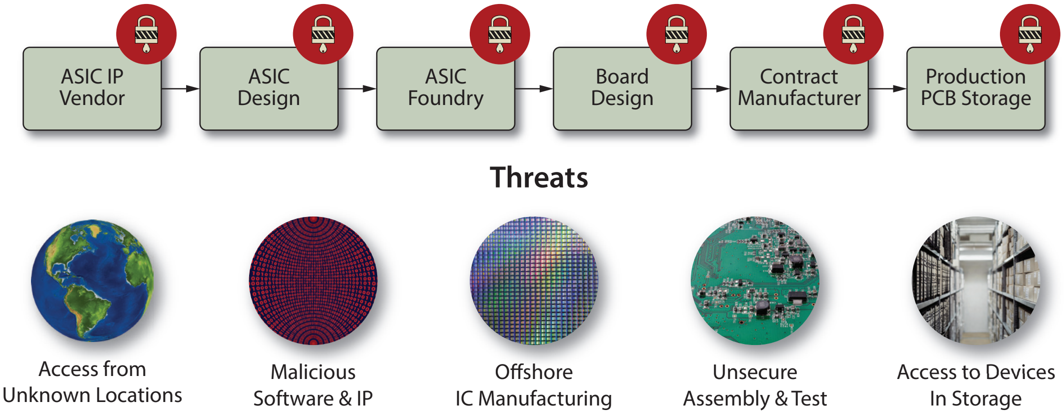
Product Brief

Maximize Hardware Assurance Using Embedded FPGAs

Risks Associated with Hardware Assurance in Custom ASICs

Implementing a secure IP solution when developing a custom ASIC involves overcoming many risks along the development, manufacturing and supply chain flow. Anyone with physical access to an ASIC over its entire lifetime, which can span 10+ years, presents a potential threat to maintaining hardware assurance and keeping critical IP secure. Hardware assurance continues to become more critical for military and defense applications as worldwide threats increase. Examples of hardware assurance risks include:

- Fraudulent Products – Counterfeit and non-genuine devices, possibly even obtained from legally authorized sources, which could include production overruns, relabeled, recycled, cloned, defective, and out-of-spec devices.
- Malicious Insertion – The intentional insertion of malicious code or defects to degrade performance or cause mission failure. Malicious insertions could include logic bombs, Trojan "kill switches" and back doors for unauthorized access to control logic functions and/or alter data.
- Tampering – Unauthorized extraction of sensitive intellectual property using reverse engineering, side-channel scanning, run-time security analysis, and embedded-system security weaknesses.
- Quality Escape – The introduction of product defects, deficiencies, vulnerabilities, or product inadequacies either by mistake or through negligence during the design, production, or post-production handling of a device or system that degrades the product's performance at any time over its entire life cycle.
- Emerging threats – New threats, such as counterfeit component trends, security attacks, and trust issues that combine two or more existing threats into a new vulnerability exploit.



Supply Chain Security for ASIC Only Design

Benefits of eFPGA IP for Hardware Assurance

An embedded FPGA (eFPGA) is IP that designers can embed within an ASIC device. Speedcore™ eFPGA IP from Achronix can be customized to meet an application's specific logic, memory and DSP requirements. Speedcore eFPGA IP is available on TSMC 7nm, 16FF+ and 12 FFC process technology nodes and can be ported to support other process technology nodes.

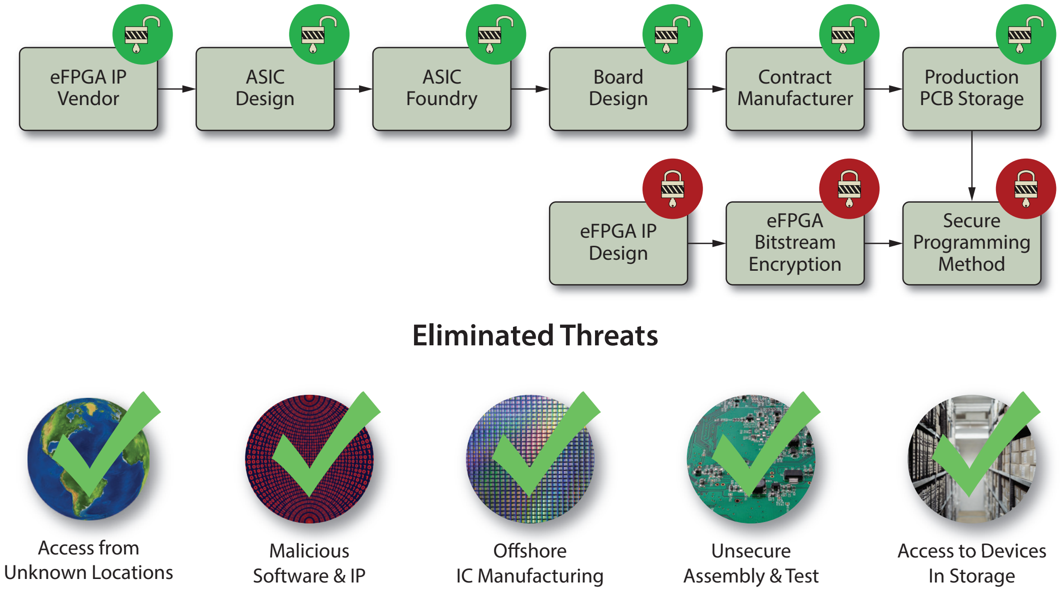
Augmenting an ASIC with eFPGA IP aids hardware assurance efforts by minimizing the number of supply-chain and life-cycle risks inherent to ASICs. Speedcore eFPGA IP deliver benefits such as:

- Ability to deploy in-field upgrades to address future design threats
- Tight integration between ASIC and eFPGA IP to optimize secure and non-secure IP placement
- Reduced cost, power and board space compared to a discrete FPGA solution

Secure Supply Chain Model Using FPGAs

When developing and manufacturing an ASIC, critical IP is exposed across many touch points in the supply chain. These touch points include design implementation, physical design, silicon foundries, test, packaging, PCB assembly, system integration and long-term storage, complicating hardware assurance across the entire supply chain.

However, an ASIC that includes eFPGA IP where critical IP is stored, allows manufacturers to bypass a significant portion of the ASIC supply chain and only need to control the programming file that will be downloaded into the eFPGA portion of the ASIC design, enhancing and simplifying supply chain security. By using an eFPGA IP solution to store mission critical IP, supply chain security is greatly simplified compared to the traditional ASIC design flow where there are many more stages where hardware assurance and trust is required.



Supply Chain Security for eFPGA and ASIC Design

Authentication and Encryption of eFPGA Configuration

Embedded FPGAs offer the ability for critical IP to change over time as required to address:

- New security threats such as side-channel attacks unforeseen during the initial design
- Changes in design operation after hardware is deployed into the field
- New features required during extended 10+ year product lifecycle

When the requirement arises that the initial design needs to be modified, Achronix's eFPGA IP includes industry leading bitstream security hardware, including:

- RSA public/private key authentication before the block starts to decrypt a configuration
- 256-bit AES-GCM encryption to provide strong encryption and authentication of the configuration
- Rotating keys and differential power analysis (DPA) countermeasures used to protect against side-channel attacks
- Secure key stores leveraging physically unclonable functions against cloning and overbuilding

Achronix Semiconductor – Headquarters
2903 Bunker Hill Lane
San Jose, CA 95054
Tel: 408-889-4100
Email: info@achronix.com
www.achronix.com