Achronix®

Maximize Hardware Assurance Using Embedded FPGAs

www.Achronix.com

Abstract

- ASIC plus eFPGA aids hardware assurance by minimizing supply chain threats
- Custom ASICs expose critical IP across the supply chain
- Critical IP does not exist until the eFPGA is securely configured inside the host ASIC
- Achronix eFPGAS are tamperproof and uprgradable at anytime to mitigate future threats

Risks in Custom ASICs

- Fraudulent Products
- Malicious Insertion
- Tampering
- Quality Escape
- Reliability Failure
- Emerging Threats

Benefits of eFPGA IP for Hardware Assurance

An eFPGA is FPGA IP that chip designers embed within an ASIC device to meet logic, memory and DSP requirements. Augmenting an ASIC with eFPGA IP minimizes the number of supply-chain and life-cycle risks inherent to ASICs such as:

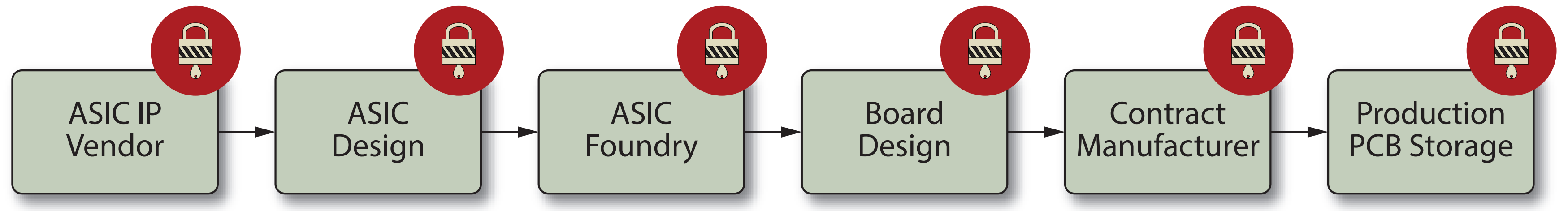
- Ability to deploy in-field upgrades to address future design threats
- Tight integration between ASIC and eFPGA IP to optimize secure and non-secure IP placement
- Reduced cost, power and board space compared to a discrete FPGA solution
- Power to thwart reverse engineering

Achronix Speedcore™ eFPGA IP Includes Leading Bitstream Security Hardware

- 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 DPA countermeasures used to protect against side-channel attacks
- Secure key storage, with physically unclonable functions against cloning and overbuilding

Supply Chain Security for ASIC Only

When developing and manufacturing an ASIC, critical IP is exposed across many touch points in the supply chain.

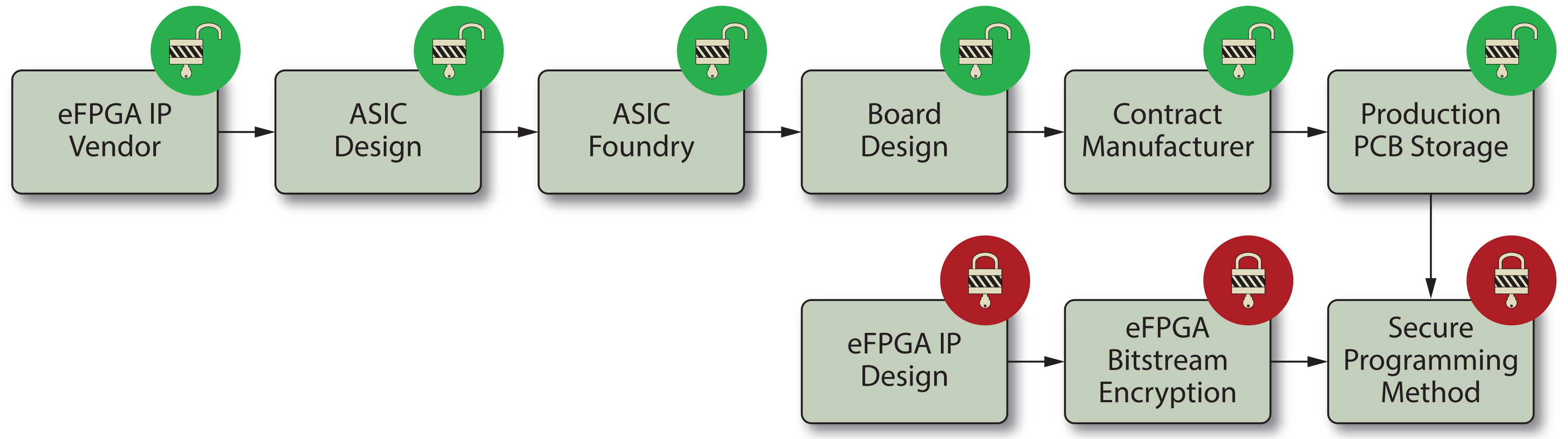


Threats

Access from Unknown Locations
Malicious Software & IP
Offshore IC Manufacturing
Unsecure Assembly & Test
Access to Devices In Storage

Supply Chain Security for eFPGA + ASIC

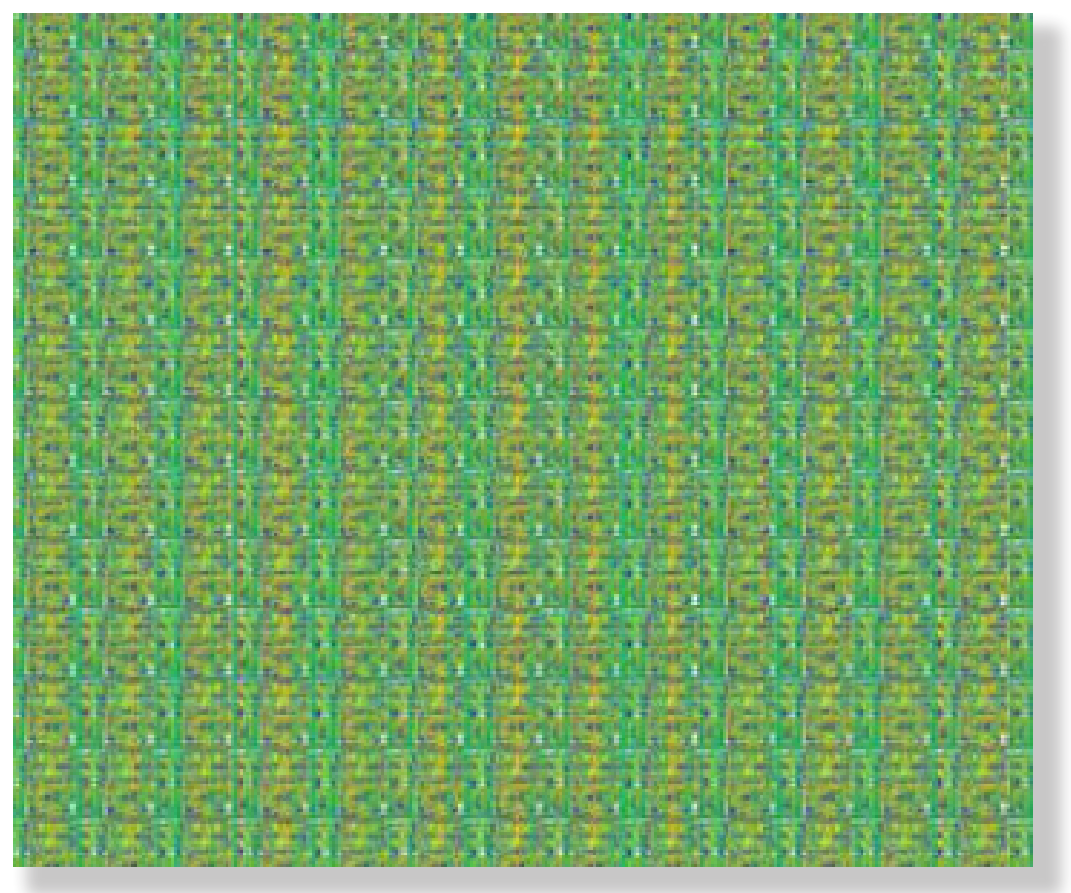
An ASIC that includes eFPGA IP allows manufacturers to eliminate threats in the supply chain, making it much more secure and easier to control.



Eliminated Threats

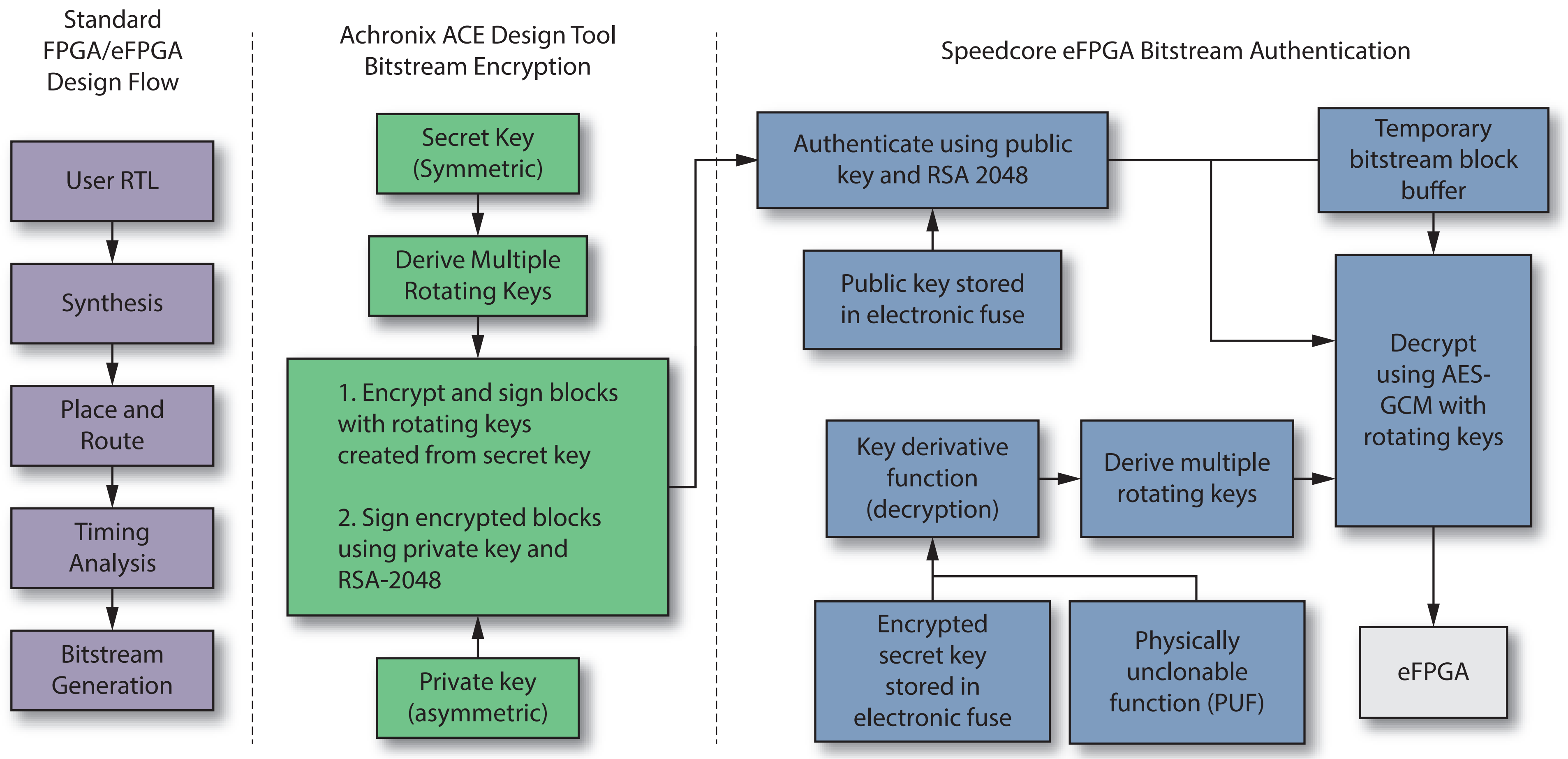
Access from Unknown Locations
Malicious Software & IP
Offshore IC Manufacturing
Unsecure Assembly & Test
Access to Devices In Storage

Tamperproof Architecture



The embedding of the critical design into the field-reprogrammable hardware fabric cannot be known to any adversary to whom the fabric is exposed, which makes unnoticed tampering impossible.

Authentication and Encryption of eFPGA Configuration



Standard FPGA/eFPGA Design Flow
User RTL
Synthesis
Place and Route
Timing Analysis
Bitstream Generation
Achronix ACE Design Tool Bitstream Encryption
Secret Key (Symmetric)
Derive Multiple Rotating Keys
1. Encrypt and sign blocks with rotating keys created from secret key
2. Sign encrypted blocks using private key and RSA-2048
Private key (asymmetric)
Speedcore eFPGA Bitstream Authentication
Authenticate using public key and RSA 2048
Public key stored in electronic fuse
Temporary bitstream block buffer
Decrypt using AES-GCM with rotating keys
Key derivative function (decryption)
Derive multiple rotating keys
Encrypted secret key stored in electronic fuse
Physically unclonable function (PUF)
eFPGA

eFPGAs Offer the Ability for Critical IP to Change Over Time

- 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