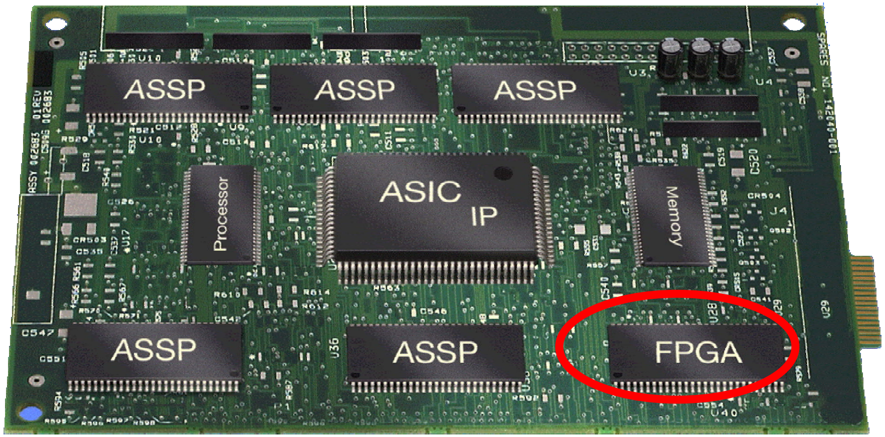
# Actel FPGAs Security Features

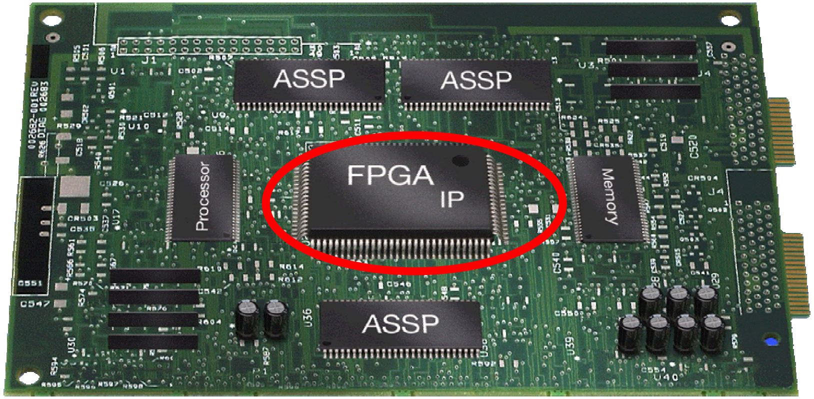
Actel

# The Rising Need for Security

System Design circa 1995

System Design circa 2004





FPGA = Glue Logic

FPGA = ASIC Replacement

Today, the FPGA is the heart of the system

# Security Exposure

- **Cloning**
  - A competitor makes a copy of the boot prom or intercepts the bitstream from the on-board processor and copies the code.
- **Reverse Engineering**
  - A competitor copies a design by reconstructing a "schematic" or netlist level representation; in the process, he understands how the design works and how to improve it.
- **Over-building**
  - An unscrupulous contract manufacturer buys standard parts on the open market and over builds, selling the extra production for profit with none of the support and design overhead costs.

# Security Attacks Review

## Two Principal Types:

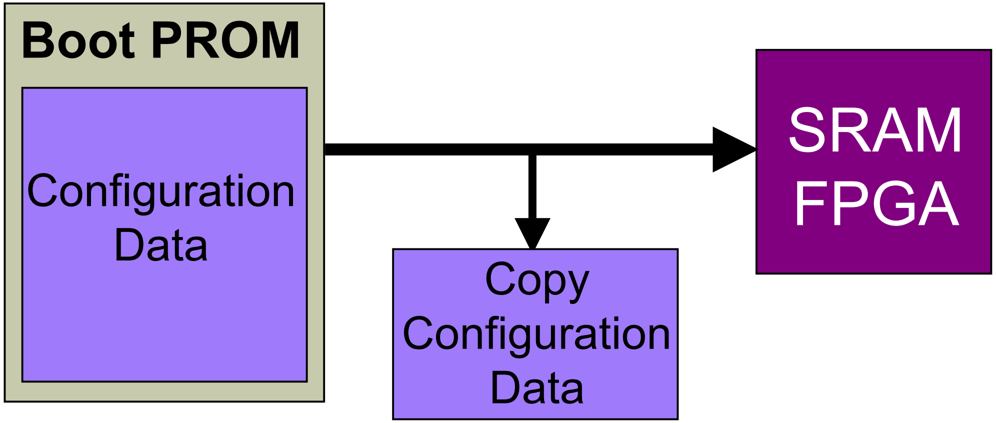
- Noninvasive: Monitored by external means such as brute force key generation, changing voltages to discover hidden test modes, etc.
- Invasive: Decapped and then microprobed using Focused Ion Beams, or other sophisticated techniques to determine the contents of the device.

## Security Threats

- IP Security:  Protecting the integrity of the design or IP that is in the chip
- Data Security: Protecting the flow of data from the chip

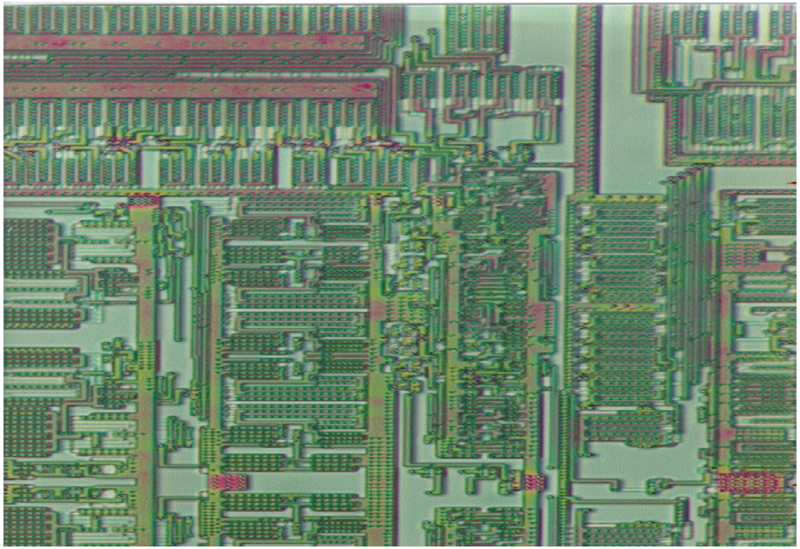
# SRAM Security

- SRAM based devices are volatile
- Configuration data must be loaded each time power is cycled.
- This configuration data is stored in a PROM or microprocessor
- This data can be easily copied at boot-up



# The Myth of ASIC Security

- Often considered a “secure” technology, ASICs are actually relatively easy to reverse engineer
- Packages are de-capped, layers are stripped and photographed one by one
- 4 layer metal ASIC stripped to metal layer 1



# Actel Antifuse/Flash-based FPGAs

## Two Actel FPGA technologies

- Antifuse
  - Nonvolatile and One Time Programmable
- Flash
  - Nonvolatile and Reprogrammable

## Both technologies are nonvolatile

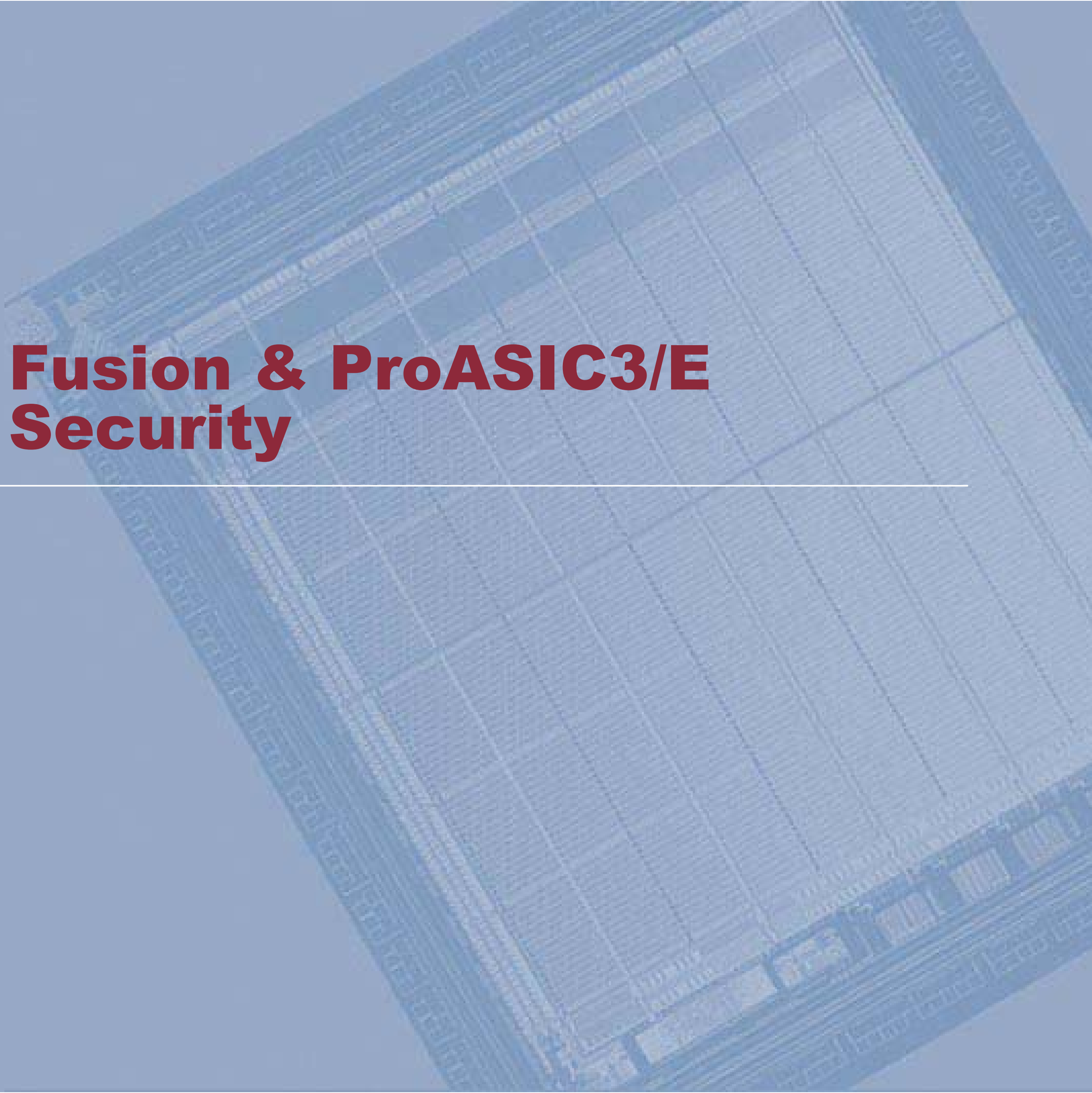
- After being programmed in a secure environment, Flash-based & Antifuse-based FPGAs do not require an external bit stream
- The bitstream does not need to be loaded at system power-up.

# Flash/Antifuse-based FPGA Design Security

- After being programmed in a secure environment, flash/Antifuse-based devices do not require an external bit stream
- Highly resistant to invasive attacks, de-capping and stripping only reveals the structure of the device, not the actual contents
- Large number of switch elements; therefore, attempting to determine the state of millions of switches is prohibitive

# Antifuse FPGA Security

- **Antifuse FPGAs have all data internal to chip**
  - No external bitstream or boot-up PROM required
- **No optical change is visible in a programmed Antifuse**
  - Requires a difficult invasive attack and SEM analysis to identify a programmed link
- **An Axcelerator AX2000 contains approximately 53 million antifuses**
  - Attempts to determine their state physically would take years
  - Only a small fraction (2%-3%) are actually programmed



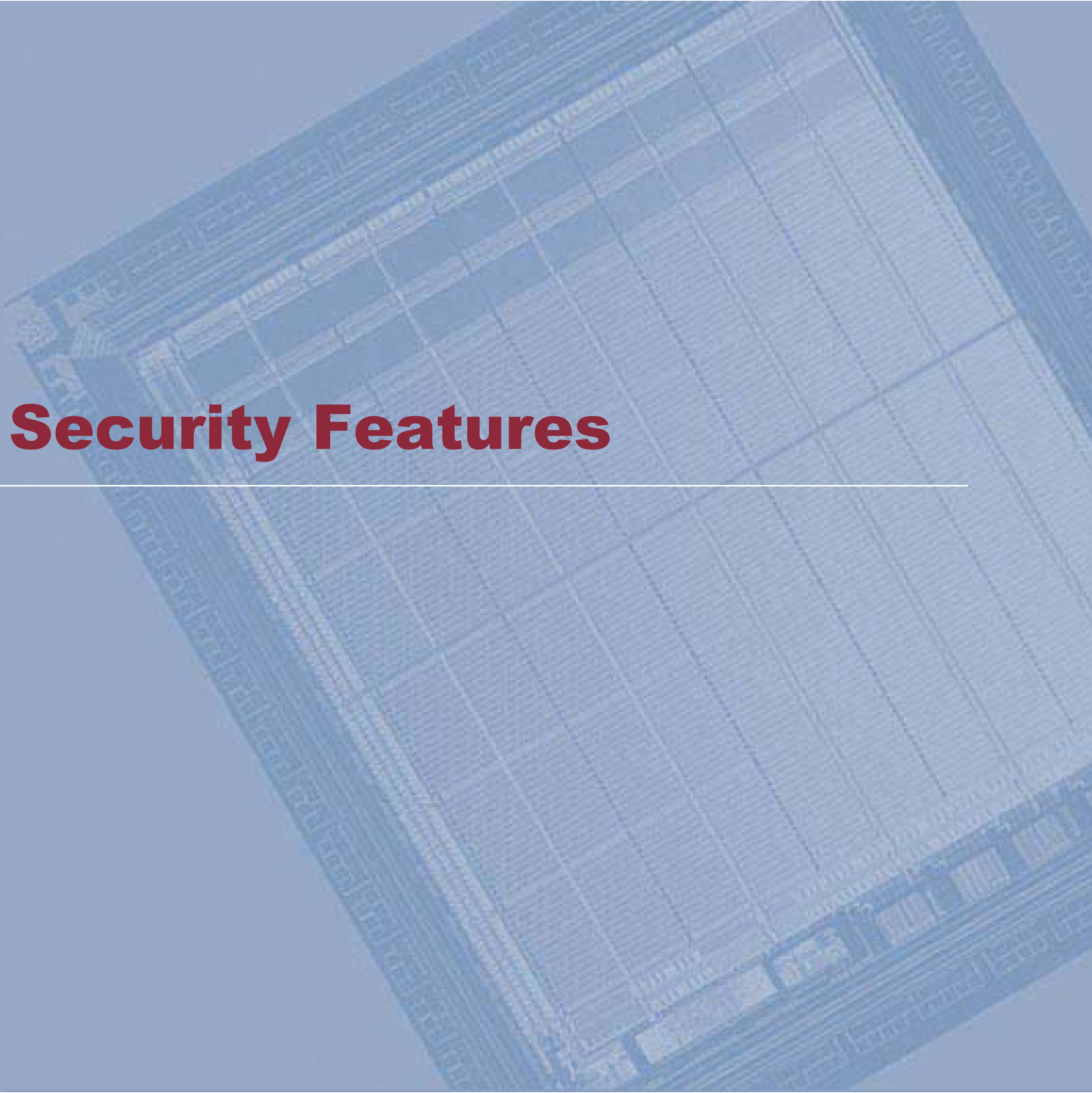
# Fusion & ProASIC3/E Security

# Agenda

- **Security Features**
  - Terminology
  - A3P/E & AFS Security Features Overview
- **Security Usage**
  - Software Settings
  - Security Use Models
  - Permanent Lock

# Security Features

Actel



# Terminology

- **FlashLock Key**
  - Protects Device Security Settings
- **Permanently lock the security settings**
  - Individual Security Settings for Array and FROM can be set Permanently
- **Permanent Lock**
  - Permanently Lock the Array from being Erased/Written or Verified
  - Permanently Lock the FROM from being Erased/Written or Read (verify always allowed)
- **AES Encryption**
  - Protects Programming Data for File Transfer into Device

# AFS and A3P/E Security Features

| | AFS | A3P/E |
|---|---|---|
| FlashLock™ | ✓ | ✓ |
| FlashLock Key | 128 bits | 128 bits |
| Years to Uncover Key[1] | $5.4 \times 10^{23}$ | $5.4 \times 10^{23}$ |
| Permanent FlashLock | ✓ | ✓ |
| AES Encryption on Programming File | ✓ | ✓ |
| AES Key | 128 bits | 128 bits |
| Years to Uncover Key | 149 trillion[2] | 149 trillion[2] |
| Permanent Lock Individual Security Settings | ✓ | ✓ |

[1] - Based on maximum JTAG clock frequency 20MHz

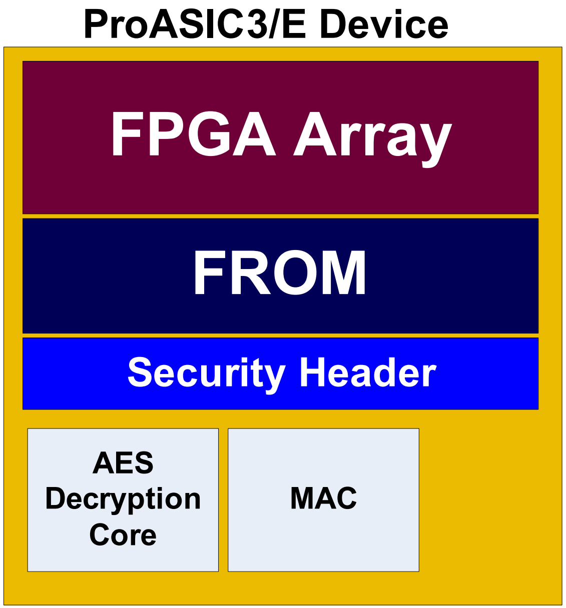
[2] - Using a computing system that could recover a DES key in one second (DES standard has a 56-bit key size)

[*National Institute of Standards and Technology, "ADVANCED ENCRYPTION STANDARD (AES) Questions and Answers," 28 January 2002, http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html*]

# A3P/E & AFS Security Features
## *Device Security Overview*

## Device Security Features

- Security Header
  - 128-bit FlashLock Key
  - 128-bit AES Key
  - Security Access Mode Control
- Built-in 128-bit AES Decryption Core
  - Decrypts Incoming Encrypted Programming Data Using AES
- Message Authentication Control (MAC)
- Flash Cells Located beneath Seven Metal Layers
  - Cannot Remove Layers without Disturbing the Charge on Programmed (or Erased) Flash Gates



# Options for Security Features

- **FlashLock Key Protection (without AES Encryption)**
  - Protection for FROM Only, FPGA Array Only, or Both
- **AES Encryption with FlashLock Key Protection**
  - AES Key Always Protected by FlashLock Key
    - AES-encrypted File Does NOT Contain FlashLock Key
  - Encrypted for FROM Only, FPGA Array Only, or Both
- **Can Update FROM and FPGA Arrays Independently with …**
  - … STAPL File in Plaintext Format OR
  - … STAPL File with AES-encrypted Programming Data
  - STAPL Files Can Be for FROM Only, Array Only, or Both

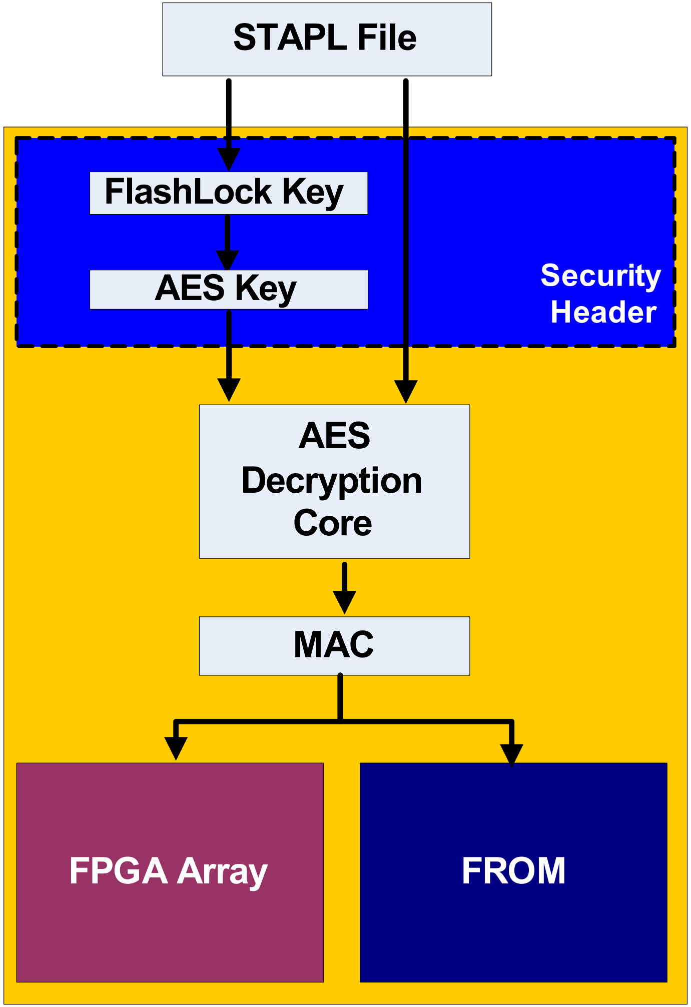
| Security Options | FROM | FPGA Array | Both FROM and FPGA Array |
|---|---|---|---|
| No AES / No FlashLock | ✓ | ✓ | ✓ |
| FlashLock only | ✓ | ✓ | ✓ |
| AES and FlashLock | ✓ | ✓ | ✓ |

# Security Header

- **Security Header Contains Security Keys and Access Mode Control for Both Array and FROM**
  - FlashLock Key
  - AES Key
  - Array Security Setting
    - Access Control for both Write/Erase and Verify
    - Access Control for Encryption/No Encryption (Write/Erase, Verify)
  - FROM Security Setting
    - Access Control for Write/Erase and Read
      - *Verify Always Enabled*
    - Access Control for Encryption/No Encryption (Write/Erase, Read)

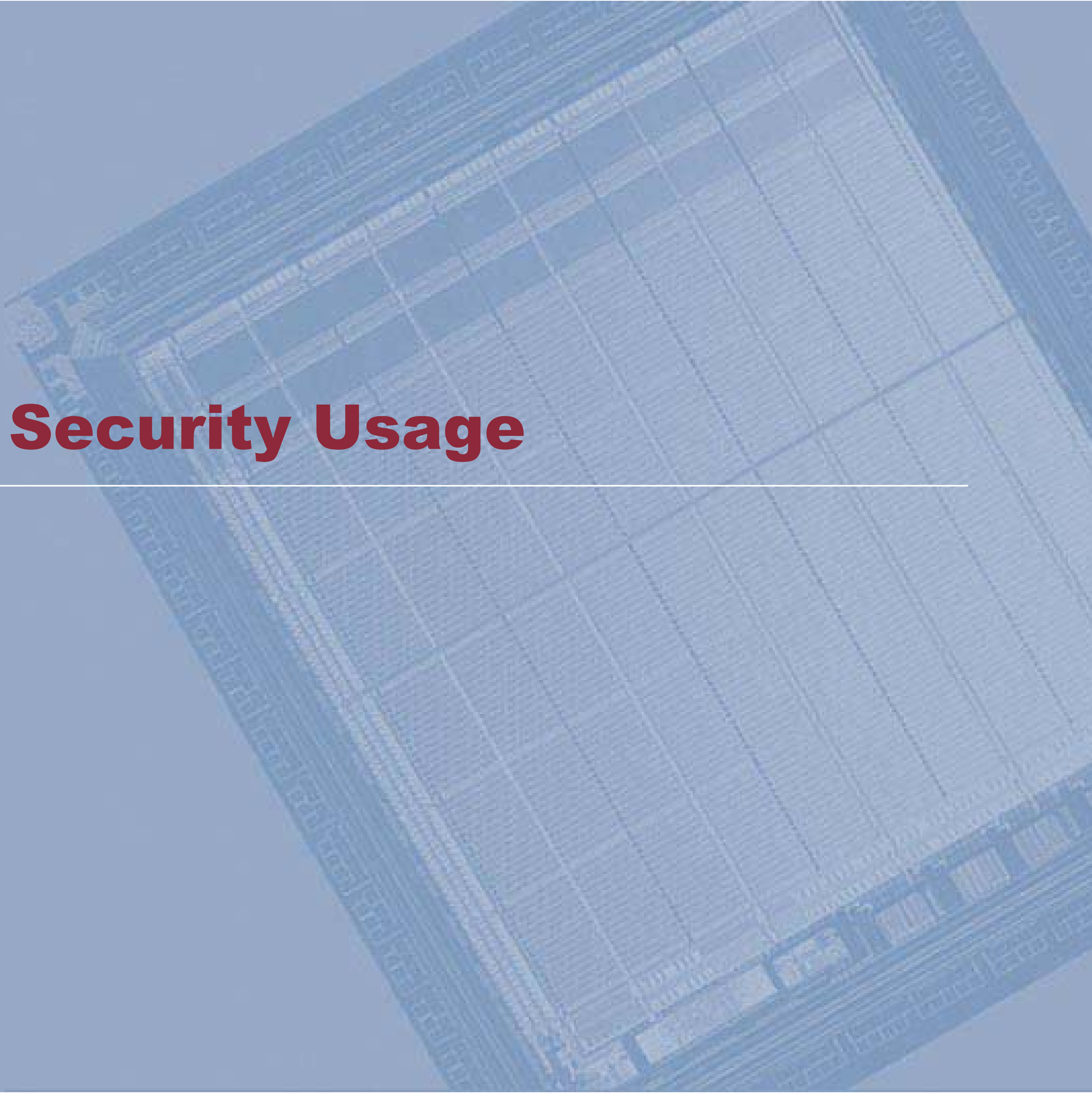
# Message Authentication Control (MAC)

- **Authenticates Entire Programming Data Stream**
  - AES Decryption Core Decrypts STAPL File
  - MAC Checks if Decrypted Data Is Recognizable
    - If Valid, Device Can Be Erased and Programmed
    - If Not, Software Prevents Programming Sequence from Starting
  - Device Operation Still Allowed during Authentication
- **Detects Programming Data Corruption during Data Transfer into Device**
  - Validates each Data Packet before Programming Device



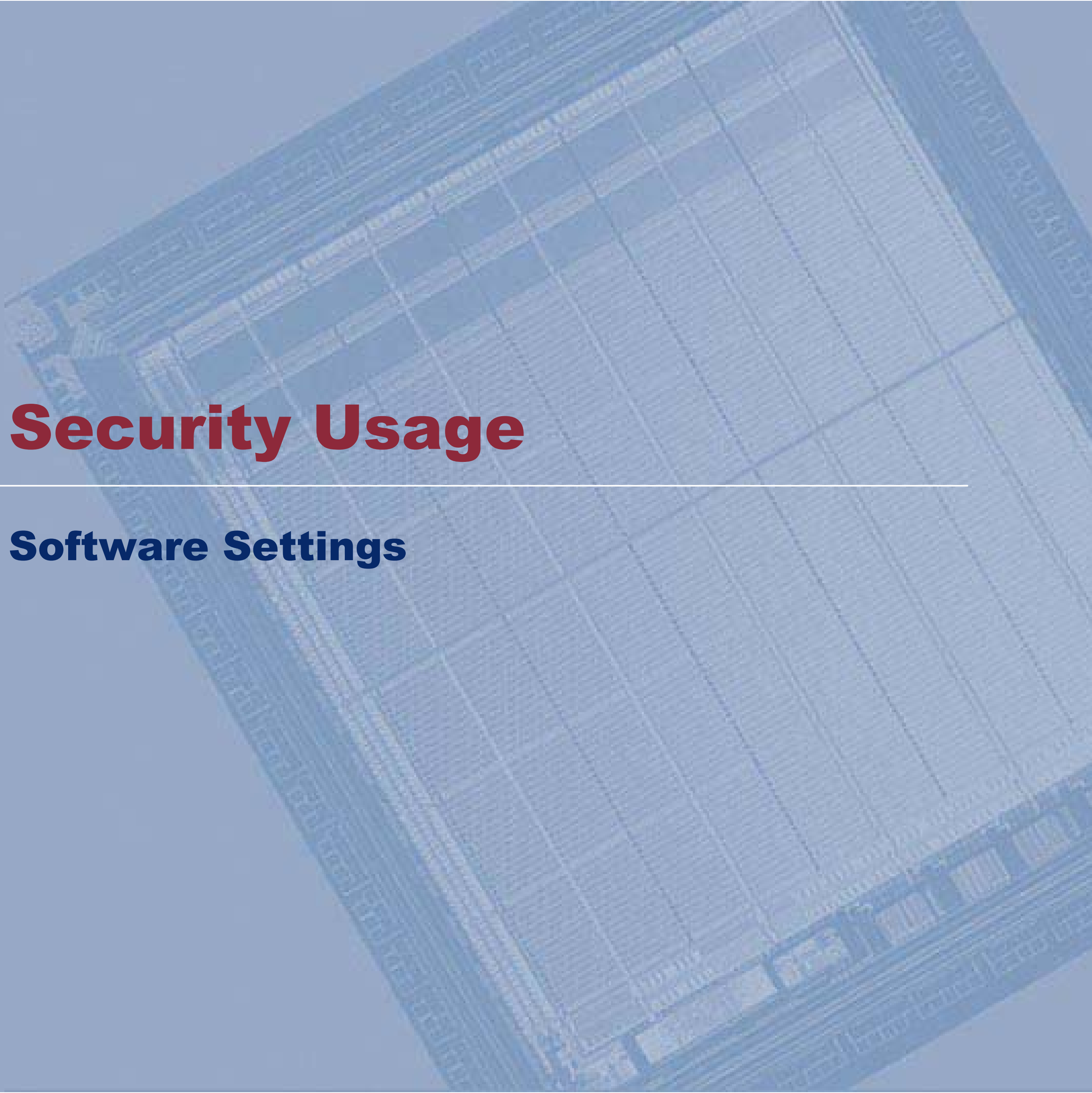
ProASIC3/E Device

# Security Usage



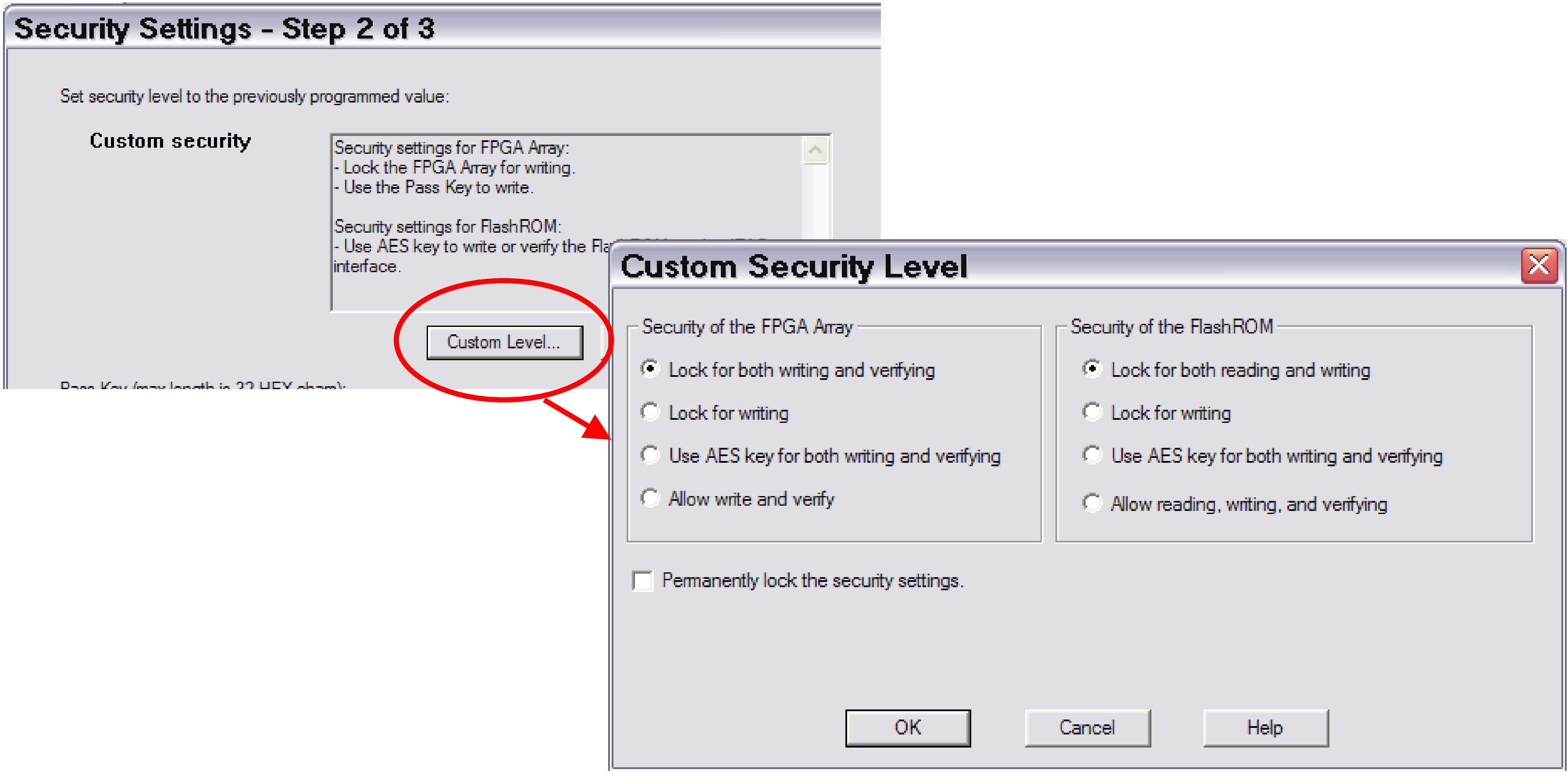
# Security Usage

## Software Settings



# Software Settings
## *Custom Security Levels*

- User Can Choose Custom Settings



**Security Settings - Step 2 of 3**

Set security level to the previously programmed value:

**Custom security**

Security settings for FPGA Array:
- Lock the FPGA Array for writing.
- Use the Pass Key to write.

Security settings for FlashROM:
- Use AES key to write or verify the Fla
interface.

Pass Key (max length is 32 HEX chars):

**Custom Security Level**

Security of the FPGA Array
- ● Lock for both writing and verifying
- ○ Lock for writing
- ○ Use AES key for both writing and verifying
- ○ Allow write and verify

Security of the FlashROM
- ● Lock for both reading and writing
- ○ Lock for writing
- ○ Use AES key for both writing and verifying
- ○ Allow reading, writing, and verifying

☐ Permanently lock the security settings.

# Implications of Security Levels
## *Reading/Writing/Verifying FPGA Array*

- **Lock for Both Writing and Verifying**
  - Allows Write/Erase and Verify only with Valid FlashLock Key
- **Lock for Writing**
  - Allows Write/Erase only with Valid FlashLock Key
  - Verify Is Allowed without Requiring FlashLock Key
- **Use the AES Key for Both Writing and Verifying**
  - Allows Write/Erase and Verify only with a Valid AES Key in the Device
  - Configures the Device to Accept an Encrypted Programming File for Reprogramming and Verifying FPGA Array
  - Requires Valid AES Key in the Device
- **Allow Write and Verify**
  - Allows Write/Erase and Verify with Plaintext STAPL File without Requiring a FlashLock Key or AES Key

# Implications of Security Levels
## *Reading/Writing/Verifying FROM*

## Lock for Both Reading and Writing

- Allows Write/Erase and Read only with a Valid FlashLock Key
- Verify Is Allowed without Requiring a FlashLock Key

## Lock for Writing

- Allows Write/Erase of the FROM only with a Valid FlashLock Key
- Read and Verify Is Allowed without Requiring a FlashLock Key

## Use the AES Key for Both Writing and Verify

- Allows Write/Erase and Verify only with a Valid AES Key in the Device
- This Configures the Device to Accept an Encrypted STAPL File for Reprogramming and Verifying the FROM
- Requires a Valid AES Key in the Device
- Read Is Disabled in this Mode
  - Encrypted FlashROM Contents Only Allow Verify

## Allow Reading, Writing, and Verifying

- Allows Write/Erase, Read, and Verify with a Plaintext STAPL File without Requiring a Valid FlashLock Key or AES Key

# Security Usage

## Security Use Models

# Trusted Environment
## *Use Models*

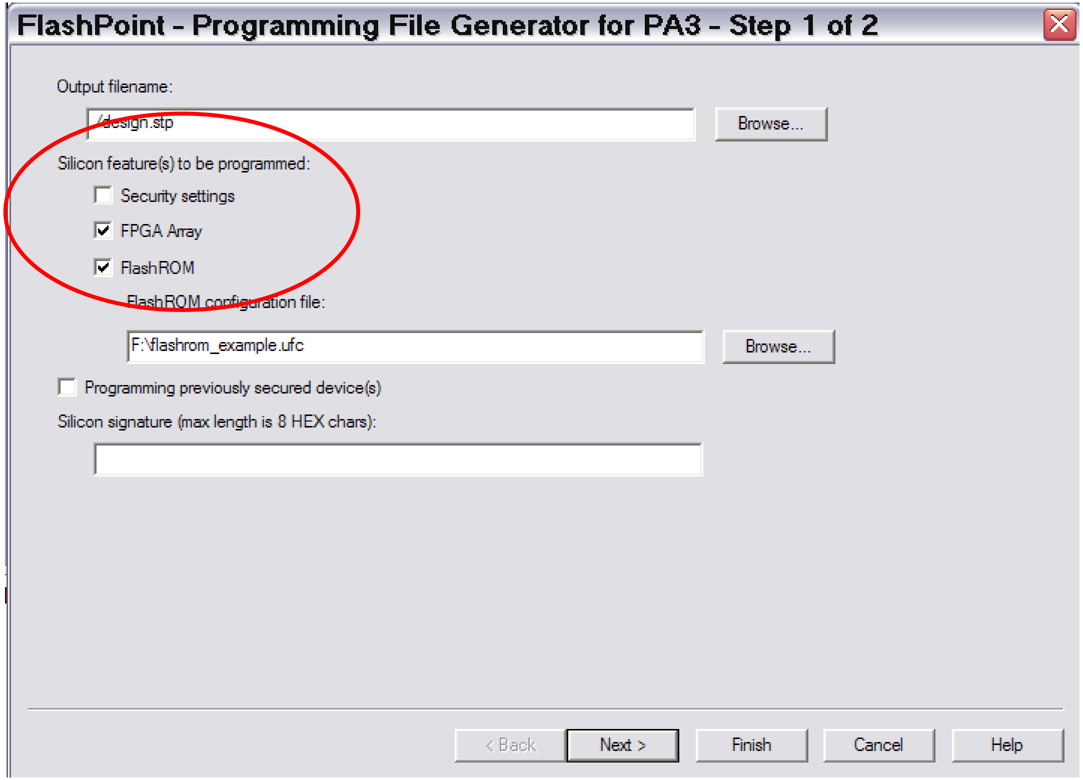
- **Scenarios**
  - Prototyping at design location
  - Programming at trusted IHP location
- **NO Requirements for Security Settings**
  - STAPL File Generation in Plaintext Format
  - Encryption Not Required
    - STAPL Files Not Sent to Unknown Locations
  - Locking Devices Optional
    - User Can Protect Programmed Devices

# Trusted Environment

## *STAPL File Generation*

## Select Silicon Features to Be Programmed

- Check FPGA Array, FROM (FlashROM in software), or Both
- Security Settings Optional



FlashPoint - Programming File Generator for PA3 - Step 1 of 2

Output filename:

/design.stp

Silicon feature(s) to be programmed:

□ Security settings

☑ FPGA Array

☑ FlashROM

FlashROM configuration file:

F:\flashrom_example.ufc

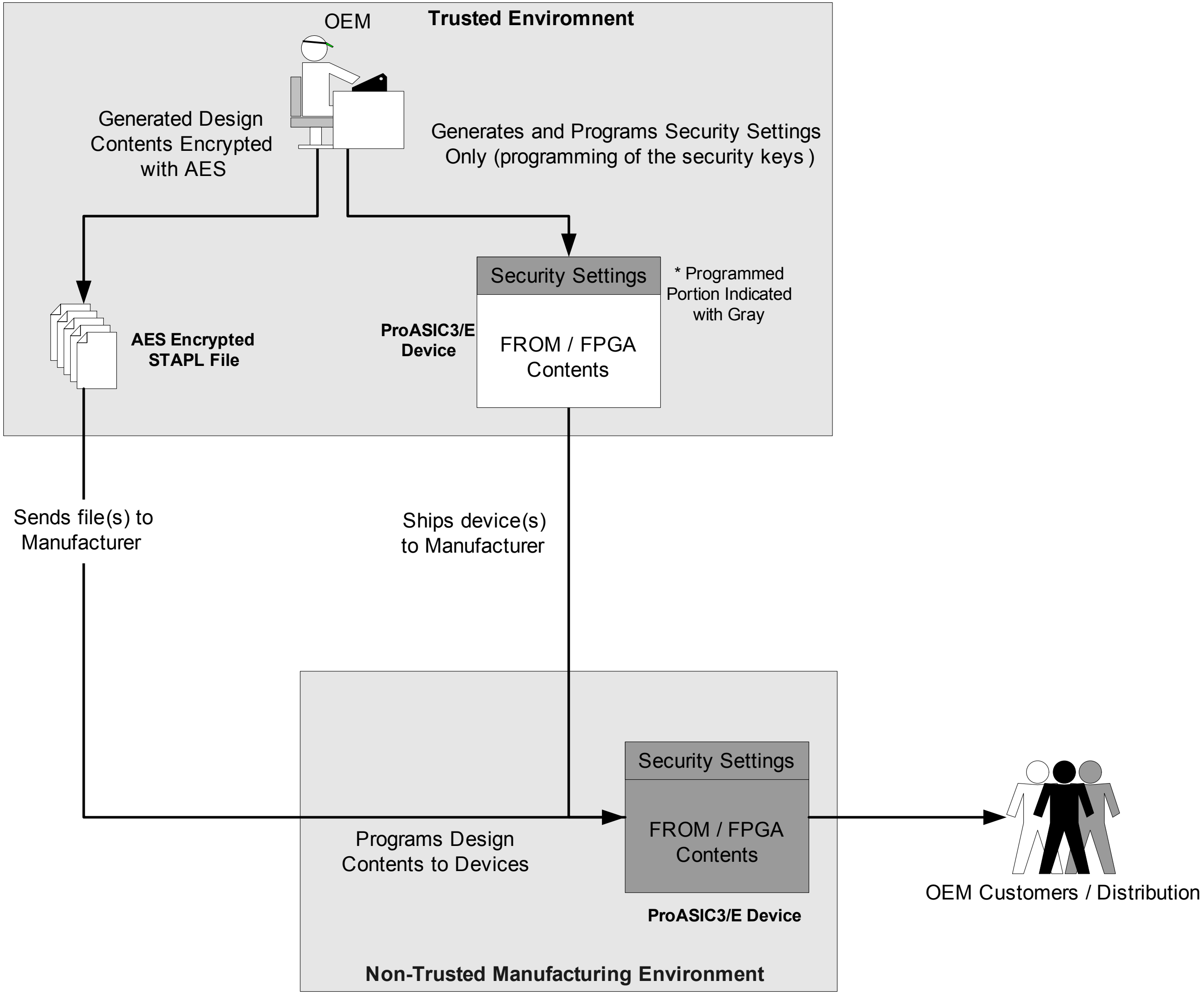
□ Programming previously secured device(s)

Silicon signature (max length is 8 HEX chars):

# Non-Trusted Environment
## *Use Model*

- **Scenario**
  - Production programming at contract manufacturers
- **Pre-programming at Trusted Environment**
  - Devices Pre-programmed in-house with FlashLock Key and AES Key
  - STAPL File Contains FlashLock Key / AES Key
- **Final Programming Done in Non-trusted Environment**
  - STAPL File Generated with AES Encryption
    - For Array, FROM, or Both
  - STAPL File MUST Be Encrypted with Same AES Key Used for Pre-programming
  - STAPL File Does Not Contain FlashLock Key / AES Key

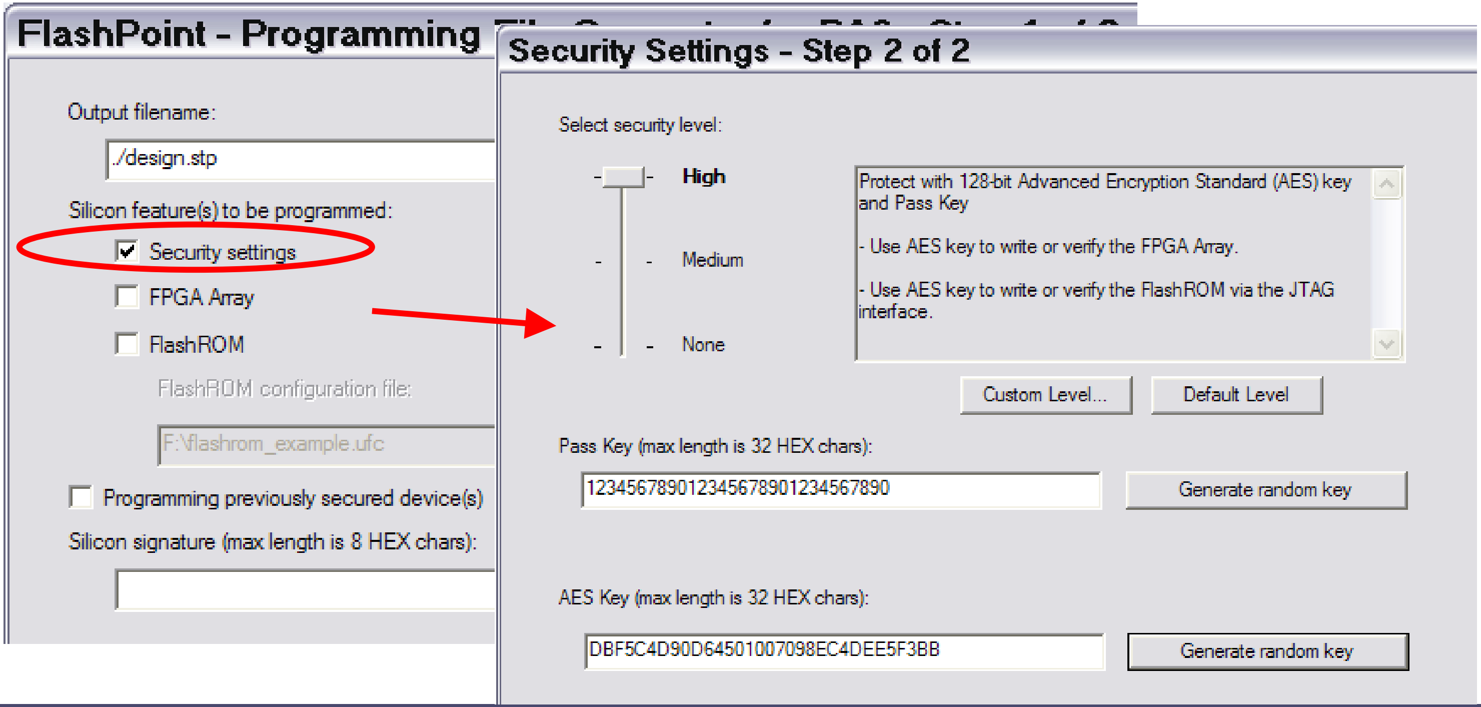
# Non-Trusted Environment
## *Programming Flow*


OEM
Trusted Environment
Generated Design Contents Encrypted with AES
Generates and Programs Security Settings Only (programming of the security keys )
Security Settings
* Programmed Portion Indicated with Gray
AES Encrypted STAPL File
ProASIC3/E Device
FROM / FPGA Contents
Sends file(s) to Manufacturer
Ships device(s) to Manufacturer
Security Settings
FROM / FPGA Contents
Programs Design Contents to Devices
ProASIC3/E Device
OEM Customers / Distribution
Non-Trusted Manufacturing Environment

# Non-Trusted Environment
## *STAPL File Generation – Pre-Programming*

## Configuring Security Header

- Check Security Settings Option
- Uncheck FPGA Array / FlashROM
- Select Desired Security Settings
- Enter FlashLock key (Pass Key in software) and AES Key



FlashPoint - Programming

Output filename:

./design.stp

Silicon feature(s) to be programmed:

☑ Security settings

☐ FPGA Array

☐ FlashROM

FlashROM configuration file:

F:\flashrom_example.ufc

☐ Programming previously secured device(s)

Silicon signature (max length is 8 HEX chars):

Security Settings - Step 2 of 2

Select security level:

High

Medium

None

Protect with 128-bit Advanced Encryption Standard (AES) key and Pass Key

- Use AES key to write or verify the FPGA Array.

- Use AES key to write or verify the FlashROM via the JTAG interface.

Pass Key (max length is 32 HEX chars):

123456789012345678901234567890

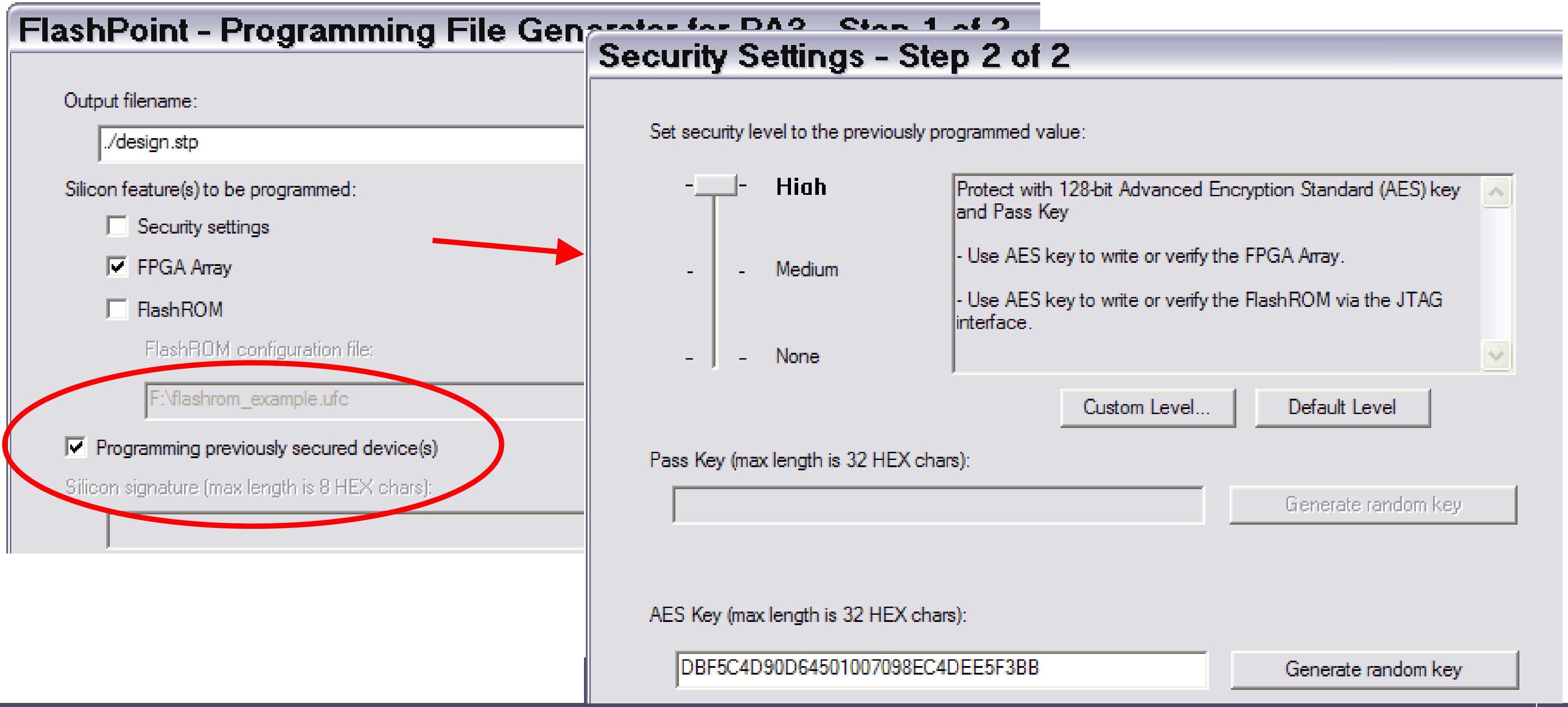
AES Key (max length is 32 HEX chars):

DBF5C4D90D64501007098EC4DEE5F3BB

# Non-Trusted Environment
## *STAPL File Generation – Programming*

## Configuring STAPL File for Encrypted Programming

- Check "Programming previously secured device(s)" Option
- Check FPGA Array Only, FlashROM Only, or Both
- Provide Same AES Key Previously Used for Pre-programming



FlashPoint - Programming File Gen

Output filename:

./design.stp

Silicon feature(s) to be programmed:

☐ Security settings

☑ FPGA Array

☐ FlashROM

FlashROM configuration file:

F:\flashrom_example.ufc

☑ Programming previously secured device(s)

Silicon signature (max length is 8 HEX chars):

Security Settings - Step 2 of 2

Set security level to the previously programmed value:

High

Medium

None

Protect with 128-bit Advanced Encryption Standard (AES) key and Pass Key

- Use AES key to write or verify the FPGA Array.

- Use AES key to write or verify the FlashROM via the JTAG interface.

Pass Key (max length is 32 HEX chars):

AES Key (max length is 32 HEX chars):

DBF5C4D90D64501007098EC4DEE5F3BB

# Remote Field Updates
## *Use Model*

## Scenario

- Devices reprogrammed remotely with updated information

## Update Design

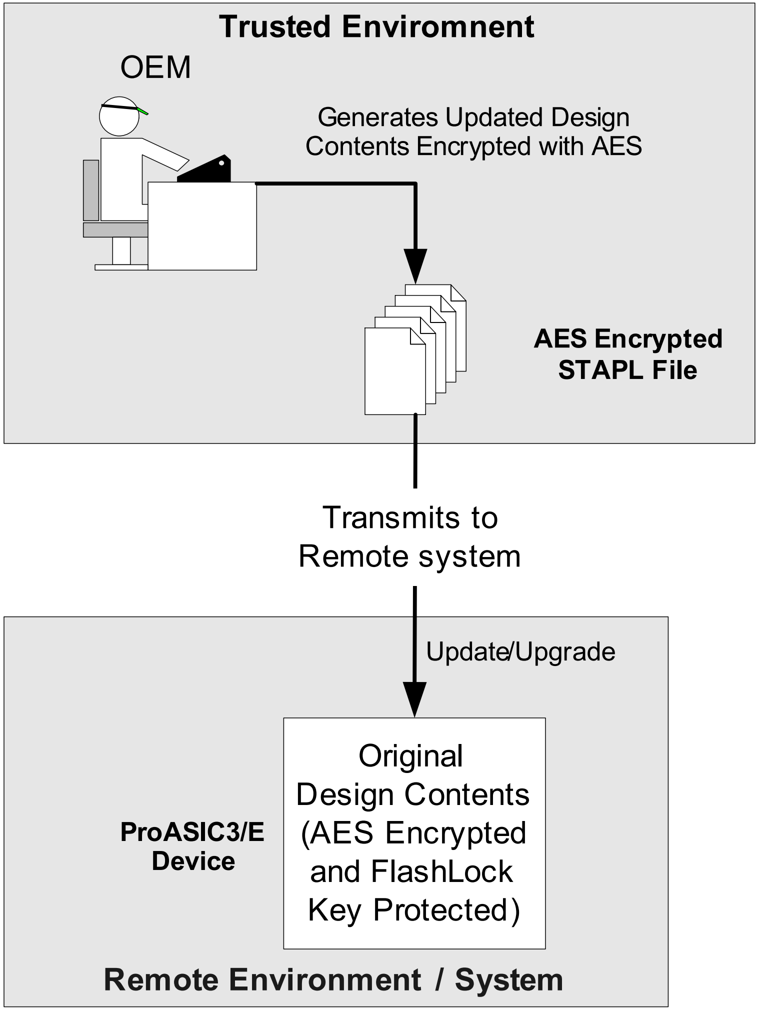
- Update Design for FPGA Array Only, FROM Only, or Both
- STAPL File Generated with AES Encryption

## Encryption

- Must Be Encrypted with Same AES Key Previously Pre-programmed to Device

## Programming Update

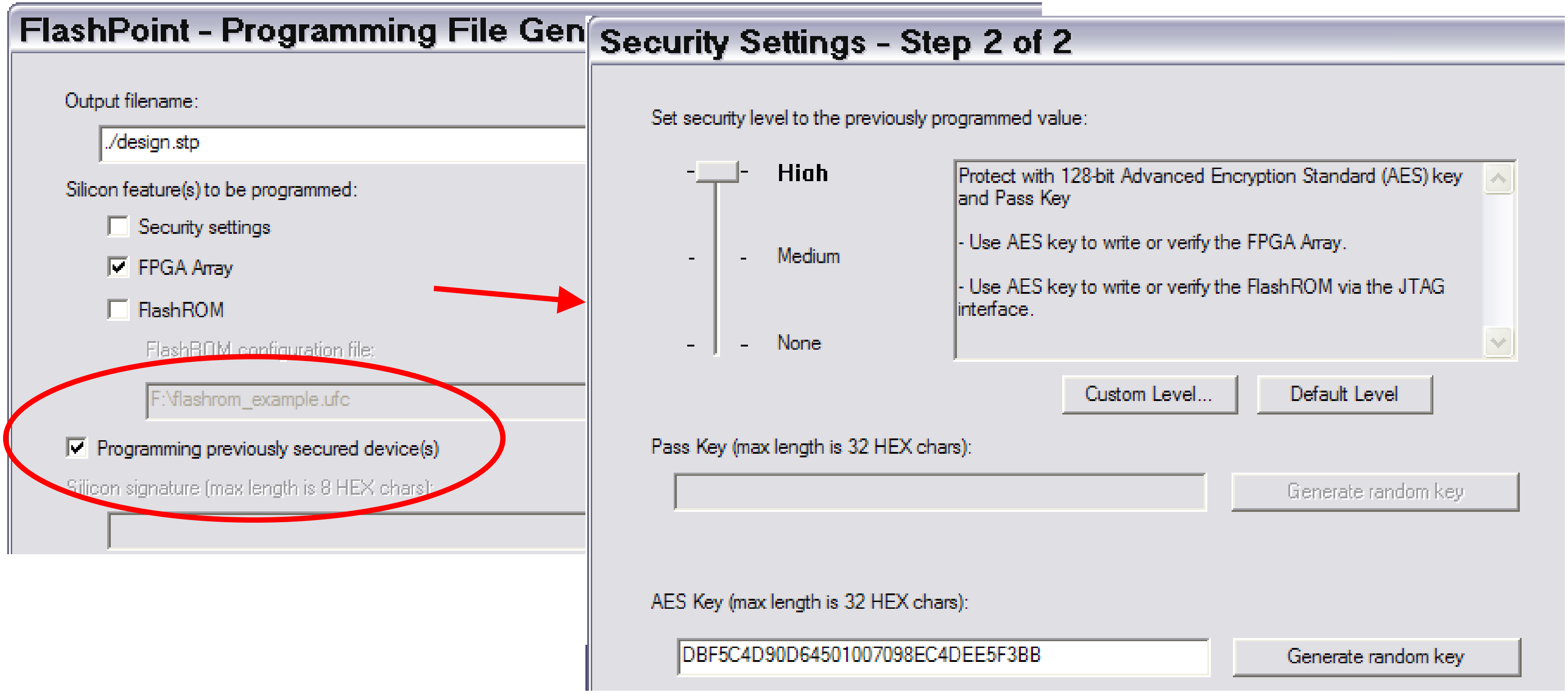
- STAPL File Sent through Web or Service to Remote System


Trusted Enviromnent
OEM
Generates Updated Design Contents Encrypted with AES
AES Encrypted STAPL File
Transmits to Remote system
Update/Upgrade
ProASIC3/E Device
Original Design Contents (AES Encrypted and FlashLock Key Protected)
Remote Environment / System

# Remote Field Updates
## *STAPL File Generation – Programming*

### ■ Configuring STAPL File for Encrypted Programming

- Check “Programming previously secured device(s)” Option
- Check FPGA Array Only, FlashROM Only, or Both
- Provide Same AES Key Previously Programmed to Device



FlashPoint - Programming File Gen

Output filename: ./design.stp

Silicon feature(s) to be programmed:

☐ Security settings

☑ FPGA Array

☐ FlashROM

FlashROM configuration file: F:\flashrom_example.ufc

☑ Programming previously secured device(s)

Silicon signature (max length is 8 HEX chars):

Security Settings - Step 2 of 2

Set security level to the previously programmed value:

Protect with 128-bit Advanced Encryption Standard (AES) key and Pass Key

- Use AES key to write or verify the FPGA Array.

- Use AES key to write or verify the FlashROM via the JTAG interface.

Pass Key (max length is 32 HEX chars):

AES Key (max length is 32 HEX chars): DBF5C4D90D64501007098EC4DEE5F3BB

# Subscription Use Model

OEM programs AES Key and FROM with a unique TAG

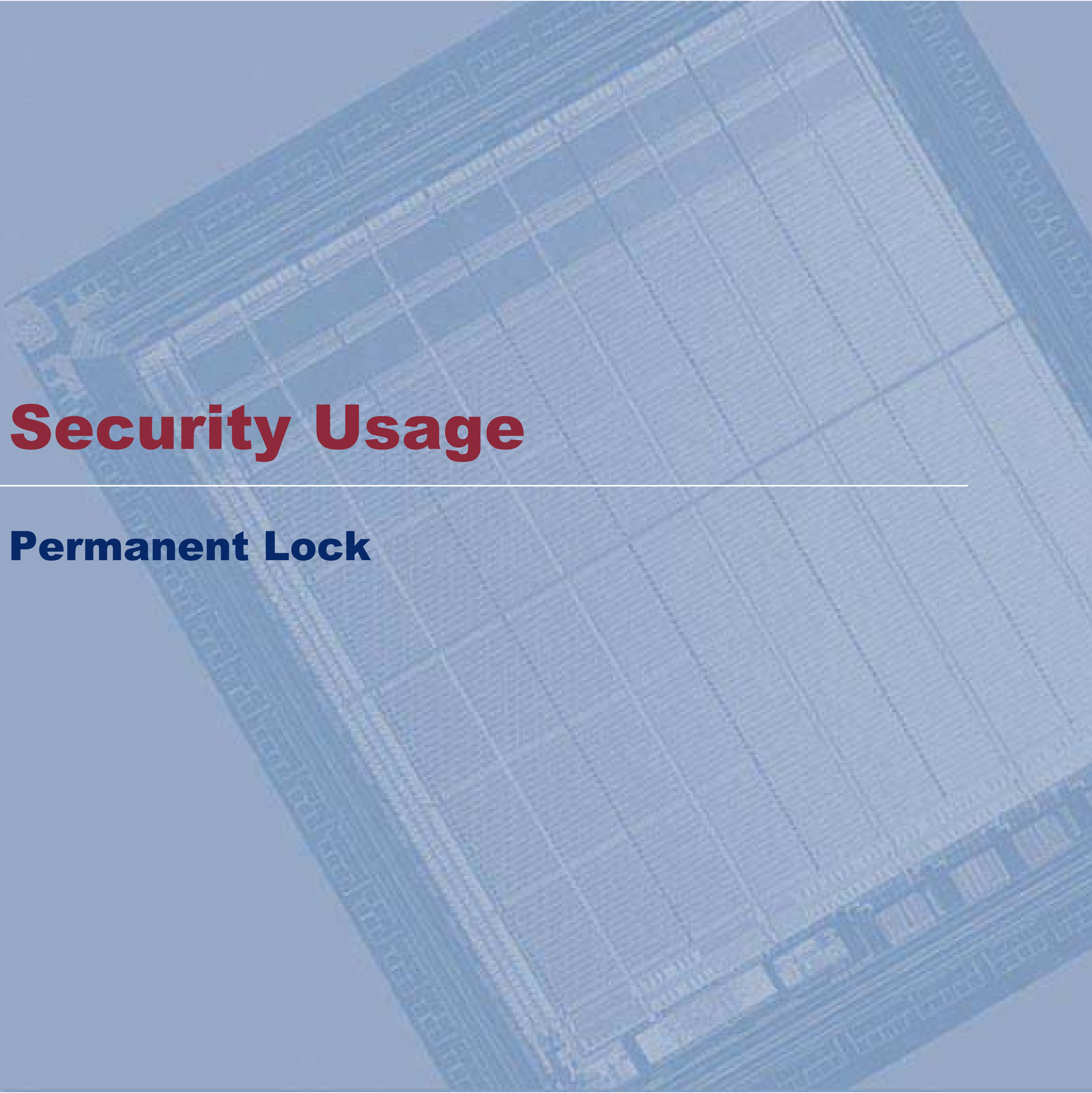
Part is deployed in ‘box’

‘Customer’ requests additional feature by supplying TAG value of ‘box’ over Internet

OEM looks up AES Key based on TAG supplied

New feature-enabled design is encrypted with AES Key and sent to customer via Internet, satellite or direct to ‘box’  for secure ISP

New feature is enabled and will only work with the correctly encrypted design supplied



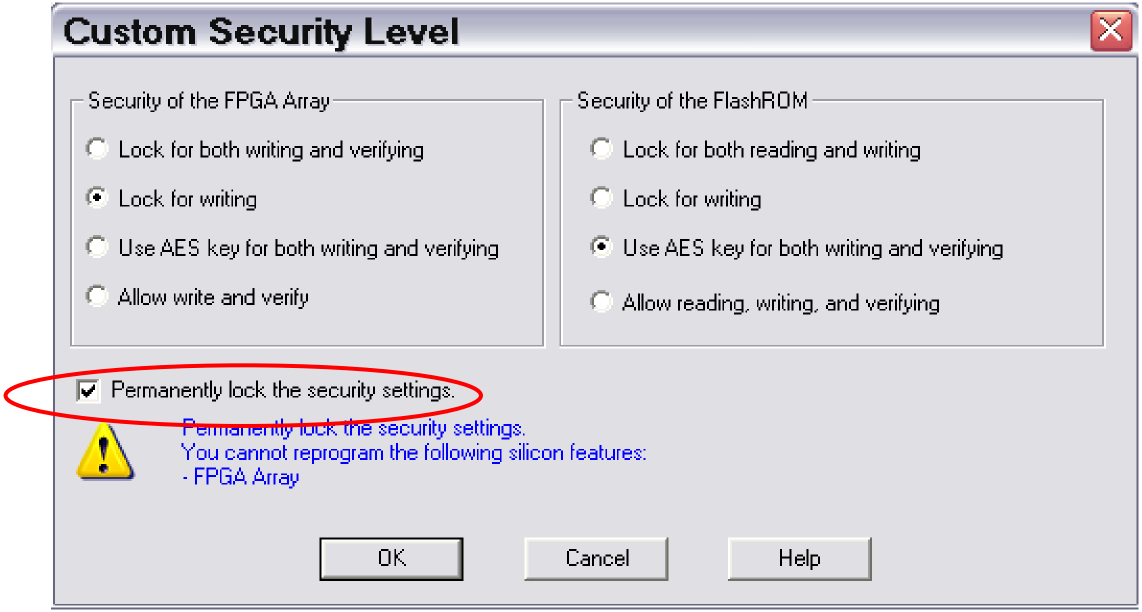
# Security Usage

Actel

## Permanent Lock

# A3P/E & AFS Permanent Security Settings

- Select ‘Permanently Lock the Security Settings’
- No Changes to Security Settings Are Possible after Programming



Custom Security Level

Security of the FPGA Array

○ Lock for both writing and verifying

● Lock for writing

○ Use AES key for both writing and verifying

○ Allow write and verify

Security of the FlashROM

○ Lock for both reading and writing

○ Lock for writing

● Use AES key for both writing and verifying

○ Allow reading, writing, and verifying

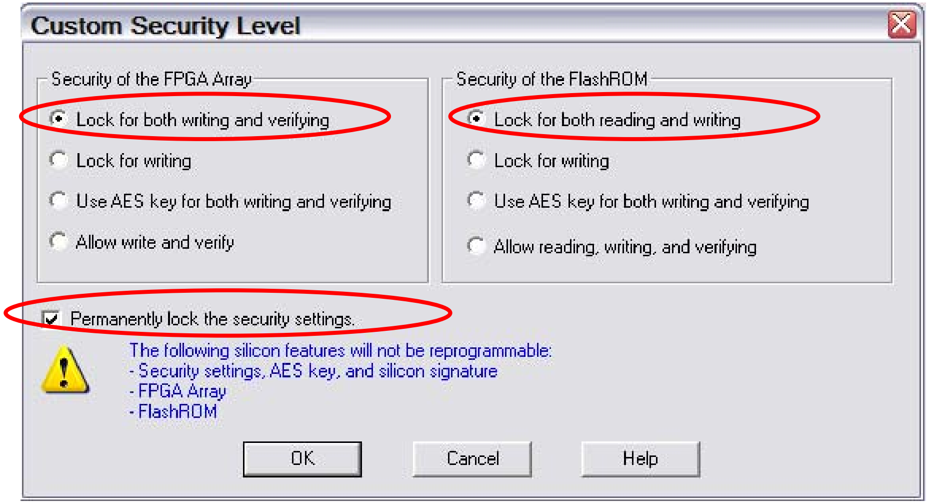
☑ Permanently lock the security settings.

Permanently lock the security settings.
You cannot reprogram the following silicon features:
- FPGA Array

# A3P/E & AFS Permanent Security Settings

## Permanent FlashLock

- Select the Following Settings in the Software
  - FPGA Array – Lock for Both Writing and Verifying
  - FlashROM – Lock for Both Reading and Writing
  - Permanently Lock the Security Settings
- Similar to APA Permanent Lock
  - FPGA Array – Does Not Allow Reprogramming or Verifying
  - FlashROM – Does Not Allow Reprogramming or Reading
    - *Only Allows Verify*



Custom Security Level

Security of the FPGA Array

● Lock for both writing and verifying

○ Lock for writing

○ Use AES key for both writing and verifying

○ Allow write and verify

Security of the FlashROM

● Lock for both reading and writing

○ Lock for writing

○ Use AES key for both writing and verifying

○ Allow reading, writing, and verifying

☑ Permanently lock the security settings.

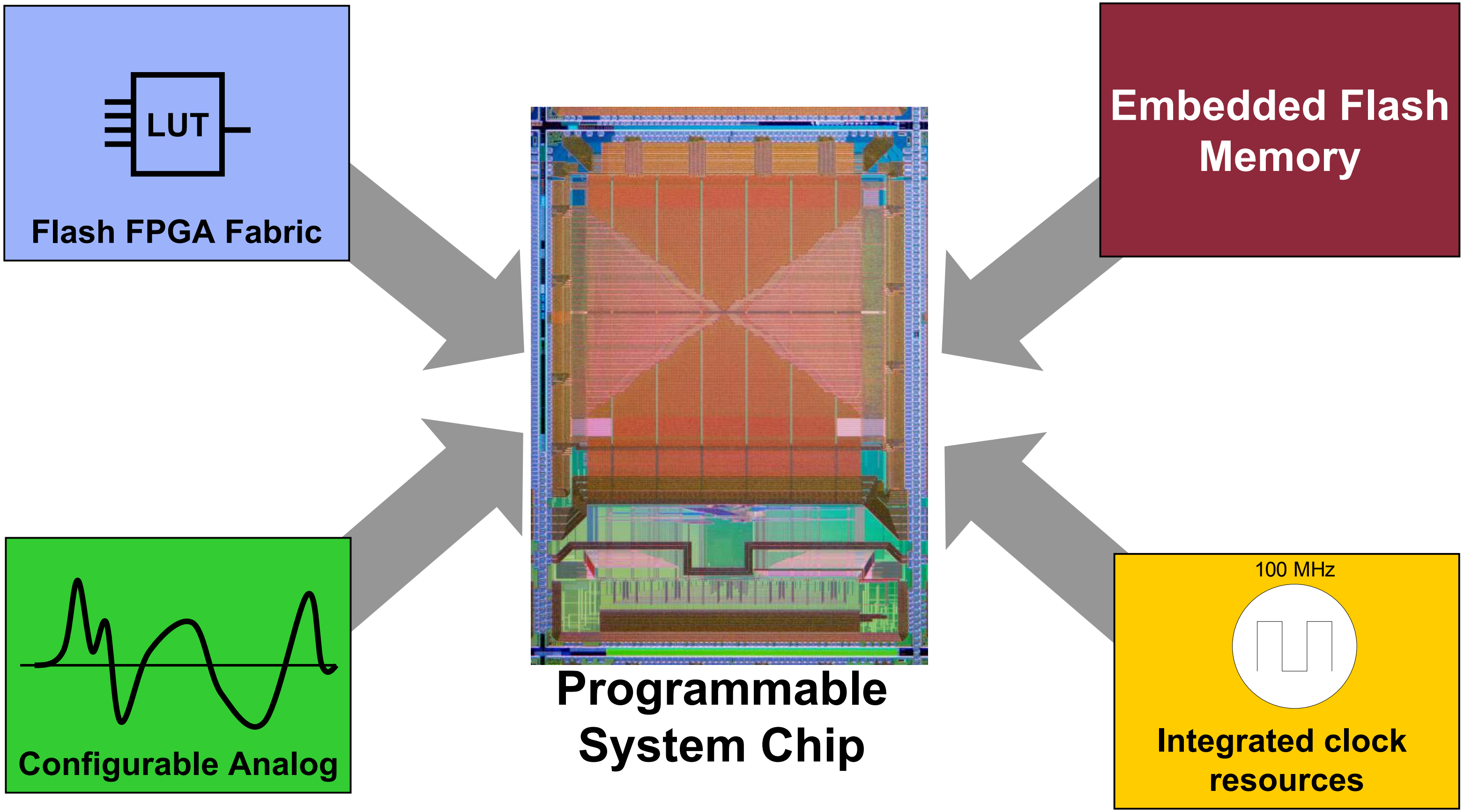
The following silicon features will not be reprogrammable:
- Security settings, AES key, and silicon signature
- FPGA Array
- FlashROM

# Fusion Features

# Fusion – Programmable System Chip

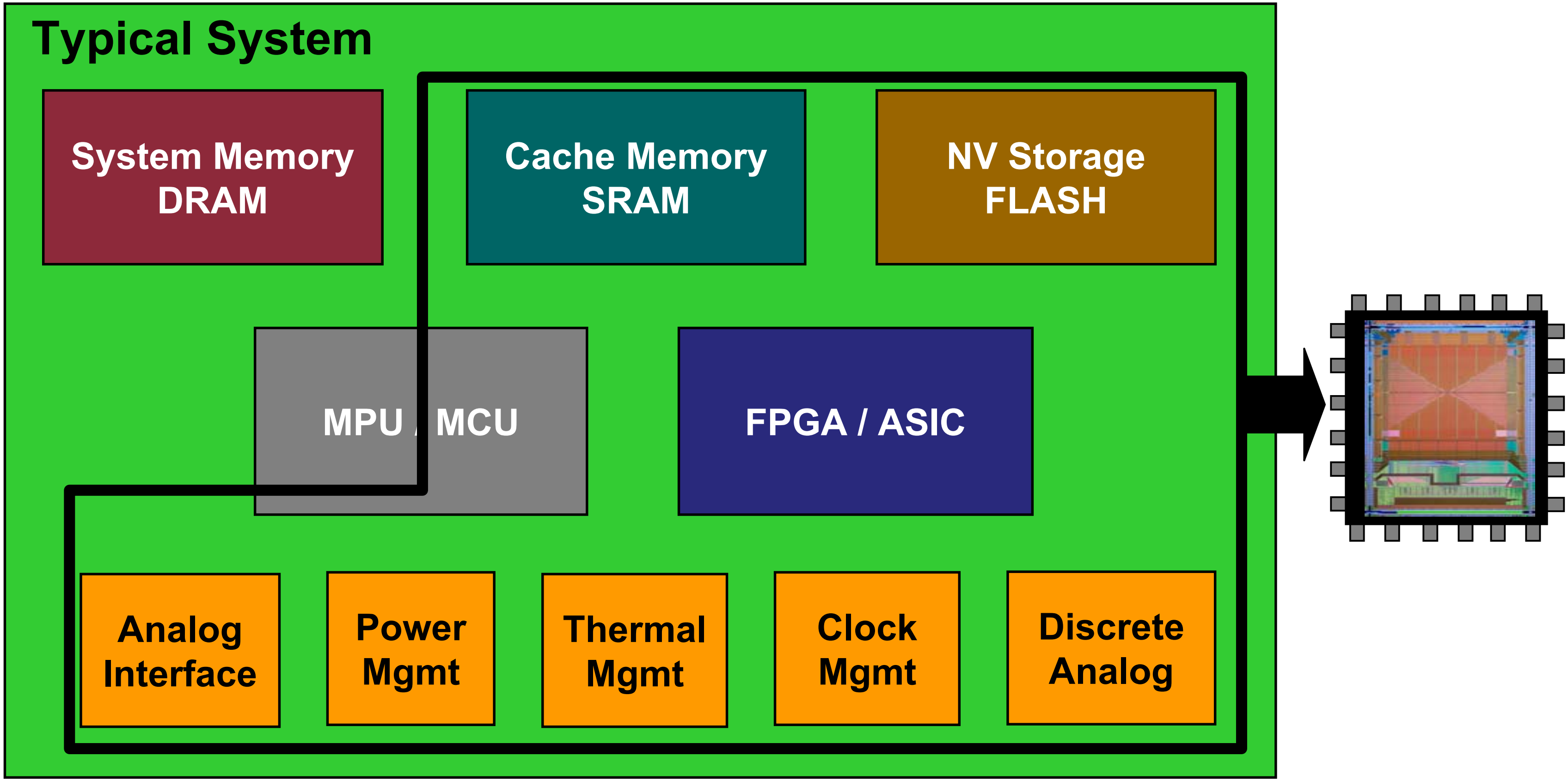
## Changes the competitive landscape

- The world’s first mixed-signal FPGA
- Fusion unlocks creativity: New architecture provides configurability and new tools provide simplified design flow



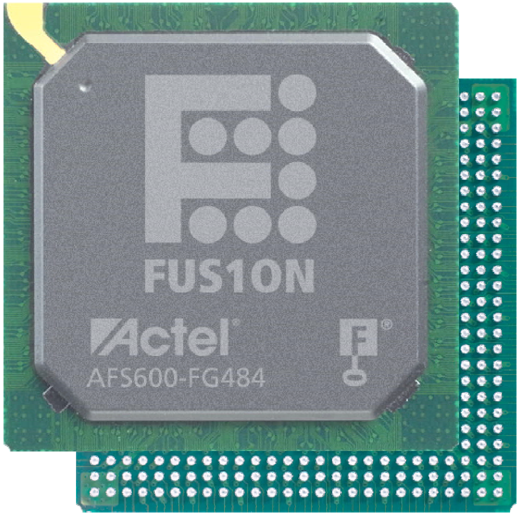
# Fusion – Unprecedented Integration

- **Integrates across functional boundaries**



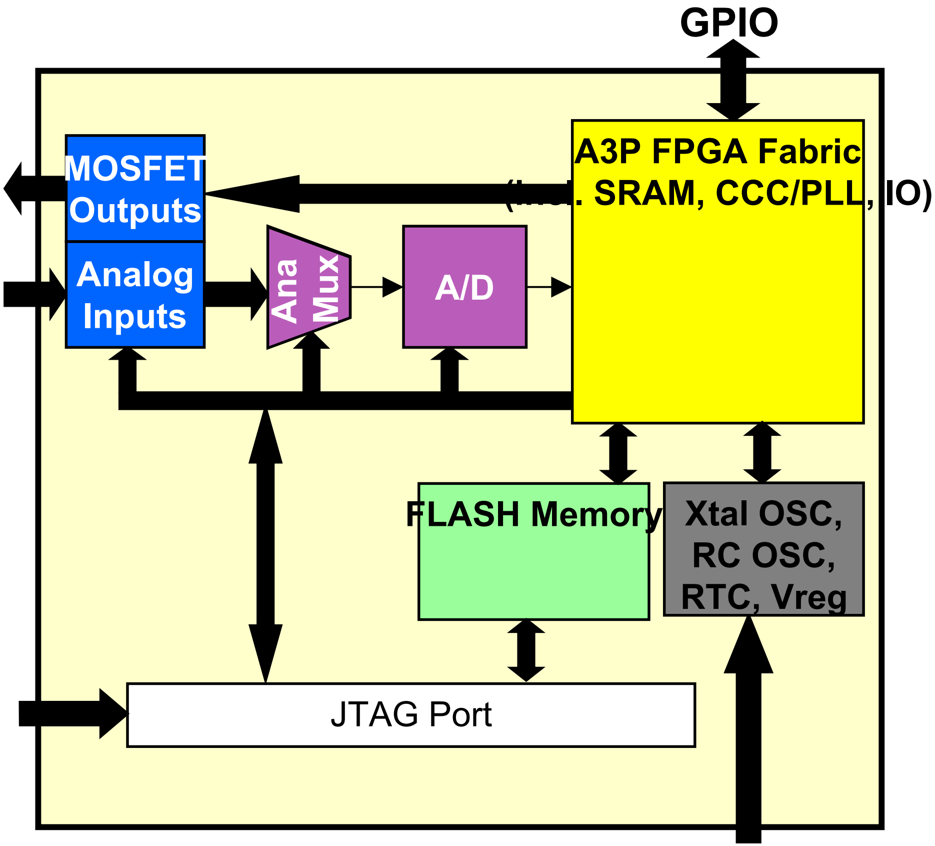
# Fusion Configurability Benefits

- **In System Programmable**
  - Late-stage manufacturing
  - Secure field updates
  - Single update for firmware (flash) and hardware
- **Single chip, many projects**
  - One-stop shop and economies of scale
  - Market-specific customization
- **Increase precision**
  - On-the-fly analog dynamic range selection
- **Power optimization**
  - Multiple configurable clocks sources and PLL



- **Configurable peripherals provide ultimate soft MCU platform**

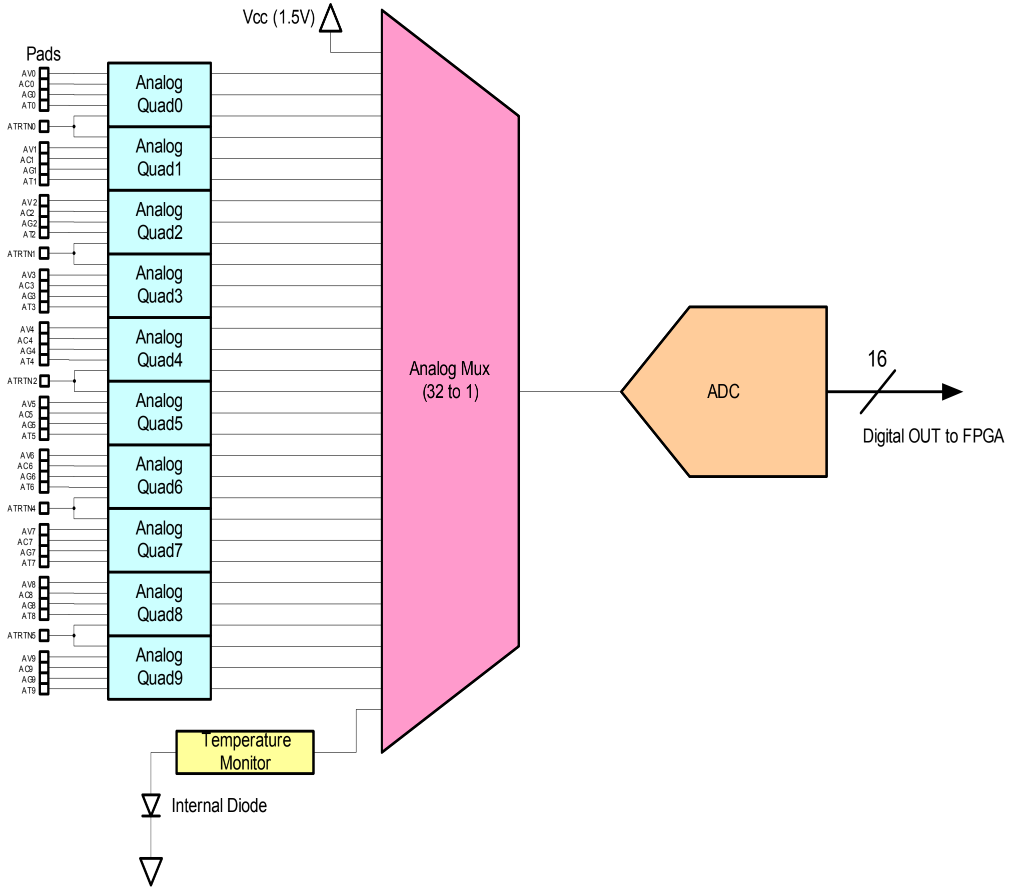
# Fusion: Analog Features



- **Successive Approximation Register (SAR) ADC**
  - Up to 12 bit or 600 Ksps
- **Analog Input**
  - Up to 30 channels input
  - Current monitor block
  - Temperature monitor block
- **Flash memory 2 Mb density**
- **On chip clock resources:**
  - 1 or 2 PLLs
  - Internal 100MHz RC oscillator
  - Crystal Oscillator circuit
  - Real Time Counter (RTC)
- **On chip 1.5V voltage regulator**
- **MOSFET Gate driver output**
  - P and N channel devices
  - Programmable drive strength

# Elements of Analog Block

- **ADC**
  - **Selectable 8/10/12 bit resolution**
  - **32 input channels**
  - **Up to 600K samples per second**
  - **Internal reference voltage**
- **Analog Quad (up to 10 Analog quads)**
  - **Voltage monitor block**
  - **Current Monitor block**
  - **Temperature monitor block**
  - **Gate control/driver block**
- **1.5V Voltage regulator**



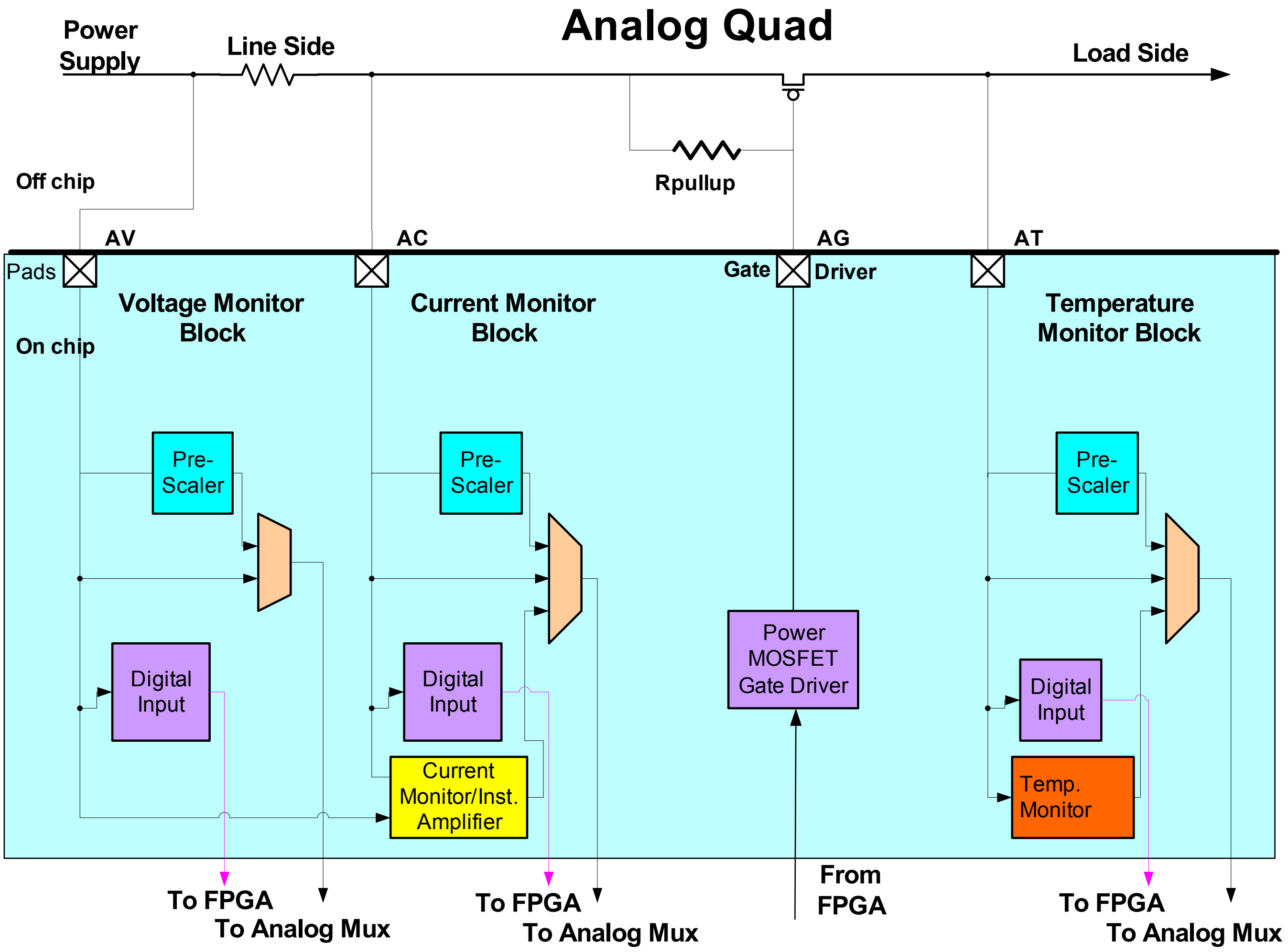
# Fusion ADC – Flexible to meet your needs

- **8/10/12 bit configurable resolution**
- **Resources abound with 30 user input channels**
  - Plus 1 channel monitors device Vcc
  - Plus 1 channel monitors internal temperature diode
- **Robust and accurate**

| Resolution | Through put | TUE (total unadjusted error) |
|---|---|---|
| 8 bit | 600 ksps | ± 2 LSB |
| 10 bit | 550 ksps | ± 4 LSB |
| 12 bit | 500 ksps | ± 6 LSB |

- **Configurable timing controls**
  - ADC interface clock max frequency – 100MHz
  - Selectable clock divider (divide by 4 to 1024) to generate ADC internal clock
  - ADC internal clock frequency range – 1 – 10MHz
  - Sample and Hold
    - Selectable sample time 2 – 257 * ADC internal clock period

# Fusion Analog I/O – Analog Quad



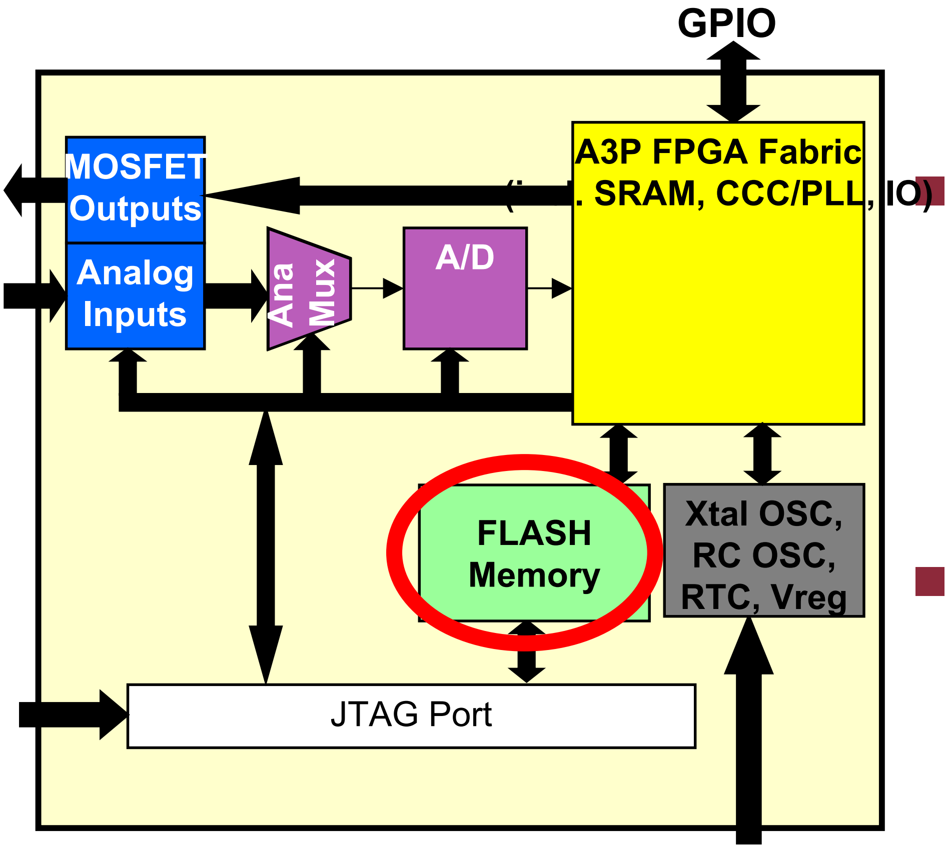
# Fusion: Analog Quad

- **Includes 4 analog interface pins**
  - AV pin – Input: direct and prescaler voltage monitor
  - AC pin – Input: direct and prescaler voltage monitor, current monitor
  - AT pin – Input: direct and prescaler voltage monitor, temp monitor
  - AG pin – Output Power Fet gate control or high voltage, high drive output
- **Configurable as digital I/O**
  - AV, AC, AT pads can be used as high voltage, lower speed digital inputs (10 MHz max)
- **Modular building block used on all Fusion family members**

# Fusion: Only FPGA with Flash Memory

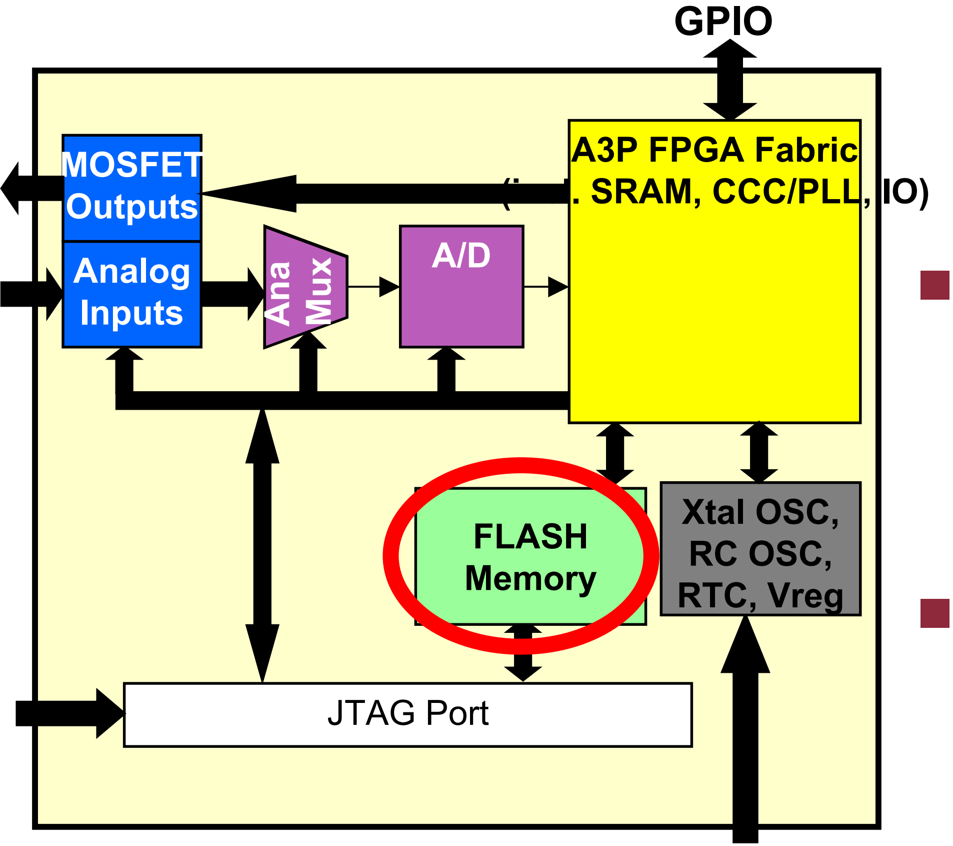
Actel

# Fusion: Flash Features



- **Flash memory 2 Mb density**
  - 1 – 4 blocks/device
  - Each 2 Mb array operates independently (controller)
  - Independent JTAG access
- **Very Flexible operation**
  - x8, x16, and/or x32 FPGA
  - Each supports multiple partitions
  - Small page size (1kb)
  - Can be accessed by either on-chip or off chip resources
- **Supports High performance**
  - 60 ns random access
  - Pipelined 10 ns access of sequential memory addresses

# Fusion:
# Flash Features (cont.)



- **Flash Memory level:**
  - FPGA access
  - Password security
  - JTAG access for programming
- **Page level:**
  - JTAG read / write protection
  - Program/erase
  - Partition on page boundaries
- **Block level error detect:**
  - Single error correct
  - Double error detect

# Module Security Features

- **Status Flash Control of JTAG access to flash block**
  - Similar security for flash data as PA3/E design security
  - 3 lock_controls / module (read/write/encrypt)
  - Chip "user pass code" overrides all JTAG locks
  - Flash access through FPGA core must be secured by FPGA design

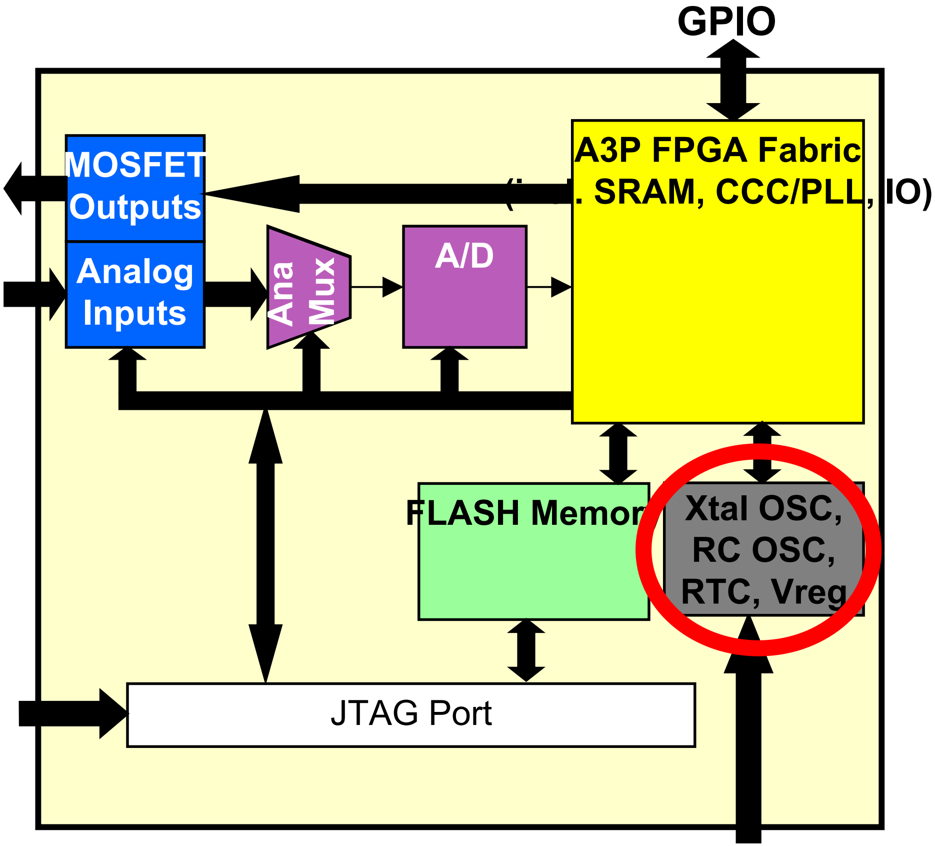
1. **JTAG write lock**
   - Inhibits JTAG update of flash module
2. **JTAG read lock**
   - Inhibits JTAG read of flash module
3. **Enforce Encrypted JTAG download stream**
   - Uses PA3's AES decryption engine
   - Inhibits plain text download to flash module
   - AES decrypt ensures integrity of received data stream (MAC check)

# Page Protection Features

- **Inhibits JTAG read / write to a page**
  - Independent read and write access controls
- **Does not inhibit access from FPGA core**
- **Set on page by page bases**
  - Set at design entry time
  - Sets lock bits in page
  - Overridden by user_pass_code match
  - Modify protection mask by changing parameters at design entry and match of user_pass_code

# Fusion Clocking

# Fusion: Comprehensive Clocking resources



## Fusion builds up clocking resources:

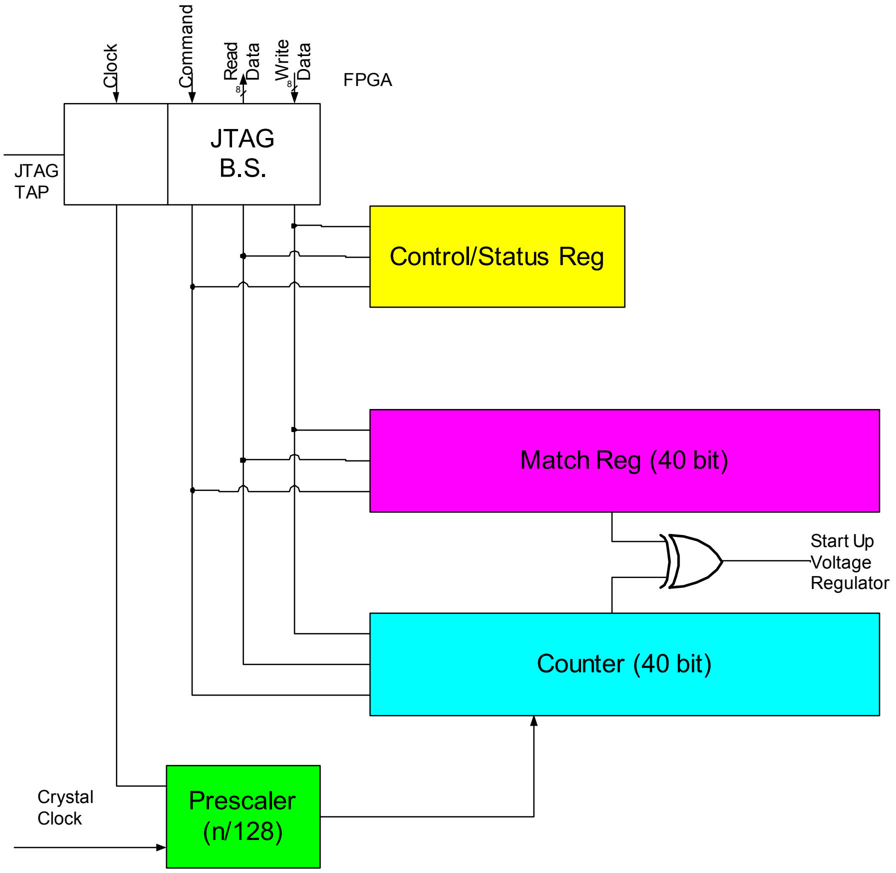
- On chip clock sources:
  - CCC (6) / PLLs (1 or 2)
  - RC oscillator
  - Crystal Oscillator
- Real Time Counter (RTC)

## Use Models

- Internal 100MHz RC oscillator
  - ±1% over I-temp range
- Crystal OSC circuit
  - 32 KHz – 20 MHz
- CCC/PLLs can multiply, divide, and phase shifts clock signals for user applications
  - Sources include: crystal Osc, RC Osc, or external clock
- RTC enables low power standby mode

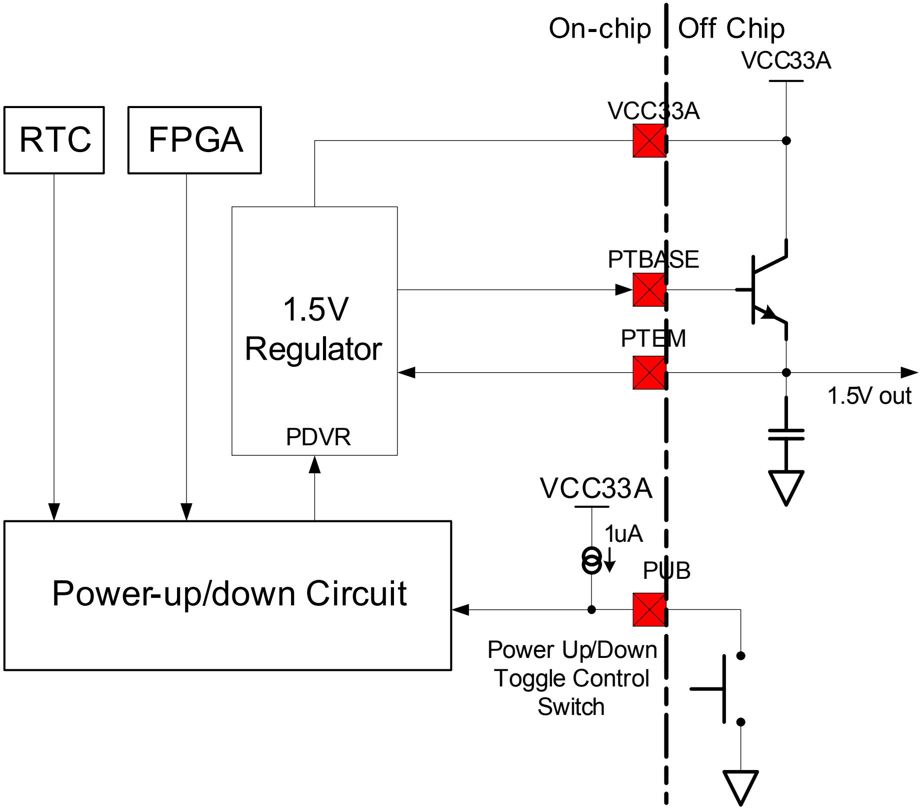
# Real Time Counter (RTC)

- **Added in the 3.3V section**
- **Comprised of:**
  - Control / Status register which is access through ACM
  - 40 bit counter
  - 40 bit match register
  - Input scaler 1/128
    - w/32 kHz clock bit 7 toggles as 1s tick
    - Full counter >20 yr life
- **Can be used for…**
  - Watchdog timer
  - Track real time
  - Long term timed alarms
  - Life of product



# Voltage Regular (V-Reg)

- **Runs off of single 3.3V supply**
- **Generates 1.5 V supply up to 500 mA**
  - Uses external pass transistor
- **1.5V supply is external to the device and can be routed to**
  - Power FPGA
  - Embedded Flash
- **Single supply for both core and Embedded Flash**
  - Cannot be powered down independently
- **Configurable control includes:**
  - FPGA power down signal
  - External wake up signal – push button, wake up signal…
  - Internal wake up – RTC


On-chip
Off Chip
VCC33A
VCC33A
RTC
FPGA
1.5V Regulator
PDVR
PTBASE
PTEM
1.5V out
VCC33A
1uA
PUB
Power-up/down Circuit
Power Up/Down Toggle Control Switch