Enabling Security in ProASIC®3 FPGAs with Hardware and Software Features

Hans Schmitz

Area Technical Manager / Field Applications Engineer

September 2, 2009

Abstract

- Two types of security features available in Actel's ProASIC3 family for applications requiring security
  - Hardware security features
  - Software security features
- Hardware security features exist in the ProASIC3 FPGA fabric
  - Hardware security features are selectable in Actel's Libero® Integrated Design Environment (IDE) software
- Software security features exist in Libero IDE
  - Design examples will illustrate how these features work

Actel Corporation © 2009. May be published with permission by MAPLD 2009

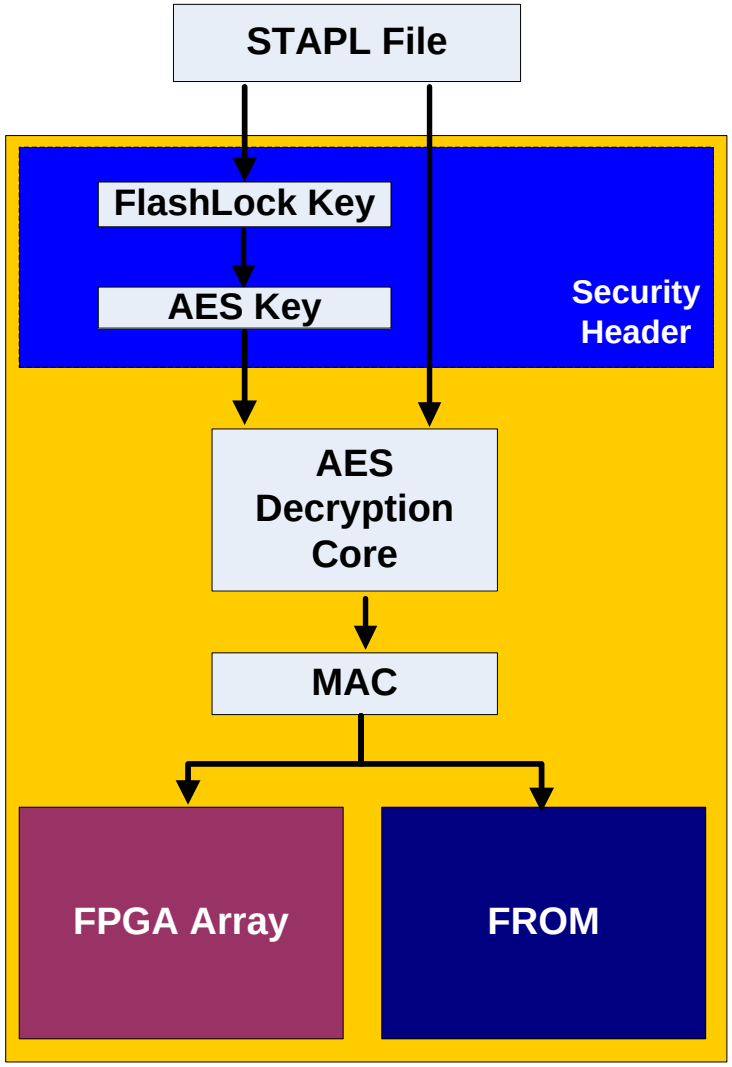
What is Security?

- Security is defined in various ways, and Actel supports various methods of security
  - Hardware
    - Single-chip component, with no bitstream susceptible to interception during power-up
    - Inability to read the data out of the device (this is good)
    - Encrypted programming file (AES128)
    - FlashLock® security key (128-bit key)
  - Software
    - Placement and routing constraints
    - Block methodology

Actel Corporation © 2009. May be published with permission by MAPLD 2009

Hardware Security Description

- FlashLock Key
  - None
    - No security key selected
  - FlashLock
    - A “key” locks the array from being erased, programmed or verified
    - Individual security settings for logic array and FlashROM
  - Permanent lock
    - Permanently lock the array from being erased, programmed or verified
    - Permanently lock the FROM from being erased/written or read (verify always allowed)
- AES encryption
  - AES128 encryption protects programming data for file transfer into device



Actel Corporation © 2009. May be published with permission by MAPLD 2009

Hardware Security: Value to User

	A3P/E
FlashLock	✓
FlashLock Key	128 bits
Years to Uncover Key[1]	$5.4x10^{23}$
Permanent FlashLock	✓
AES Encryption on Programming File	✓
AES Key	128 bits
Years to Uncover Key	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*]

Actel Corporation © 2009. May be published with permission by MAPLD 2009

Software Security

- Physical design constraints
  - Preserve block routing, prevent routing conflicts
    - “Floorplanning” design with multiple blocks
    - “Moving” routed block or cross family/die block instantiation
    - Multiple block instantiation
  - Isolation and security applications
    - Secure boundaries/fences
    - Secure inter-block connections
    - Applications examples
      - Redundant type 1 encryptions
      - Red and black data resident
      - Multiple independent levels of security on a single chip
  - Control routing
    - Timing or congestion issues

Actel Corporation © 2009. May be published with permission by MAPLD 2009

Software Security: Region Definitions

- Region constraint: a rectilinear area with assigned macros
  - 3 types: inclusive, exclusive or empty
- Such region divides all nets into
  - Internal net – all pins belong to the region
  - External net – no pin belongs to the region
  - Interface net – has pins inside and outside of the region
- Such region divides all routing resources into
  - Internal resource – all switches belong to the region
  - External resource – no switch belongs to the region
  - Interface resource – has switches inside and outside of the region

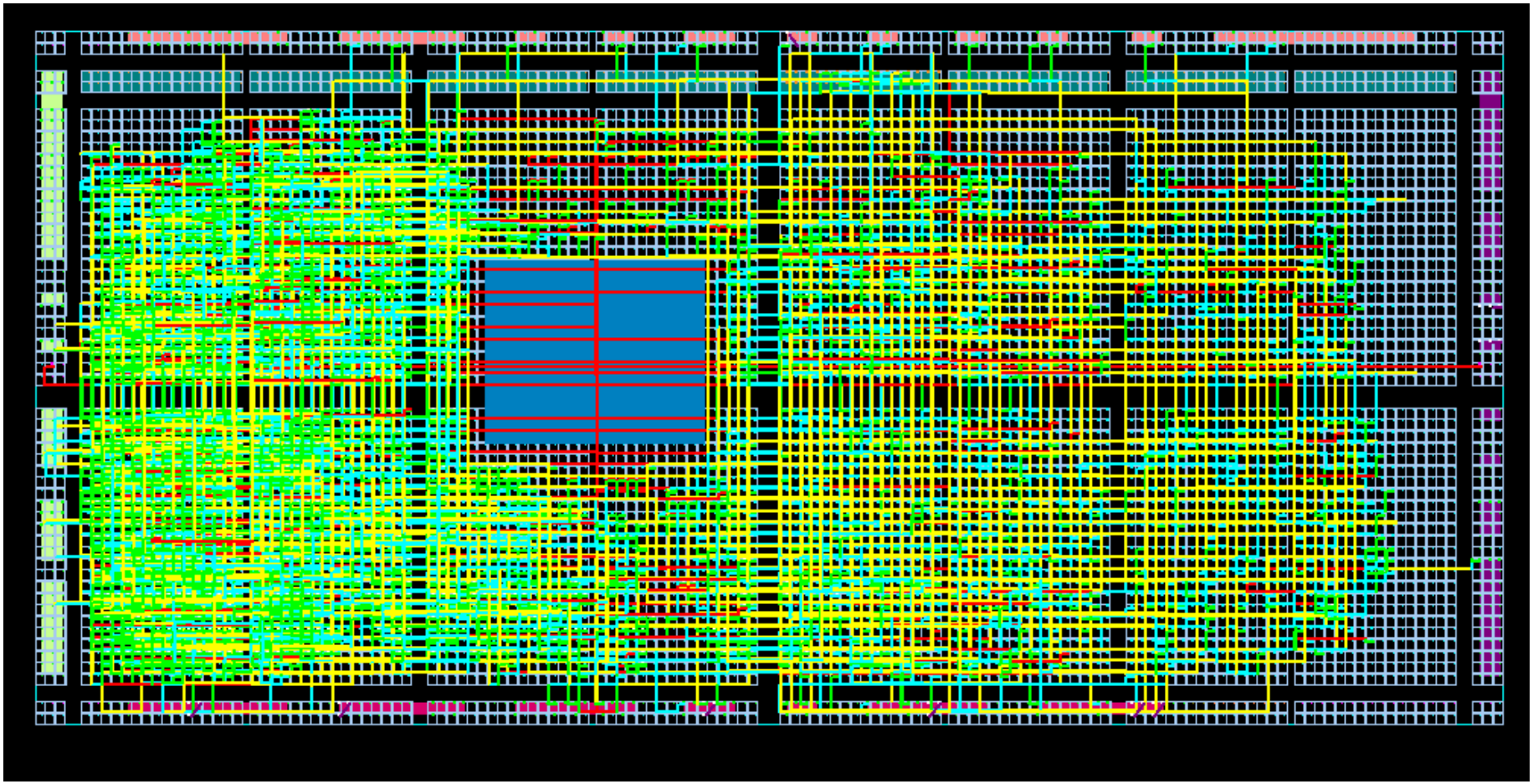
Actel Corporation © 2009. May be published with permission by MAPLD 2009

Software Security: Routing Definitions

- An inclusive routing region is an inclusive placement region along with the following additional constraints
  - All internal nets must use only internal routing resources
  - All other nets can be routed anywhere
- An exclusive routing region is an exclusive placement region along with the following additional constraints
  - All internal nets must use only internal routing resources
  - All external nets must use only external resources
  - Interface nets can be routed anywhere
    - They will cross region boundaries
  - Globals, quadrant clocks and local clocks are excluded
- An empty routing region is an empty placement region along with the following additional constraints
  - All nets must use only external resources
  - Globals, quadrant clocks and local clocks are excluded

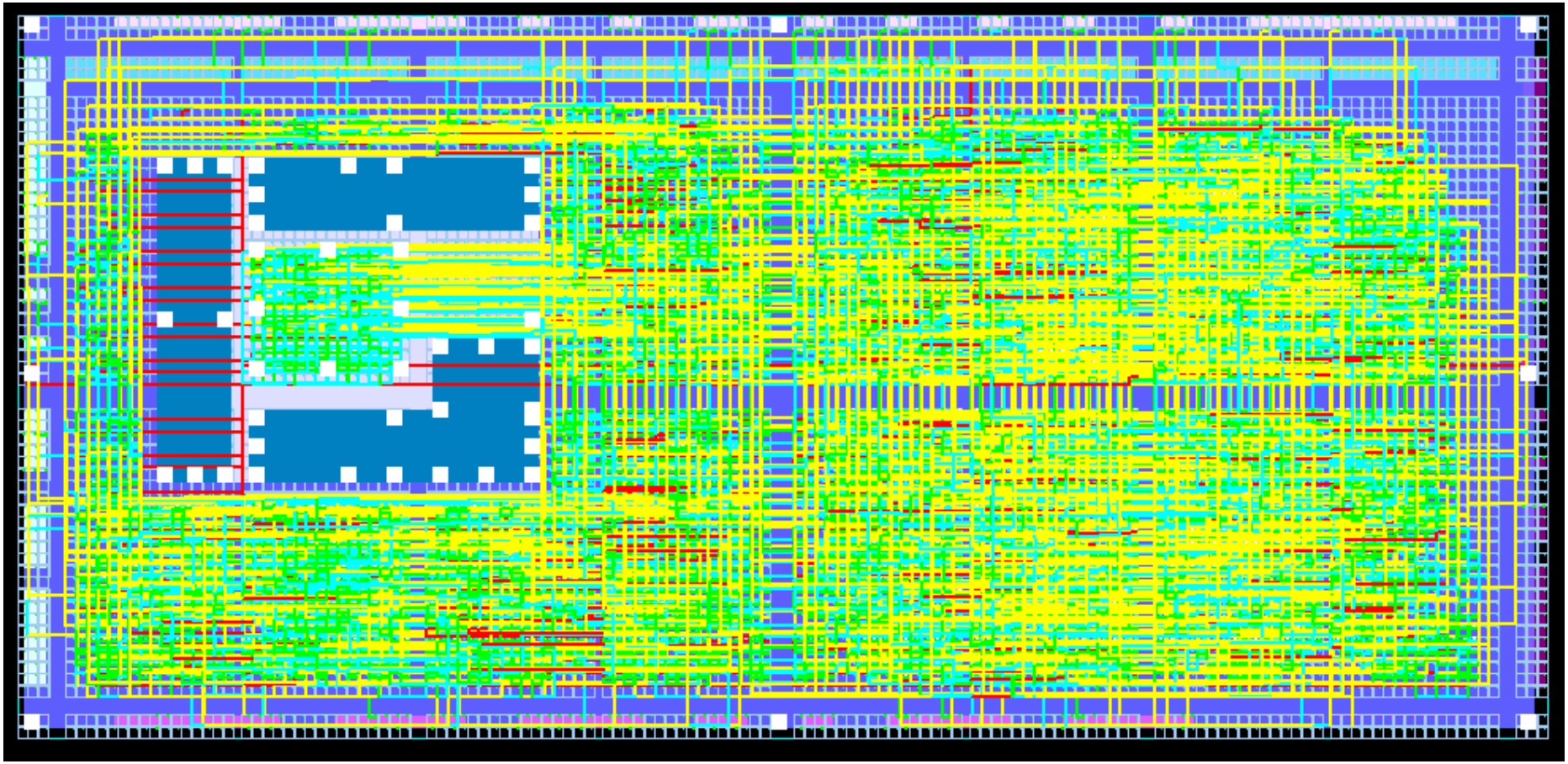
Actel Corporation © 2009. May be published with permission by MAPLD 2009

Example 1: An Empty Routing Region



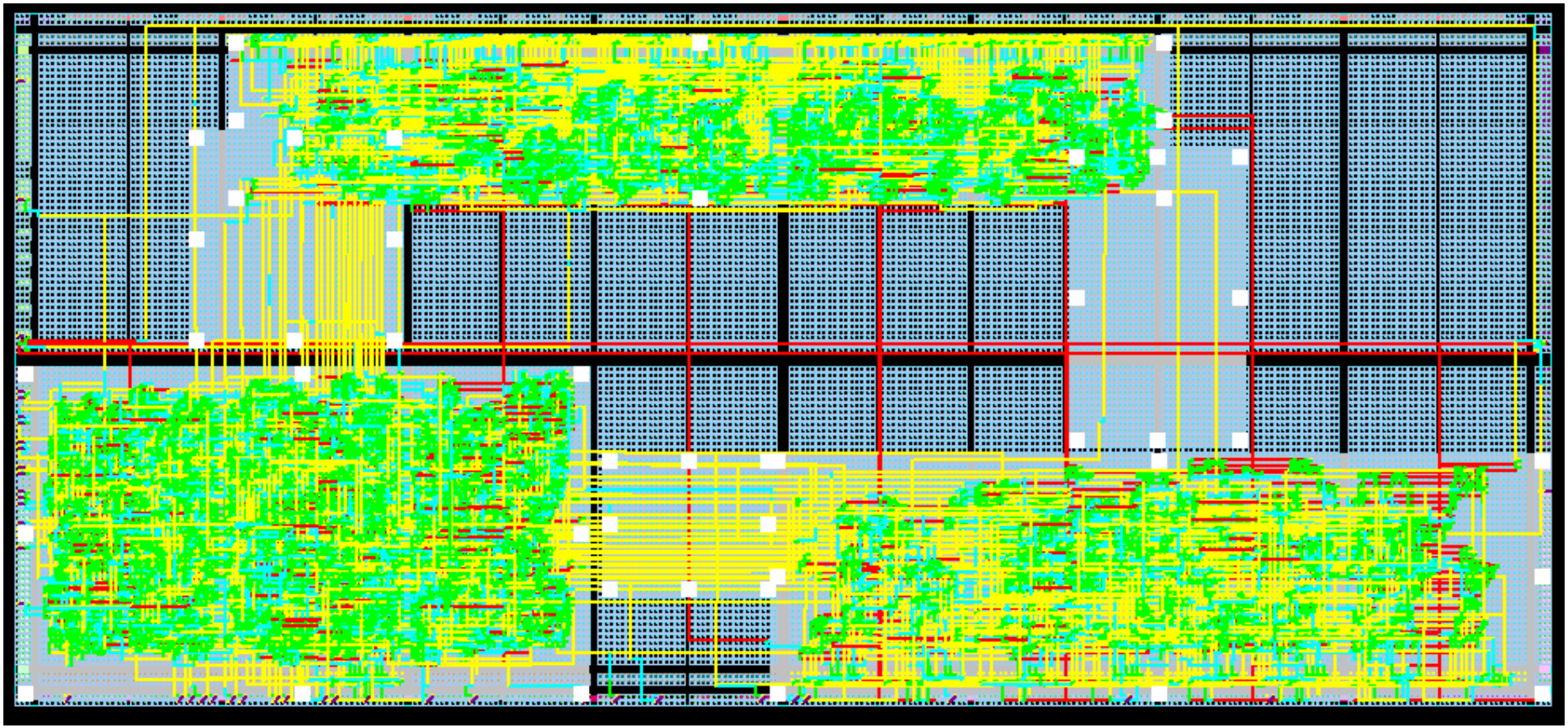
Actel Corporation © 2009. May be published with permission by MAPLD 2009

Example 2: Secure Fence and Connections



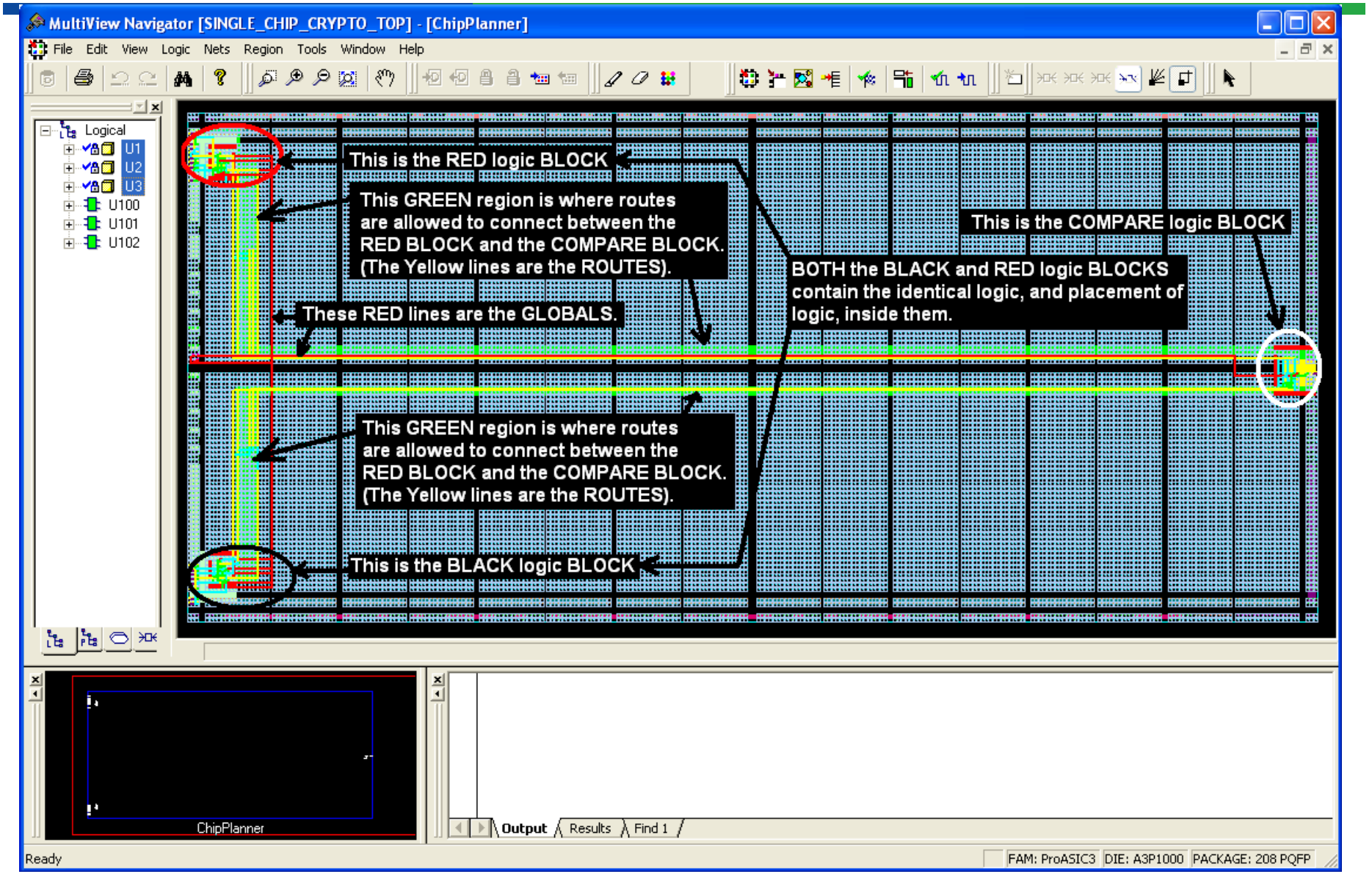
Actel Corporation © 2009. May be published with permission by MAPLD 2009

Example 3: Isolation of Red and Black Datapaths



Actel Corporation © 2009. May be published with permission by MAPLD 2009

Example 4: Isolation of Red and Black Datapaths



Actel POWER MATTERS

Actel Corporation © 2009. May be published with permission by MAPLD 2009