Efinix FPGA Security Features

Maximilian Werner, EMEA FAE

V: 1.0

Agenda

- Efinix Introduction
- FPGA Families
- Security features
- IP
- Eval Boards
- Software

Efinix Global

Foundet in 2012
Worldwide Presence with 170+ Employees
EMEA HQ: Munich/Unterschleißheim
AE Office: Manchester

Executive Leadership

Ming Ng
COO

Sammy Cheung
Chairman,
President and CEO

Tony Ngai
CTO and
Sr. VP Engineering

Jeff Suto
General Counsel

Harald Werner
Managing Director
(EMEA)

Ikuo Nakanishi
VP Sales and BDM
(JAPI)

Greg Barrett
CFO, Sr. VP Finance

Jay Schleicher
Sr. VP Software
Engineering

Mark Oliver
VP, Marketing

Distribution Network Europe :

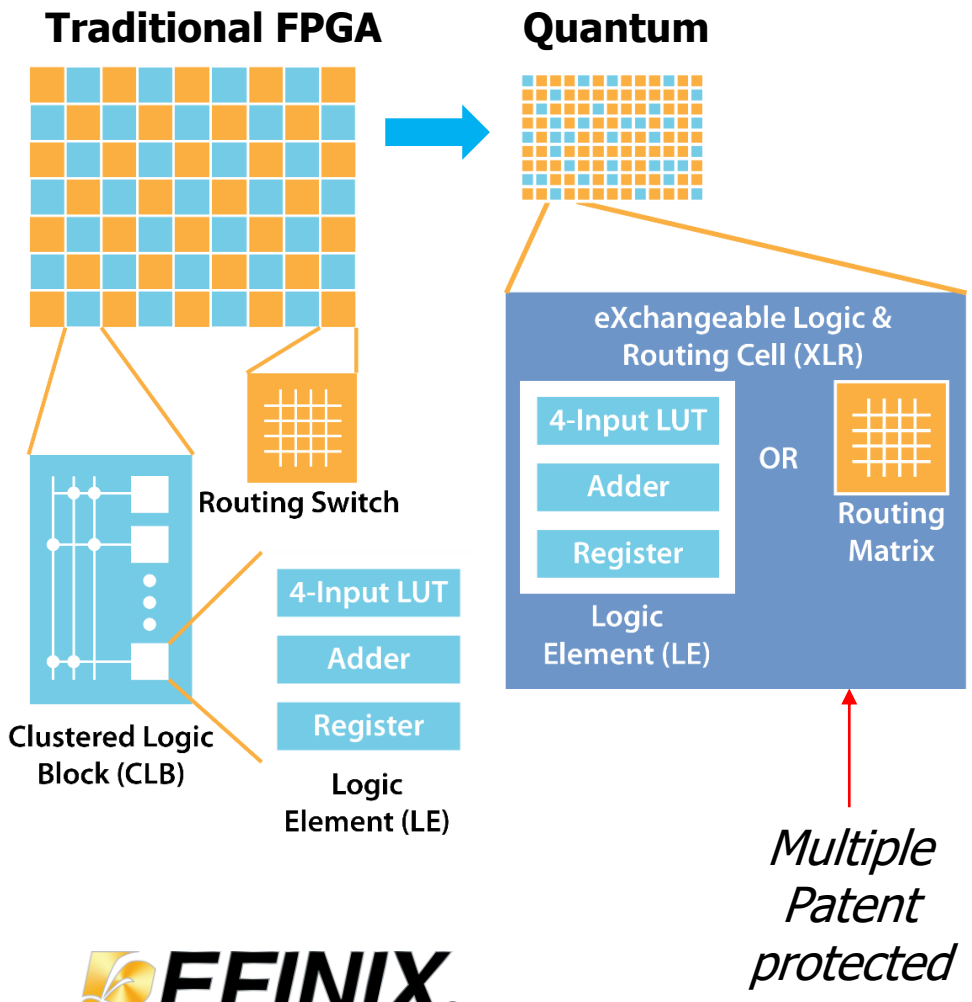
DigiKey

RUTRONIK
ELECTRONICS WORLDWIDE

TRS-STAR

KUANTEK
ultimate technology
Turkey

Quantum FPGA Technology



Advantages over traditional FPGAs

- **4X Better Power-Performance-Area (PPA)**
- 7 layers of metal vs.12+ layers in traditional FPGA
- Single architecture scalable to 1 million+ logic elements (LE)
- Silicon process agnostic

Architectural Highlights

- Flexible, fine grained
- Software configurable logic/routing
- High performance adaptive interconnect
- Hybrid place and route algorithm
- Standard silicon recipe

EFINIX®

Trion® FPGAs (Gen 1)

- Focus on **Consumer, Industrial Markets, Communications Markets** with varied applications
  - Traditional FPGA markets
  - Emerging edge AI computing markets
  - Applications: mobile, IoT, LED, automation, robotics, video, audio, sensing integration, display, computer vision, etc.
- 4K to 120K LEs on 40LL SMIC silicon process
- Traditional SRAM-based FPGA
  - Masked option for T20/T13/T8/T4 – boots internally vs. using a configuration device
- Optimized for low power
- Hard core blocks for DDR memory controllers and D-PHY v1.1 and CSI-2 v1.3
  - Up to 3 independent RX/TX interfaces, 4 lanes x 1.5 Gbps

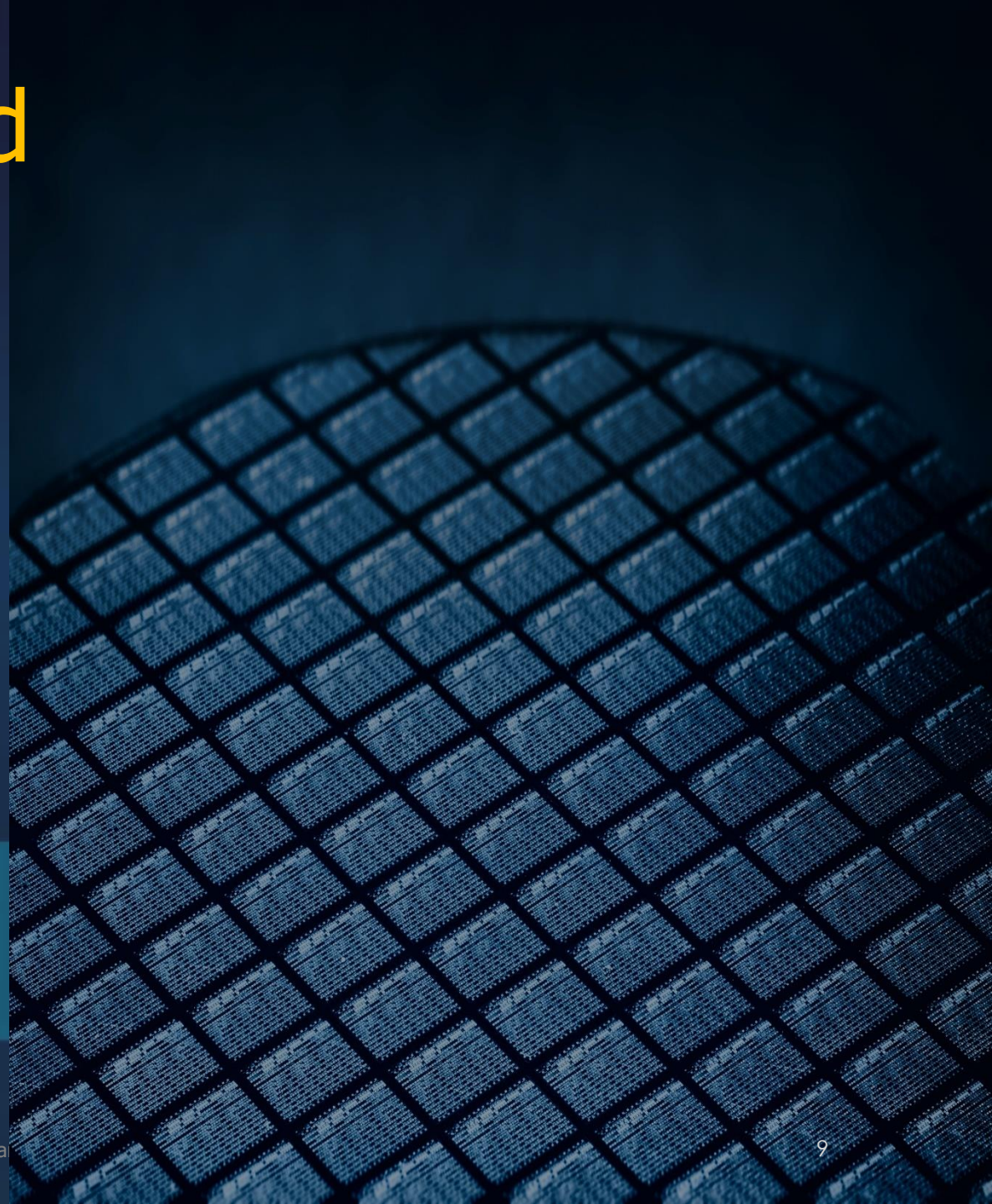
Trion Family Table

Feature	T4	T8	T13	T20	T35	T55	T85	T120
Logic Elements (LEs)	3,888	7,384	12,828	19,728	31,680	54,195	84,096	112,128
Mask Programmable Memory	√	√	√	√	—	—	—	—
Embedded RAM bits (kb)	77	77	727	1,044	1,475	2,765	4,055	5,407
18 x 18 Multipliers	4	4	24	36	120	150	240	320
49-ball FBGA (0.4 mm, 3x3 mm)	4	33 1 -						
80-ball WLCSP (0.4, 4.5x3.6mm)				33 5 - 1, 1 -				
81-ball FBGA (0.5, 5x5 mm)	55 1	55 1 -						
100-pin LQFP (0.5, 14x14 mm)			65 4 4,4 - -	65 4 4,4 - -				
144-pin LQFP (0.5, 20x20 mm)		97 5 6, 6		97 5 6, 6 - -				
169-ball FBGA (0.65, 9x9 mm)			73 5 8,12 2, 2 -	73 5 8,12 2,2 -				
256-ball FBGA (0.8, 13x13 mm)			195 5 13,13 - -	195 5 13,13 - -				
324-ball FBGA (0.65, 12x12 mm)				130 7 20,26 2,2 x8,x16	130 7 20,26 2, 2 x8,x16	130 7 20,26 2,2 x8,x16	130 7 20, 26 2,2 x8,x16	130 7 20, 26 2,2 x8,x16
400-ball FBGA (0.8 16x16 mm)				230 7 20,26 - x8,x16	230 7 20,26 - x8,x16			
484-ball FBGA (0.8, 18x18 mm)						256 8 40,40 - x16,x32	256 8 40,40 - x16,x32	256 8 40,40 - x16,x32
576-ball FBGA (0.65, 16x16 mm)						278 8 52,52 3,3 x16,x32	278 8 52,52 3,3 x16,x32	278 8 52,52 3,3 x16,x32

GPIO	PLLs	LVDS Pairs (TX, RX)	MIPI 4-Lane D-PHY with CSI-2 Controller (TX, RX)	DDR3, LPDDR3, LPDDR2 (800 Mbps)

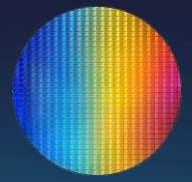
Titanium Under the Hood

- TSMC 16nm Process
  - High Performance for the Most Demanding Applications
  - High Density and Low Power Consumption
- 2nd Generation Quantum Fabric
  - Optimized for Compute & Artificial Intelligence
- High Speed Interfaces
  - Designed for Video and Quantum Acceleration

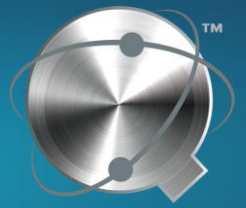


EFINIX®

High-Performance Titanium

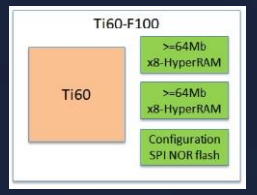


TSMC 16 nm Process



QUANTUM
Quantum Compute Accelerated

Innovative Package Options



System in Package

			Ti35	Ti60	Ti90	Ti120	Ti180	Ti240	Ti375	Ti550	Ti750	Ti1000
LE (k)			36	62	92	123	176	237	370	533	727	969
10K RAM (Mb)			1.53	2.62	7.34	9.80	13.11	19.37	27.53	39.65	54.07	72.09
DSP			93	160	359	478	640	946	1344	1936	2640	3520
PLLs			4	4	10	10	10	10	10	10	10	10
MIPI DPHY 1.5G, support CSI-2/DSI			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MIPI DPHY x4 2.5Gbps Hard IP			-	-	X4	X4	X4	X3	X3	X3	X3	X3
LPDDR4/X (> 3Gbps)			-	-	X32	X32	X32	2 X32	2 X32	2x72	2x72	2x72
RISC-V hardwired								x	x	x	x	x
16 Gbps Serdes			-	-	X8	X8	X8	X16	X16	X16	X16	X16
25.8 Gbps Serdes			-	-	-	-	-	-	-	X8	X8	X8
PCIE Gen4 (16G) hard controller			-	-	1x PCIE Gen4x4	1x PCIE Gen4x4	1x PCIE Gen4x4	2x PCIE Gen4x4	2x PCIE Gen4x4	2x PCIE Gen4x8	2x PCIE Gen4x8	2x PCIE Gen4x8
Packages (HSIO/HVIO/LPDDR4/MIPI /SERDES)												
W64	0.4mm	3.5x3.4mm	-	34/0			-	-	-		-	-
F100 (SIP)	0.5mm	5.5x5.5mm	61/0	61/0			-	-	-		-	-
F225	0.65mm	10x10mm	140/23	140/23				-	-		-	-
J361	0.65mm	13x13mm	-	-	110/20/16/2/0	110/20/16/2/0	110/20/16/2/0	-	-		-	-
G400	0.8mm	16x16mm			200/74/0/0/0	200/74/0/0/0	200/74/0/0/0					
L484	0.8mm	18x18mm	-	-	116/27/0/4/0	116/27/0/4/0	116/27/0/4/0	-	-		-	-
J484	0.8mm	18x18mm	-	-	116/27/32/4/0	116/27/32/4/0	116/27/32/4/0	-	-		-	-
G529	0.8mm	19x19mm	-	-	210/48/32/0/0	210/48/32/0/0	210/48/32/0/0	-	-			
N529	0.8mm	19x19mm	-	-	-	-	-	100/51/32/0/0	100/51/32/0/0			
N529**	0.8mm	19x19mm	-	-	-	-	-	100/51/32/0/8	100/51/32/0/8			
N676**	0.65mm	18x18mm	-	-	-	-	-	130/60/32/2/12	130/60/32/2/12			
N900**	0.8mm	25x25mm	-	-	-	-	-	172/87/32x2/1/16	172/87/32x2/1/16			
P1156**	1.0mm	35x35mm	-	-	-	-	-	256/118/32x2/3/16	256/118/32x2/3/16			

** subject to change

F100 (SIP) :16 MbFlash + 256Mbit HyperRAM

Security features

Trion

- You can use MPM method to deploy your bitstream directly to the T4 up to T20 Silicon, where you can select that readout is not possible.
- Only applicable for high volume application as we have to do a new mask, which includes as well NRE cost.
- Not more security features available in Trion.

Titanium Security

Secure Configuration with Trusted Image

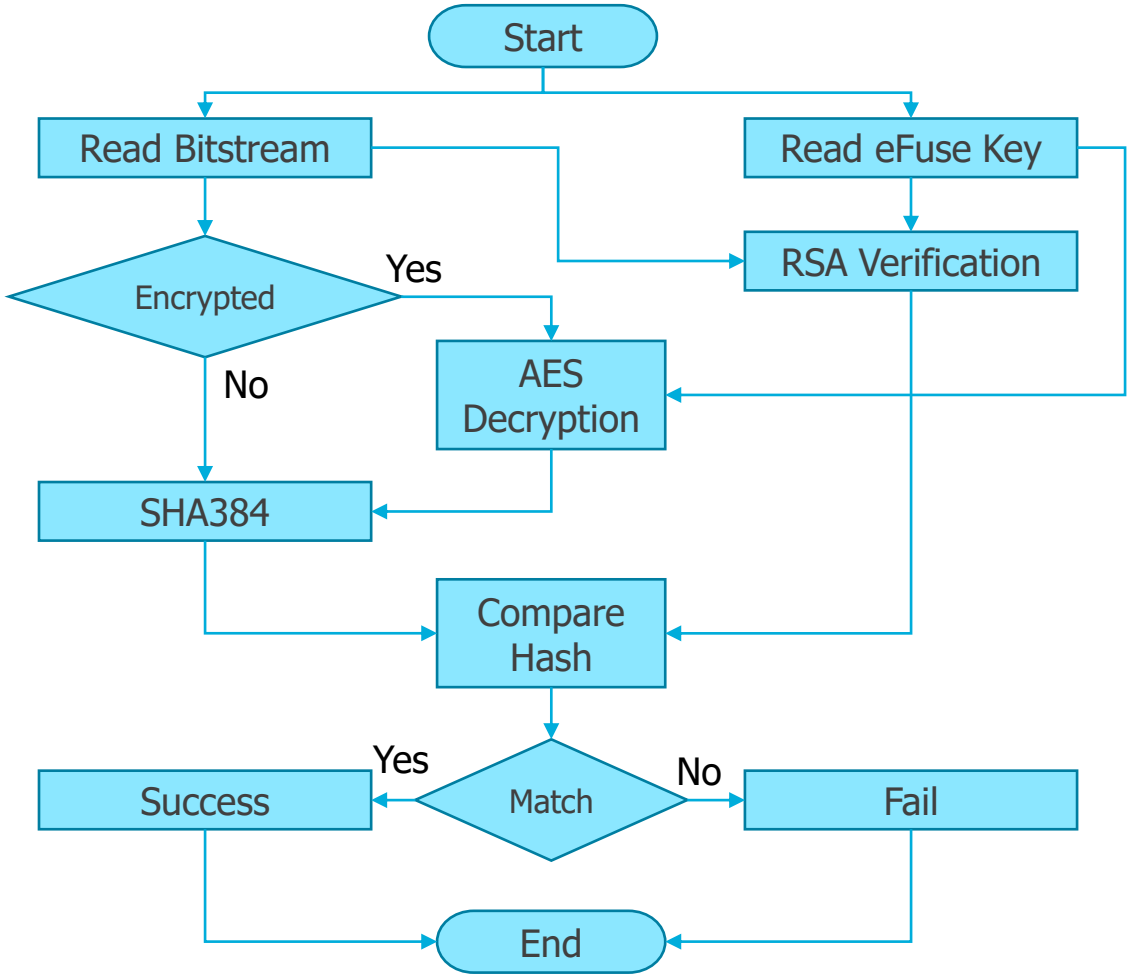
- Authentication
  - Public Key Encryption of Signed Digital Bitstream
  - Only Trusted Images Are Loaded Into Device

Intellectual Property Protection

- Encryption
  - Configuration Bitstreams Are Encrypted for Copy Protection

Secure Configuration Flow

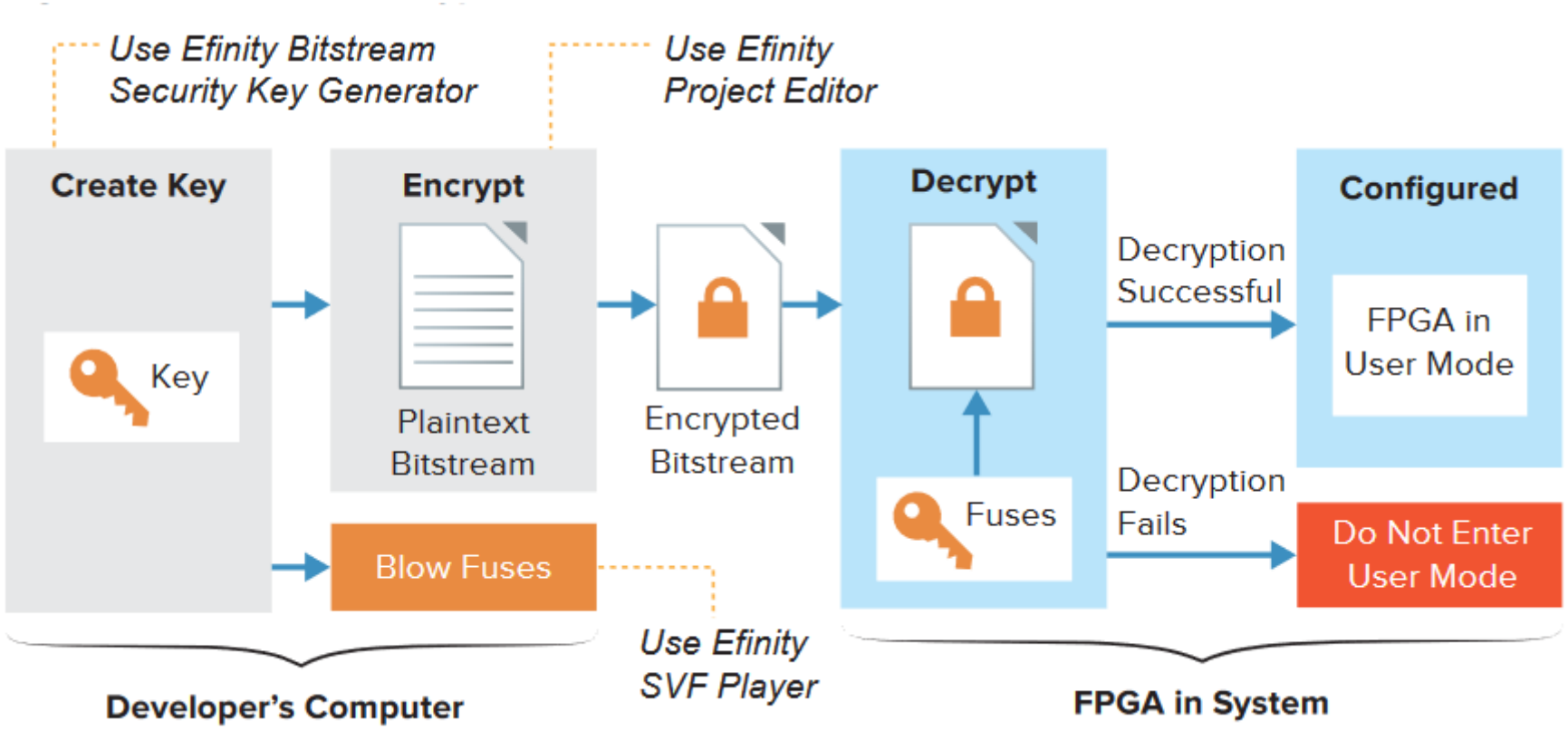
- Public Key RSA4096 Authentication
  - Private Keys Remain With OEM
  - Only Know Good Bitstreams Used
- Private Key AES256 Encryption
  - Lightning-Fast Boot
  - Encryption of Valuable IP
- Totally Secure Root of Trust
  - No Users Access to Security Engine
- eFuse Key Storage
  - OEMs Can Program Their Own Keys During Manufacture
  - Keys Remain Secure Inside Device



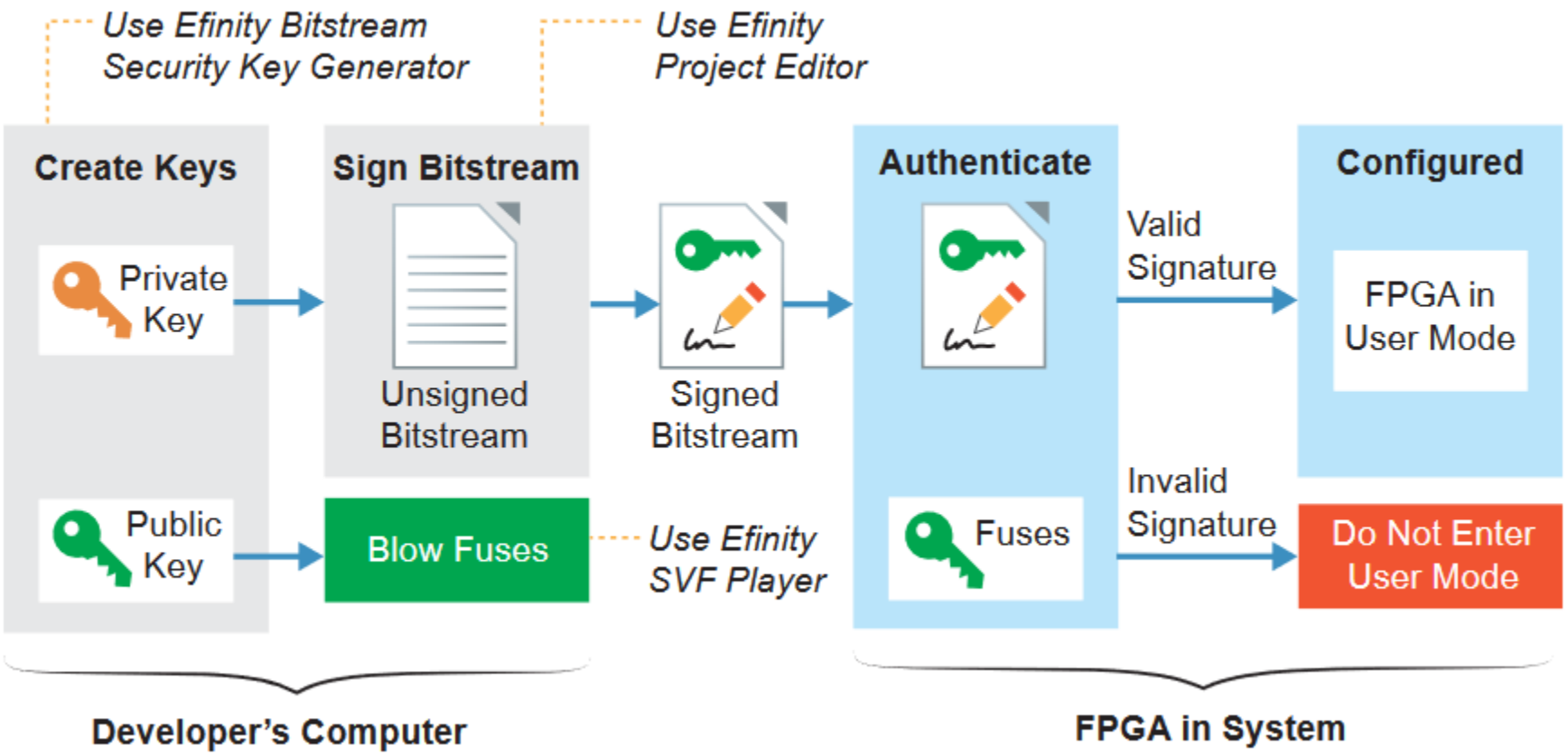
Efinity Tools used for Securing Bitstream

Tool	Used for
 Bitstream Security Key Generator	Create or specify an AES-256 key. Create or specify an RSA-4096 private key. Specify whether to disable JTAG.
 SVF Player	Program the fuses in the Titanium FPGA with the AES-256 key and/or RSA certificate data. After you blow the fuses with an RSA key, the FPGA only accepts a bistream signed with the correct private key. After you blow fuses with an AES-256 key, the FPGA only accepts a plaintext bitstream or a bitstream signed with the correct key. Program the JTAG fuse to disable JTAG function. After you blow the JTAG fuse, you cannot use any JTAG command except `IDCODE`, `DEVICE_STATUS`, and `BYPASS`.
 Project Editor	Turn on bitstream encryption and/or authentication, and specify the **.bin** file created by the Bitstream Security Key Generator. Turn on bitstream authentication and specify the private key (**.pem**) file to sign the bitstream.

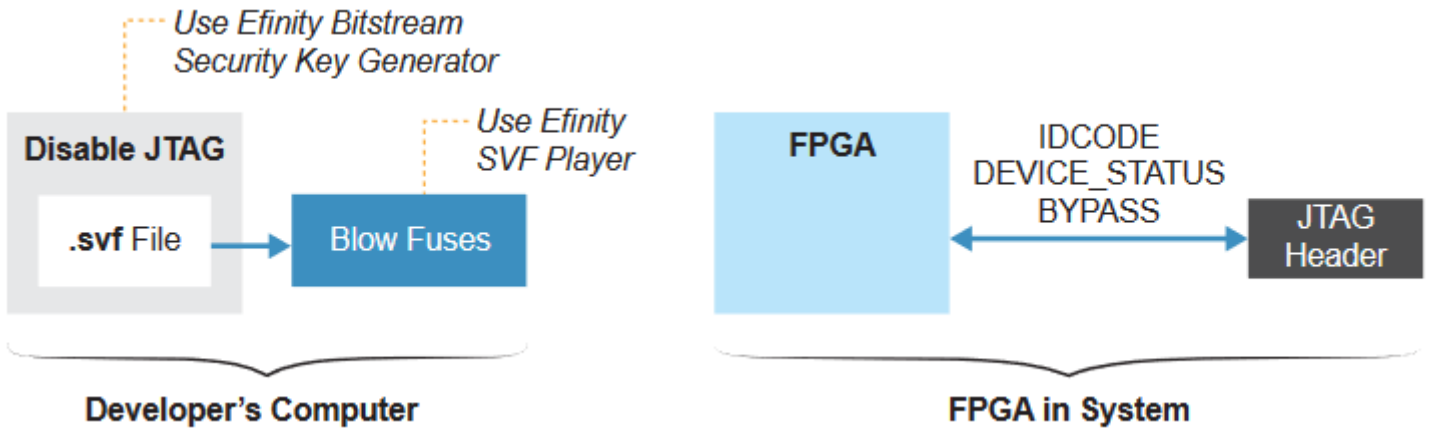
Bitstream Encryption



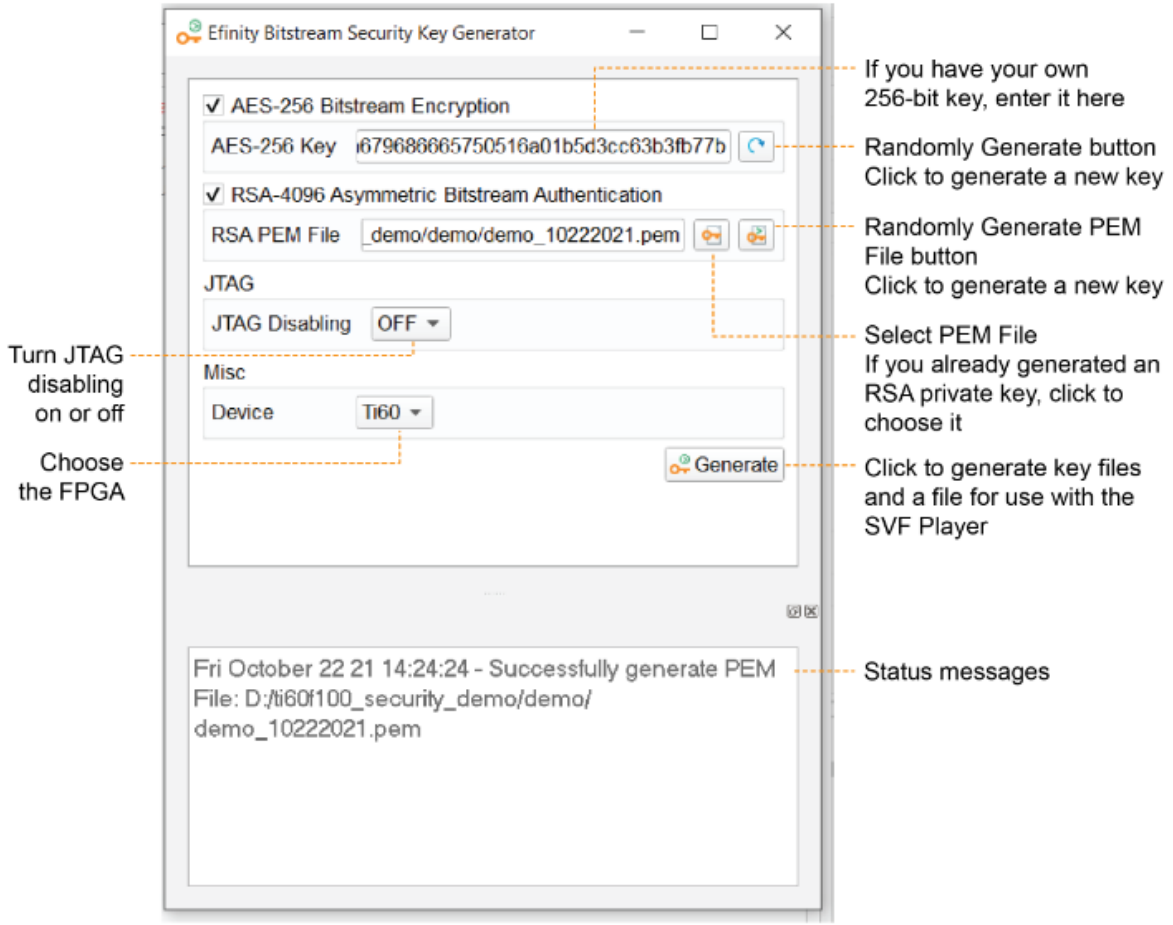
Bitstream Authentication



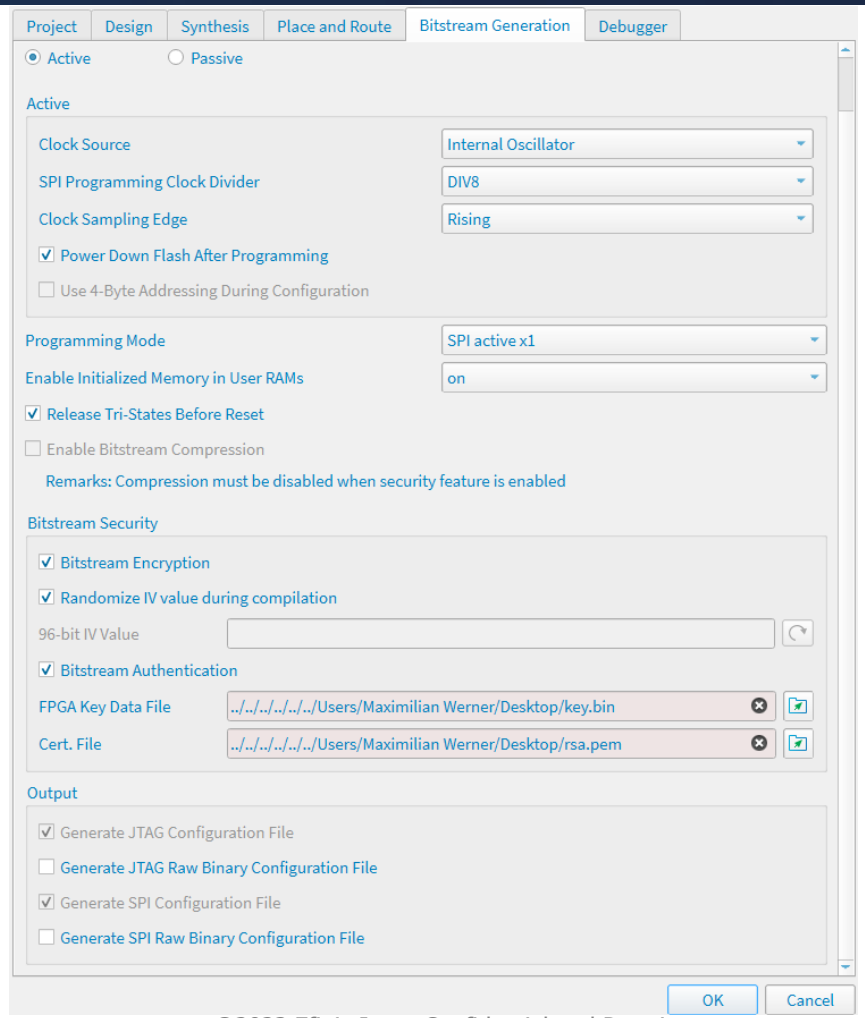
Disabling JTAG



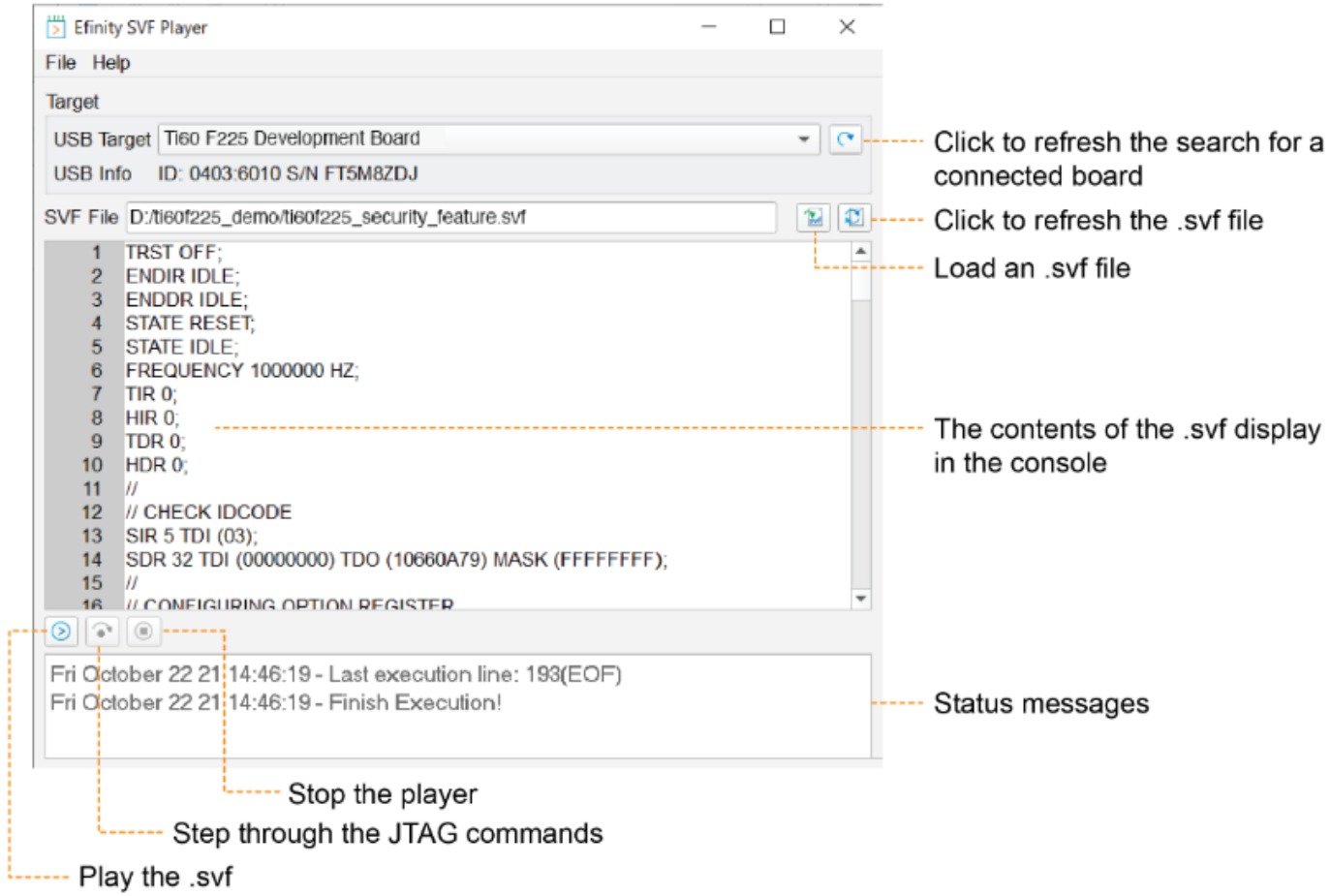
Security Key Generator



Project Editor



Efinity SVF Player



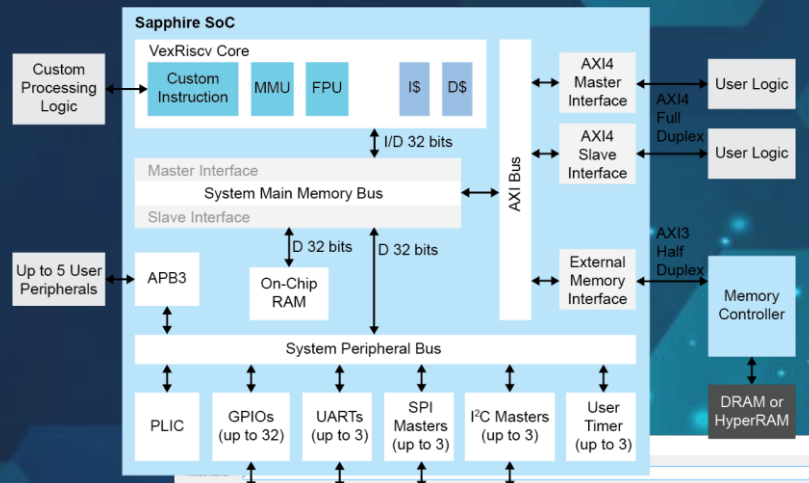
Notes

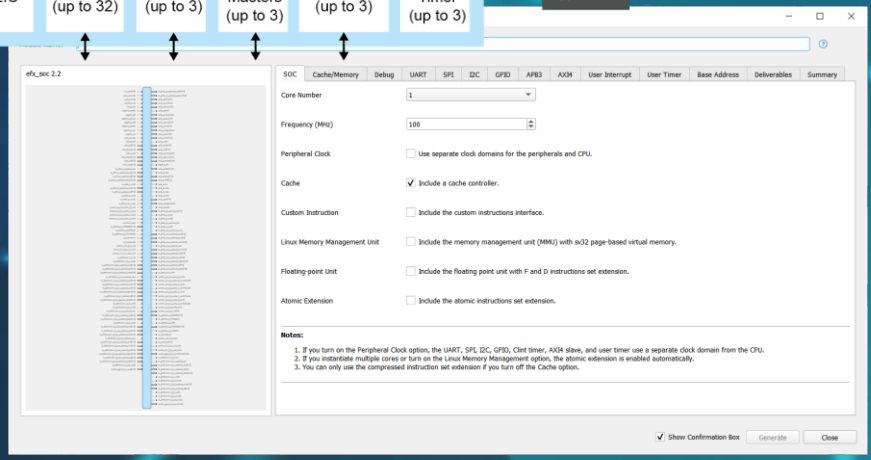
- With AES encryption enabled it is possible to use unencrypted bitstreams
- With RSA authentication only signed bitstreams are accepted
- Detailed description and examples can be found in Efinity UserGuide

SoftIP/ RISC-V® SOC offering

RISC-V Cores Implementation

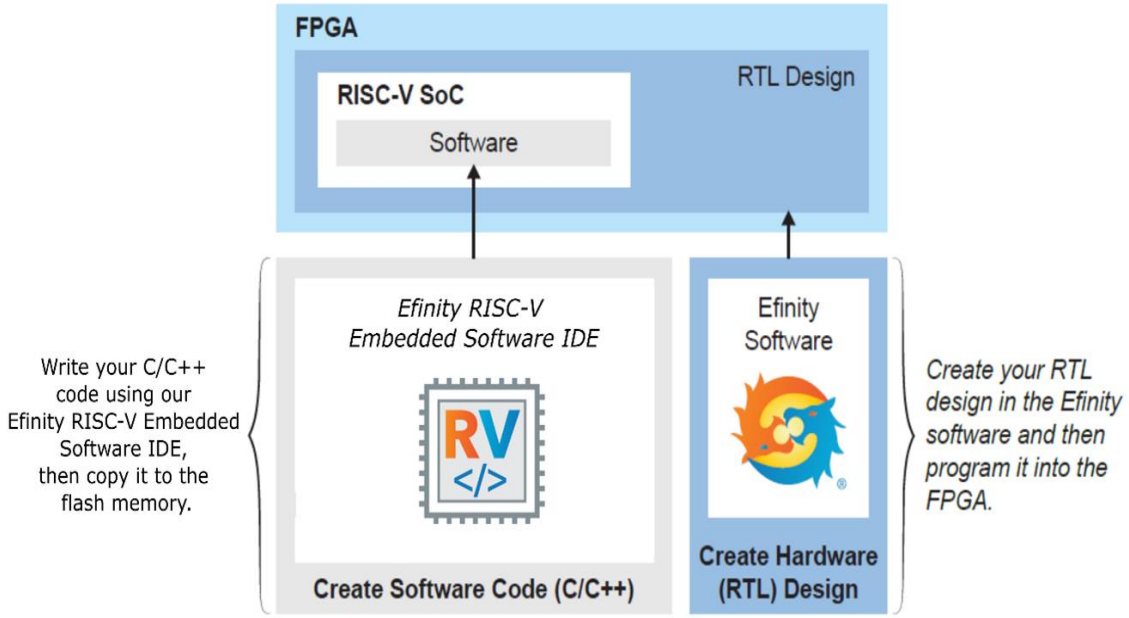
- 65+ available now with commercial and open-source licenses
- Efinix solution based on VexRiscv by Charles Papon
  - 32-bit single core CPU
  - 6 pipeline stages
  - ISA RISCV32I with extensions M, A, F, D
    - Includes a floating point unit
    - Includes an optional Linux memory management unit
    - Includes a custom instruction interface with 1,024 IDs to perform different functions
    - Supports optional RISC-V extensions such as atomic and compressed





Required Software and Tools

- Efinity ® software
- Pre-compiled, open-source SDK
- Eclipse IDE for managing projects and software with Ashling GUI
- RISC-V GCC compiler and GDB debugger
- OpenOCD debugger for debugging applications
- Windows build tools (Windows)
- Available from our web page
  - https://www.efinixinc.com/products-riscv.html



Development Kits

Development Kits

Titanium Ti60 F225 Development Board

Titanium Ti180 J484 Development Board

Trion T120 BGA576 Development Kit

Featuring T120 FPGA with hardened MIPI CSI-2 and DDR DRAM

Trion T120 BGA324 Development Kit

Featuring T120 FPGA with hardened MIPI CSI-2 and DDR DRAM

Trion T20 MIPI Development Kit

Featuring T20 FPGA with hardened MIPI CSI-2 and D-PHY

Trion T20 BGA256 Development Kit

Featuring the T20 BGA256 FPGA

Trion T8 BGA81 Development Kit

Featuring the T8 BGA81 FPGA

Xyloni Development Kit

Thumb-sized USB board for hobbyists and makers

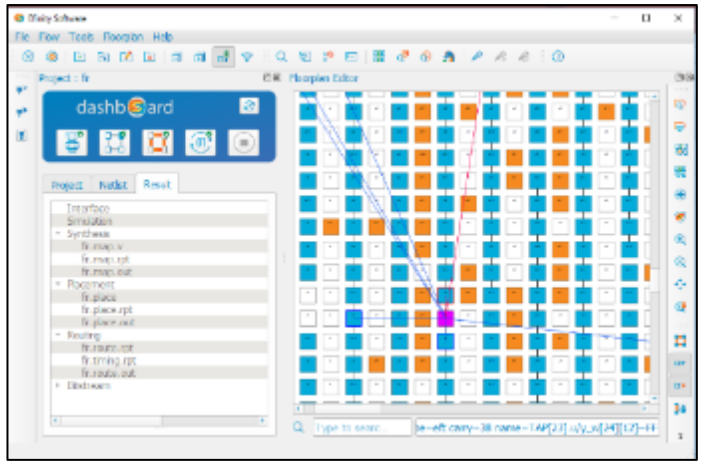
Software Efinity

Efinity® Integrated Development Suite

- Standard RTL-to-bitstream FPGA development tool (free of charge)
- Core and interface concept enables system integration

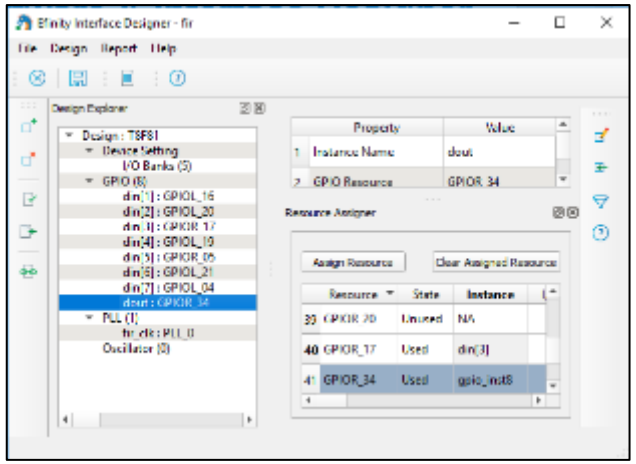
Core Designer

FPGA Core Fabric
(Synthesis, Place and Route)



Interface Designer

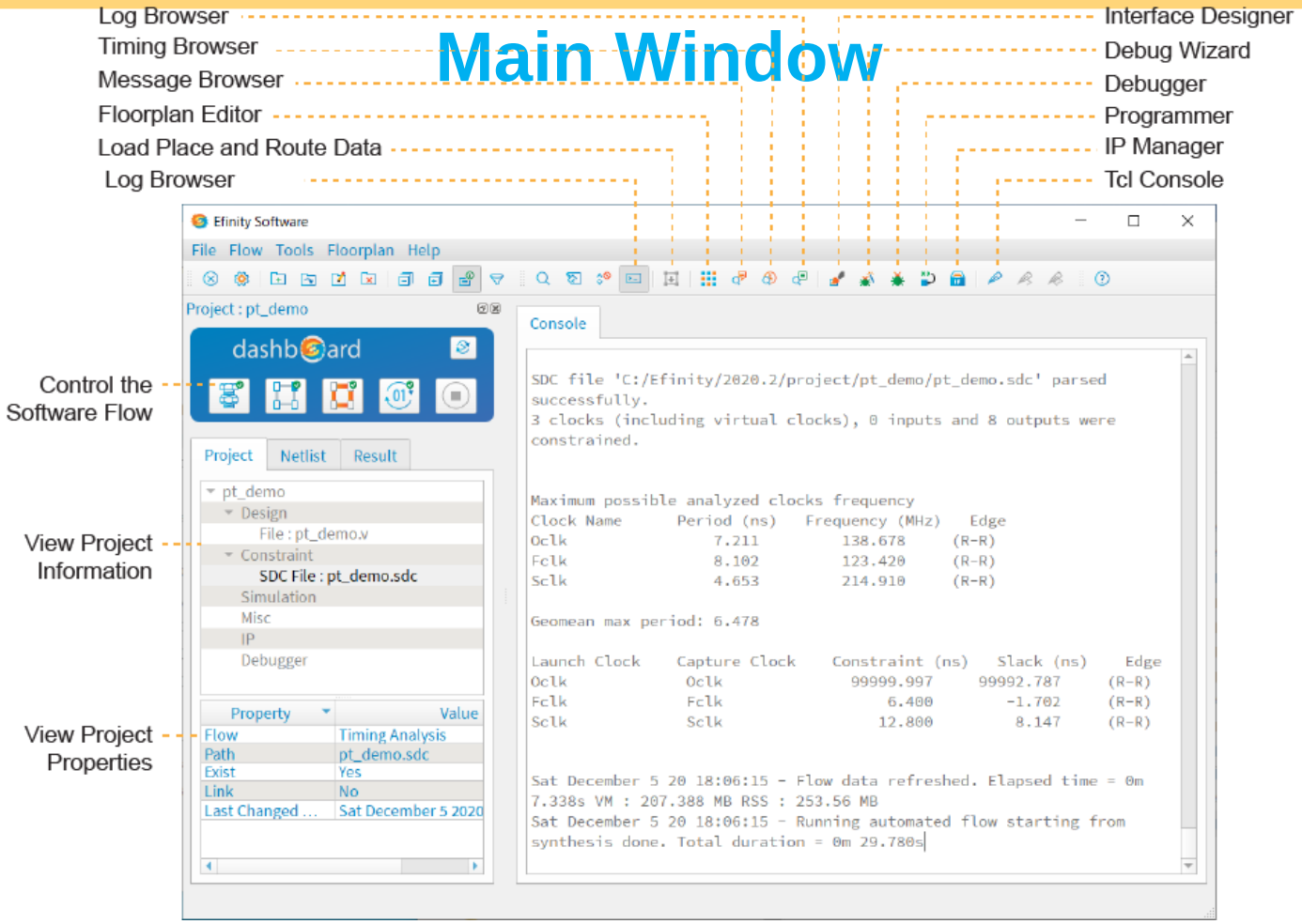
Subsystems
(I/O, DDR, MIPI, etc.)



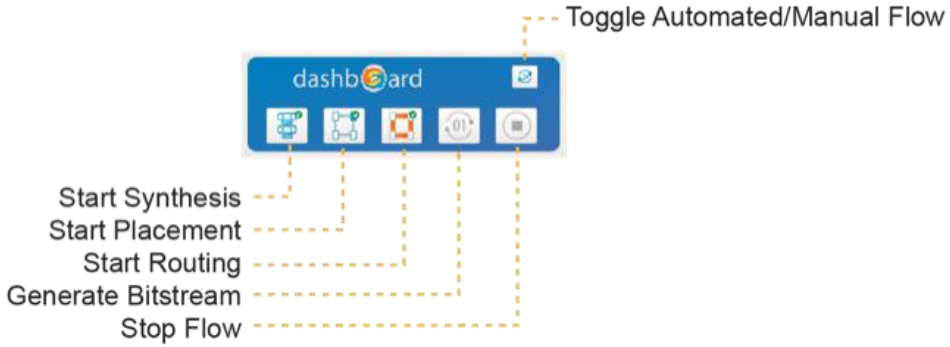
Design Entry → Synthesis → Place & Route → Timing Analysis → Debugging → Bitstream Generation

Efinity® Integrated Development Suite

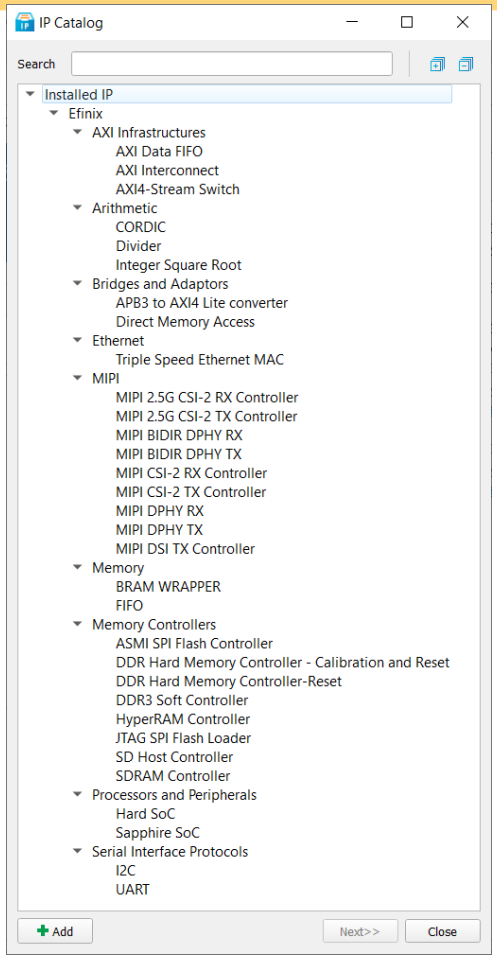
Main Window

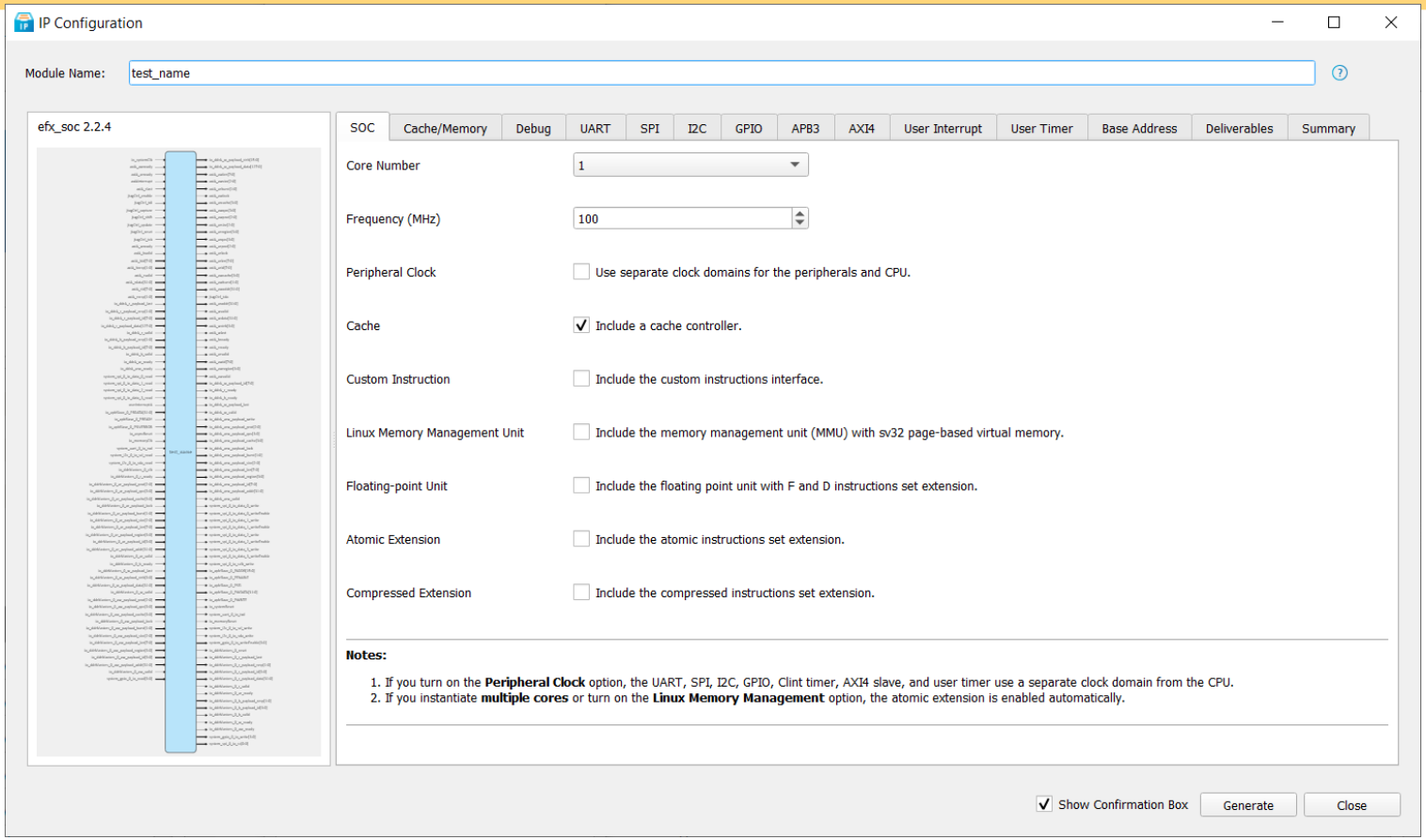


Dashboard Control



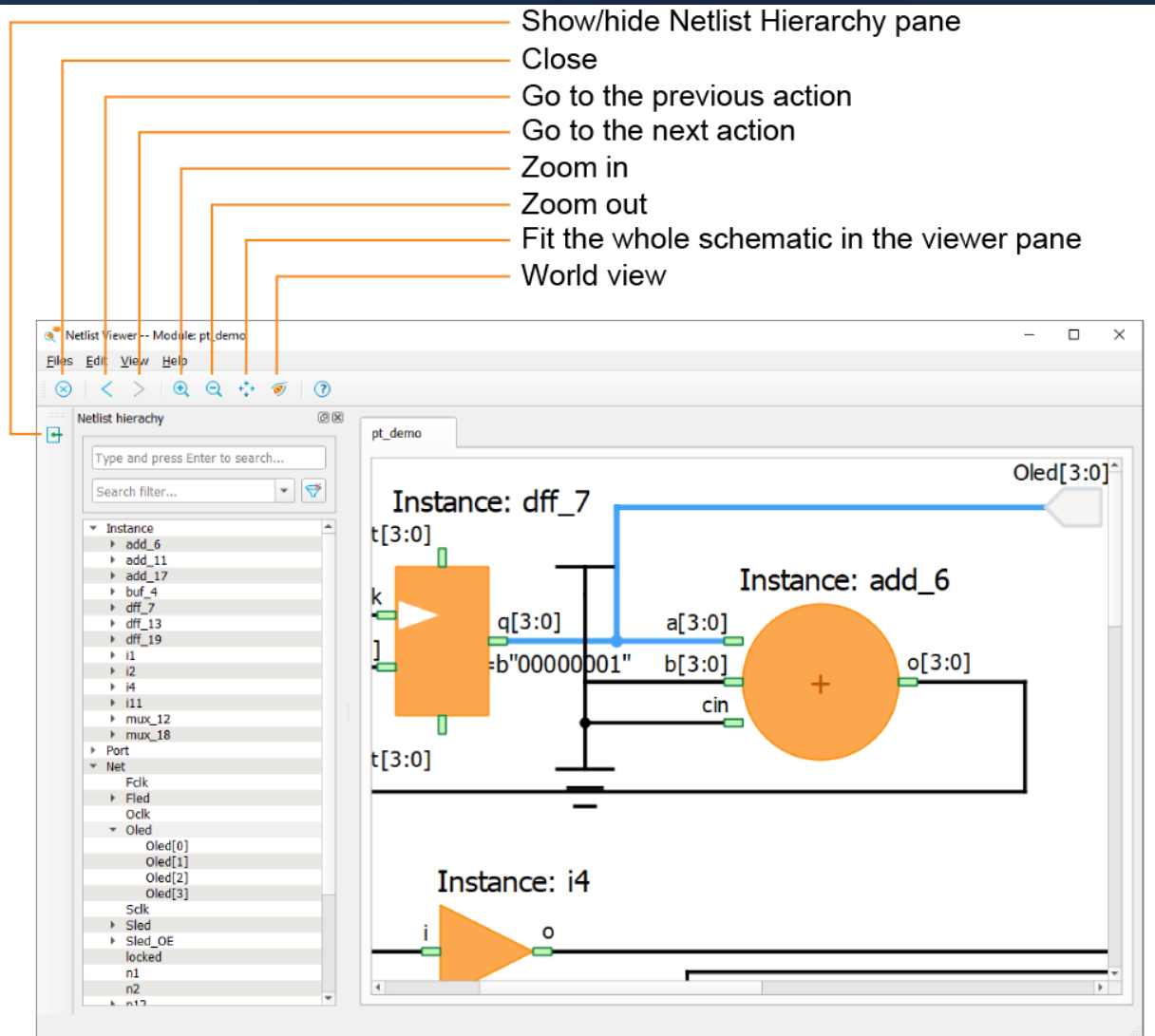
IP Catalog (2023.2)



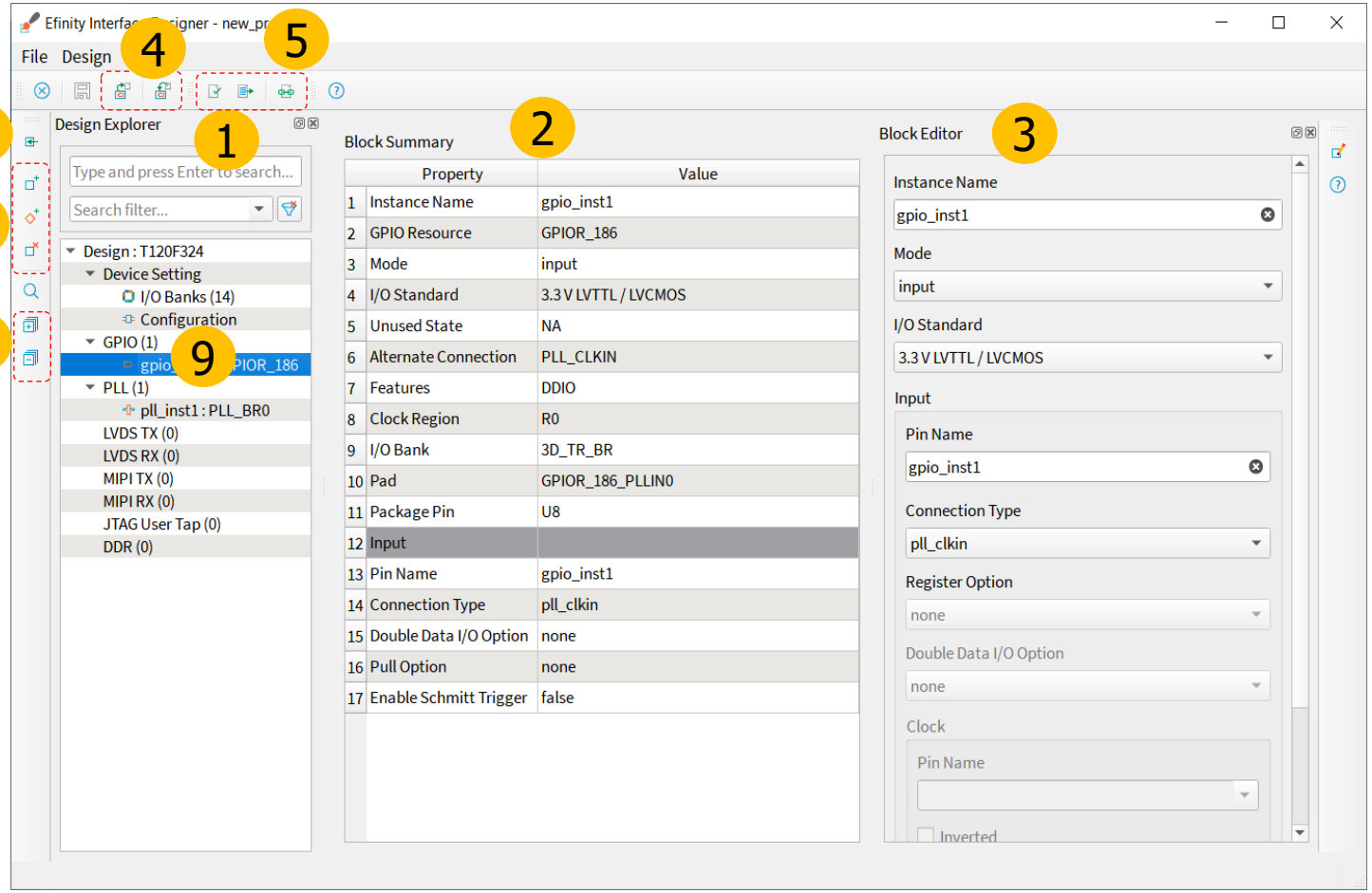


Configure and generate your specific IP Core/Module

RTL/Netlist View (2023.1)



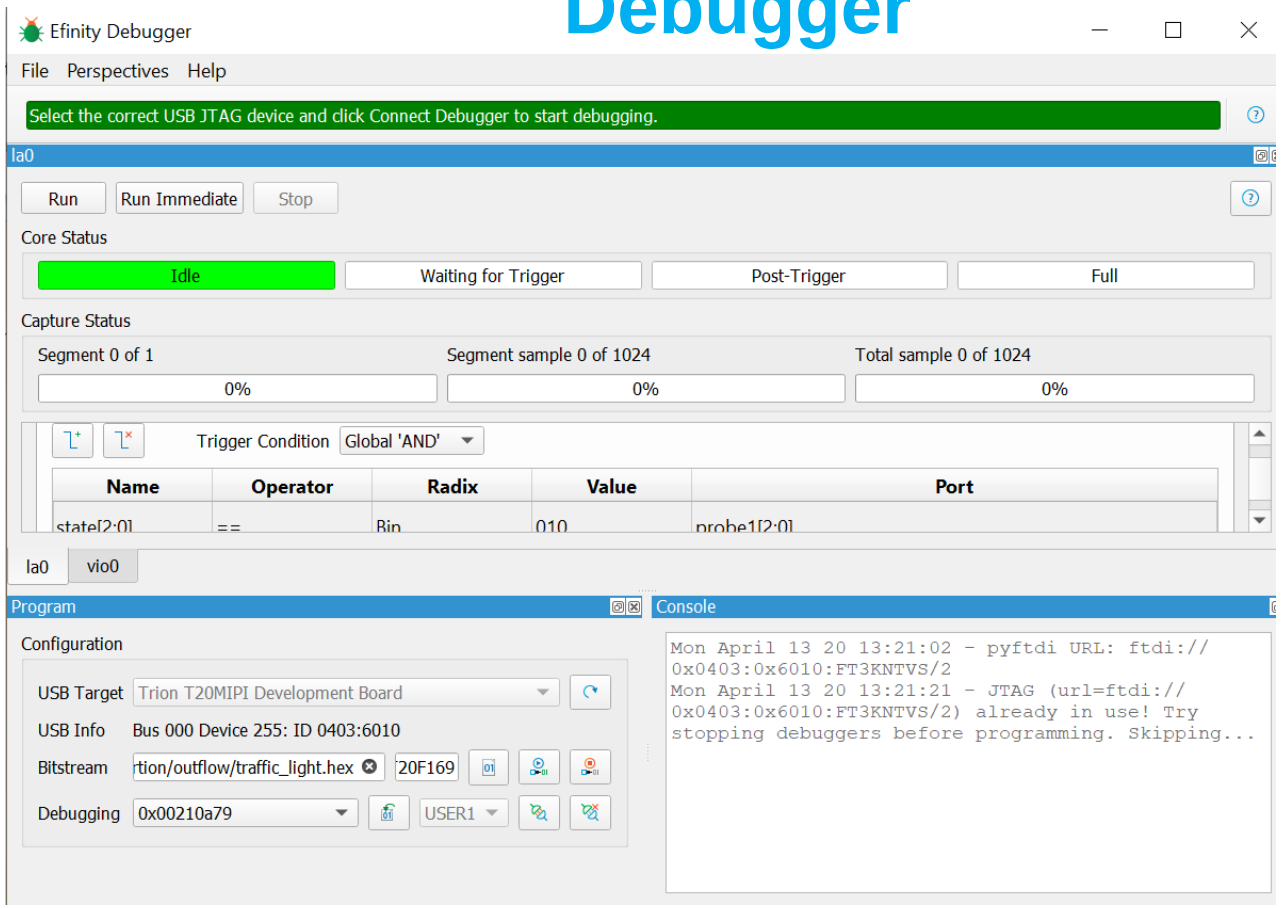
Interface Designer

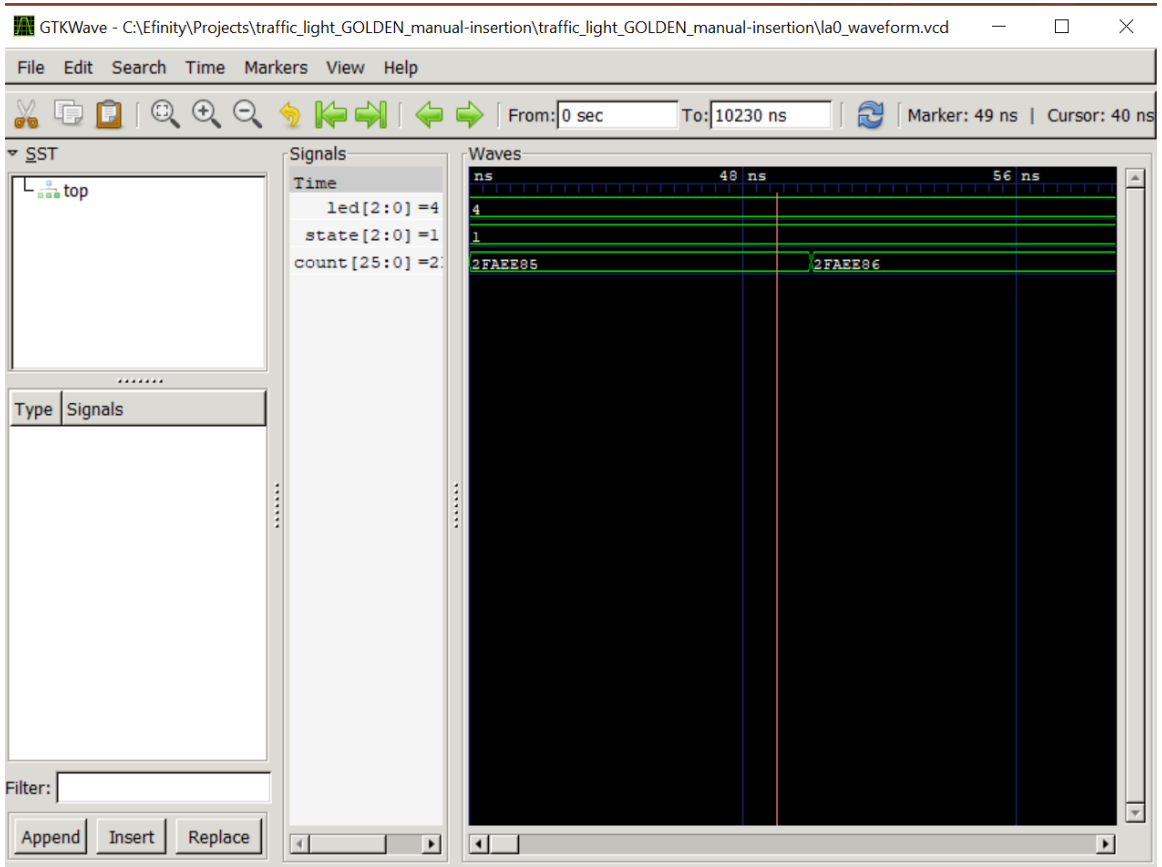


1. The Design Explorer shows the interfaces in your Design
2. Block Summary shows settings for the selected Block
3. Block Editor add or change settings
4. Import/Export GPIO assignments
5. Project Managfement Tools for design check
6. Show/Hide Resource Assigner
7. Block Tools add/delete blocks
8. Expand/Collaps Design Explorer folder
9. Number of used blocks()

Efinity® Integrated Development Suite

Debugger





ISO26262/ ICE61508

The manufacturer may use the mark:

Revision 1.0 August 4, 2023
Surveillance Audit Due
September 1 , 2026

Certificate / Certificat
Zertifikat / 合格証

EFI 2207092 C001

exida hereby confirms that the:

Efinity® IDE and Toolchain v2023.1

Efinix Technology (M) Sdn. Bhd.
Penang - Malaysia

Has been assessed per the relevant requirements of:
IEC 61508:2010 and ISO 26262:2018

and meets requirements providing a level of integrity to:
SIL 4 / ASIL D Qualified

Tool Functions:
The Efinity® IDE and Toolchain suite is an integrated development environment designed for Efinix FPGA development. Using Efinity, customers can develop, compile and test their FPGA design from RTL source code all the way down to bitstream programming on FPGA development boards.

Application Restrictions:
The tools of the Efinity® IDE and Toolchain must be used per the defined use cases, and all requirements specified for the tool users (conditions and assumptions of use) shall be fulfilled, as described in the Functional Safety Manual for each tool.

finity® IDE and
oolchain

Certificate / Certificat / Zertifikat / 合格証

EFI 2207092 C001

SIL 4 / ASIL D Tool Qualification:
The Efinity® IDE and Toolchain have met the requirements for support tools up to Safety Integrity Level (SIL) 4 of IEC 61508-3 (section 7.4.4). The product has also met the requirements for confidence in use of software tools of Automotive Safety Integrity Level (ASIL) D of ISO 26262-8 (Section 11). These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

Tool Confidence Level (TCL)
Several use cases were defined for each Efinity® IDE tool. A software tool evaluation according to ISO 26262-8, clause 11 determined a required tool confidence level of TCL1 for all tools and use cases, without the need for software tool qualification. Individual tools or the complete tool chain can be used in the development of FPGAs with allocated safety requirements up to ASIL D.

Tool users must confirm the validity of the pre-determined TCL1 in their own design environment, and confirm that all tools are used per the defined use cases and that all conditions and assumptions of use (CoU and AoU) are fulfilled, as specified in the tool functional safety manuals. Otherwise, tool users must perform their own detailed software tool evaluation and possibly software tool qualification.

The following documents are a mandatory part of the certification:

exida Assessment Report:
- EFI 22-07-092 R011 V1R1 61508 26262 Tool Assessment Report - Efinix IDE

Efinix Functional Safety Manuals:
- Efinity_IDE Functional Safety Manual v3 or later
- Interface_Designer Functional Safety Manual v2 or later
- IP_Manager Functional Safety Manual v2 or later
- Code_Editor Functional Safety Manual v2 or later
- Synthesis Functional Safety Manual v2 or later
- PnR Functional Safety Manual v2 or later
- Bitgen Functional Safety Manual v2 or later
- Programmer Functional Safety Manual v2 or later
- Timing_Engine Functional Safety Manual v2 or later
- Debugger Functional Safety Manual v2 or later

Efinity Features

- Project management to keep your design files organized
  - Support for Verilog HDL , System Verilog and VHDL languages
  - Graphical views of design hierarchy, result files, and reports
- VHDL LIBRARY support
- Easy to use dashboard to run through the flow (synthesis, placement, routing, bitstream generation) automatically or manually
- IP Manager to configure IP cores
- Support for Python scripting and command line tool flow
- Interface Designer to constrain logic and assign pins to blocks in the device periphery
- Floorplan Editor to browse through your design's logic and routing placement
- Timing Browser and static timing analysis to measure your design's performance
  - Tcl Command Console to perform timing analysis
- Supports simulation flows using the ModelSim, Aldec, NCSim, or free iVerilog simulators
- GUI and command-line Programmer
- Efinity Debugger with Virtual I/O and Logic Analyzer debug cores

System Needs

Product	Model	Memory
Trion	T4, T8, T13, T20, T35	16 GB
	T55, T85, T120	32 GB
Titanium	Ti35, Ti60	16 GB
	Ti90, Ti120, Ti180	32 GB

- Minimum requirements
  - Computer with a 64 bit operating system, dual-core processor, and 16 GB RAM
- Linux environments
  - Operating system: Ubuntu x86-64 v18.04 or later, Red Hat Enterprise x86-64 v7.4 or later
  - Linux X11 windowing system (for Efinity® GUI)
  - Udev device manager for Efinix USB programming cable
  - Open-source Java 64-bit runtime environment; required for configuring the Sapphire RISC-V SoC in the IP Manager; available from: https://developers.redhat.com/products/openjdk/download (OpenJDK 8 or 11) – http://jdk.java.net/16/ (OpenJDK 16)
- Windows environments
  - Windows 10 or later, 64 bit
  - Microsoft Visual C++ 2019 x64 runtime library (or latest version)
  - Open-source Java 64-bit runtime environment; required for configuring the Sapphire RISC-V SoC in the IP Manager; available from: – https://www.java.com/en/download/manual.jsp (Java 8)

Contact Data EMEA

Harald Werner

Efinix GmbH

EMEA Senior Sales Director and General Manager

Phone: +49 171 696 2330

E-Mail: haraldw@efinixinc.com

Joachim Mueller

Efinix GmbH

FAE Manager EMEA

Phone: +49 171 696 2331

E-Mail: joachimm@efinixinc.com

Contact Data EMEA

Maximilian Werner
Efinix GmbH
FAE EMEA
Phone: +49 171 696 2332
E-Mail: maximilianw@efinixinc.com

Fabian Heinrici
Efinix GmbH
RSM EMEA
Phone: +49 171 696 2333
E-Mail: fabianh@efinixinc.com

Web Registration

- For support page access https://efinixinc.com/support/account.php?do=create

Thanks !