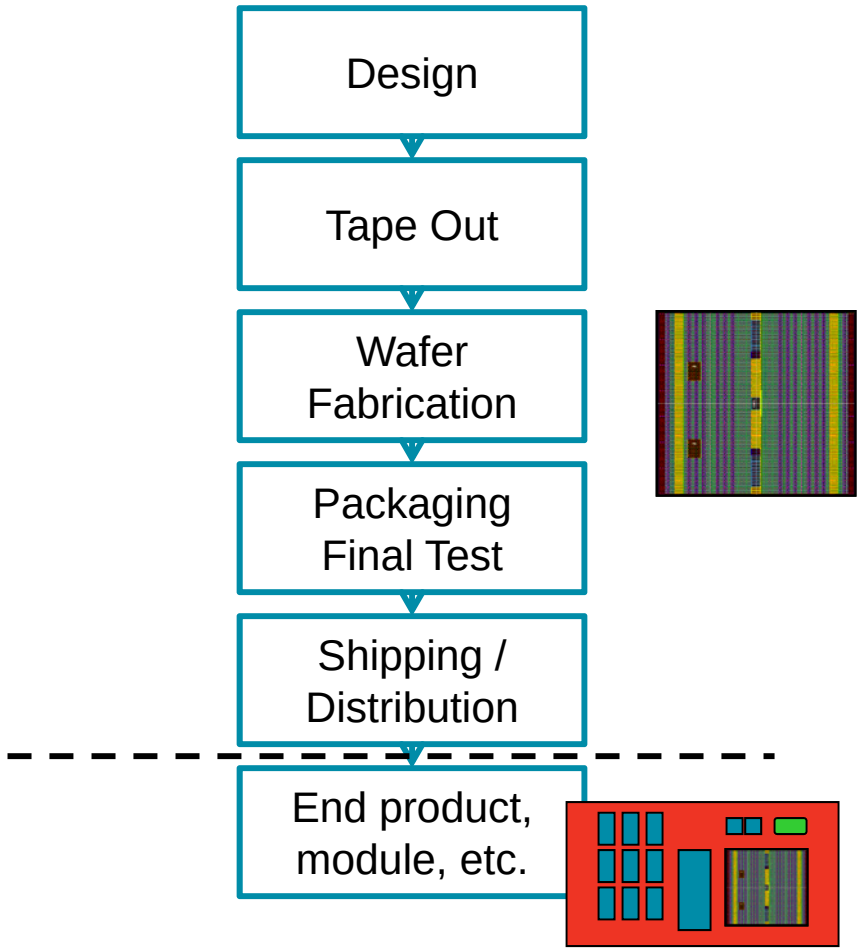
The FPGA Flow

Steve Trimberger
Xilinx
15 January 2013

© Copyright 2013 Xilinx

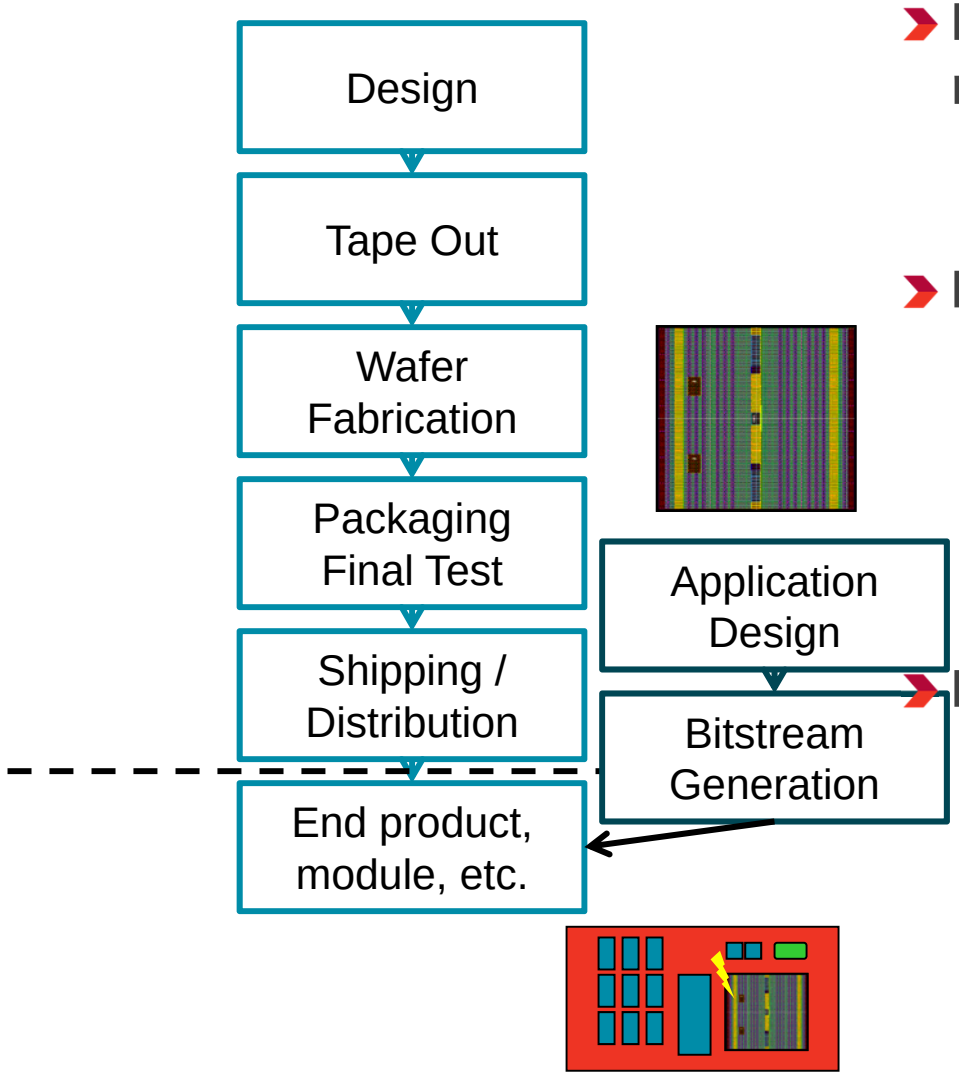
The IC Manufacturing Flow



- **Concerns:**
  - Theft of the design
  - Overbuilds
  - Tampering with the design
- **Challenges: securing the design**
  - Through all phases
  - For all parties
  - For months of elapsed time
- **Don't forget shipping between suppliers!**

© Copyright 2013 Xilinx

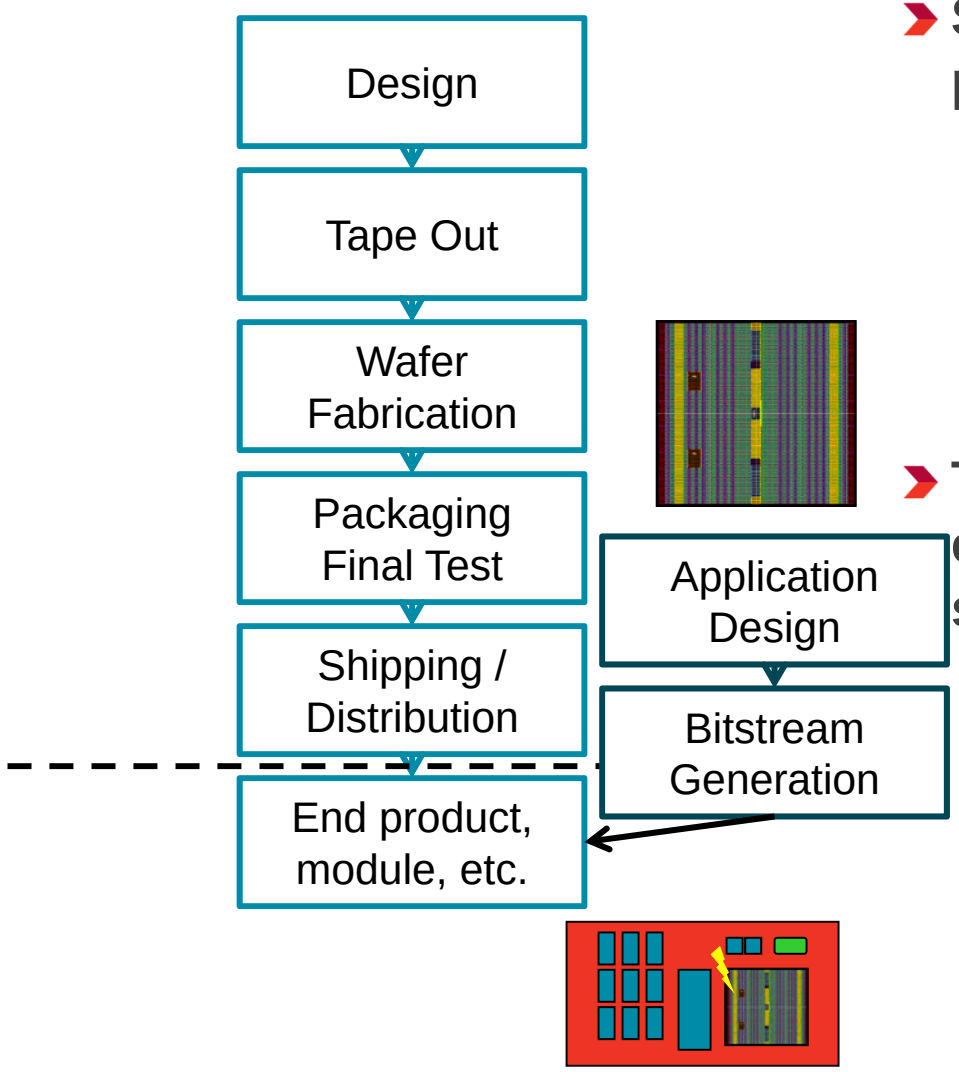
The FPGA “Manufacturing” Flow



- **During base array design and manufacture**
  - Same as custom device design and manufacture
- **During application design**
  - Same as custom device design
  - Do you trust your tools and libraries?
  - But FPGA application functionality is not exposed through the manufacturing flow (like software)
- **During deployment**
  - Same as software
  - Prevent bitstream piracy
  - Prevent loading malicious bitstream

© Copyright 2013 Xilinx

The FPGA “Manufacturing” Flow

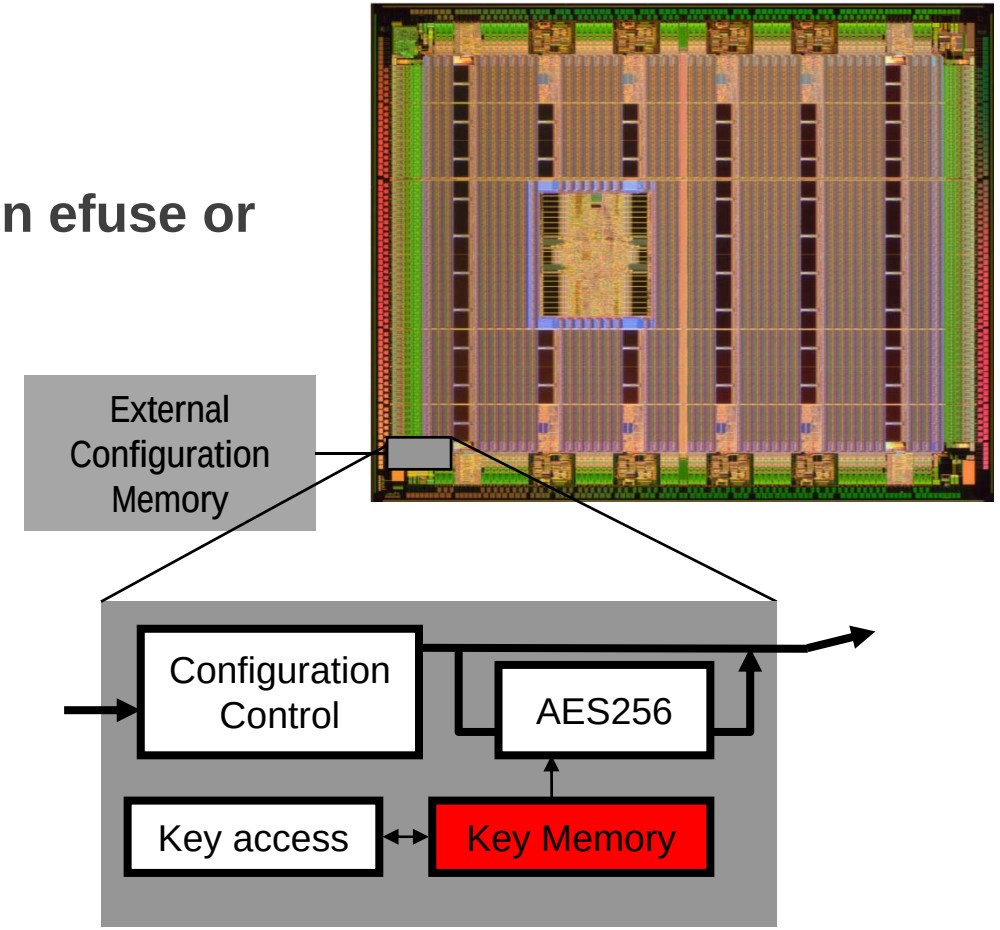


- **Sensitive algorithm is in the programming.**
  - It is not exposed through the manufacturing process.
  - It can be loaded into the device at a secure facility.
  - Hard to attack
- **The issues of IC manufacturing evaporate, but we must still secure the design in the field.**
  - The attacker has physical access to the system
  - This is the same as the embedded software protection problem
  - This is an information security problem. We know how to deal with it: algorithms for encryption and authentication.

© Copyright 2013 Xilinx

Virtex-II Configuration Hardware

- AES 256 encryption
- SHA256 authentication
- User selectable key stored in efuse or battery-backed RAM

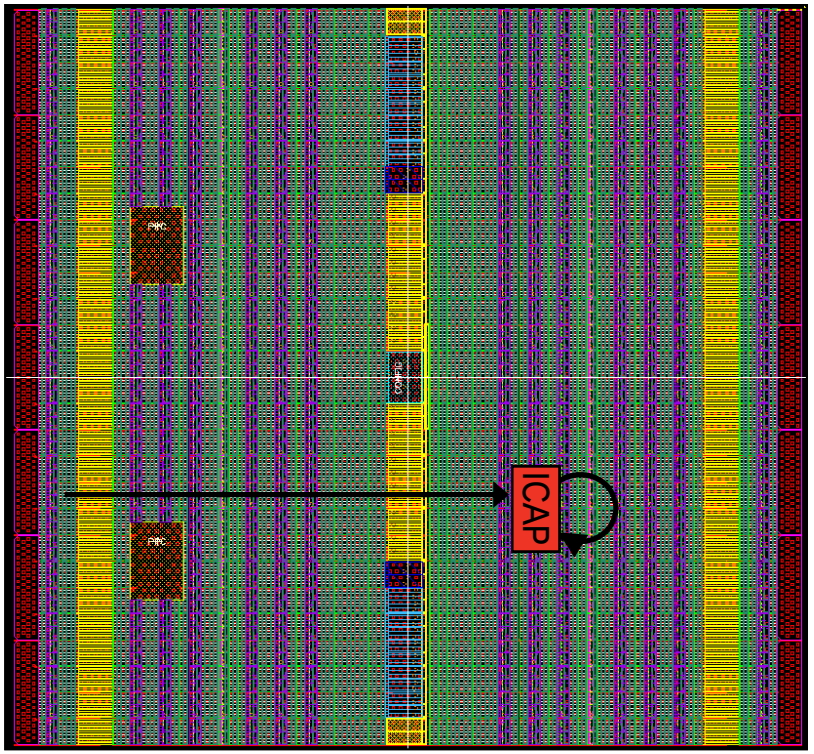


© Copyright 2013 Xilinx

Q: What About Attacks on Fielded Devices?

A: Self-check

- FPGA can read back configuration internally
- Check stored configuration and use ECC to correct configuration errors
- Monitor temperature, voltage internally
- TMR, …

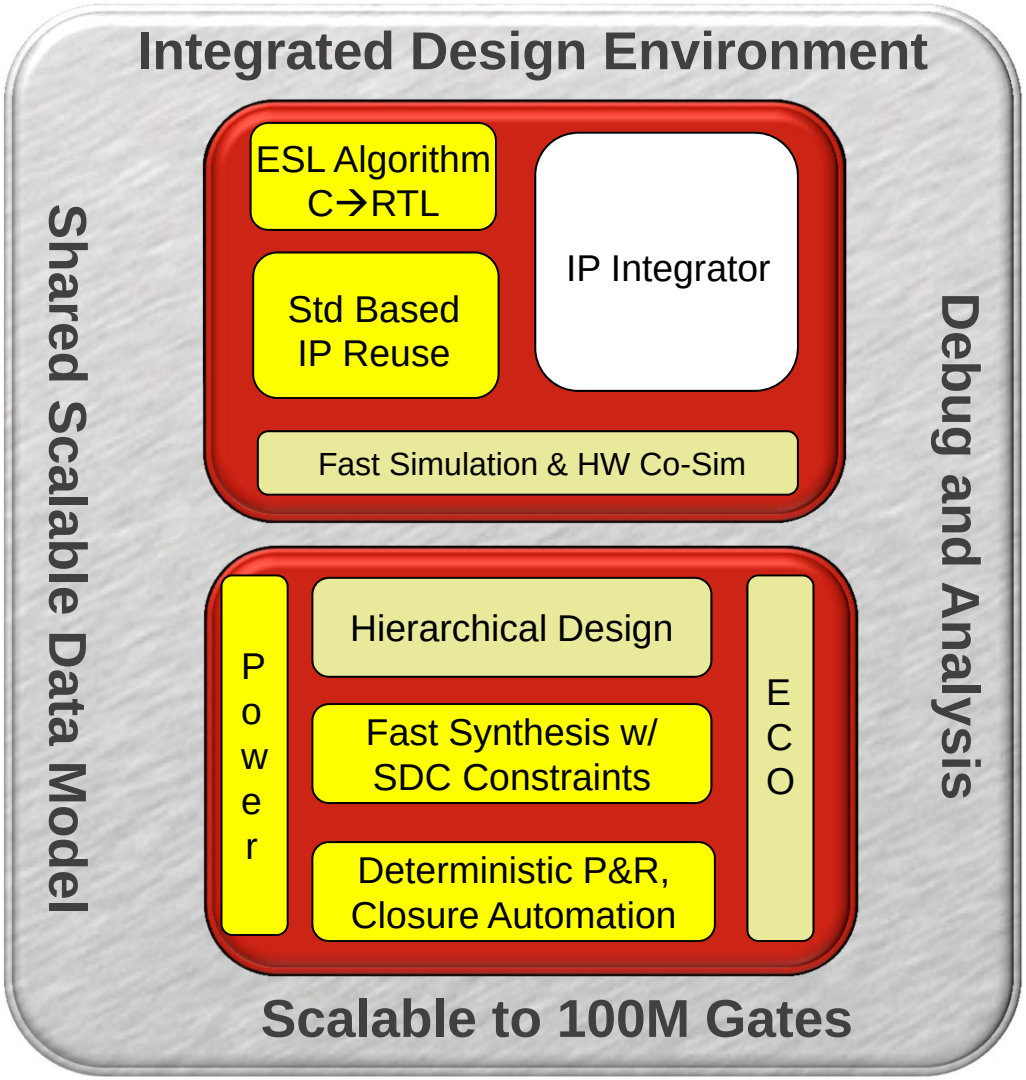


ICAP – Internal Configuration Access Port

© Copyright 2013 Xilinx

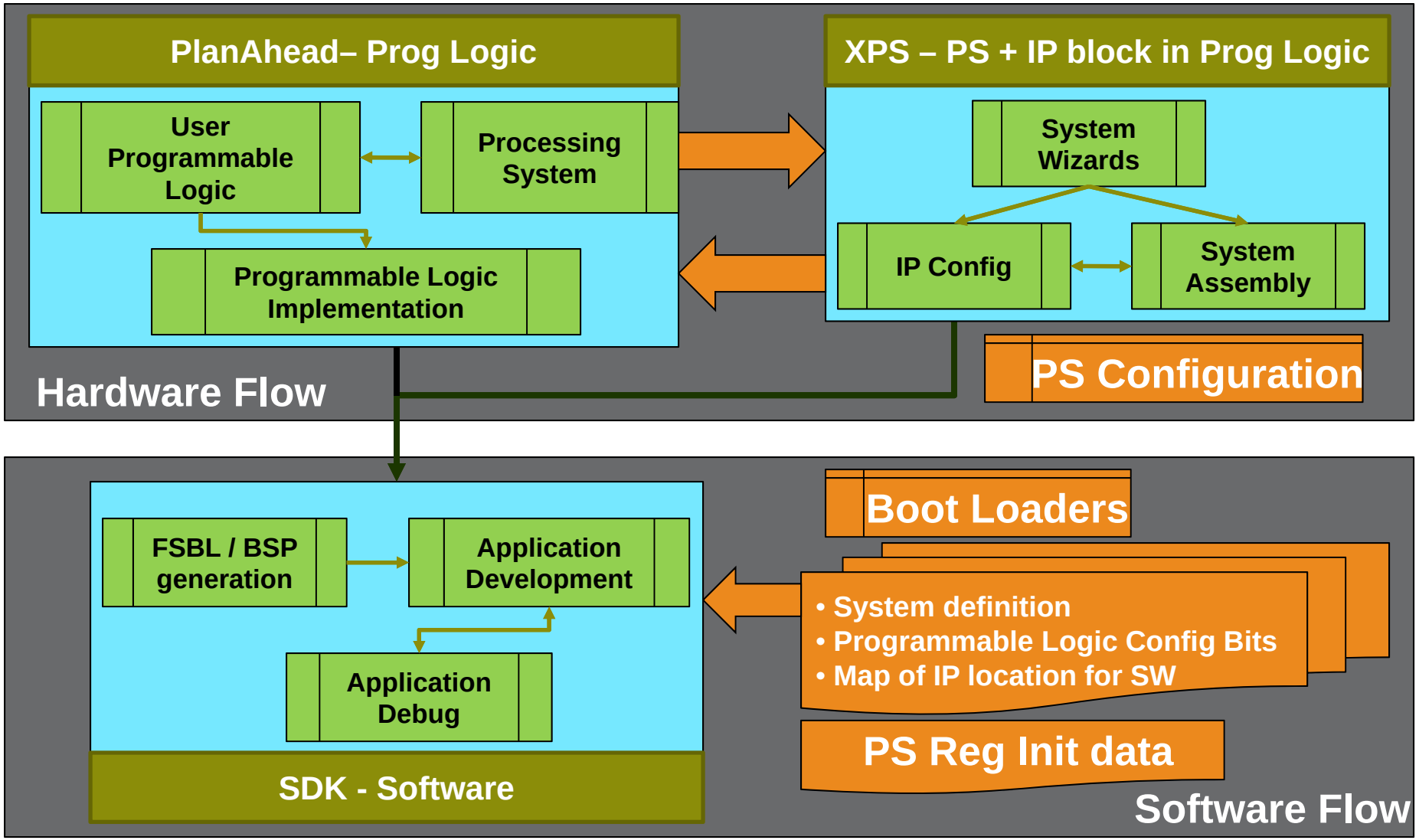
The FPGA Design Environment

- Xilinx Vivado integrated design suite
- Complete design capability
- Limited interactions with 3rd-party tools
- Supports IP integration from internal and external sources
- Supports FPGA design and Zynq AP SoC HW+SW flows
- Can close the loop from front to back of the design process.



© Copyright 2013 Xilinx

Zynq-7000 SoC Design Flow



© Copyright 2013 Xilinx