Hardware IP Protection

FPGA Manufacturing Flow

Base array design

Mask making

Wafer fabrication

Sort (test)

Packaging

Final test

Base array manufacture

Generic FPGA

Application design

System Manufacture

Deployed system

IP Security through Data Security

XILINX > ALL PROGRAMMABLE.
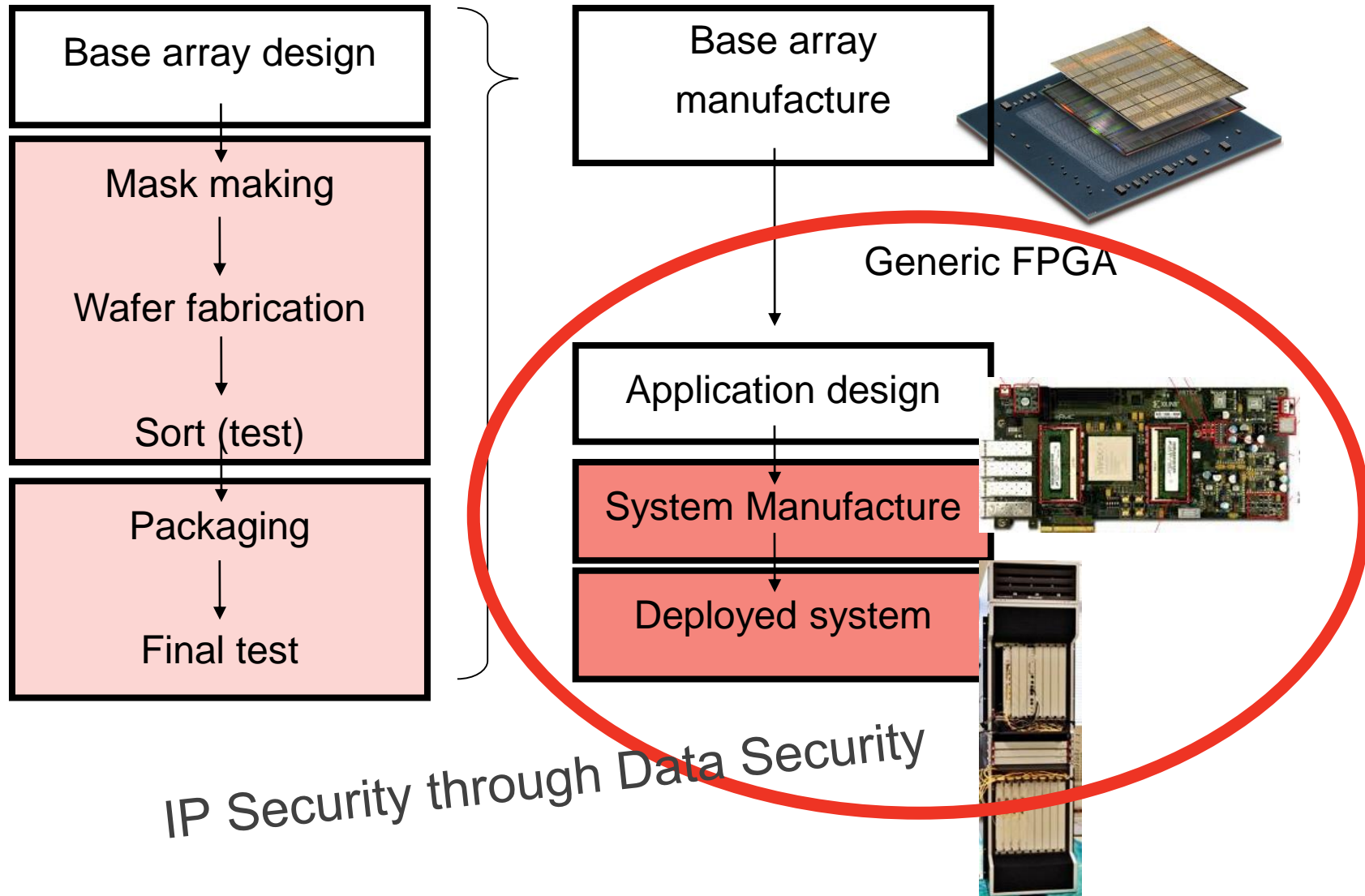
Risk and Trust in the IC Supply Chain

```
Base array design
        ↓
   Mask making
        ↓
  Wafer fabrication
        ↓
     Sort (test)
        ↓
    Packaging
        ↓
     Final test
```

> **Big companies can monitor this processes.**

> **There are many tools in place throughout the supply chain to thwart malicious actors**

> **Not happy? Do what we do: test it yourself!**

© Copyright 2015 Xilinx

XILINX ➤ ALL PROGRAMMABLE.

SEU

Temp spec

IP

SW
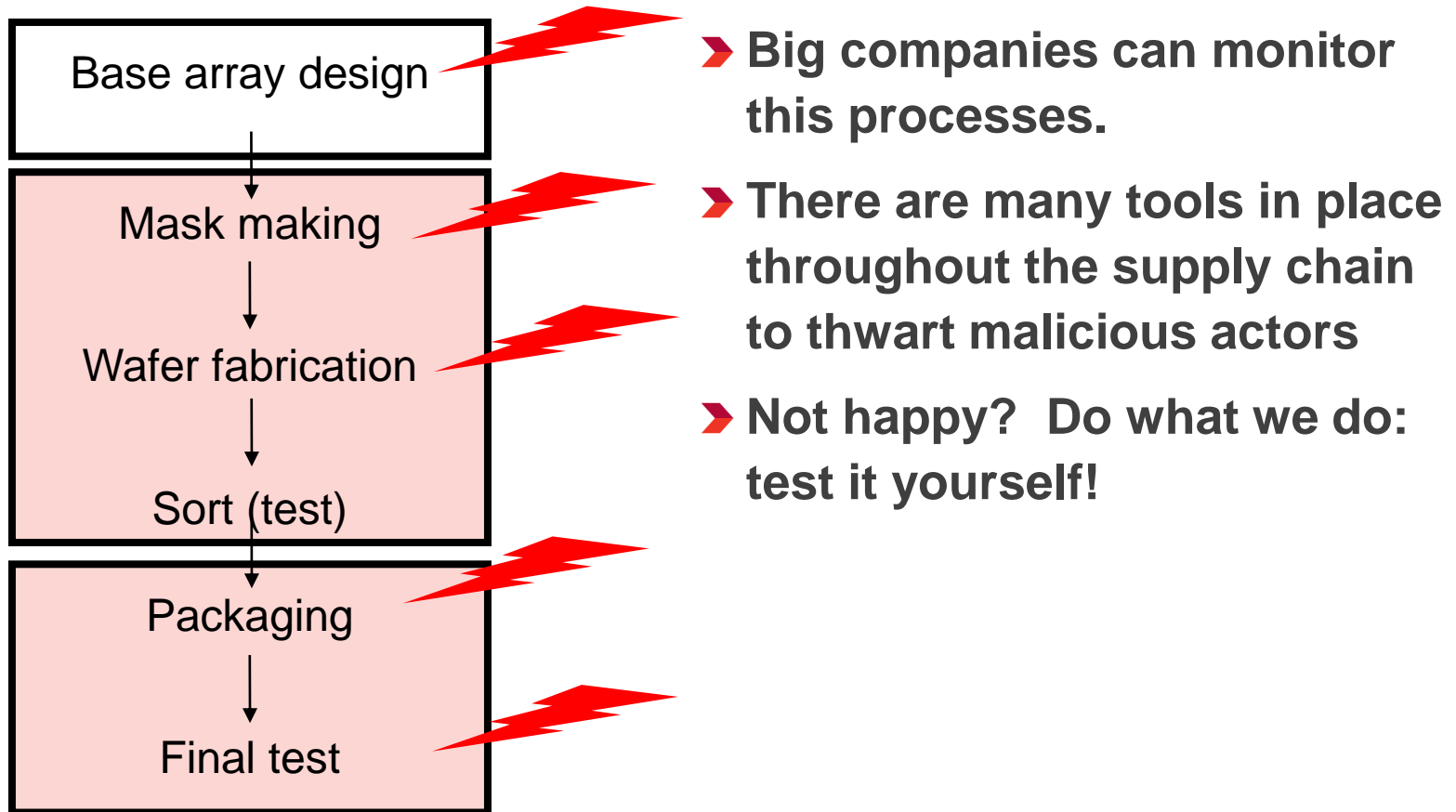
No back door

Functional test

You Trust Me!

Performance

Config

Base Array

Reliability

XILINX > ALL PROGRAMMABLE.

For the Student: How to Secure Integrated Circuit IP
(Hint, remember information security!)

➤ **What are the physical equivalents of encryption and authentication?**

➤ **Privacy: Obfuscated circuits and layout**

➤ **Authentication: PUF is a password, not a MAC**

➤ **Secure the design side.**

➤ **Validate incoming IP before use!**

⚡ XILINX ➤ ALL PROGRAMMABLE.