# Panel: Hardware-Enabled System Security

2016 HOST

Jon Ballast
Ethan Cannon
Eric Miller
Kristine Skinner

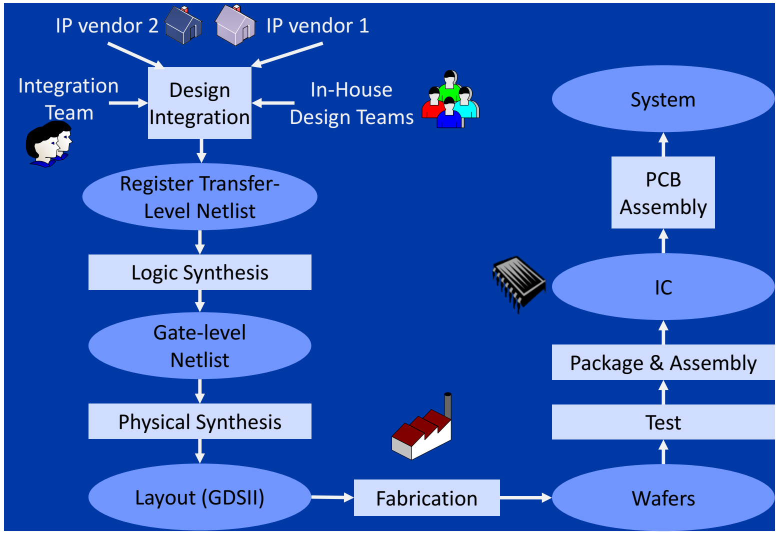
***The Boeing Company***

# Problem Statement

- Globalization in manufacturing supply chain
  +
  Decentralized manufacturing process
  =
  Products that pass through many different facilities and countries during development

- How do we ensure Critical Program Information (CPI) is protected when many different people have access to it?

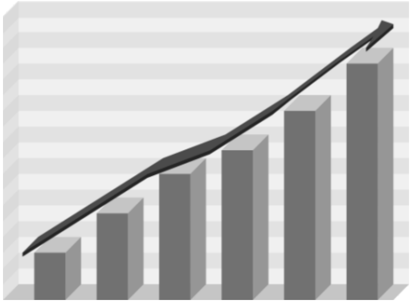
- Need to protect information that could be
  - Stolen by a competitor for profit or other advantage
  - Used to disable or disrupt a product's functionality



# Design for Security Approach

1. **Model attacker capabilities**

2. **Determine security metrics**



3. **Engineer the defense**

*Source: Karri et. al "Security Analysis of IC Camouflaging," ACM CCS 2013 (Best Student Paper Award)*

| Level | Technique |
|---|---|
| 5 | Trusted Flow |
| 4 | Split Fabrication |
| 3 | Heterogeneous Integration |
| 2 | Obfuscation |
| 1 | Commercial, verification |

***Source: B. Chappell, NSA Microelectronics Symp, 3/1/2016***

| | | User | |
|---|---|---|---|
| | | Trusted | Untrusted |
| Foundry | Trusted | Trusted Flow | Camouflaging |
| | Untrusted | Split manufacturing | Logic Locking |

# Protecting CPI

- Once key risks and vulnerabilities are identified, generate a plan to provide CPI protection

- Once initial plan is in place, need additional metrics: how do CPI protection techniques impact design?
  - Cost
  - Performance
  - Schedule

- Watch out for moving targets
  - Continuous changes in the supply chain (company mergers, new technologies, etc.) will change CPI vulnerabilities