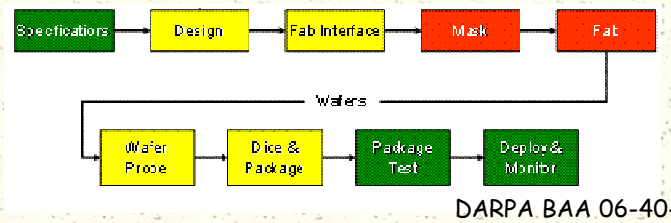
HT and Trusted IC
-- HT Taxonomy

Cybersecurity Specialization
-- Hardware Security

Hardware Trojan Taxonomy

- IC supply chain phase: when HT is embedded
- Abstraction level: when HT is embedded during the design phase
- Activation: how HT is activated
- Effects: what does the HT do
- Location: where on-chip the HT is
- Type: functional or parametric
- Size: big/small, tight/loose
- Layout: change or no-change

HT Taxonomy: IC Supply Chain

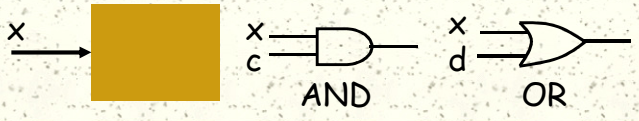


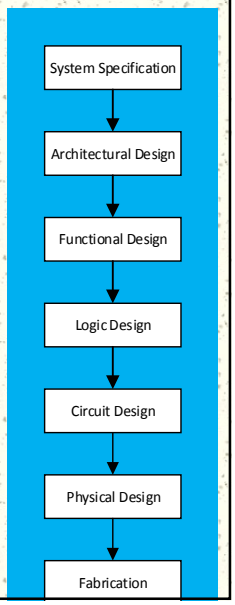
Source: DARPA BAA 06-40-Trust for IC

- Specification: modify modules or interconnect
- Design phase
- Fabrication: change mask, speedup circuit aging
- Assembly: extra connections, unshielded wires
- Testing: false negative

HT Taxonomy: Abstraction Level

- System specification level
- Architectural level or RTL
- Functional level
- Logic synthesis or gate level
- Circuit or transistor level
- Physical design or layout level
- Design environment or tools





HT Taxonomy: Type

- Functional:
  - Addition/deletion of components
  - Modification of component's functionality
- Parametric: damage reliability or increase the likelihood of performance failure
  - Thinning wires
  - Weakening of transistors or logic gates
  - Modification of power distribution network

HT Taxonomy: Activation Method

- Always-on: parametric HTs
- (Rare) Event/signal triggered
  - Sensor vs. logic triggered
  - Internally vs. externally triggered
- Example:
  - Time bomb: internally and logic triggered
  - Temperature: sensor triggered
  - External signals (user input, data input, environmental condition, etc.): externally triggered

HT Taxonomy: Effect or Payload

- Payload is the action or the damage that a HT will do once it is activated.
- Change/control of functionality
  - Killer switch, time bomb, the $F(x)=x^2$ example
- Leak sensitive information
  - side channels: power, timing, optical, thermal, EM emission
- Reduce circuit reliability or lifetime
  - Parametric HTs, drain resource (power, bandwidth, CPU, etc.) from the system

HT Taxonomy: Locations

- Processing units: change/control of the system functionality
- Memory structure: alter memory contents, monitor memory activity and leak information
- I/O devices: control/modify/monitor data communication between chip and outside
- Power supply units: change power/current supply to cause failure, or leak information
- Clock grids: change frequency to cause fault or failure, timing side channel information leak

HT Taxonomy: Physical Features

- Size
  - Big functional blocks: sophisticated time bomb, powerful antenna
  - Small gates: killer switch, small sensor
- Layout
  - Need redo layout: add functional blocks
  - No change: parametric HTs
- Distribution
  - Tight/centralized: big
  - Loose/distributed: small