The Fourteenth International Conference on Advances in Circuits, Electronics and Micro-electronics
CENICS 2021
November 14, 2021 to November 18, 2021 - Athens, Greece

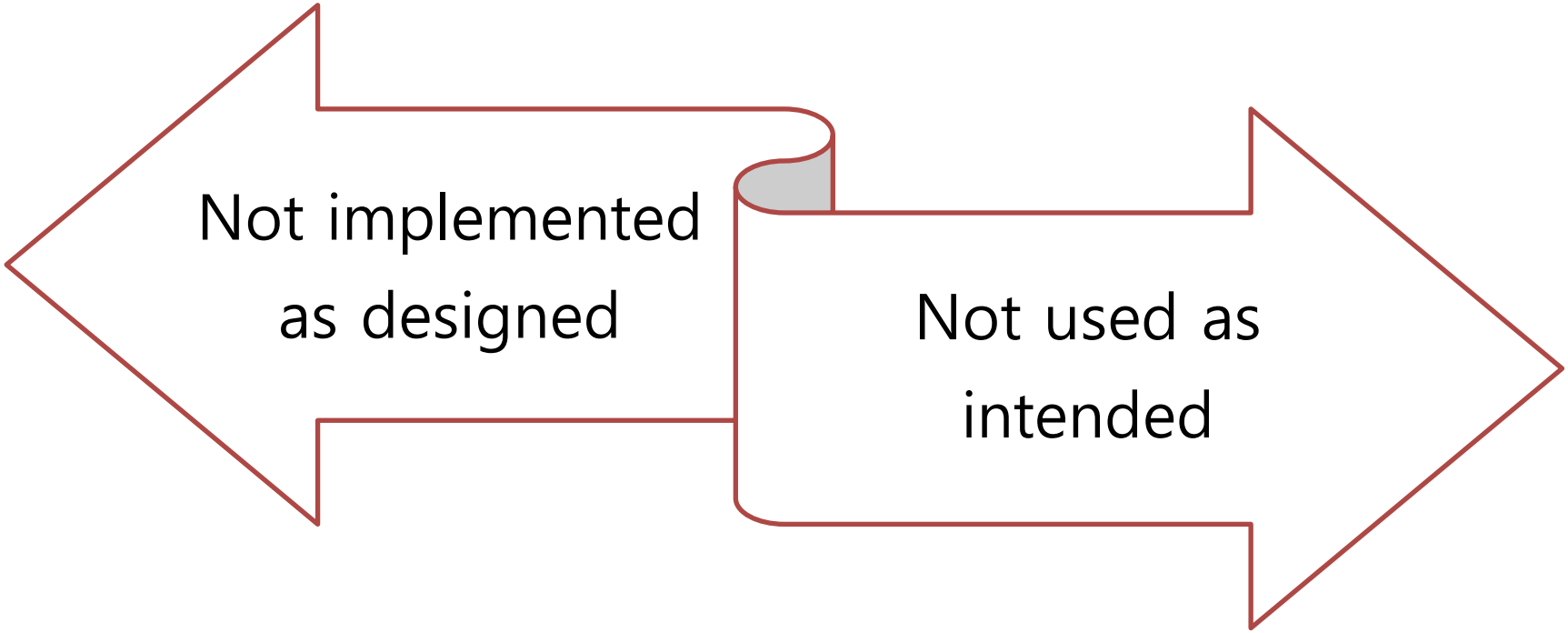
Trust Issues in the Semiconductor Industry

Junghee Lee
j_lee@korea.ac.kr

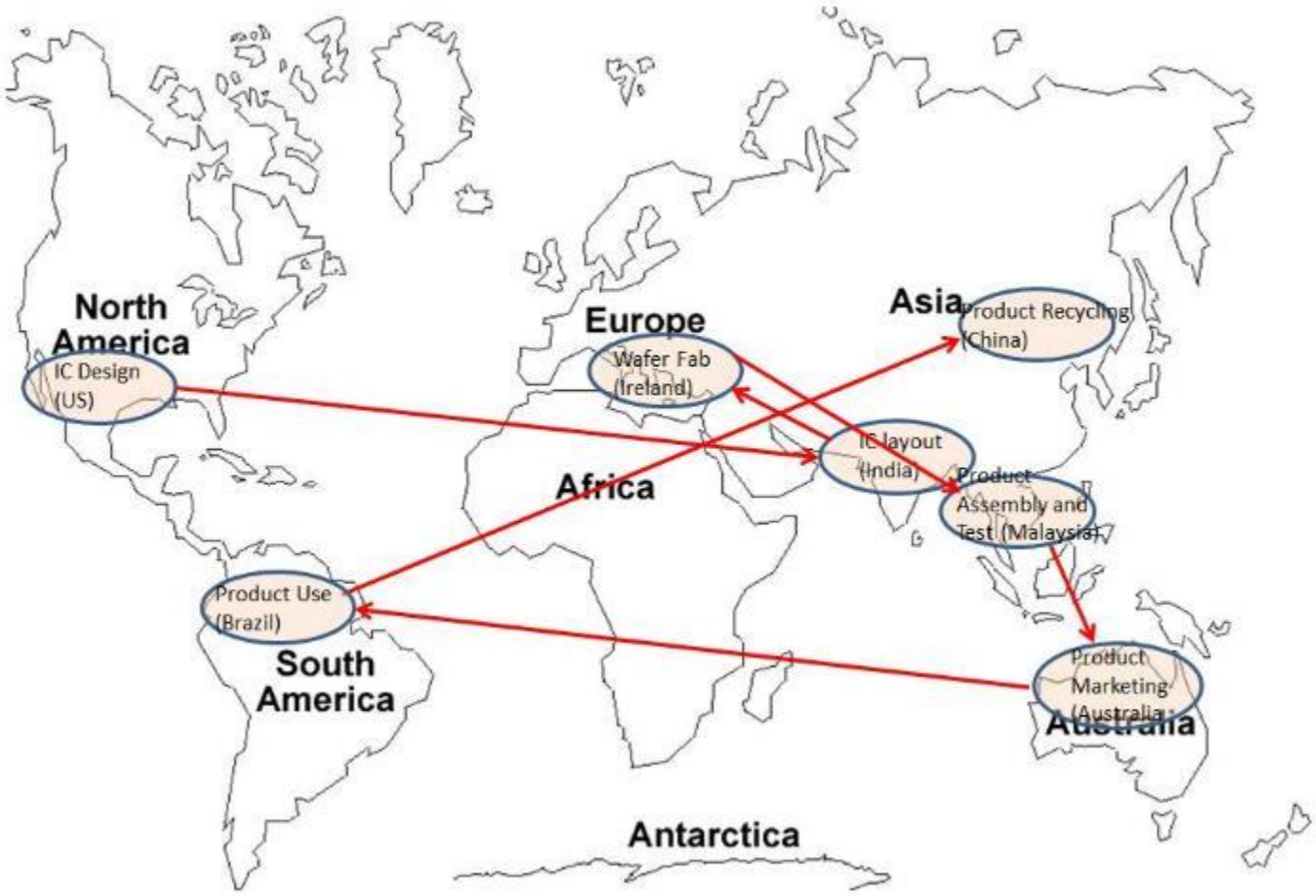
Your Speaker

- Education
  - Ph.D Georgia Institute of Technology (2013)
  - M.S. Seoul National University (2003)
  - B.S. Seoul National University (2000)
- Appointments
  - Assistant/Associate Professor
    Korea University (2019-Present)
  - Assistant Professor
    University of Texas at San Antonio (2014-2019)
  - Engineer
    Samsung Electronics (2003-2008)
- Research area
  - Hardware security (processor, memory, non-volatile memory, storage, dedicated hardware)

Trust vs Security

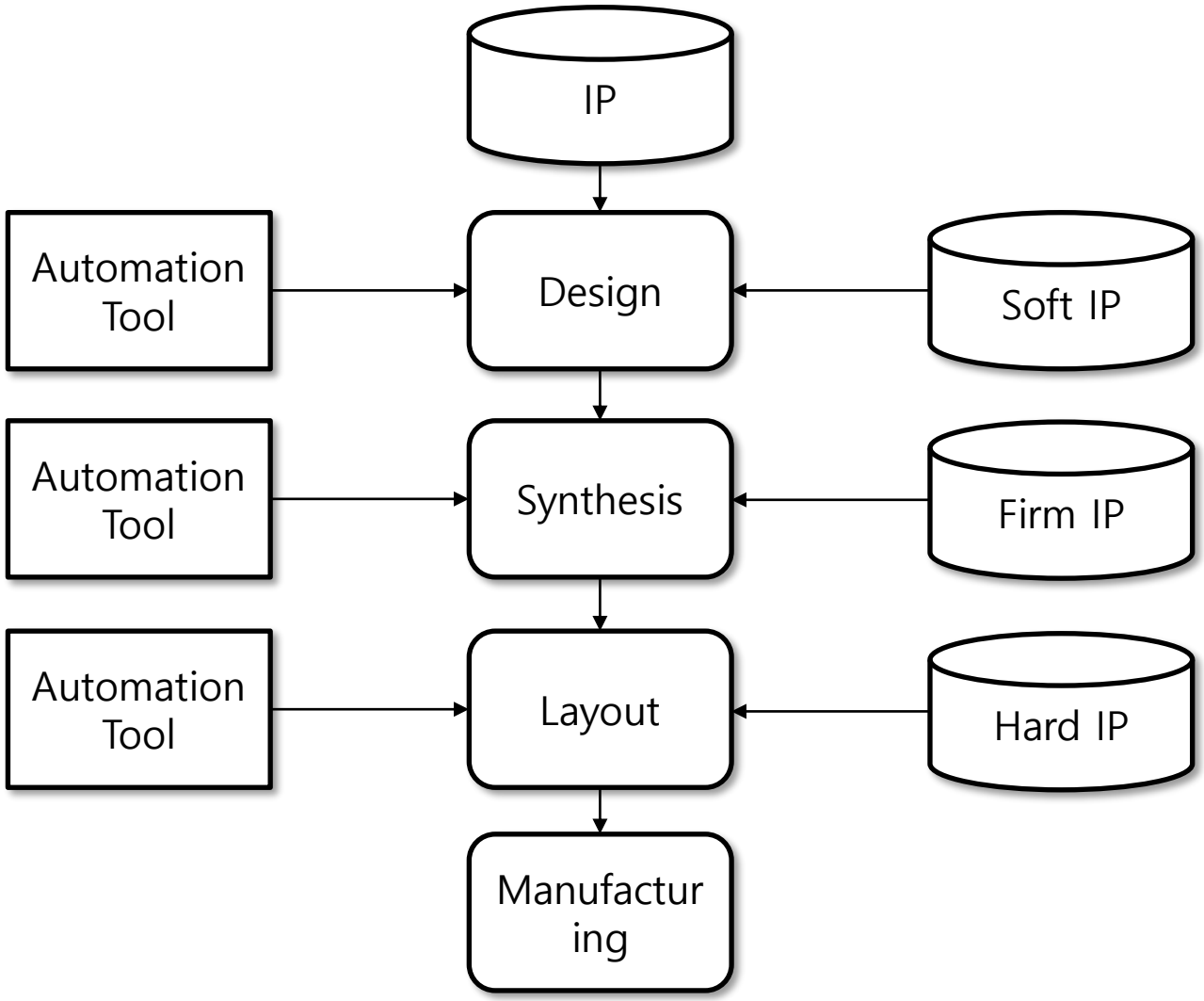


Globalization



http://proutglobe.org/2013/12/three-tier-business-model-semiconductor-industry/

Typical Design Flow



Untrusted Foundry

Overproduction

Recycling

Counterfeit

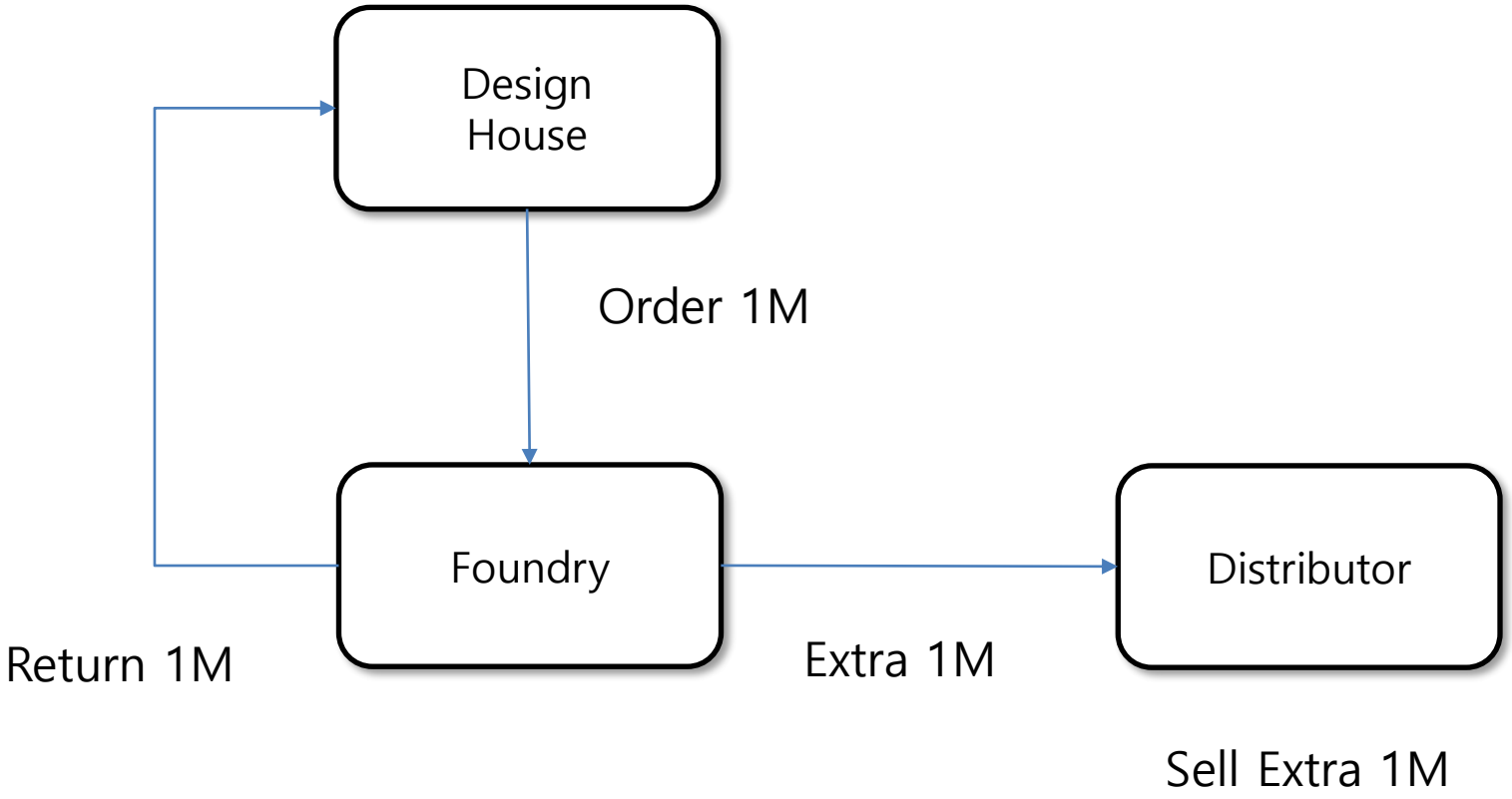
IC Recycling

Collect discarded ICs

Replace the marking

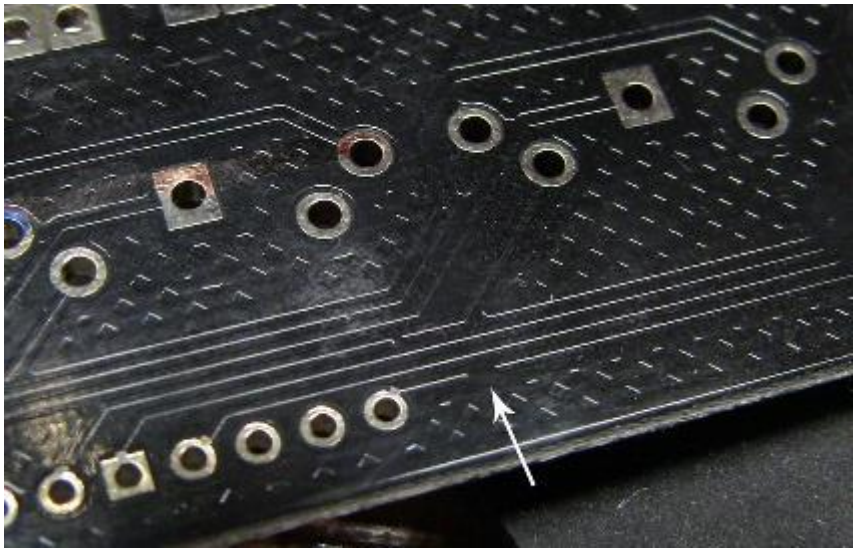
Sell as new

Overproduction

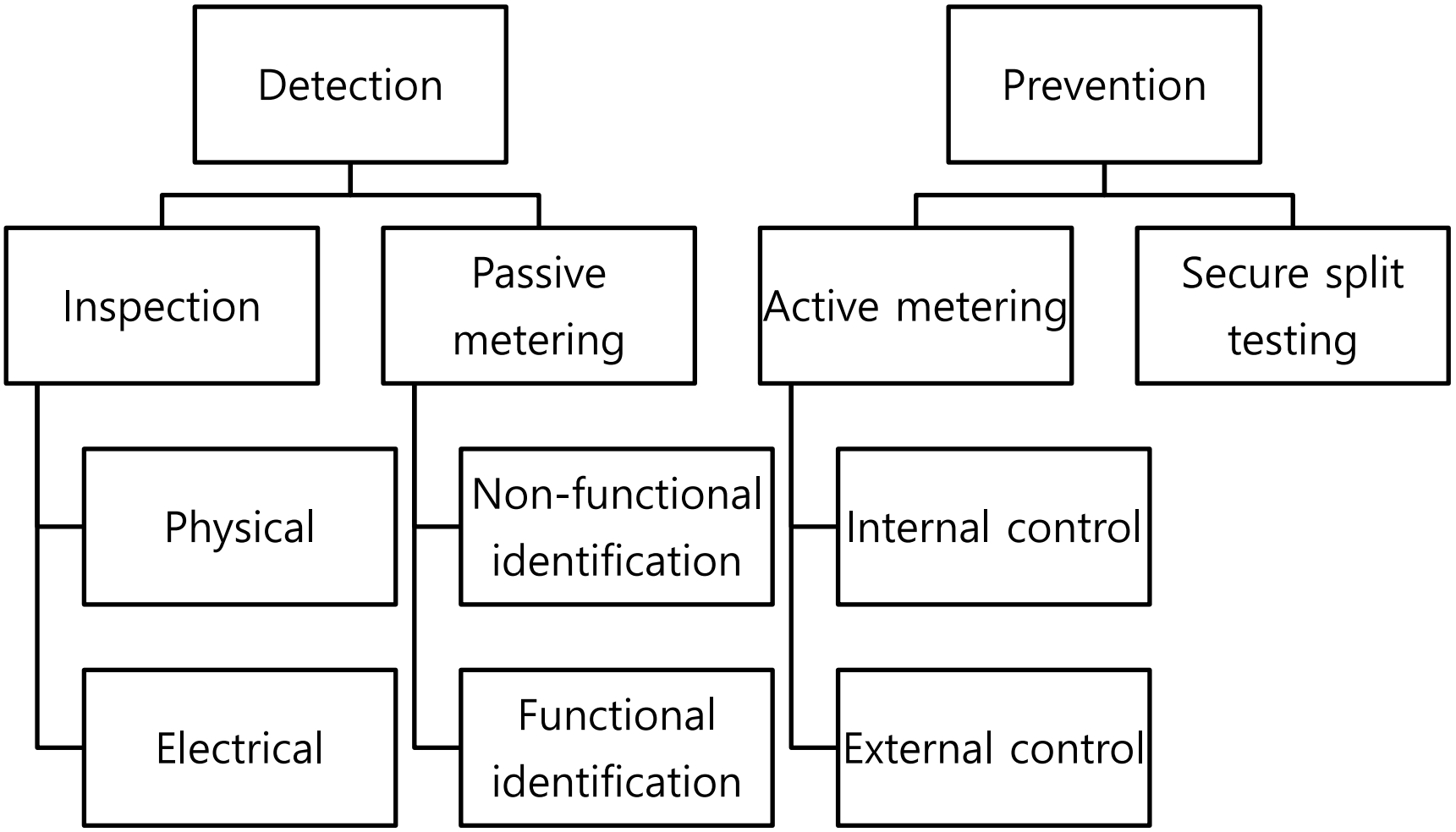


Counterfeit

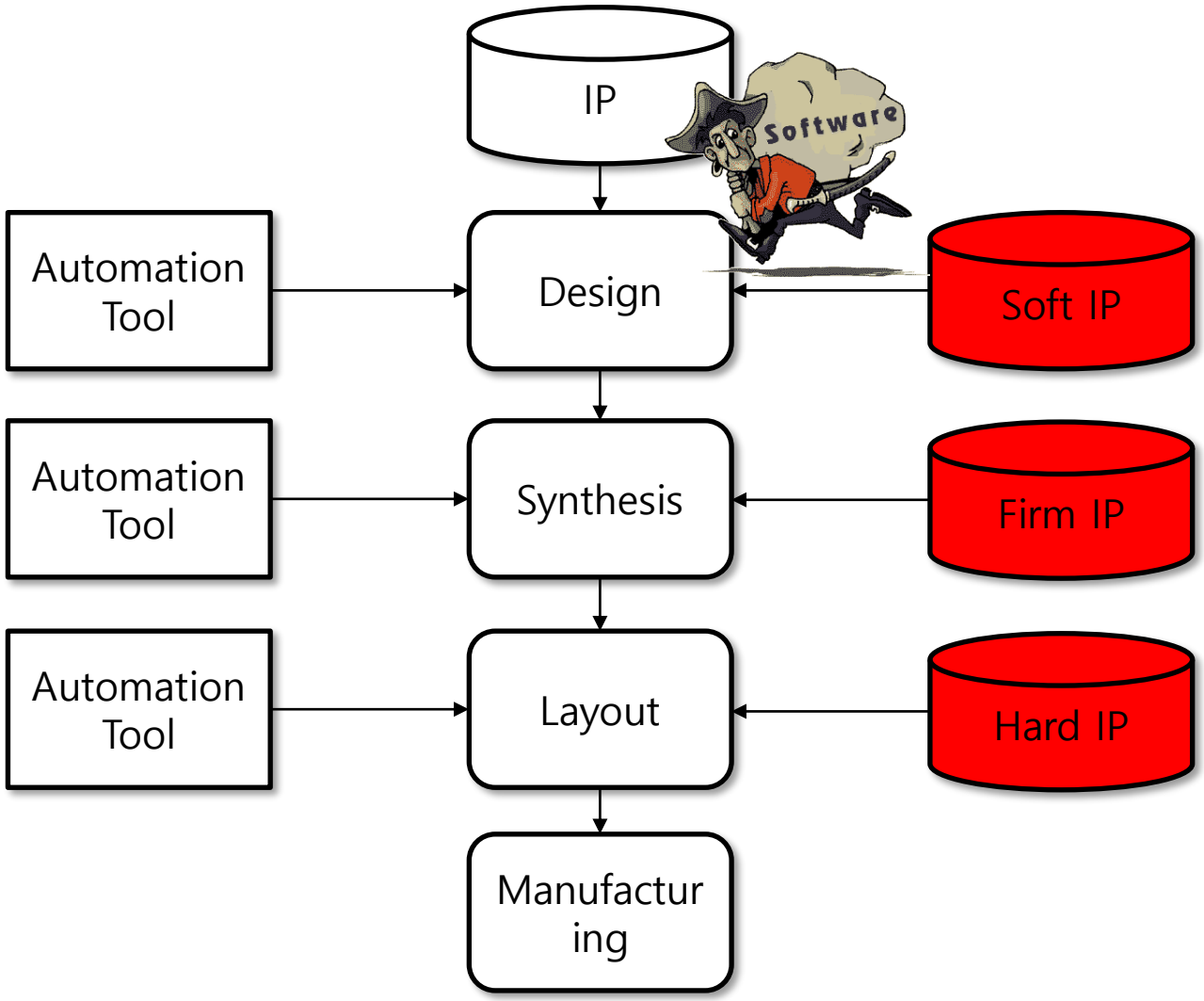
- Recycling
- Overproduction
- Forged documents
- Defective parts



Countermeasures

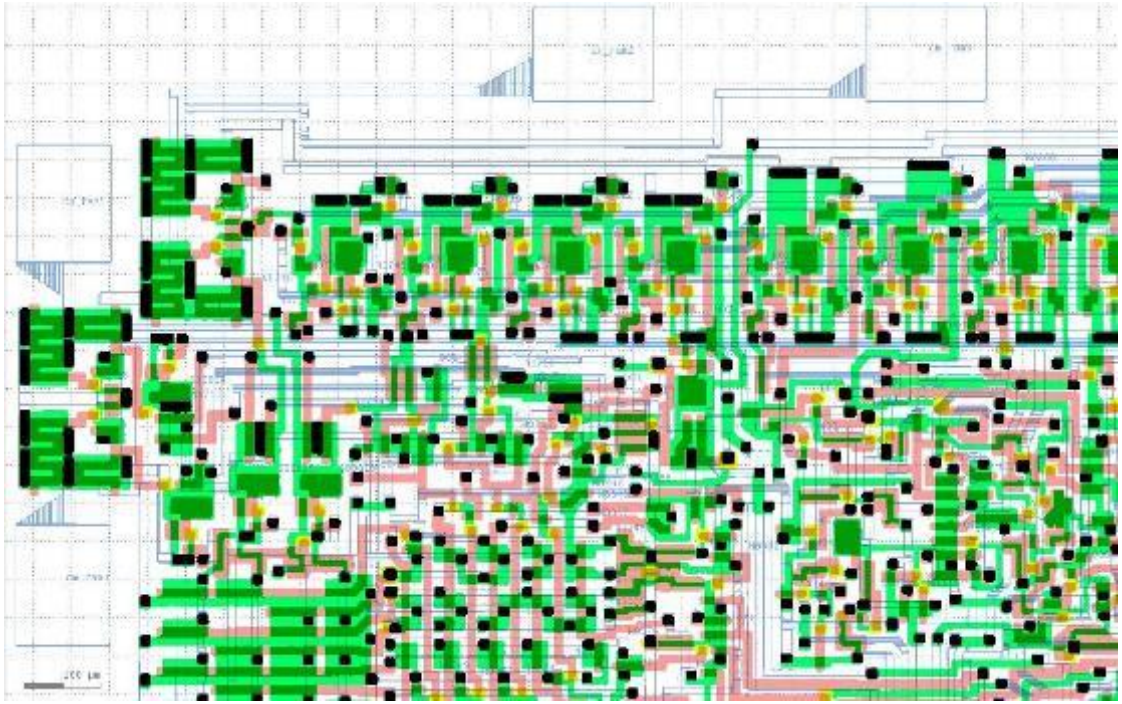


Untrusted Design House

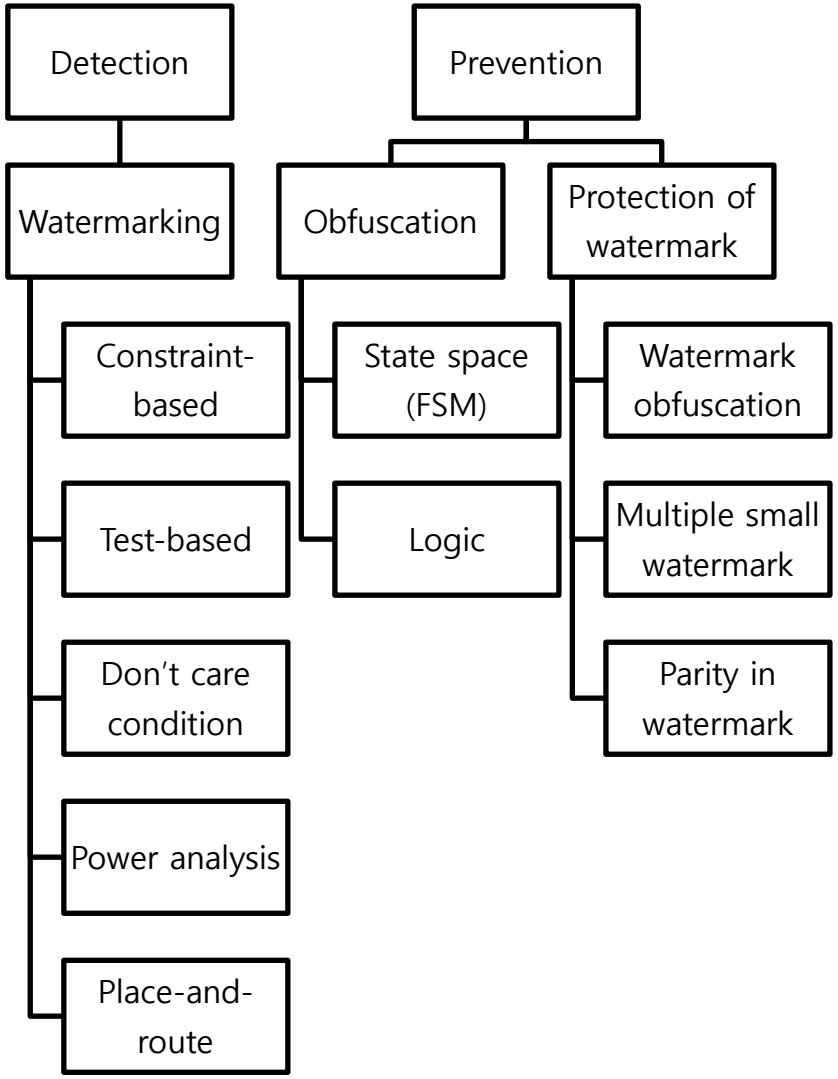


Piracy

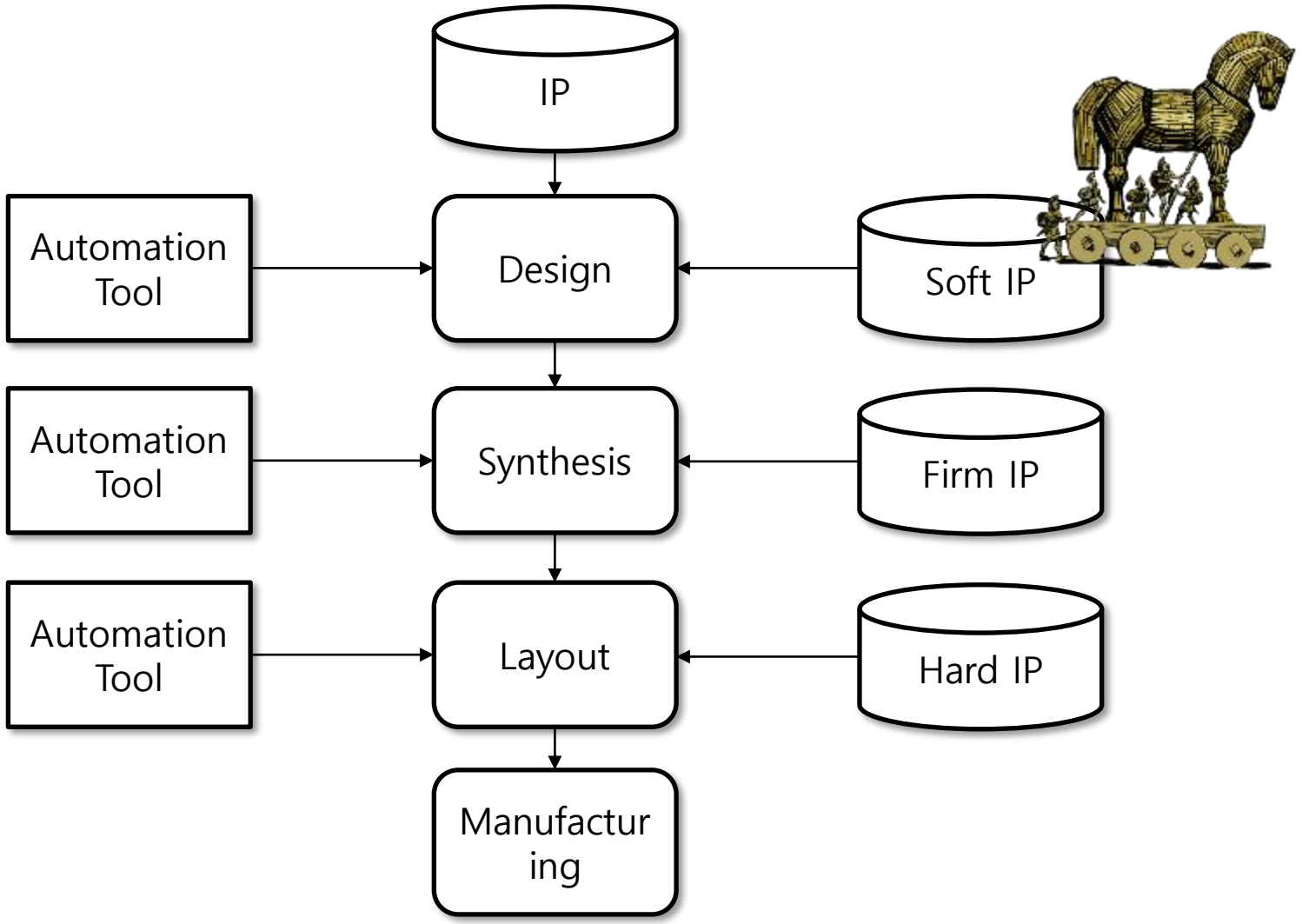
- Unlicensed usage
- Reverse engineering



Countermeasures



Untrusted IP



Hardware Trojan

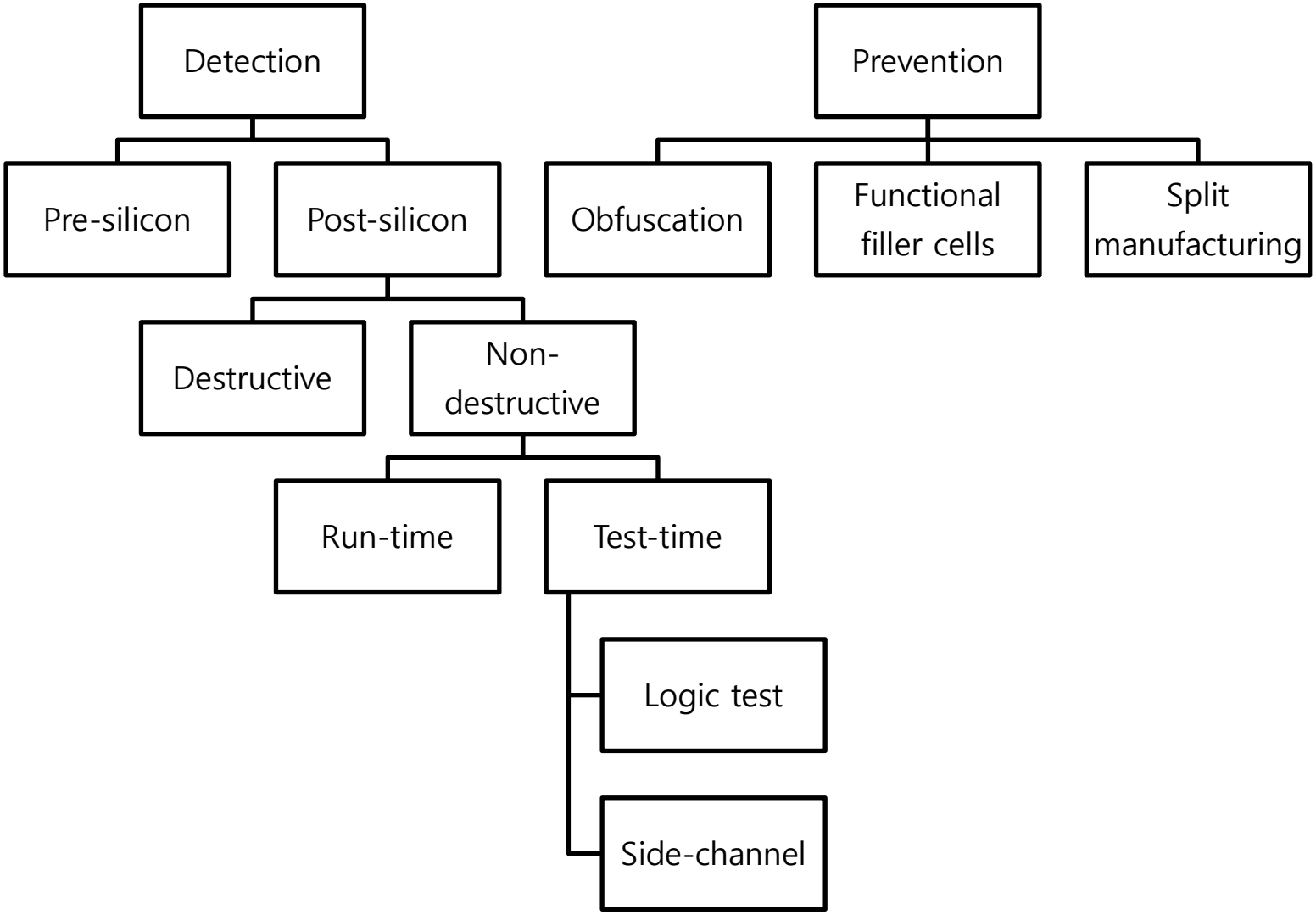
- A hidden malicious circuit
- It does
  - Lead to malfunction
  - Leak information
- Motivation
  - Military
  - Financial

Trojan Structure

Combinational
Sequential

Change signals
Leak information
Downgrade performance

Countermeasures



Summary

- Globalization of semiconductor industry
- Untrusted parties
- Counterfeit, piracy, Trojan, …
- Technical countermeasures