Workshop on Hardware based Attacks & Defenses

Module 1

Patanjali SLPSK
Postdoctoral Researcher
Electrical and Computer Engineering Department
University of Florida

UF Warren B. Nelms Institute for the Connected World
UNIVERSITY of FLORIDA

Outline

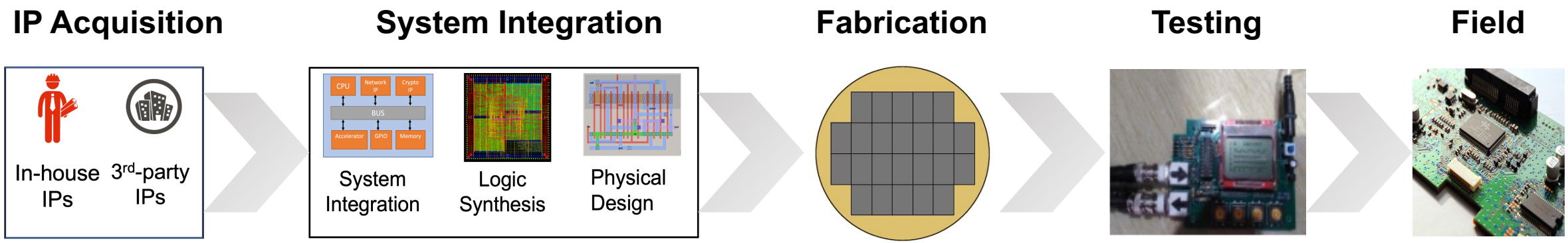
- Hardware security
  - Why Hardware Security?
  - Trust Issues in the Supply chain
  - Challenges for Trustworthy Hardware

Why Hardware Security?

- Today's hardware design complex entities with hundreds of moving parts
- The chip designer has to meet:
  - Complex user requirements
  - Challenges of manufacturing at lower nanometer nodes
  - Aggressive time-to-market demands

Why Hardware Security ?

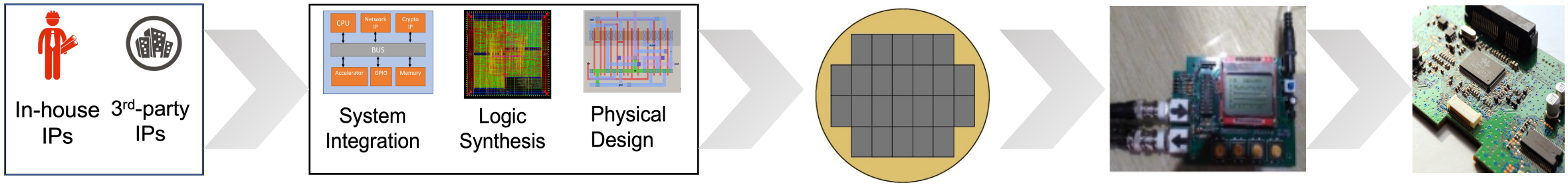
Semiconductor Supply chain



- Distributed model => multiple entities each focusing on a dedicated aspect of the design process
- Instead of designing IPs in-house use pre-designed models
- Foundry focusses on lower nanometer challenges
- System Integrator can operate as a “fabless” entity and reduce cost
- Easily meet time-to-market demands
- **Cons: Multiple entities, across the globe => Trust Issues**

Trust Issues in Supply Chain

Semiconductor Supply chain



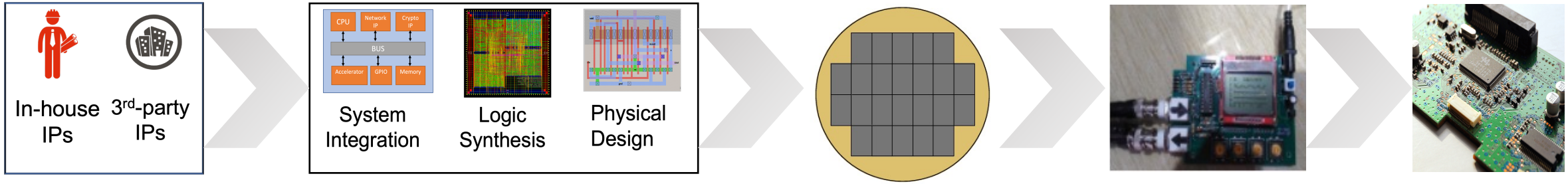
Trust Issues

- Trojans
- Trojans
- Piracy /Counterfeiting
- Reverse-Engineering
- Extraction of Design Secrets
- Trojans
- Piracy /Counterfeiting
- Reverse-Engineering
- Extraction of Design Secrets
- Piracy /Counterfeiting
- Reverse-Engineering
- Extraction of Design Secrets
- Side-channels
- Extraction of Design Secrets

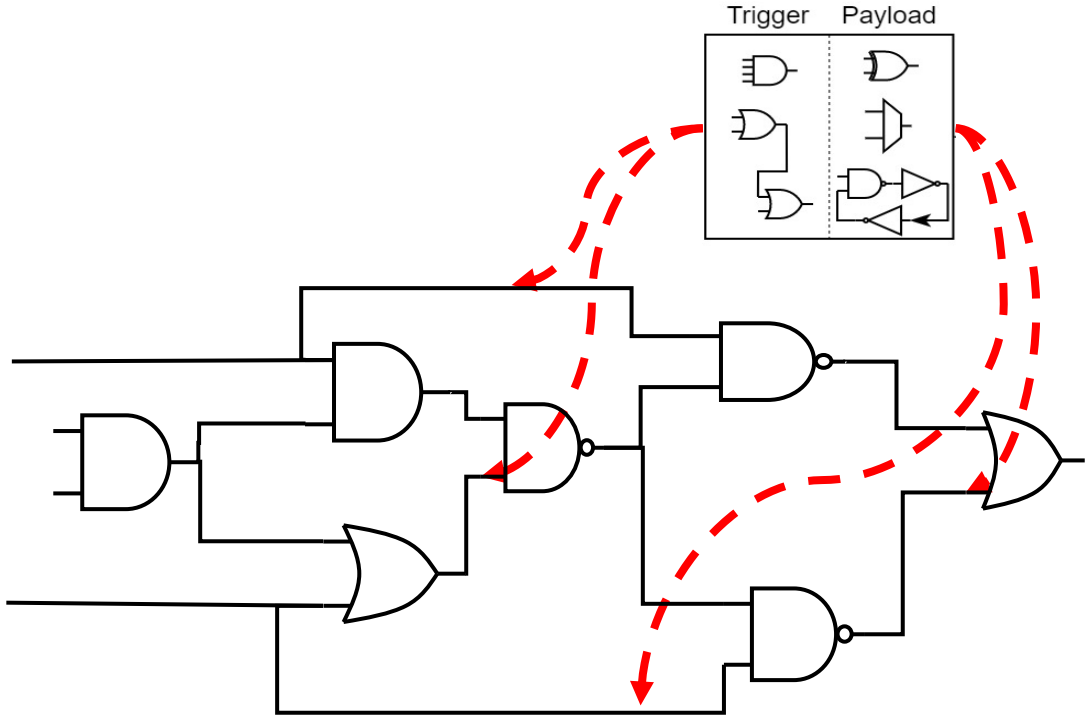
Trust Issues in Supply Chain

Semiconductor Supply chain

IP Acquisition | **System Integration** | **Fabrication** | **Testing** | **Field**



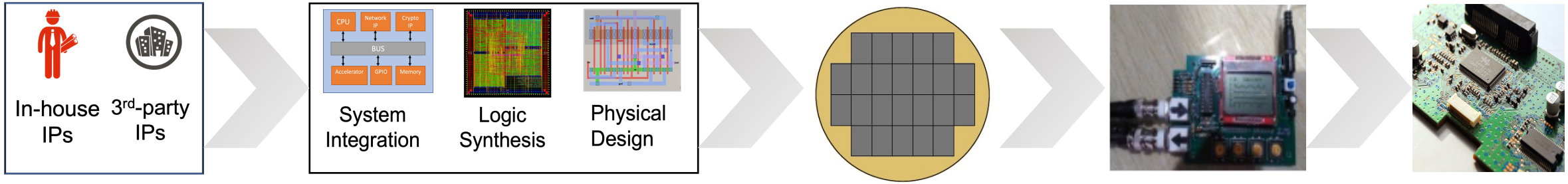
Trojans



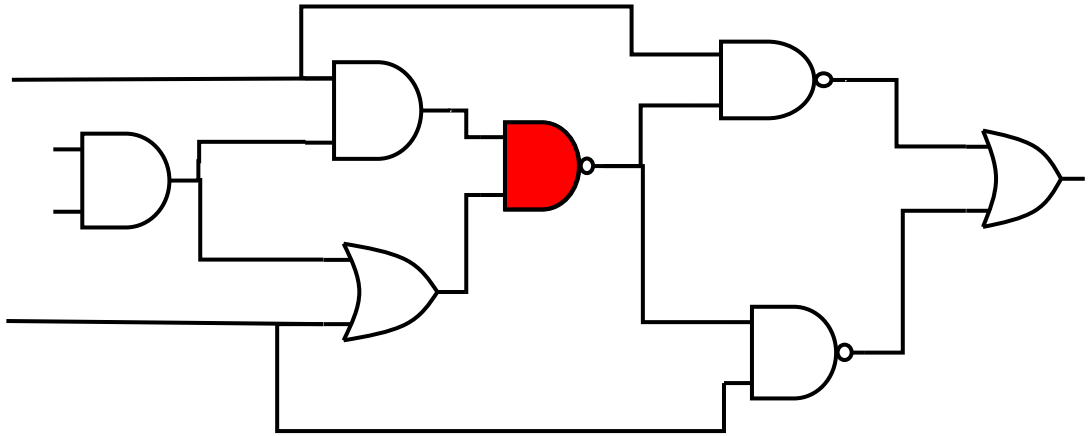
Trust Issues in Supply Chain

Semiconductor Supply chain

IP Acquisition | **System Integration** | **Fabrication** | **Testing** | **Field**



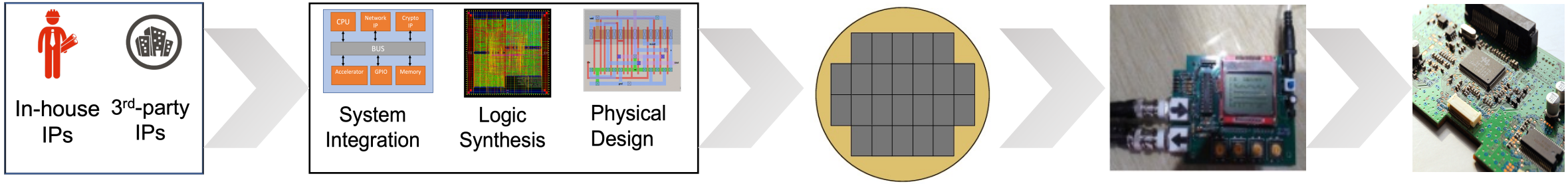
Piracy/Counterfeiting



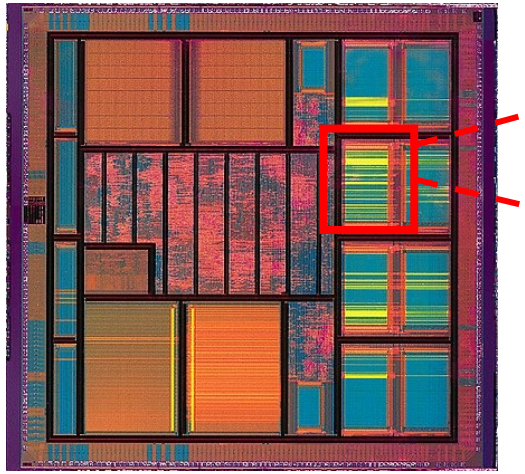
Trust Issues in Supply Chain

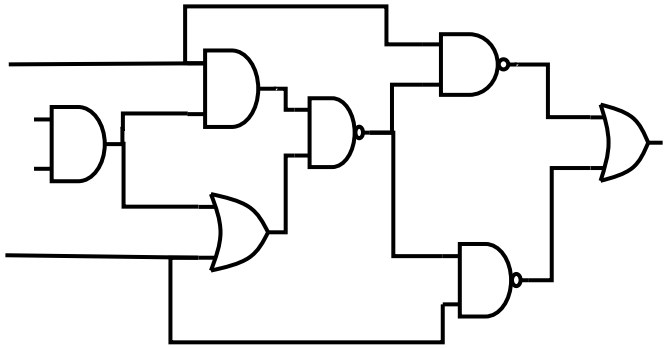
Semiconductor Supply chain

IP Acquisition | **System Integration** | **Fabrication** | **Testing** | **Field**



Reverse-Engineering

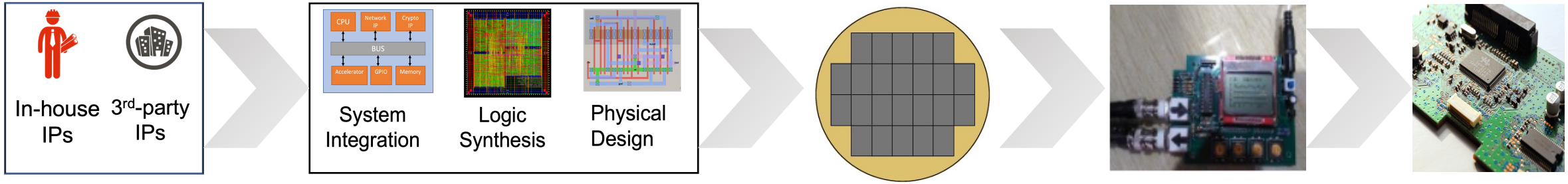




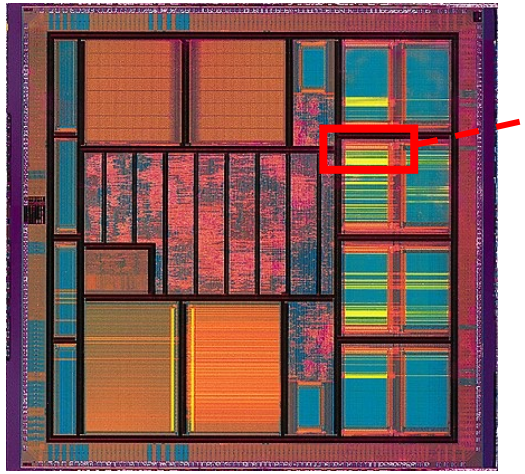
Trust Issues in Supply Chain

Semiconductor Supply chain

IP Acquisition | **System Integration** | **Fabrication** | **Testing** | **Field**



Extraction of Design Secrets

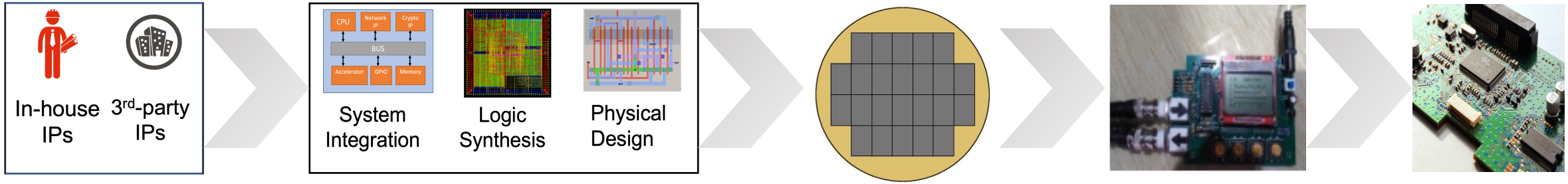


0xd3adc4fe

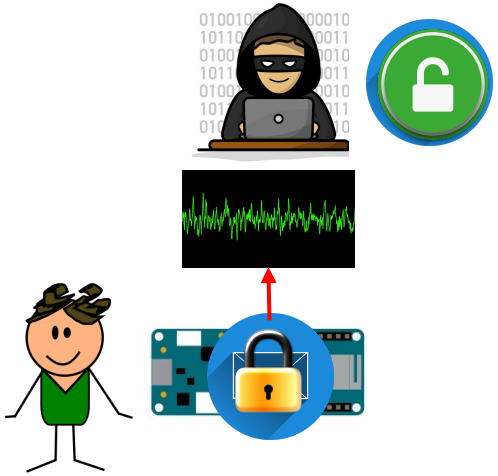
Trust Issues in Supply Chain

Semiconductor Supply chain

IP Acquisition | **System Integration** | **Fabrication** | **Testing** | **Field**



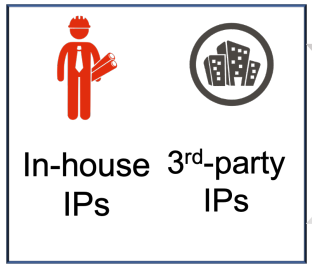
Side-channel attacks

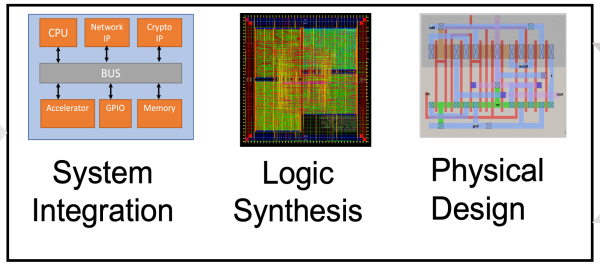


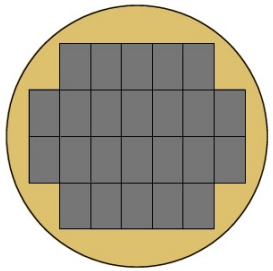
Challenges for Trustworthy Hardware

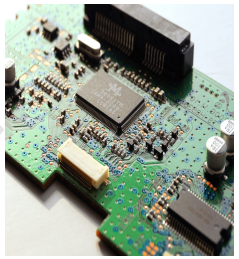
Semiconductor Supply chain

IP Acquisition | **System Integration** | **Fabrication** | **Testing** | **Field**



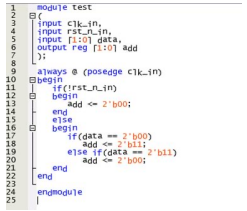


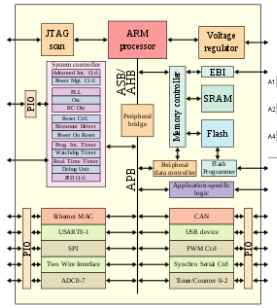


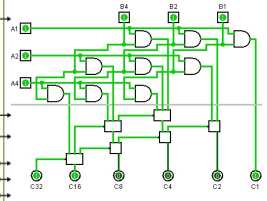


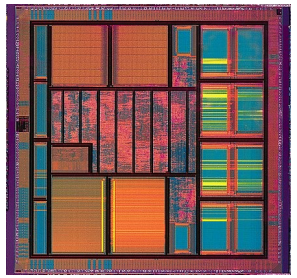
Design Transformation

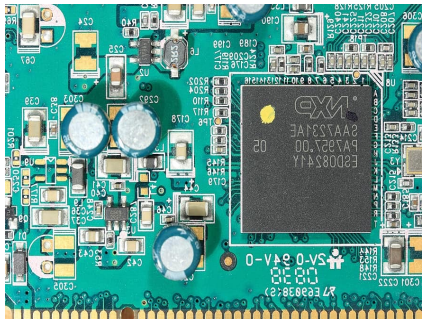
RTL | **System Integration** | **Gate-level netlist** | **Physical Design** | **Fabricated Design** | **Packaged IC**









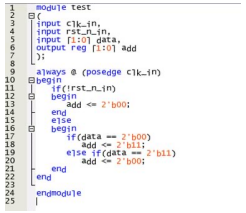


- **Challenge 1:**
  - Any security solution must remain immutable to design transformation
  - Must respect the design constraints at each stage

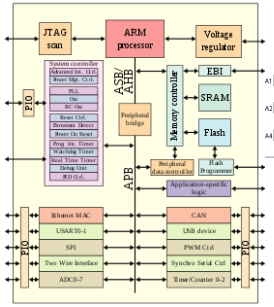
Challenges for Trustworthy Hardware

Design Transformation

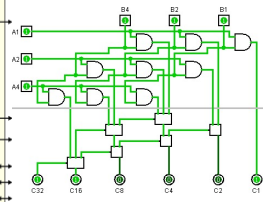
RTL



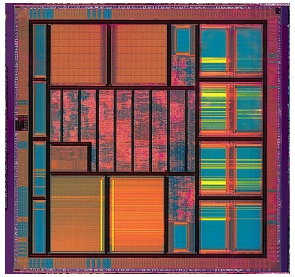
System Integration



Gate-level netlist

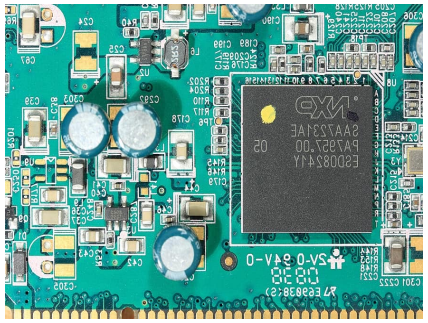


Physical Design



Fabricated Design

Packaged IC



Design Constraints

Functionality

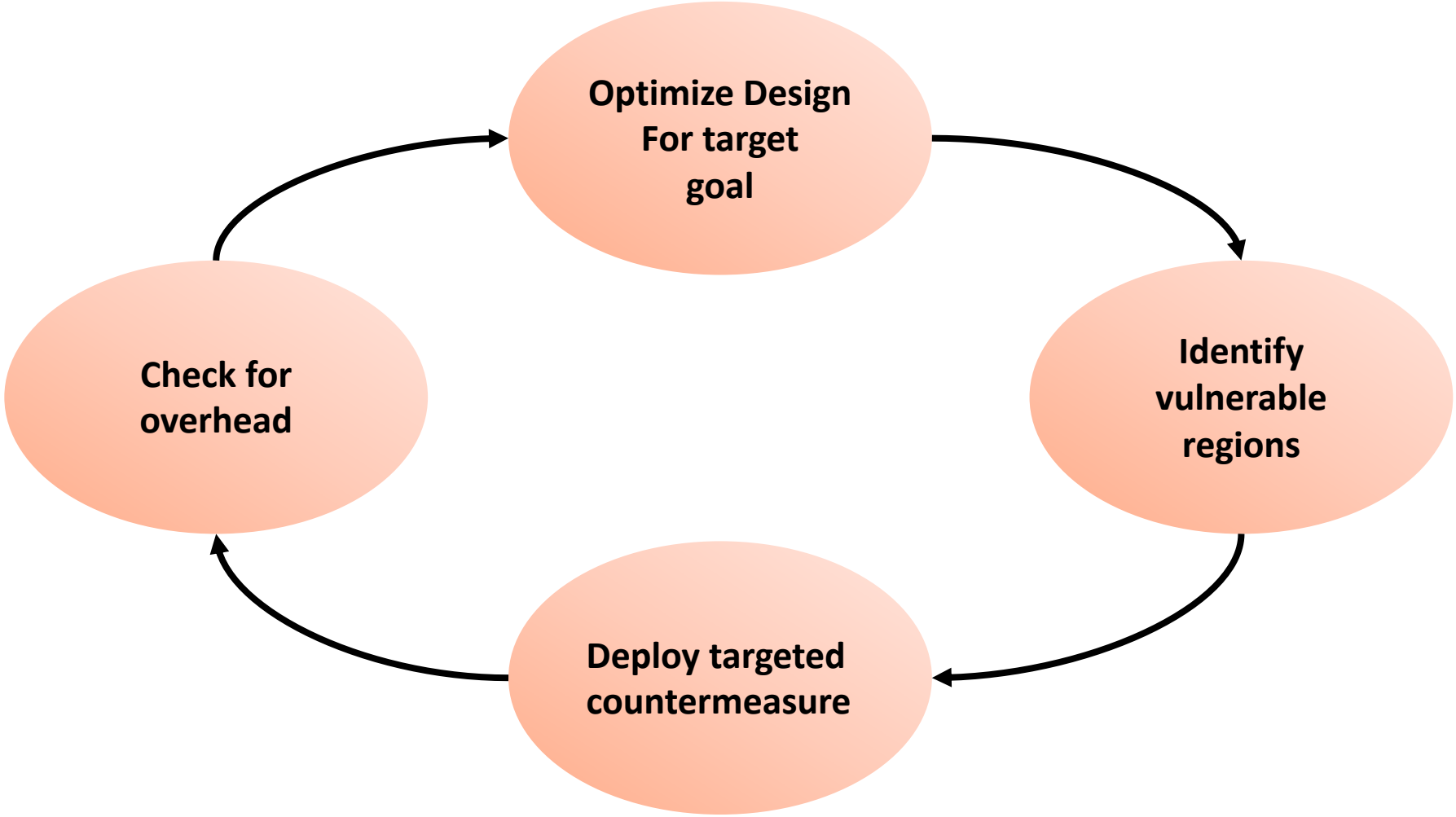
Functionality, Power Performance and Area

Functional Correctness

Functionality

- **Challenge 2:**
  - Current Design Flows do not allow for security optimizations
  - Security Integration is a separate process that needs to happen at each stage

Challenges for Trustworthy Hardware



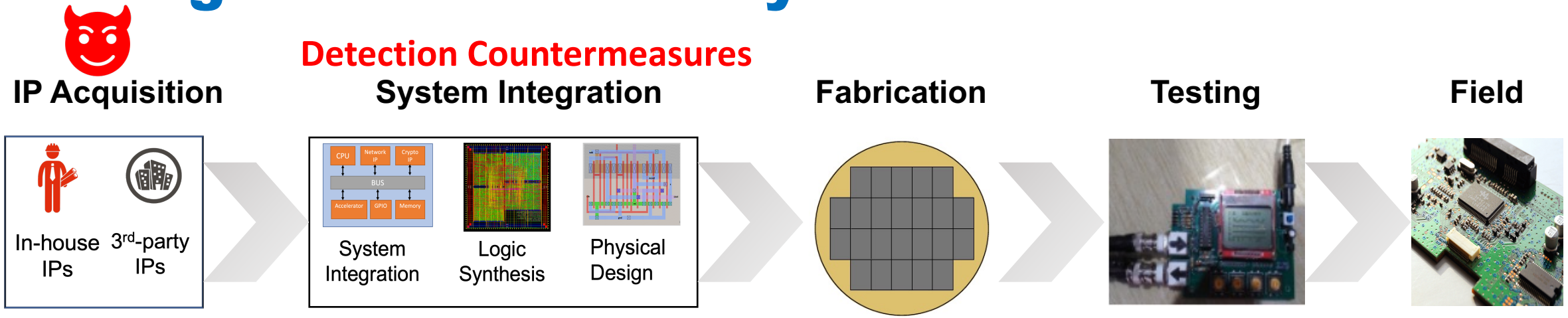
- **Challenge 3:**
  - Integrating security separately impacts the design constraints
  - Creates a cyclic dependency between design constraints and security

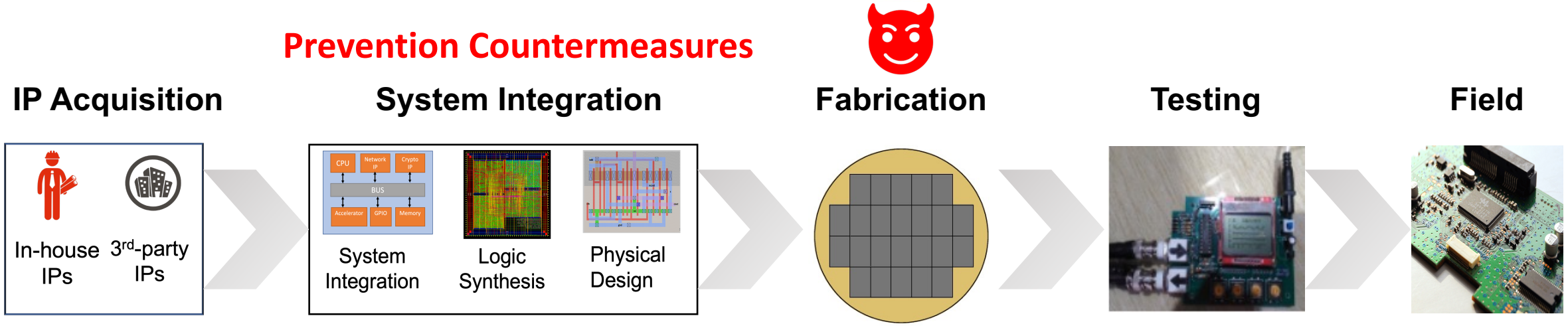
Challenges for Trustworthy Hardware

Delay	Power	Area	Memory	Security
Hz, ns, FLOPS, MBps, Cycle count	J, W, W/mm, W/cycle	Sq.mm, Gates/sq.mm, #AND gates	GBps, rpm, MB/GB	??

- **Challenge 4:**
  - Lack of a security metric makes it harder for design optimization
  - EDA tools can only optimize for power, performance or area not security
  - Makes it harder to quantify the impact of EDA optimizations on security

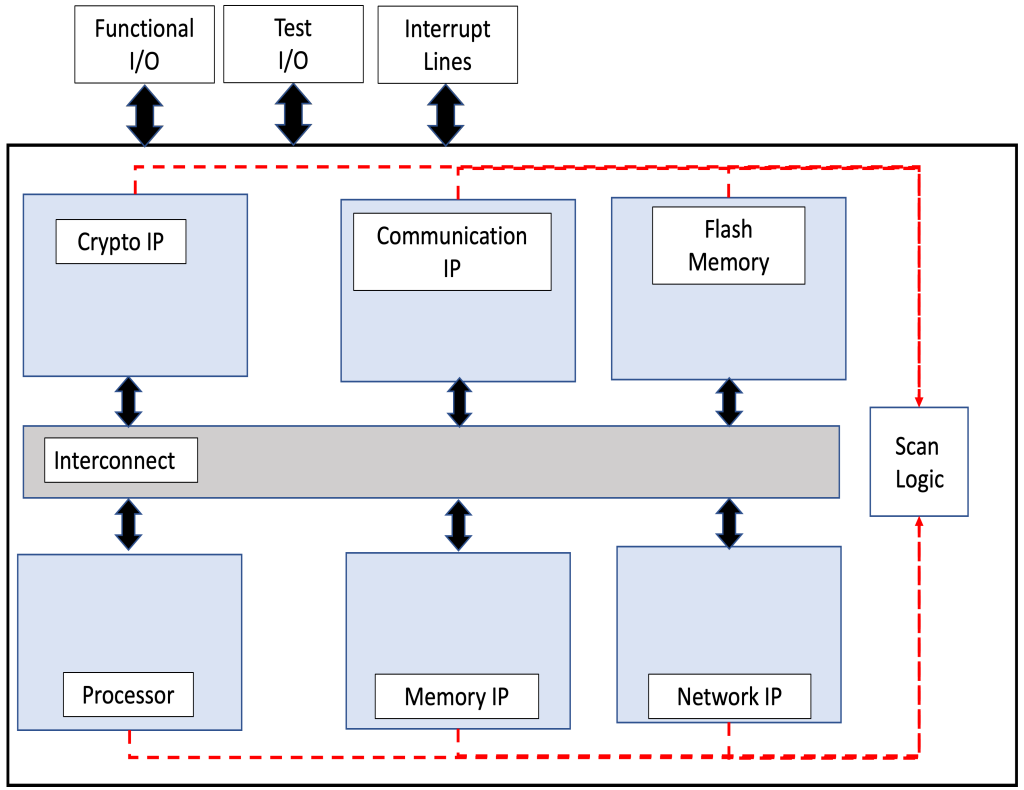
Challenges for Trustworthy Hardware

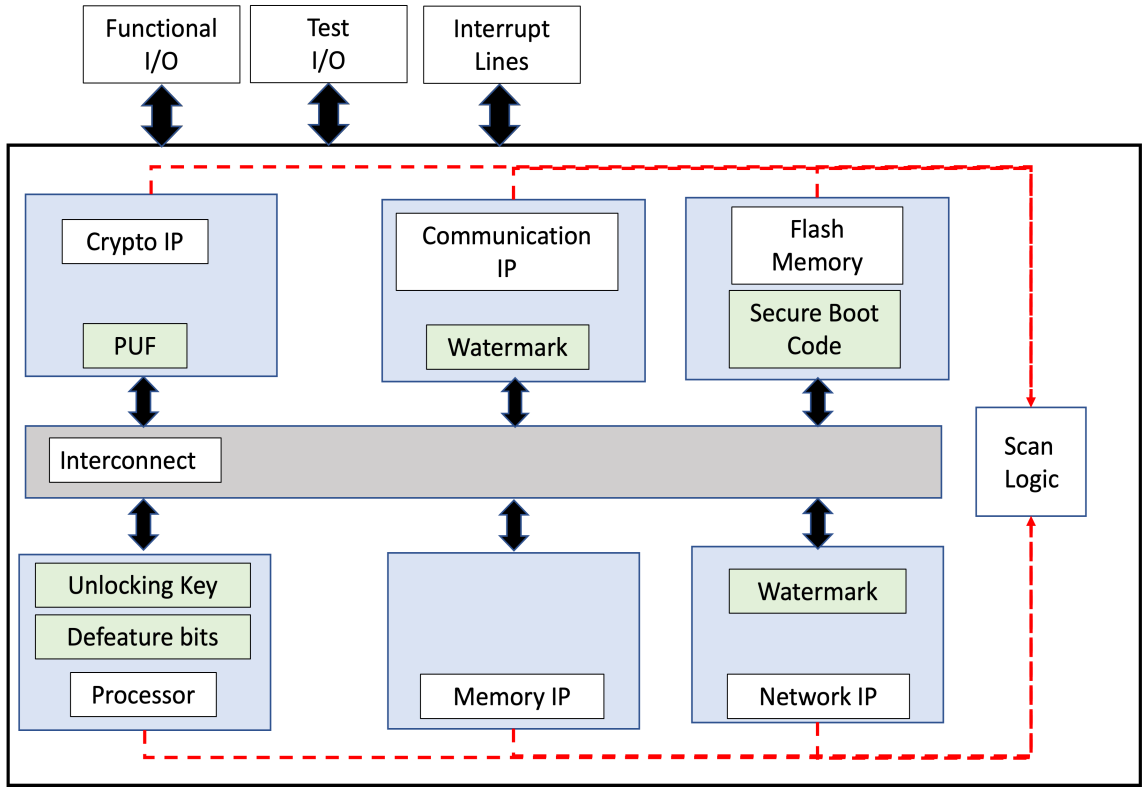


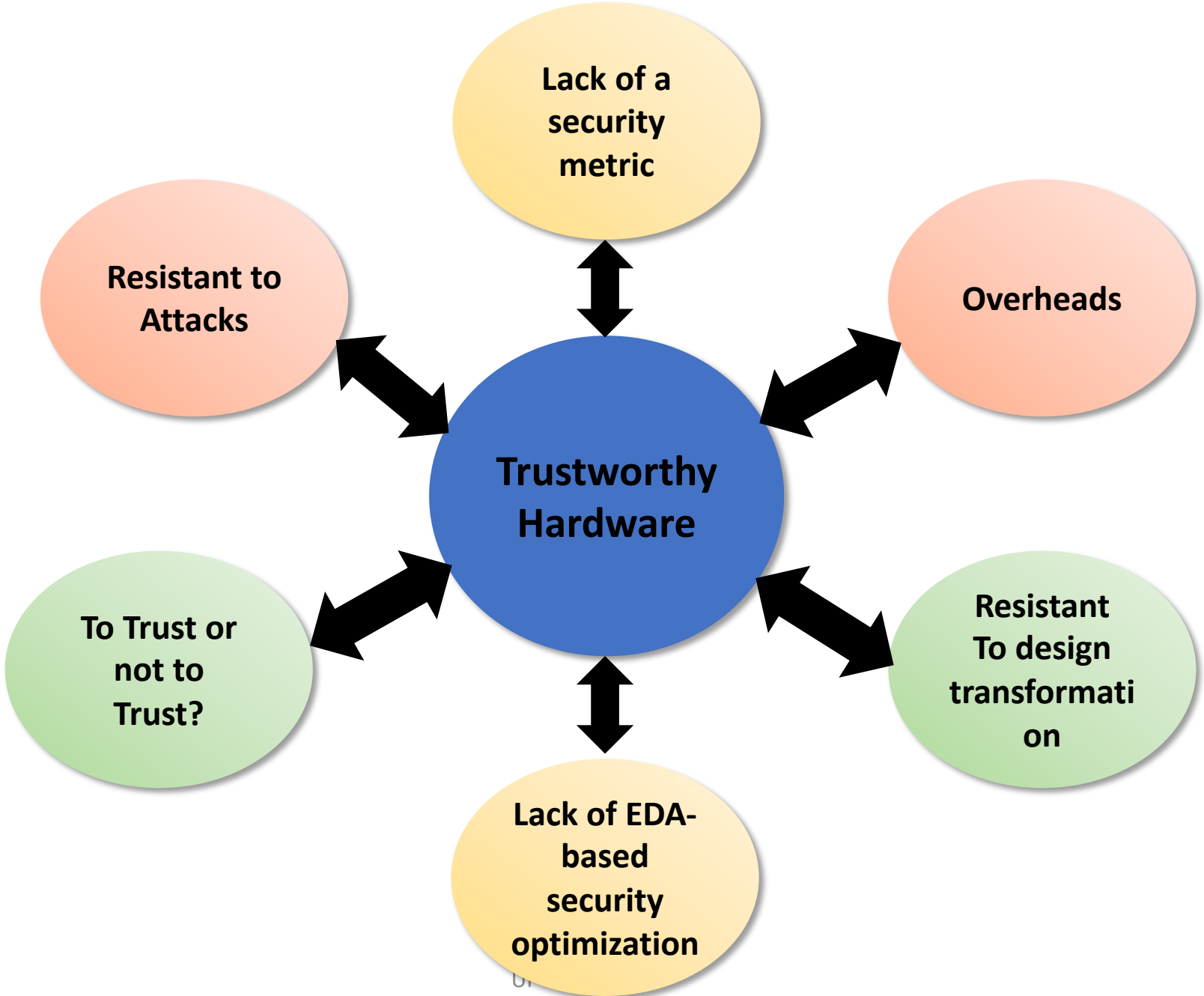


- **Challenge 5:**
  - To Trust or not to Trust?
  - Attacks in the upstream supply chain require detection techniques
  - Attacks in the downstream supply chain require prevention techniques

Challenges for Trustworthy Hardware





- **Challenge 6:**
  - Modern systems contain multiple IPs each with their own security constraints
  - Each IP can have its own distinct threat model
  - Overall security = IP-level security + overall SoC security
  - IP functionality constraints have to be respected
  - Integrating security individually creates provisioning challenges

Challenges for Trustworthy Hardware