UNIVERSITY OF WINDSOR
SHIELD
AUTOMOTIVE CYBERSECURITY
CENTRE OF EXCELLENCE

# SHIELD

## Automotive Cybersecurity Centre Of Excellence

University of Windsor

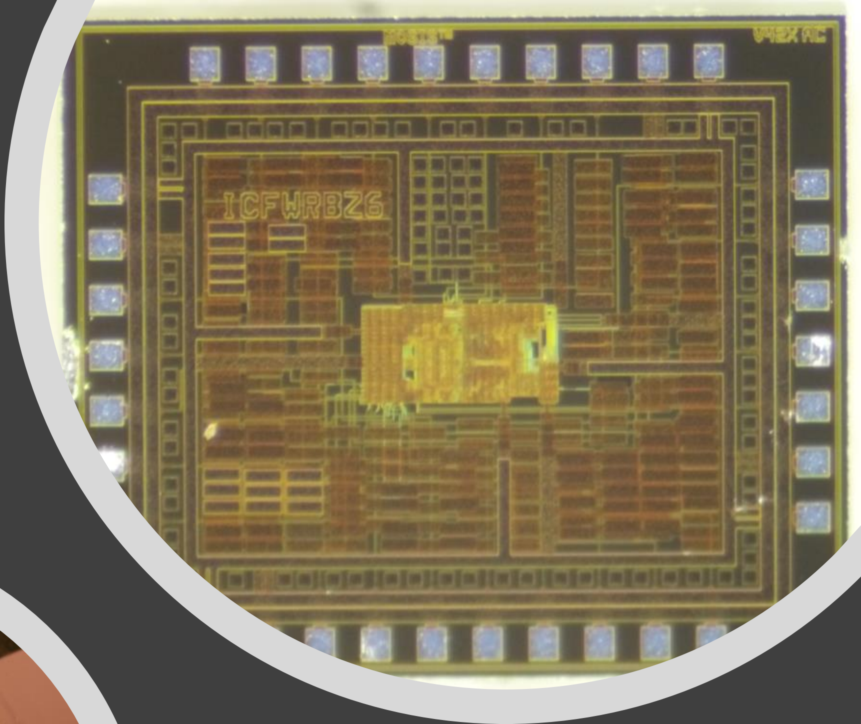
# Automobility In Windsor-Essex

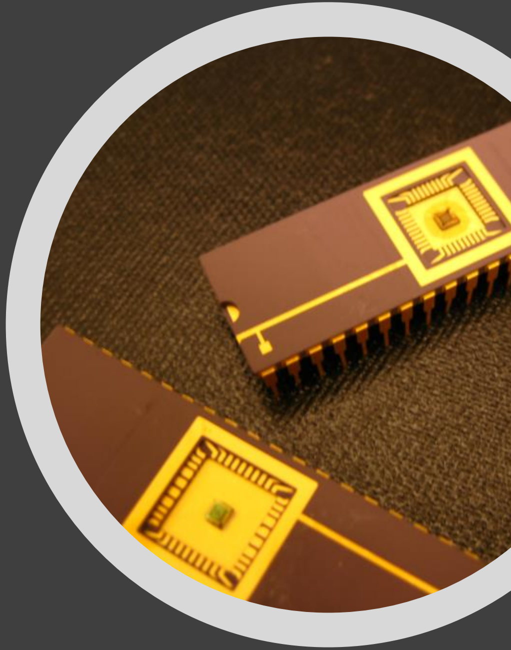
- Regional Economic Diversification and Growth Effort
- CASE emerging technologies
  - CONNECTED, AUTONOMOUS, SECURE & ELECTRIC
- Leveraging regional assets including:
  - Canada’s Largest publicly accessible virtual reality cave

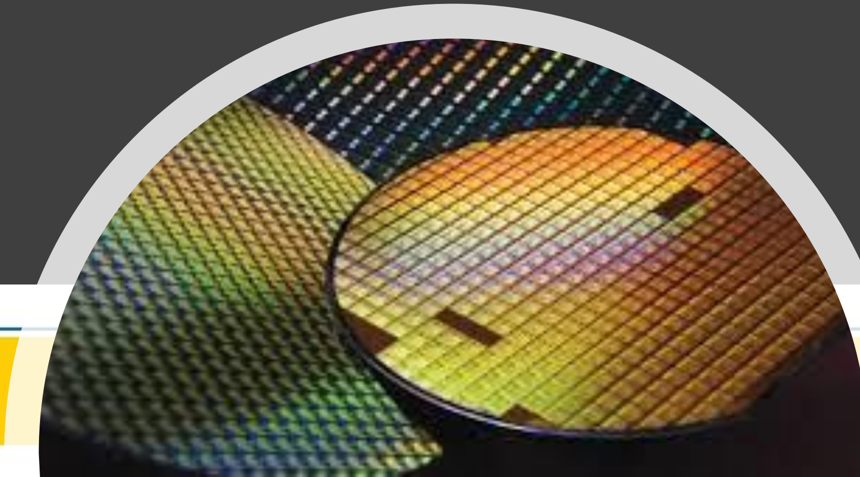
A center for mobility excellence in manufacturing and innovation
Attract businesses, develop industry ready talent, foster entrepreneurship and innovation

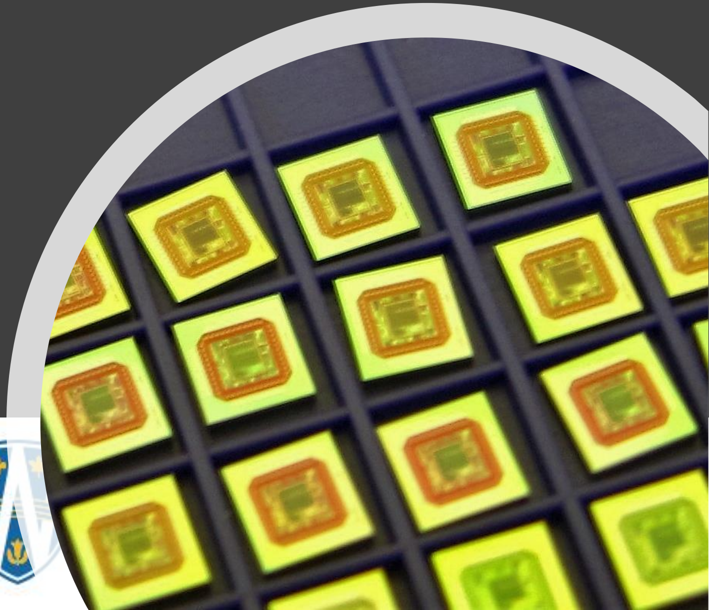
# Motivation

- With the rise of IoT, attacks on devices has a more devastating impact
  - Manufacturing of parts is not a horizontal line
    - Manipulating the devices by unknown, third-party manufacturing units is easier
  - Detection of Trojan Hardware is complicated, due to increased complexity of electronic devices









# Hardware Trojan War

# The one big threat when it comes to cyber-security has nothing to do with software

# Trojan Hardware

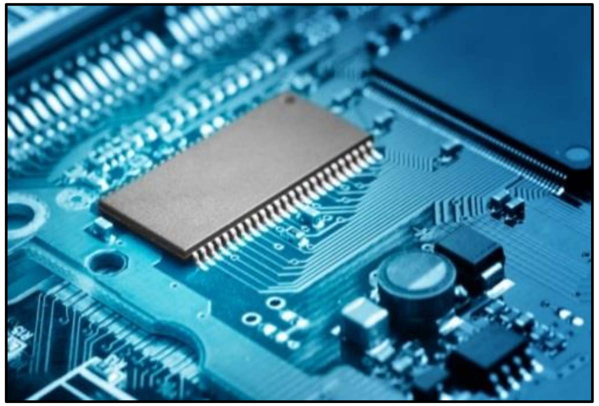
- Authenticity and integrity of hardware components in modern ICT systems
- Security challenged by improving attacks
- Recent trends:
  - “Hardware Trojans”: Hidden functions in Integrated Circuits

# Trojan Hardware

Modifications to circuitry by adversaries

to exploit hardware

or to use hardware mechanisms to gain access to data or software running on the chips

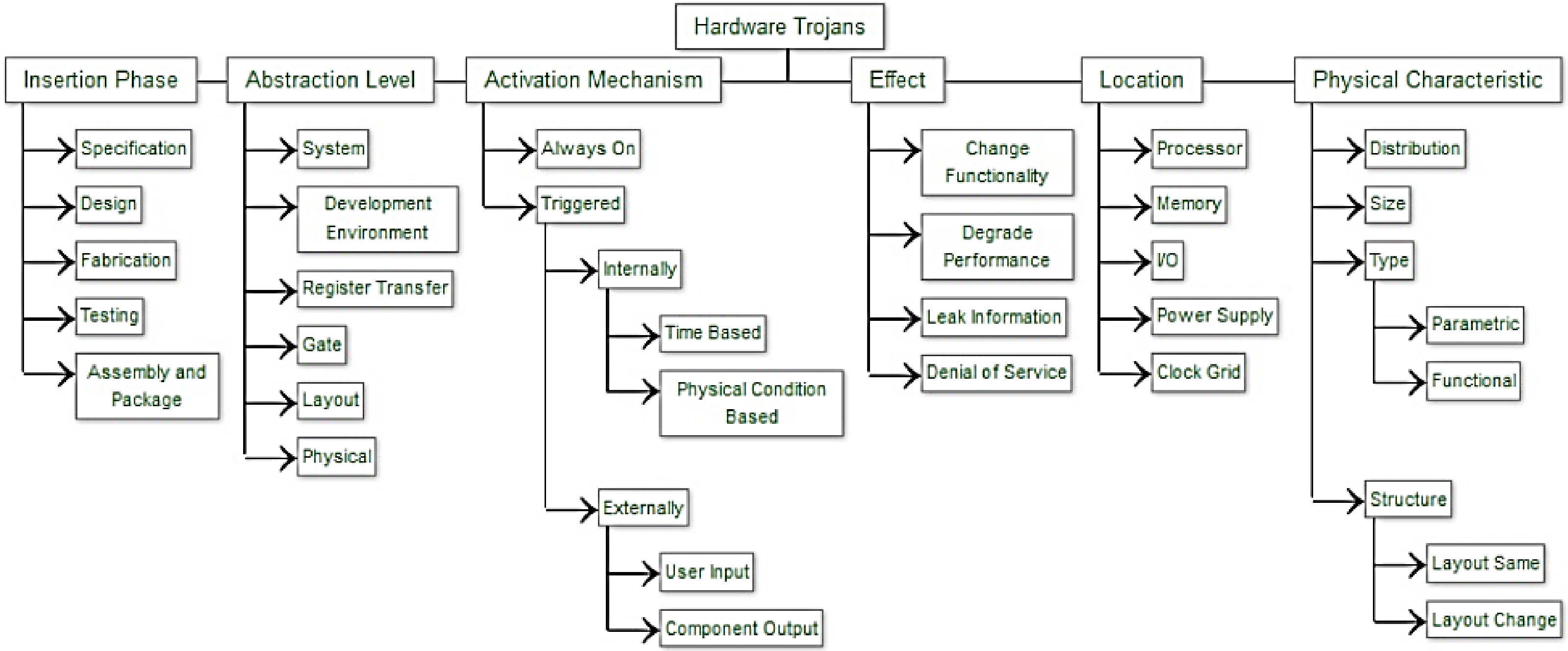


# Trojan Hardware

Designed to

- Disable or destroy a system at some future time
- Leak confidential information and secret keys covertly to an adversary.

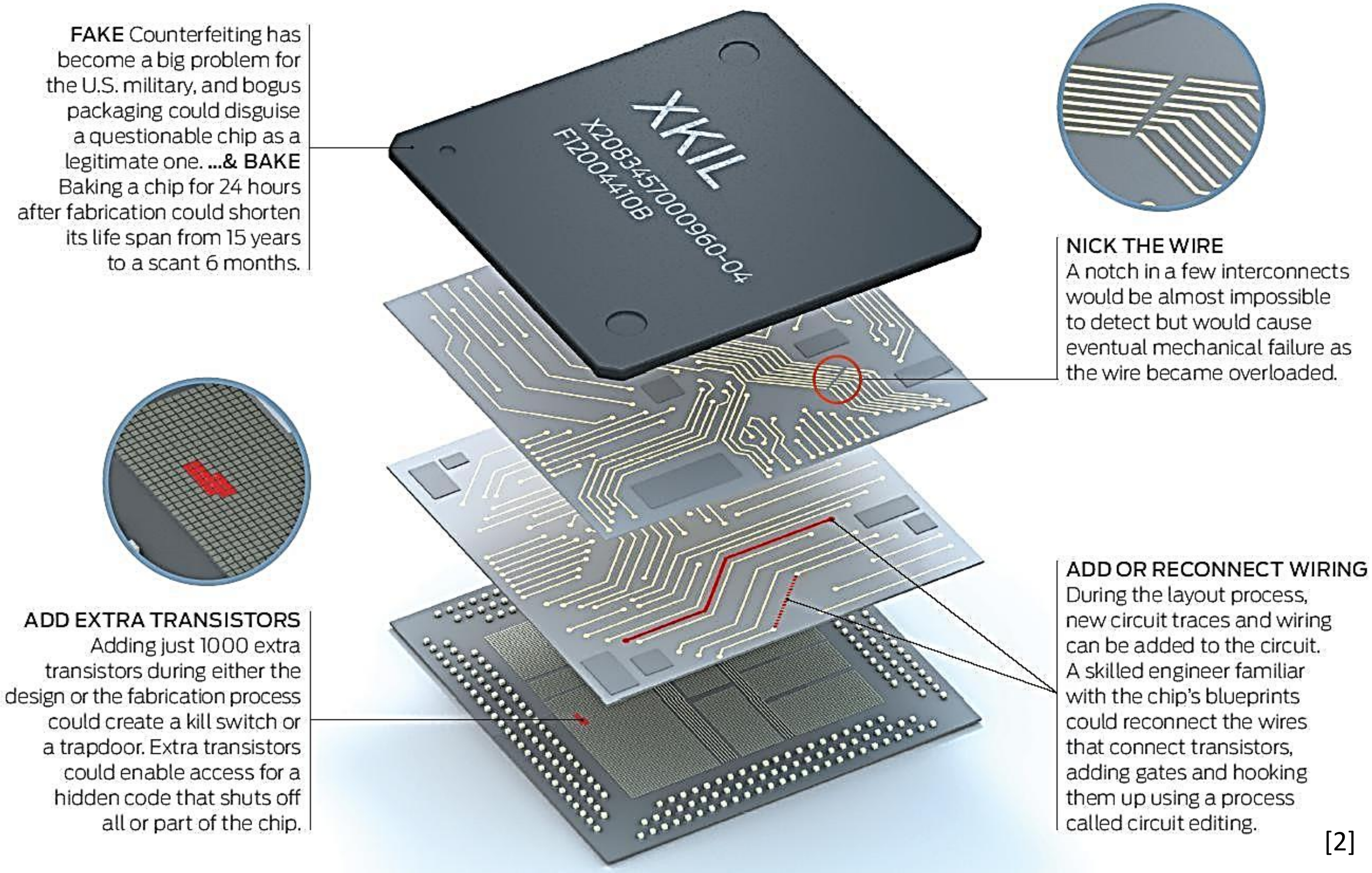
# Hardware Trojan Taxonomy



- Hardware Trojans
  - Insertion Phase
    - Specification
    - Design
    - Fabrication
    - Testing
    - Assembly and Package
  - Abstraction Level
    - System
    - Development Environment
    - Register Transfer
    - Gate
    - Layout
    - Physical
  - Activation Mechanism
    - Always On
    - Triggered
      - Internally
        - Time Based
        - Physical Condition Based
      - Externally
        - User Input
        - Component Output
  - Effect
    - Change Functionality
    - Degrade Performance
    - Leak Information
    - Denial of Service
  - Location
    - Processor
    - Memory
    - I/O
    - Power Supply
    - Clock Grid
  - Physical Characteristic
    - Distribution
    - Size
    - Type
      - Parametric
      - Functional
    - Structure
      - Layout Same
      - Layout Change

[1]

# Trojan Hardware



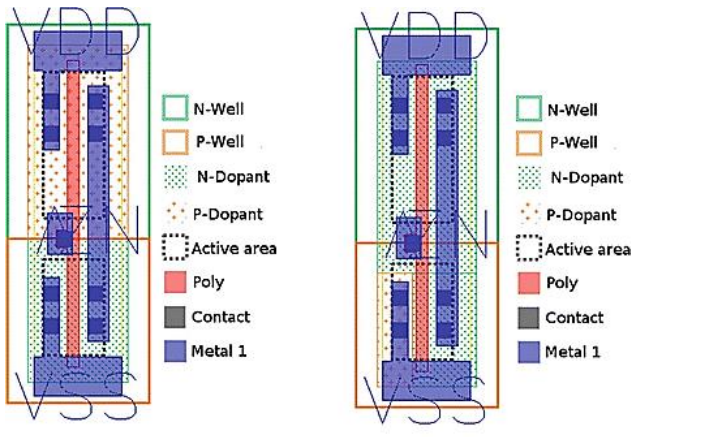
**FAKE** Counterfeiting has become a big problem for the U.S. military, and bogus packaging could disguise a questionable chip as a legitimate one. **...& BAKE** Baking a chip for 24 hours after fabrication could shorten its life span from 15 years to a scant 6 months.

**NICK THE WIRE**
A notch in a few interconnects would be almost impossible to detect but would cause eventual mechanical failure as the wire became overloaded.

**ADD EXTRA TRANSISTORS**
Adding just 1000 extra transistors during either the design or the fabrication process could create a kill switch or a trapdoor. Extra transistors could enable access for a hidden code that shuts off all or part of the chip.

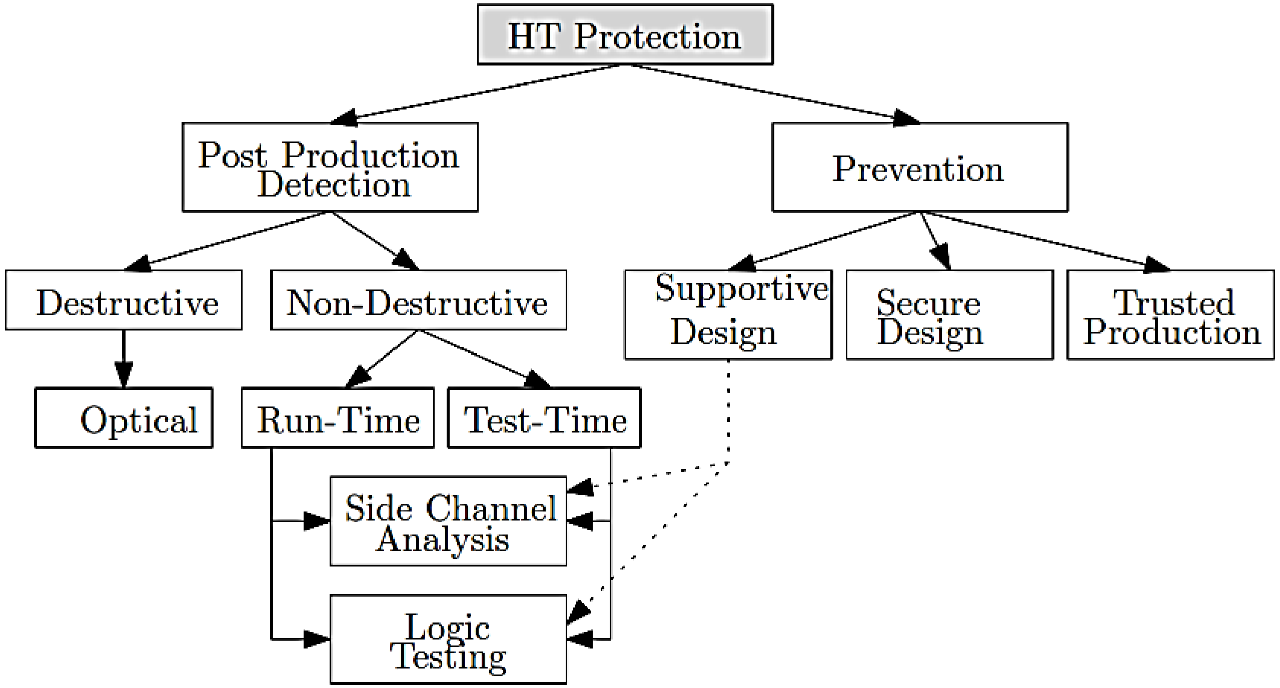
**ADD OR RECONNECT WIRING**
During the layout process, new circuit traces and wiring can be added to the circuit. A skilled engineer familiar with the chip's blueprints could reconnect the wires that connect transistors, adding gates and hooking them up using a process called circuit editing.

[2]



**(a)** Original **(b)** Trojan

# Detection


HT Protection
Post Production Detection
Prevention
Destructive
Non-Destructive
Supportive Design
Secure Design
Trusted Production
Optical
Run-Time
Test-Time
Side Channel Analysis
Logic Testing

[3]

# Summary

- Hardware Trojans are real threats for integrated circuits
  - No HT detection method of the state-of-the-art is 100% successful
- 3lines of defense:
  - Design for Hardware Trust
  - Test-Time Methods
  - Run-Time Methods

# Challenges

- Challenges:
  - Tiny: several gates within millions of gates
  - Quiet: hard-to-activate (rare event) or triggered itself (time-bomb)
  - Hard to model: human intelligence
  - Conventional test and validation approaches fail to reliably detect hardware Trojans.
    - Focus on manufacture defects and does not target detection of additional functionality in a design

# New Challenges

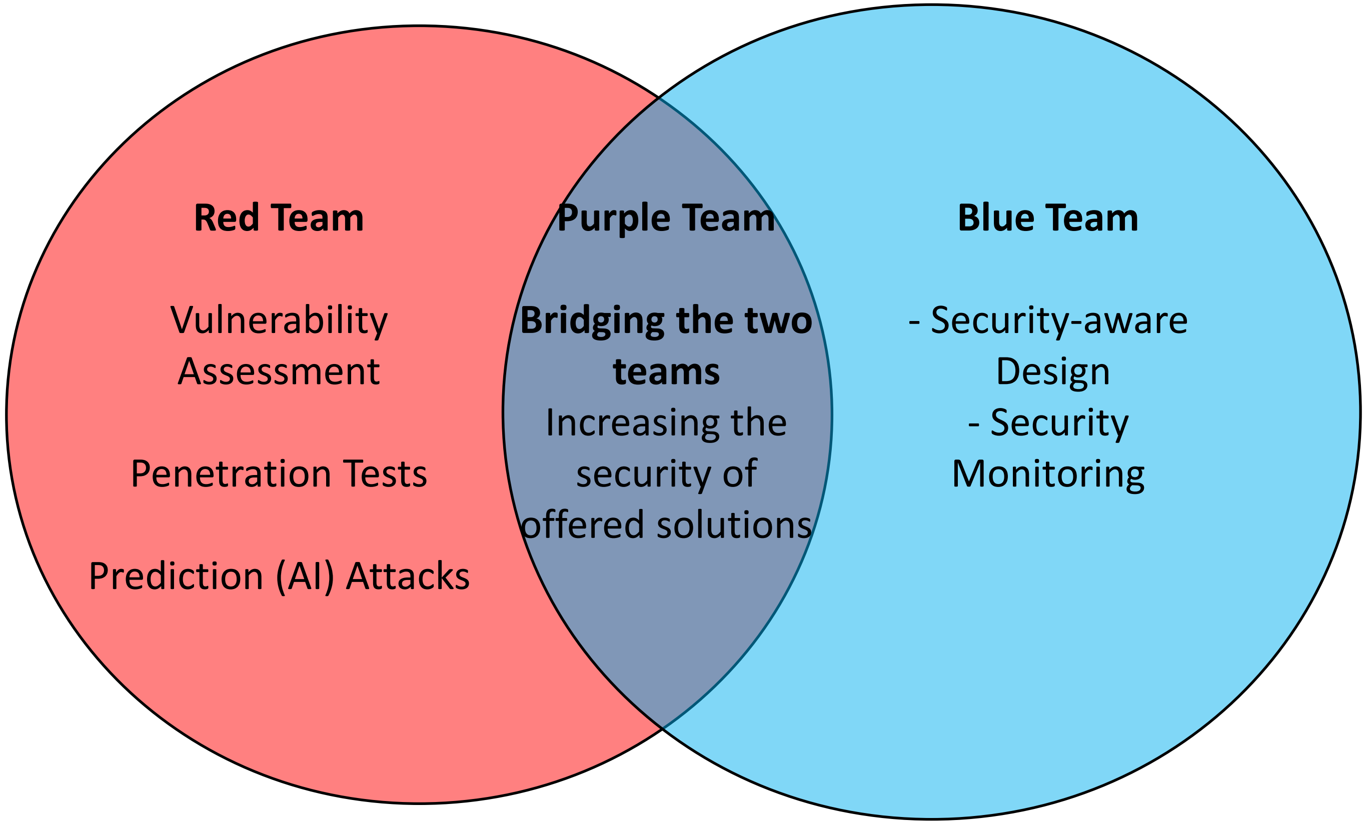
- New and more stealthy attacks are found out
  - No need of adding additional circuitry to the target design
  - Attacks are developed by modifying the dopant polarity of existing transistors
  - The modified circuit appears legitimate on all wiring layers (including all metal and polysilicon)
    - Resistant to most detection techniques, including fine-grain optical inspection and checking against “golden chips”

# Research Approach

- Hardware development, with security concerns upfront in the design process
  - Prototyping and test operations of the developed hardware
- Creating Blue/Red/Purple team approach to ensure of the security
  - One of the only academic teams in Canada, adopting this approach

# Research Approach

UNIVERSITY OF WINDSOR
SHIELD
AUTOMOTIVE CYBERSECURITY
CENTRE OF EXCELLENCE



**Red Team**

Vulnerability Assessment

Penetration Tests

Prediction (AI) Attacks

**Purple Team**

**Bridging the two teams**
Increasing the security of offered solutions

**Blue Team**

- Security-aware Design
- Security Monitoring