# Security and Energy Tradeoffs in Consumer Electronics

Keynote – ZINC 2018

31st May 2018

Novi Sad, Serbia

Saraju P. Mohanty

University of North Texas, USA.

**Email: saraju.mohanty@unt.edu**

**More Info: http://www.smohanty.org**

# Talk - Outline

- Big picture of current trends in CE
- Challenges in the current generation CE design
- Security, Privacy, IP Rights solutions
- Energy consumption solutions
- Hardware vs Software in CE for tradeoffs
- Conclusions and Future Directions

# Big Picture

# Smart Cities

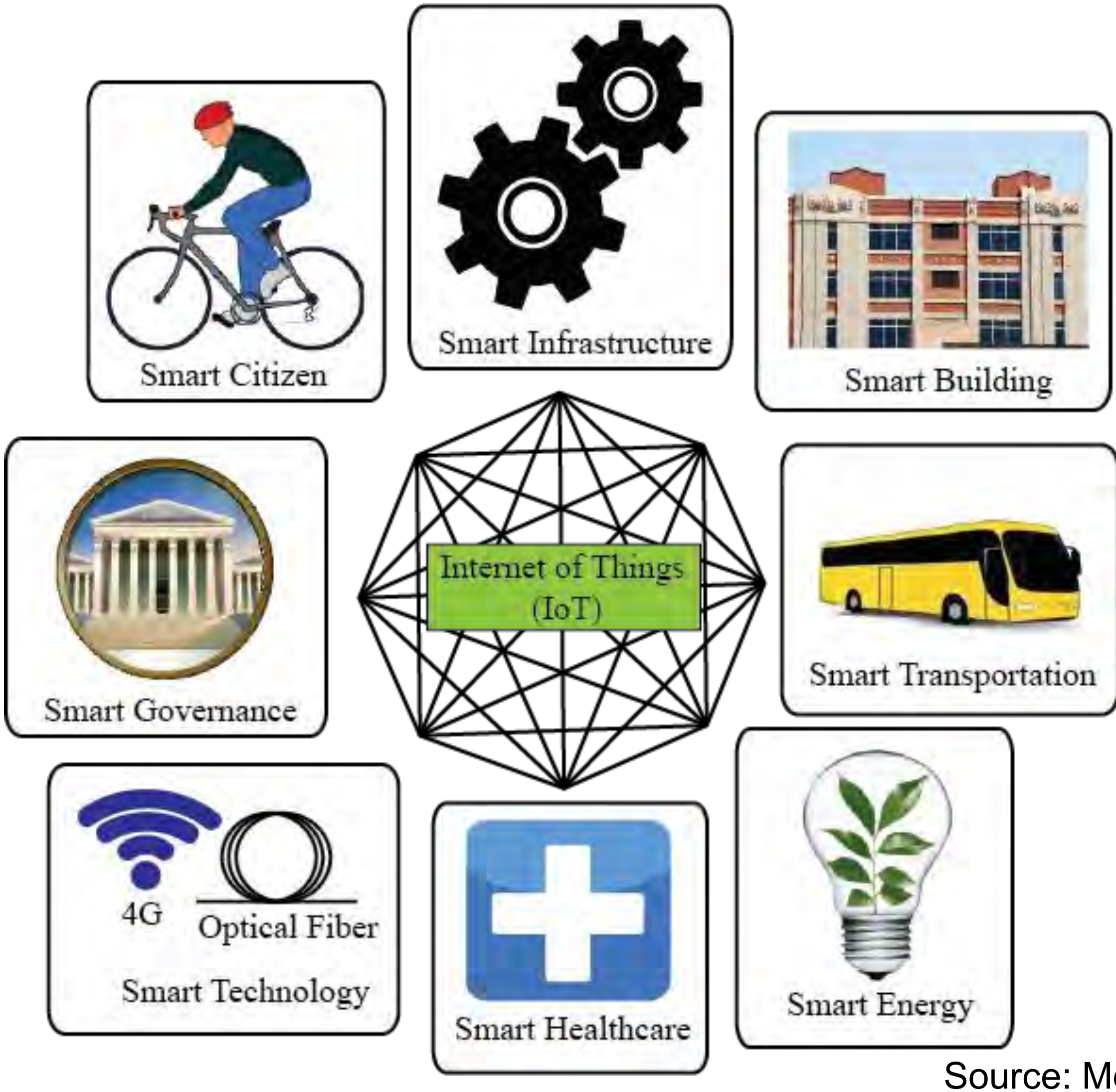
- Smart Cities: For effective management of limited resource to serve largest possible population to improve:
  - Livability
  - Workability
  - Sustainability

“Cities around the world could spend as much as $41 trillion on smart tech over the next 20 years.”

Source: http://www.cnbc.com/2016/10/25/spending-on-smart-cities-around-the-world-could-reach-41-trillion.html


July 2016

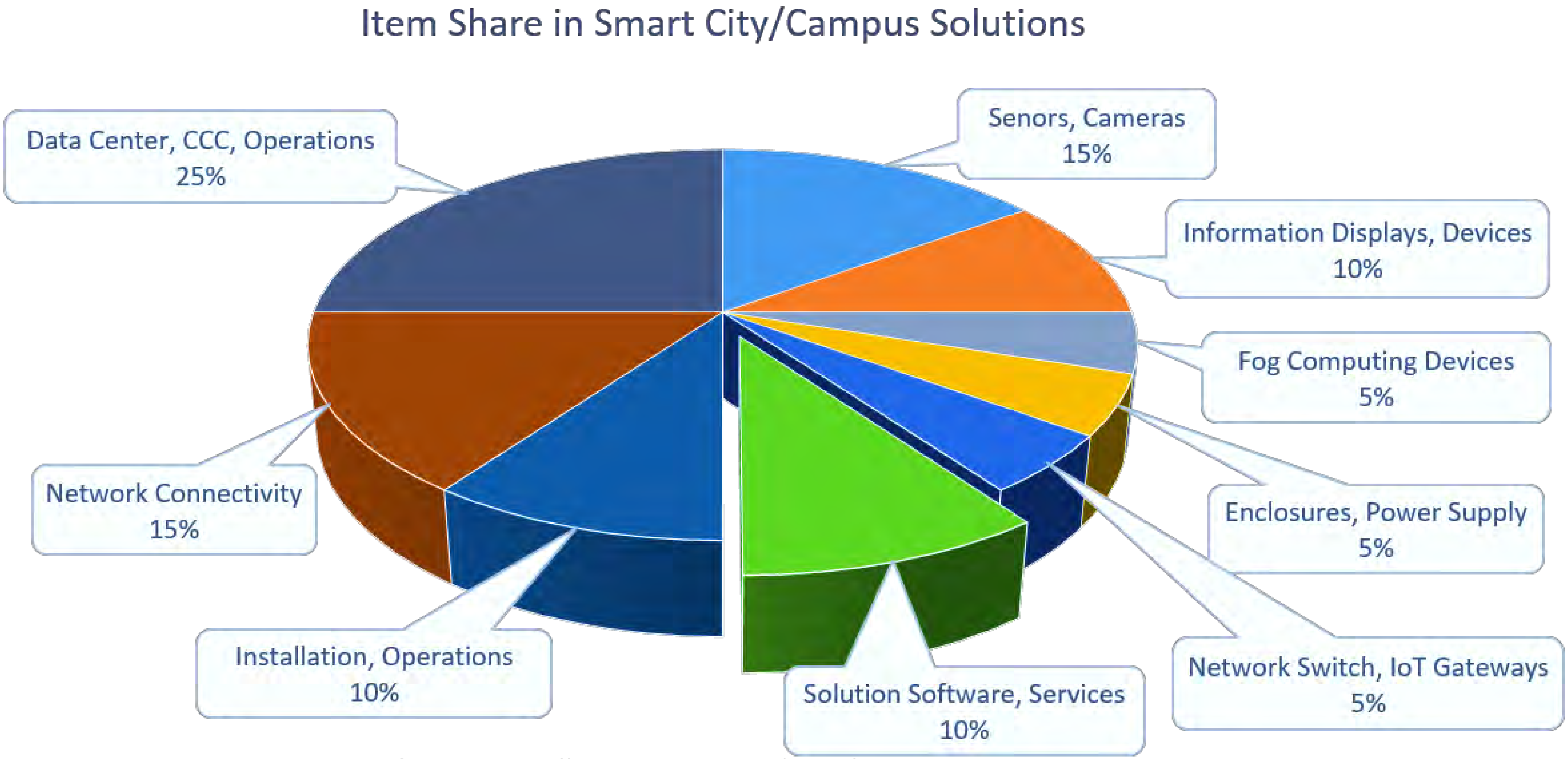
# IoT is the Backbone Smart Cities




A smart city can have one or more of the smart components.

Source: Mohanty 2016, CE Magazine July 2016

# Smart City Design - Verticals




Source: https://www.linkedin.com/pulse/smart-citiescampus-what-could-your-share-suresh-kumar-kk

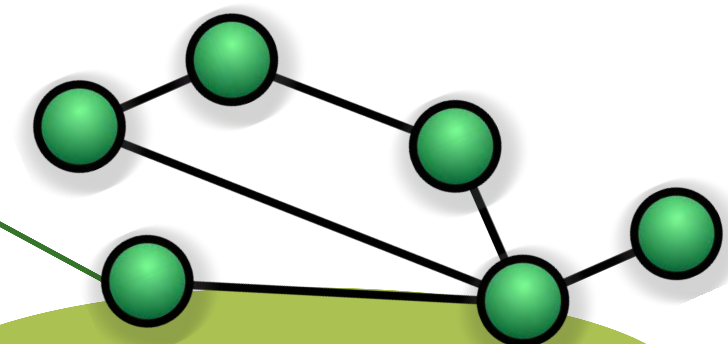
# Smart Cities - 3 Is


Instrumentation

The 3Is are provided by the Internet of Things (IoT).

Smart Cities

Intelligence



Interconnection

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

# Internet of Things (IoT) - History


Source: http://events.linuxfoundation.org/sites/events/files/slides/Design%20-%20End-to-End%20%20IoT%20Solution%20-%20Shivakumar%20Mathapathi.pdf

# Internet of Things (IoT) – Concept

**Things**
Sensors/actuators with IP address that can be connected to Internet

**Local Network**
Can be wired or wireless: LAN, Body Area Network (BAN), Personal Area Network (PAN), Controller Area Network (CAN)

**Cloud Services**
Data either sent to or received from cloud (e.g. machine activation, workflow, and analytics)

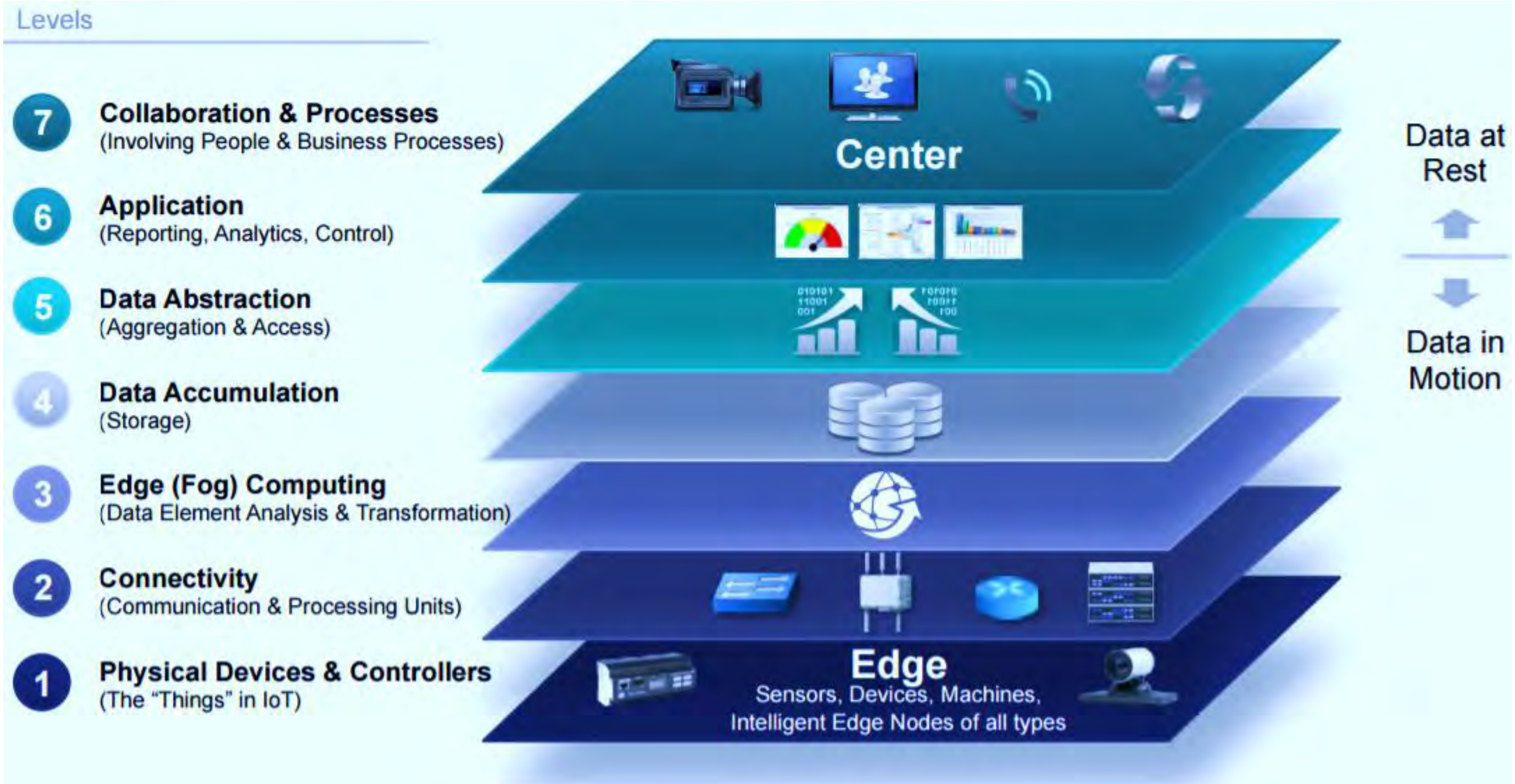
**Global Network**
Connecting bridge between the local network, cloud services and connected consumer devices

**Connected Consumer Electronics**
Smart phones, devices, cars, wearables which are connected to the Things

Overall architecture:
- A configurable dynamic global network of networks
- Systems-of-Systems

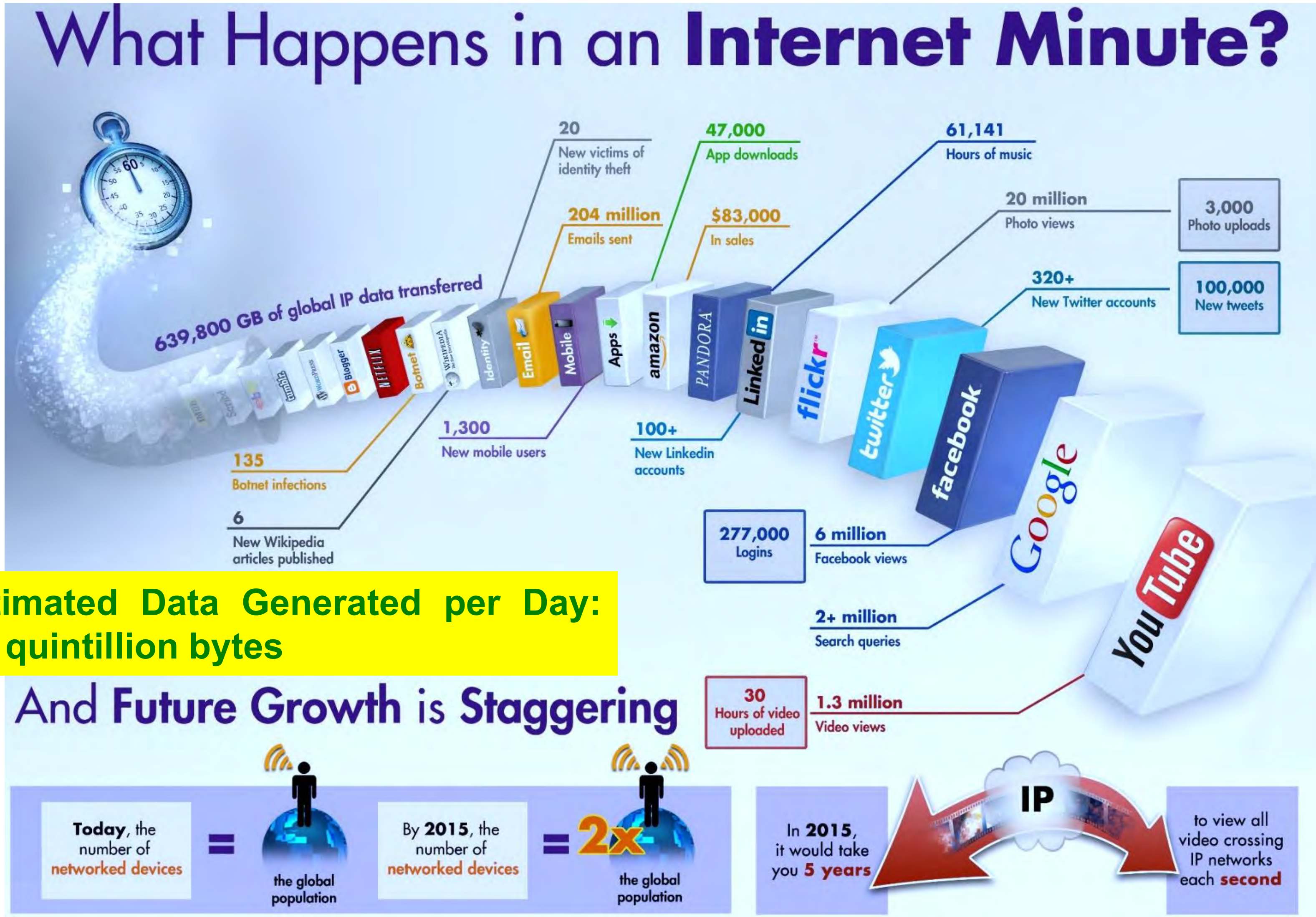
Source: Mohanty ICIT 2017 Keynote

# IoT Architecture - 7 Level Model




Source: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

# Huge Amount of Data




**Estimated Data Generated per Day: 2.5 quintillion bytes**

# Data is Most Valuable


"The world's most valuable resource is no longer oil, but data"

Source: http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

# Issues Challenging Sustainability

➢ Cyber Attacks

**Hacked:** US Department Of Justice

**Who did it:** Unknown

**What was done:** Information on 10,000 DHS and 20,000 FBI employees.

**Details:** The method of the attack is still a mystery and it's been said that it took a week for the DOJ to realize that the info had been stolen.

February 2016

**Hacked:** Yahoo #2

**Who did it:** Unknown

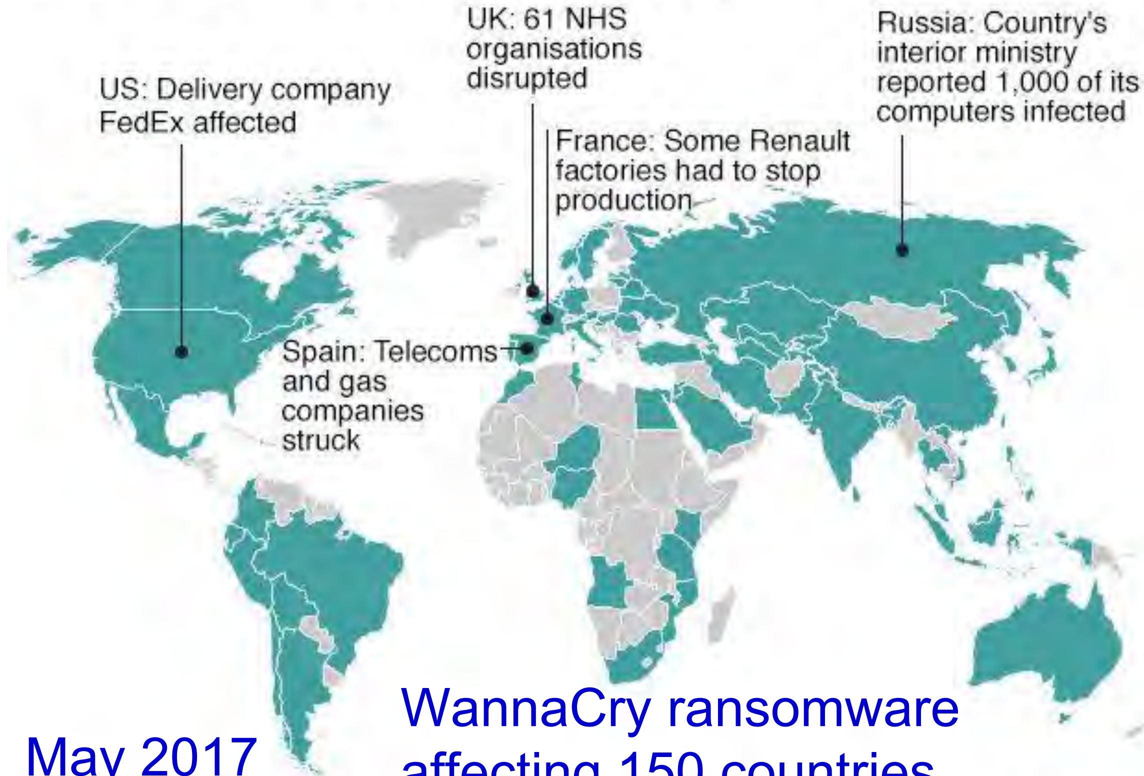
**What was done:** 1 billion accounts were compromised.

**Details:** Users names, email addresses, date of birth, passwords, phone numbers, and security questions were all taken.

December 2016

Source: https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/#73bb0bee48e3

**Countries hit in initial hours of cyber-attack**




May 2017

WannaCry ransomware affecting 150 countries

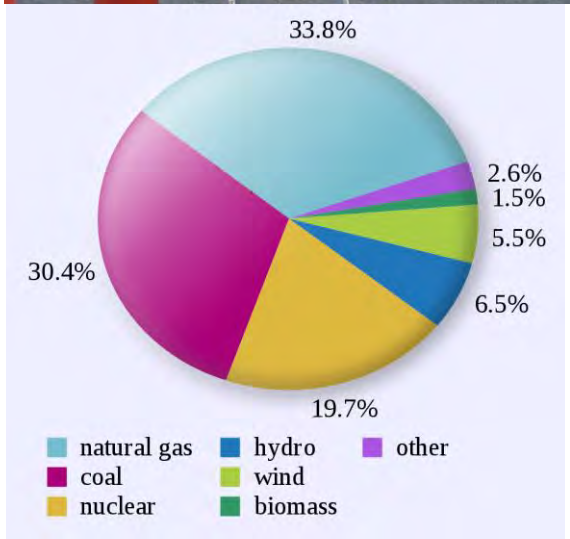
*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team BBC

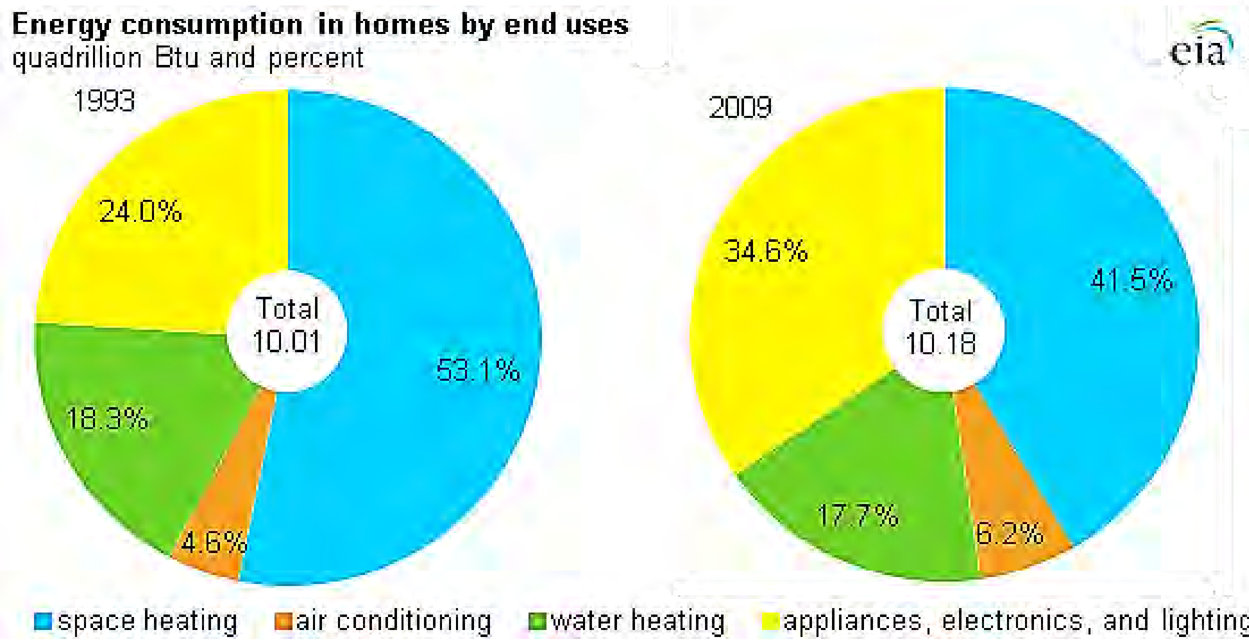
Source: http://www.bbc.com/news/technology-39920141

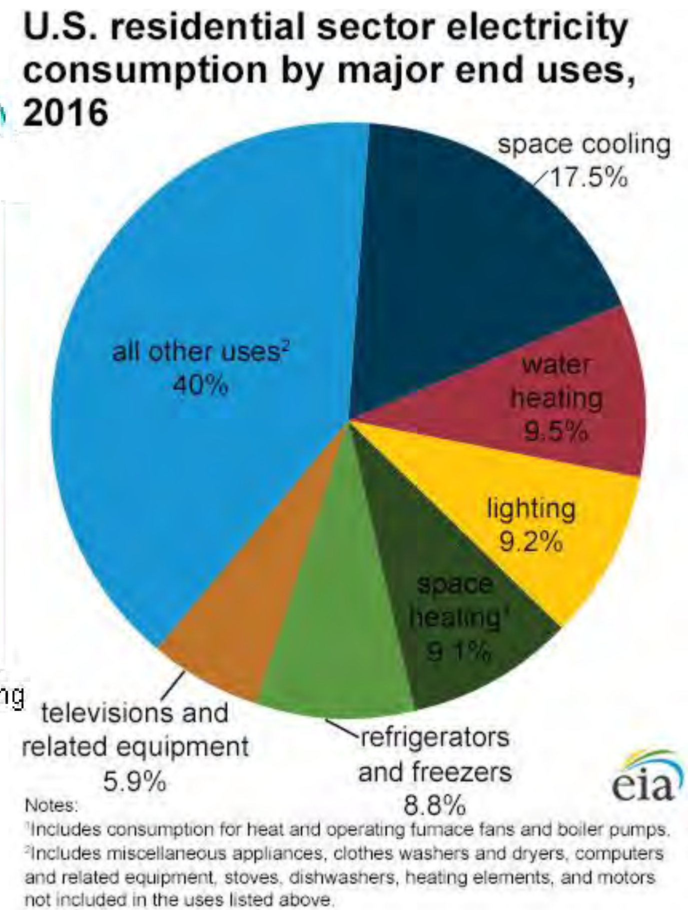
# Issues Challenging Sustainability


- Energy Crisis




# Consumer Electronics Demand More and More Energy



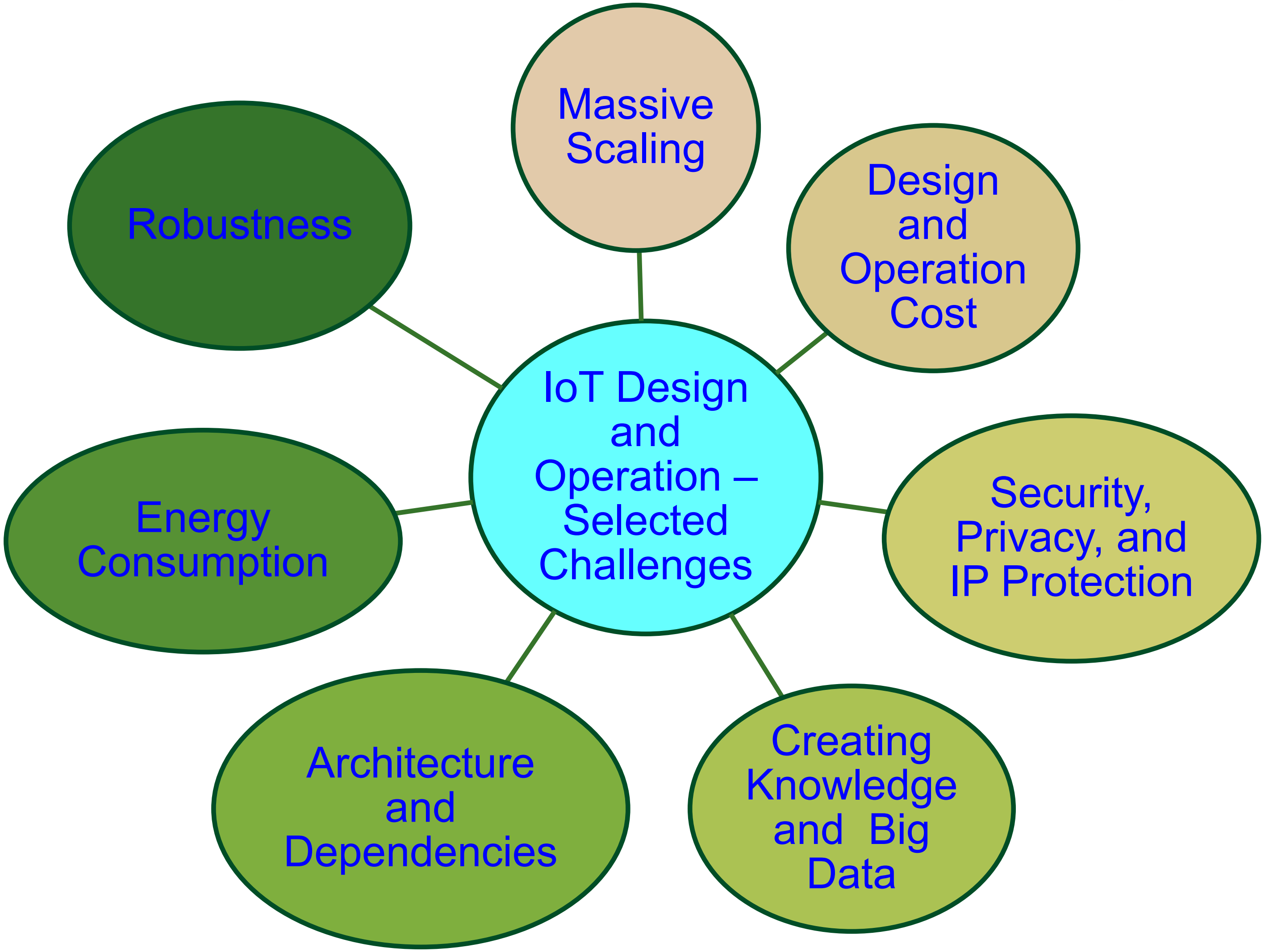




Quadrillion BTU (or quad): 1 quad = $10^{15}$ BTU = 1.055 Exa Joule (EJ).

**Source**: U.S. Energy Information Administration

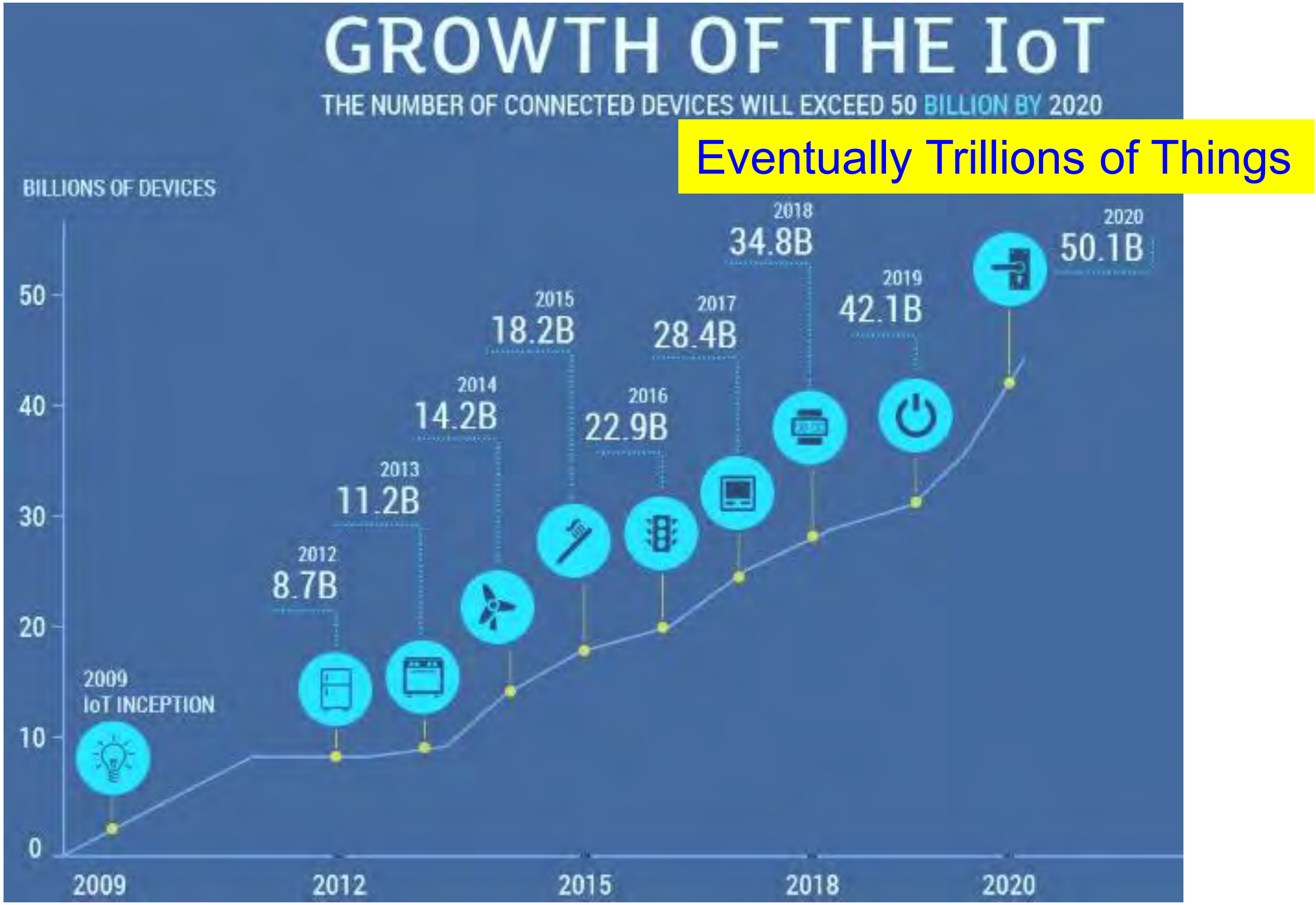
# Challenges in Current Generation CE Design

# IoT – Selected Challenges




Source: Mohanty ICIT 2017 Keynote

# Massive Scaling




Source: https://www.linkedin.com/pulse/history-iot-industrial-internet-sensors-data-lakes-0-downtime

# Design and Operation Cost

- The design cost is a one-time cost.
- Design cost needs to be small to make a IoT realization possible.
- The operations cost is that required to maintain the IoT.
- A small operations cost will make it easier to operate in the long run with minimal burden on the budget of application in which IoT is deployed.

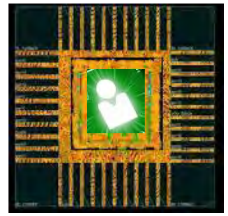

Source: http://www.industrialisation-produits-electroniques.fr

“Cities around the world could spend as much as $41 trillion on smart tech over the next 20 years.”

Source: http://www.cnbc.com/2016/10/25/spending-on-smart-cities-around-the-world-could-reach-41-trillion.html

# Security, Privacy, and IP Rights

Hardware
Trojan



Counterfeit
Hardware


July 2017

Source: Mohanty ICIT 2017 Keynote

# Security Challenge – Information

Online Banking

...

Credit Card Theft


**Hacked:** Linkedin, Tumbler, & Myspace

Linkedin
tumblr.
myspace

**Who did it:** A hacker going by the name Peace.

**What was done:** 500 million passwords were stolen.

**Details:** Peace had the following for sale on a Dark Web Store:

167 million Linkedin passwords
360 million Myspace passwords
68 million Tumbler passwords
100 million VK.com passwords
71 million Twitter passwords

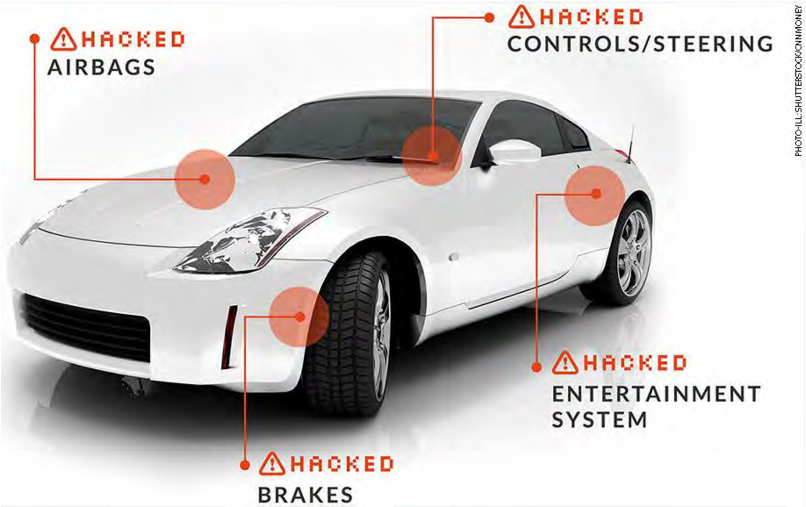
Personal Information

Credit Card/Unauthorized Shopping

# Security Challenge - System …

Power Grid Attack

Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html




Source: http://money.cnn.com/2014/06/01/technology/security/car-hack/


Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

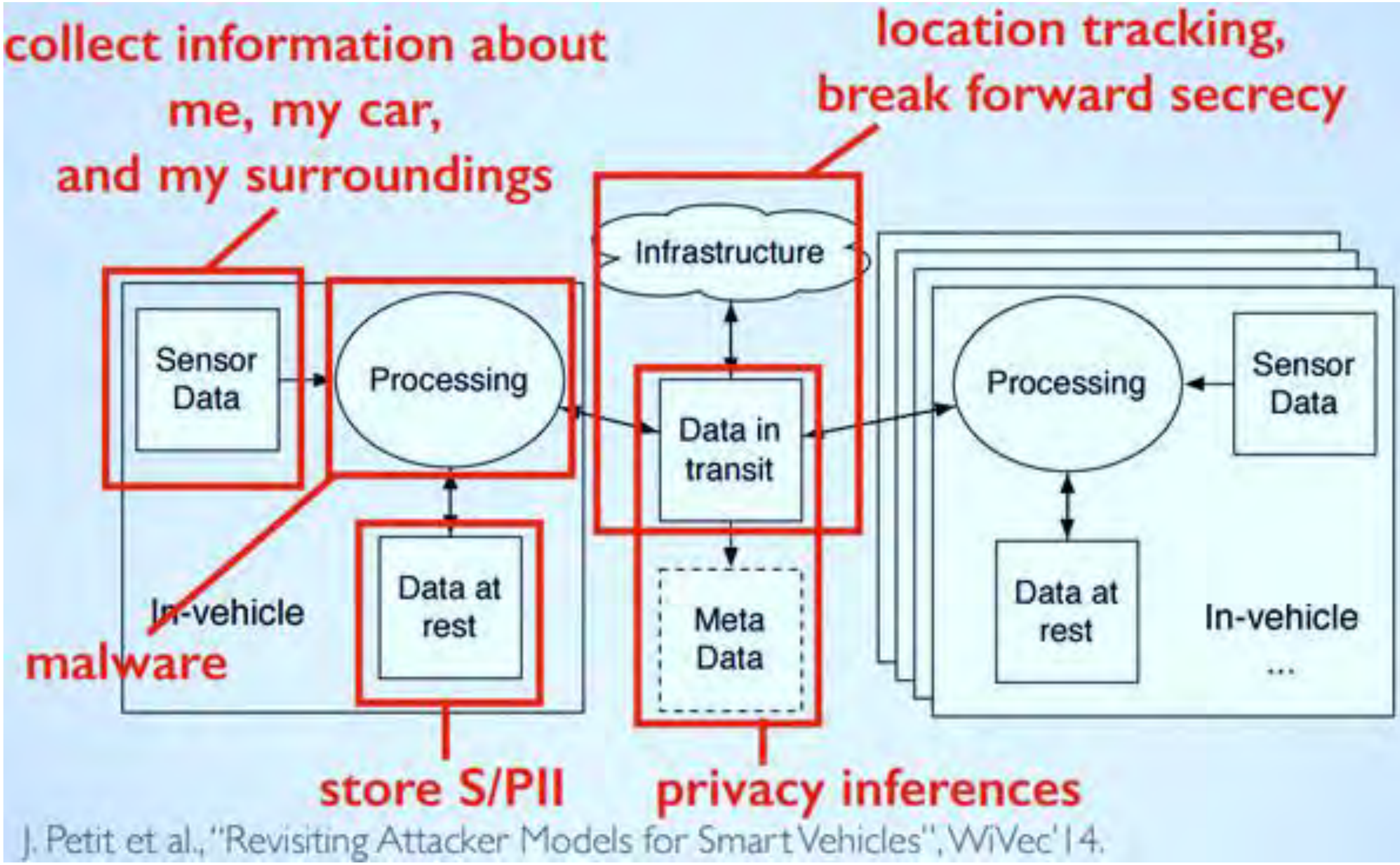
# Privacy Challenge - Information



Source: http://ciphercloud.com/three-ways-pursue-cloud-data-privacy-medical-records/

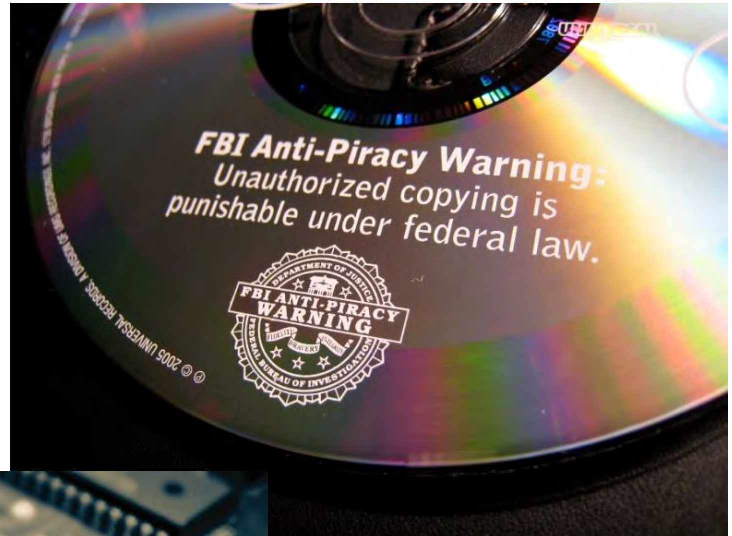

Source: http://blog.veriphyr.com/2012/06/electronic-medical-records-security-and.html

# Privacy Challenge – System, Smart Car

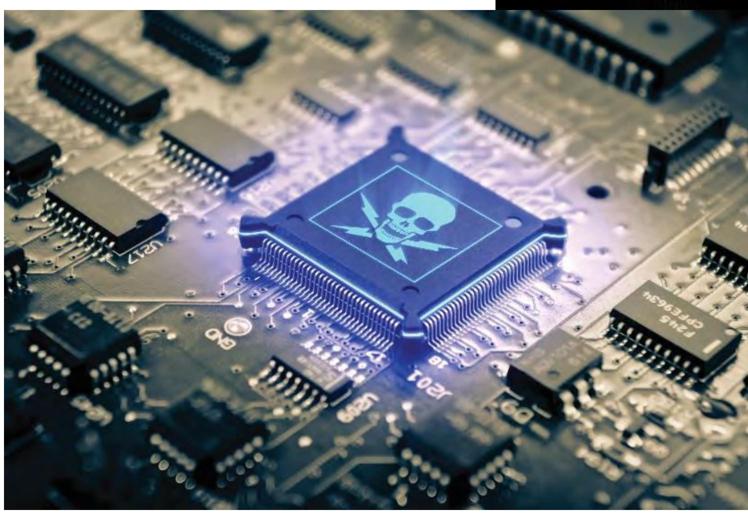



Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

# Ownership - Media, Hardware, Software




Media Piracy



Hardware Piracy → Counterfeit Hardware

Software Piracy

# Media Piracy – Movie/Video

High

Studio

Cinema

On-line

Video on Demand

DVD/Blu-ray

Pay-TV Broadcasting

Free-to-Air Broadcasting

Low

Piracy Threat Level


"Film piracy cost the US economy $20.5 billion annually."

Source: http://www.ipi.org/ipi_issues/detail/illegal-streaming-is-dominating-online-piracy

# Counterfeit Hardware Challenge

2014 Analog Hardware Market (Total Shipment Revenue US $)

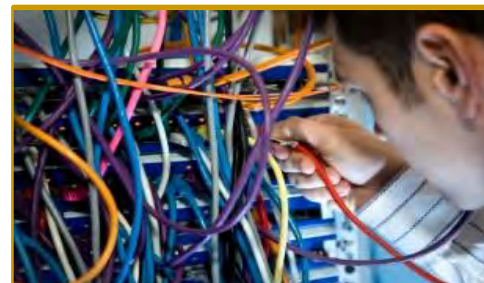
Wireless Market
$18.9 billion (34.8%)

Consumer Electronics
$9.0 billion (16.6%)

Industrial Electronics
$8.9 billion (16.5%)

Automotive
$8.5 billion (15.7%)

Data Processing
$6.0 billion (11%)



Wired Communications
$2.9 billion (5.4%)

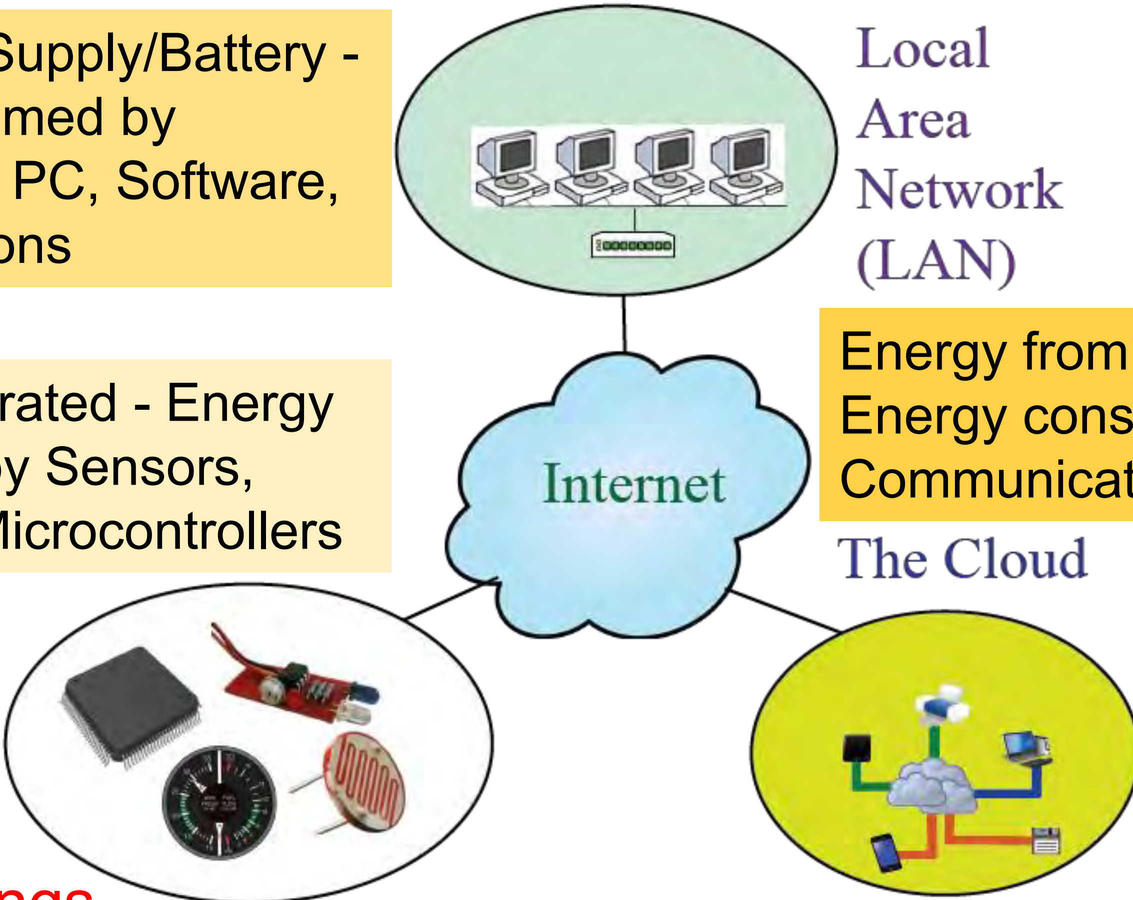
Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october

Top counterfeits could have impact of $300B on the semiconductor market.

# Energy Consumption Challenge in IoT

Energy from Supply/Battery - Energy consumed by Workstations, PC, Software, Communications

Battery Operated - Energy consumed by Sensors, Actuators, Microcontrollers



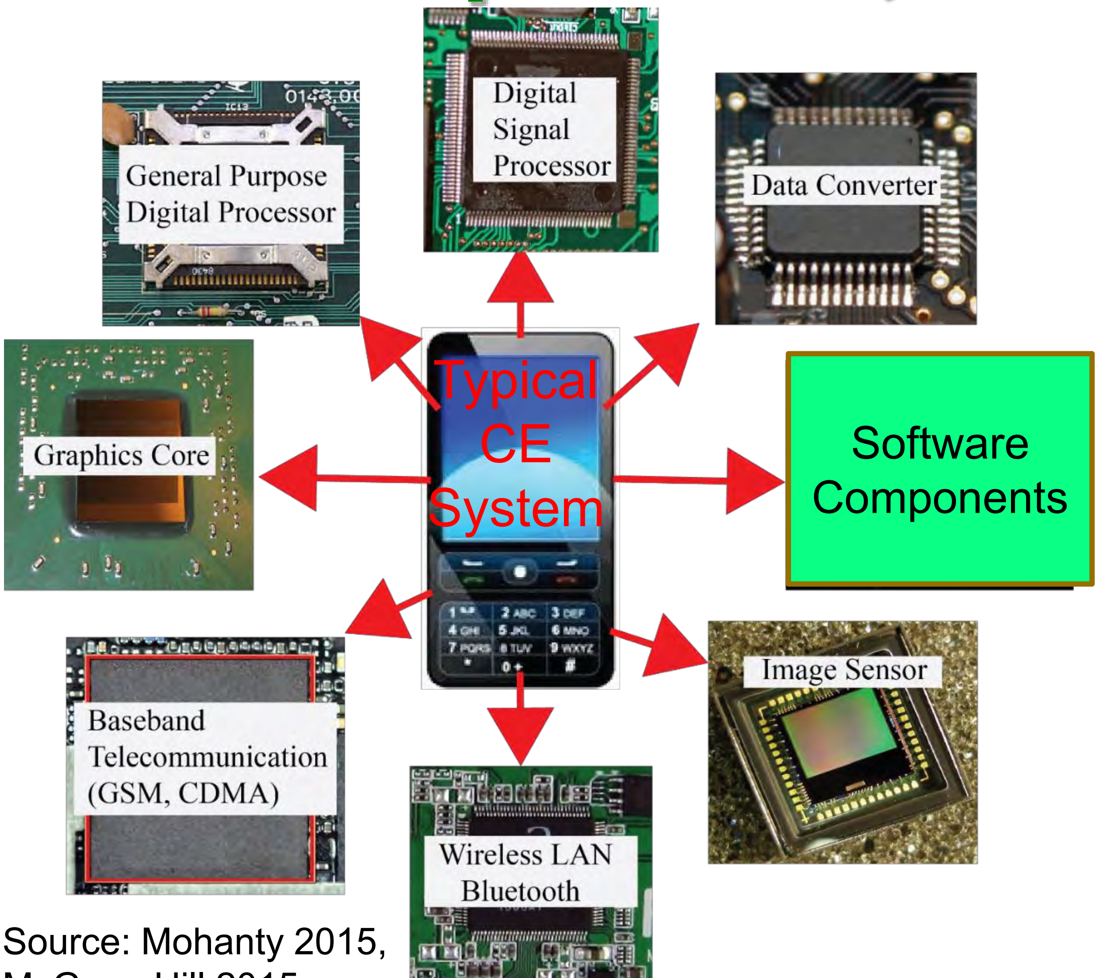

Energy from Supply/Battery - Energy consumed by Communications

Energy from Supply - Energy consumed in Server, Storage, Software, Communications

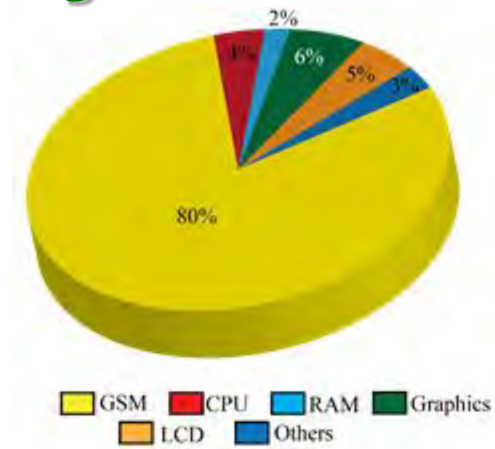
Four Main Components of IoT.

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

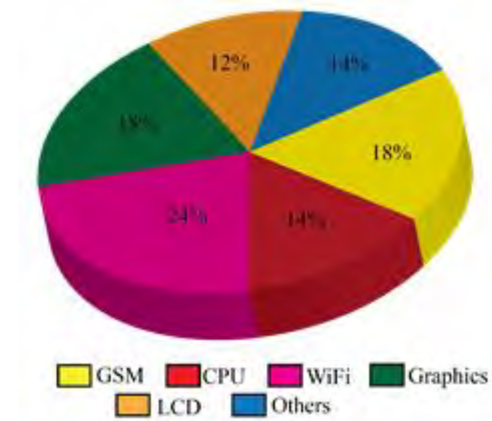
# Energy Consumption of Sensors, Components, and Systems




Source: Mohanty 2015, McGraw-Hill 2015




During GSM Communications




During WiFi Communications

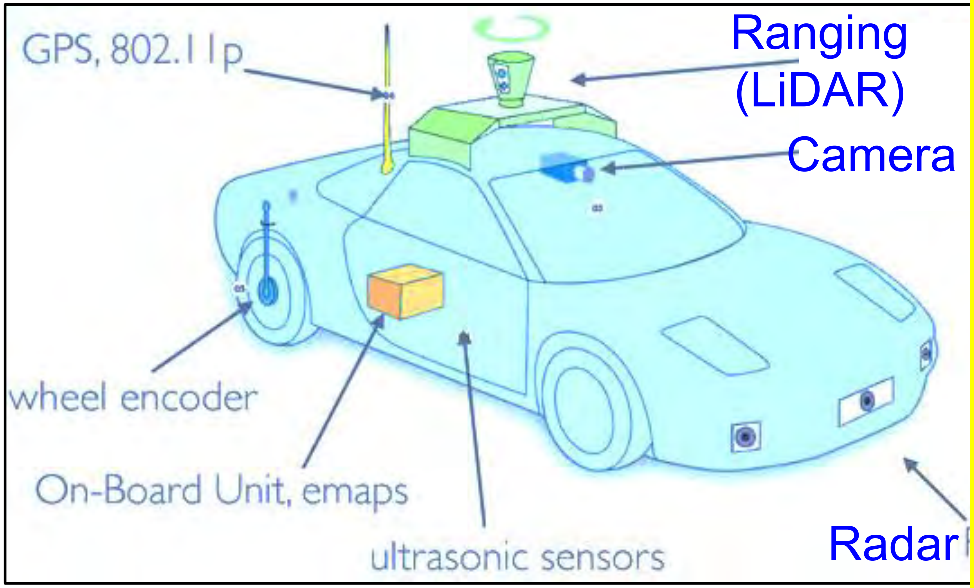
# Energy Consumption and Latency in Communications

- Connected cars require latency of ms to communicate and avoid impending crash.
  - Faster connection
  - Low latency
  - Low power and energy
- 5G for connected world: Enables all devices to be connected seamlessly.
- LoRa: Long Range, low-powered, low-bandwidth, IoT communications as compared to 5G or Bluetooth.
- How about 5G, WiFi working together effectively?

Source: https://www.linkedin.com/pulse/key-technologies-connected-world-cloud-computing-ioe-balakrishnan

Source: https://eandt.theiet.org/content/articles/2016/08/lora-promises-cheap-low-power-alternative-to-5g-for-iot-devices/

# CE System Example - Autonomous Car




Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

**Level 0**
- Complete Driver Control

**Level 1**
- Most functions by driver, some functions automated.

**Level 2**
- At least one driver-assistance system is automated.

**Level 3**
- Complete shift of critical safety systems to vehicle; Driver can intervene

**Level 4**
- Perform All Safety-Critical Functions
- Limited to Operational Domain

**Level 5**
- All Safety-Critical Functions in All Environments and Scenarios

"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

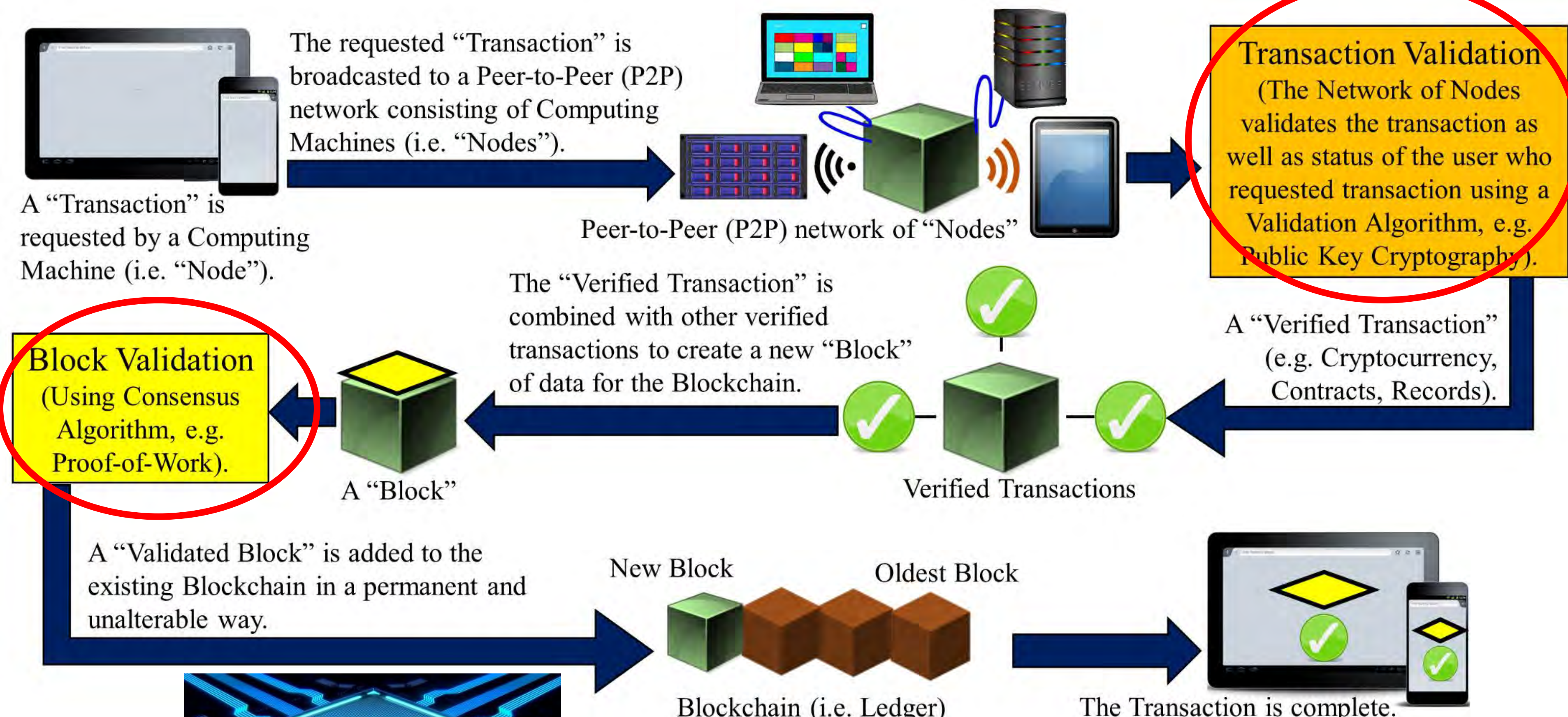
Datta 2017: CE Magazine Oct 2017

# Autonomous Vehicle – Computing Need


Source: https://www.engadget.com/2017/10/10/nvidia-introduces-a-computer-for-level-5-autonomous-cars/

Computing need in small server room stored in the trunk:
- ❖ Artificial Intelligence (AI) and data-crunching
- ❖ Huge amounts of data coming from dozens of cameras, LiDAR sensors, short and long-range radar

# Blockchain Technology




Source: Mohanty 2018, CE Magazine July 2018

# Blockchain – Energy Consumption Issue

Scalability

High Latency

Blockchain Challenges

Fake Block Generation

Energy Consumption

Source: Mohanty 2018, CE Magazine July 2018

- Energy for mining of 1 bitcoin → 2 years consumption of a US household
- Energy consumption for each bitcoin transaction → 80,000X of energy consumption of a credit card processing

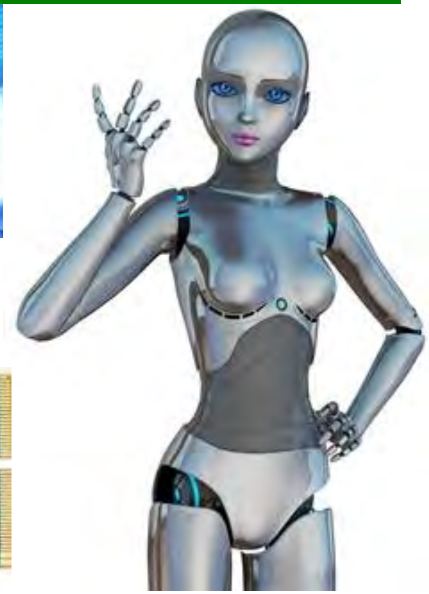

Source: N. Popper, "There is Nothing Virtual About Bitcoin's Energy Appetite", The New York Times, 21st Jan 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html.

# Artificial Intelligence Technology

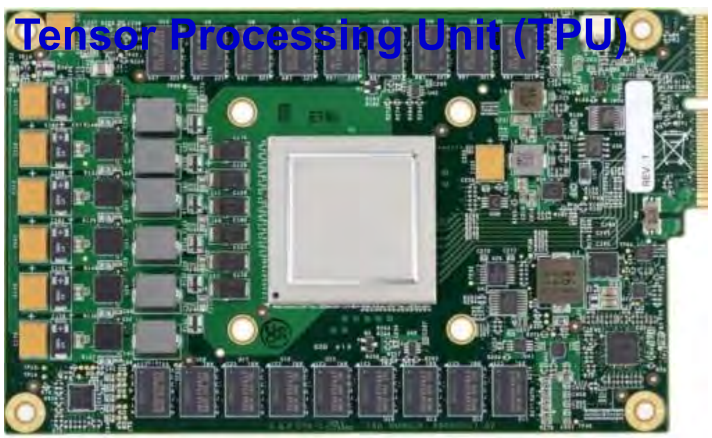
Machine Learning

Deep Learning

Source: http://transmitter.ieee.org/impact-aimachine-learning-iot-various-industries/

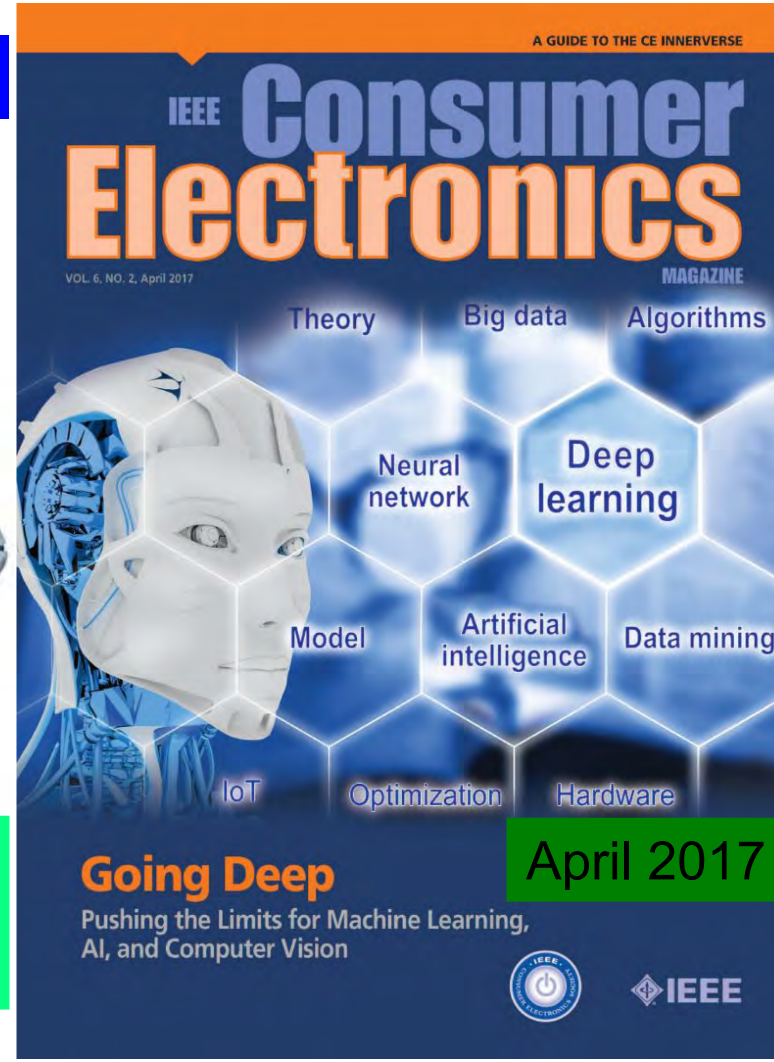


Tensor Processing Unit (TPU)



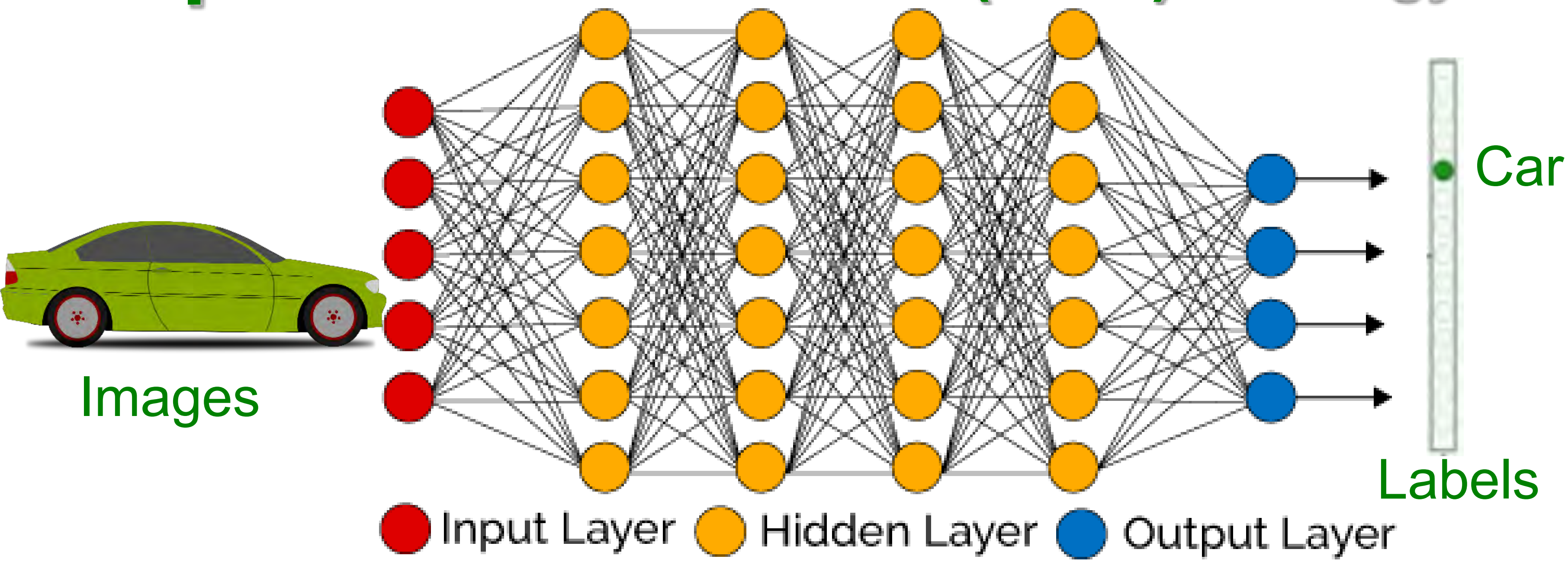
Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

Smart City Use:
- Better decision
- Faster response




April 2017

# Deep Neural Network (DNN) - Energy Issue




- DNN considers many training parameters, such as the size, the learning rate, and initial weights.
- High computational resource and time: For sweeping through the parameter space for optimal parameters.
- DNN needs: Multicore processors and batch processing.
- DNN training can happen in cloud not at edge or fog.

# Impact of High Energy Consumption


Source: Mohanty 2015, McGraw-Hill 2015

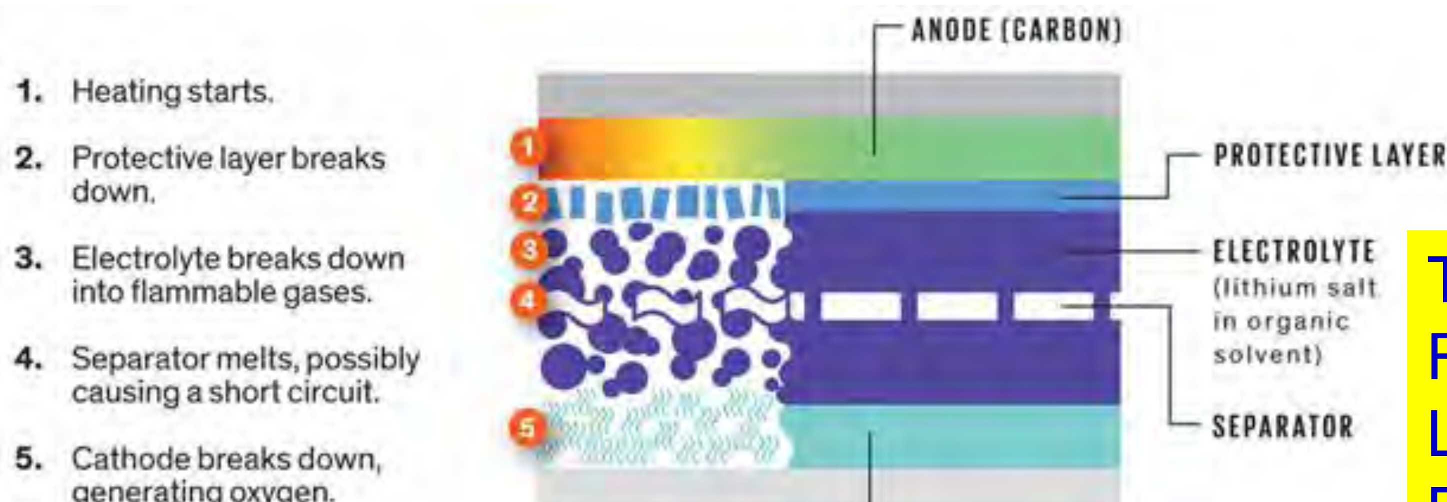
- Smartwatch → 1 day battery life of 1 time charging.

- Fitness Tracker → 3 hours battery life of 1 time charging if GPS is ON.

Source: Mohanty 2013, CARE 2013 Keynote

# Safety of Electronics

Smartphone Battery

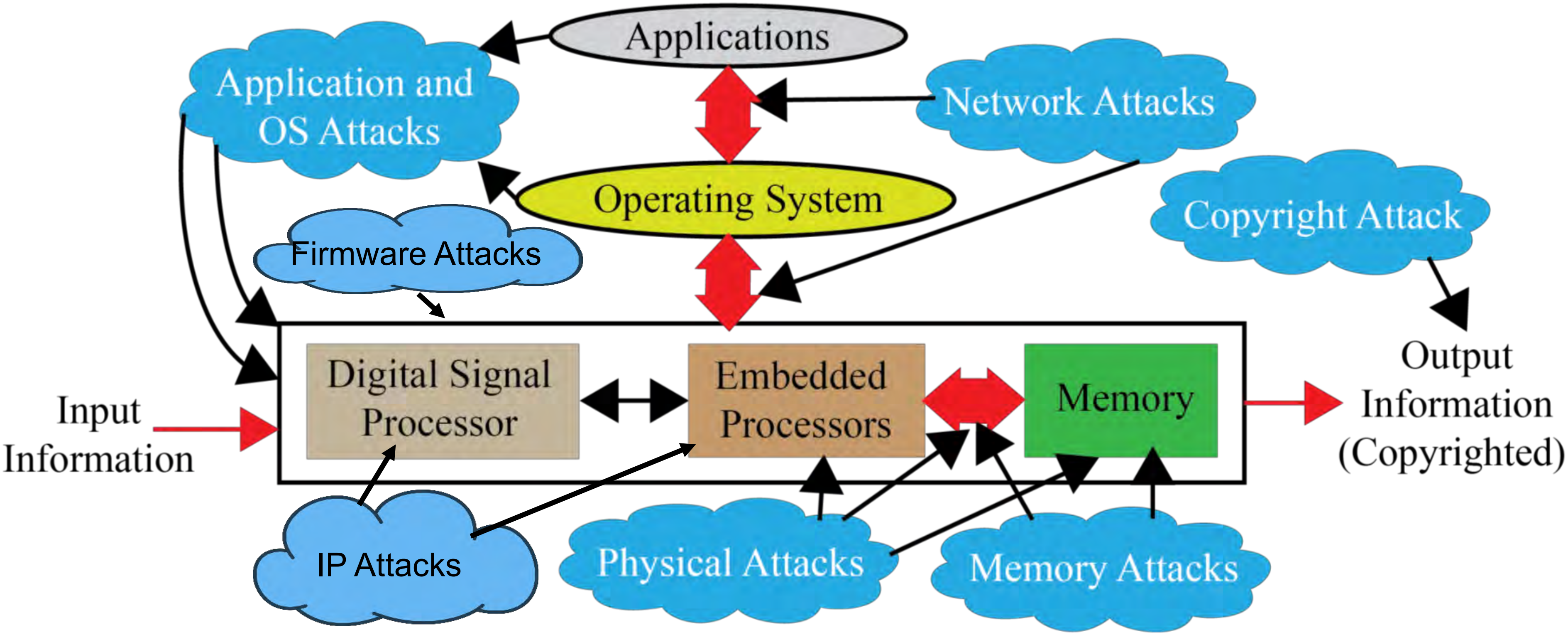



Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery

Thermal Runaway in a Lithium-Ion Battery

# Addressing Security Constraints in CE

# Selected Attacks on a CE System – Security, Privacy, IP Rights




Diverse forms of Attacks, following are not the same: System Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

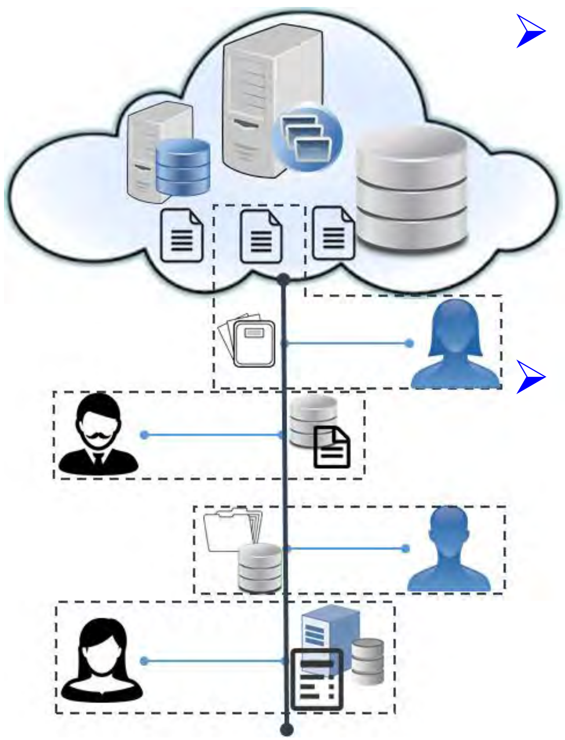
# IoT Security - Software Defined Perimeter (SDP)

TCP/IP based security | Traditional

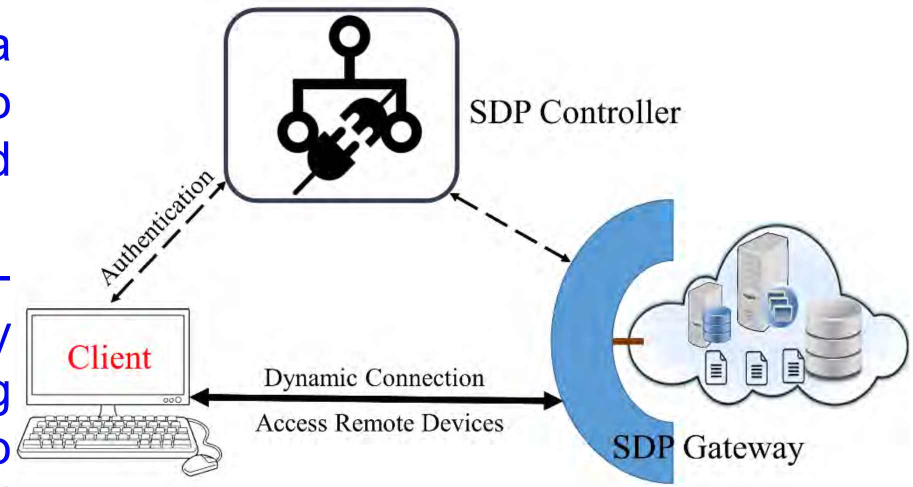
Connect First and then Authenticate

Software-Defined Perimeter | Advanced

Authenticate First and then Connect

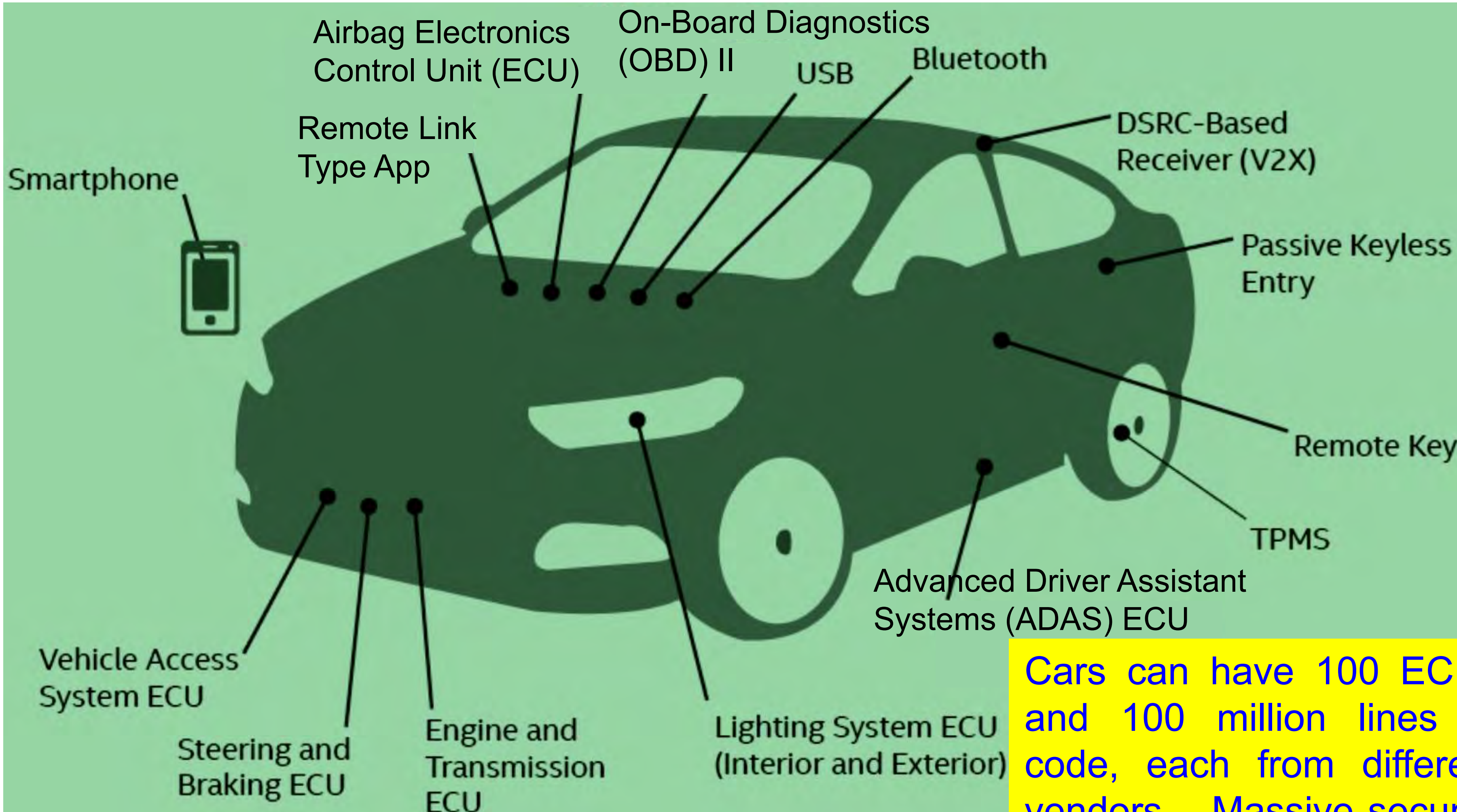


- SDP creates a cryptographic perimeter from a source device to the edges and cloud data center.
- SDP provides user-centric security solution by creating a perimeter to enclose source and destination within the perimeter.




Source: Mohanty 2017, CEM Oct 2017

# Smart Car – Security Venerability

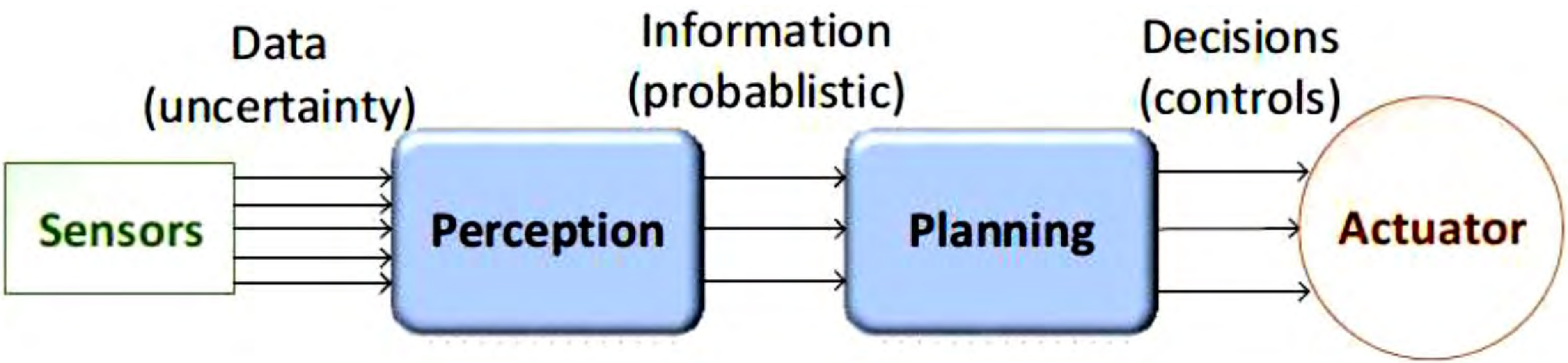



Cars can have 100 ECUs and 100 million lines of code, each from different vendors – Massive security issues.

Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

# Smart Car – Decision Chain

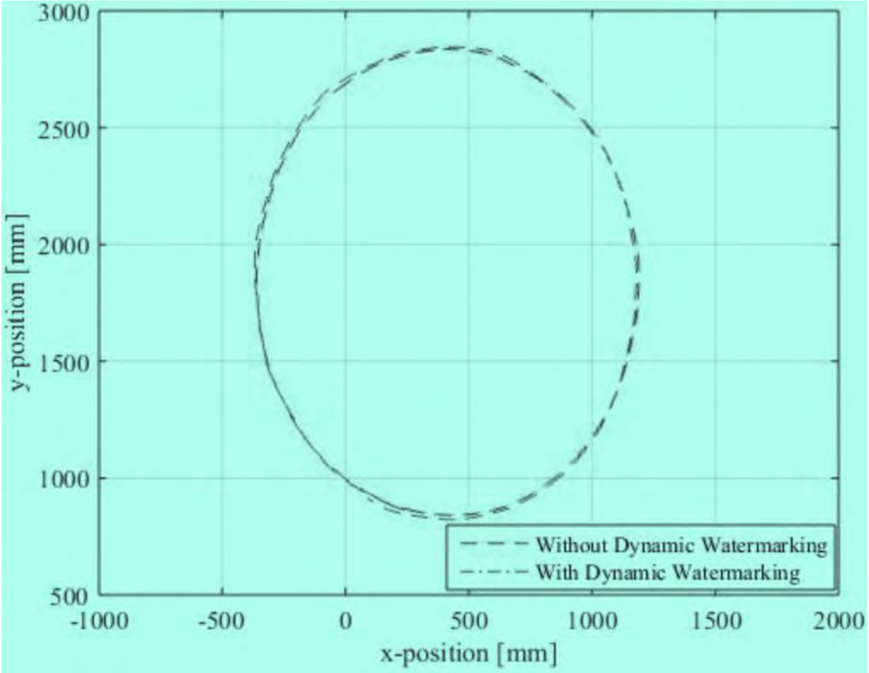
- Designing an AV requires decision chains.
- Human driven vehicles are controlled directly by a human.
- AV actuators controlled by algorithms.
- Decision chain involves sensor data, perception, planning and actuation.
- Perception transforms sensory data to useful information.
- Planning involves decision making.




Source: Plathottam 2018, COMSNETS 2018

# Autonomous Car Security – Collision Avoidance

- Attack: Feeding of malicious sensor measurements to the control and the collision avoidance module. Such an attack on a position sensor can result in collisions between the vehicles.
- Solutions: "**Dynamic Watermarking**" of signals to detect and stop such attacks on cyber-physical systems.
- Idea: Superimpose each actuator *i* a random signal $e_i[t]$ (watermark) on control policy-specified input.

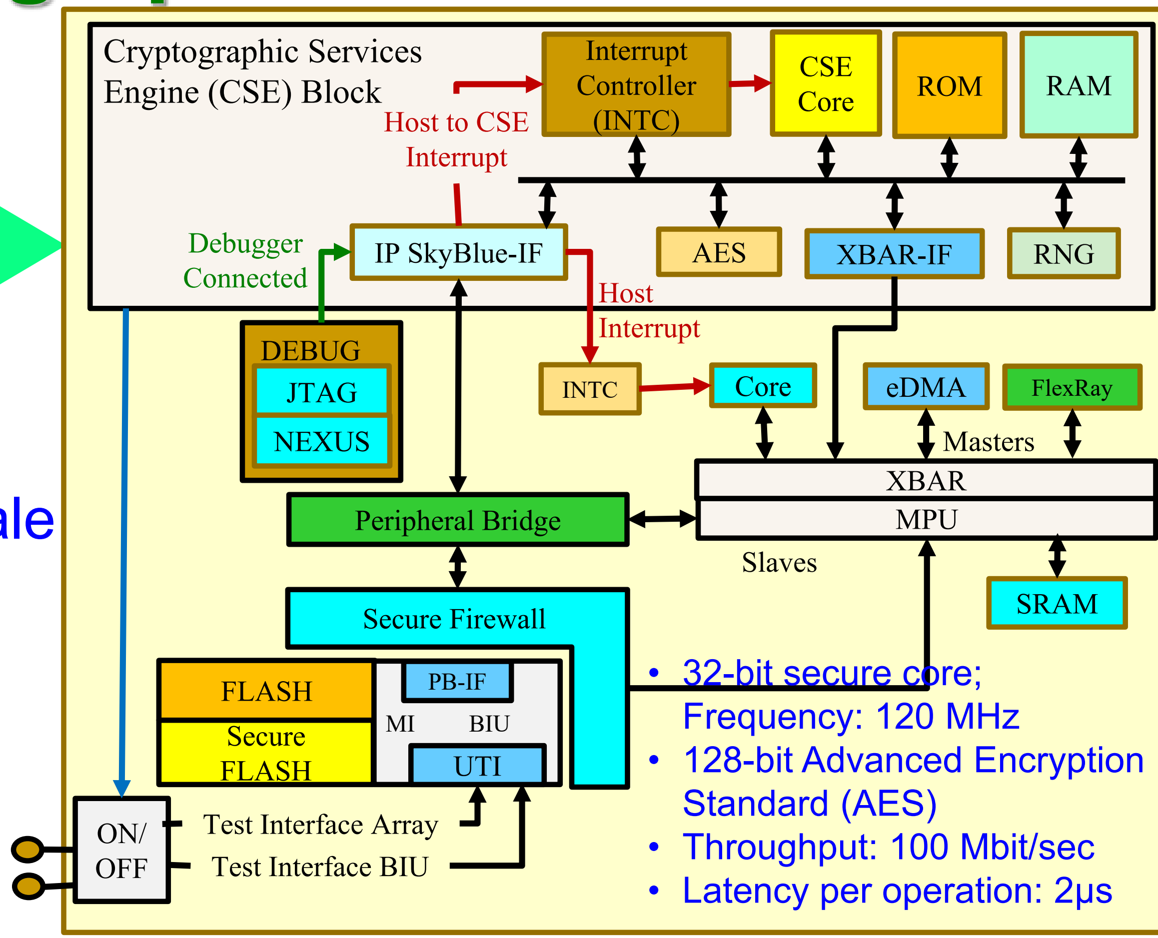



Source: Ko 2016, CPS-Sec 2016

# Autonomous Car Security – Cryptographic Hardware

Cryptographic Services Engine (CSE) Block

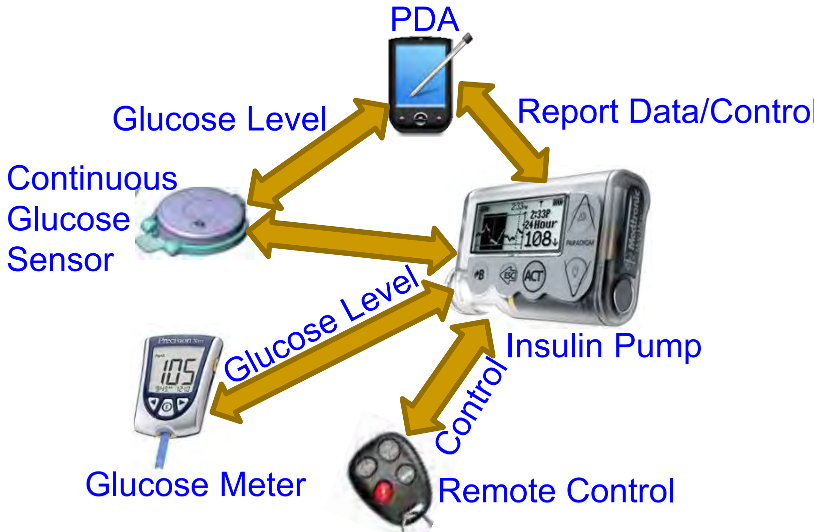
Qorivva MPC564xB/C Family from NXP/Freescale



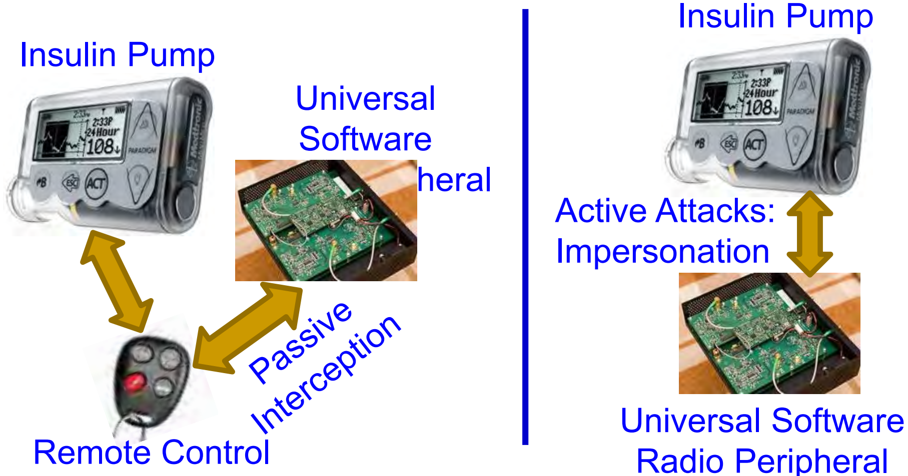

- 32-bit secure core; Frequency: 120 MHz
- 128-bit Advanced Encryption Standard (AES)
- Throughput: 100 Mbit/sec
- Latency per operation: 2μs

Source: http://www.nxp.com/assets/documents/data/en/supporting-information/DWF13_AMF_AUT_T0112_Detroit.pdf

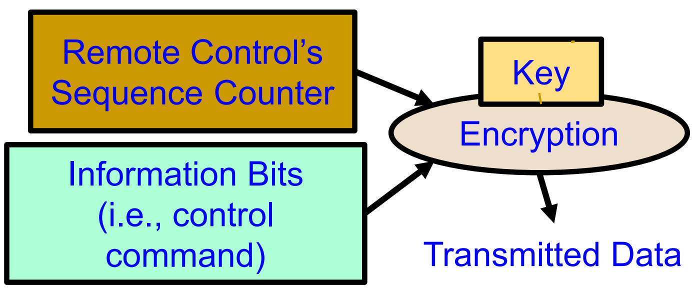
# Smart Healthcare Security



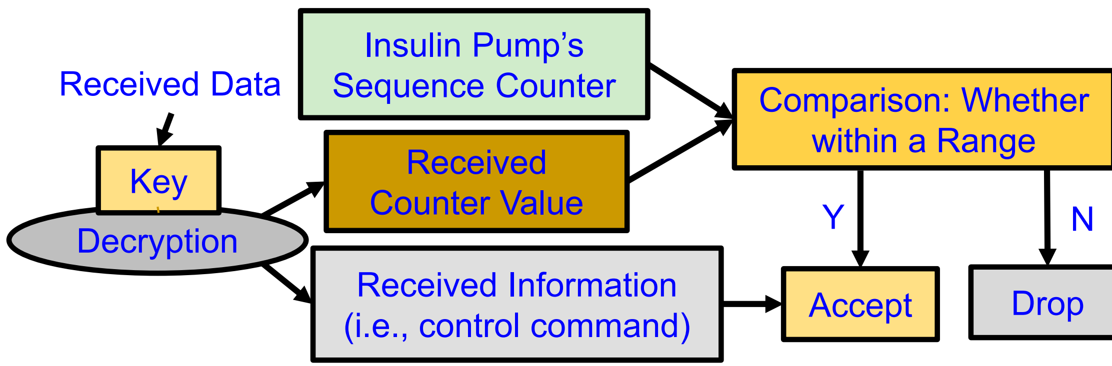

Insulin Delivery System




Security Attacks




Rolling Code Encoder in Remote Control



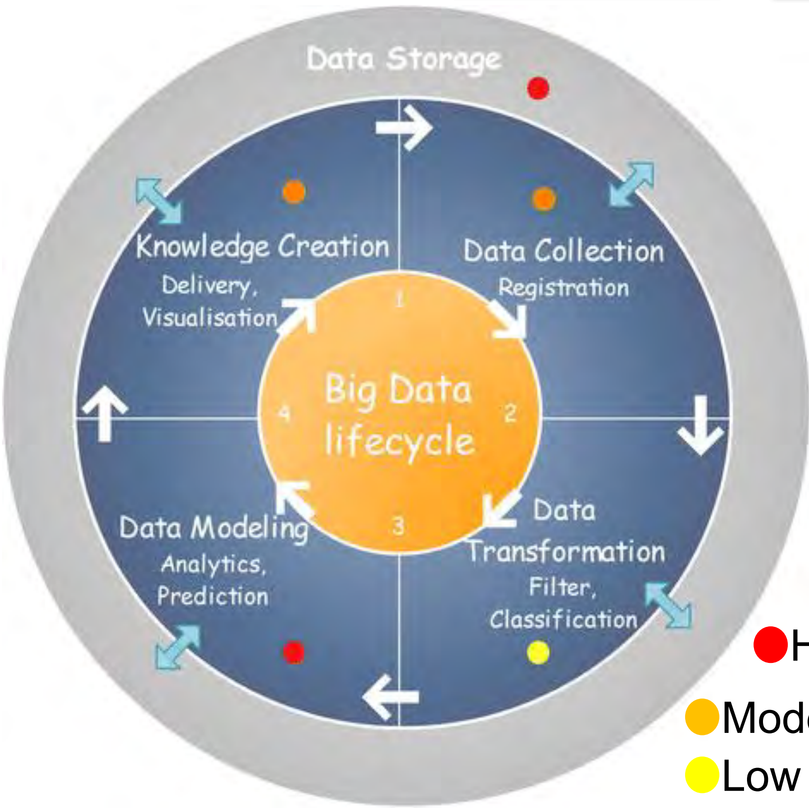

Rolling Code Decoder in Insulin Pump

Li 2011: HEALTH 2011

# Smart Healthcare - Privacy Issue

**Privacy Protection**

- Untraceability
- Unlinkability
- Unobservability
- Anonymity
- Pseudonymity




High Risk
Moderate Risk
Low Risk

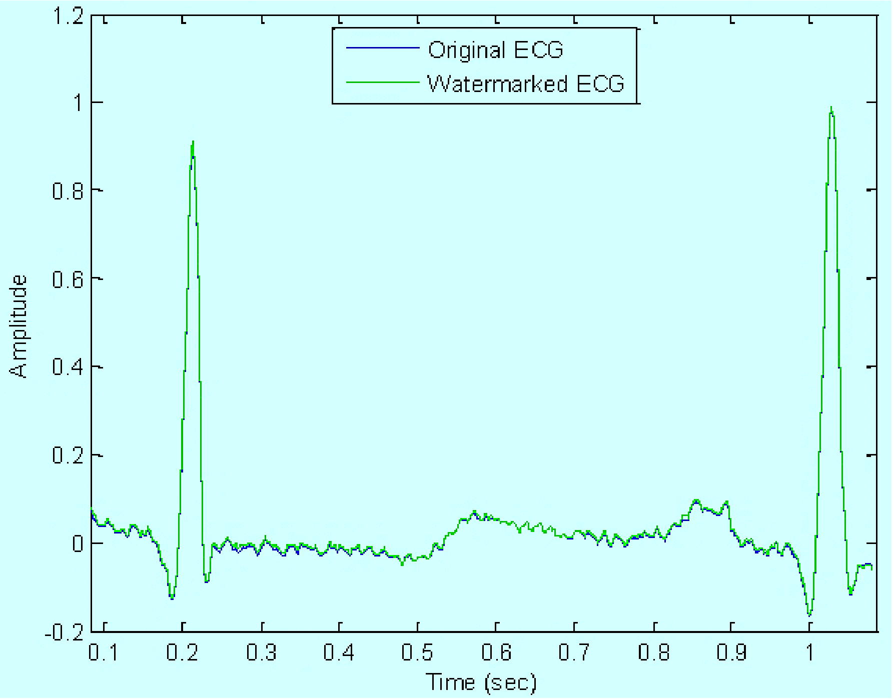
**Smart Healthcare Security /Privacy Methods**

- Authentication
- Data Encryption
- Data/Signal Watermarking
- Data Masking
- Access Control
- Monitoring and Auditing
- De-identification
- Hybrid Execution Model
- Identity-based Anonymization

Source: Abouelmehdi et al., Springer BigData 2018 Dec

# Smart Healthcare Data Integrity – Medical Signal Authentication

- Physiological signals like the electrocardiogram (EKG) are obtained from patients, transmitted to the cloud, and can also stored in a cloud repository.
- With increasing adoption of electronic medical records and cloud-based software-as-service (SaaS), advanced security measures are necessary.
- Protection from unauthorized access to Protected Health Information (PHI) also protects from identity theft schemes.
- From an economic stand-point, it is important to safeguard the healthcare and insurance system from fraudulent claims.

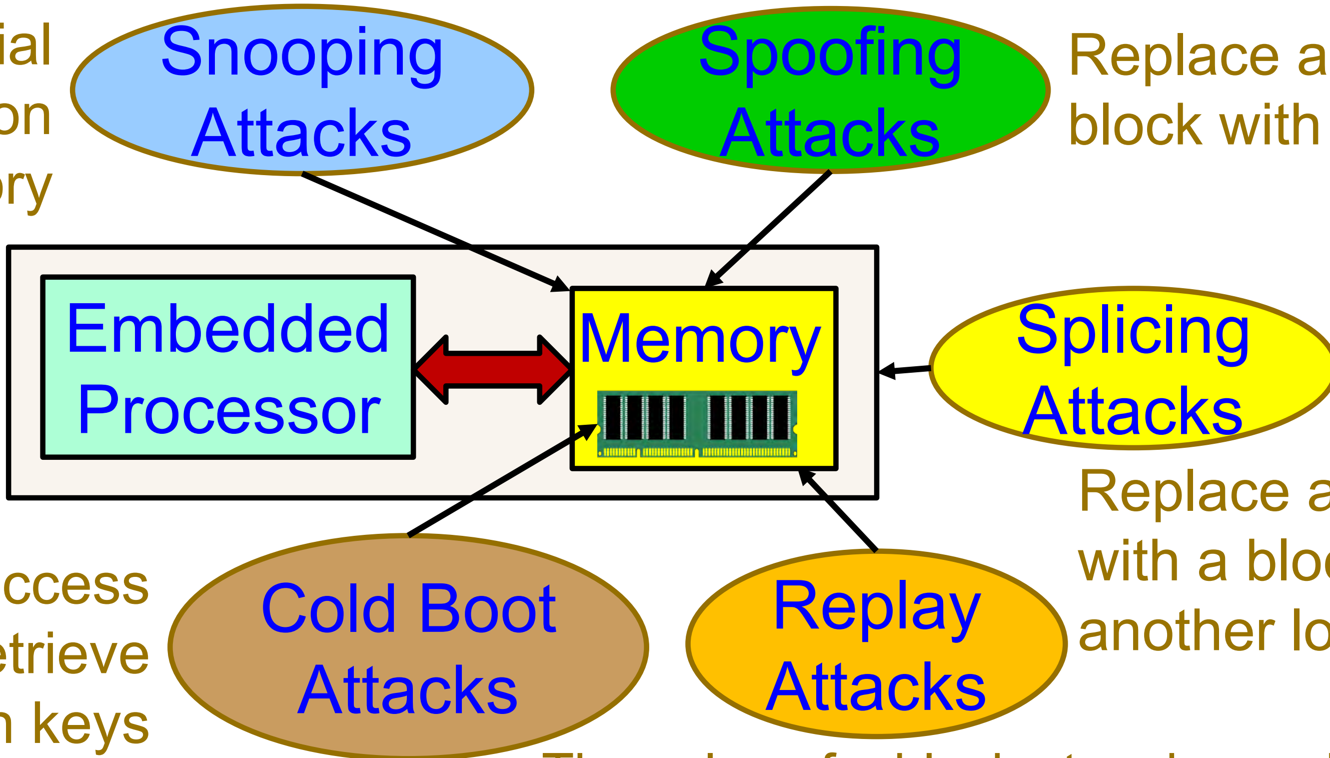



Source: Tseng 2014, Tseng Sensors Feb 2014

# Memory Attacks

Read confidential information in memory

Replace a block with fake




Replace a block with a block from another location

Physical access memory to retrieve encryption keys

The value of a block at a given address at one time is written at exactly the same address at a different times; Hardest attack.

Source: Mohanty 2013, Springer CSSP Dec 2013

# Nonvolatile Memory Security and Protection


Source: http://datalocker.com

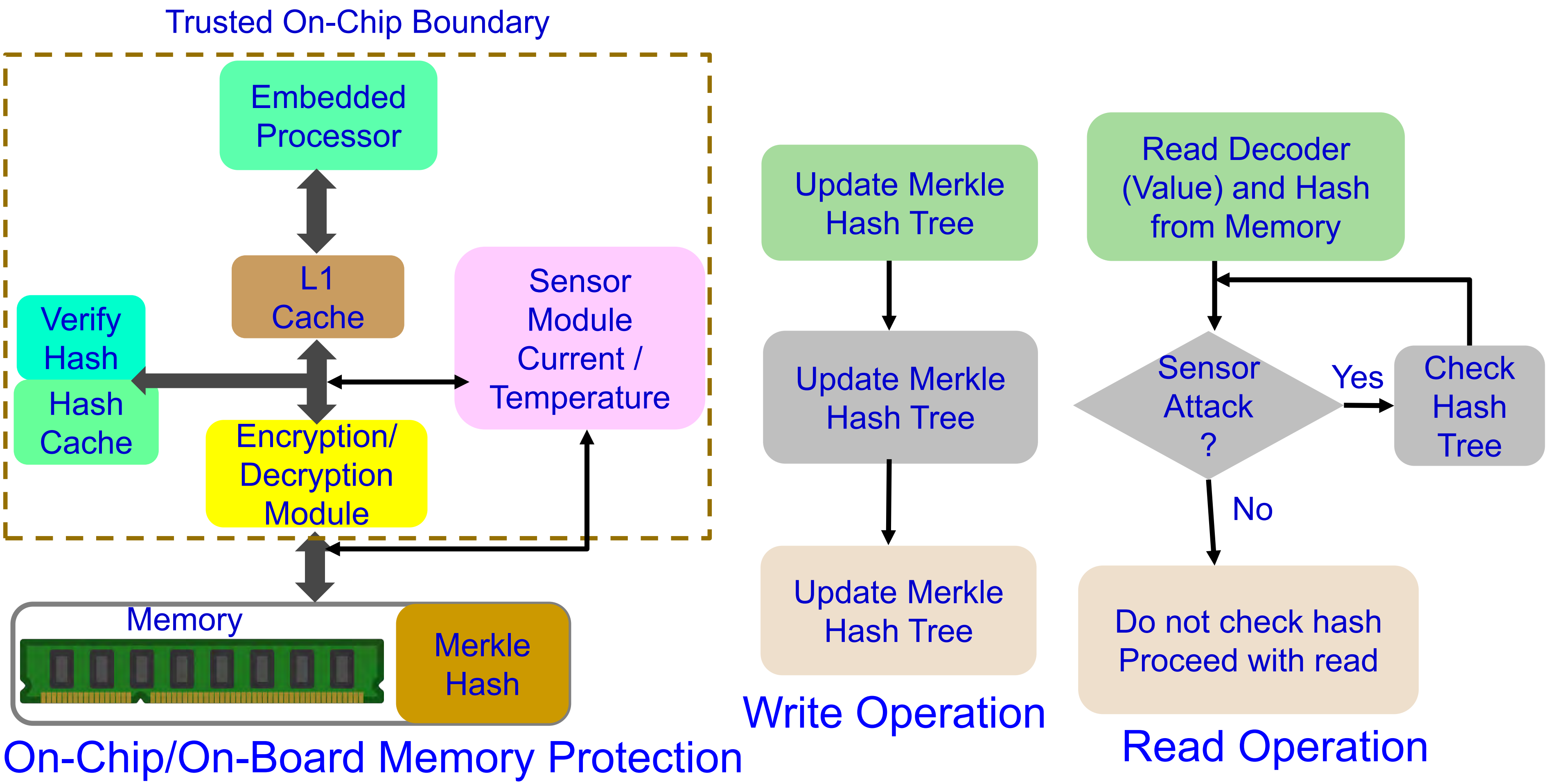
Nonvolatile / Harddrive Storage

Hardware-based encryption of data secured/protected by strong password/PIN authentication.

Software-based encryption to secure systems and partitions of hard drive.

Some performance penalty due to increase in latency!

# Embedded Memory Security and Protection



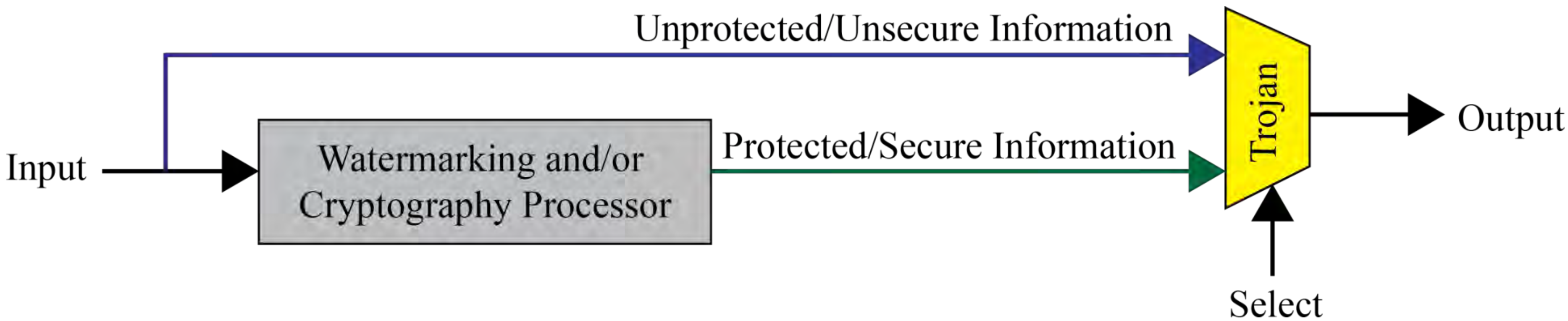

**Some performance penalty due to increase in latency!**

Source: Mohanty 2013, Springer CSSP Aug 2013

# Malicious Design Modifications Issue

Information may bypass giving a non-watermarked or non-encrypted output.

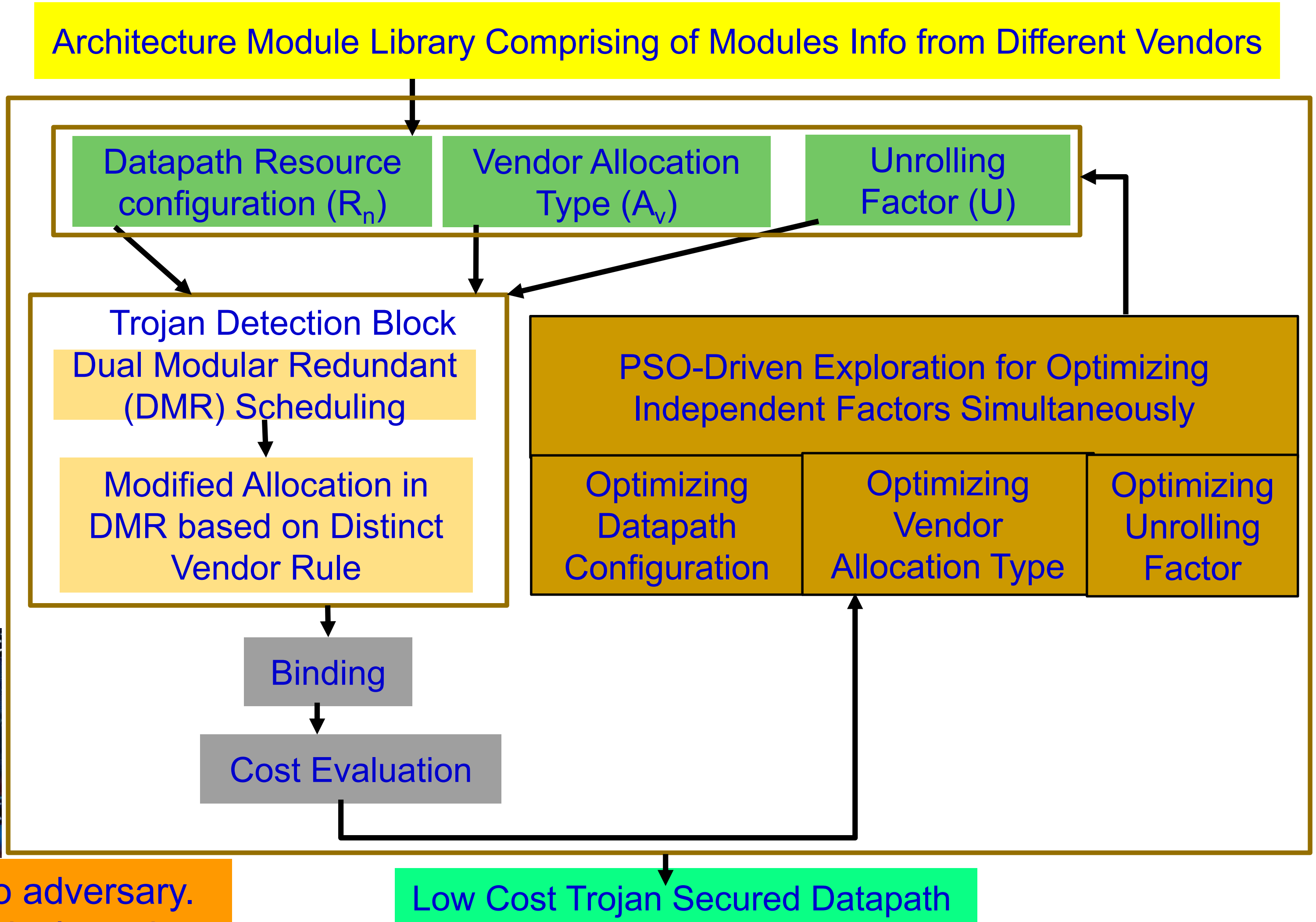
Hardware Trojans




Source: Mohanty 2015, McGraw-Hill 2015

Provide backdoor to adversary.
Chip fails during critical needs.

# Trojan Secure Digital Hardware Synthesis

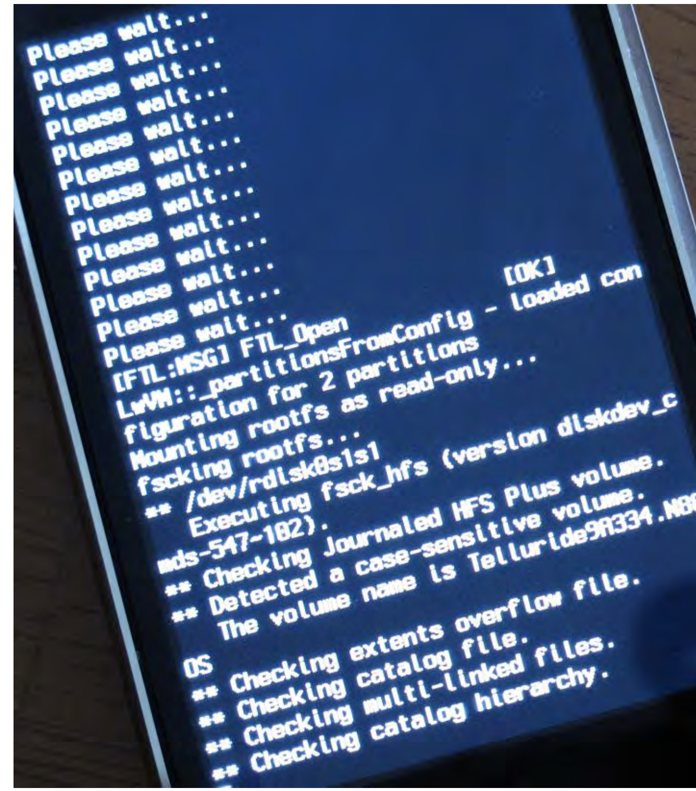



Provide backdoor to adversary.
Chip fails during critical needs.

Source: Sengupta, Mohanty 2017: TCAD April 2017

# Firmware Reverse Engineering


Extract, modify, or reprogram code

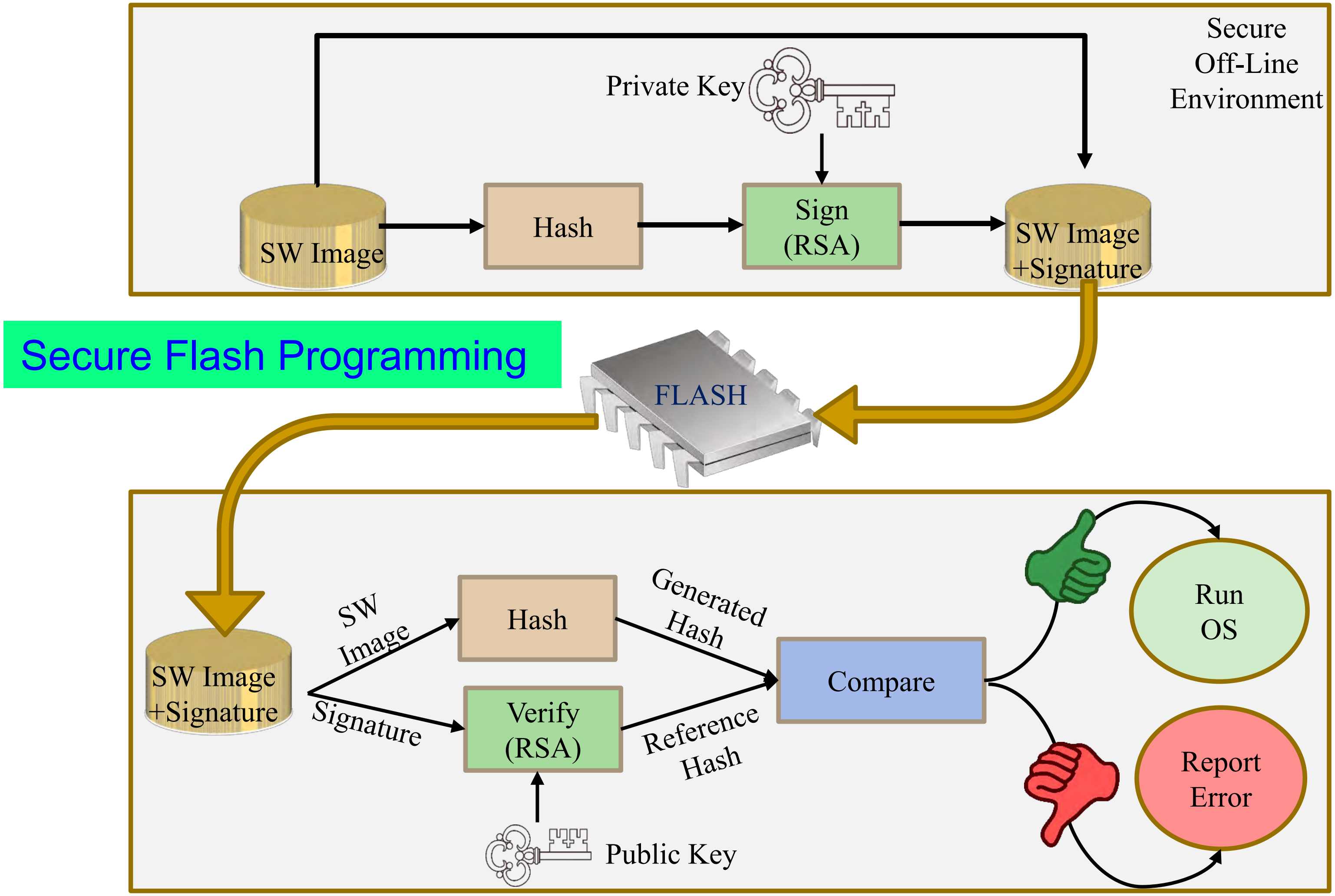



OS exploitation,
Device jailbreaking

Source: http://jcjc-dev.com/

Source: http://grandideastudio.com/wp-content/uploads/current_state_of_hh_slides.pdf

# Smart Car - Firmware Security




Source: https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf

# How Secure is AES Encryption?

- Brute force a 128 bit key ?
- If we assume:
  - Every person on the planet owns 10 computers
  - Each of these computers can test 1 billion key combinations per second
  - There are 7 billion people on the planet
  - On average, we can crack the key after testing 50% of the possibilities
  - Then the earth's population can crack one 128 bit encryption key in 77,000,000,000 years (77 billion years)

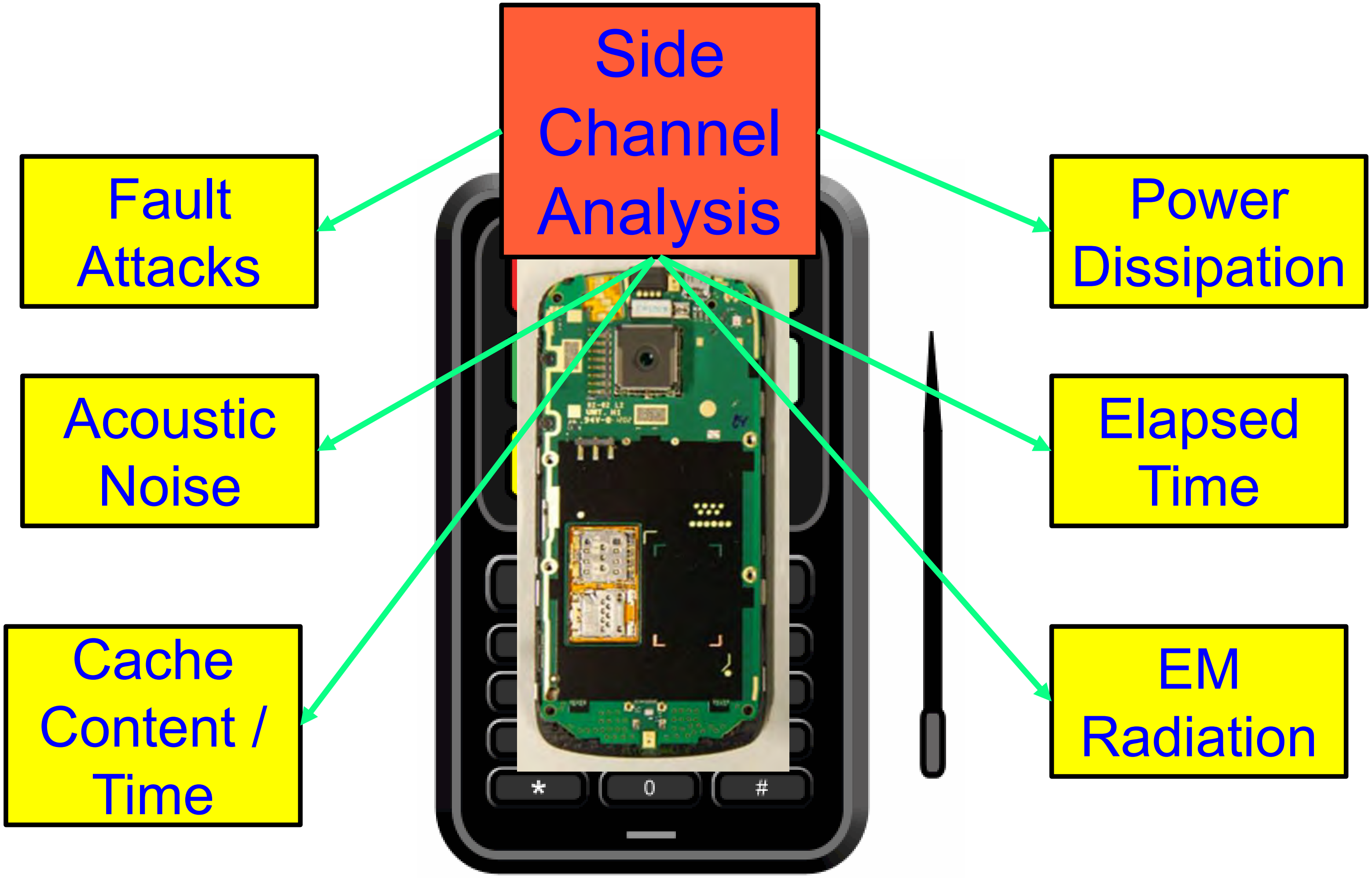
Encryptions ←→ Security

**Age of the Earth 4.54 ± 0.05 billion years**

**Age of the Universe 13.799 ± 0.021 billion years**

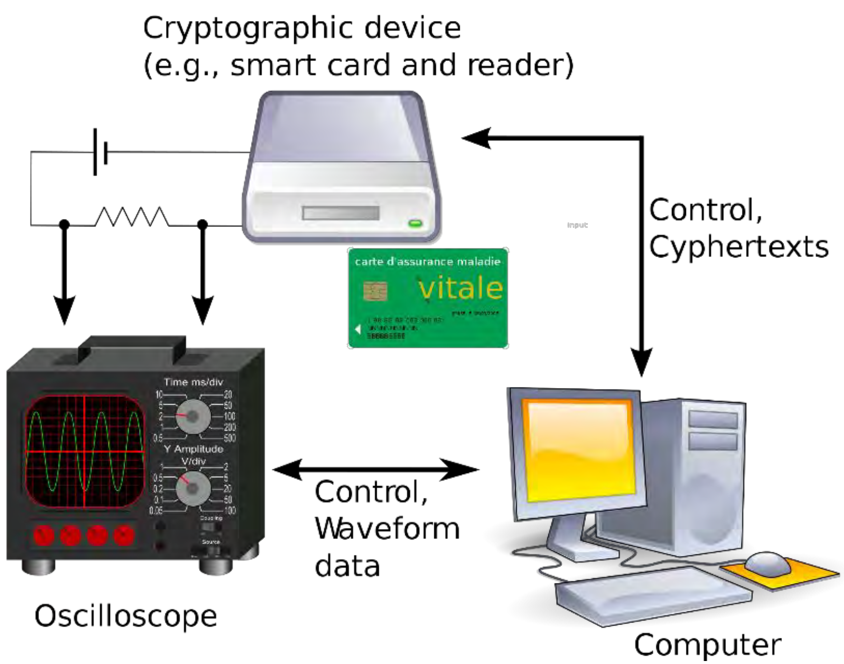
Source: Parameswaran Keynote iNIS-2017

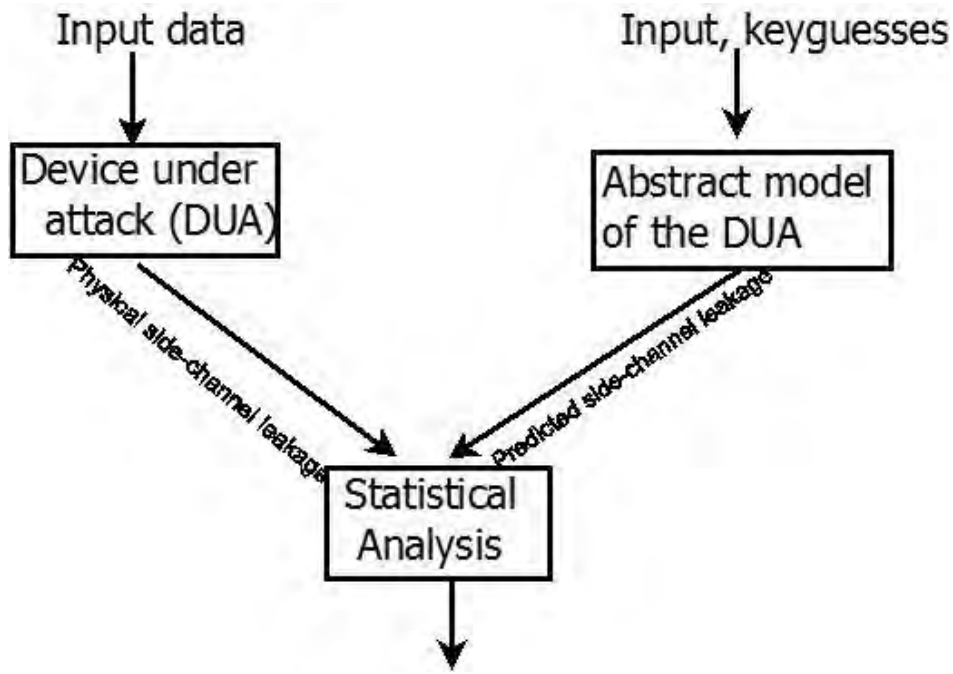
# Side Channel Analysis Attacks




Source: Parameswaran Keynote iNIS-2017

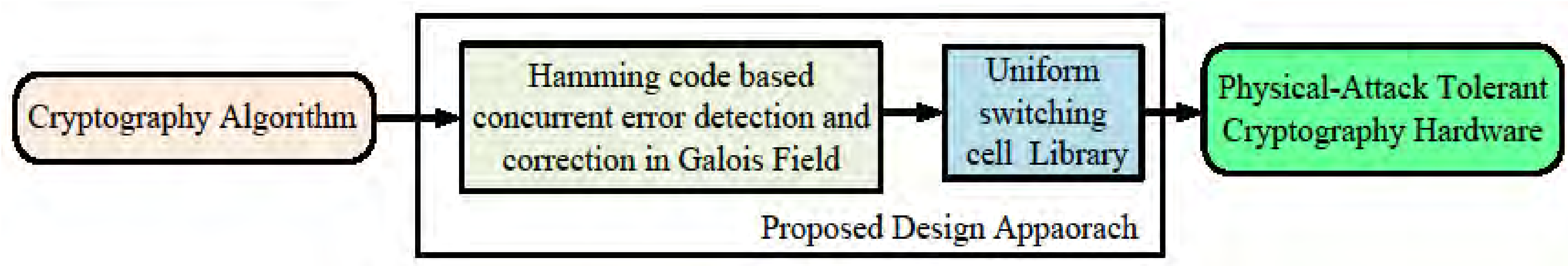
# Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CDA)

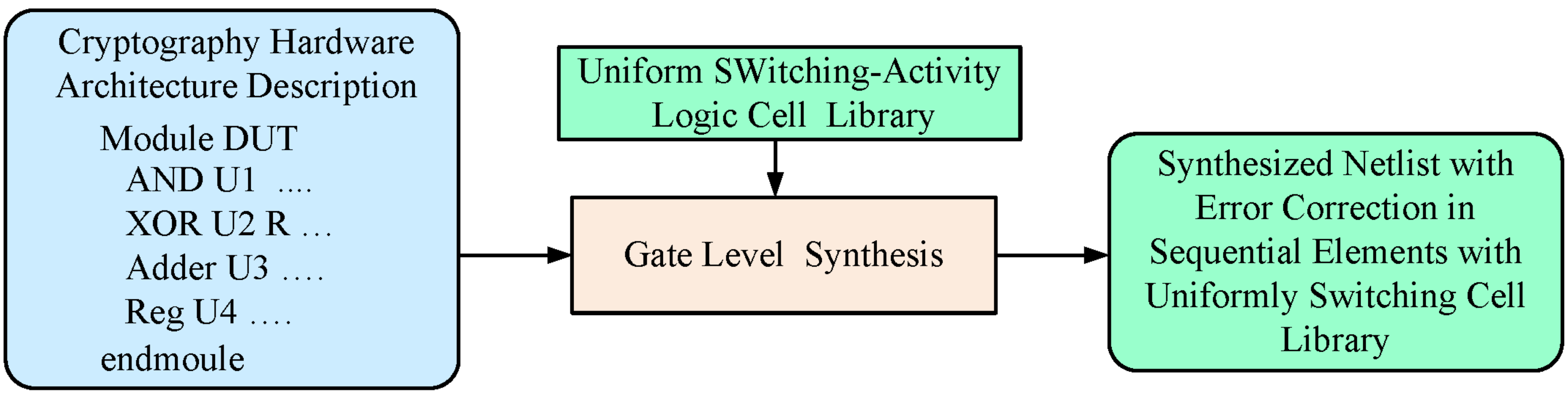



Decision on key guess

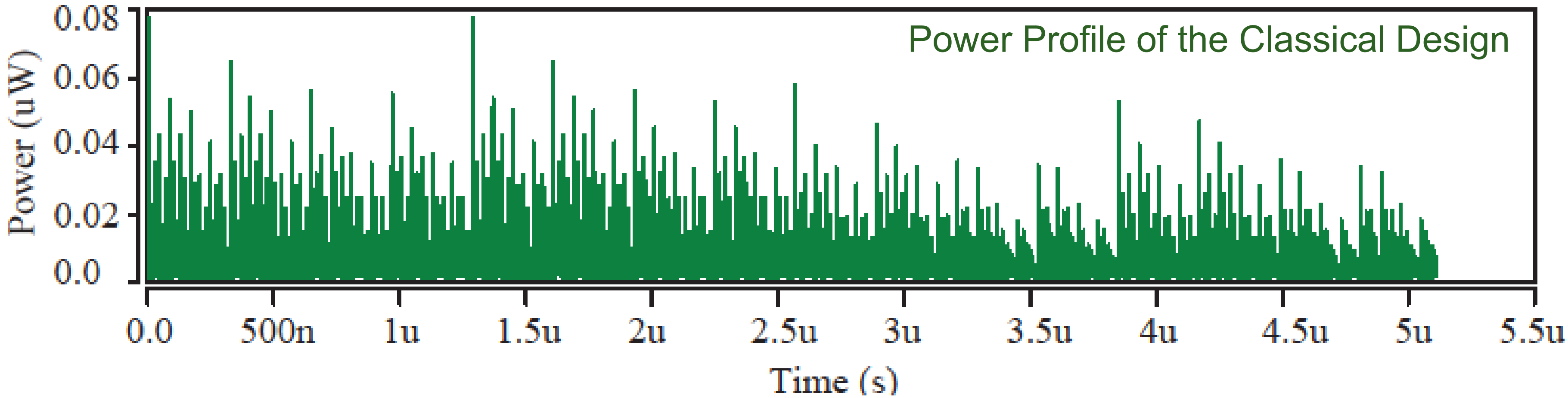
# DPA Resilience Hardware: Synthesis Flow

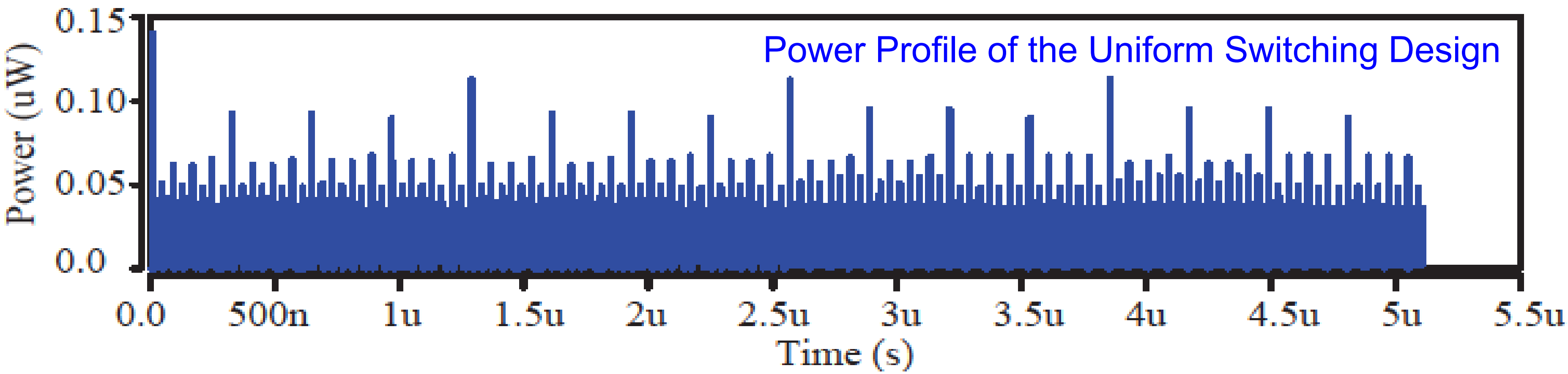



Source: Mohanty 2013, Elsevier CEE 2013.

# DPA Resilience Hardware



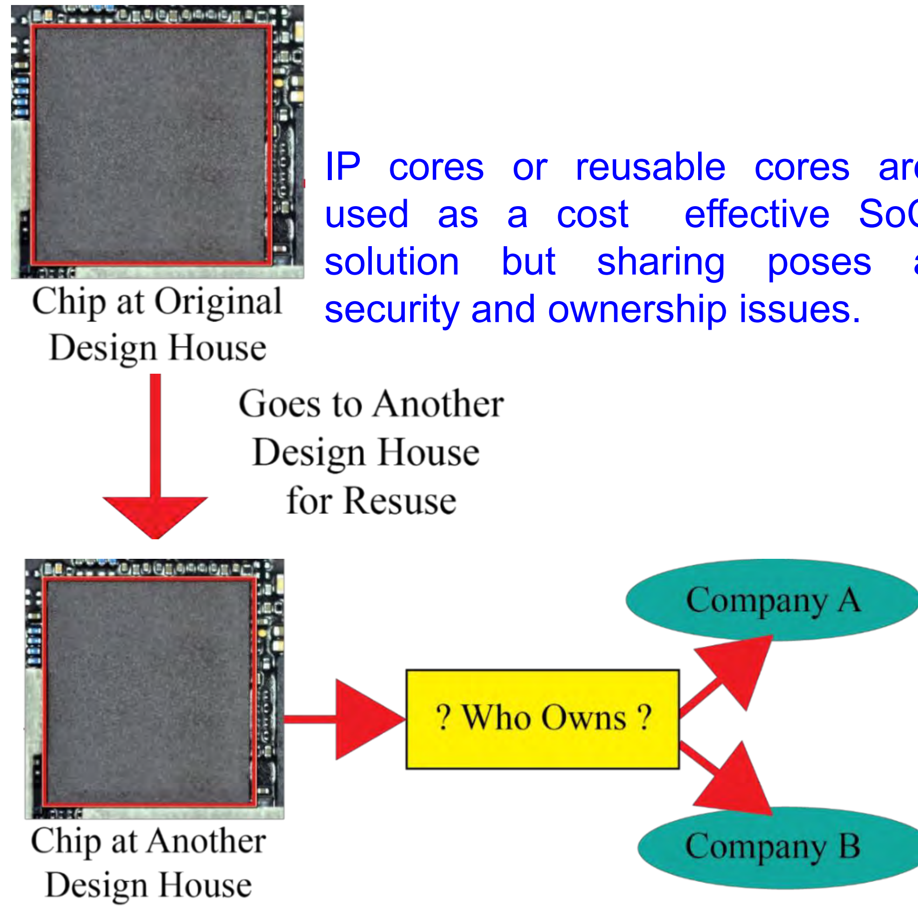

Source: Mohanty 2013, Elsevier CEE 2013.

# Copyright, Intellectual Property (IP), Or Ownership Protection

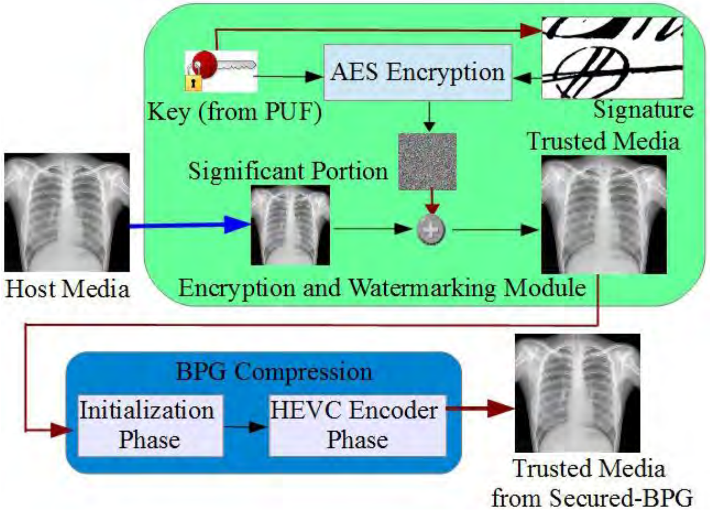
## Media Ownership


## Hardware Ownership

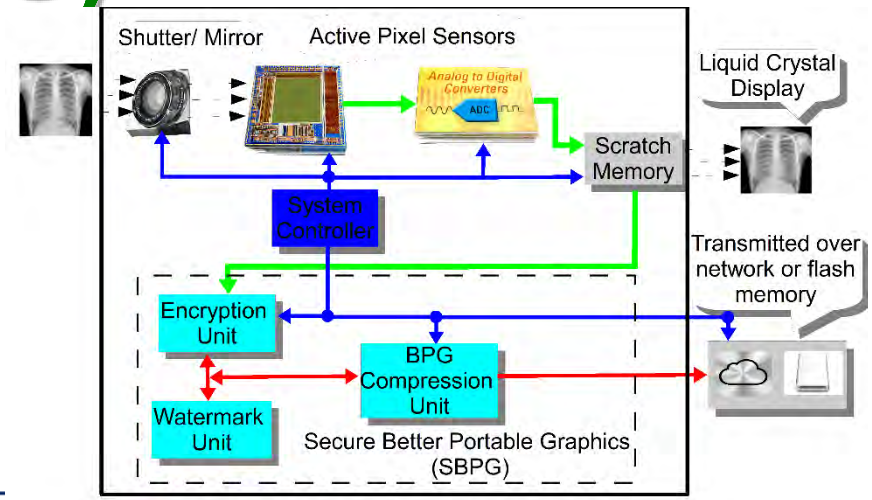
IP cores or reusable cores are used as a cost effective SoC solution but sharing poses a security and ownership issues.



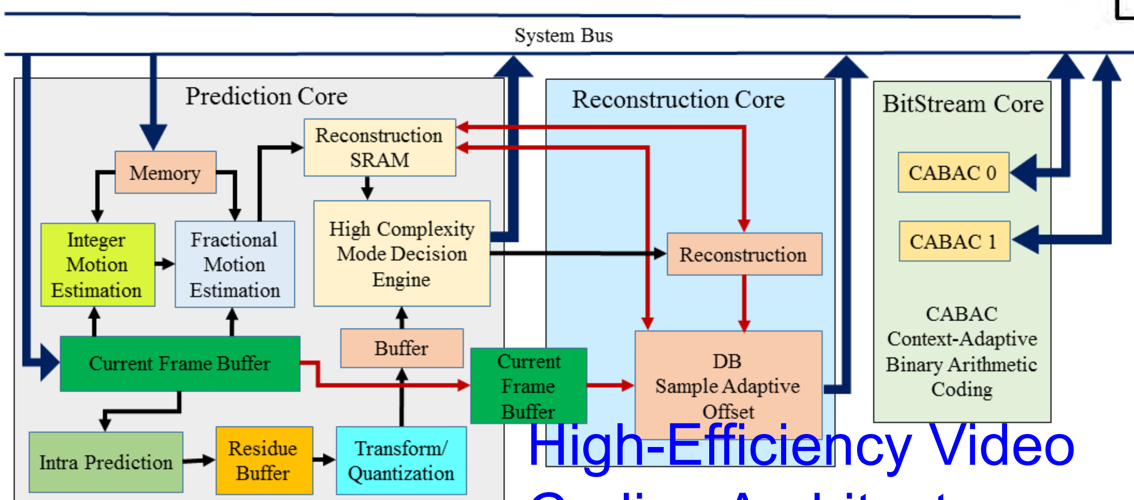
# Secure Better Portable Graphics (SBPG)




Secure BPG (SBPG)




Secure Digital Camera (SDC) with SBPG

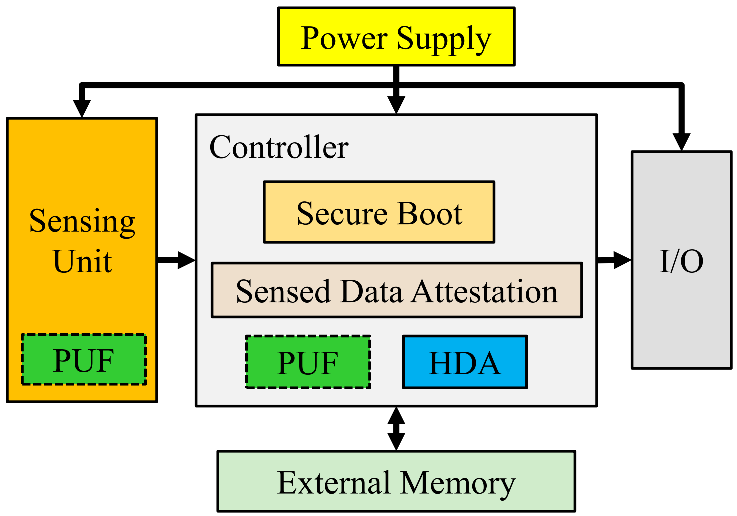



High-Efficiency Video Coding Architecture

Simulink Prototyping
Throughput: 44 frames/sec
Power Dissipation: 8 nW

Source: Mohanty 2018, IEEE-Access 2018

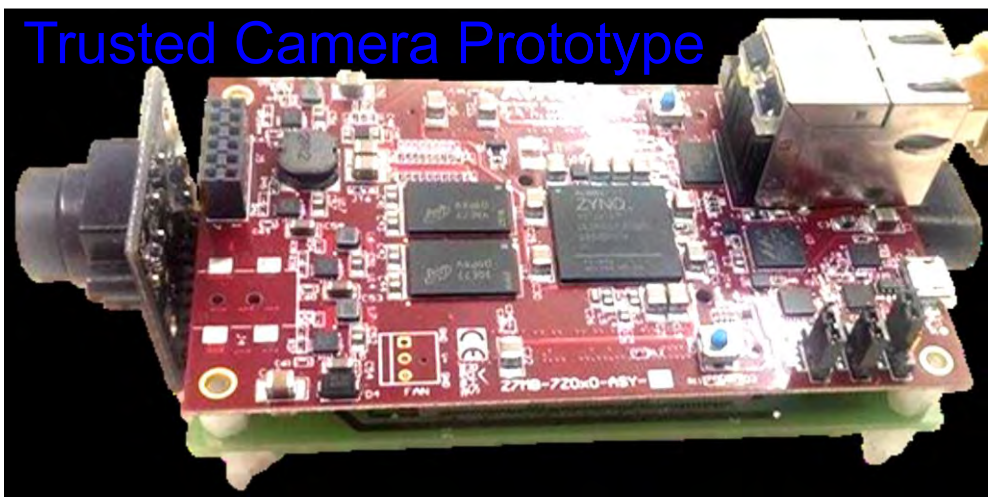
# PUF-based Trusted Sensor




PUF-based Trusted Sensor

PUF-based Secure Key Generation and Storage module provides key:

- Sensed data attestation to ensure integrity and authenticity.
- Secure boot of sensor controller to ensure integrity of the platform at booting.

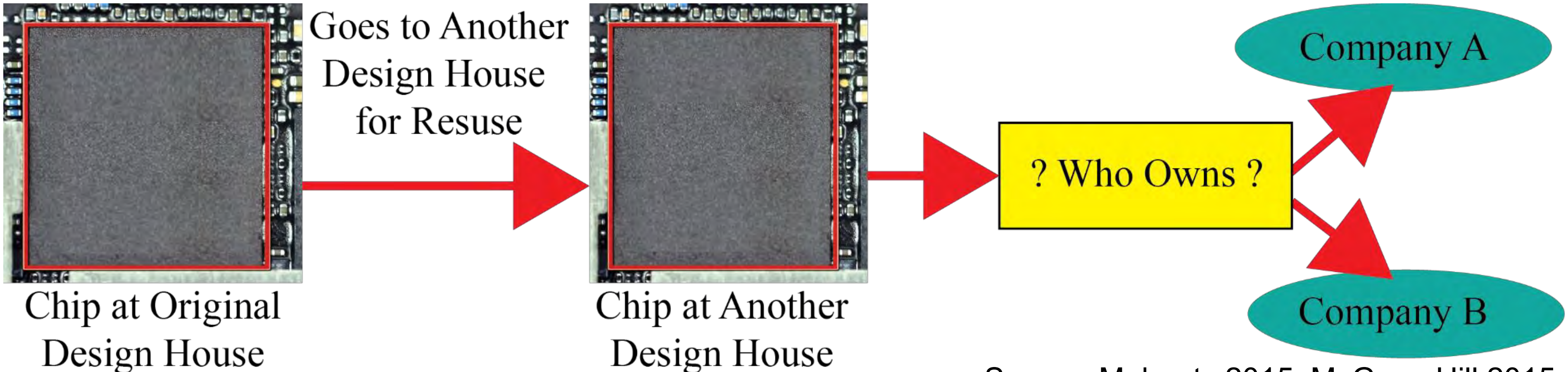



Source: https://pervasive.aau.at/BR/pubs/2016/Haider_IOTPTS2016.pdf

- ❖ On board SRAM of Xilinx Zynq7010 SoC cannot be used as a PUF.
- ❖ A total 1344 number of 3-stage Ring Oscillators were implemented using the Hard Macro utility of Xilinx ISE.

Process Speed: 15 fps
Key Length: 128 bit

# Hardware IP Right Infringement




Source: Mohanty 2015, McGraw-Hill 2015

Hardware IPR Infringement

- False Ownership Claim
- Sub-licensing
- Piracy (Reverse Engineering)

# Cloned/Fake Electronics Hardware – Example - 1


Source: https://petapixel.com/2015/08/14/i-bought-a-fake-nikon-dslr-my-experience-with-gray-market-imports/

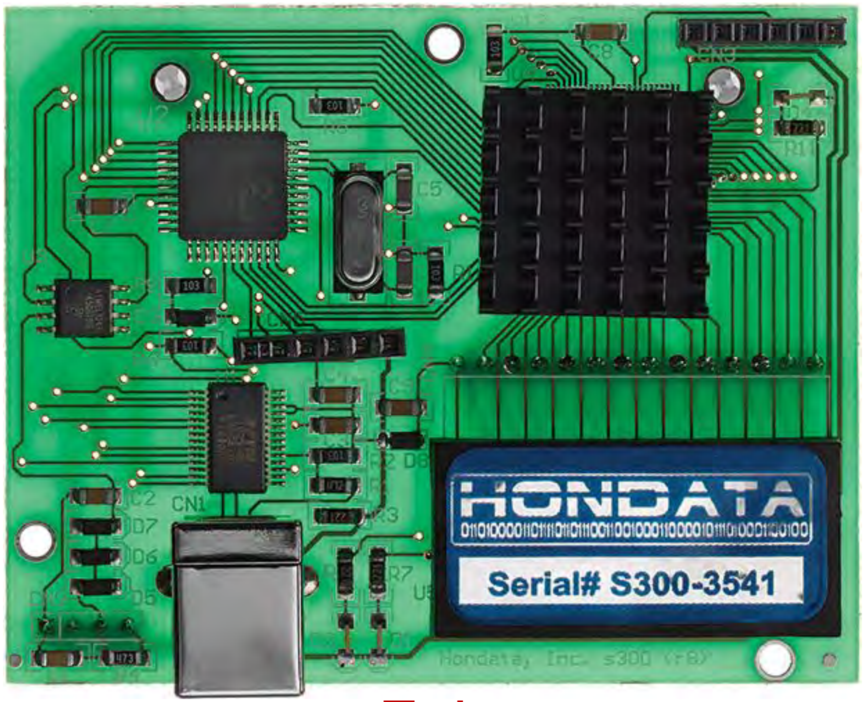


Source: http://www.manoramaonline.com/

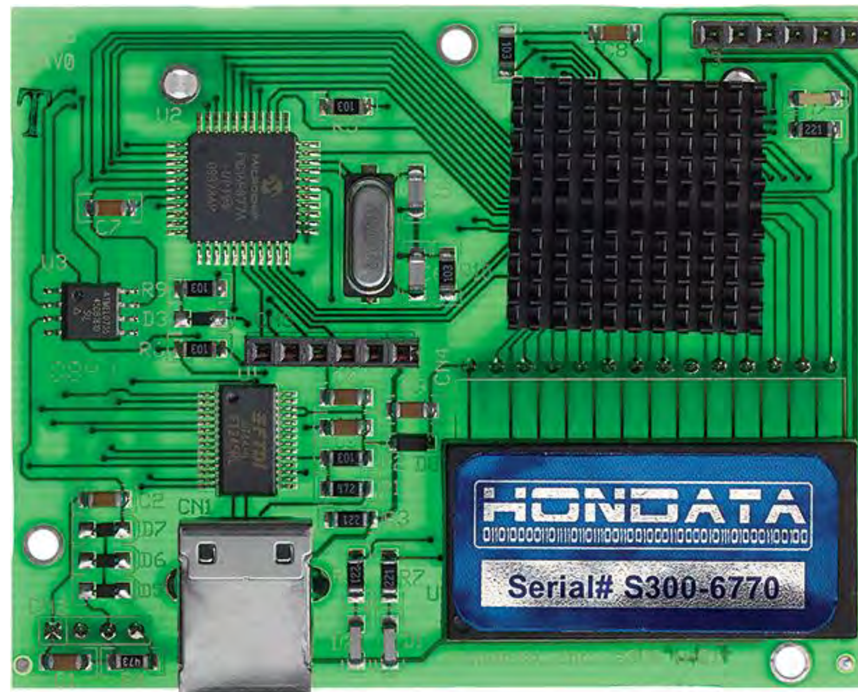

Source: http://www.cbs.cc/fake-capacity-usb-drives/

## Typical Consumer Electronics

# Cloned/Fake Electronics Hardware – Example - 2




Fake

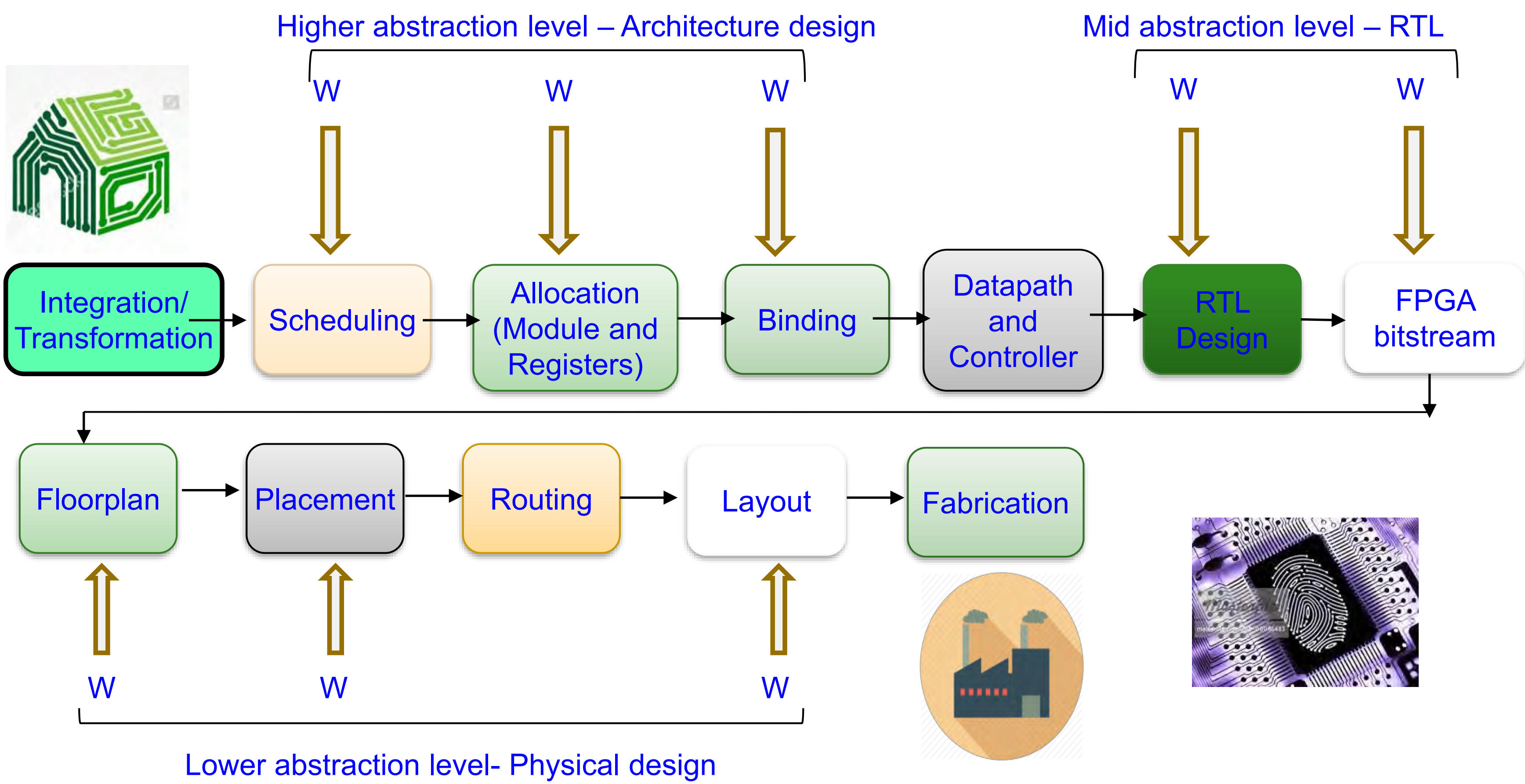



Authentic

A plug-in for car-engine computers.

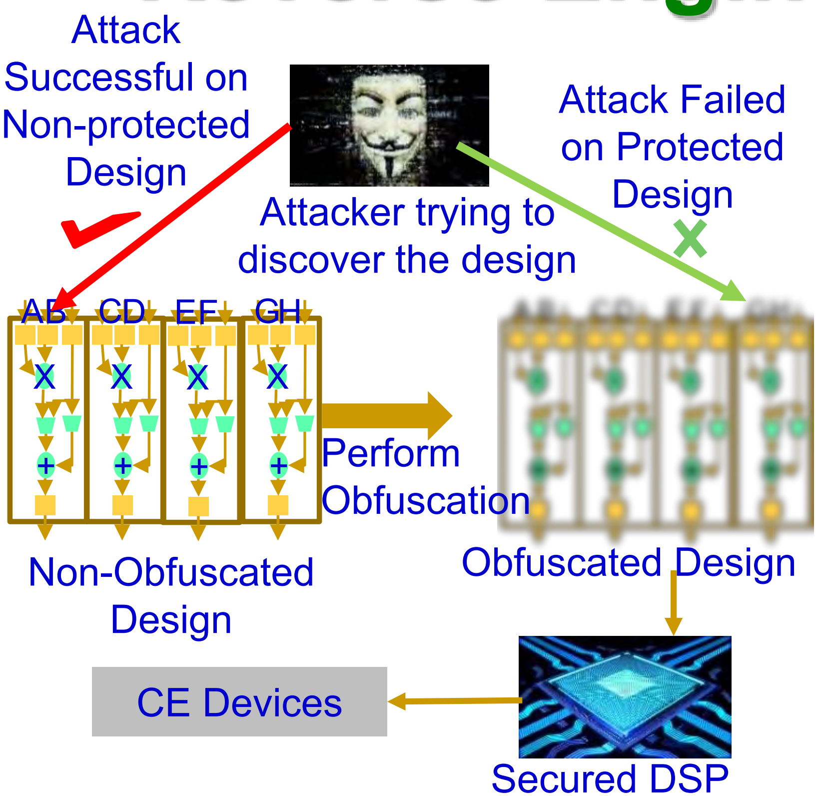
Source: http://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

# Digital Hardware - Watermark




Source: Mohanty 2017: CE Magazine October 2017

# Digital Hardware Synthesis to Prevent Reverse Engineering - Obfuscation




Obfuscation – Intentional modification of the description or the structure of electronic hardware to conceal its functionality for making reverse-engineering difficult.

**Input Block**

Input for Proposed Structural Obfuscation
- CDF/DFG
- Preprocessing of Unrolling Factors

Input for PSO-DSE
- Module Library
- User Constraints
- Maximum Number of Iteration
- Control Parameters: e.g. Swarm Size, # Iterations, etc.

Perform Structural Obfuscation based on 5 Different HLT Techniques

Obfuscated Design for Low Cost Solution

PSO based Design Space Exploration

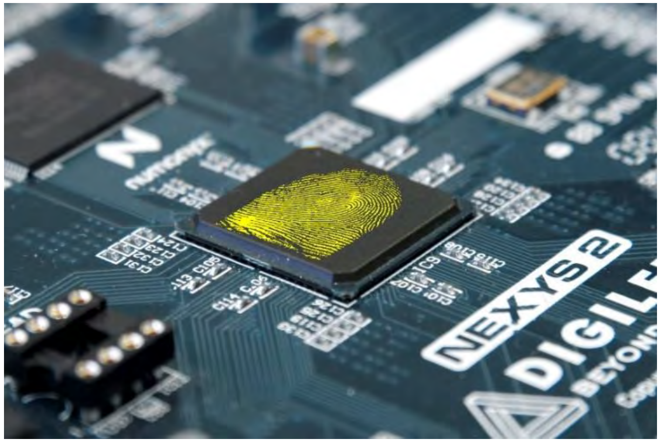
Structurally Obfuscated Low Cost IP Core

**Transformation Techniques**
- Redundant Operation Elimination
- Logic Transformation
- Tree Height Transformation
- Loop Unrolling
- Loop Invariant Code Motion

Source: Sengupta, Mohanty 2017, TCE November 2017

# Protecting Hardware using PUF

- A countermeasure against electronics cloning is a physical unclonable function (PUF).
- It can potentially protect chips, PCBs, and even high-level products like routers.
- PUFs give each chip a unique "fingerprint."

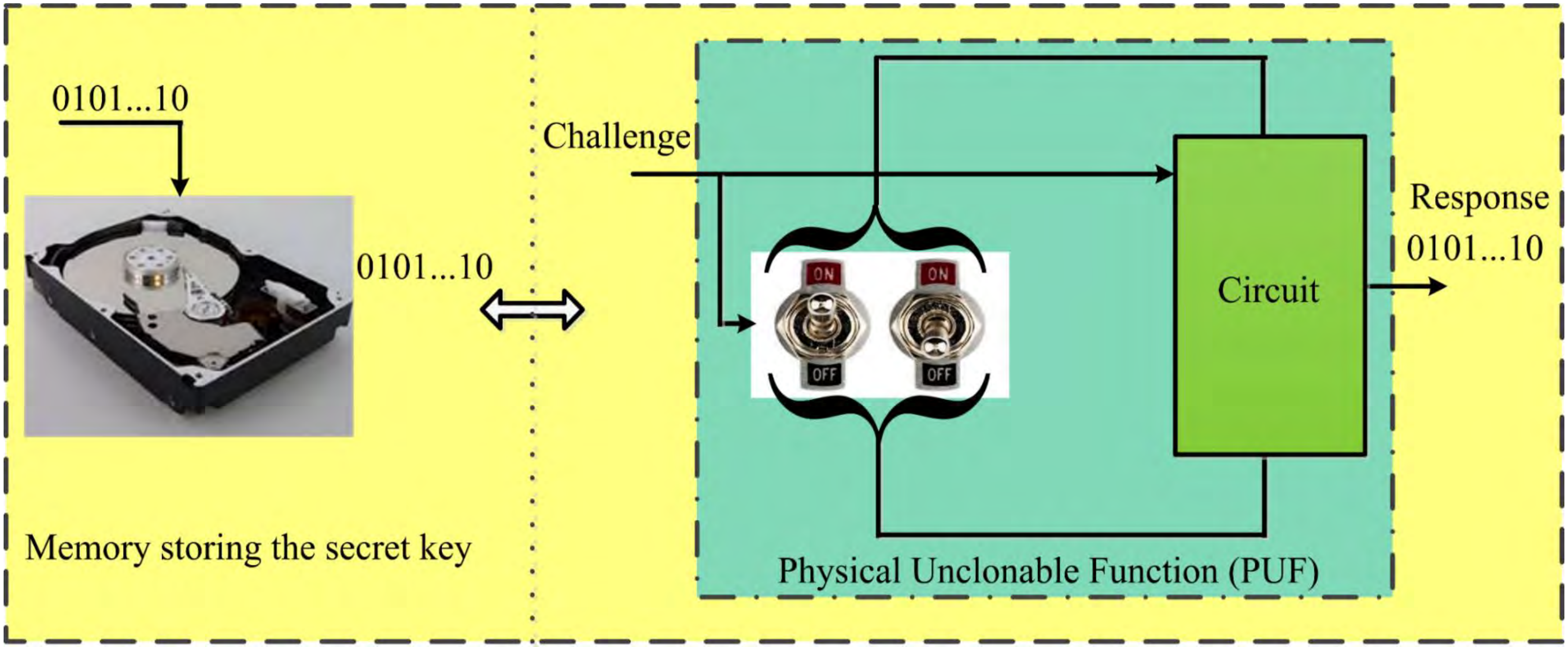



Source: https://phys.org/news/2011-02-fingerprint-chips-counterfeit-proof.html

An on-chip measuring circuit (e.g. a ring oscillator) can generate a characteristic clock signal which allows the chip's precise material properties to be determined. Special electronic circuits then read these measurement data and generate the component-specific key from the data.

Source: http://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

# PUF – Principle …

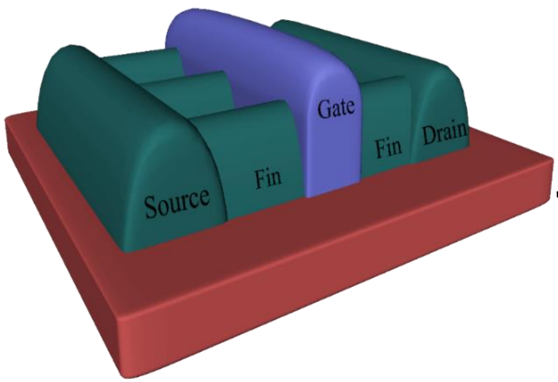



PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

Source: Mohanty 2017, IEEE Potentials Nov-Dec 2017

# PUF - Principle

Manufacturing Variations
(e.g. Oxide Growth, Ion
Implantation, Lithography)




Parameters
Affected
Due to
Variations
(e.g. Length,
Gate-Oxide
Thickness,
Fin Height,
Fin Width)

Challenge Inputs
(Inputs given to PUF Module,
e.g. Select line of Multiplexer)

PUF Design
(e.g. Arbiter PUF,
SRAM PUF,
Ring Oscillator
PUF)

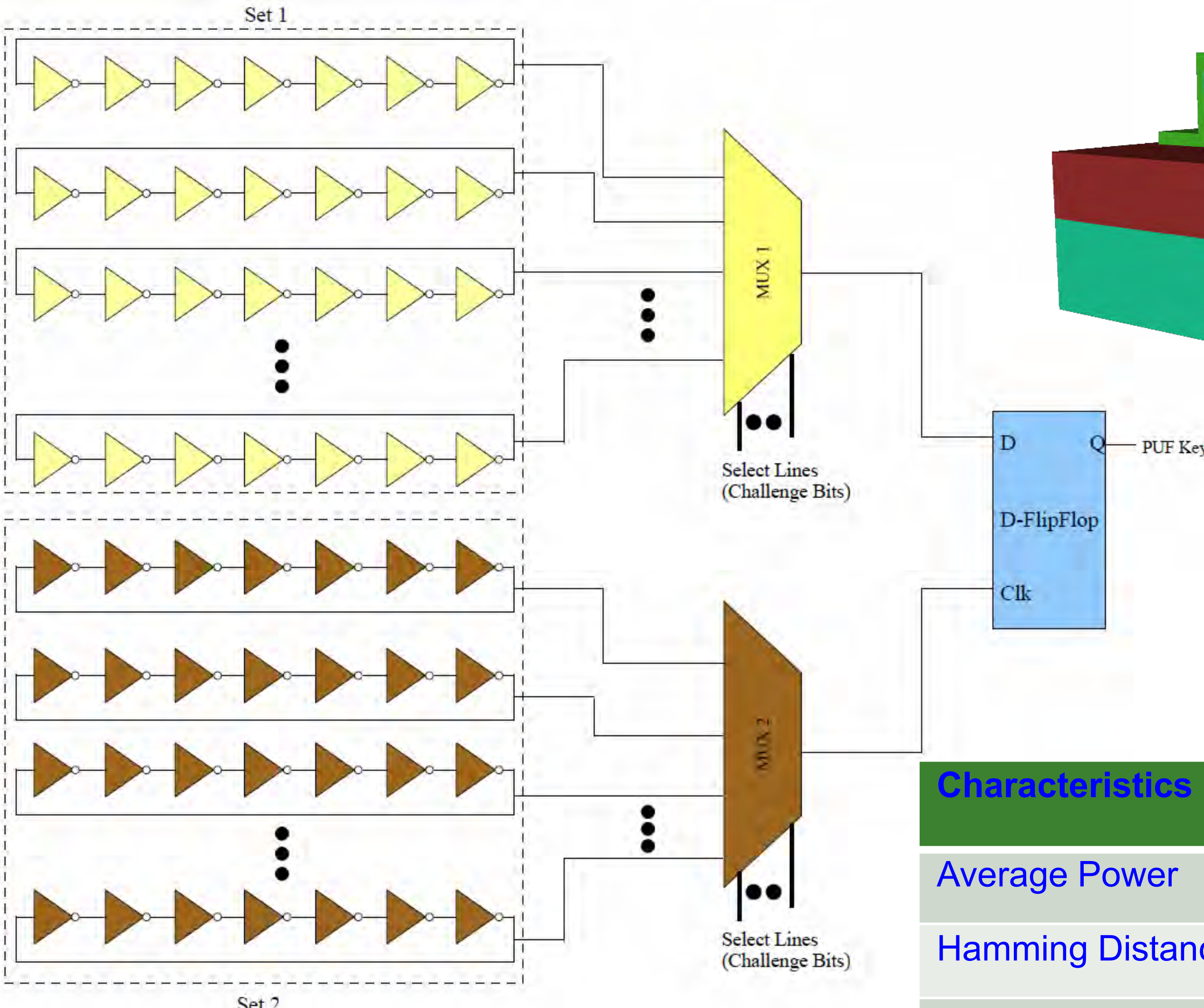
Challenge
Response
(Outputs from a
PUF Module)

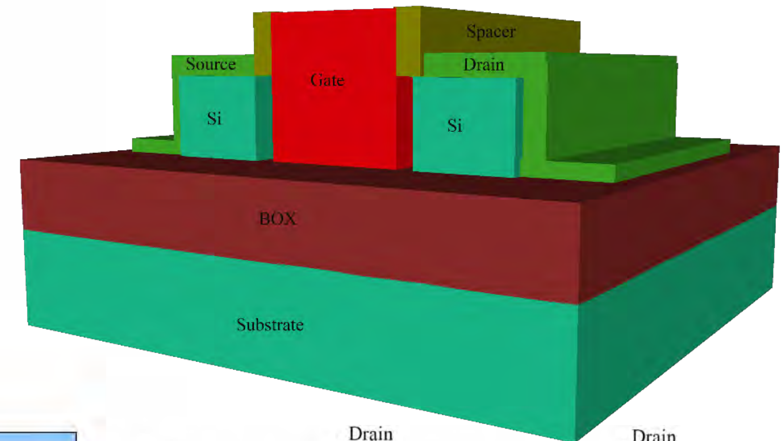
Random
Binary Output
010101 …

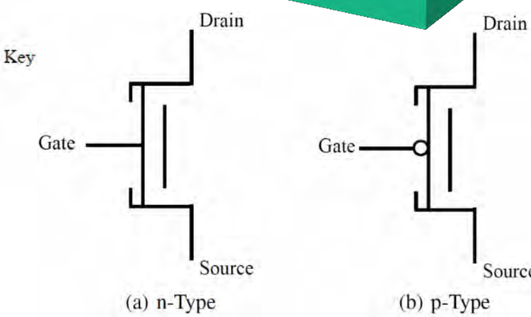
Silicon manufacturing process variations are turned into a feature rather than a problem.

Source: Mohanty 2017, Springer ALOG 2017

# Power Optimized Hybrid Oscillator Arbiter PUF



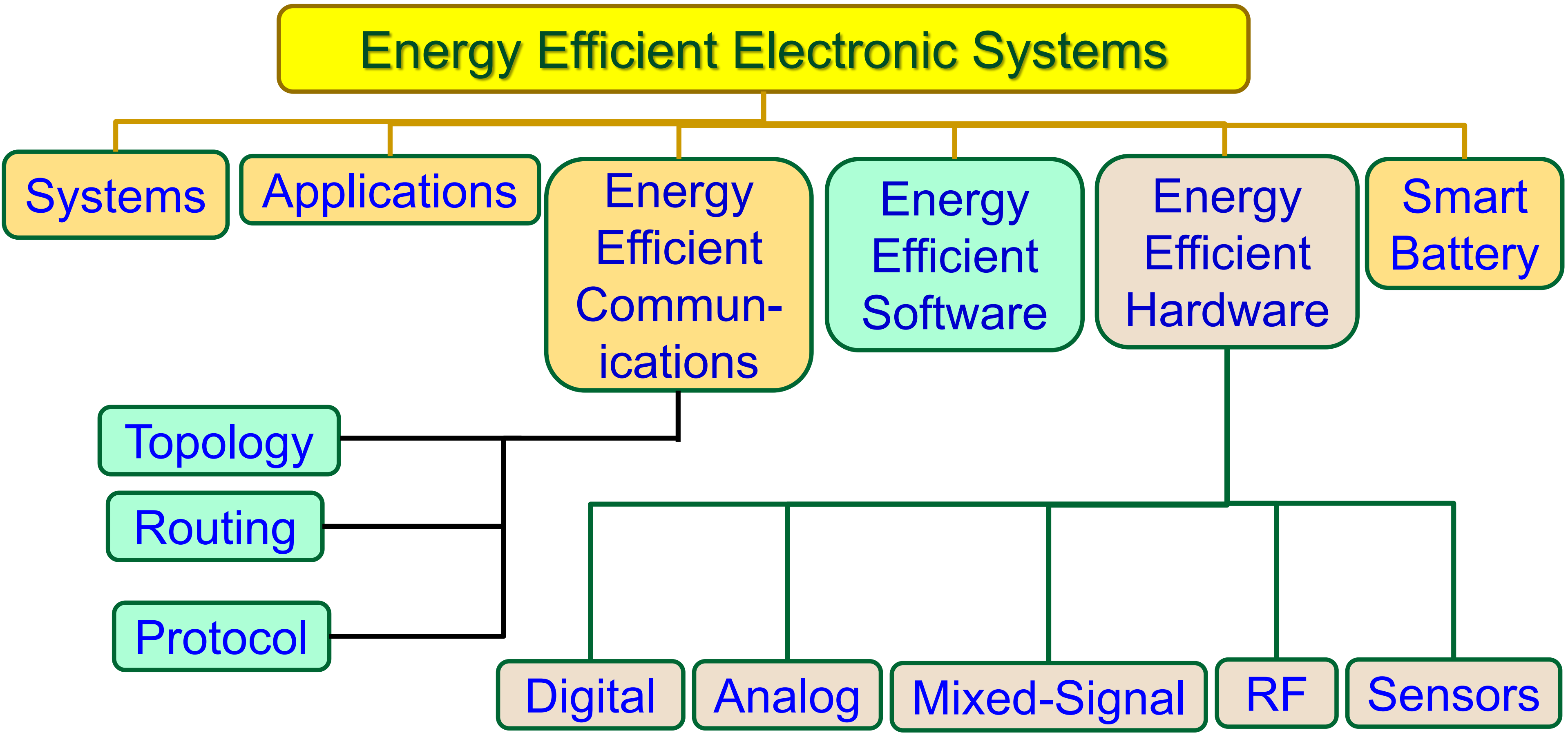




| Characteristics | FinFET Technology | DLFET Technology |
|---|---|---|
| Average Power | 219.34 μW | 121.3 μW |
| Hamming Distance | 49.3 % | 48 % |
| Time to generate key | 150 ns | 150 ns |

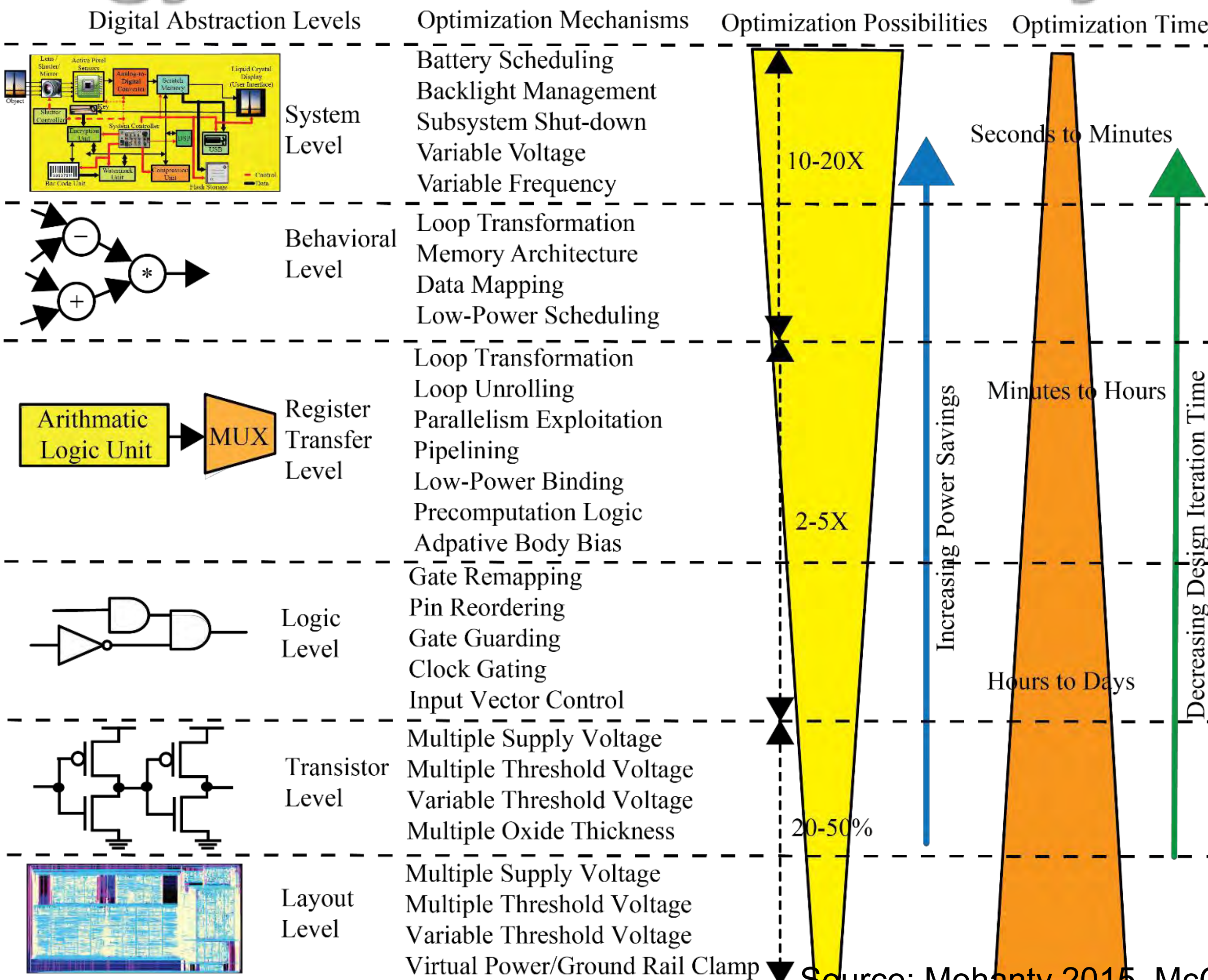
Source: Mohanty 2018, TSM May 2018

# Addressing Energy Constraints in CE

# Energy Efficient Electronic Systems: Possible Solution Fronts



# Energy Reduction in CE Systems



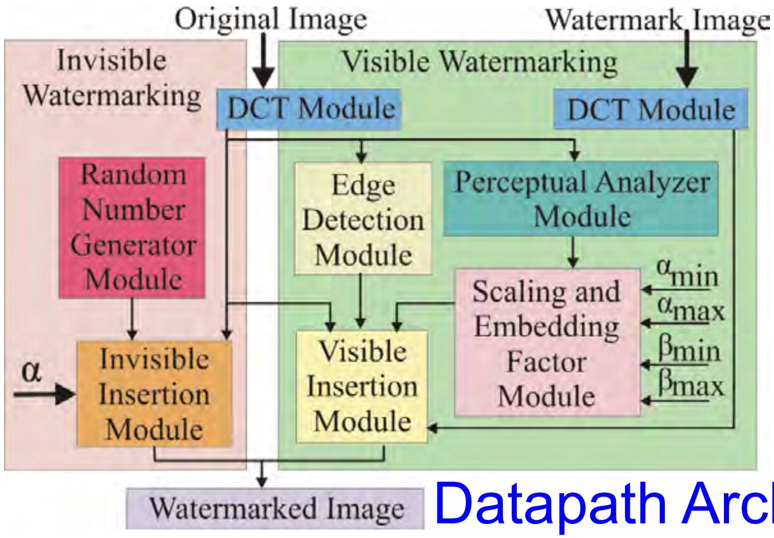

Source: Mohanty 2015, McGraw-Hill 2015

# Energy Reduction in CE Hardware

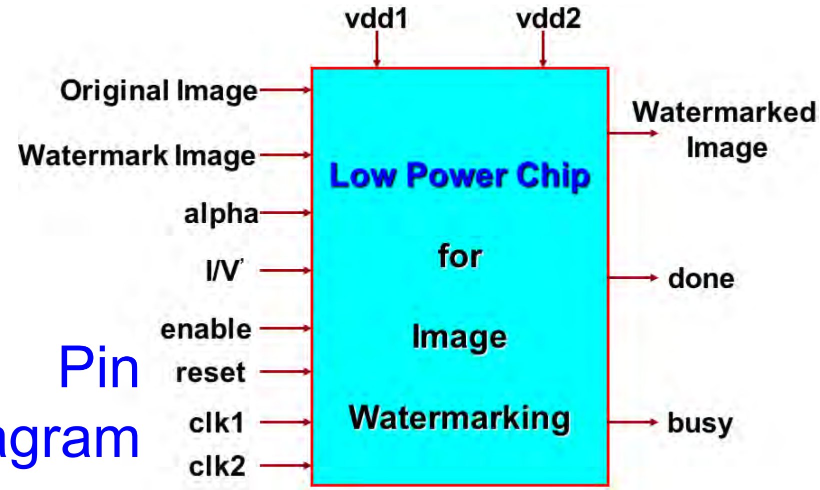
- System-on-a-chip (SoC) Power or Energy Optimization
  - Presilicon Techniques
    - Multiple Voltage Islands
    - Multiple Threshold Devices
    - Multiple Oxide Devices
    - Minimize Capacitance Design
    - Microarchitecture Parallelism
  - Postsilicon Techniques
    - Through Hardware
      - Clock Gating
      - Data Gating
      - Power Gating
      - Variable Frequency
      - Variable Supply Voltage aka Dynamic Voltage Scaling
      - Variable Threshold Devices
      - Intelligent Battery
    - Through Software
      - Adaptive Body Bias for Variable Threshold
      - Variable Supply Voltage aka Dynamic Voltage Scaling
      - Operation Scheduling
      - Battery Scheduling
      - Backlight Management
      - Software Optimization

Source: Mohanty 2015, McGraw-Hill 2015

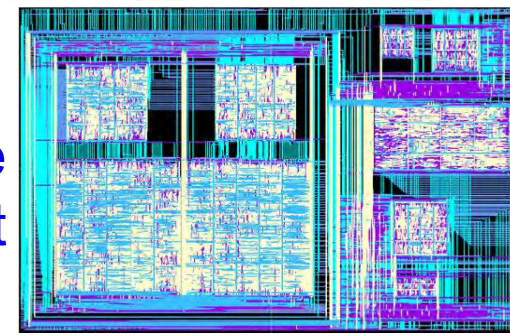
# Dual-Voltage/Frequency Based Hardware



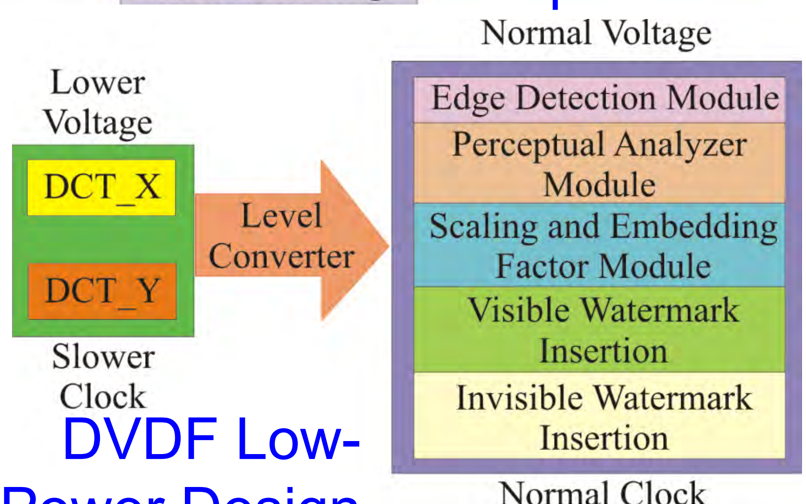

Datapath Architecture




Pin Diagram



Hardware Layout




DVDF Low-Power Design

Source: Mohanty 2006, TCASII May 2006

**Physical Design Data**
Total Area : 16.2 sq mm
No. of Transistors: 1.4 million
Power Consumption: 0.3 mW

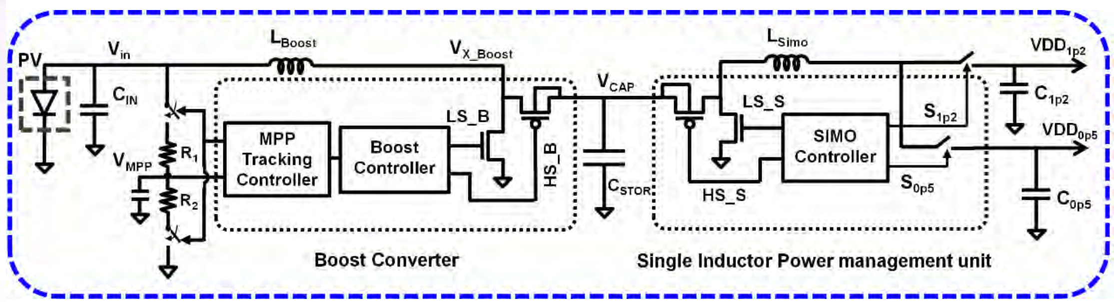
# Battery-Less IoT

Battery less operations can lead to reduction of size and weight of the edge devices.


Source: http://newscenter.ti.com/2015-02-25-TI-makes-battery-less-IoT-connectivity-possible-with-the-industrys-first-multi-standard-wireless-microcontroller-platform


Batter-Less SoC

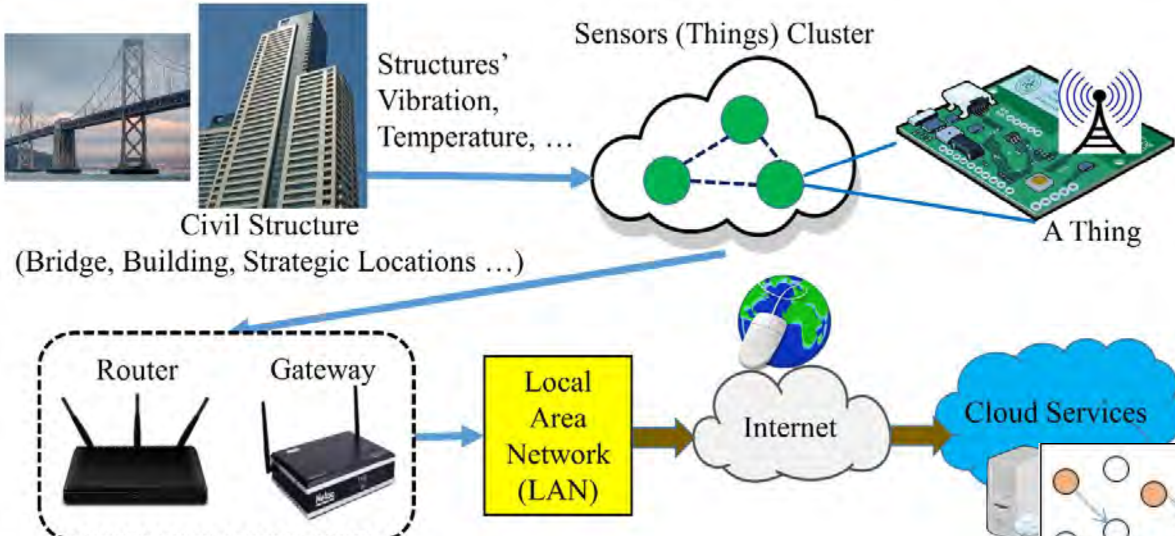
Source: https://www.technologyreview.com/s/529206/a-batteryless-sensor-chip-for-the-internet-of-things/



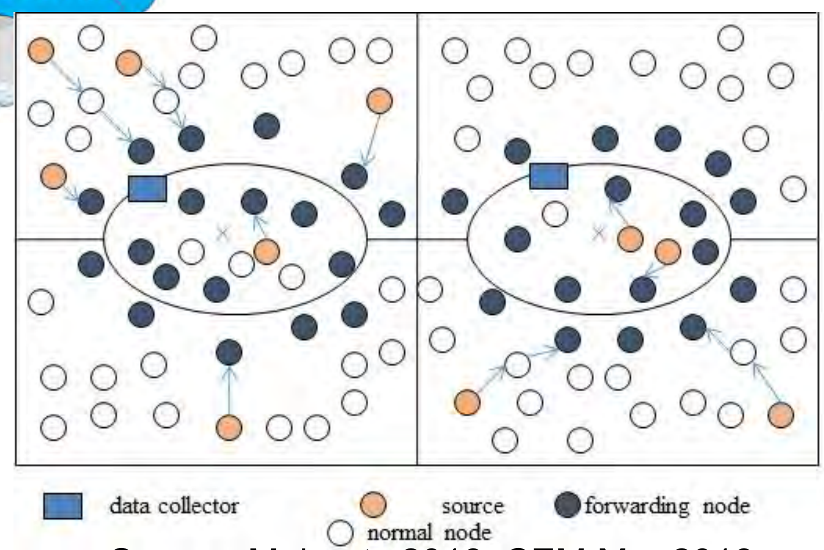

Energy Harvesting and Power Management

Source: http://rlpvlsi.ece.virginia.edu/node/368

# Sustainable IoT – Low-Power Sensors and Efficient Routing



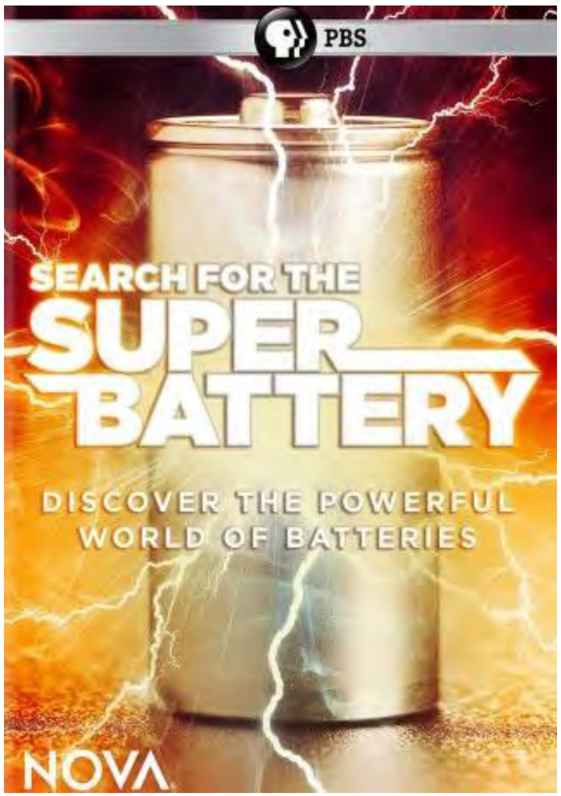

- IoT - sensors near the data collector drain energy faster than other nodes.
- Solution Idea - Mobile sink in which the network is balanced with node energy consumption.
- Solution Need: New data routing to forward data towards base station using mobile data collector, in which two data collectors follow a predefined path.



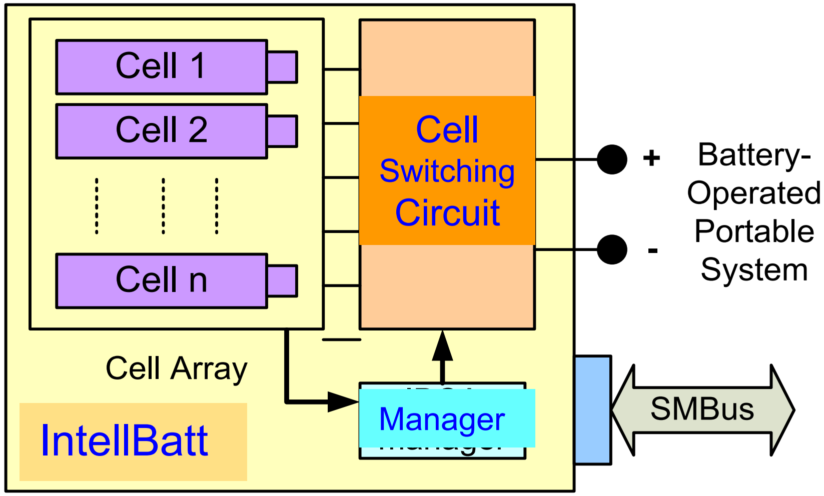

Source: Mohanty 2018, CEM Mar 2018

# Energy Storage - High Capacity and Efficiency Needed

| Battery | Conversion Efficiency |
|---|---|
| Li-ion | 80% - 90% |
| Lead-Acid | 50% - 92% |
| NiMH | 66% |




Intelligent Battery

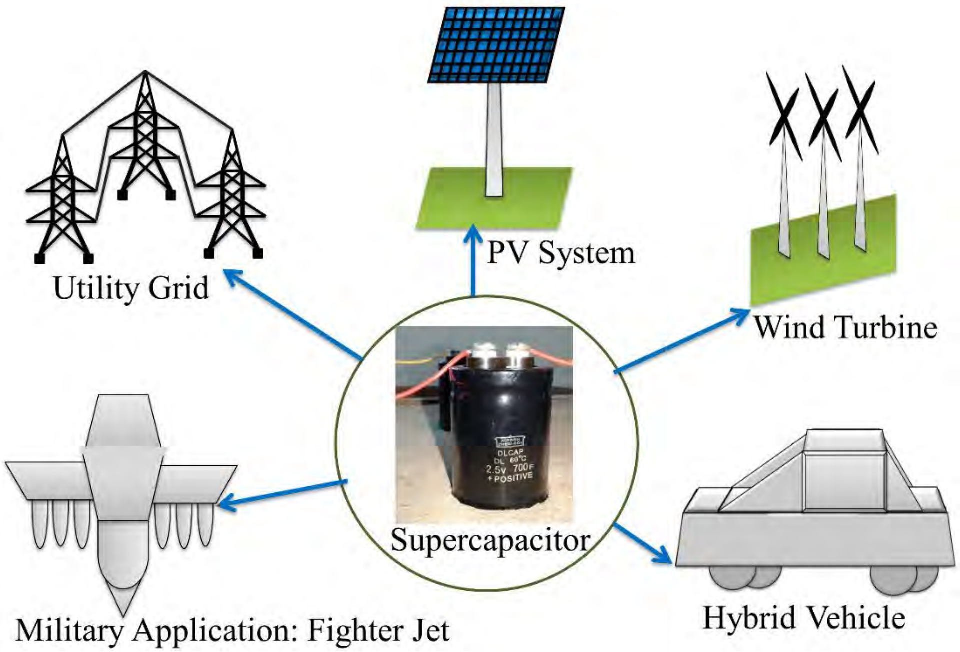


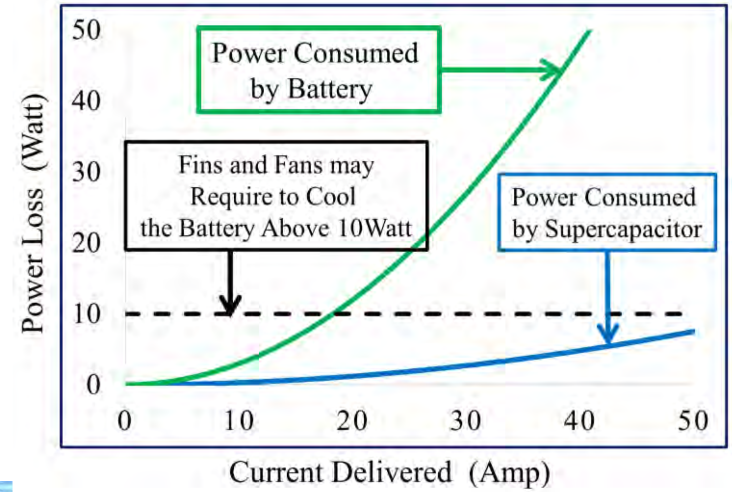

Mohanty 2010: IEEE Computer, March 2010.
Figure 1: IntellBatt Architecture
Mohanty 2018: ICCE 2018

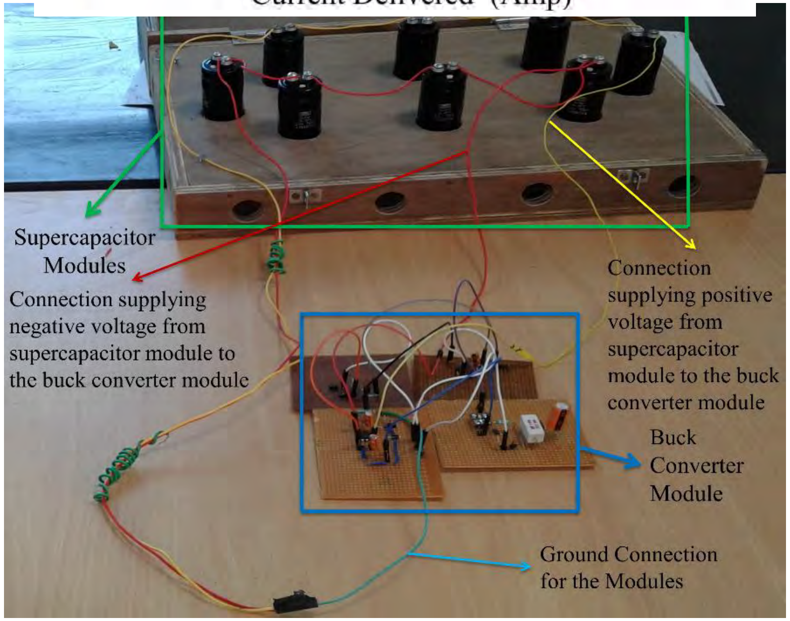

Lithium Polymer Battery


Supercapacitor

# Supercapacitor based Power for CE



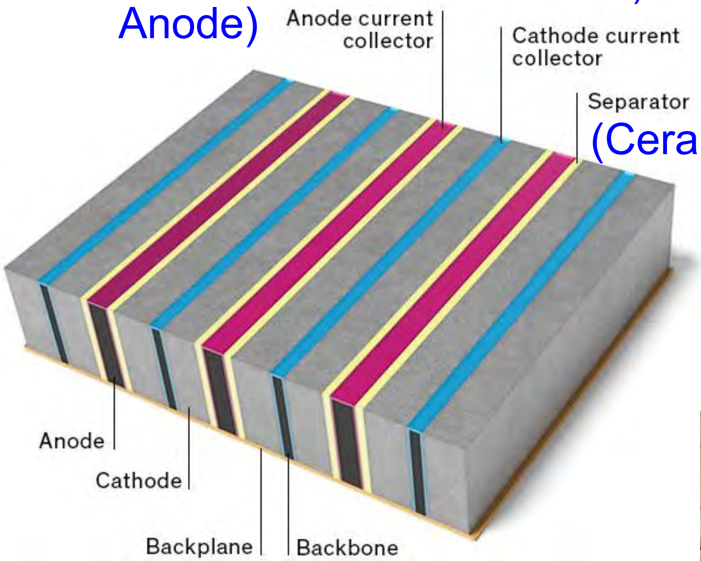

Source: Mohanty 2018, CEM Sep 2018

# Energy Storage - High Capacity and Safer Needed

(Silicon Anode)

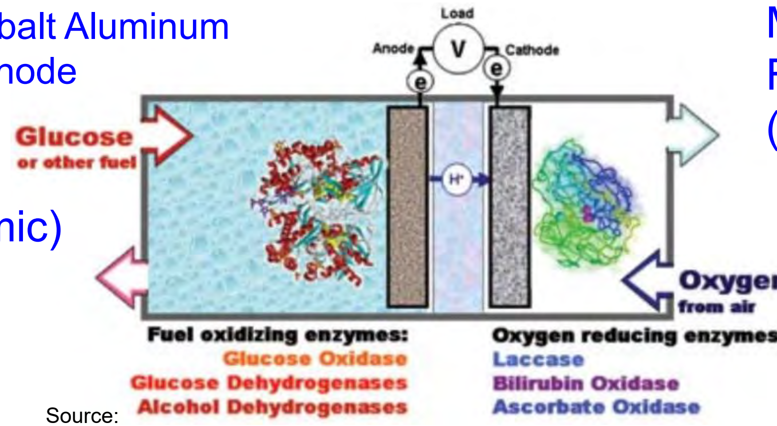
(Lithium Nickel Cobalt Aluminum Oxide - NCA) Cathode

(Ceramic)





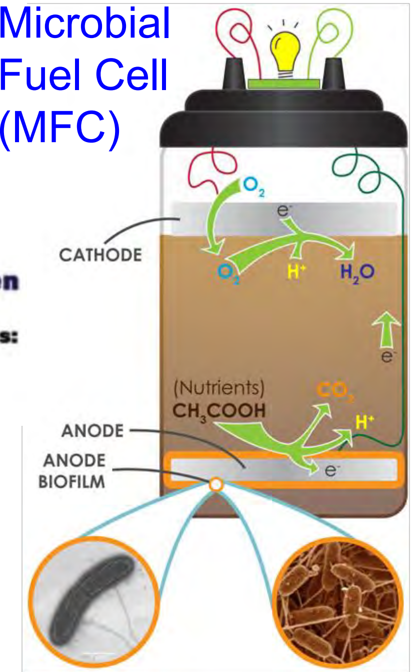
Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery

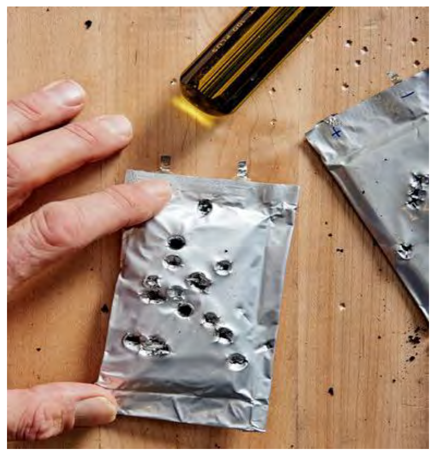



Source: https://www.electrochem.org/dl/interface/sum/sum07/su07_p28_31.pdf

Enzymatic Biofuel Cell

Microbial Fuel Cell (MFC)

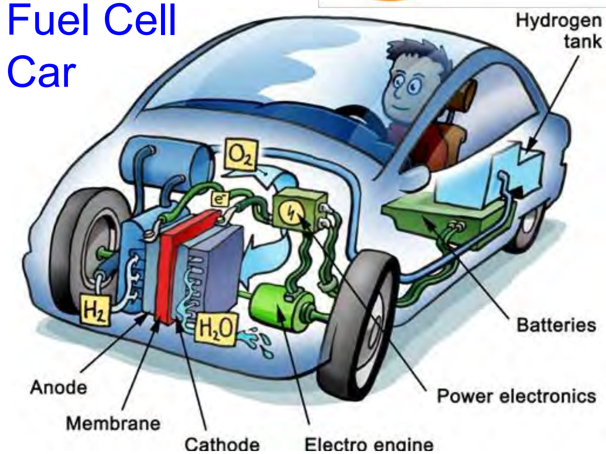


Solid Polymer Lithium Metal Battery

Source: https://www.nytimes.com/2016/12/11/technology/designing-a-safer-battery-for-smartphones-that-wont-catch-fire.html

Fuel Cell Car



# Software Vs Hardware Attacks and Solutions in CE

# CE System Security – Smart Car

**Protecting Communications**
Particularly any Modems for In-vehicle Infotainment (IVI) or in On-board Diagnostics (OBD-II)

**Over The Air (OTA) Management**
From the Cloud to Each Car

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive security issues.

**Protecting Each Module**
Sensors, Actuators, and Anything with an Microcontroller Unit (MCU)

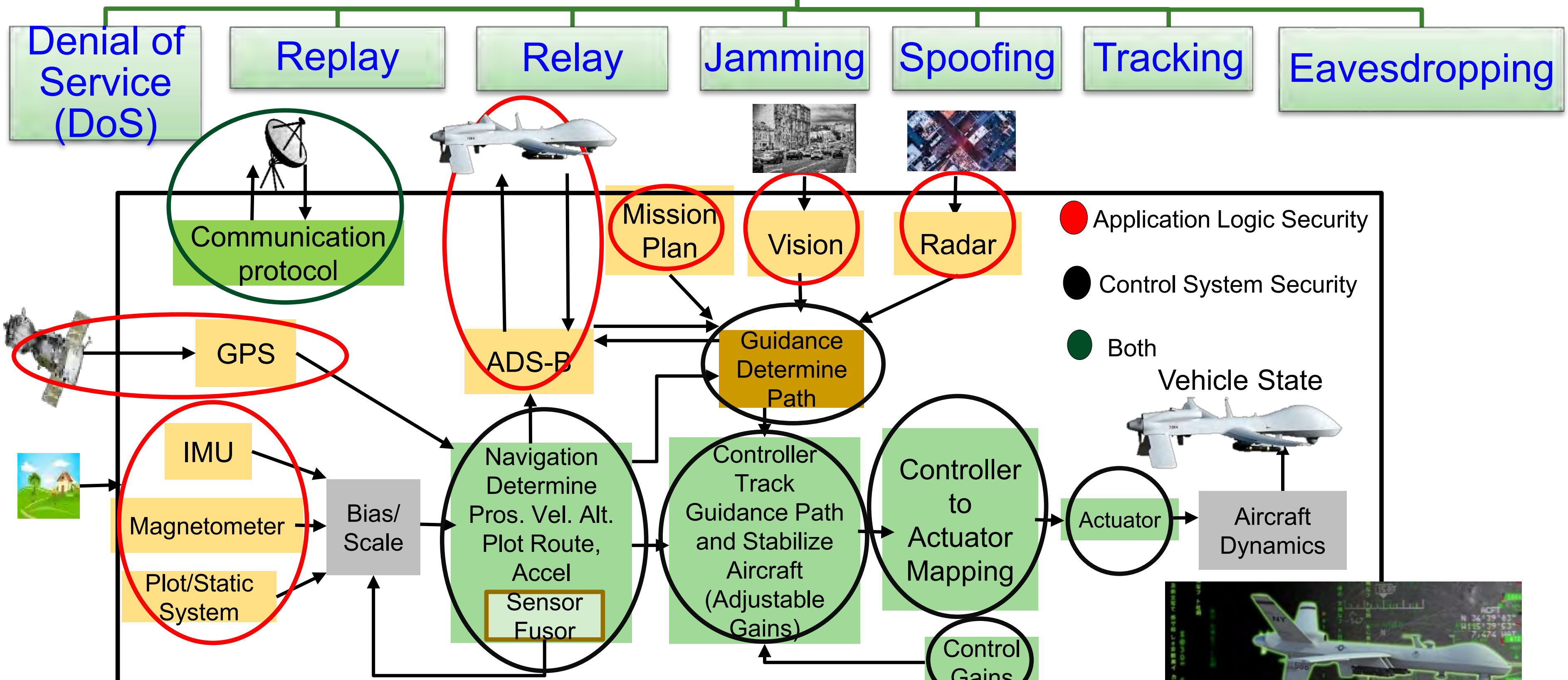
**Mitigating Advanced Threats**
Analytics in the Car and in the Cloud

- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

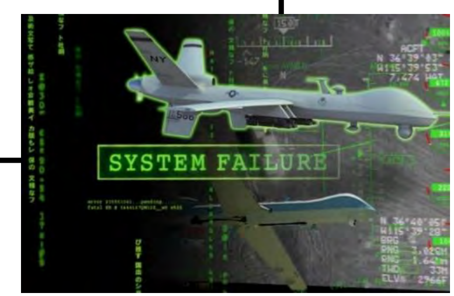
Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

# CE System Security – UAV



Source: http://www.secmation.com/control-design/



Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

## Security Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

# Attacks - Software Vs Hardware

## Software Based

- Software attacks via communication channels
- Typically from remote
- More frequent
- Selected Software based:
  - Denial-of-Service (DoS)
  - Routing Attacks
  - Malicious Injection
  - Injection of fraudulent packets
  - Snooping attack of memory
  - Spoofing attack of memory and IP address
  - Password-based attacks

## Hardware Based

- Hardware or physical attacks
- Maybe local
- More difficult to prevent
- Selected Hardware based:
  - Hardware backdoors (e.g. Trojan)
  - Inducing faults
  - CE system tampering/jailbreaking
  - Eavesdropping for protected memory
  - Side channel attack
  - CE hardware counterfeiting

# Security - Software Vs Hardware

**Software Based**

- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can't stop hardware reverse engineering

**Hardware Based**

- High-Speed operation
- Energy-Efficient operation
- Low-cost using ASIC and FPGA
- Tasks of encryption easy compared to software – bit permutation
- Easy integration in CE systems
- Possible security at source-end like sensors, better suitable for IoT
- Susceptible to side-channel attacks
- Can't stop software reverse engineering

Maintaining of Security of Consumer Electronics, CE Systems, IoT, CPS, etc. needs Energy and affects performance.

# Hardware Assisted Security

- Software based Security:
  - A general purposed processor is a deterministic machine that computes the next instruction based on a program counter.
  - Software based security approaches that rely on some form of encryption can't be full proof as breaking them is just matter of time.
  - Quantum computers that use different paradigms than the existing computers will make things worse.
- Hardware-Assisted Security: Security/ Protection provided by the hardware:
  - for information being processed by a CE system,
  - for hardware itself, and/or
  - for the overall CE system.

# Hardware Assisted Security

- Hardware-Assisted Security: Security provided by hardware for:

  (1) information being processed,

  (2) hardware itself, and/or

  (3) overall system.

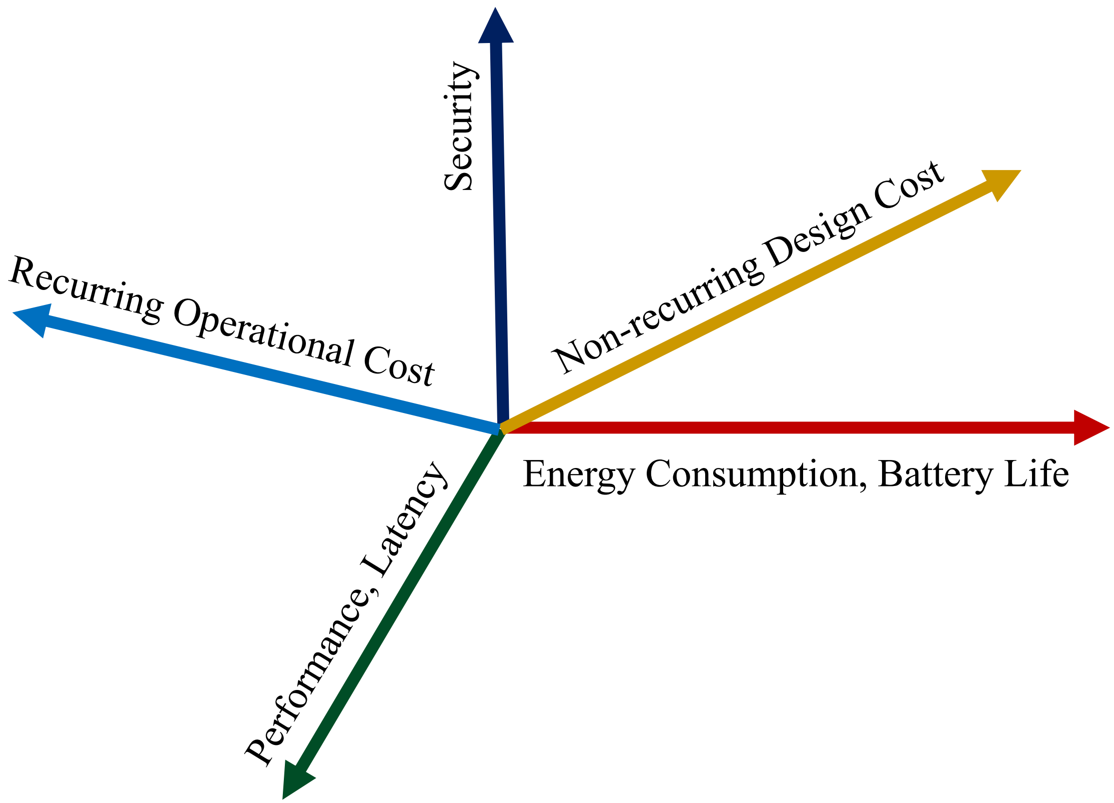
- Additional hardware components used for security.
- Hardware design modification is performed.
- System design modification is performed.

RF Hardware Security | Digital Hardware Security – Side Channel

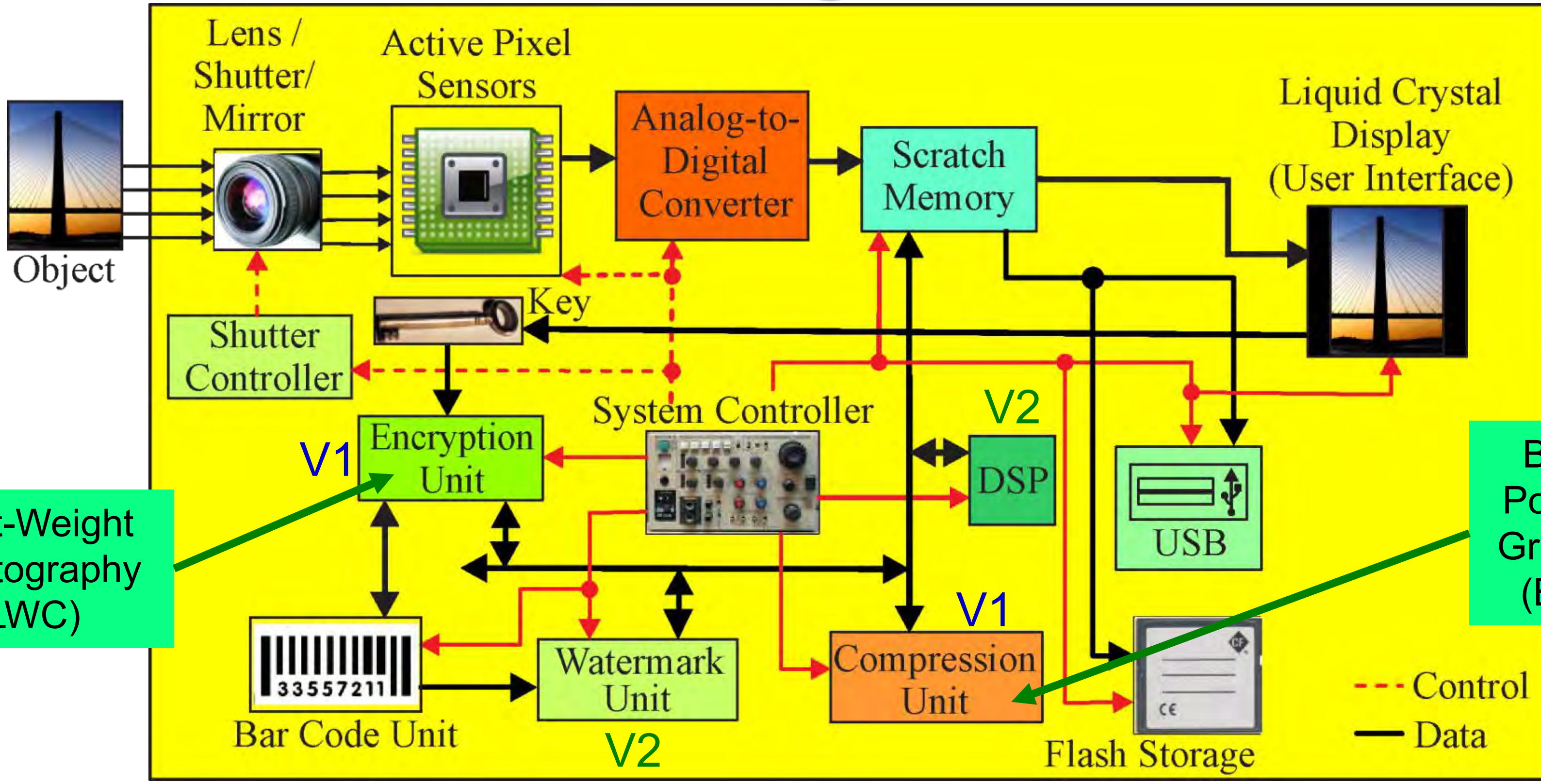
Hardware Trojan Protection | Information Security, Privacy, Protection

IR Hardware Security | Memory Protection | Digital Core IP Protection

# CE System Design and Operation Tradeoffs



# CE System Security & Energy Tradeoffs – System Level



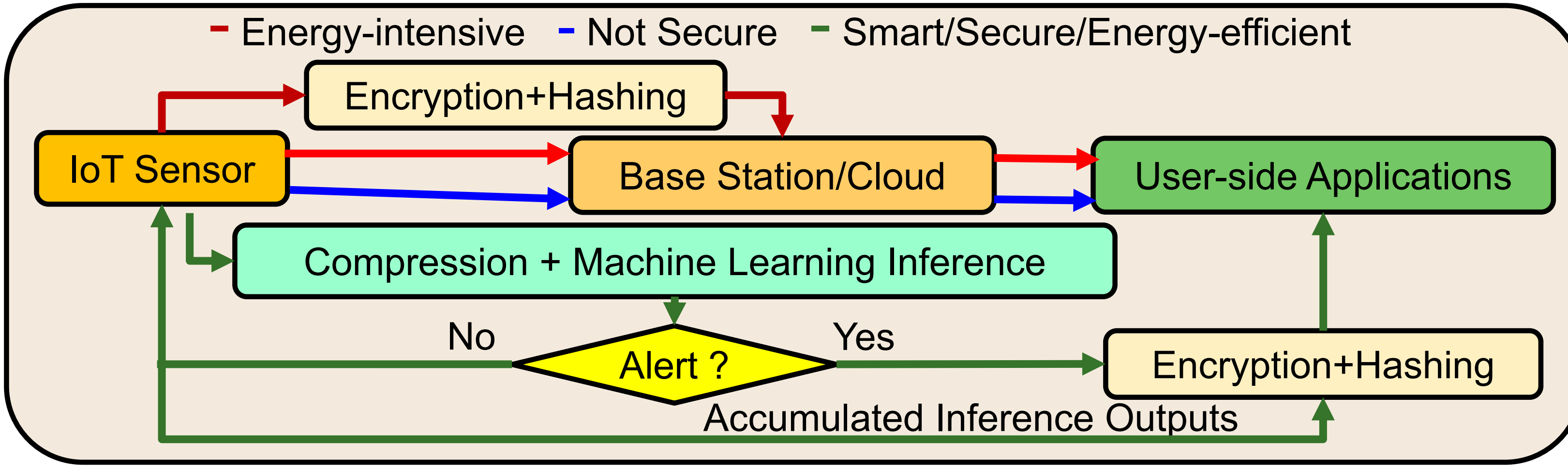

Light-Weight Cryptography (LWC)

Better Portable Graphics (BPG)

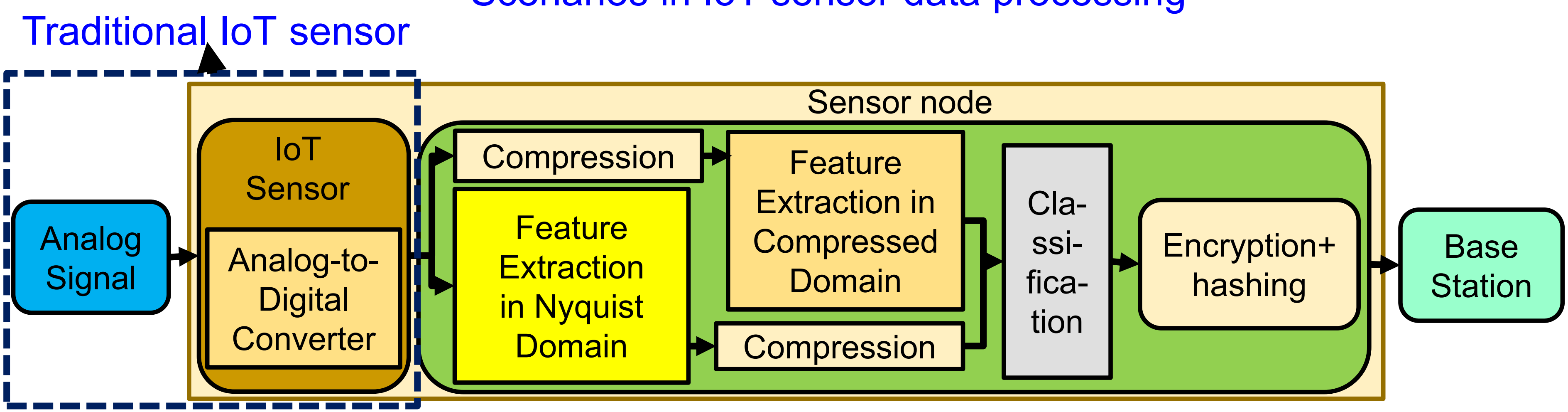
Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

Source: Mohanty 2006, TCAS-II May 2006; Mohanty 2009, JSA Oct 2009; Mohanty 2016, Access 2016

# Security & Energy Tradeoff - Sensor



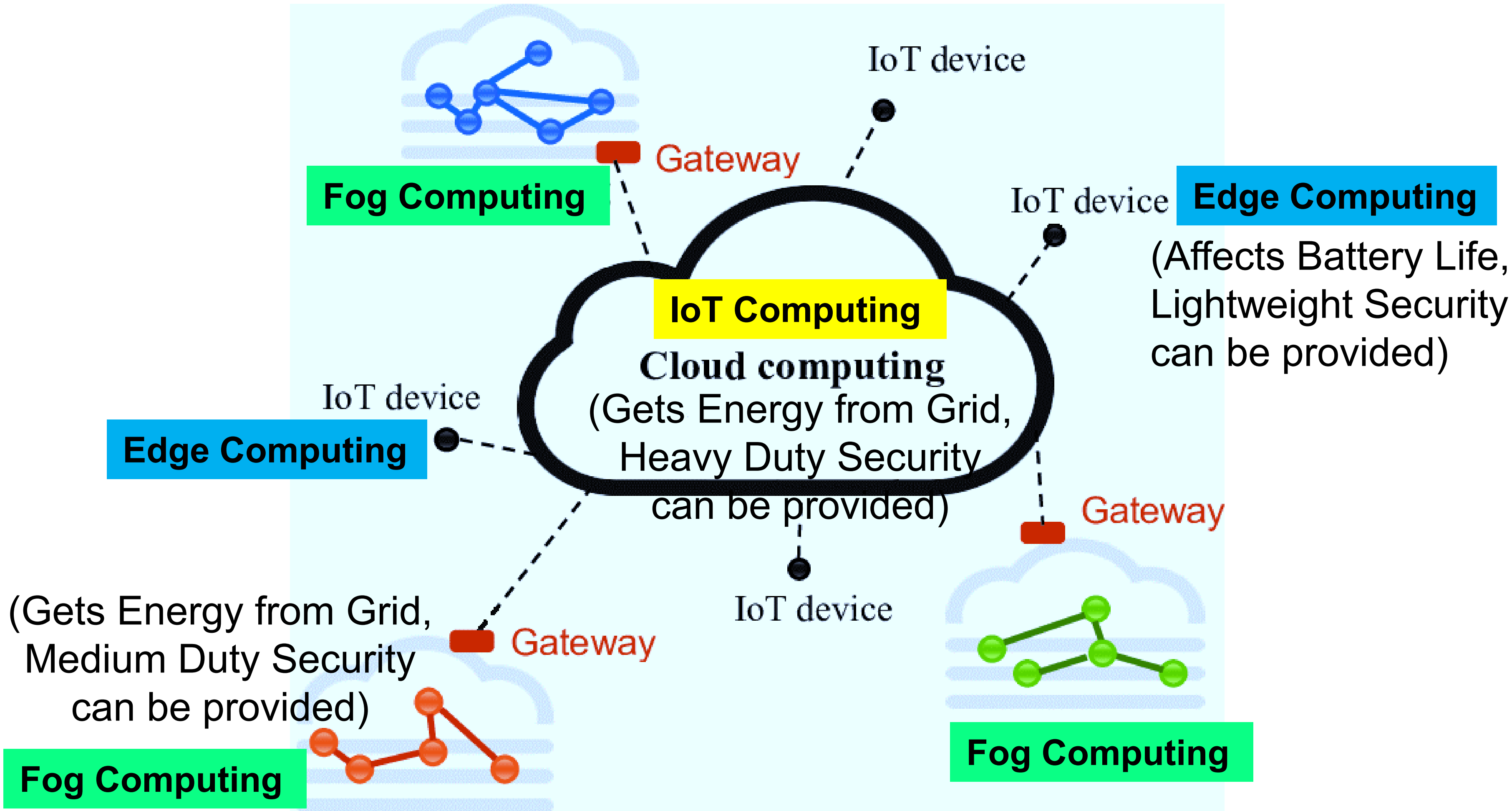

Scenarios in IoT sensor data processing




Smart, secure, and energy-efficient IoT sensor architecture

Source: Akmandor 2018: CICC 2018

# IoT Vs Fog Vs Edge Computing – Security, Energy Tradeoffs



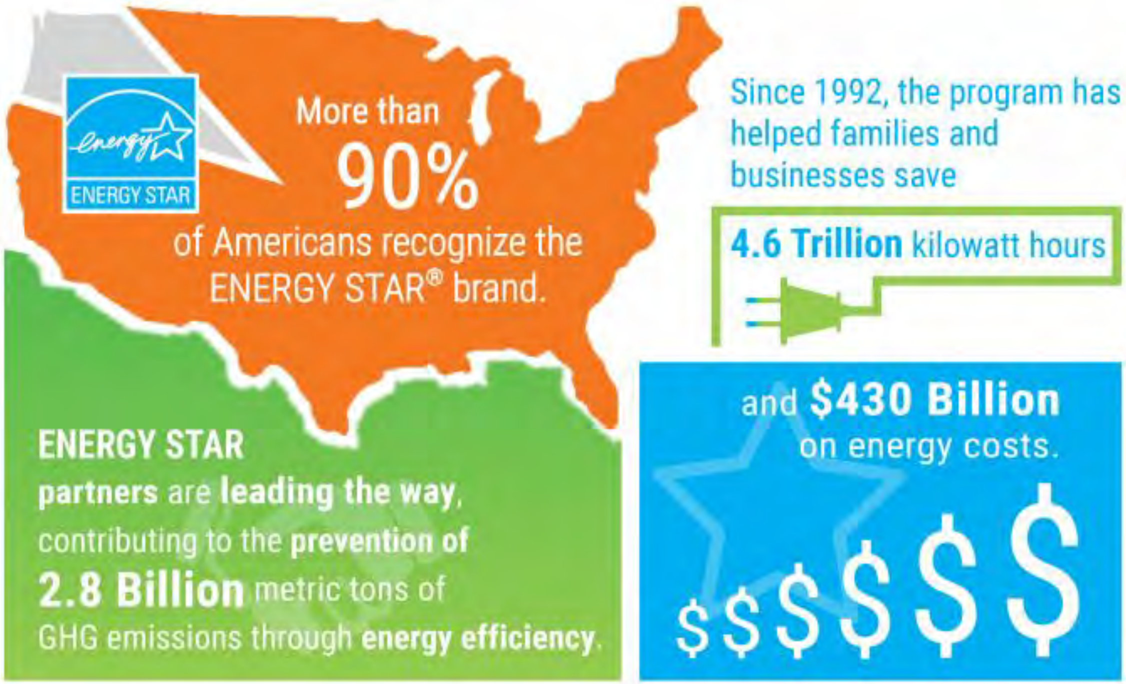

Source: https://www.researchgate.net/figure/311918306_fig1_Fig-1-High-level-architecture-of-Fog-and-Cloud-computing

# Trustworthy CE System

- A selective attributes of CE system to be trustworthy:
  - It must maintain integrity of information it is processing.
  - It must conceal any information about the computation performed through any side channels such as power analysis or timing analysis.
  - It must perform only the functionality it is designed for, nothing more and nothing less.
  - It must not malfunction during operations in critical applications.
  - It must be transparent only to its owner in terms of design details and states.
  - It must be designed using components from trusted vendors.
  - It must be built/fabricated using trusted fabs.

# Can there be Security Rating for CE Appliances or Systems?

# Energy Star Ratings



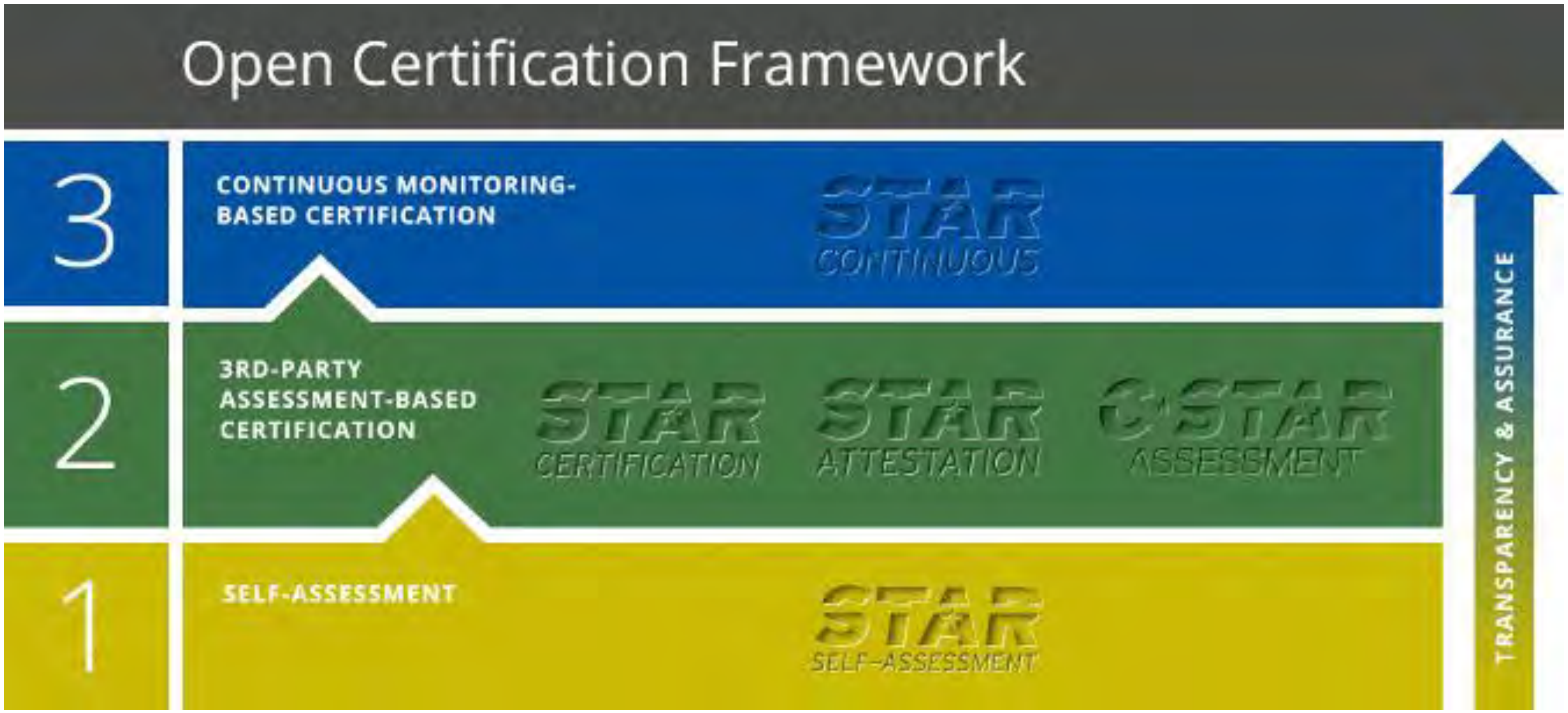

Source: https://www.energystar.gov/about/2017_energy_star_award_winners

CODE FOR A SUSTAINABLE BUILT ENVIRONMENT
BREEAM
BRE GLOBAL

Source: https://www.breeam.com/


Source: https://new.usgbc.org/leed

# Security Star Ratings




Source: https://cloudsecurityalliance.org/star/#_overview

Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)

# Conclusions

# Conclusions

- Privacy, security, and ownership rights are important problems in CE systems.
- Energy dissipation and performance are also key challenges.
- Hardware-Assisted Security: Security provided by hardware for: (1) information being processed, (2) hardware itself, (3) overall system.
- It is low-cost and low-overhead solution as compared to software only based.
- Many hardware based solutions exist for media copyright and information security.
- Many hardware design solutions exist for IP protection and security of the CE systems that use such hardware.
- NFC and RFID security are important for IoT and CE security.
- Privacy and security in smart healthcare need research.

# Future Directions

- Energy-Efficient CE is needed.
- Security, Privacy, IP Protection of Information and System need more research.
- Security of the CE systems (e.g. smart healthcare device, UAV, Smart Cars) needs research.
- Safer and efficient battery need research.
- Important aspect of smart CE design: trade-offs among energy, response latency, and security

2018 IEEE CONSUMER ELECTRONICS SOCIETY
NEW MEMBER APPLICATION

Society Website: https://cesoc.ieee.org/

Membership Fee: $20
Student Membership Fee: $10

These offers apply to full conference and full conference attendees during the conference only.

Free CE Society memberships are open to all current IEEE members. Membership periods end Dec 31 2018 and must be renewed by the member through IEEE.

Incomplete or illegible applications cannot be processed. Write legibly
Enter your name as you want it to appear on you membership card and IEEE correspondence.

## Your Contact information

Male ☐ Female ☐ Date of Birth (DD/MM/YYYY) / / ________

Title First/Given Name Middle Name Last/Family Surname

**Home**

Street Address

City State/Province

Postal Code Country

Home Phone

Home Email

## Your Professional Experience

(circle your choices below)

I have graduated from a three-to-five-year academic program with a university-level degree.

This academic institution or program is accredited in the country where the institution is located.
Yes No Do not know

I have _____ years of professional experience in teaching, creating, developing, practicing, or managing within the following field:

Engineering

Computer Sciences and Information Technologies

Physical Sciences

Biological and Medical Sciences

Mathematics

Technical Communications, Education, Management, Law and Policy
Other (please specify): ____________

**Are you or were you ever a member of the IEEE?** Yes No
If Yes, provide, if known:

**Membership Number** ____________

**Grade** ____________

**Year of Expiration if no longer a member** ________

## Select Your Membership

☐ Students, IEEE Members, Joining CE Society

☐ IEEE Member, joining CE Society

Online at: https://cesoc.ieee.org/membership.html

Benefits Include:

1) A nice color magazine shipped to your door step to update you on latest CE
2) Discount in conference registration
3) Networking opportunity with global peers

# Technical Committee on VLSI (TCVLSI), IEEE-CS

http://www.ieee-tcvlsi.org

IEEE computer society

The IEEE Computer Society Technical Committee on VLSI

## What is TC-VLSI?

A technical committee of IEEE-CS serves as the focal point of the various technical activities within a technical discipline.

TCVLSI is a constituency of the IEEE-CS that oversees various technical activities related to VLSI.

### Key People

*Chair*
Saraju P. Mohanty, University of North Texas
*Vice Chair for Conferences –*
Jia Di, University of Arkansas
*Treasurer –*
Hai (Helen) Li, Duke University
*Vice Chair for Membership –*
Dhruva Ghai, Oriental University Indore, India
*Vice Chair for Liaison –*
Nagi Naganathan, Avago Technologies
*Vice Chair Outreach and Webmaster –*
Mike Borowczak, University of Wyoming
*Newsletter EiCs –*
Saraju P. Mohanty, University of North Texas
Anirban Sengupta, Indian Institute of Technology Indore
*Past Chair –*
Joseph Cavallaro, Rice University

### TCVLSI Sister Conferences

Sponsored

ARITH: www.arithsymposium.org
ASAP: http://www.asapconference.org/
ASYNC: http://asyncsymposium.org/
iNIS: http://www.ieee-inis.org
ISVLSI: http://www.isvlsi.org
IWLS: http://www.iwls.org
MSE: http://www.mseconference.org
SLIP: http://www.sliponline.org
ECMSM: http://ecmsm2017.mondragon.edu/en

Technically Co-Sponsored

ACSD: http://pn2017.unizar.es/
VLSID: http://vlsidesignconference.org

**Join TCVLSI**
It's free to join @ bit.ly/join-tcvlsi

FREE

**Technical Scope** Various aspects of VLSI design including design of system-level, logic-level, and circuit-level, and semiconductor processes

**TCVLSI Offers**
- Student travel grants
- Best paper awards
- Timely CFP info
- Free membership
- Venue to contribute to VLSI
- Circuits & Systems

# Thank You !!!

Slides Available at: http://www.smohanty.org

Hardwares are the drivers of the civilization, even softwares need them.