Internet of Things (IoT)

Homepage

Presentations Page

Prof./Dr. Saraju Mohanty

University of North Texas, USA.

Talk - Outline

- Motivations for IoT
- Selected Components of IoT
- Selected Applications of IoT
- Driving Technologies of IoT
- Challenges and Research in IoT
- IoT Design Flow
- Tools and Solutions for IoT
- Related Buzzwords of IoT
- Conclusions and Future Directions

Population Trend – Urban Migration

“India is to be found not in its few cities, but in its 700,000 villages.”
- Mahatma Gandhi

- 2025: 60% of world population will be urban
- 2050: 70% of world population will be urban

Source: http://www.urbangateway.org

Human Migration Problem

- Uncontrolled growth of urban population
- Limited natural and man-made resources

Source: https://humanitycollege.org

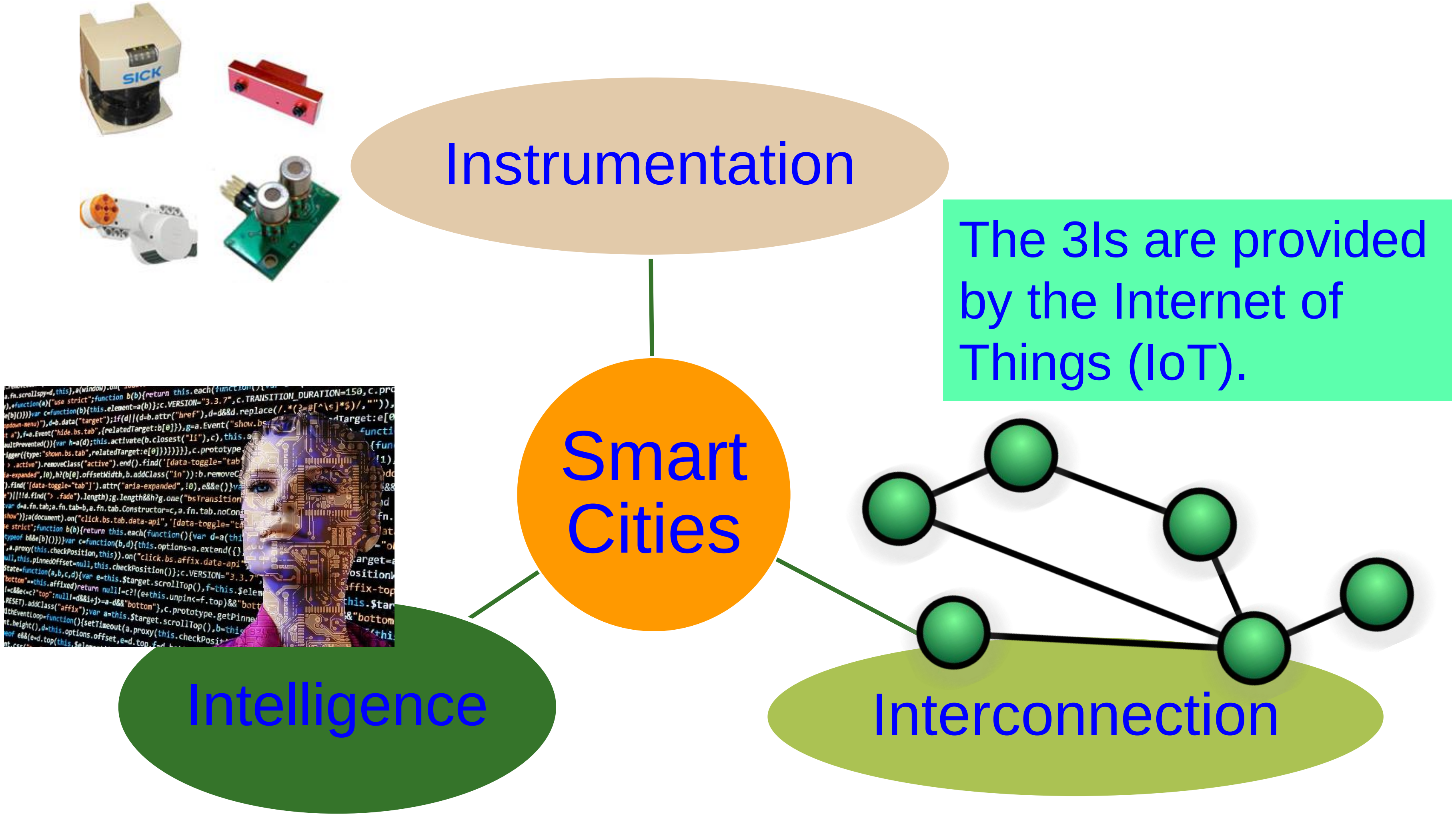
Smart Cities - A Solution

- 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.”

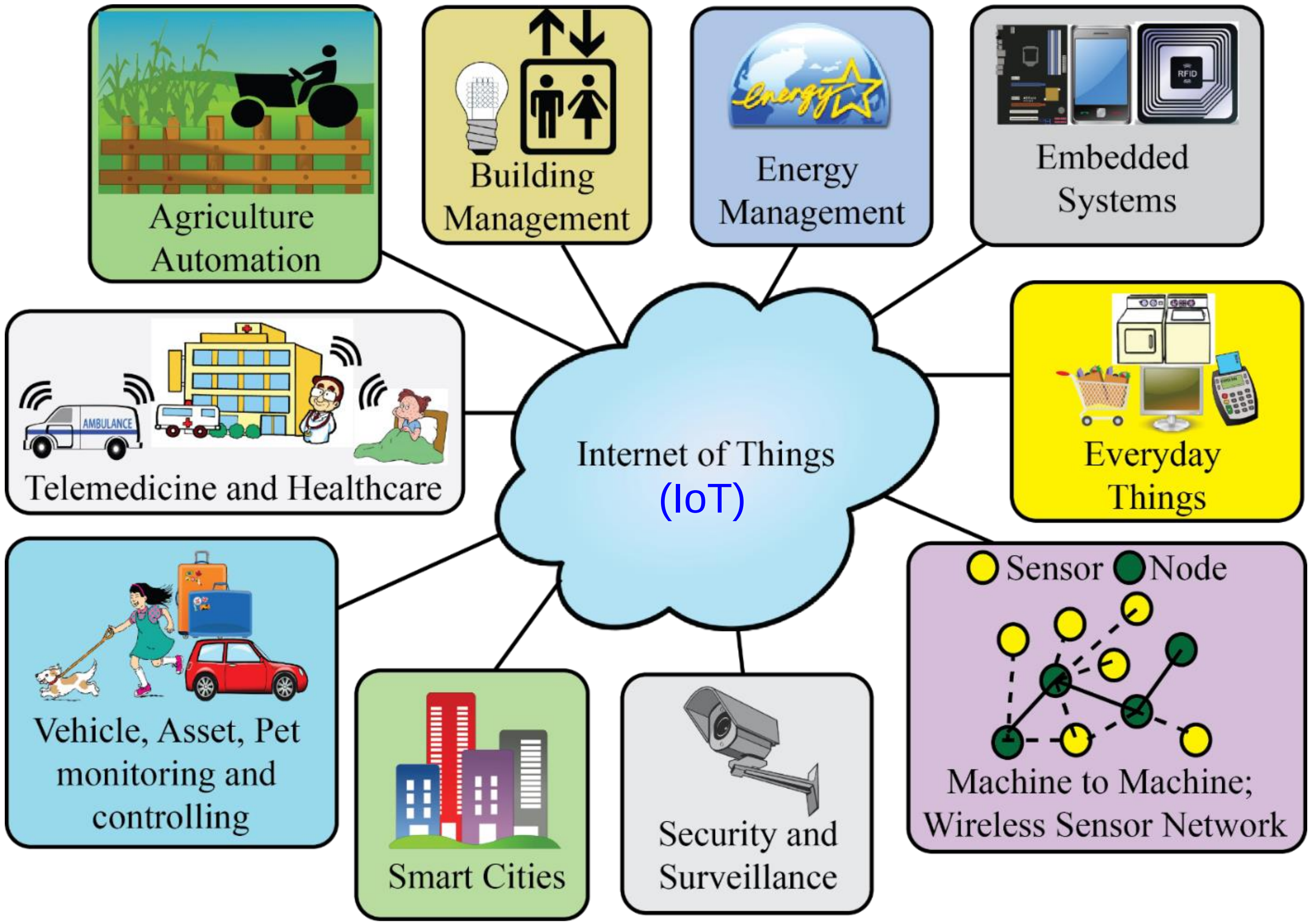
Source: http://www.cnbc.com/2016/10/25/spending-on-smart-cities-around-the-world-could-reach-41-trillion.html

Smart Cities - 3 Is



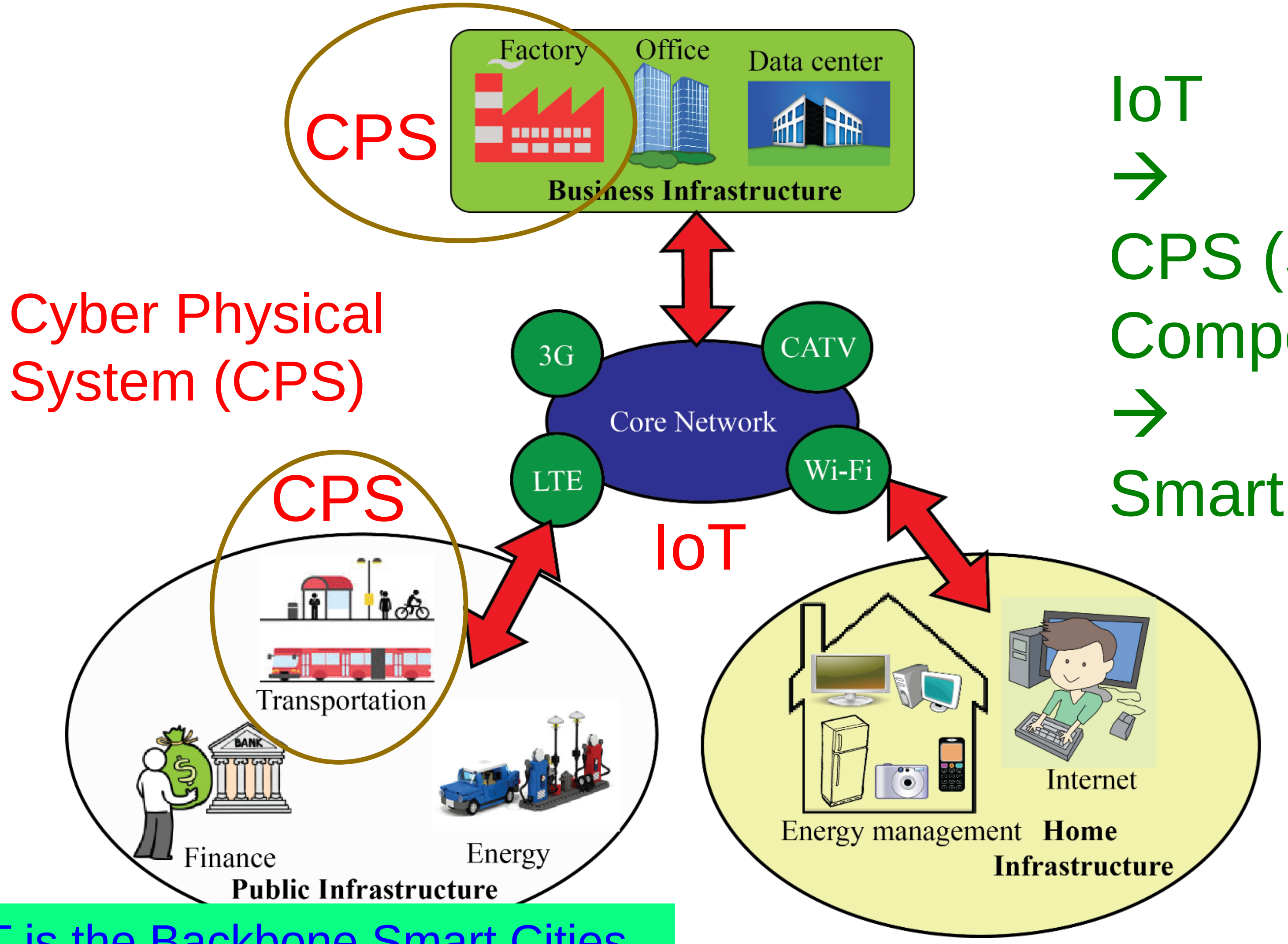
Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

IoT is the Backbone Smart Cities



Source: Mohanty 2016, CE Magazine July 2016

IoT → CPS → Smart Cities

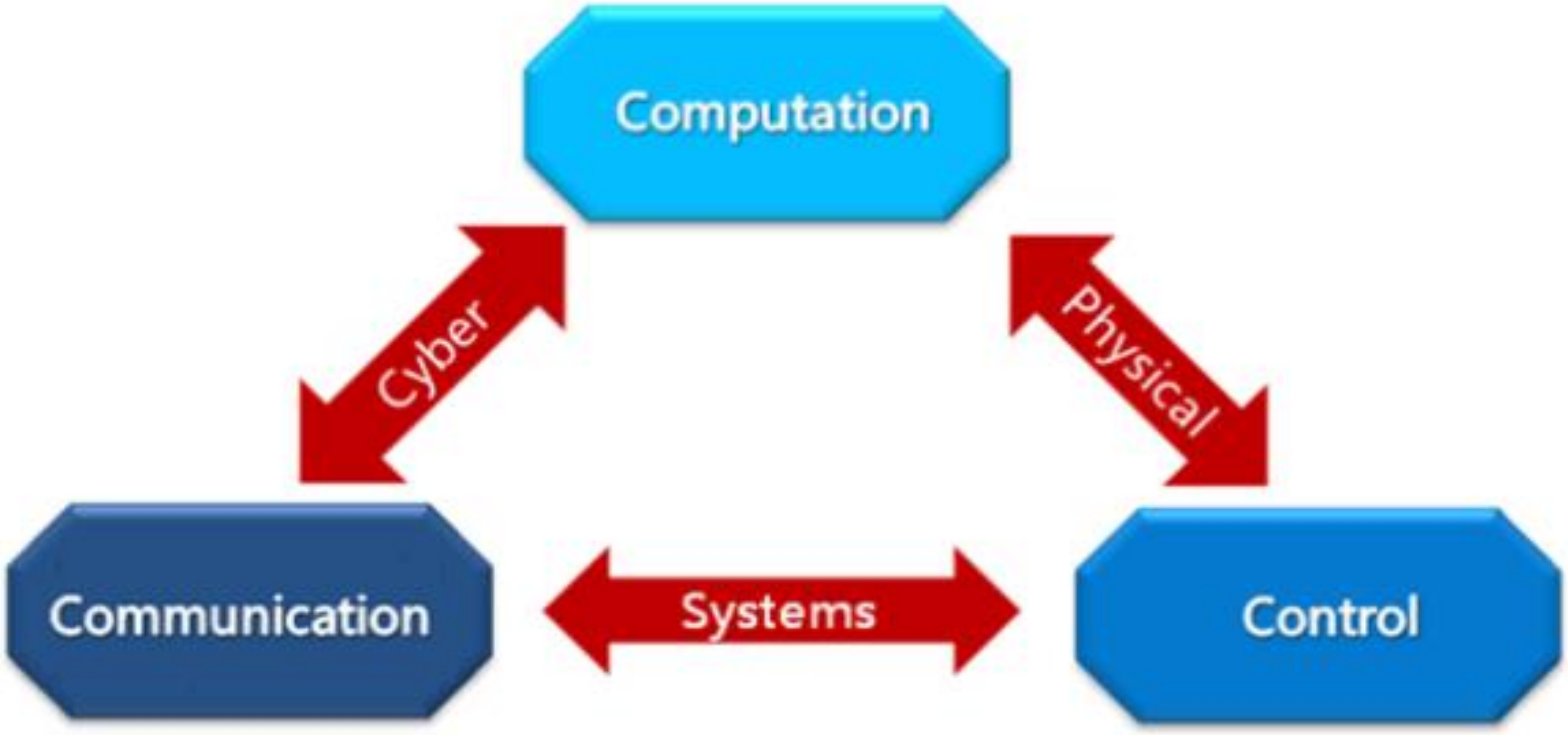


IoT → CPS (Smart Components) → Smart Cities

IoT is the Backbone Smart Cities.

Source: Mohanty CE Magazine July 2016

Cyber-Physical Systems (CPS) - 3 Cs



3 Cs of IoT - Connect, Compute, Communicate

Source: G. Jinghong, H. Ziwei, Z. Yan, Z. Tao, L. Yajie and Z. Fuxing, "An overview on cyber-physical systems of energy interconnection," in *Proc. IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, 2017, pp. 15-21.

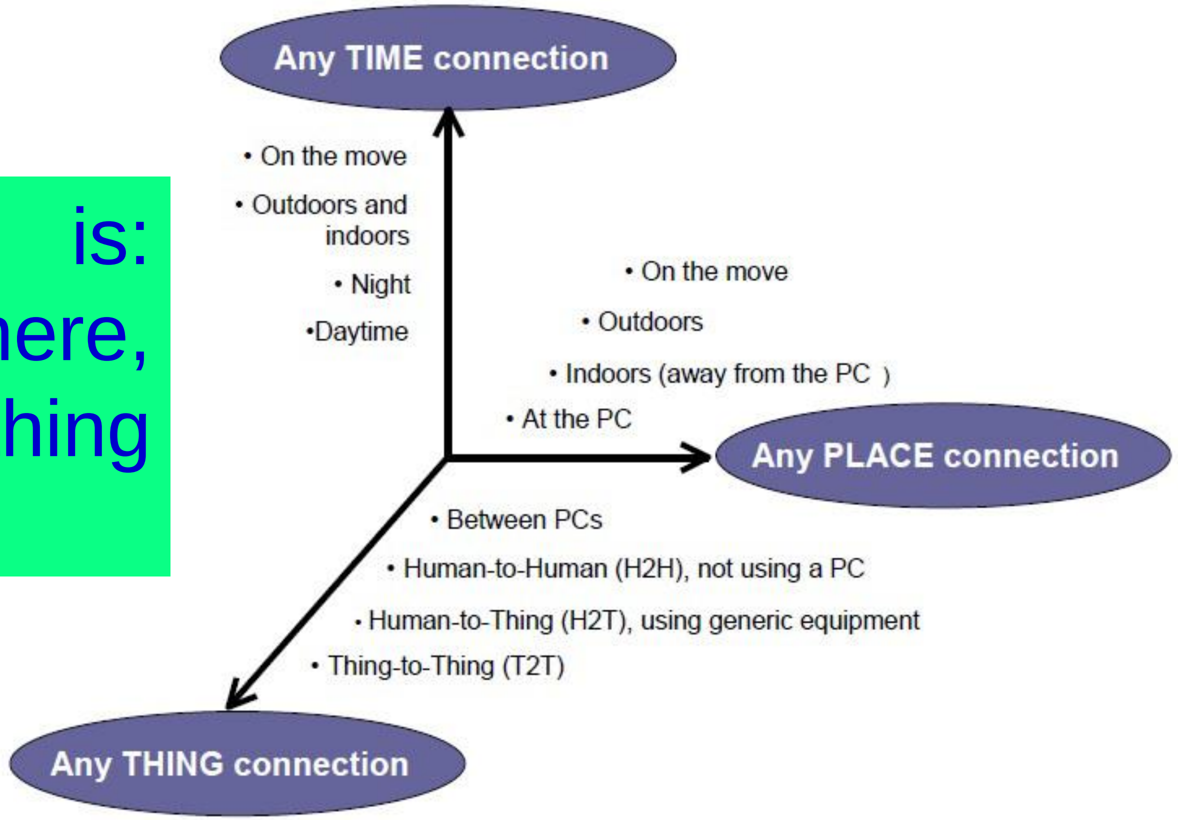
Internet of Things (IoT) - History

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

Components

IoT – Definition - International Telecommunication Union (ITU)

A network that is: “Available anywhere, anytime, by anything and anyone.”



Source: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

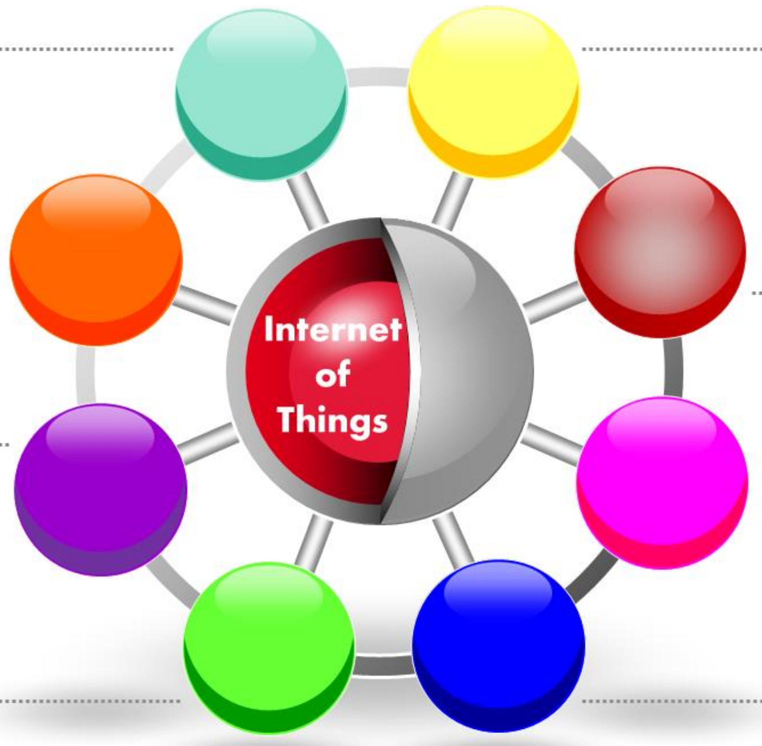
IoT – Definition - IoT European Research Cluster (IERC)

A *dynamic global network infrastructure*

with *self configuring capabilities*

based on *standard and interoperable communication protocols*

where *physical and virtual "things"*



have *identities, physical attributes, and virtual personalities*

and

use *intelligent interfaces*,

and are *seamlessly integrated*

into *the information network.*

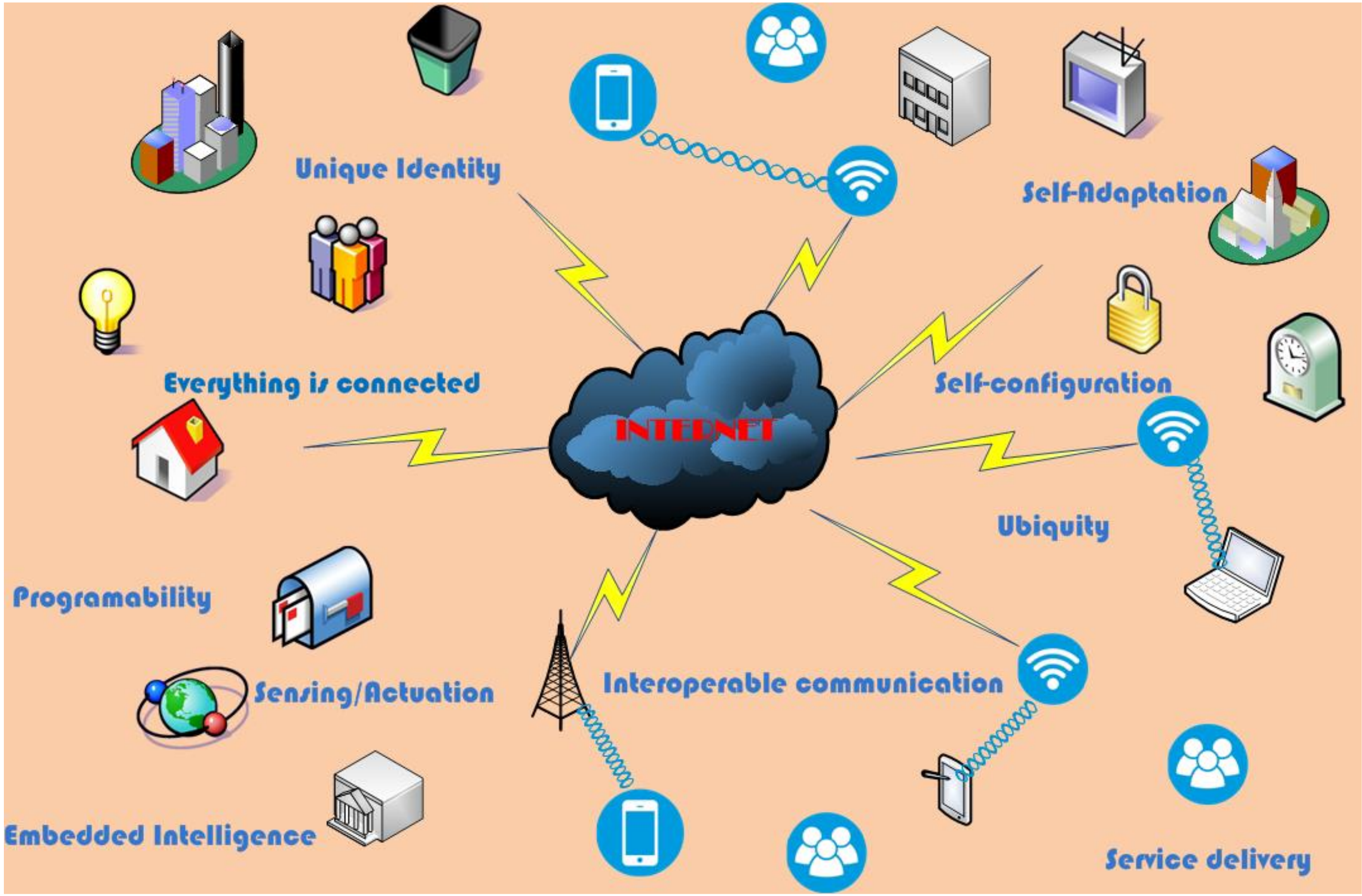
Source: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

IoT – Formal Definition - IEEE

- “Internet of Things envisions a self-configuring, adaptive, complex network that interconnects ’things’ to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing’s identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.”

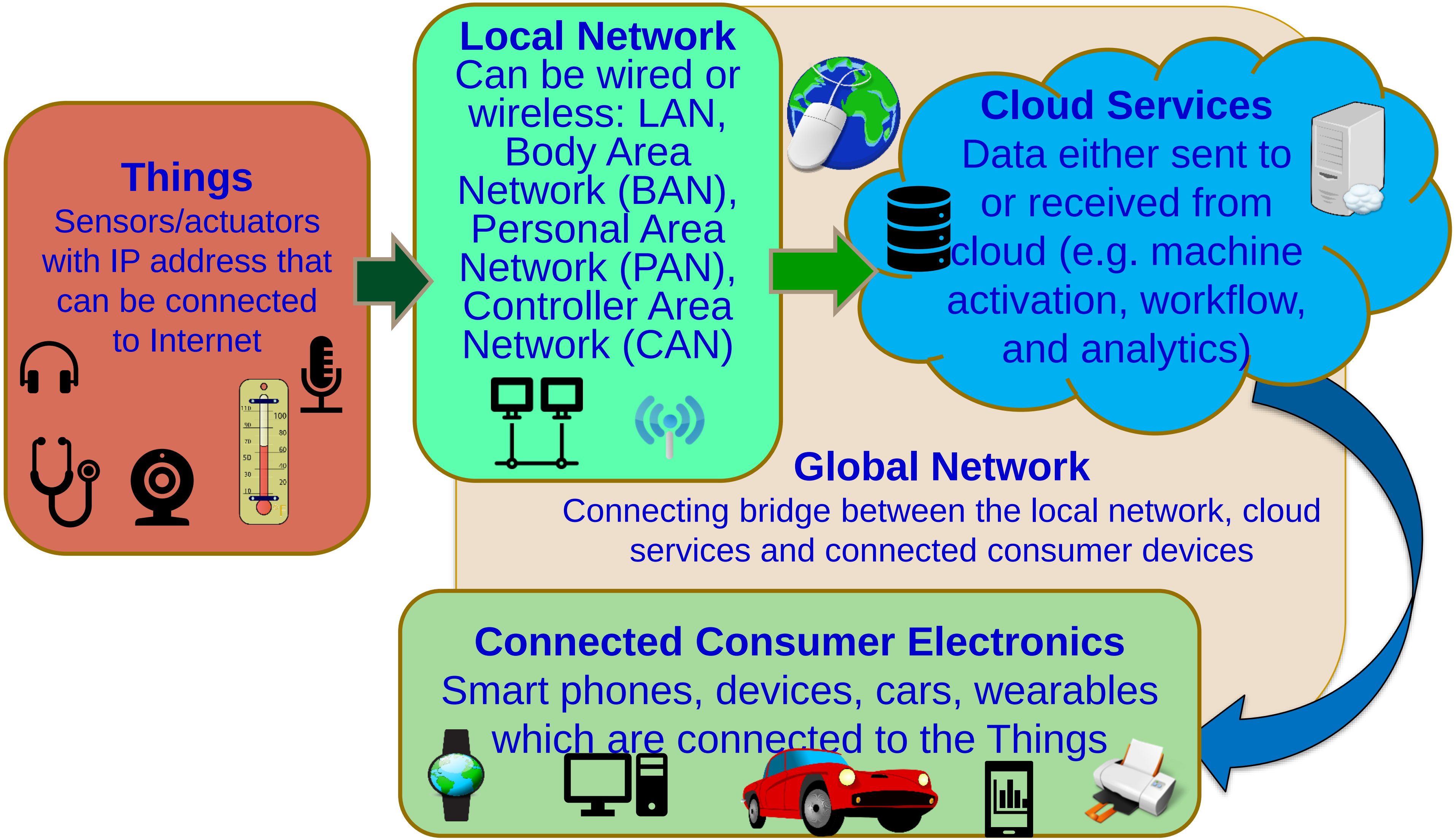
Source: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

IoT – Formal Definition - IEEE

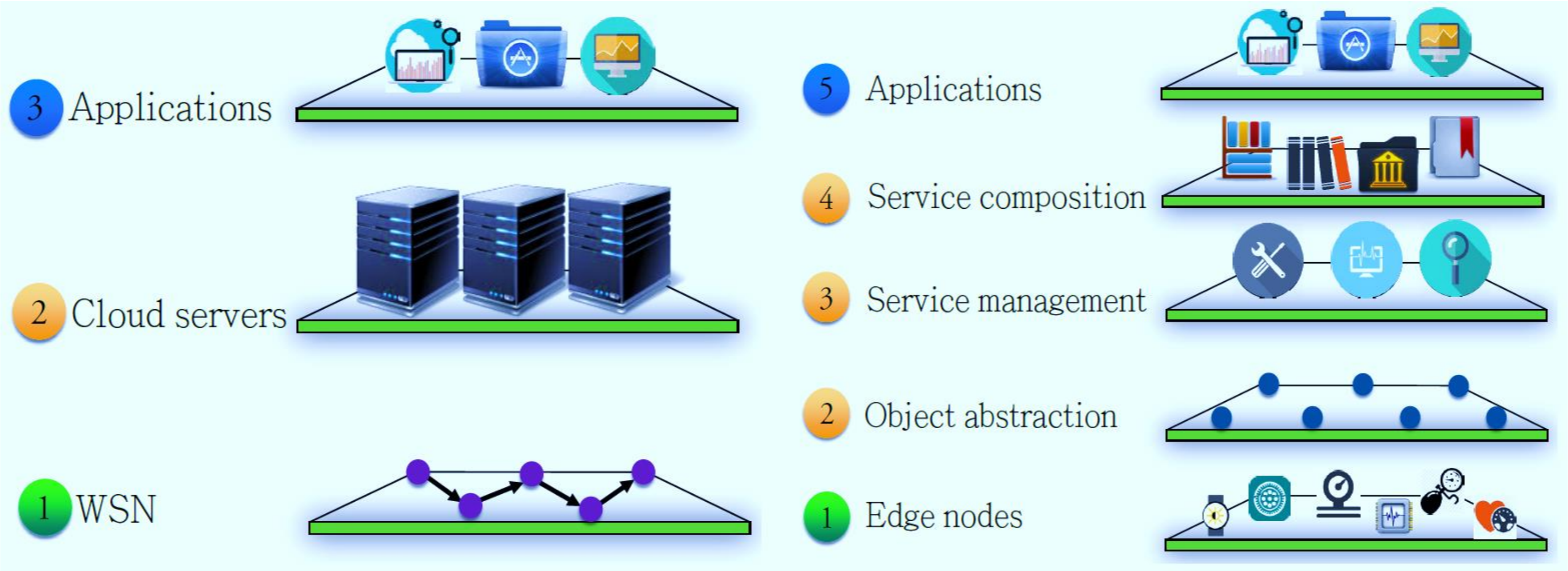


Source: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

Internet of Things (IoT) – Concept



IoT Architecture - 3 & 5 Level Model

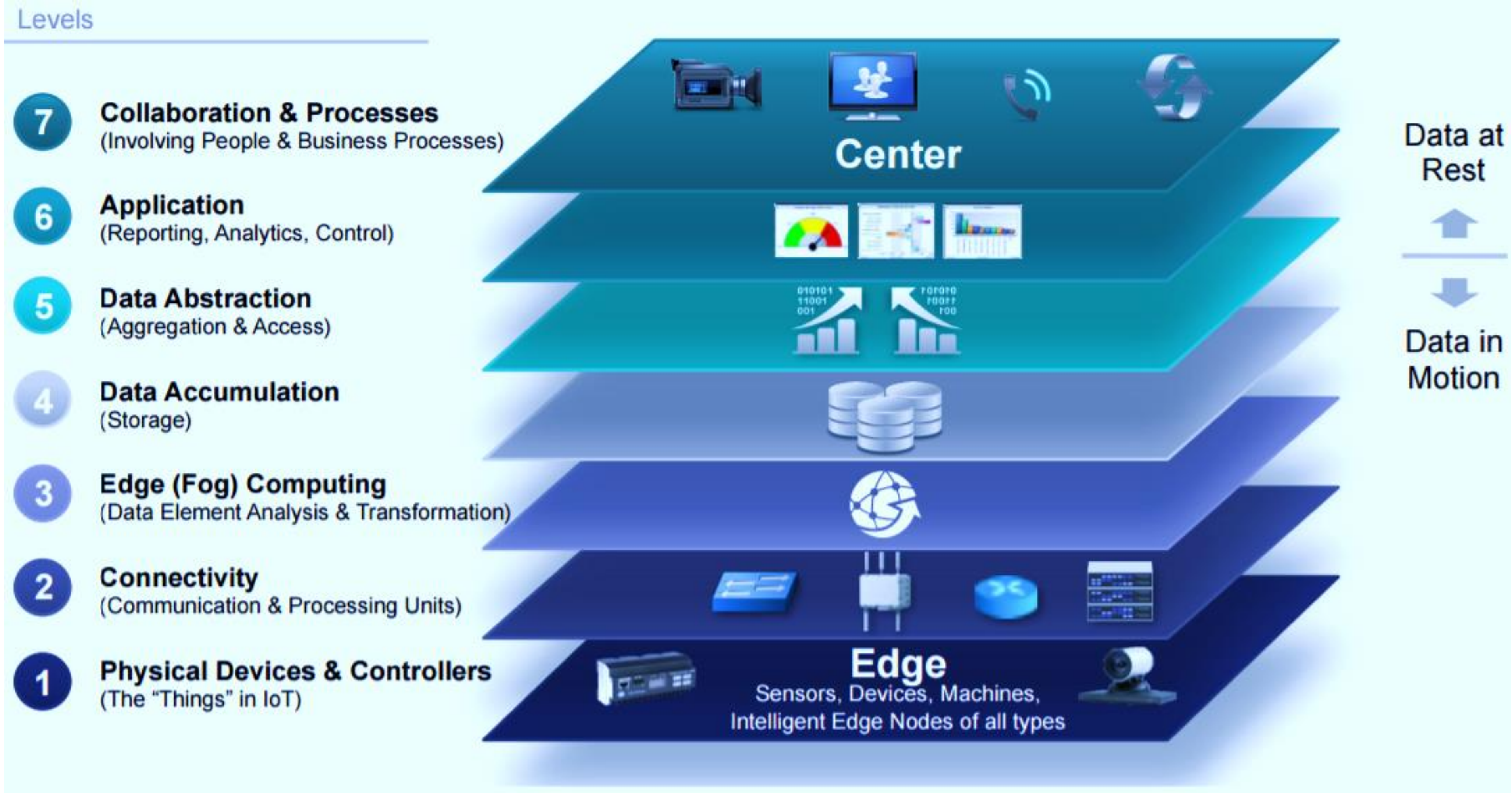


Three Level Model

Five Level Model

Source: Nia 2017, IEEE TETC 2017

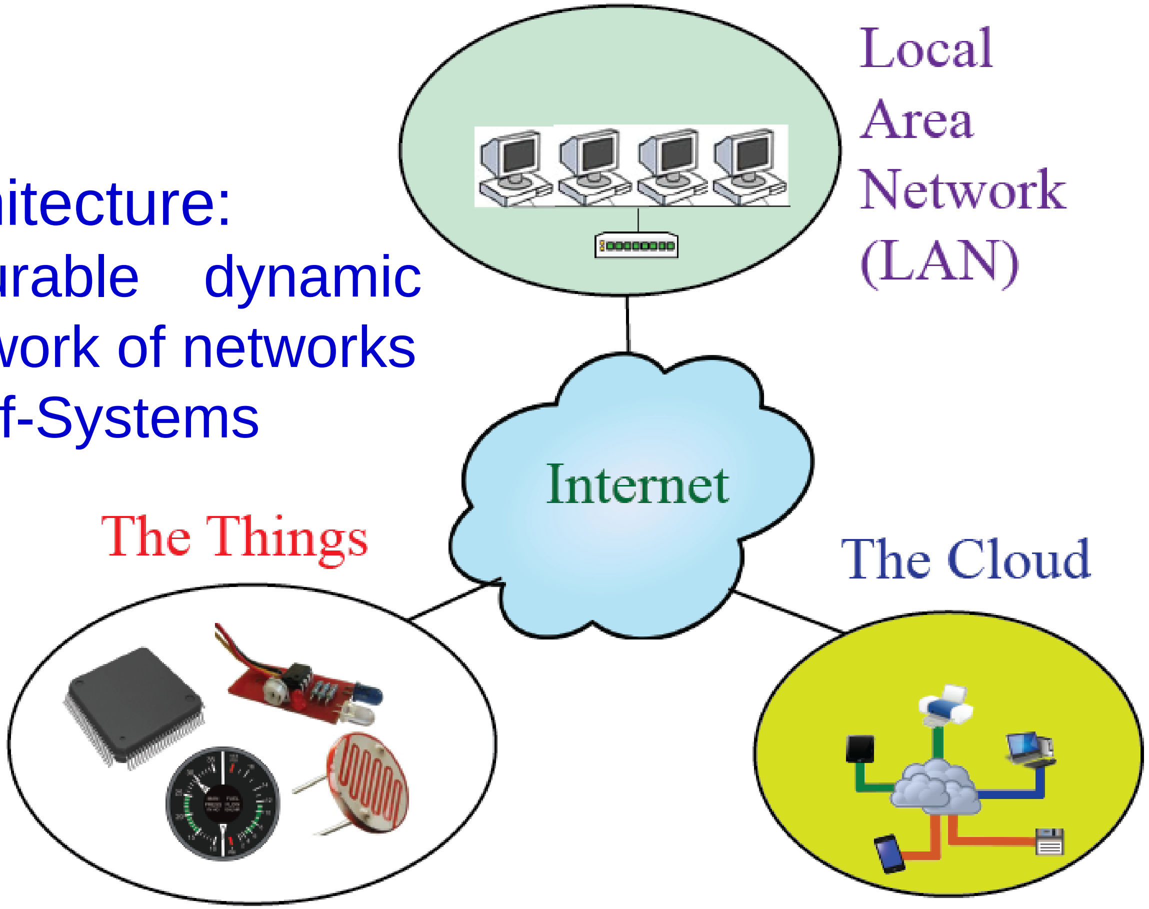
IoT Architecture - 7 Level Model



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

IoT - Architecture

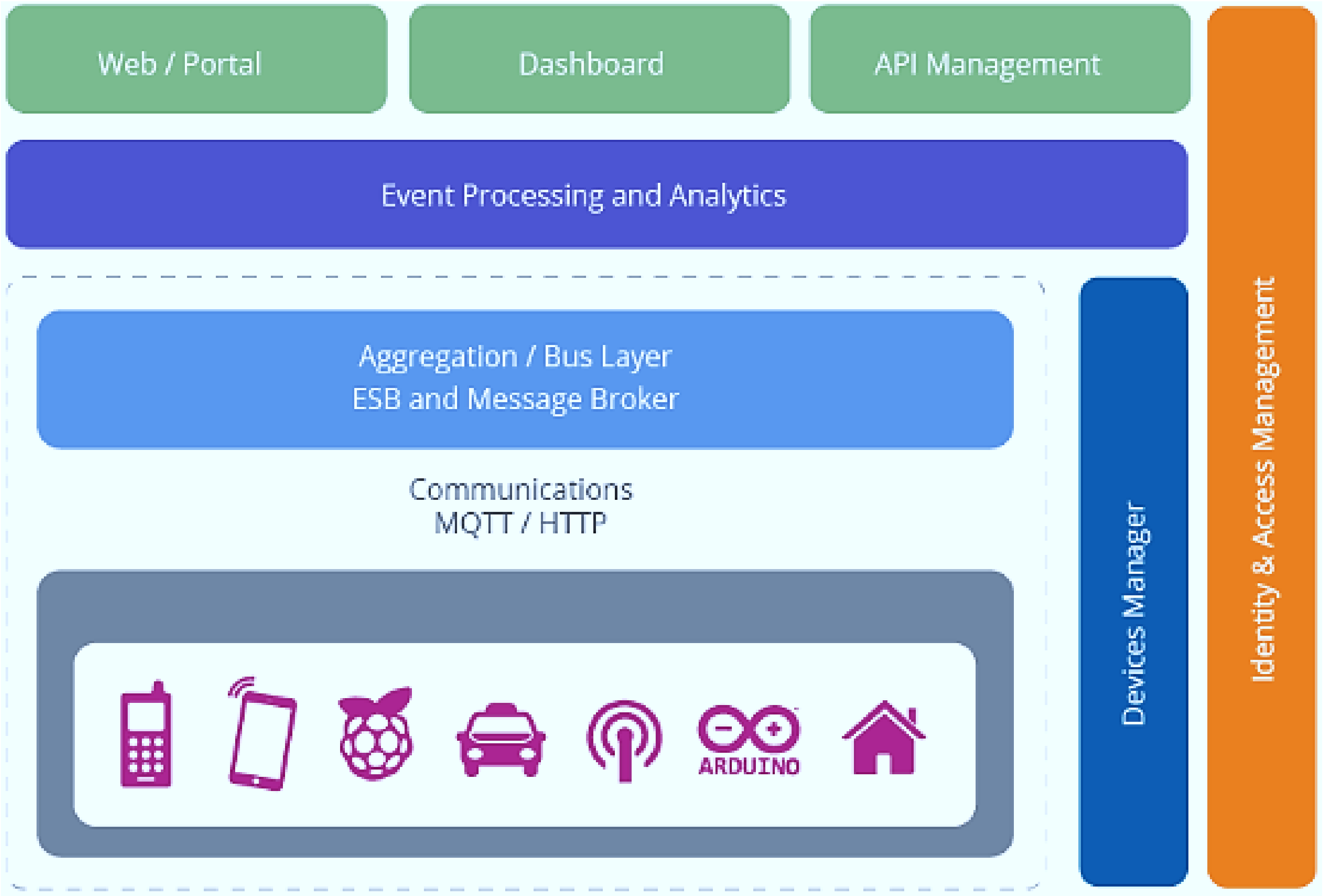
Overall architecture:
- ❖ A configurable dynamic global network of networks
- ❖ Systems-of-Systems



Four Main Components of IoT.

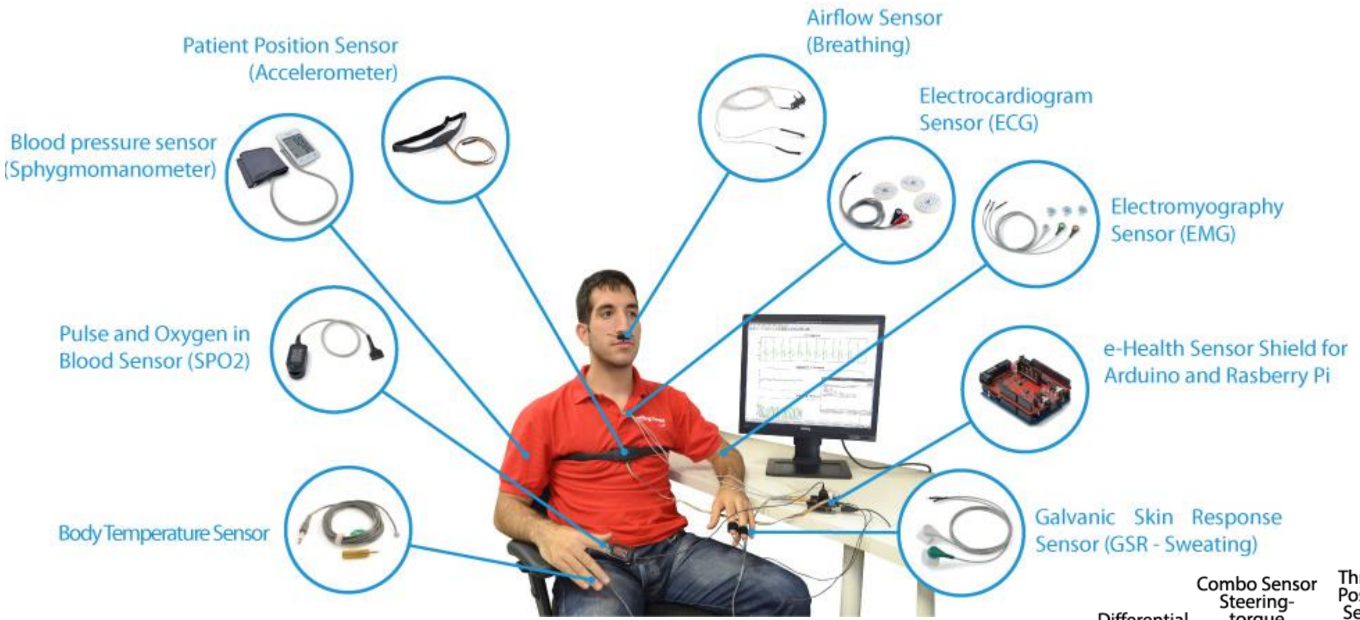
Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

IoT - Architecture

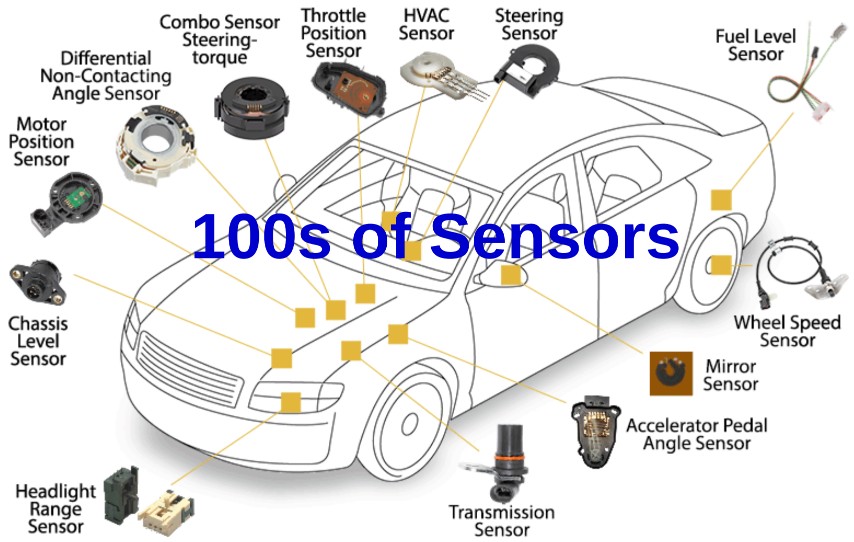


Source: http://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things/

IoT – Sensors

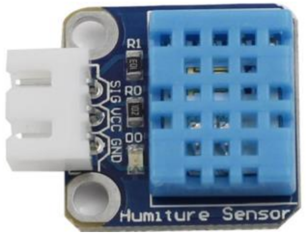


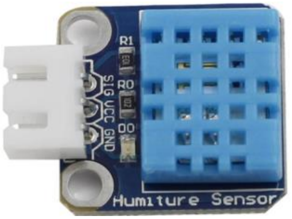
Source: http://www.libelium.com/e-health-low-cost-sensors-for-early-detection-of-childhood-disease-inspire-project-hope/



IoT – Things

Sensor





Thing

Sensors + Device with its own IP address → Things

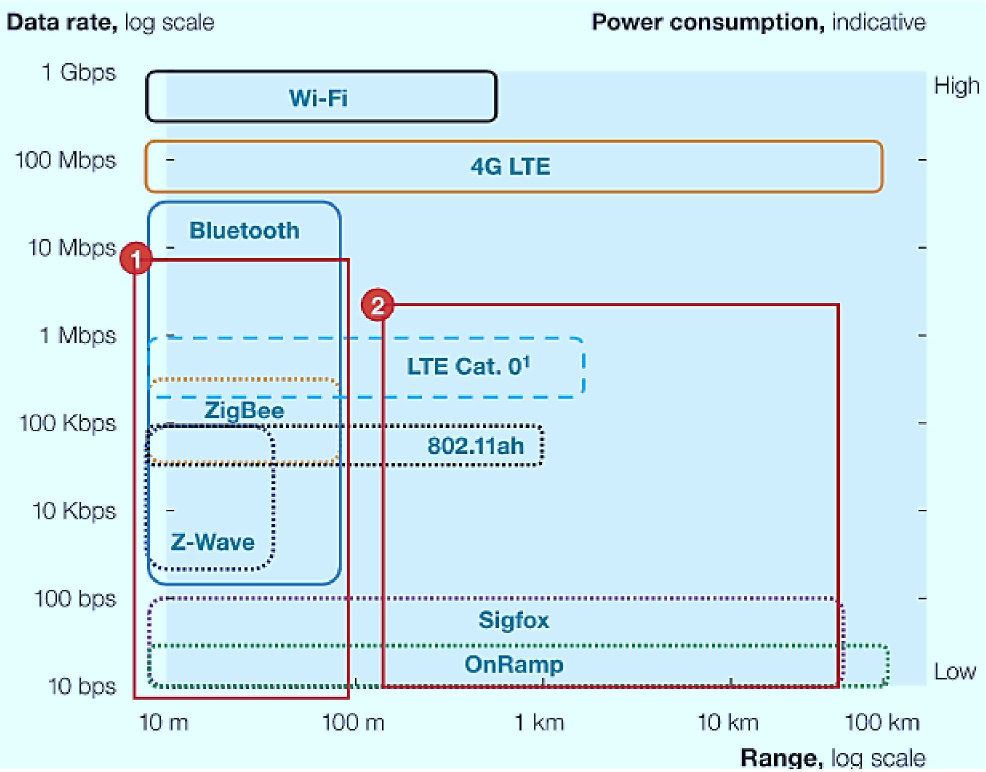
IP Address for Internet Connection

The “Things” refer to any physical object with a device that has its own IP address and can connect and send/receive data via network.

IoT - Communications

Selected IoT Communications Technology

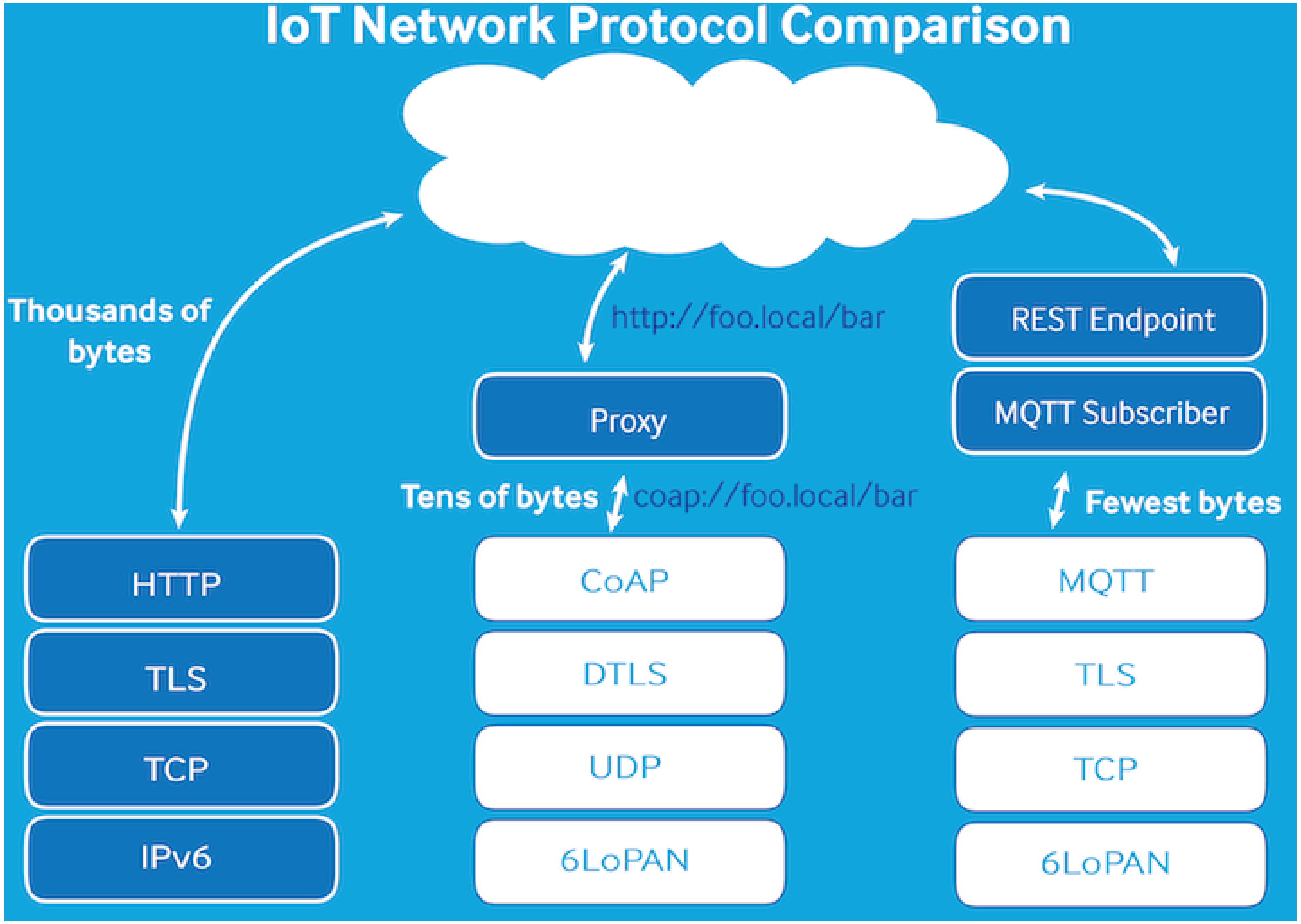
- Bluetooth Low-Energy (BLE)
- Zigbee
- Z-Wave
- 6LowPAN
- Thread
- WiFi
- Cellular
- NFC
- Sigfox
- Neul
- LoRaWAN



Source: https://www.postscapes.com/internet-of-things-protocols/

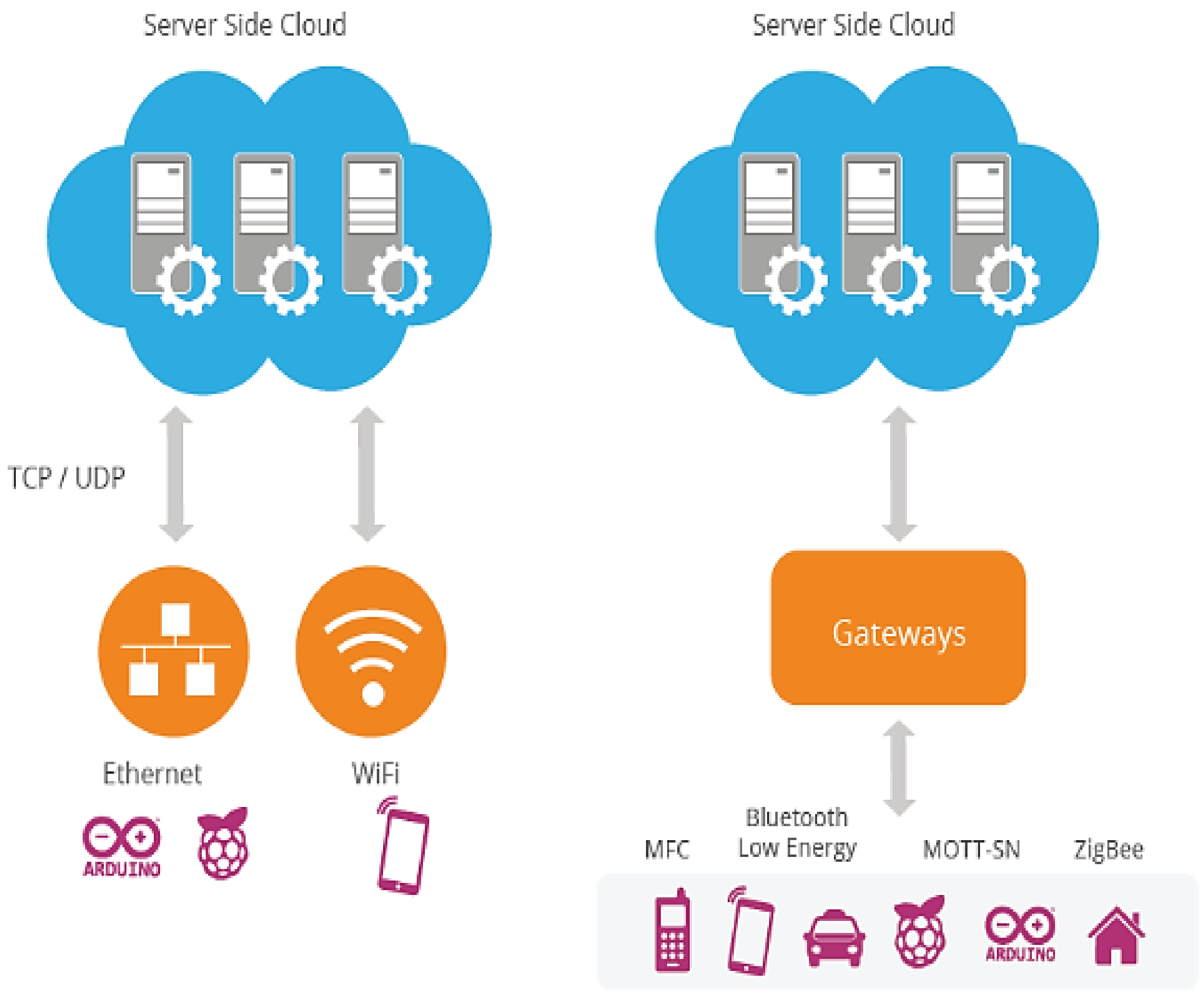
Source: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

IoT - Protocols



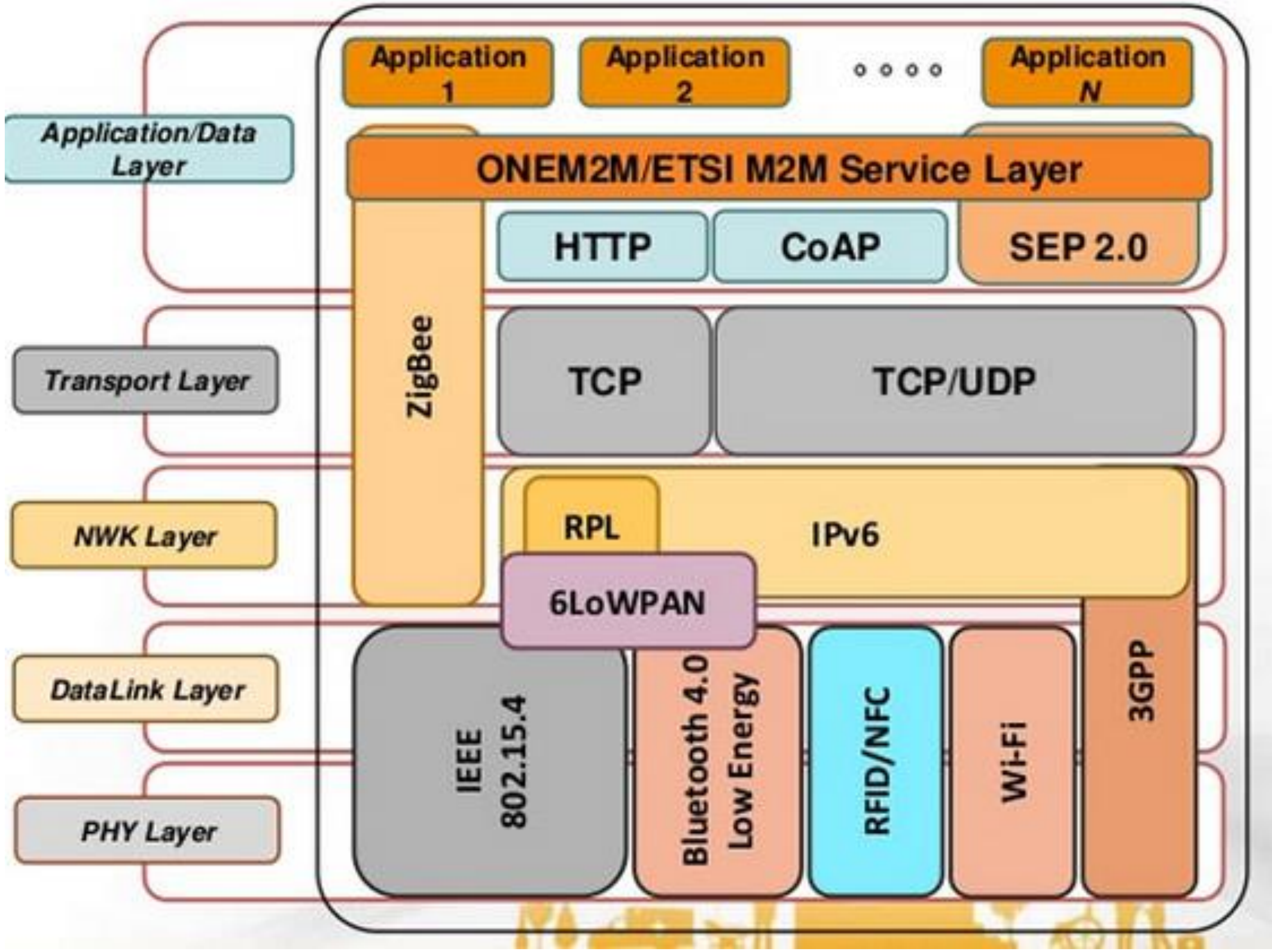
Source: https://www.artik.io/blog/2015/09/iot-101-networks/

IoT - Protocols



Source: http://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things/

IoT - Protocols



Source: https://www.postscapes.com/internet-of-things-protocols/

IoT - Protocols

- Modbus over TCP: Industry's serial de facto standard since 1979, within TCP packets to enable communication with automation devices.
- MQTT : Publish/subscribe protocol.
- MQTT-SN : More compact packet encoding for Sensor networks.
- MQTT-Broker: Receives MQTT subscribe requests from applications within the cloud/platform and sends publish messages to them.

IoT - Protocols

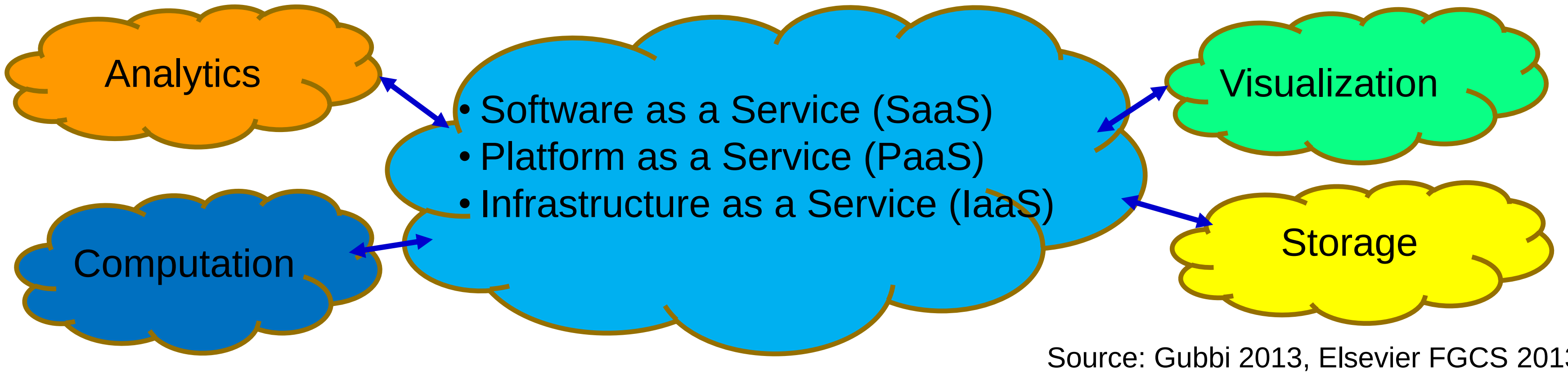
- CoAP is an IETF proposed standard for retrieving and managing information for sensors and devices in a constrained environment.
- HTTP/s client sends periodic XML/REST requests to cloud/platform servers.
- HTTP/s server responds to incoming HTTP requests with responses.
- BACnet/IP server responds to incoming BACnet unicast and broadcast requests with responses.

IoT – Data Protocol - MQTT

- MQTT stands for Message Queue Telemetry Transport.
- It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks.
- The design principles are to minimize network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery.
- These principles also turn out to make the protocol ideal of the emerging “machine-to-machine” (M2M) or “Internet of Things” world of connected devices, and for mobile applications where bandwidth and battery power are at a premium.

IoT - Cloud

Source: https://www.livewireindia.com/cloud_computing_training.php



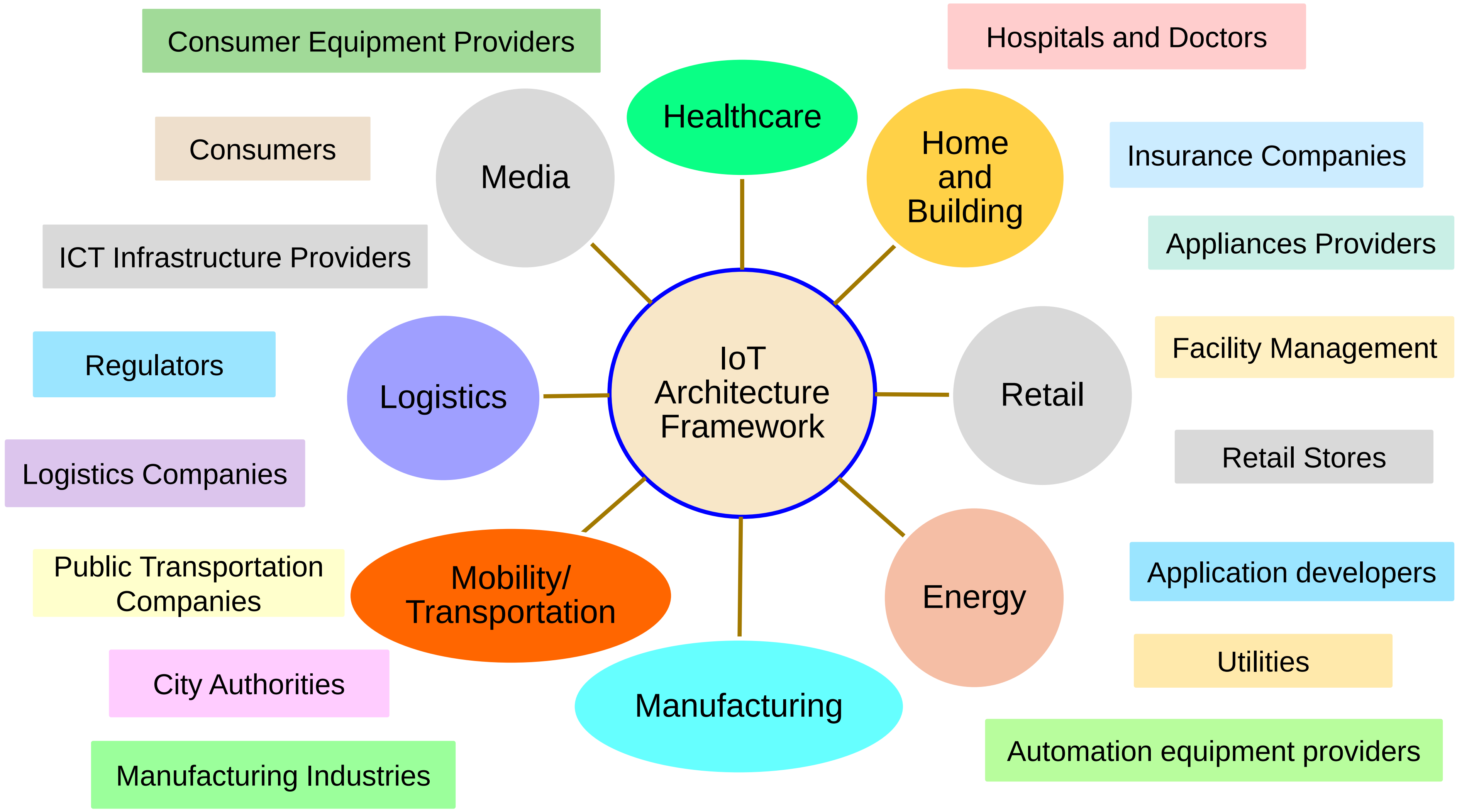
Source: Gubbi 2013, Elsevier FGCS 2013

IoT - Elements

- Sensors
- Application-Specific Hardware
- General-Purpose Hardware
- Firmware
- Operating System
- Middleware
- Software

IoT - Applications

IoT - Markets and Stakeholders



Source: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

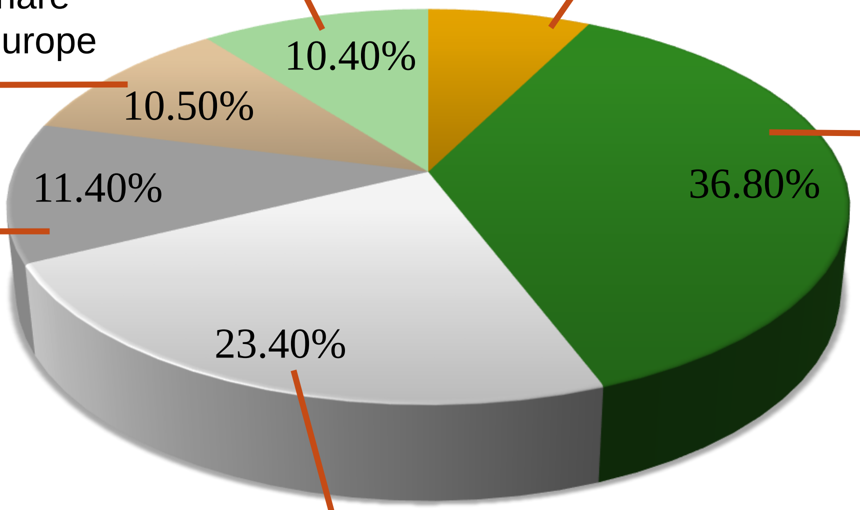
Smart City Market Segments – by 2025

5

Smart Healthcare
Market Value: $348.5Billion
CAGR: 8.8% (2012-2025)
North America to dominate Smart Healthcare market with more than 50% share by 2025 followed by Europe

6

Smart Building
Market Value: $248.65Billion
CAGR: 4.1% (2012-2025)
China and India are fastest growing markets followed by Japan and Korea



4

Smart Transportation
Market Value: $351.13Billion
CAGR: 19.6% (2012-2025)
Market growth in Latin America, Middle East, Africa, CIS + Eastern Europe

1

Smart Governance and Smart Security
Market Value: $1230.26 Billion
CAGR: 11.6% (2012-2025)
More Projects coming up in North America, Middle East and European regions

3

Smart Infrastructure
Market Value: $381.53 Billion
CAGR: 12.0% (2012-2025)
Highest growth in North America and Asia

2

Smart Energy
Market Value: $781.66 Billion
CAGR: 28.7% (2012-2025)
Highest growth in North America

Source: Frost & Sullivan analysis.

Source: https://www.slideshare.net/IoTTunisia/farouk-kamoun-smart-cities-innovative-applications-iot-tunisia-2016

IoT in Smart Healthcare

Fitness Trackers

Quality and sustainable healthcare with limited resources, anywhere, anytime.

IoT Role Includes:

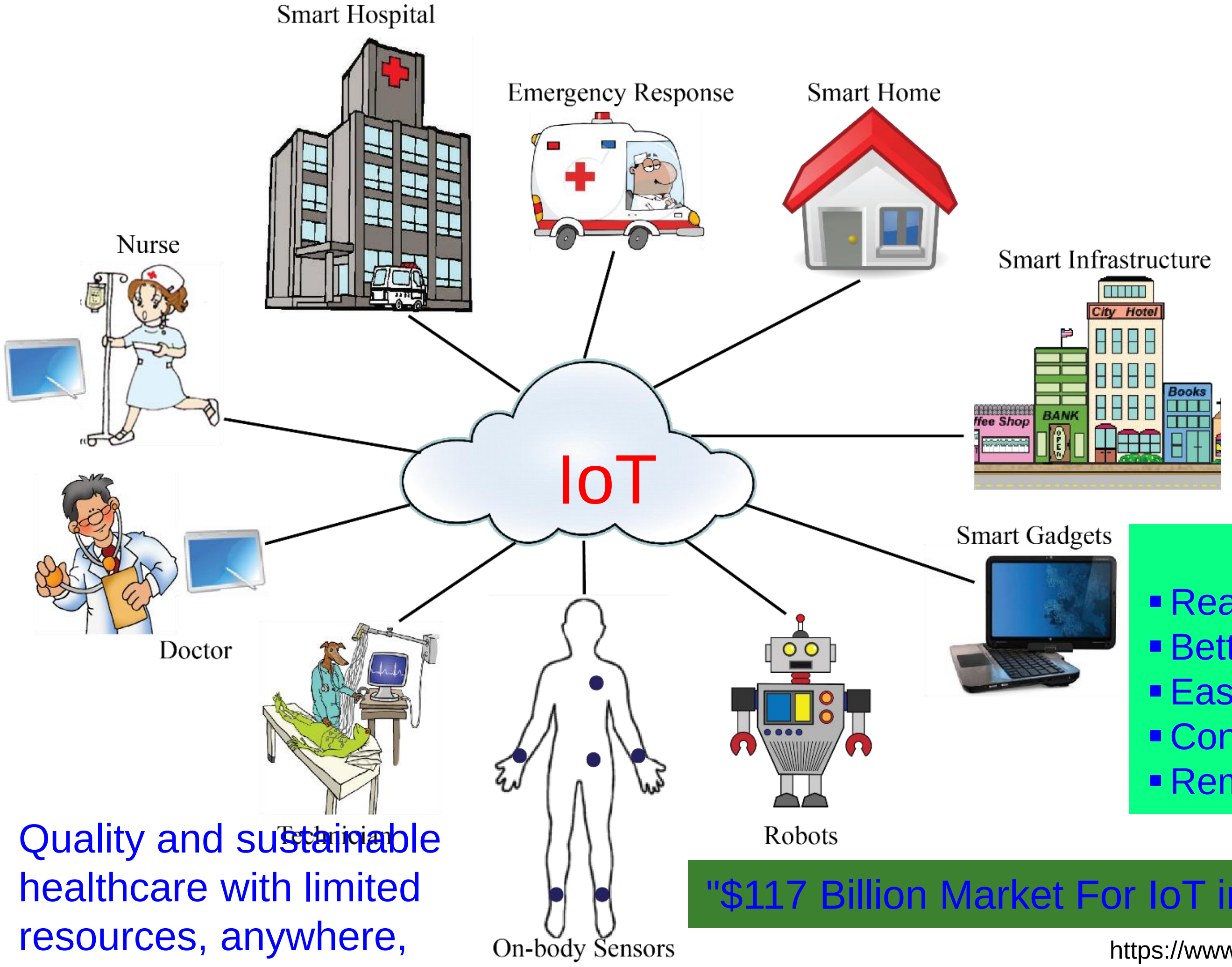
- Real-time monitoring
- Better emergency response
- Easy access of patient data
- Connectivity among stake holders
- Remote access to healthcare

Frost and Sullivan predict smart health-care market value to reach US$348.5 billion by 2025.

Source: Mohanty 2018, CE Magazine January 2018

January 2018

IoT in Smart Healthcare



Fitness Trackers

IoT Role Includes:

- Real-time monitoring
- Better emergency response
- Easy access of patient data
- Connectivity among stake holders
- Remote access to healthcare

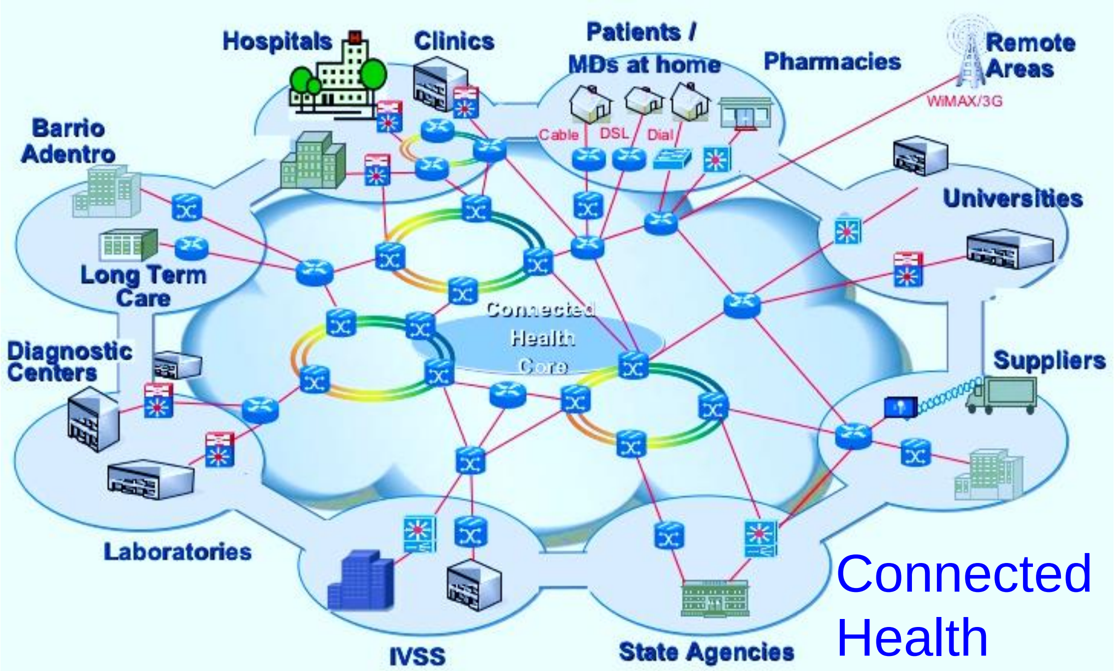
Quality and sustainable healthcare with limited resources, anywhere, anytime.

"$117 Billion Market For IoT in Healthcare By 2020."

https://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/

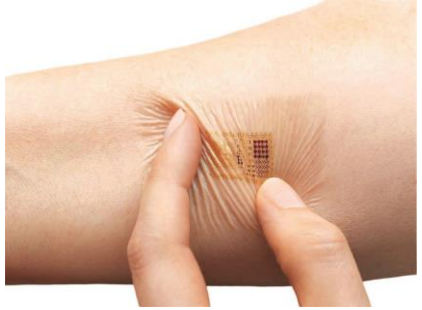
Source: Mohanty 2016, CE Magazine July 2016

IoT in Smart Healthcare



Connected Health

Source: https://www.slideshare.net/tibisay_hernandez/connected-health-venfinal



Embedded Skin Patches

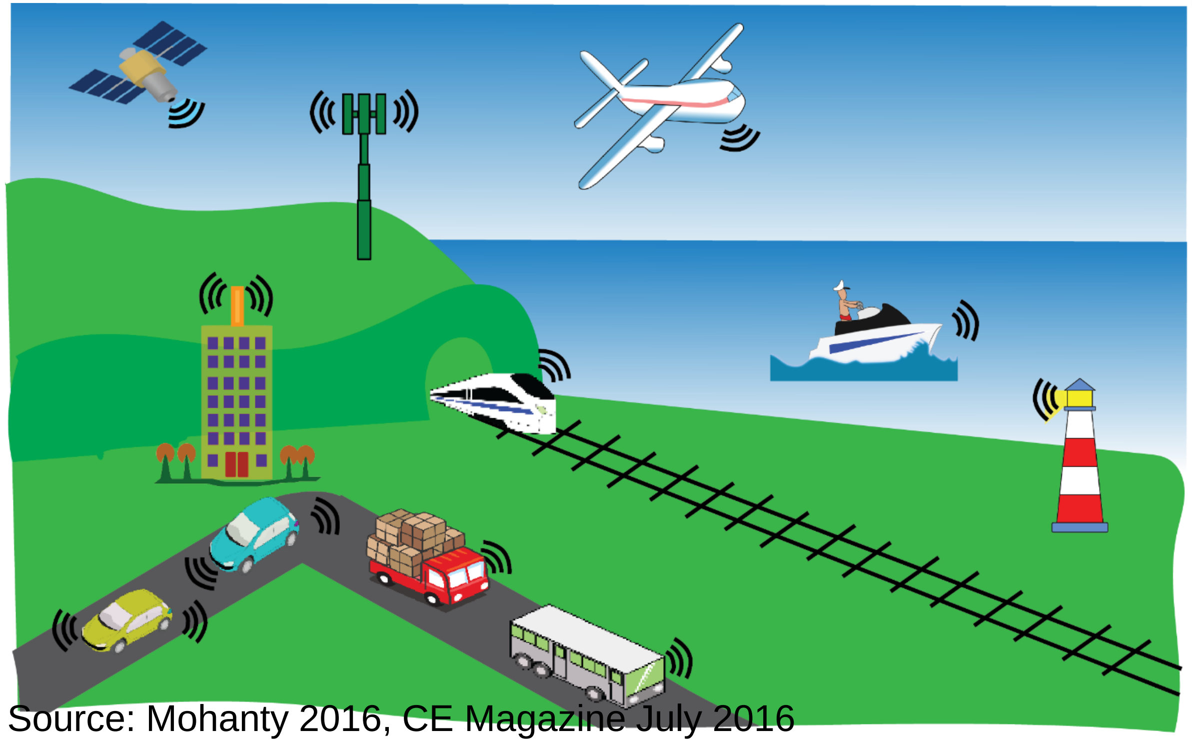
Source: Sethi 2017, JECE 2017

Virtual Reality in Healthcare

Source: http://medicalfuturist.com/5-ways-medical-vr-is-changing-healthcare/
https://touchstoneresearch.com/tag/applied-vr/

Headband with Embedded Neurosensors

IoT in Smart Transportation



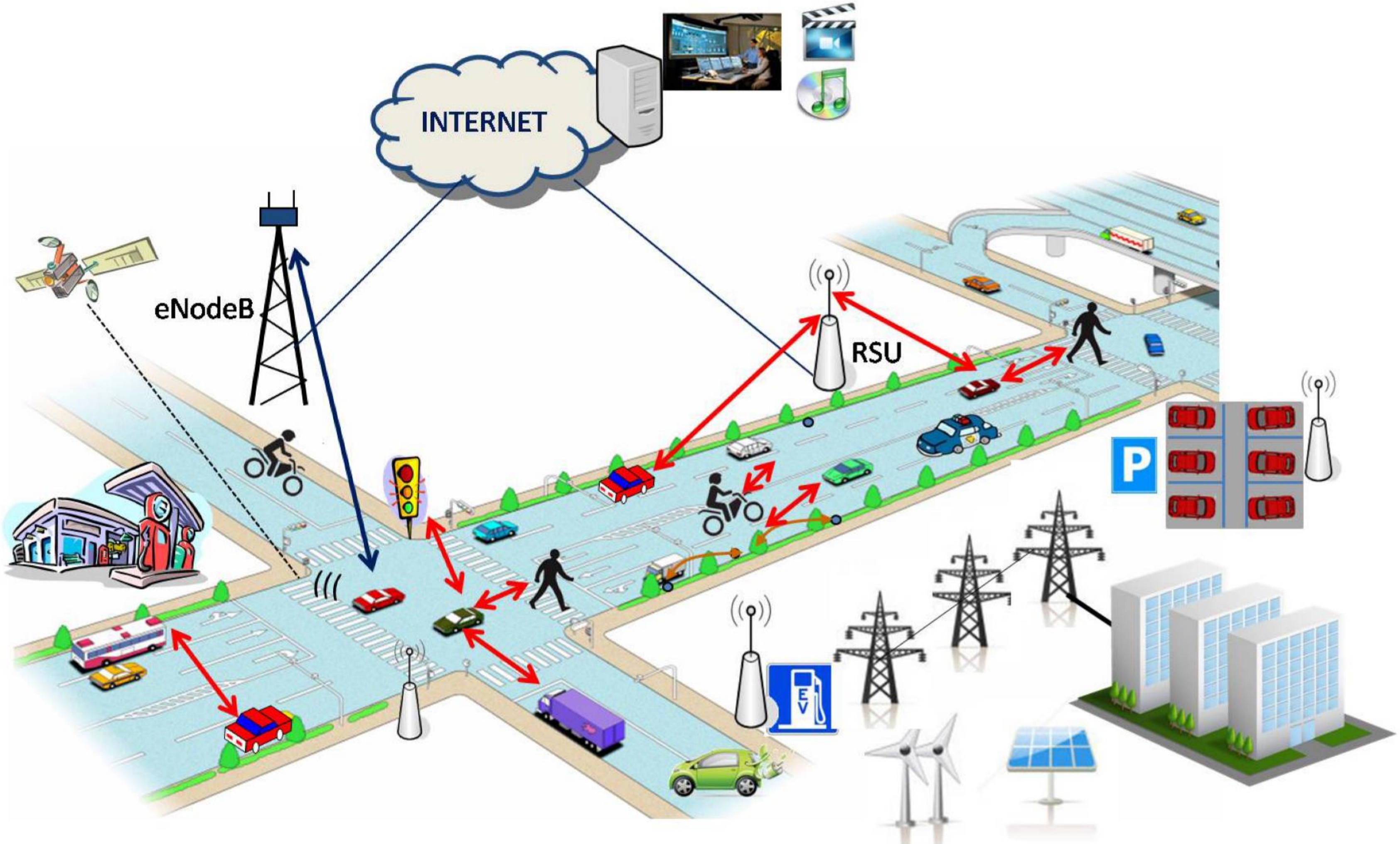
Source: Mohanty 2016, CE Magazine July 2016

Smart Transportation Features:

- Autonomous driving
- Effective traffic management
- Real-time vehicle tracking
- Vehicle safety – Automatic brake
- Vehicle-to-Vehicle communication
- Better scheduling of train, aircraft
- Easy payment system

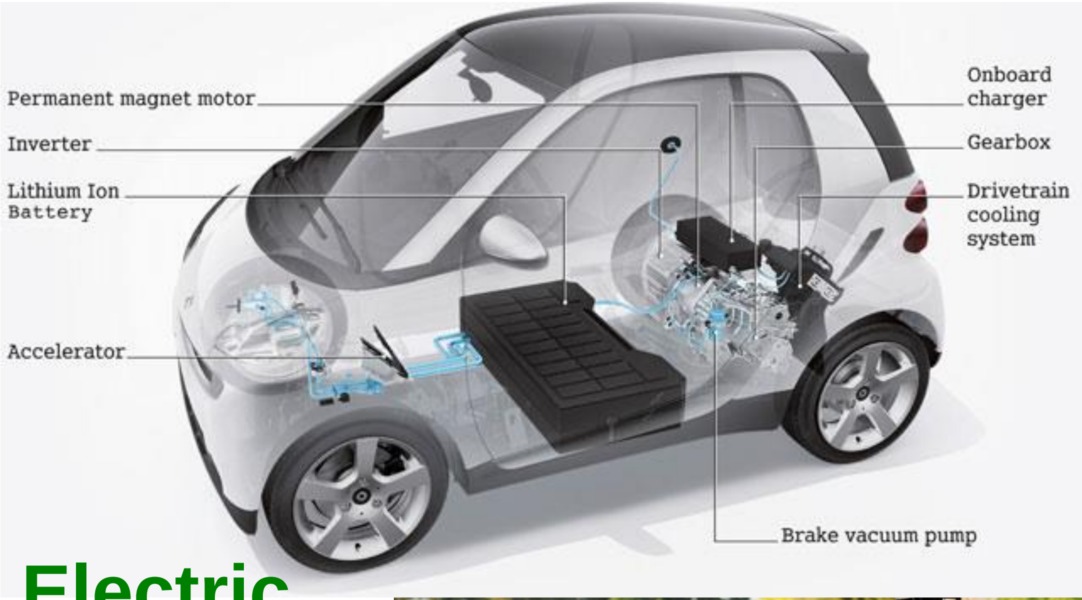
"The smart transportation system allows passengers to easily select different transportation options for lowest cost, shortest distance, or fastest route."

IoT in Smart Transportation

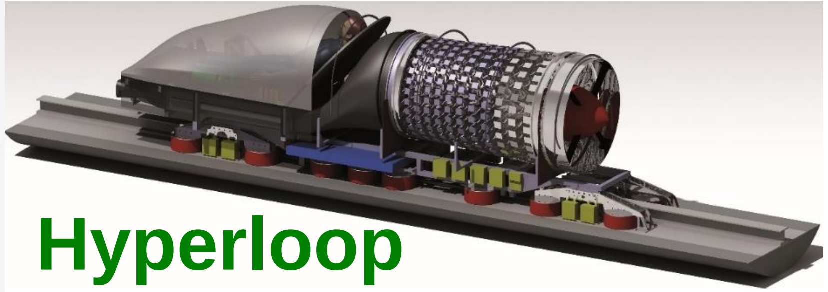


Source: Amadeo 2016, JSAN November 2016

IoT Smart Transportation



Electric Car



Hyperloop

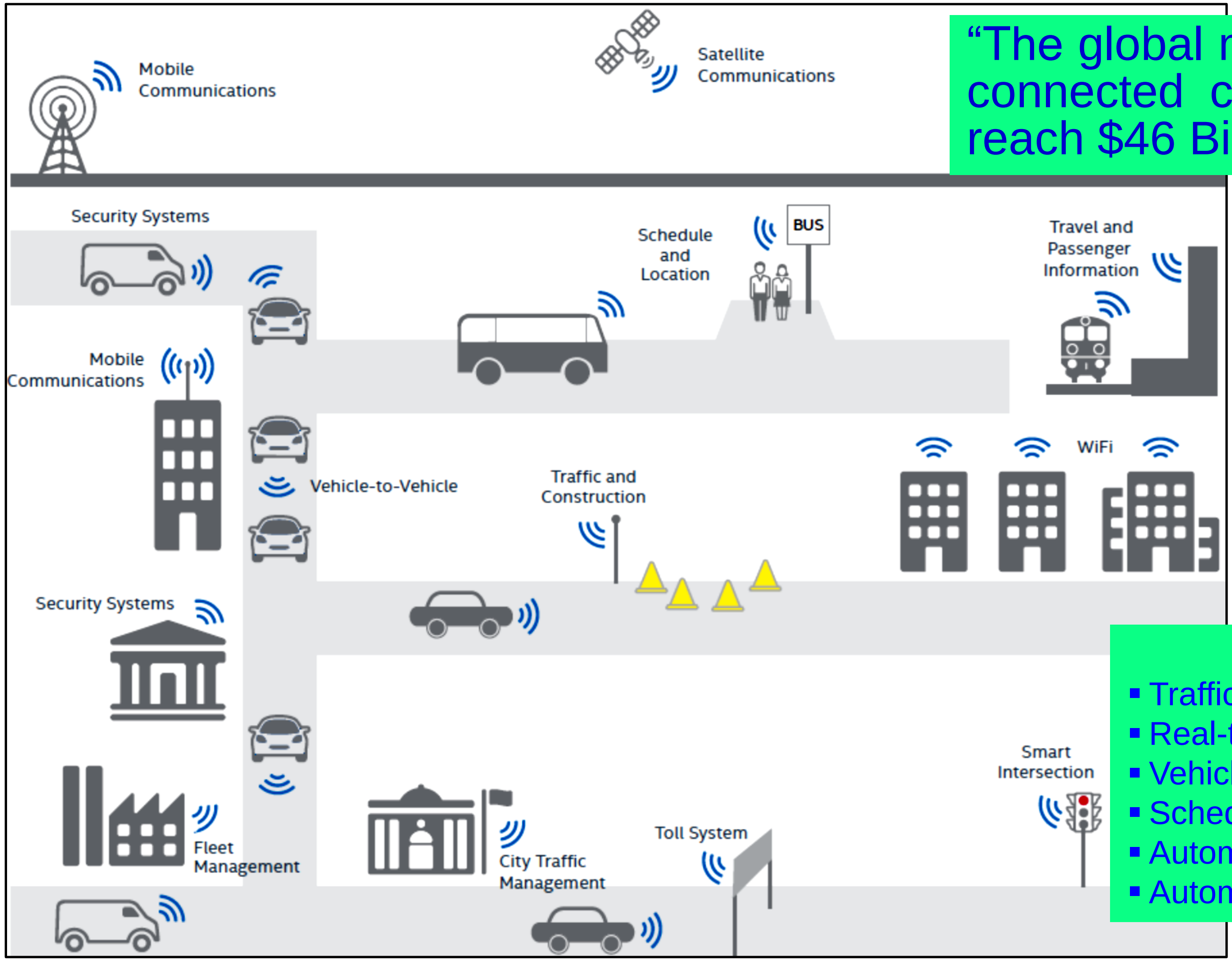
"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

Source: Datta 2017, CE Magazine Oct 2017

Drone

Driverless Car

IoT in Smart Transportation



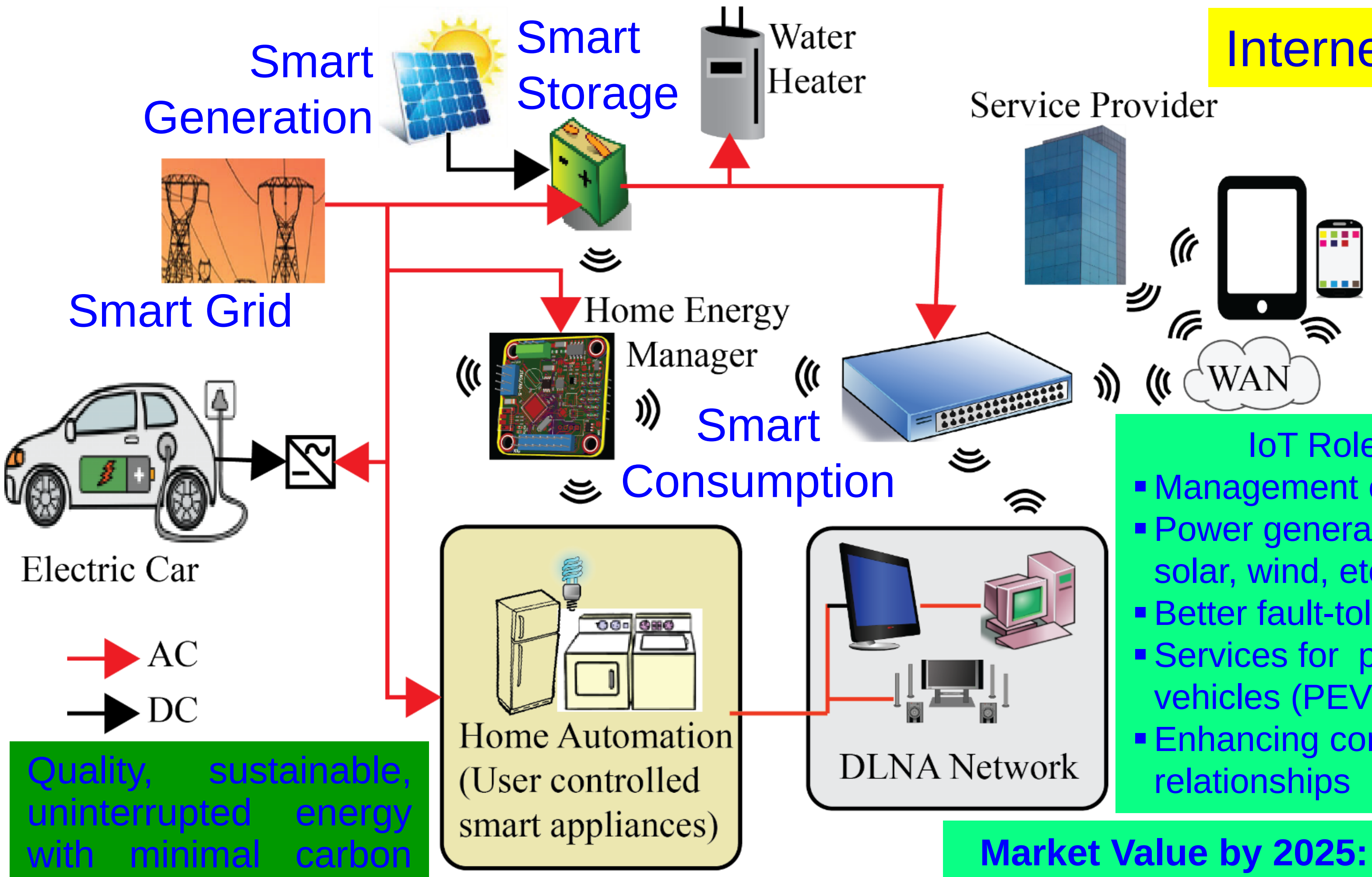
“The global market of IoT based connected cars is expected to reach $46 Billion by 2020.”

Source: Datta 2017, CE Magazine Oct 2017

IoT Role Includes:
- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

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

IoT in Smart Energy



Internet of Energy

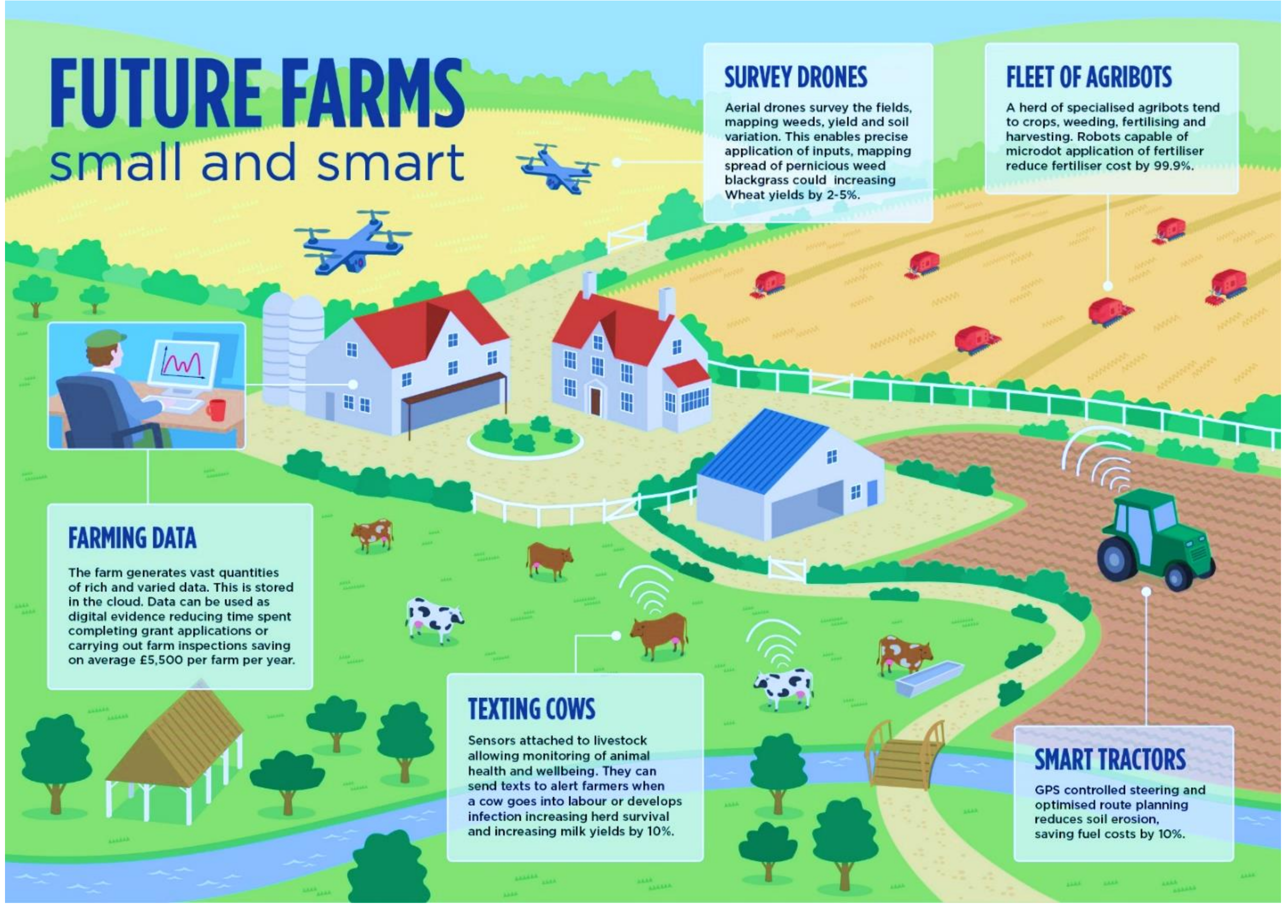
IoT Role Includes:
- Management of energy usage
- Power generation dispatch for solar, wind, etc.
- Better fault-tolerance of the grid
- Services for plug-in electric vehicles (PEV)
- Enhancing consumer relationships

Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Market Value by 2025: $781.66 Billion
Source: Frost & Sullivan

Source: Mohanty 2016, CE Magazine July 2016

IoT in Smart Agriculture



Source: http://www.nesta.org.uk/blog/precision-agriculture-almost-20-increase-income-possible-smart-farming

Climate-Smart Agriculture Objectives:

- Increasing agricultural productivity
- Resilience to climate change
- Reducing greenhouse gas

http://www.fao.org

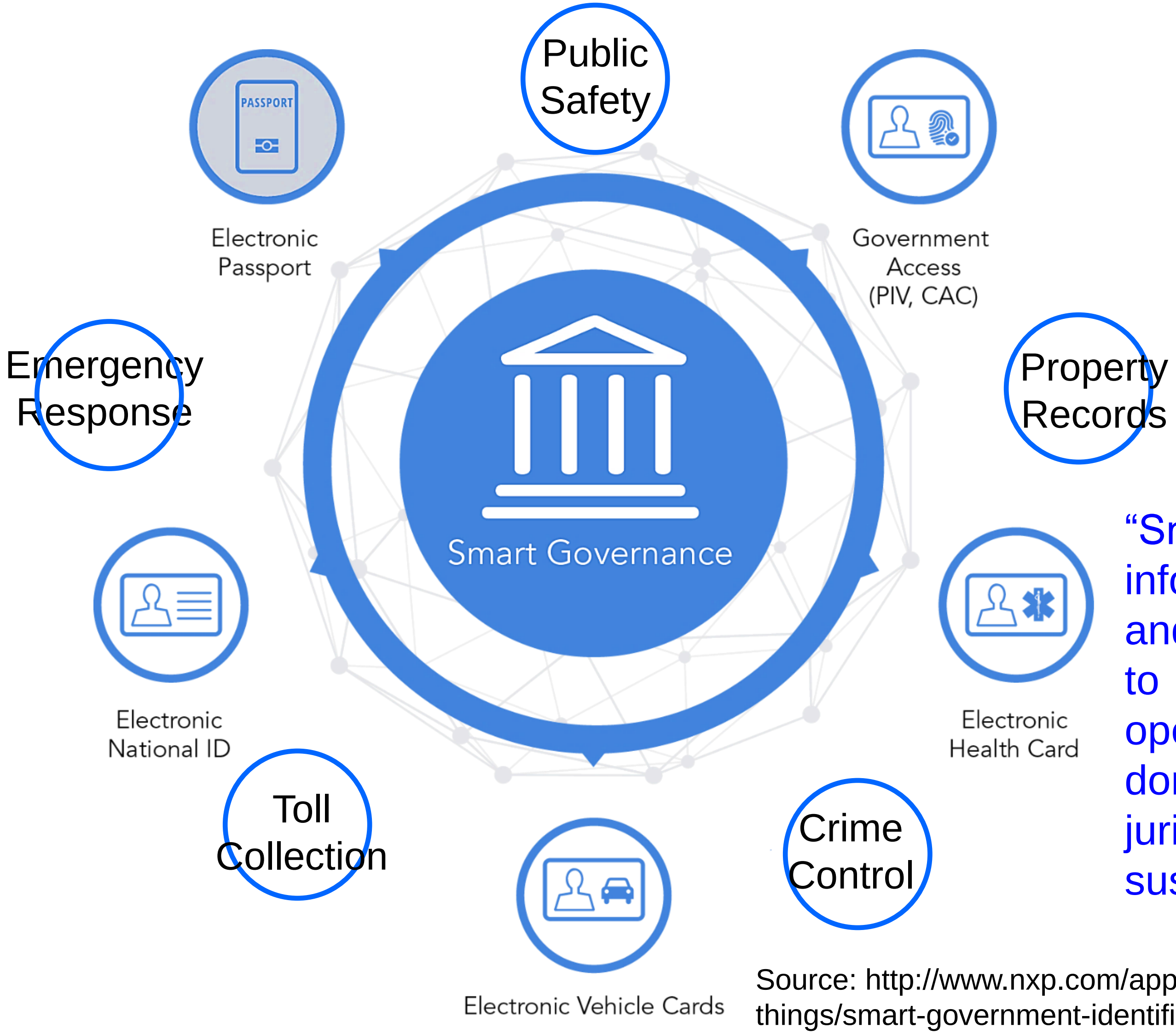
Automatic Irrigation System

Source: Maurya 2017, CE Magazine July 2017

Smart Agriculture/Farming Market Worth $18.21 Billion By 2025

Sources: http://www.grandviewresearch.com/press-release/global-smart-agriculture-farming-market

IoT in Smart Government



"Smart government integrates information, communication and operational technologies to planning, management and operations across multiple domains, process areas and jurisdictions to generate sustainable public value."
-- http://www.gartner.com

Source: http://www.nxp.com/applications/internet-of-things/secure-things/smart-government-identification:SMART-GOVERNANCE

IoT in Smart Structure

Smart Building

Source: http://www.exchangecommunications.co.uk/products/smart-building-and-cities/smart-buildings.php

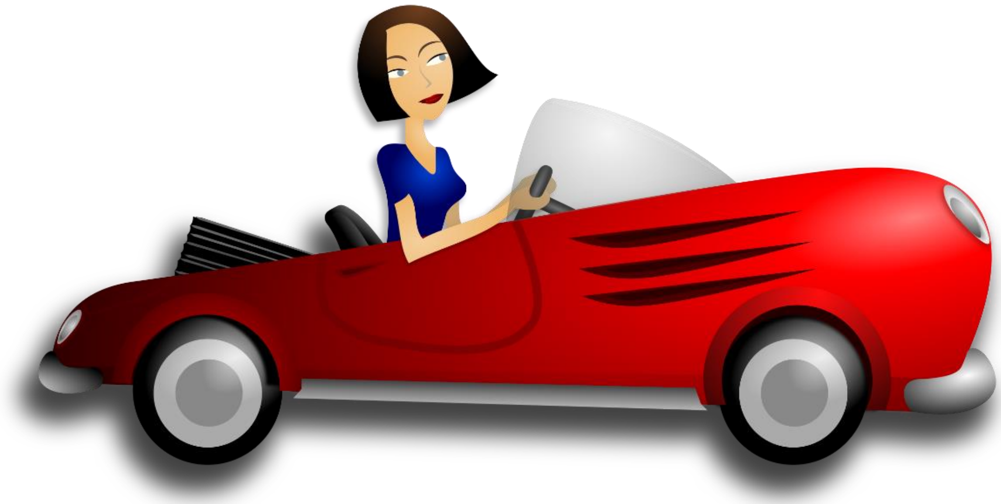
Smart Structure

Source: https://www.slideshare.net/RajivDinesh2/lelantosstructuralhealthmonitoringbrochure

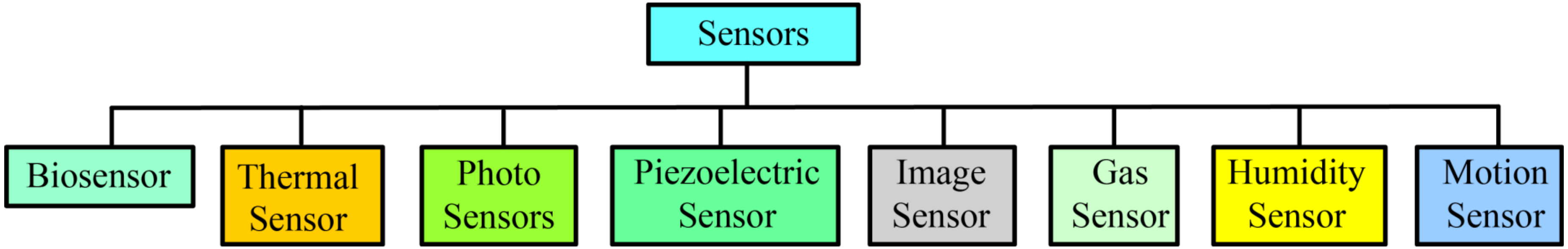
IoT in Smart Home

Source: https://community.cadence.com/cadence_blogs_8/b/ip/archive/2014/08/28/jot-applications-wrestling-with-energy_2c00_-cost-and-time-to-market-considerations

Driving Technologies



Cheap and Compact Sensor Technology



Source: Mohanty 2015, McGraw-Hill 2015

Gas Sensor

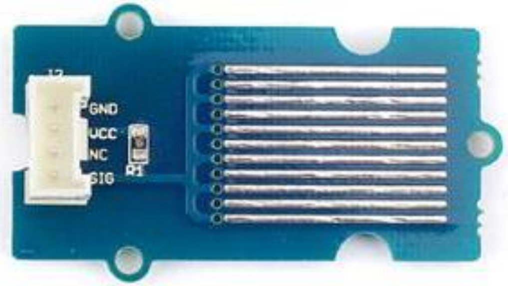
Temperature Sensor

Air Quality Sensor

Humidity and Temperature Sensor

Light Sensor

Barometer Sensor



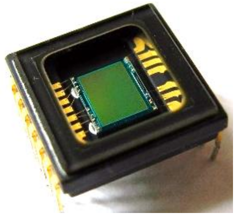
Water Sensor

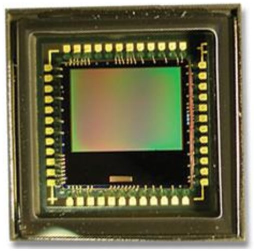
Dust Sensor

Source: http://wiki.seeed.cc/Sensor/

Better Imaging Sensor Technology

- Image Sensors
  - Charged Couple Device (CCD) Sensor
  - Complementary Metal Oxide Semiconductor (CMOS) Sensors
    - Passive Pixel Sensor (PPS)
    - Active Pixel Sensor (APS)
      - Based on Sensing Element
        - Photodiode-Type APS
        - Photogate-Type APS
      - Based on Operation Mode
        - Linear-Mode APS
        - Logarithmic-Mode APS
    - Digital Pixel Sensor (DPS)



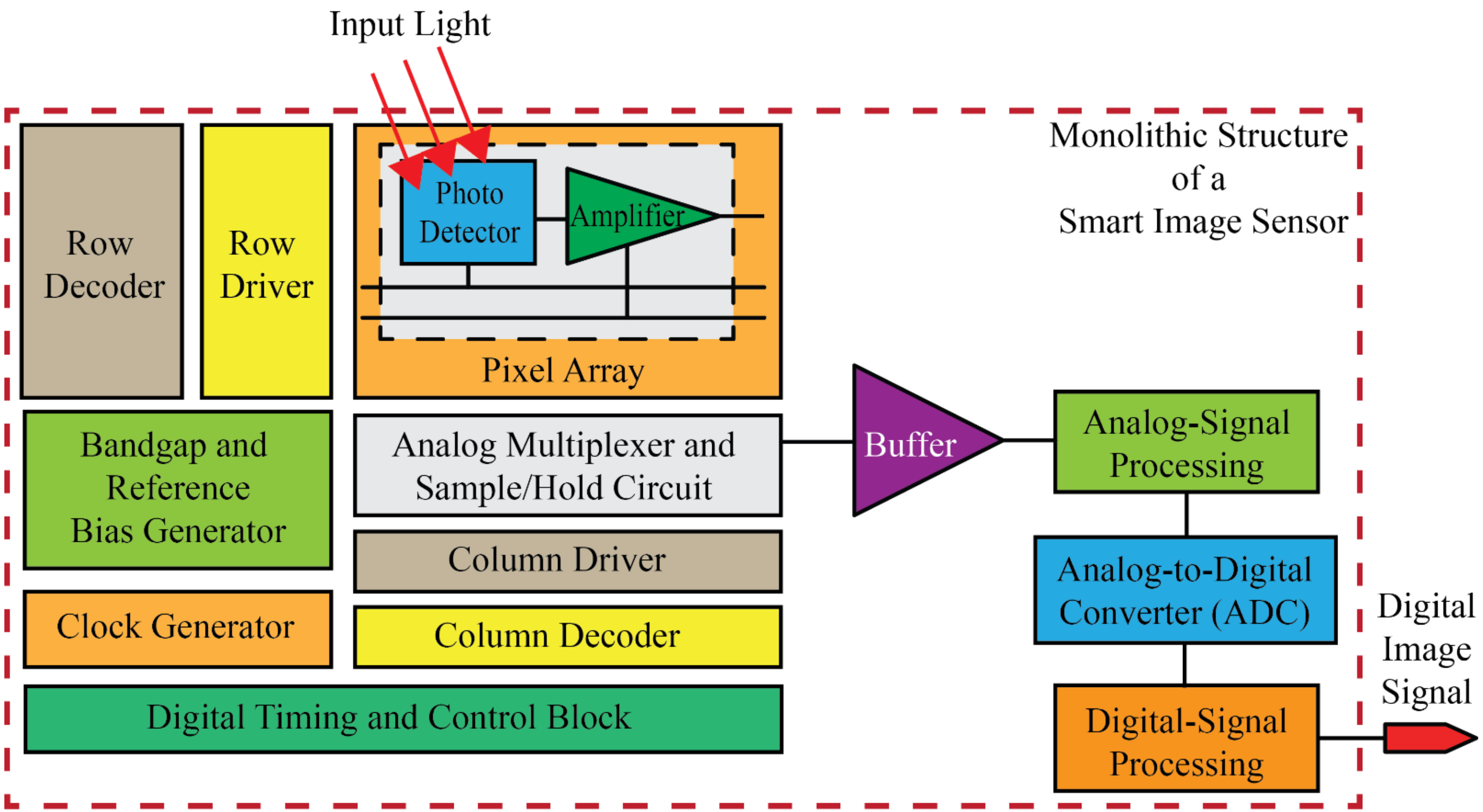


"The global CMOS image sensor market is likely to be worth $10.17 billion by 2020."

Source: Mohanty 2015, McGraw-Hill 2015

Source: http://www.grandviewresearch.com/press-release/global-cmos-image-sensors-market

Smart Image Sensor



Source: Mohanty 2015, McGraw-Hill 2015

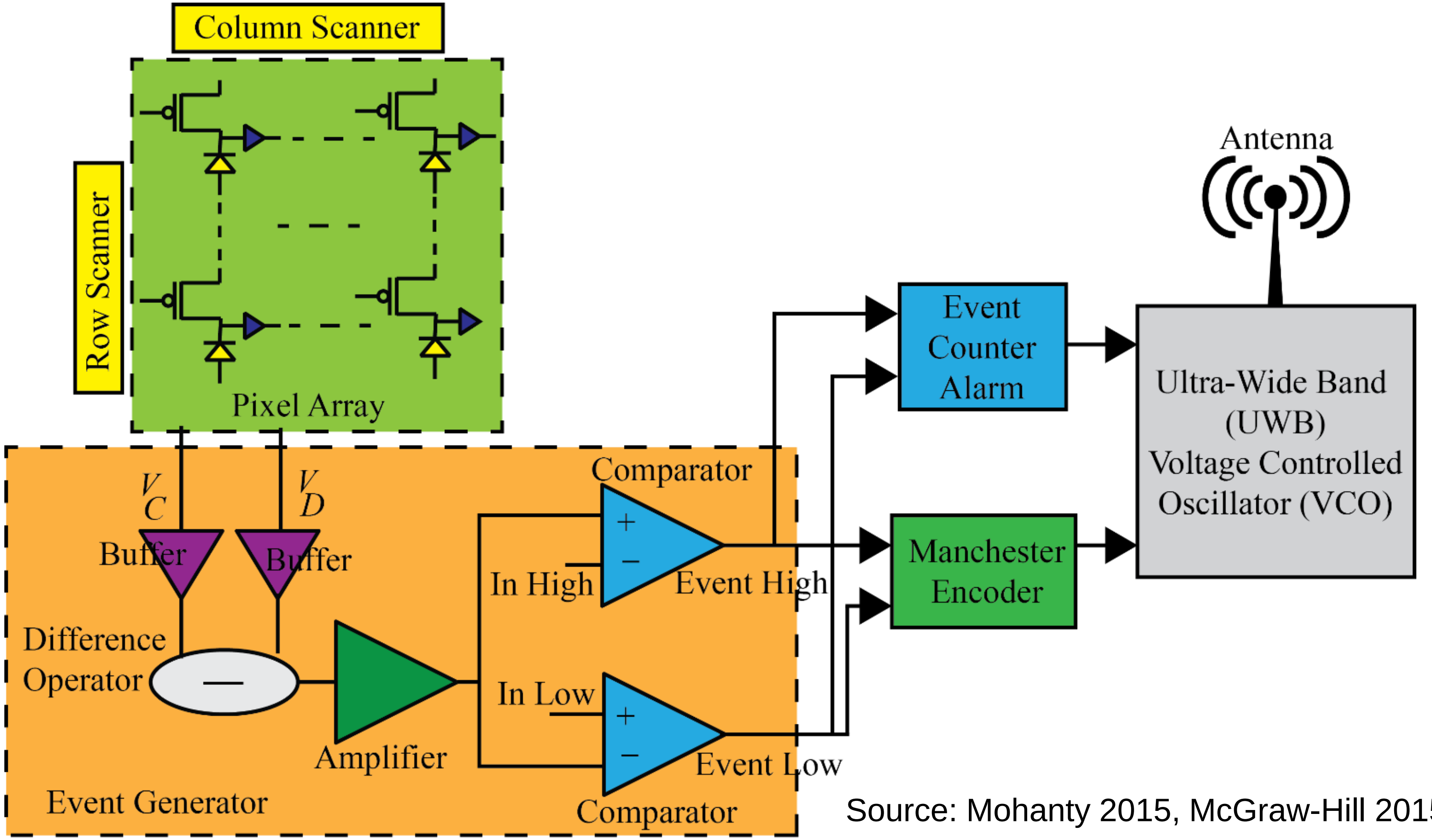
Smart Image Sensor

- Pixel array consists of photodetectors and amplifiers.
- Scanning and addressing circuitry builds digital memory-style random access reading of pixels in APS array.
- Analog MUX and sample/hold constitute the analog front-end circuitry of smart image sensor that process all the pixels in a selected row and samples onto sample/hold circuit at end of respective columns.
- ADC converts analog signal to digital for further processing.
- DSP performs wide range of processing in smart image sensor.

Smart Image Sensor

- Clock generator provides a base clock to the different components of smart image sensor
- Digital timing and control block control the operation of the complete smart image sensor.
- Band gap and reference generator produces the on-chip analog voltage and current reference for other units such as amplifiers, ADCs and clock generators.

Wireless Image Sensor



Source: Mohanty 2015, McGraw-Hill 2015

Wireless Image Sensor

- In this sensor, pixel array receives the incident light and converts into voltage.
- When a specific pixel is accessed for readout, both the integration voltage and previous voltage stored in pixel capacitor are read out.
- Event generator calculates the difference between the two and compares with a positive and negative threshold.
- Event bitstream is encoded in Manchester encoder and converted into an impulse sequence in UWB transmitter for wireless transmission.

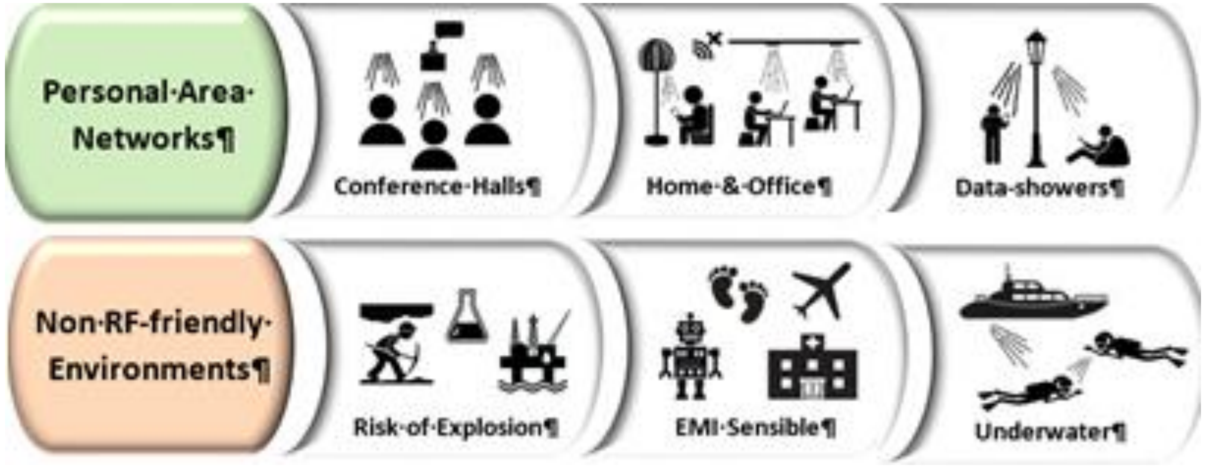
Variety of Communications Technology

Visible Light Communications (VLC)

- LEDs can switch their light intensity at a rate that is imperceptible to human eye.
- This property can be used for the value added services based on Visible Light Communication (VLC).

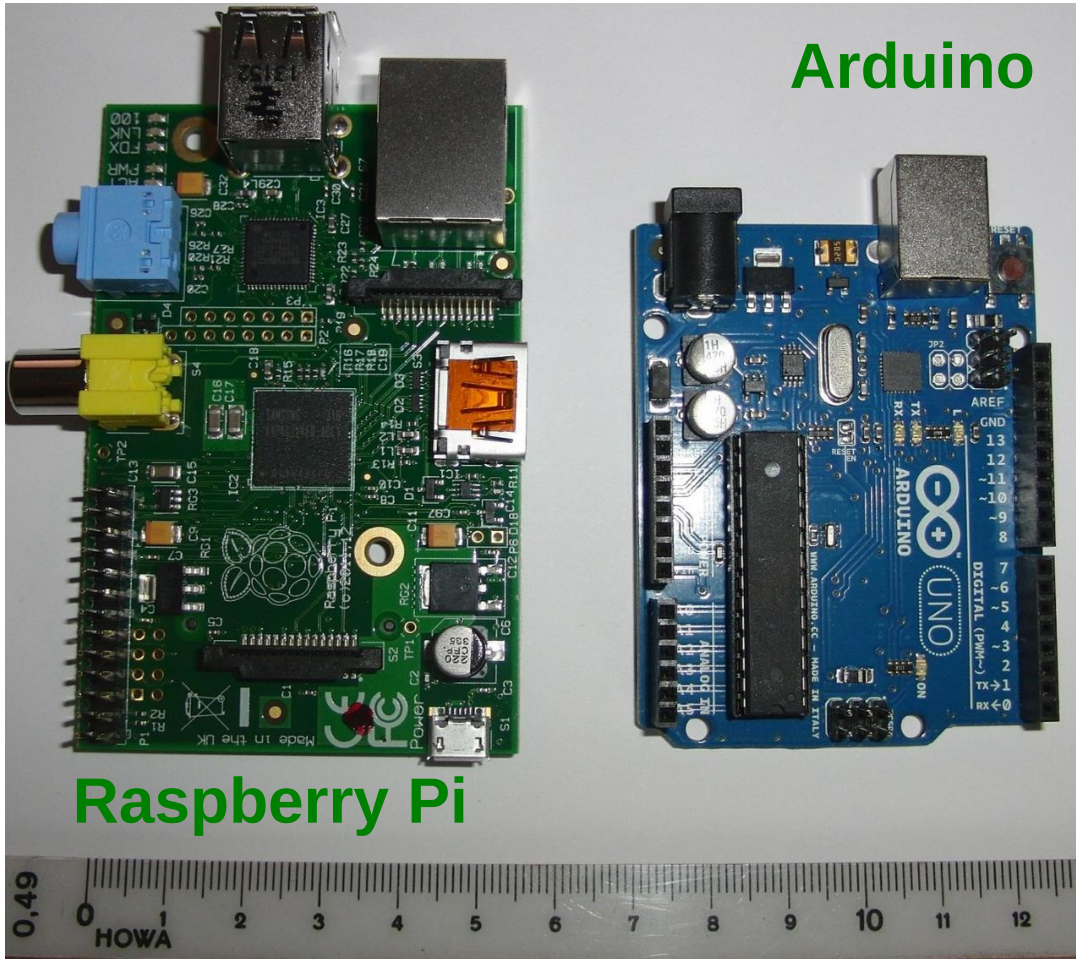
Characteristic	LiFi	WiFi
Bandwidth	Huge	Limited
Requires Line of Sight	Yes	No
EMI + Hazard Concerns	Low	High
Susceptibility to Eavesdropping	Low	High
Range	Short	Medium
Data Density	High	Limited

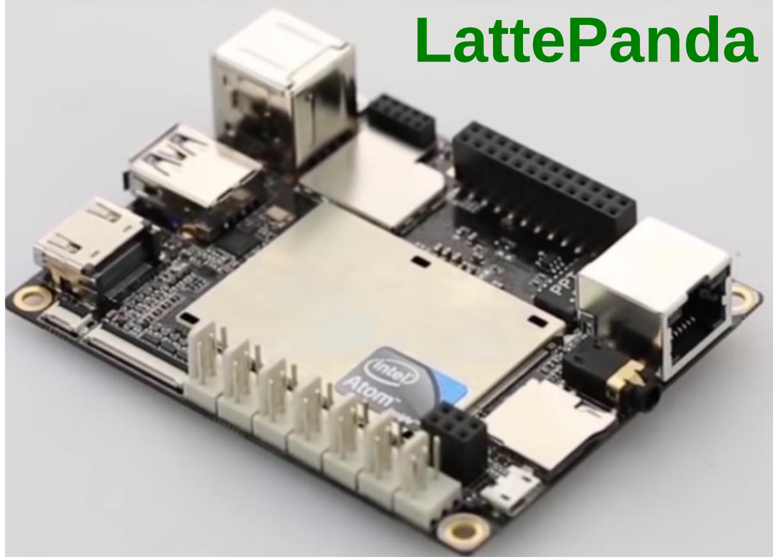
Source: VLCS-2014



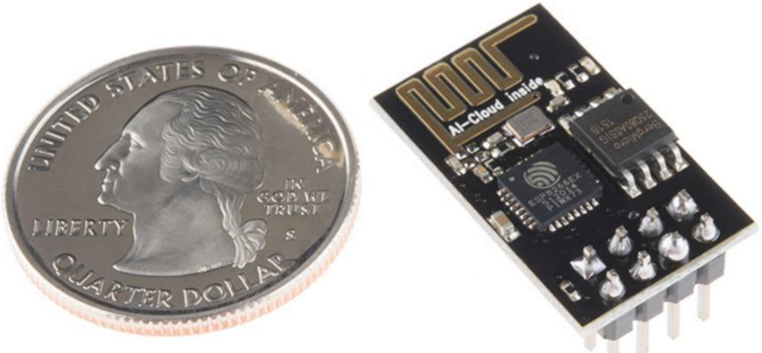
Source: Ribeiro 2017, CE Magazine October 2017

Cheap Computing Technology





Source: http://www.lattepanda.com



Source: https://www.sparkfun.com/products/13678

Efficient Media Compression – Better Portable Graphics (BPG)

- **BPG compression instead of JPEG?**
- Attributes that differentiate BPG from JPEG and make it an excellent choice include:
  - Meeting modern display requirements: high quality and lower size.
  - BPG compression is based on the High Efficiency Video Coding (HEVC), which is considered a major advance in compression techniques.
  - Supported by most web browsers with a small Javascript decoder.

JPEG Compression

BPG Compression

Source: Mohanty 2016, IEEE Access 2016

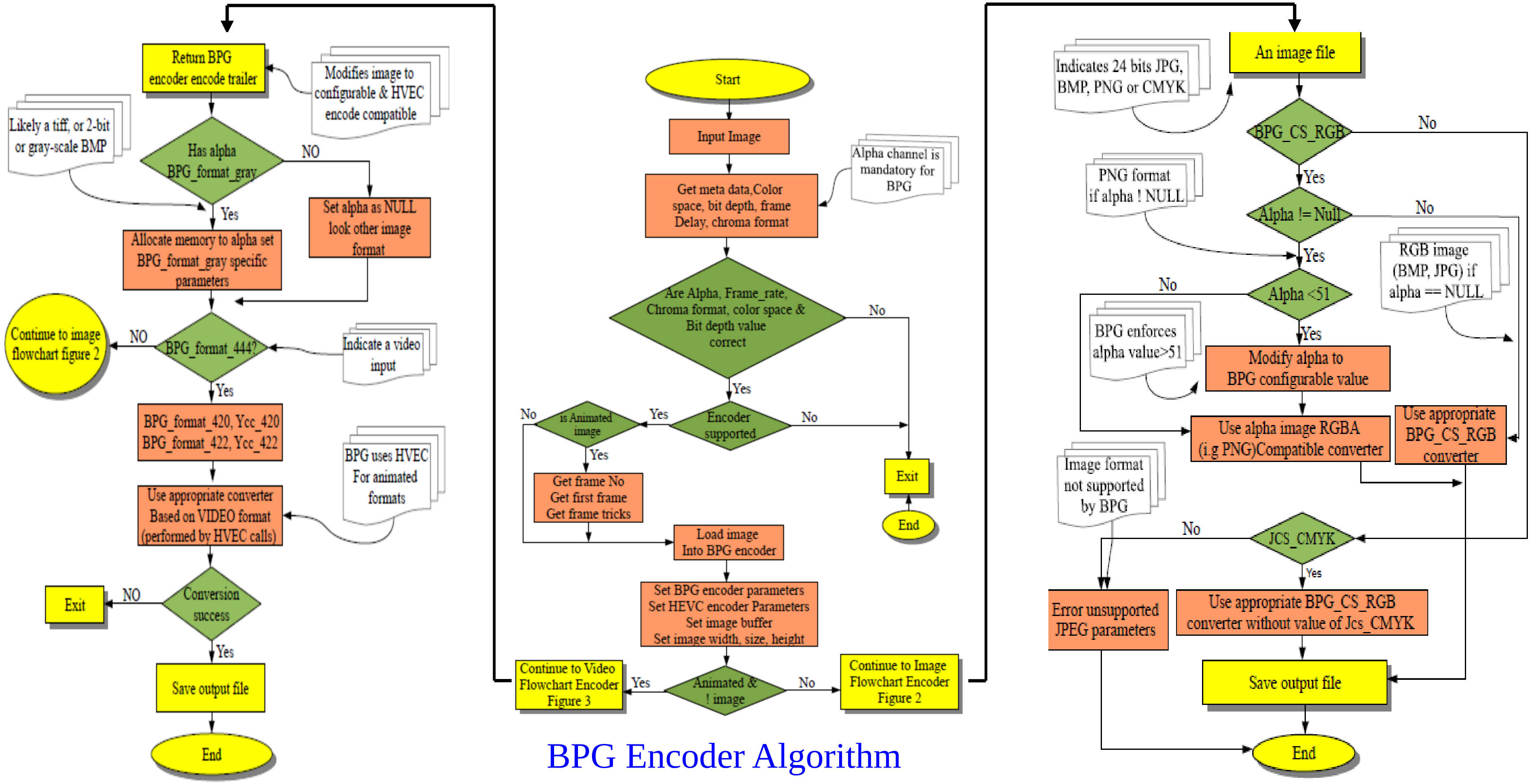
BPG Compression

- **Why BPG compression and not JPEG?**

4) It is open source.
5) BPG is close in spirit to JPEG and can offer lossless compression in the digital domain.
6) Different chroma formats supported include grayscale, RGB, YCgCo, YCbCr, Non-premultiplied alpha, and Premultiplied alpha.
7) BPG uses a range of metadata for efficient conversion including EXIF, ICC profile, and XMP.

Source: Mohanty 2016, IEEE Access 2016

Simplified BPG Algorithm



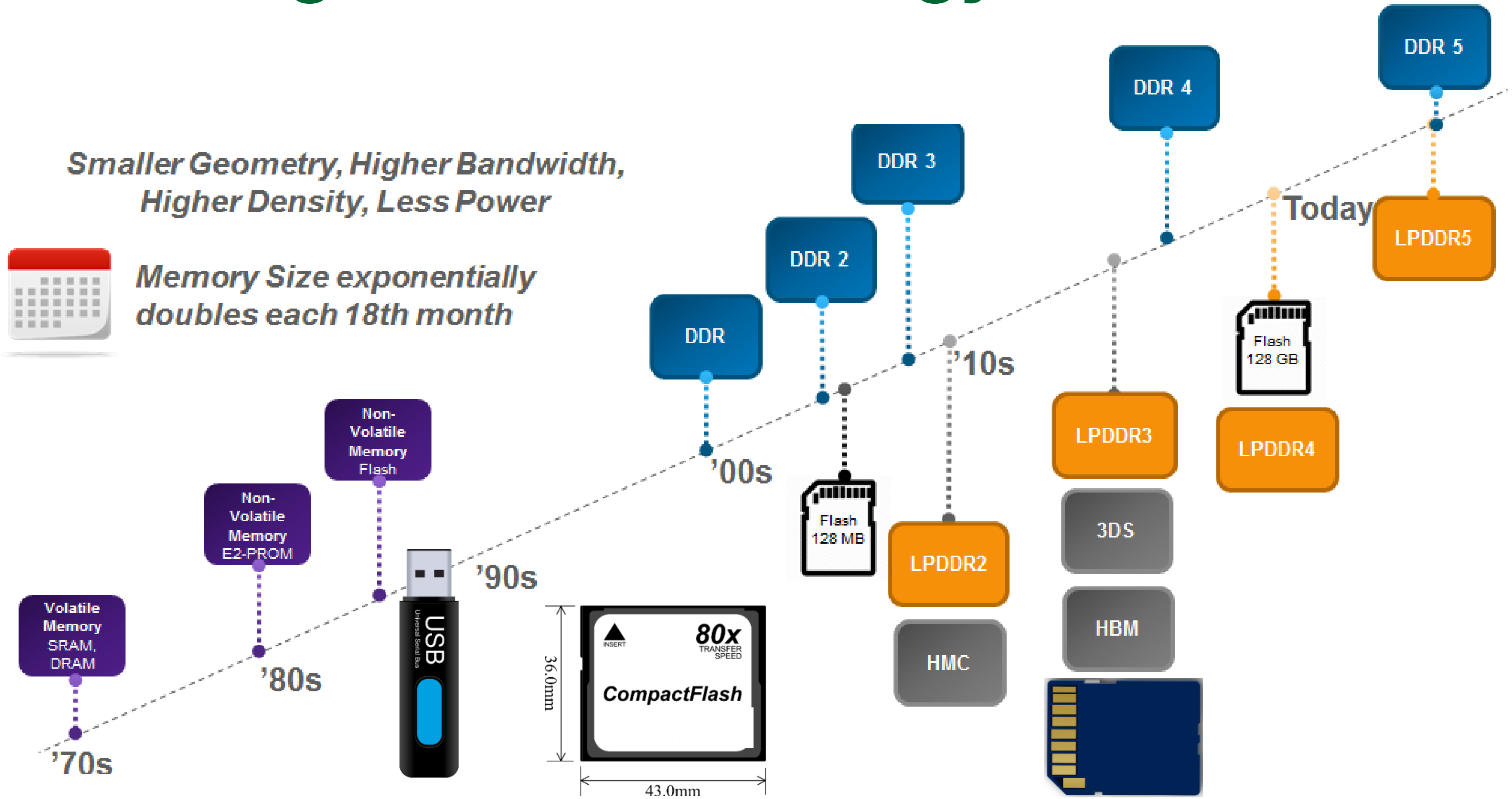
BPG Encoder Algorithm

Video Encoder Algorithm

Source: Mohanty 2016, IEEE Access 2016

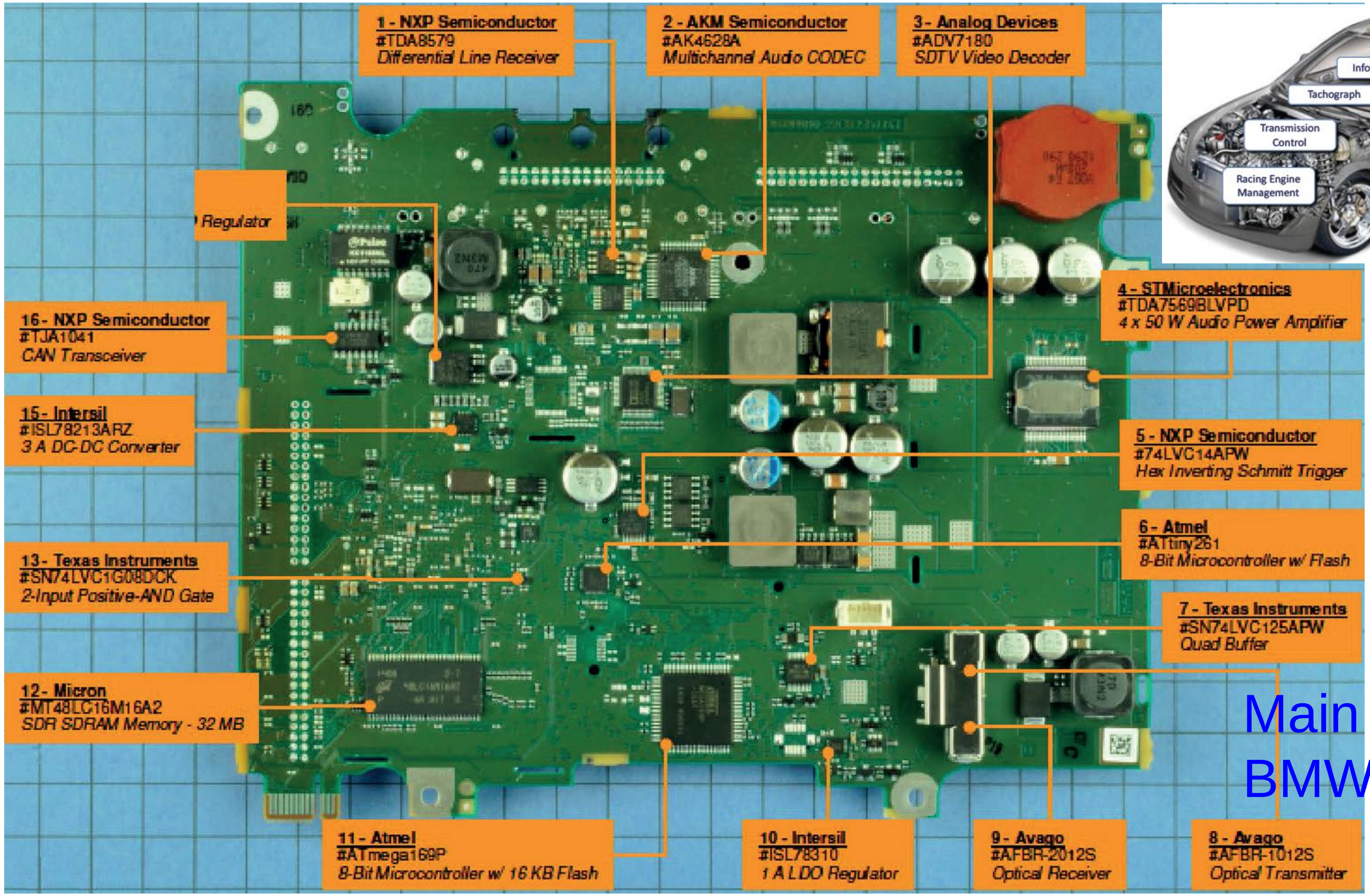
Image Encoder Algorithm

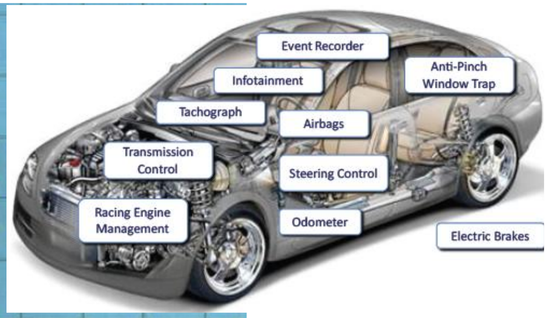
Memory Technology: Cheaper, Larger, Faster, Energy-Efficient



Source: https://blogs.synopsys.com/vip-central/2015/12/01/keeping-pace-with-memory-technology-using-advanced-verification/

Memory Technology – Car Example





Main Board of BMW HBB125.

Source: Coughlin 2016, CE Magazine October 2016

Variety of Computer Memory

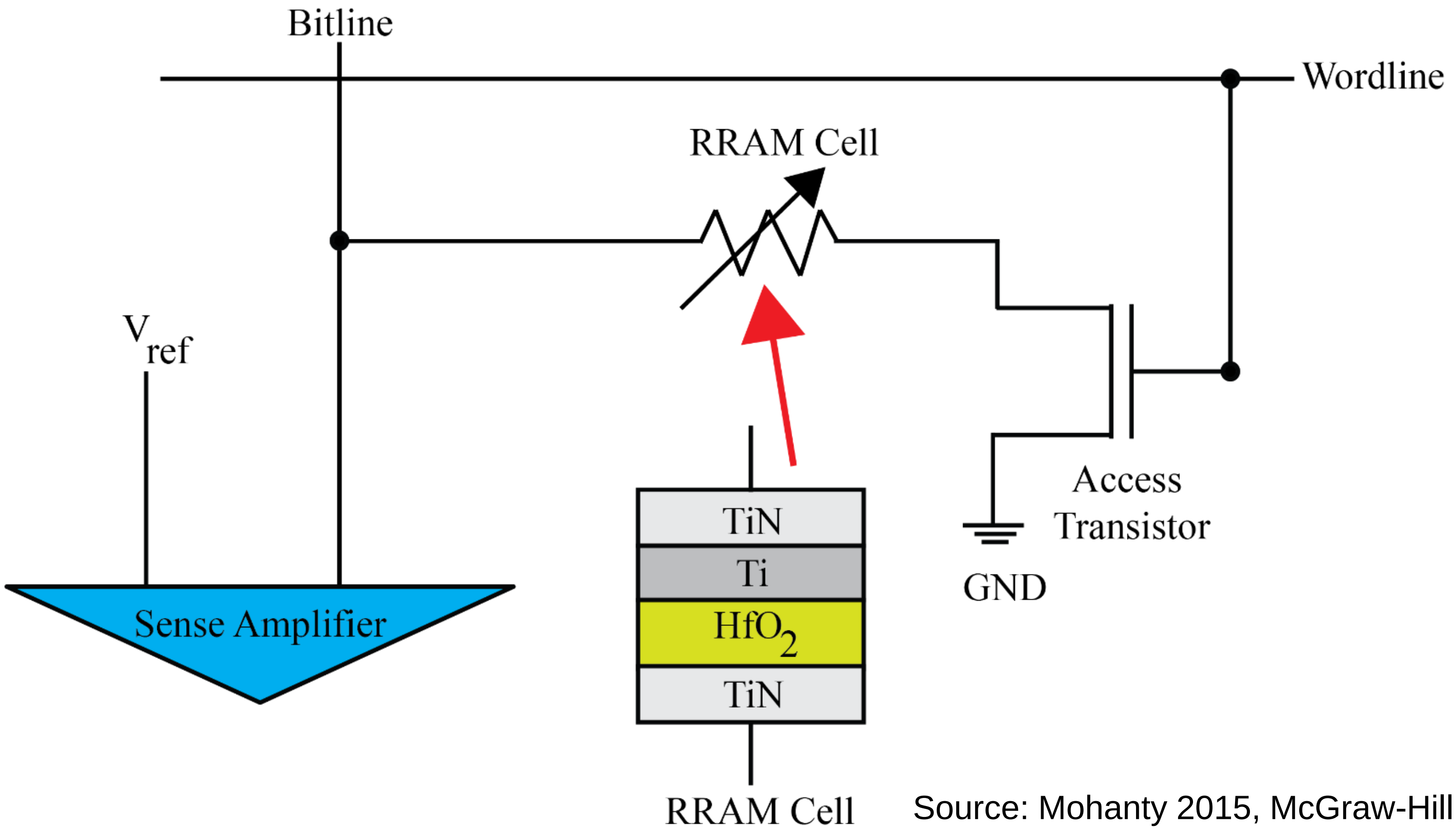
- **Computer Memory**
  - **Based on Storage Capability**
    - **Volatile**
      - Static RAM (SRAM)
      - Dynamic RAM (DRAM)
      - Twin Transistor RAM (TTRAM)
      - Zero-Capacitor RAM (ZRAM)
      - Thyristor RAM (TRAM)
    - **Nonvolatile**
      - Read-Only Memory (e.g. Programmable ROM (PROM), Erasable PROM (EPROM), Electrically Erasable PROM (EEPROM)
      - Magnetic Storage Hard Disk Drive (HDD)
      - Non-Volatile RAM (NVRAM) (e.g Flash Memory)
      - Resistive RAM (RRAM or ReRAM)
      - Magnetic or Magnetoresistive RAM (MRAM)
      - Phase-Change RAM (PRAM, PCRAM)
      - Conductive Metal Oxide (CMOX) Memory
  - **Based on Access**
    - Random-Access Memory (RAM)
    - Serial Access Memory (e.g. Shift Registers, Queues)
    - Content Addressable Memory (CAM)

Source: Mohanty 2015, McGraw-Hill 2015

The flash memory market is expected to be worth $37.6 worldwide by 2020.

Source: https://www.statista.com/statistics/553556/worldwide-flash-memory-market-size/

Schematic of Resistive RAM (RRAM or ReRAM)

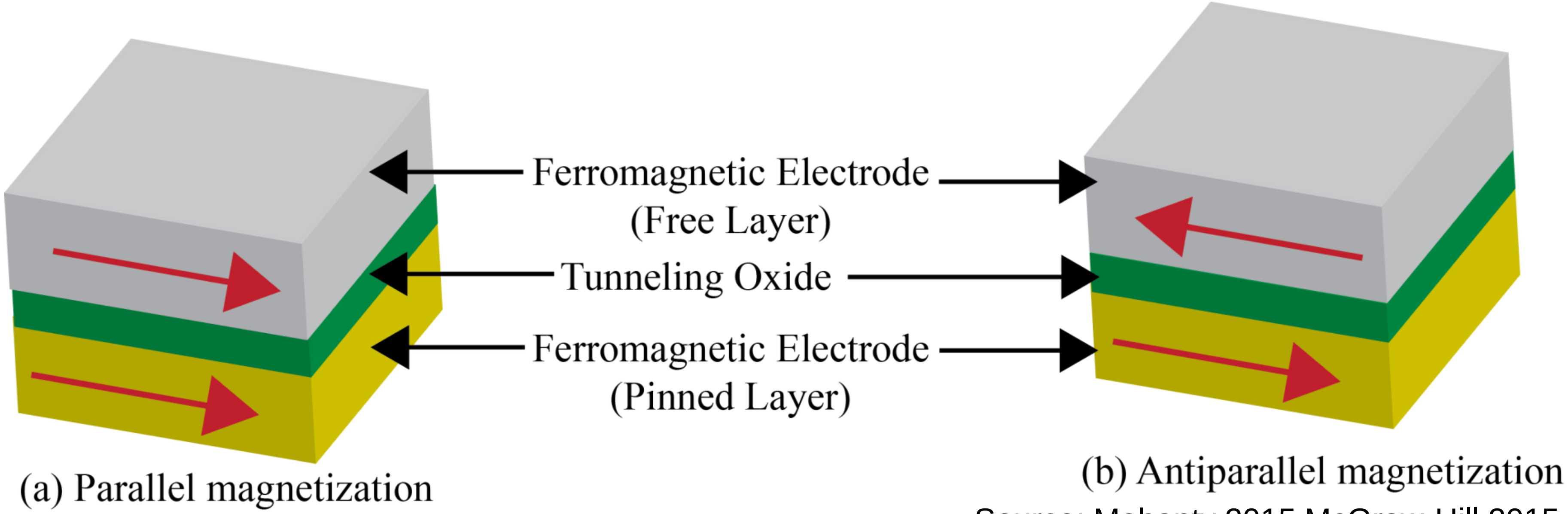


Source: Mohanty 2015, McGraw-Hill 2015

Schematic of ReRAM

- In the Figure 7.45, ReRAM cell shown is a hafnium dioxide based resistive memory where electrode is made of TiN.
- The change in resistance is caused by the trapping and detrapping of process in HfO_2.
- The traps are typically oxygen vacancies included by the oxygen guttering of reactive Ti film.

Magnetic or Magnetoresistive RAM



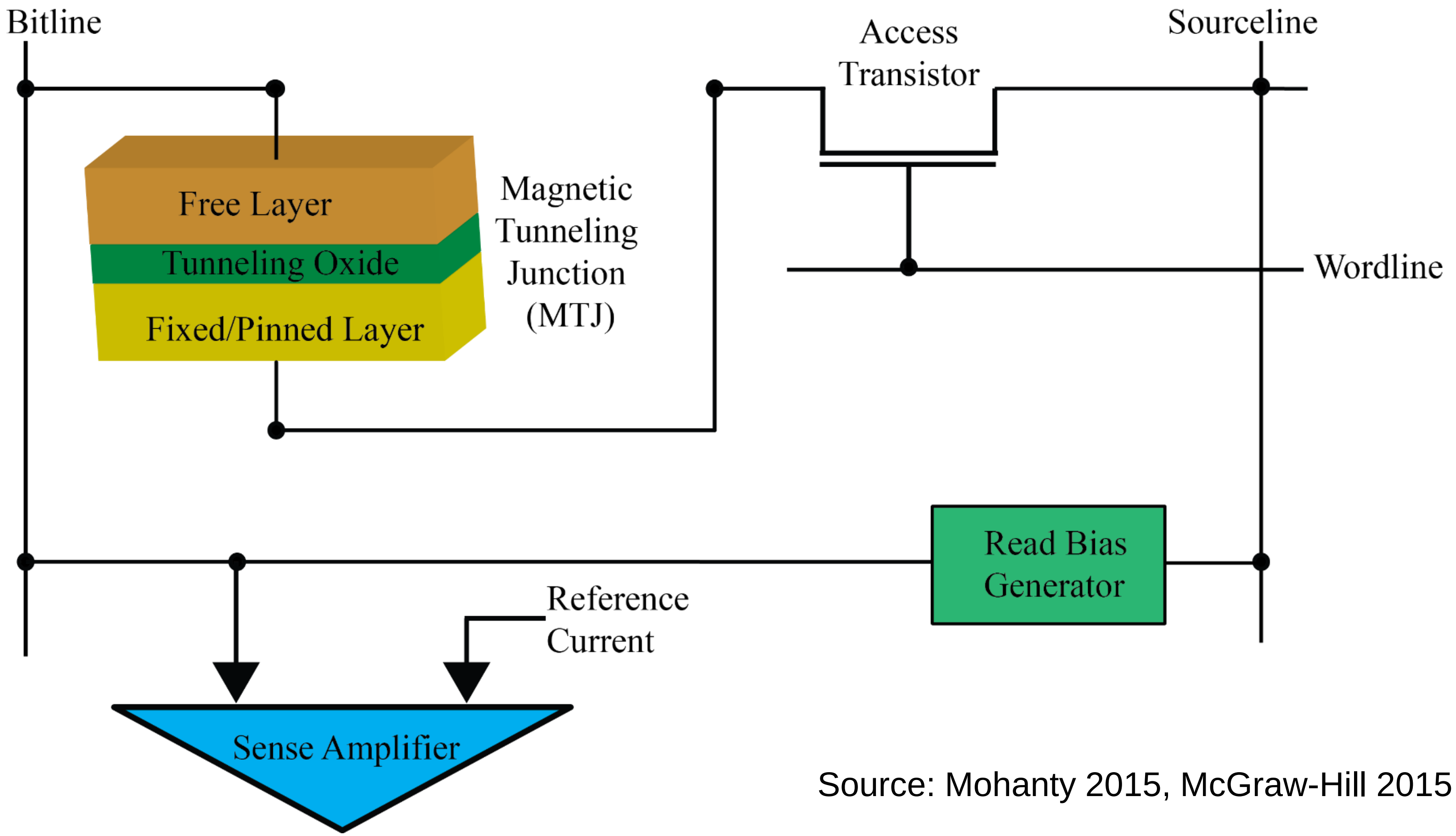
Source: Mohanty 2015 McGraw-Hill 2015

- Magnetic or Magnetoresistive RAM is a nonvolatile memory that stores data using magnetic polarization rather than electric charge.
- MRAM uses tunneling resistance that depends on the directions of the magnetization of the ferromagnetic electrodes.
- Key advantages: Simple interfaces, Compact sizes

Magnetic or Magnetoresistive RAM

- Magnetic or Magnetoresistive RAM is a nonvolatile memory that stores data using magnetic polarization rather than electric charge.
- MRAM uses tunneling resistance that depends on the directions of the magnetization of the ferromagnetic electrodes.
- Key advantages of MRAM include simple interfaces, compact sizes, wide range operating development since the 1990s and has potential to replace many types of memory.

Transistor Level STT-MRAM

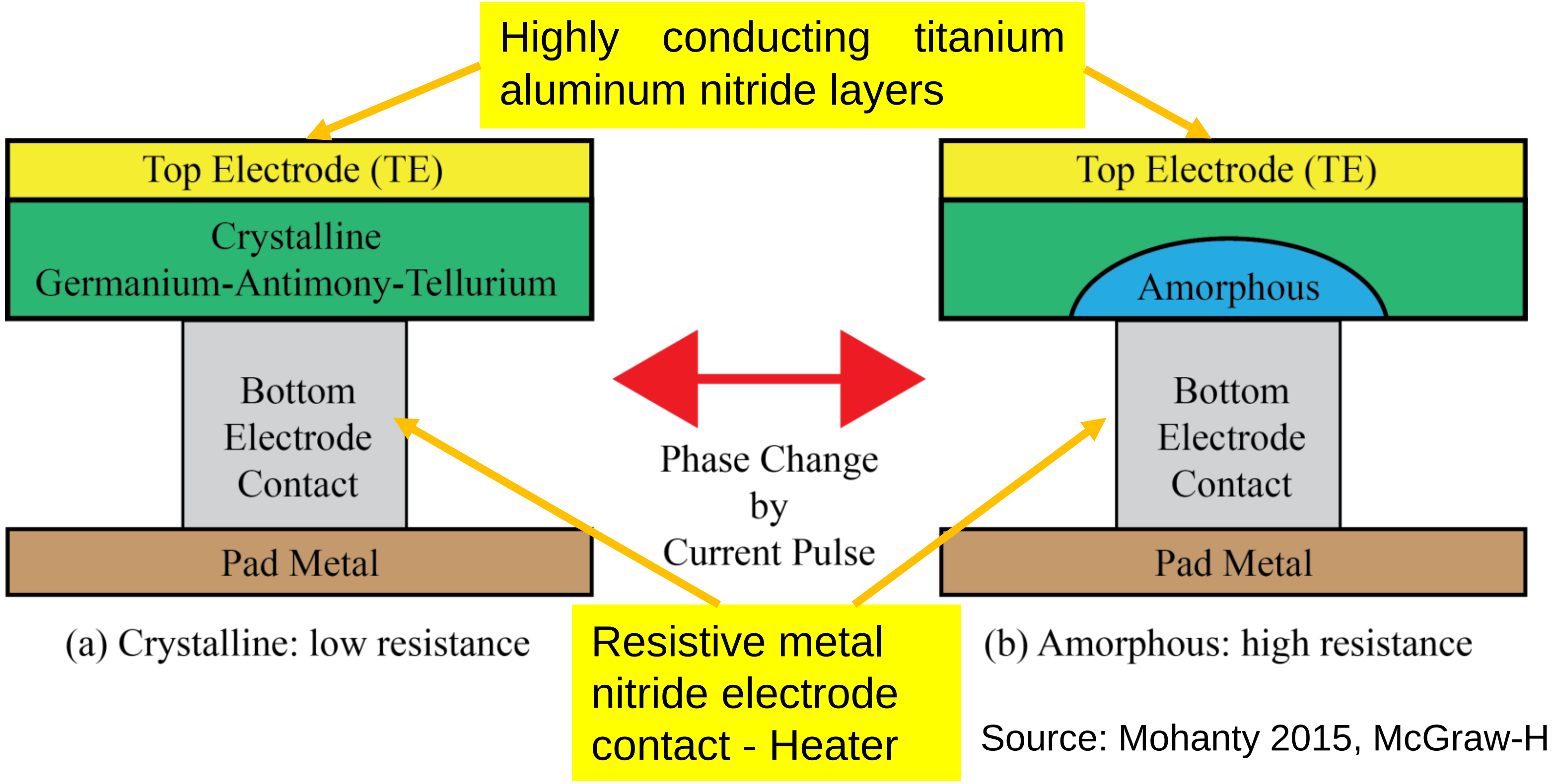


Source: Mohanty 2015, McGraw-Hill 2015

Transistor Level STT-MRAM

- The read operation of STT-MRAM can be performed in two ways: parallel read operation and anti parallel operation.
- A bidirectional flow of current is required for write operation due to hysteresis characteristic of Magnetic Tunneling Junction.
- When current of the STT-MRAM cell is above the switching threshold current of the MTJ, magnetization direction of the free layer is changed from antiparallel to parallel.

Phase–Change RAM



Source: Mohanty 2015, McGraw-Hill 2015

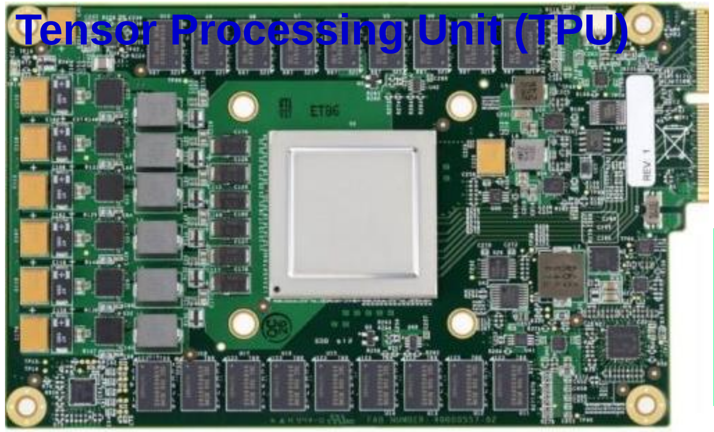
- Phase–Change RAM is a non volatile memory which uses the phase-change materials as compared to the electrical charges.
- Phase change material the actually serves as storage element is the germanium-antimony-tellurium chalcogenide alloy.

Phase–Change RAM

- Phase–Change RAM is a non volatile memory which uses the phase-change materials as compared to the electrical charges of classical SRAM and DRAM technology.
- Electrodes are made using highly conducting titanium aluminium nitride layers.
- A cylindrical resistive metal nitride electrode is deposited on the lower electrode that forms the bottom electrode contact, thereby, essentially forming a heater.
- Phase change material the actually serves as storage element is the germanium-antimony-tellurium chalcogenide alloy.

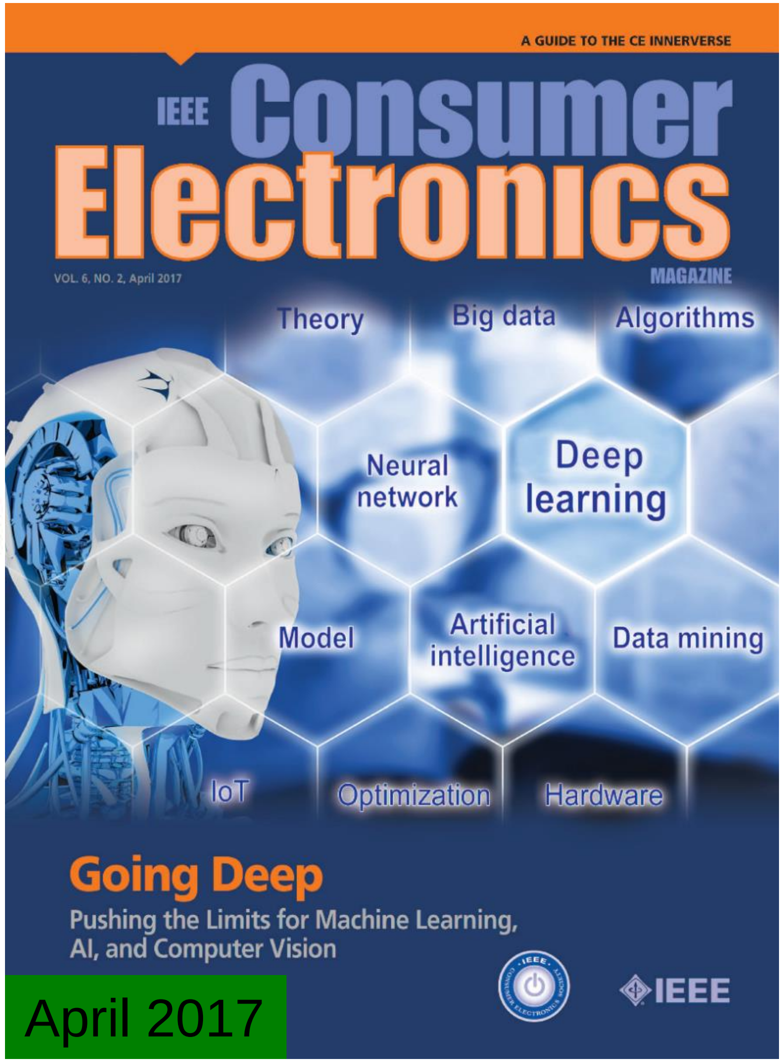
Machine Learning Technology

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

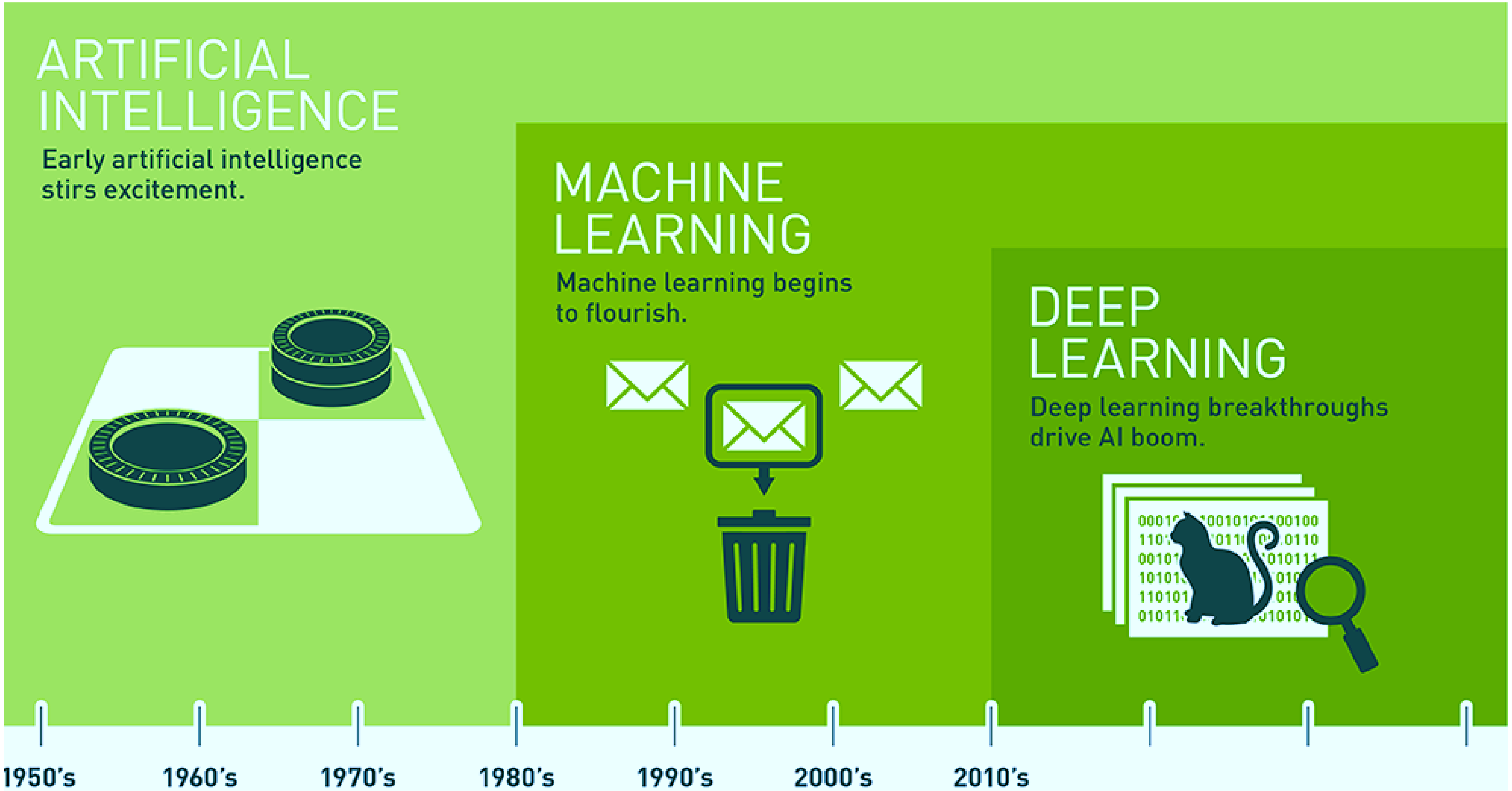


Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

IoT Use:
- Better decision
- Faster response



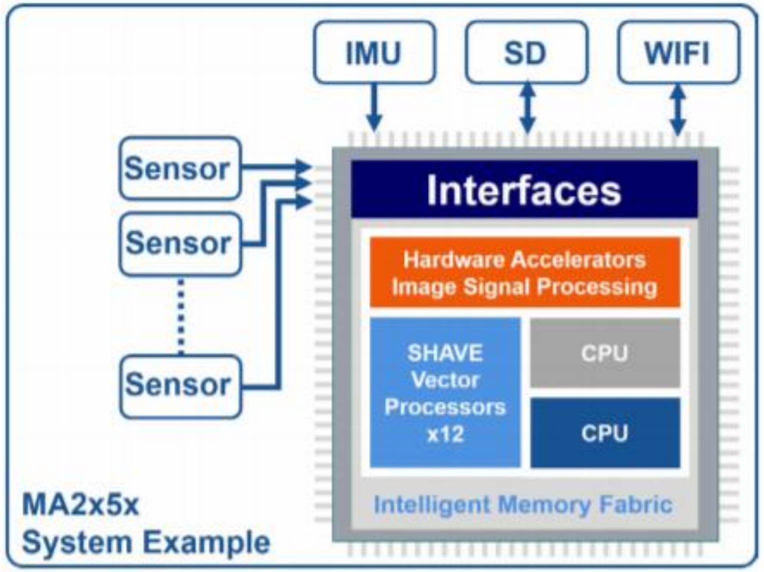
AI, Machine Learning, and Deep Learning



Source: https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/

Vision Processing Unit (VPU)

- High-Performance Machine Vision Processing
- Deep Neural Network-based Classification
- Pose Estimation
- 3D Depth Estimation
- Visual Inertial Odometry (Navigation)
- Gesture/Eye Tracking and Recognition



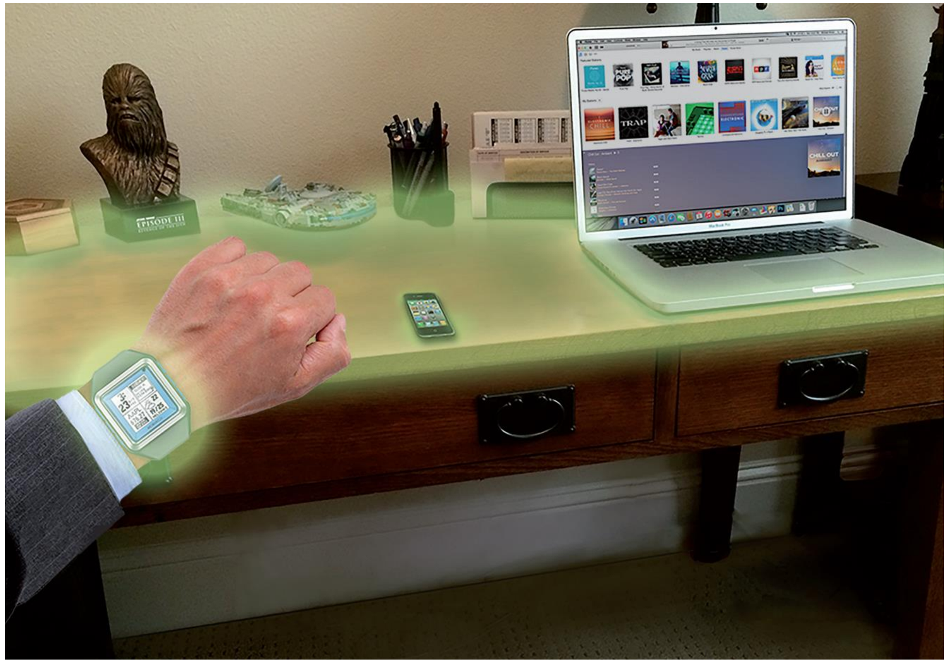
Vision Processing Unit (VPU)

Source: https://www.movidius.com/solutions/vision-processing-unit

- Video Processing Unit → Video encoding and decoding
- Graphics Processing Unit (GPU) → Rasterization and Texture Mapping
- Vision Processing Unit (VPU) → Machine vision algorithms (e.g. Convolutional Neural Network (CNN)

Magnetic Pixels

- A Magnetic Pixel is a charge surface (called emitter).
- Unique placement of these emitters in a matrix form the Magnetic Pixels (an array).
- Changes of a finger or hand approaching the pixel can be used.
- A magnetic pixel screen works in three dimensions; 3rd dimension is created by distance between finger and pixel surface.

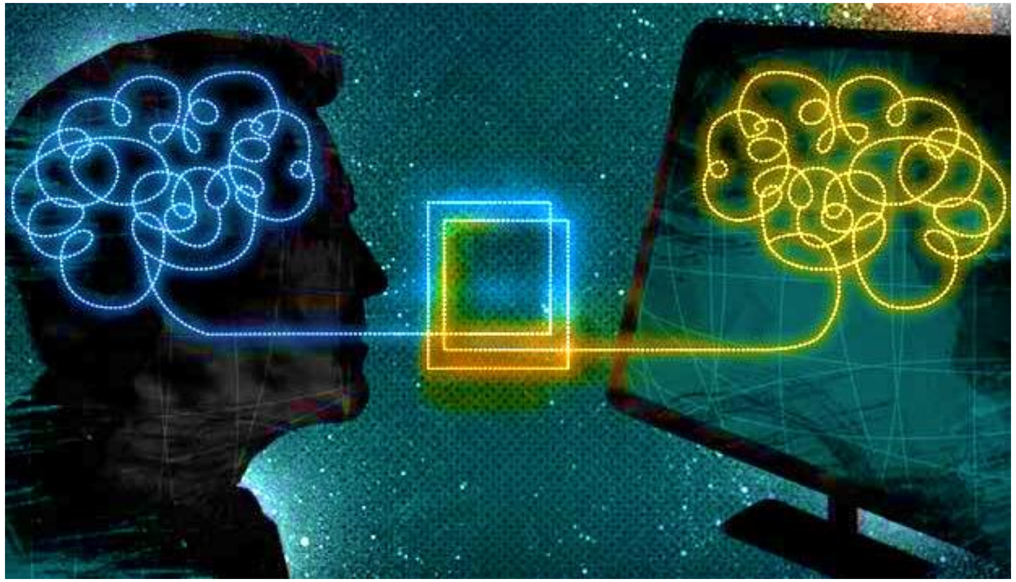


Source: Rubin 2017, CE Magazine July 2017

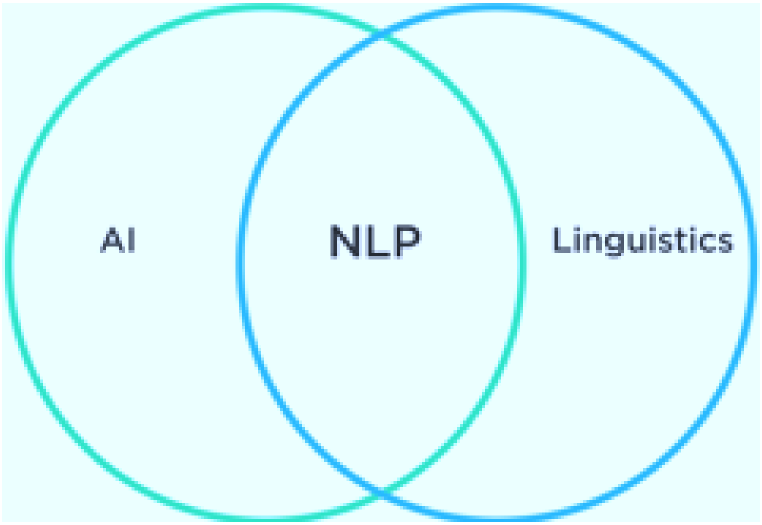
Usage:
- Touch- free control panel
- Powering/Charging CE systems

Natural Language Processing (NLP)

- NLP is the computer method to analyze, understand, and derive meaning from human language.
- Enables user to address computers as if they are communicating with a person.



Source: https://www.linkedin.com/pulse/natural-language-processing-2016-global-market-forecasts-rane



Source: http://blog.algorithmia.com/introduction-natural-language-processing-nlp/

Selected NLP Applications

- Machine Translation
- Information Retrieval
- Text Categorization
- Big Data

Cognitive Computing

The Tabulating Era (1900s – 1940s) | The Programming Era (1950s– present) | The Cognitive Era (2011 –)

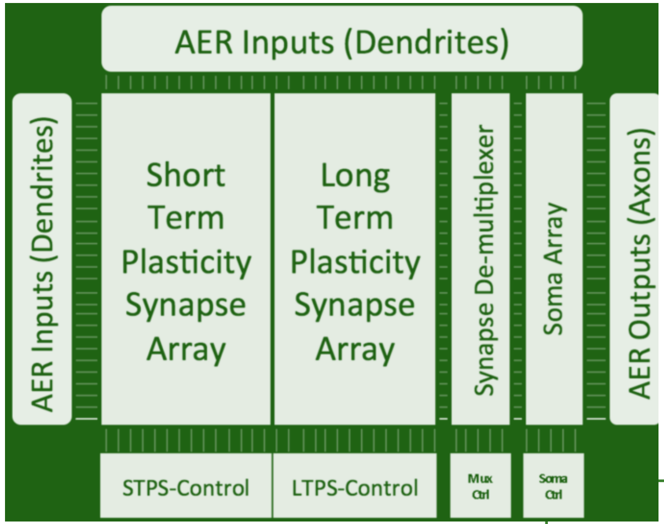
Cognitive Computing: Not just "right" or "wrong" anymore but "probably".

- Systems that learn at scale, reason with purpose and interact with humans naturally.
- Learn and reason from their interactions with humans and from their experiences with their environment; not programmed.

Usage:
- AI applications
- Expert systems
- Natural language processing
- Robotics
- Virtual reality

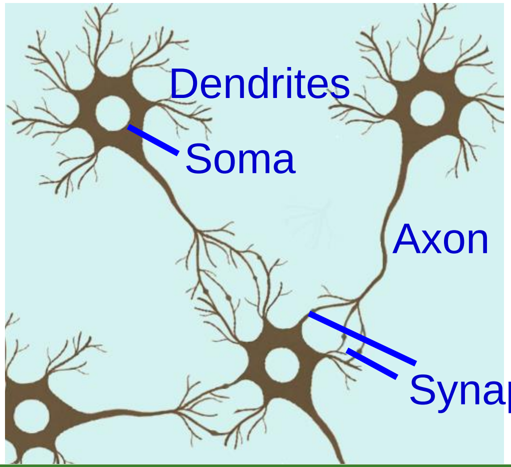
Source: http://www.research.ibm.com/software/IBMResearch/multimedia/Computing_Cognition_WhitePaper.pdf

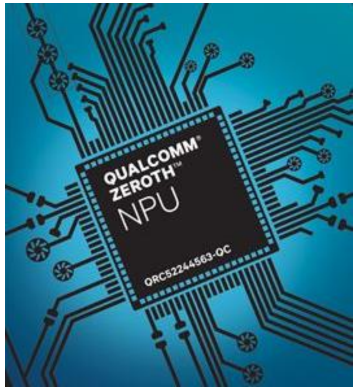
Neuromorphic Computing or Brain-Inspired Computing



Neuromorphic Architecture

Neuronal Circuits





Processing Powers MIT Technical Review

Types of Chips	Functions	Applications
Traditional Chips (von Neumann Architecture)	Reliably make precision calculations	Any numerical problem, Complex problems require more amount of energy
Neuromorphic Chips	Detect and Predict Patterns in complex data using minimal energy	Applications with significant visual/ auditory data requiring a system to adjust its behavior as it interacts with the world

Source: https://www.qualcomm.com/news/onq/2013/10/10/introducing-qualcomm-zeroth-processors-brain-inspired-computing

Neuromorphic Computing or Brain-Inspired Computing

Application 1: Integrate into assistive glasses for visually impaired people for navigating through complex environments, even without the need for a WiFi connection.

Application 2: Neuromorphic-based, solar-powered "sensor leaves" equipped with sensors for sight, smell or sound can help to monitor natural disasters.

Source: https://blogs.scientificamerican.com/observations/brain-inspired-computing-reaches-a-new-milestone/

Affective Computing

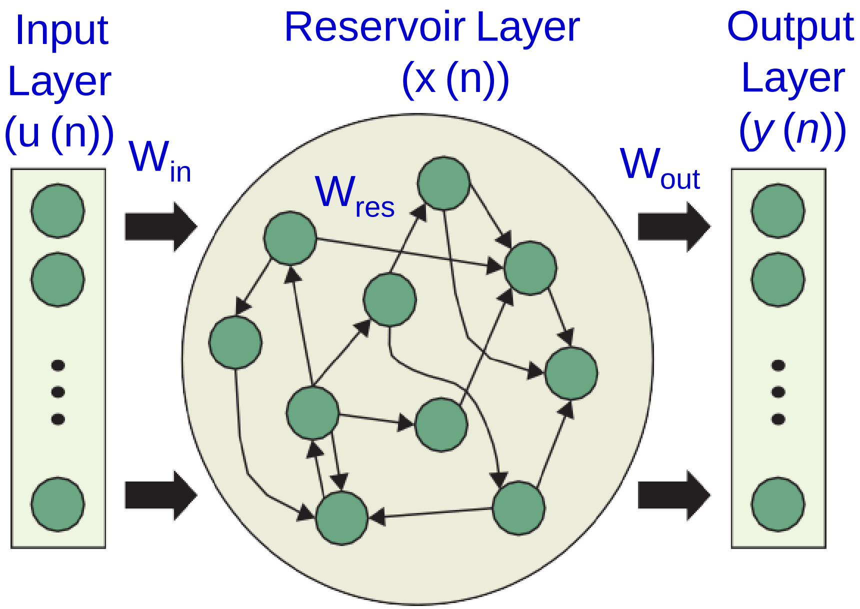
Affective Computing is the study and design of systems and devices that can recognize, interpret, process, and simulate human affective states (joy, anger, surprise, disgust, sadness, and fear).

Affective Computing ← Computer Science, Psychology, Cognitive Science, Artificial Intelligence (AI), Human–Computer Interaction (HCI)

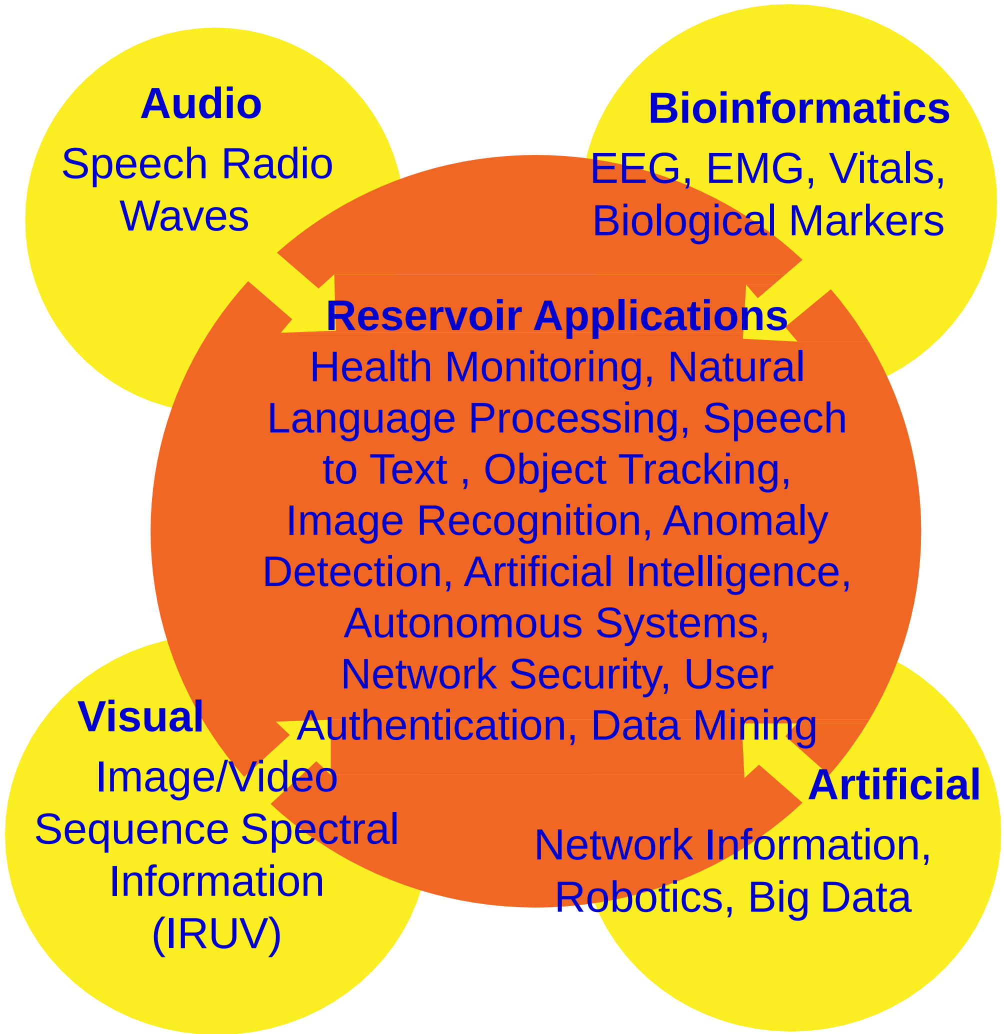
Source: http://www.telegraph.co.uk/technology/2016/01/21/affective-computing-how-emotional-machines-are-about-to-take-ove/

Reservoir Computing

Reservoir Computing is an approach to design, train, and analyze recurrent neural networks (RNNs). It uses a large, random RNN as an excitable medium (called a reservoir).

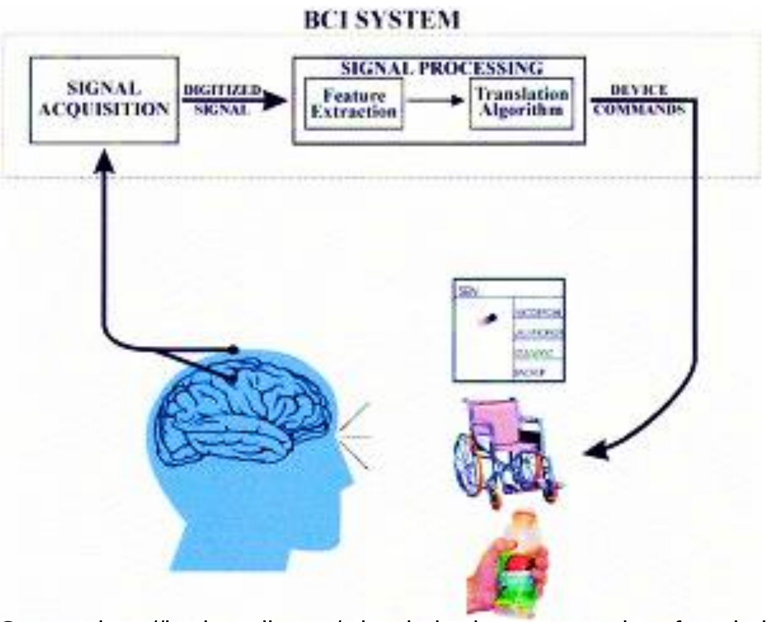


Source: http://reservoir-computing.org/



Source: Soures 2017, CE Magazine July 2017

Brain Computer Interface (BCI)



Source: http://brainpedia.org/what-is-brain-computer-interface-bci/

Source: http://brainpedia.org/brain-computer-interface-allows-paralysis-als-patients-type-much-faster/

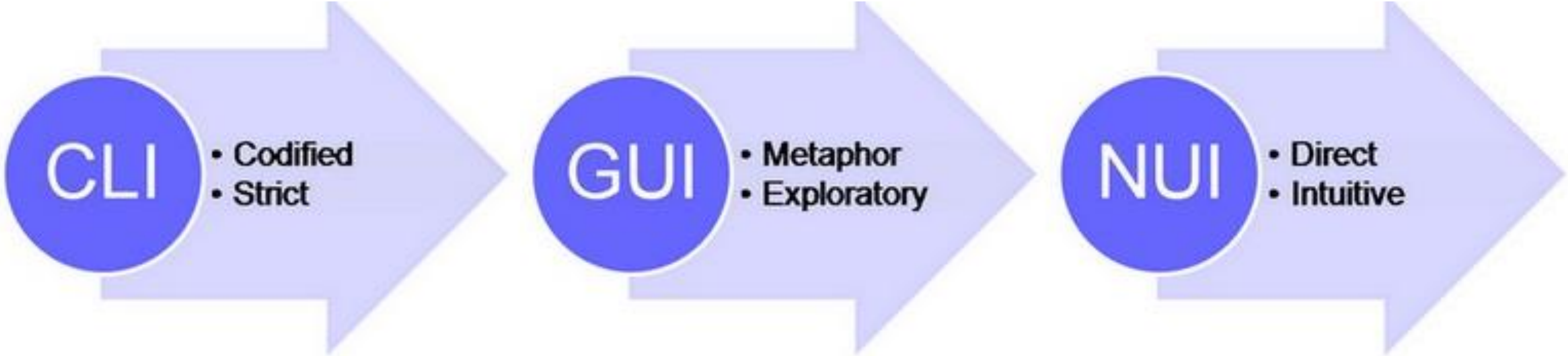
Brain-Computer Interface Allows paralysis patients to Type Faster

"Currently, people interact with their devices by thumb-typing on their phones. A high-bandwidth interface to the brain would help achieve a symbiosis between human and machine intelligence and could make humans more useful in an AI-driven world."

-- Neuralink - neurotechnology company - Elon Musk.

Sources: http://brainpedia.org/elon-musk-wants-merge-human-brain-ai-launches-neuralink/

Natural User Interface (NUI)

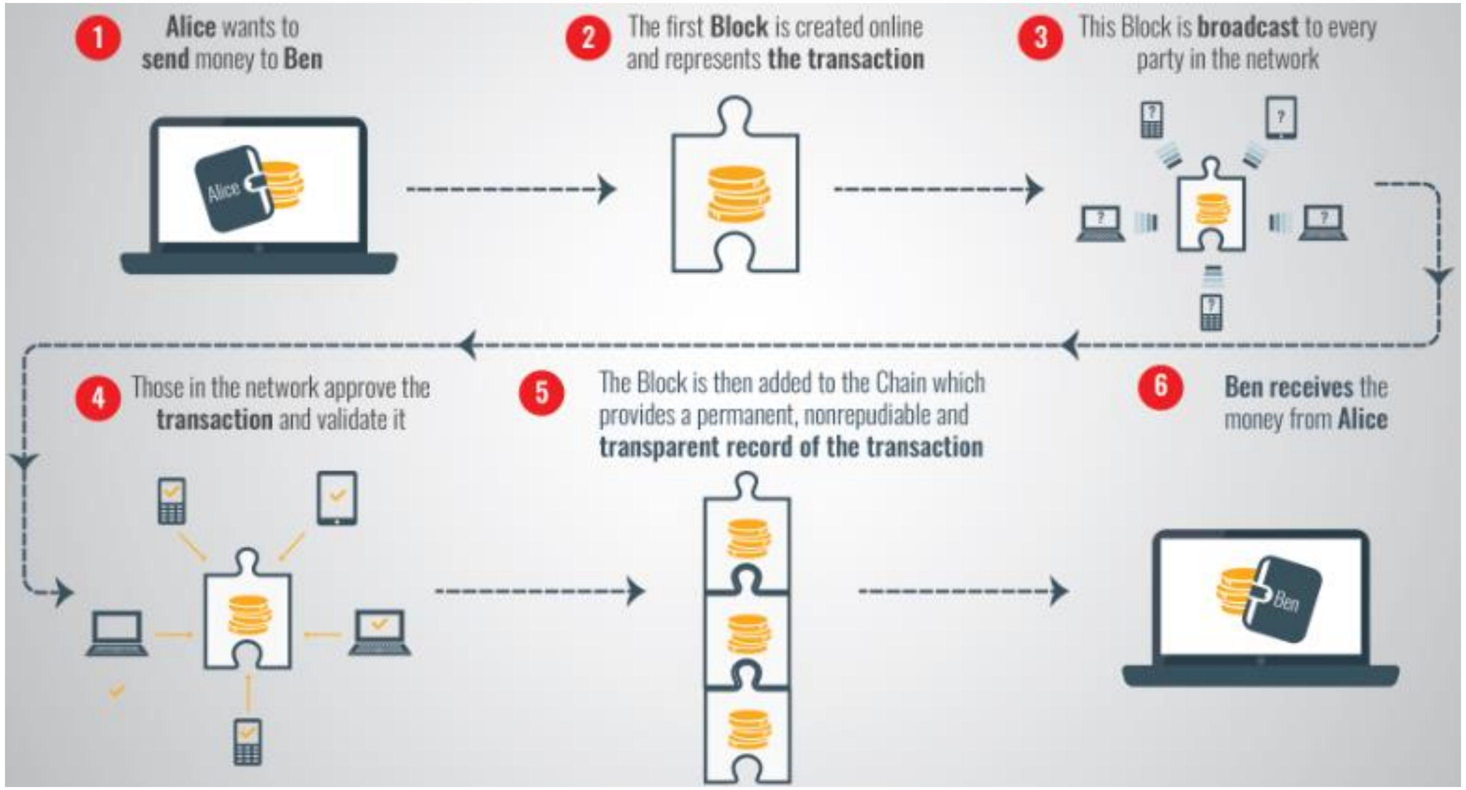


NUI : User interfaces where the interaction is direct and consistent with our “natural” behavior.

Microsoft Kinect

Source: https://www.interaction-design.org/literature/article/natural-user-interfaces-what-are-they-and-how-do-you-design-user-interfaces-that-feel-natural

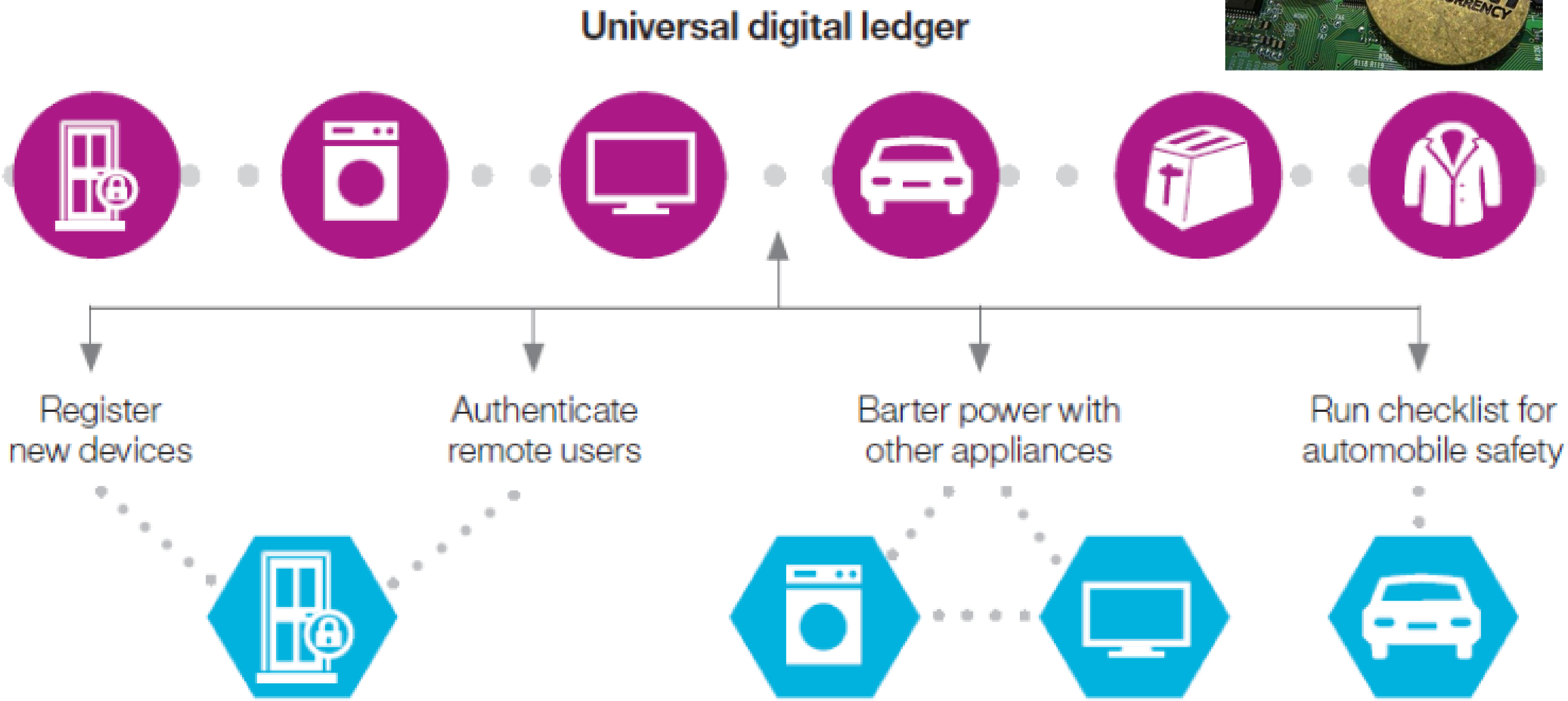
The Blockchain



"A Blockchain is a cloud based database shared by every participant in a given system, in the case of this exemplar, its currency trade. The Blockchain contains the complete transaction of the cryptocurrency or other record keeping in other applications. Think of it as cloud based peer to peer ledger."

Source: https://www.linkedin.com/pulse/securing-internet-things-iot-blockchain-ahmed-banafa

The Blockchain

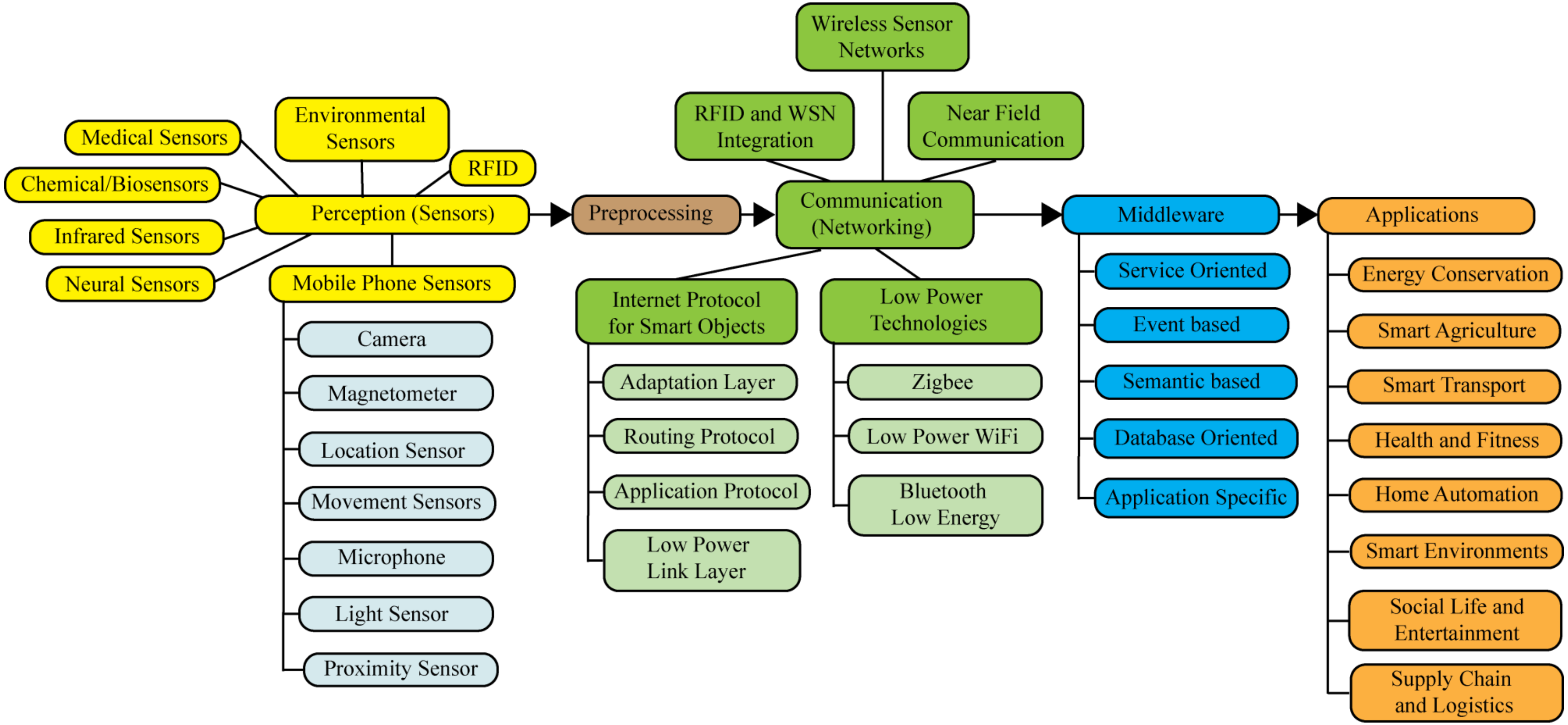


- Think of it as cloud based peer to peer ledger.
- A Blockchain is a cloud based database shared by every participant in a system.
- The Blockchain contains the complete transaction or other record keeping.

Source: https://www.linkedin.com/pulse/securing-internet-things-iot-blockchain-ahmed-banafa
Stay Tuned to: Puthal, Mohanty 2018, CE Magazine March 2018

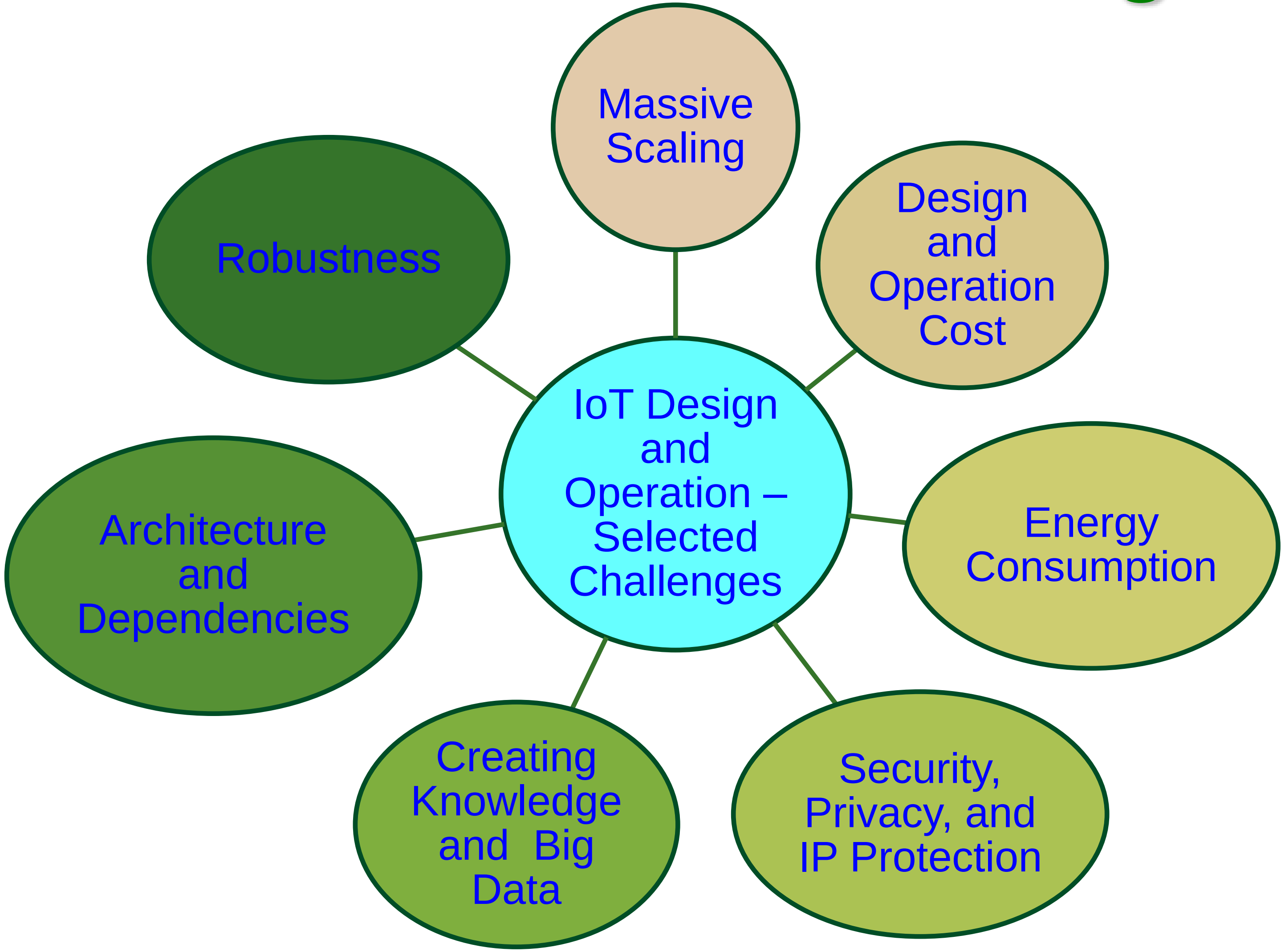
Challenges and Research

IoT – Multidiscipline Research



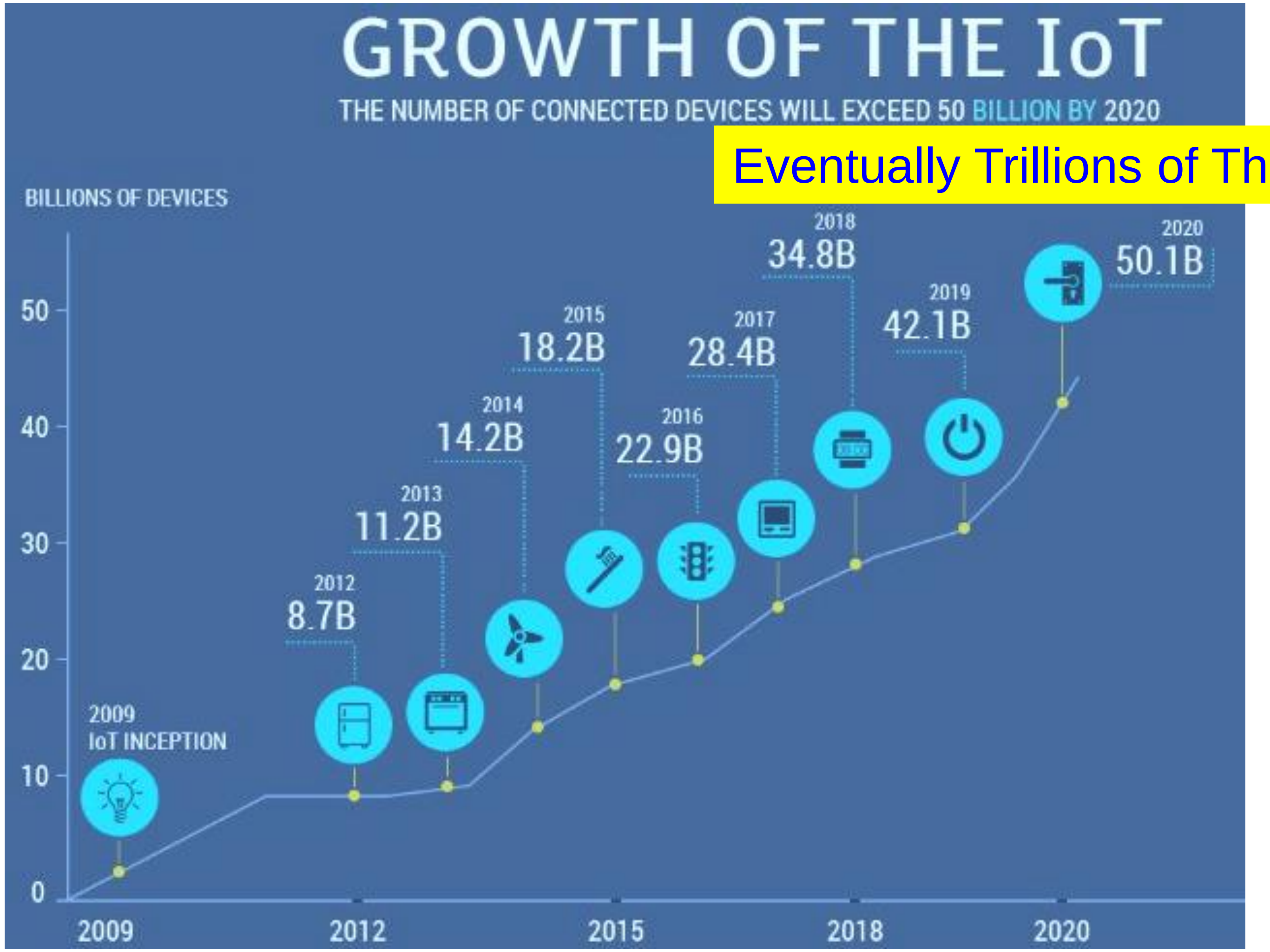
Source: Sethi 2017, JECE 2017

IoT – Selected Challenges



Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

Massive Scaling



Eventually Trillions of Things

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

High 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

Communication Latency and Energy Consumption

- Connected cars require latency of ms to communicate and avoid impending crash.
  - Faster connection
  - Low latency
  - Lower power
- 5G for connected world: This enables all devices to be connected seamlessly.
- How about 5G, WiFi working together more effectively?

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

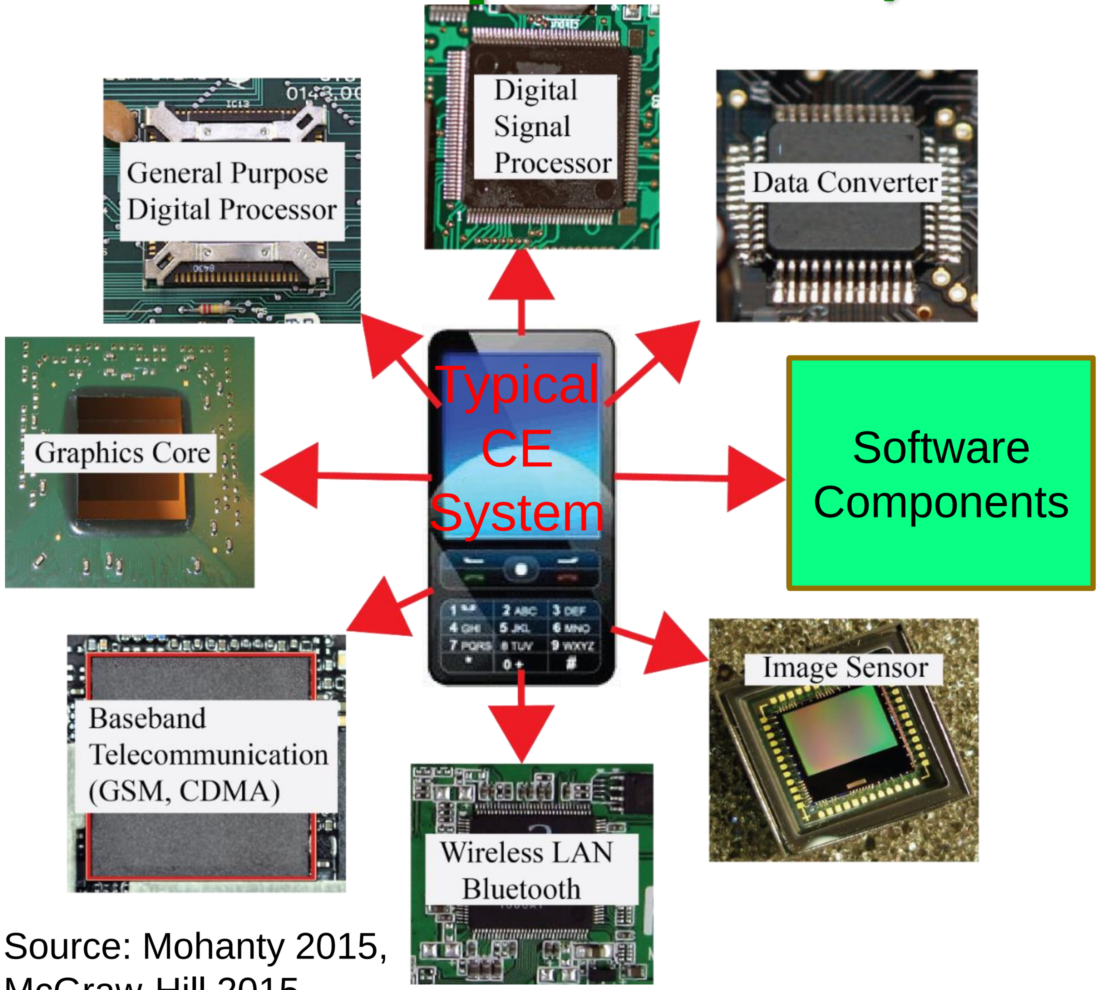
Impact of High Energy Consumption

Source: Mohanty 2015, McGraw-Hill 2015

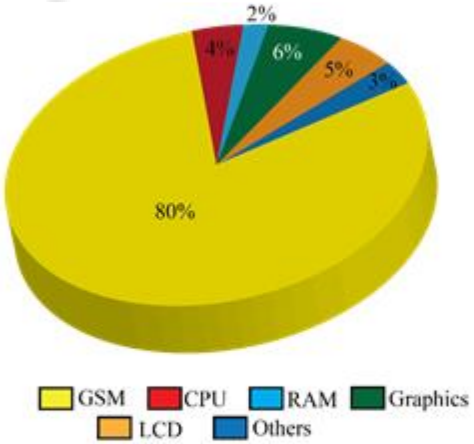
- Great idea: Smartwatch with functioning like smartphone.
- Big Problem: Battery life of one time charging is only 1 day.

Source: Mohanty 2013, CARE 2013 Keynote

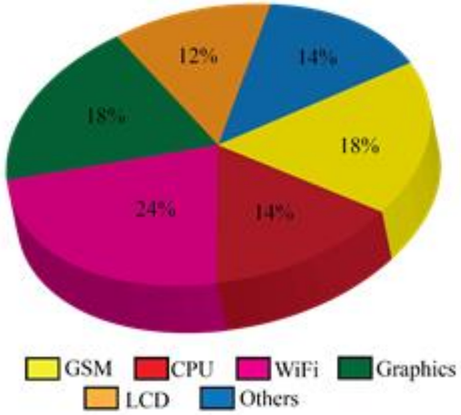
Energy Consumption of Sensors, Components, and Systems



Source: Mohanty 2015, McGraw-Hill 2015



During GSM Communications



During WiFi Communications

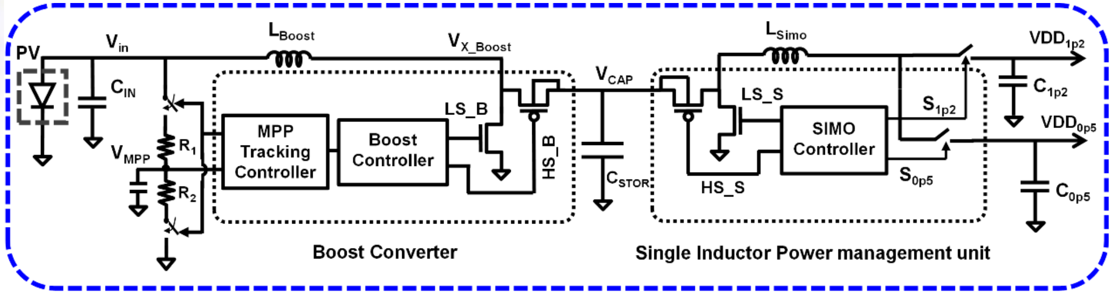
Battery-Less IoT

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

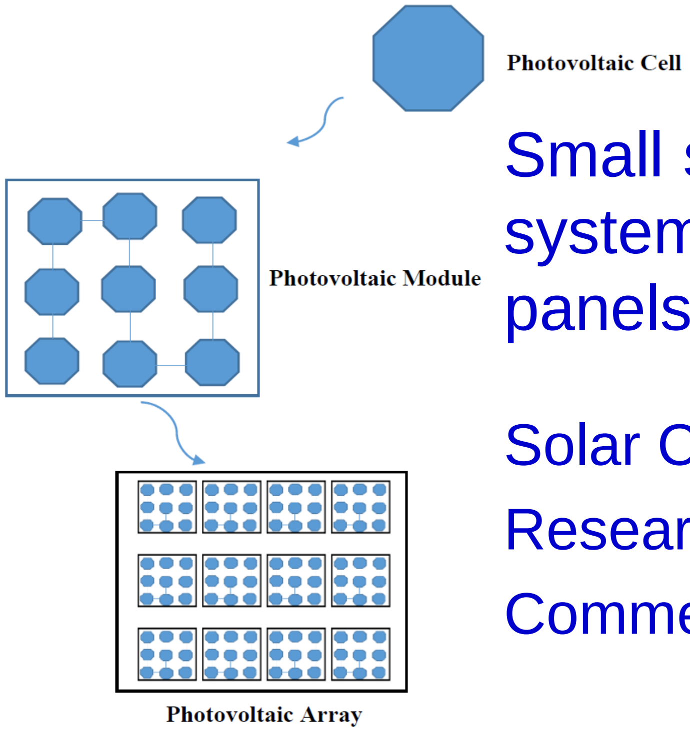
Source: https://www.technologyreview.com/s/529206/a-batteryless-sensor-chip-for-the-internet-of-things/



Energy Harvesting and Power Management

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

Energy Conversion Efficiency

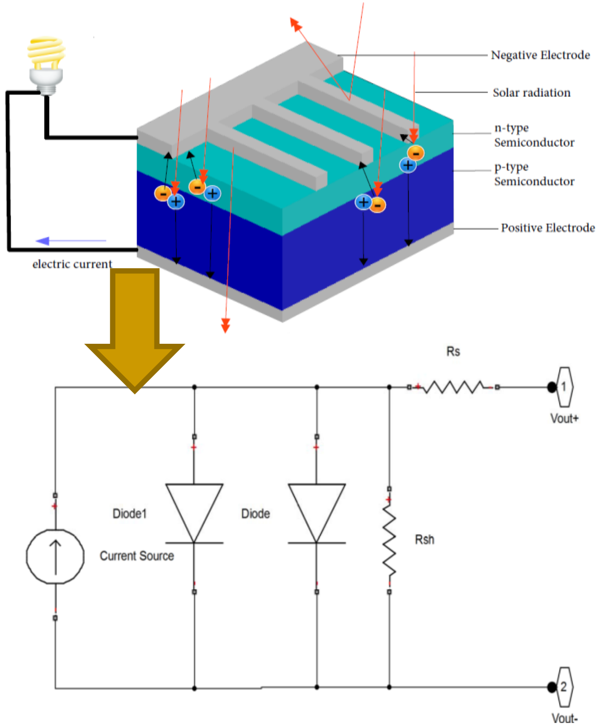


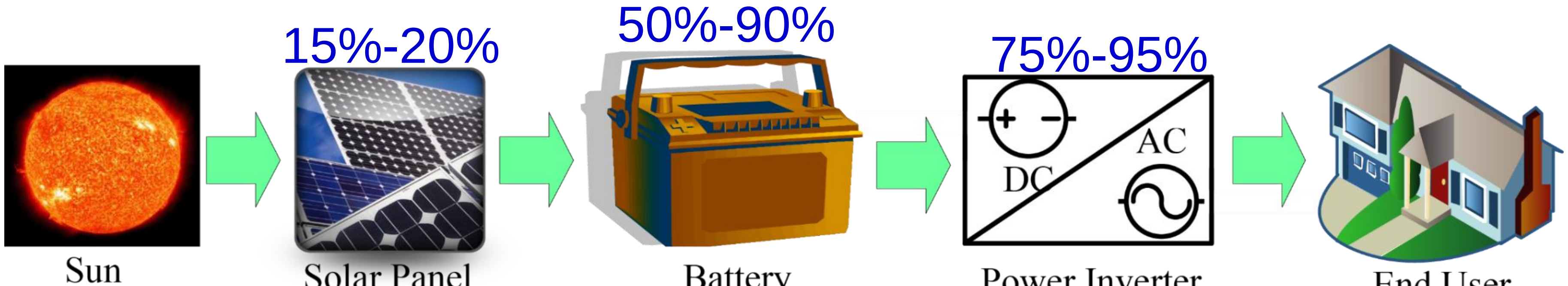
Small solar cells in CE systems to big solar panels in smart grids.

Solar Cell Efficiency:

Research stage: 46%

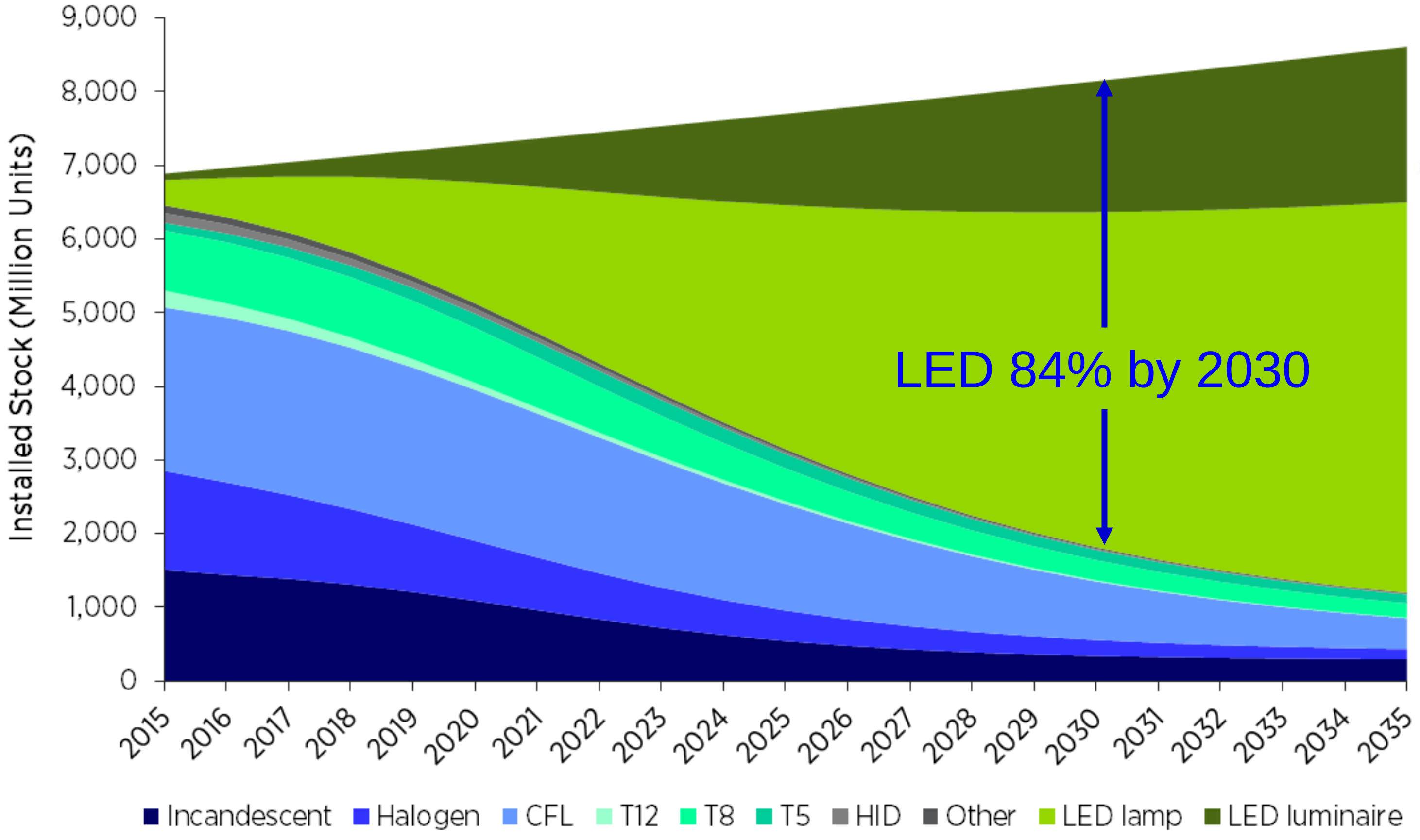
Commercial: 18%

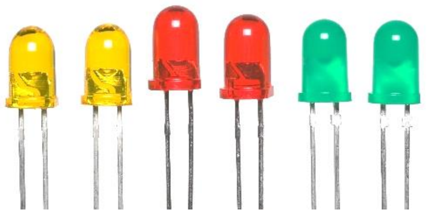




Source: Mohanty 2015, McGraw-Hill 2015

Energy Conversion Efficiency





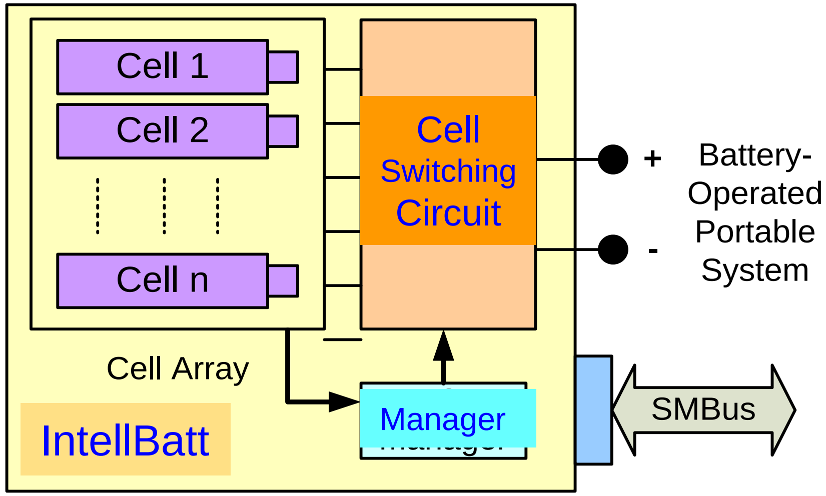
Conversion Efficiency: 4% - 53%

Source: https://energy.gov/sites/prod/files/2016/09/f33/energysavingsforecast16_2.pdf

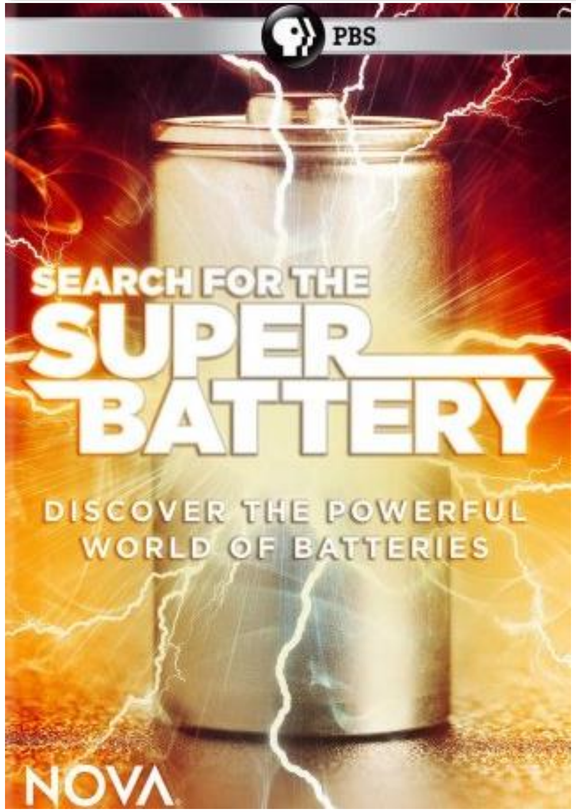
Energy Storage - High Capacity and Efficiency Needed

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

Intelligent Battery



Mohanty 2010: IEEE Computer, March 2010.
Mohanty 2018: ICCE 2018



Lithium Polymer Battery

Supercapacitor

Safety of Electronics

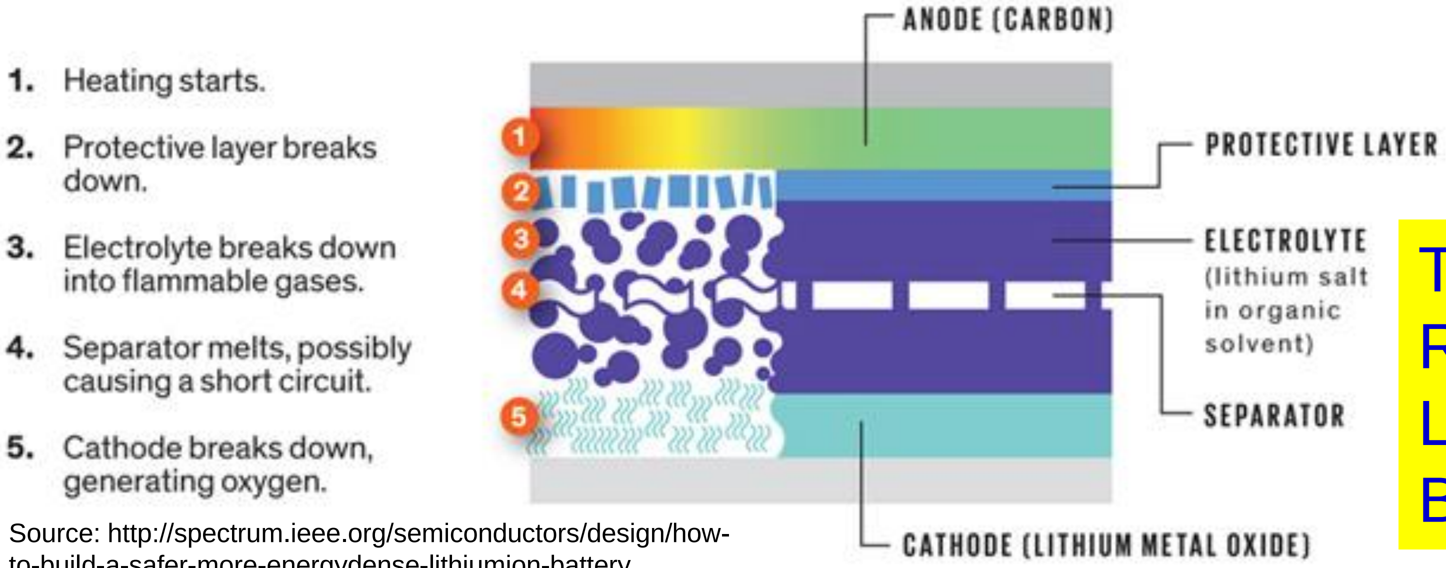
One 787 Battery: 12 Cells / 32 V DC

Source: http://www.newairplane.com

- Boeing 787's across the globe were grounded.

Safety of Electronics

Smartphone Battery



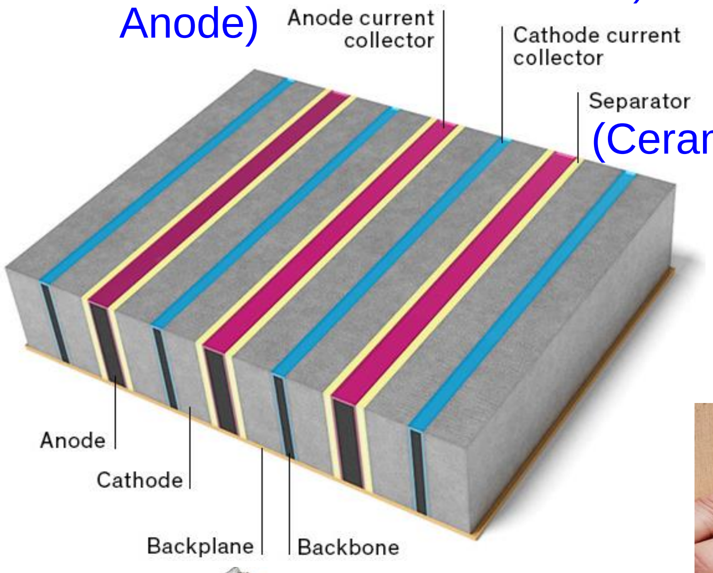
Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery

Thermal Runaway in a Lithium-Ion Battery

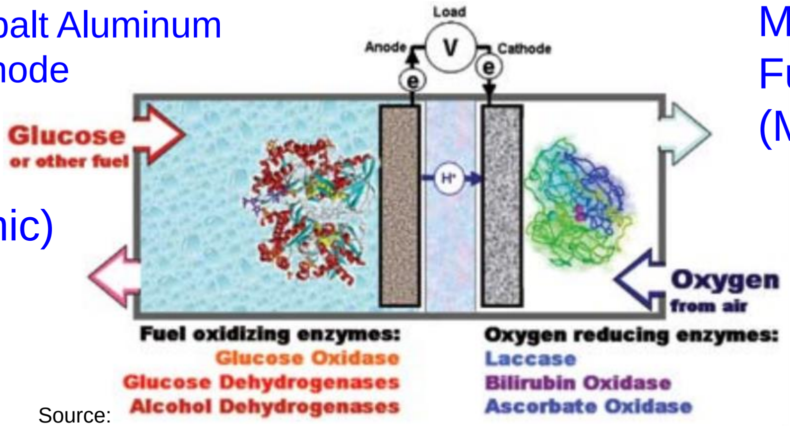
Energy Storage - High Capacity and Safer Needed

(Silicon Anode)

(Lithium Nickel Cobalt Aluminum Oxide - NCA) Cathode



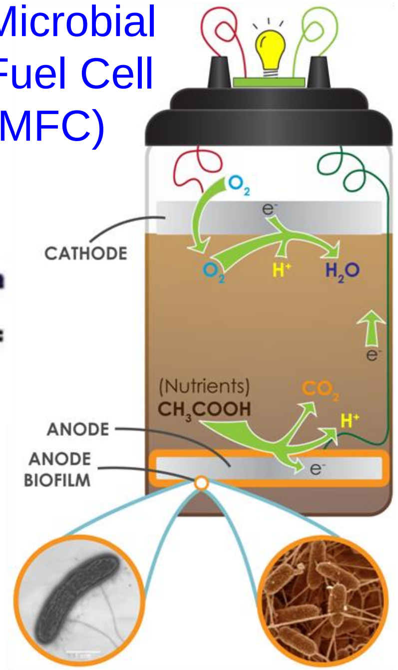
(Ceramic)



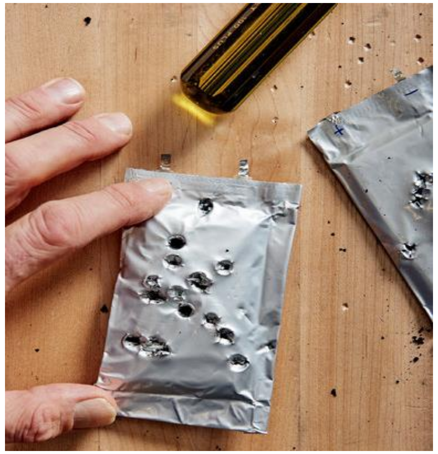
Source: https://www.electrochem.org/dl/interface/sum/sum07/su07_p28_31.pdf

Enzymatic Biofuel Cell

Microbial Fuel Cell (MFC)



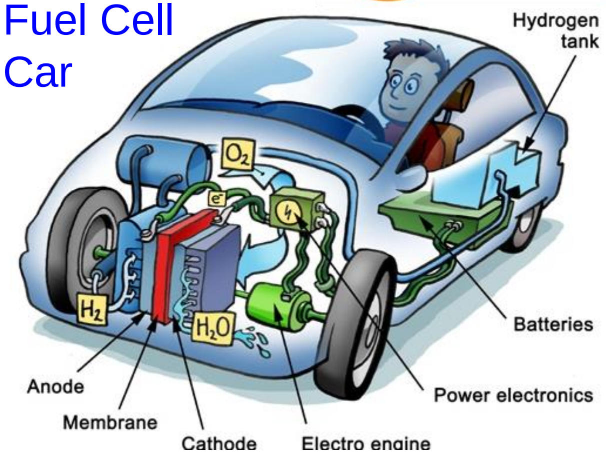
Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery



Solid Polymer Lithium Metal Battery

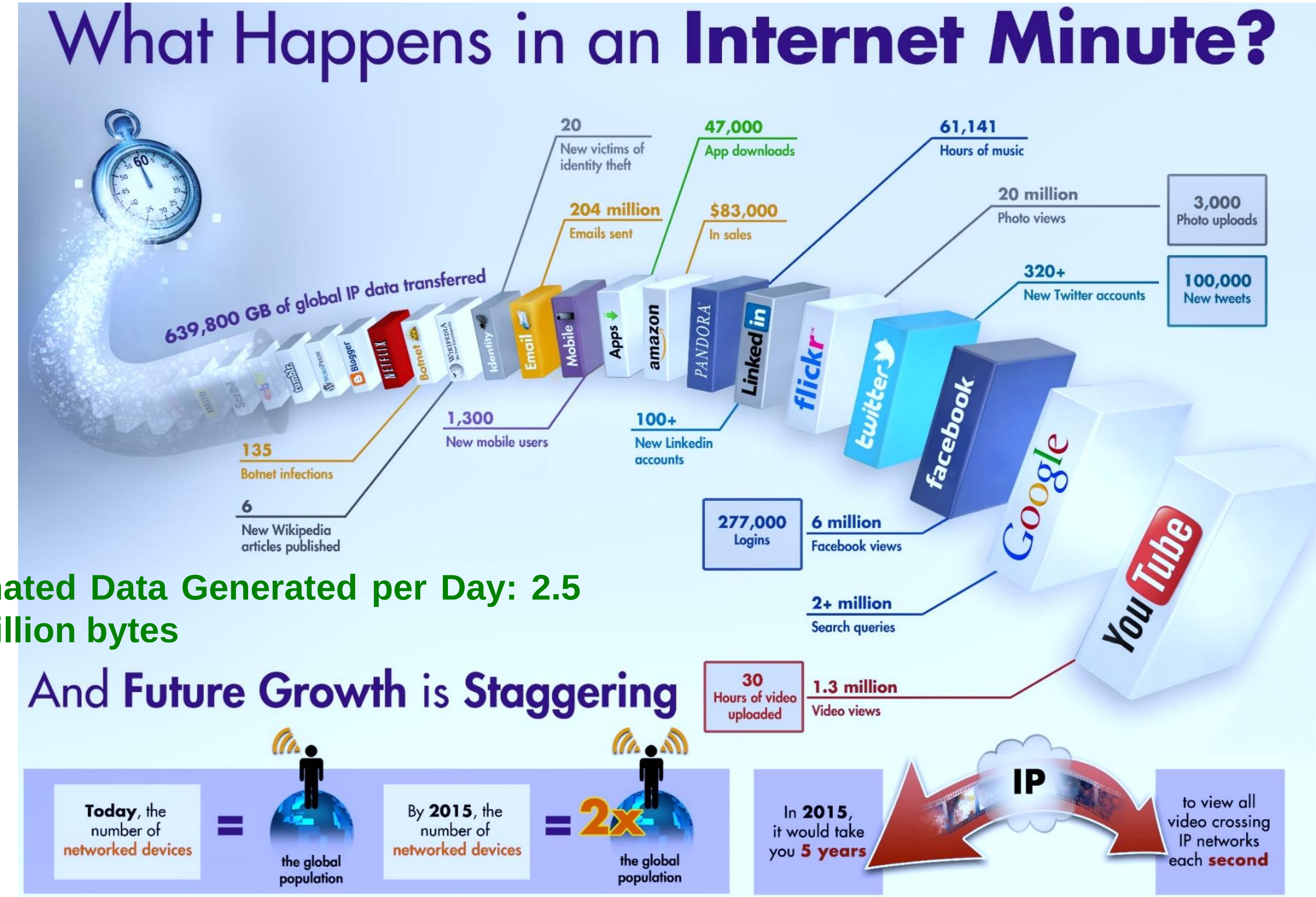
Source: https://www.nytimes.com/2016/12/11/technology/designing-a-safer-battery-for-smartphones-that-wont-catch-fire.html

Fuel Cell Car



Smart Electronic Systems Laboratory (SESL)
UNT EST. 1890

Huge Amount of Data

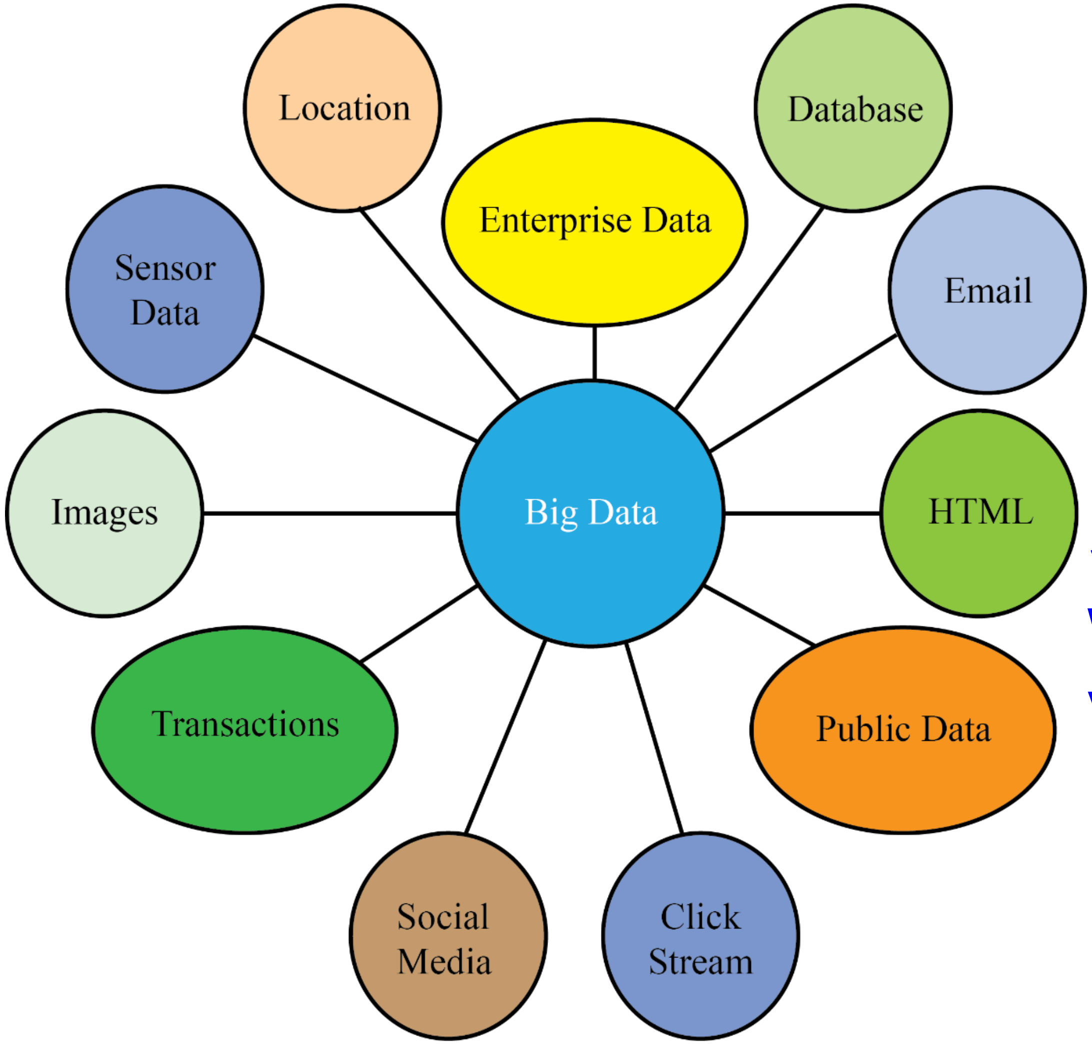


Estimated Data Generated per Day: 2.5 quintillion bytes

Data is Most Valuable

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

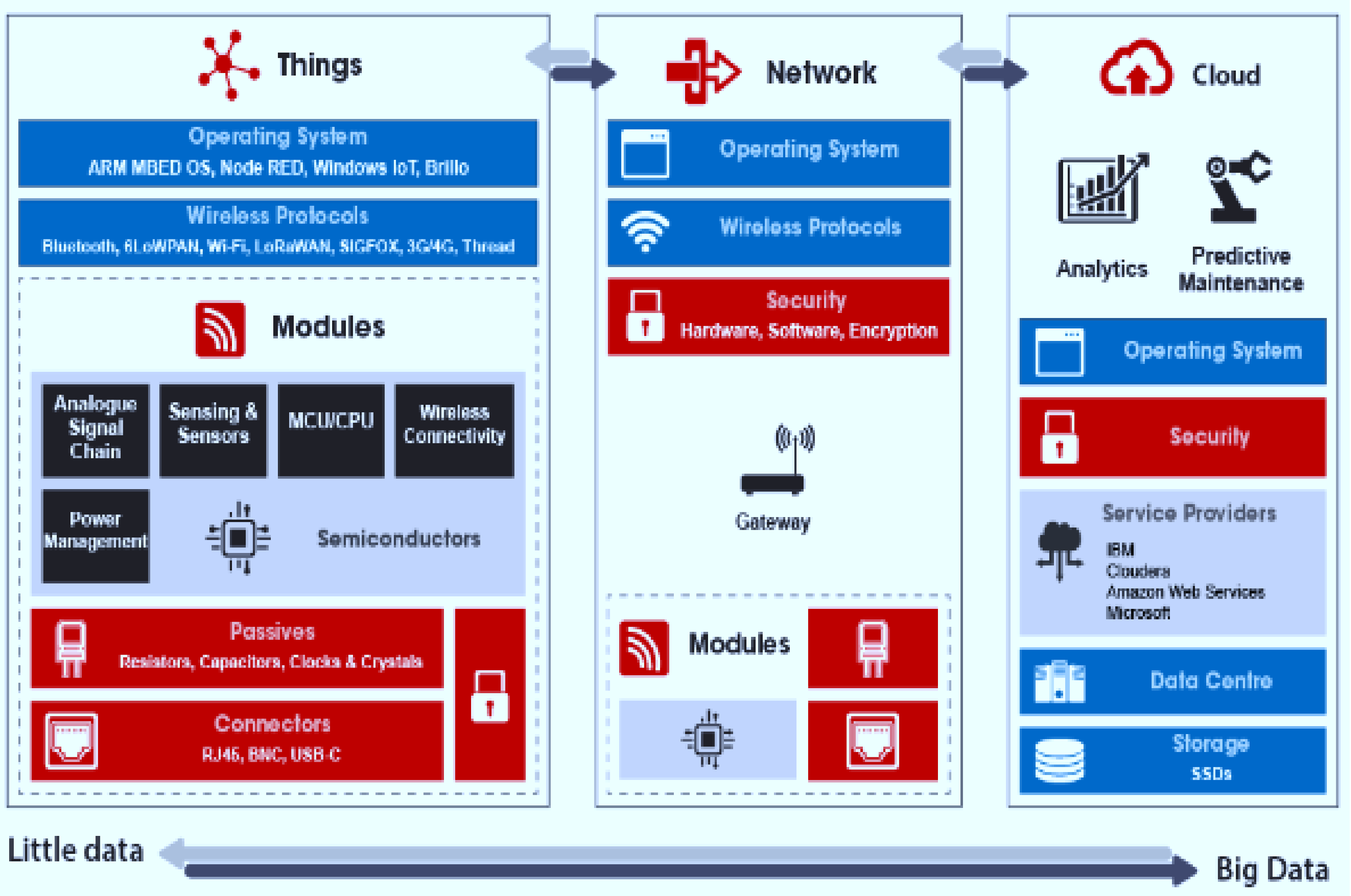
Bigdata in IoT and Smart Cities



Source: Mohanty 2016, CE Magazine July 2016

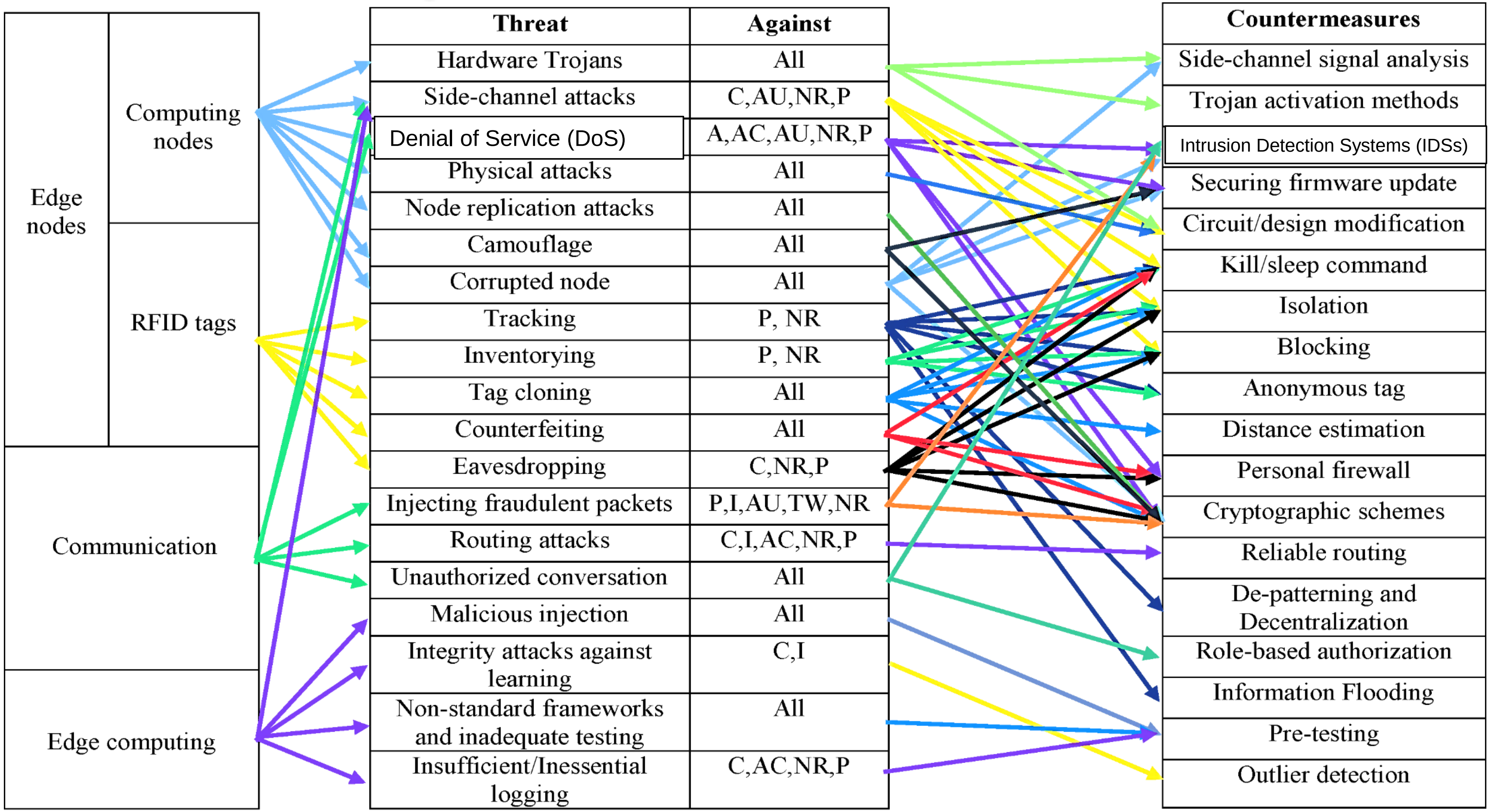
Sensors, social networks, web pages, image and video applications, and mobile devices generate more than 2.5 quintillion bytes data per day.

Bigdata in IoT and Smart Cities



Source: M. Elbeheiry, "Internet of Things (IoT) Architecture", Article, March 12, 2017.

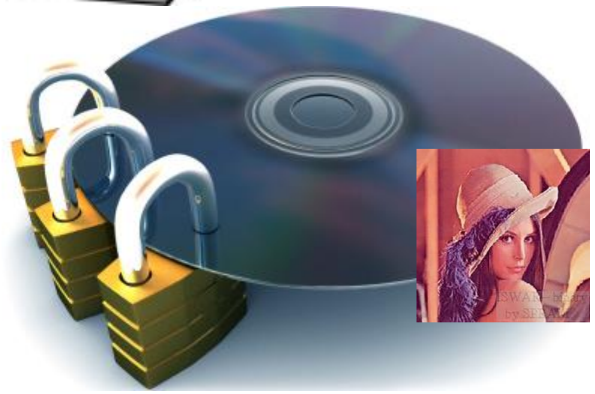
IoT Security - Attacks and Countermeasures



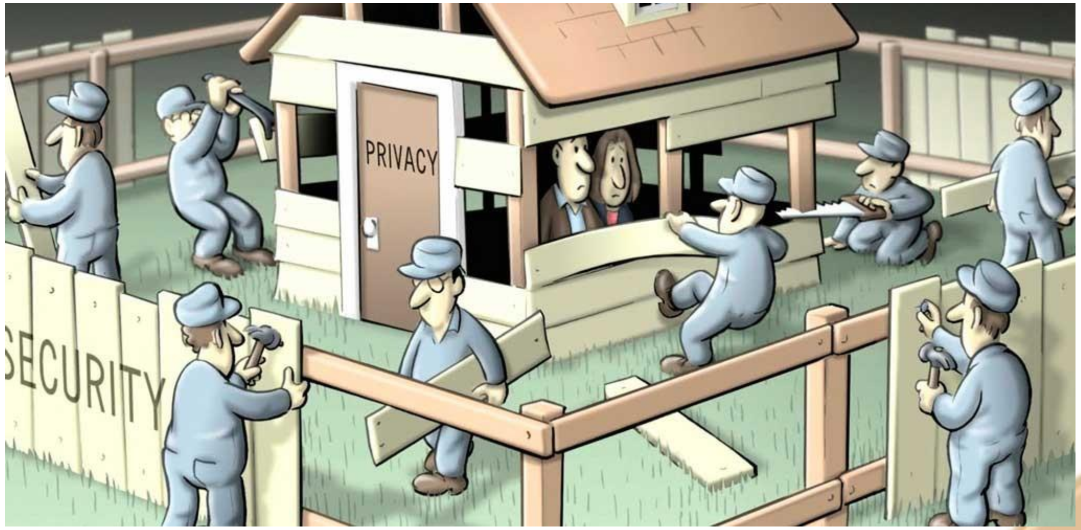
C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

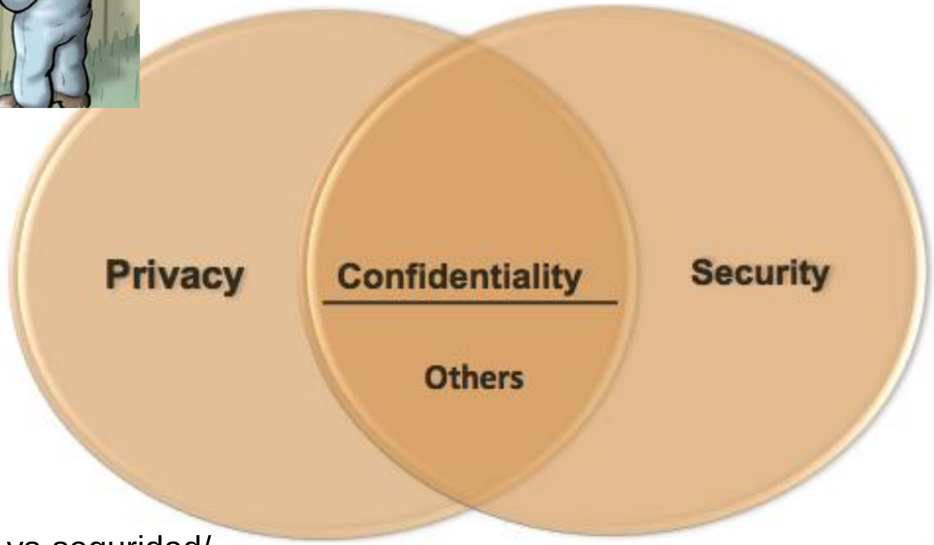
Source: Nia 2017,IEEE TETC 2017

Security, Privacy, and Copyright



Security, Privacy, IP Rights



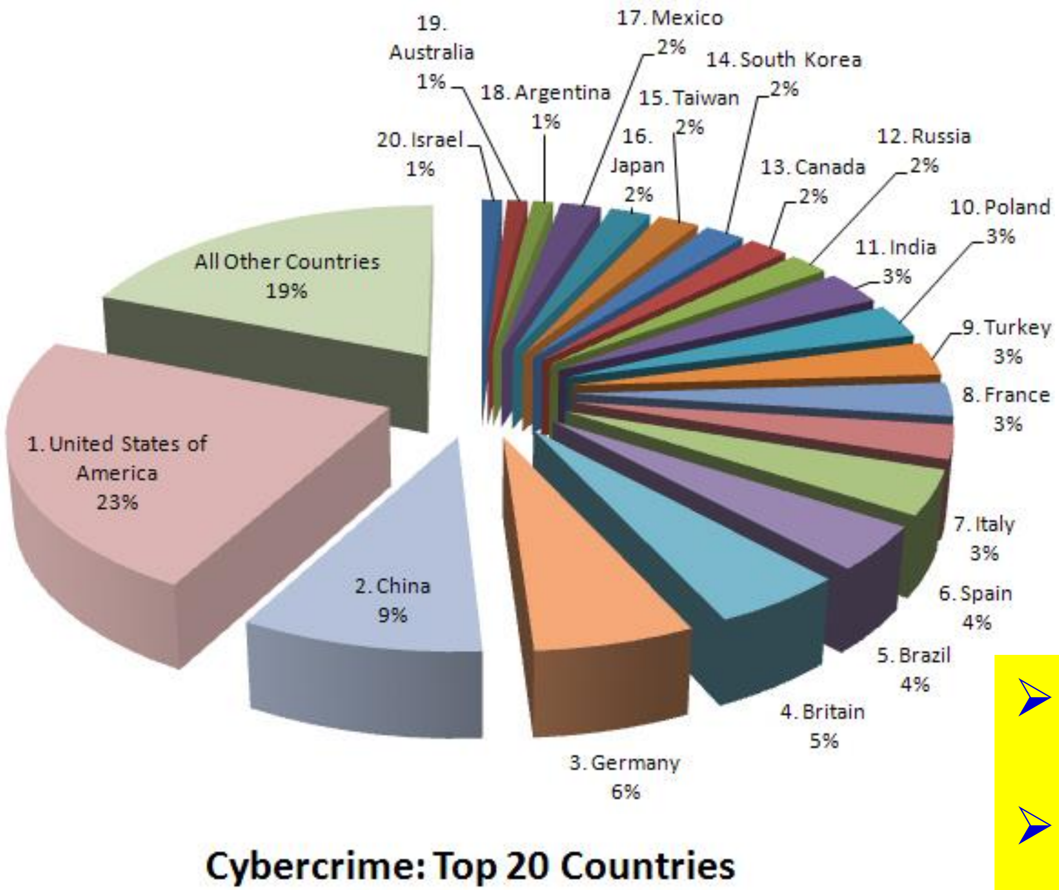


Source: https://blogs.deusto.es/master-informatica/privacidad-vs-seguridad/

Security – Different Aspects

- Security
  - Confidentiality
  - Integrity
  - Availability
  - Access Control
  - Authenticity
  - Nonrepudiation
  - Notarization

Security - Information, System



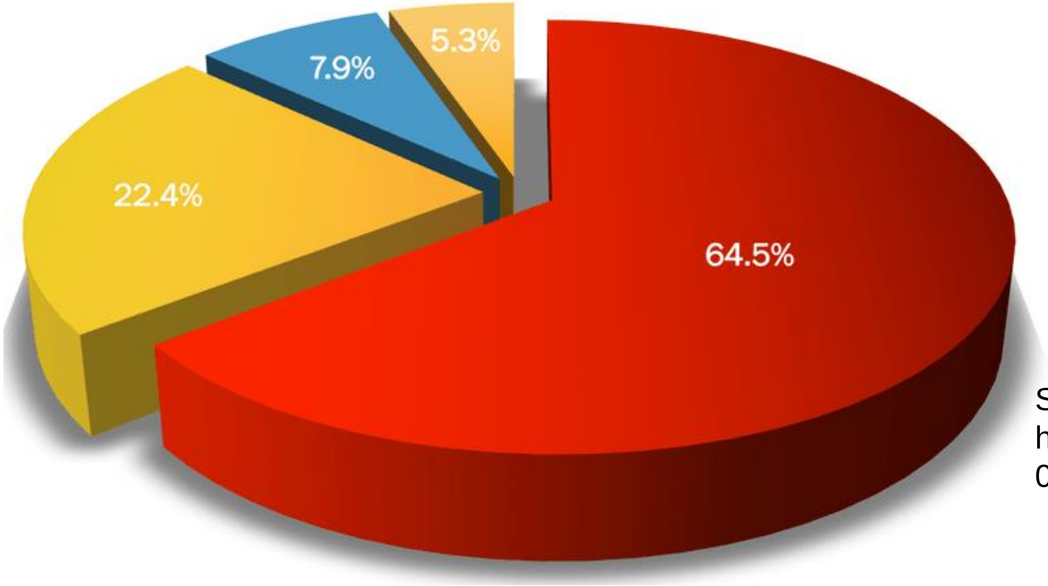
Cybercrime: Top 20 Countries

Source: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

- Cybercrime damage costs to hit $6 trillion annually by 2021
- Cybersecurity spending to exceed $1 trillion from 2017 to 2021

Source: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Security - Information, System



Source: http://www.hackmageddon.com/2017/03/20/february-2017-cyber-attacks-statistics/

- Cybercrime damage costs to hit $6 trillion annually by 2021
- Cybersecurity spending to exceed $1 trillion from 2017 to 2021

Source: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Security – Information …

Online Banking

Credit Card Theft


Hacked: Linkedin, Tumbler, & Myspace

Linked in
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

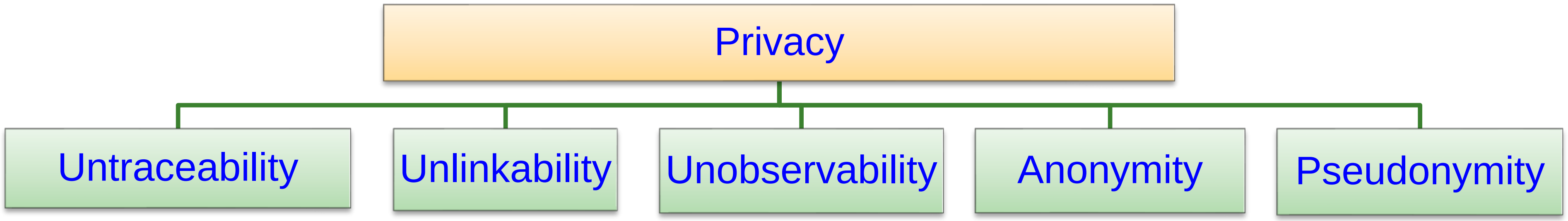
Credit Card/Unauthorized Shopping

Information Privacy

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

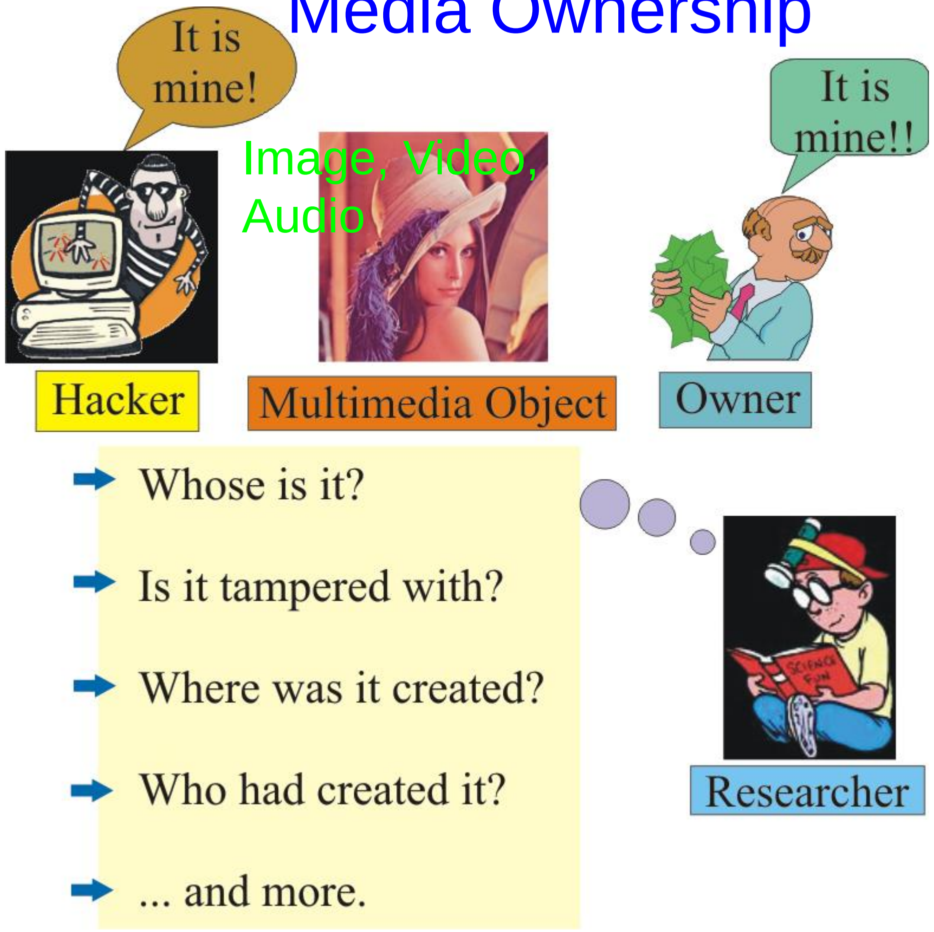
Source: http://blog.veriphyr.com/2012/06/electronic-medical-records-security-and.html

Privacy – Different Aspects



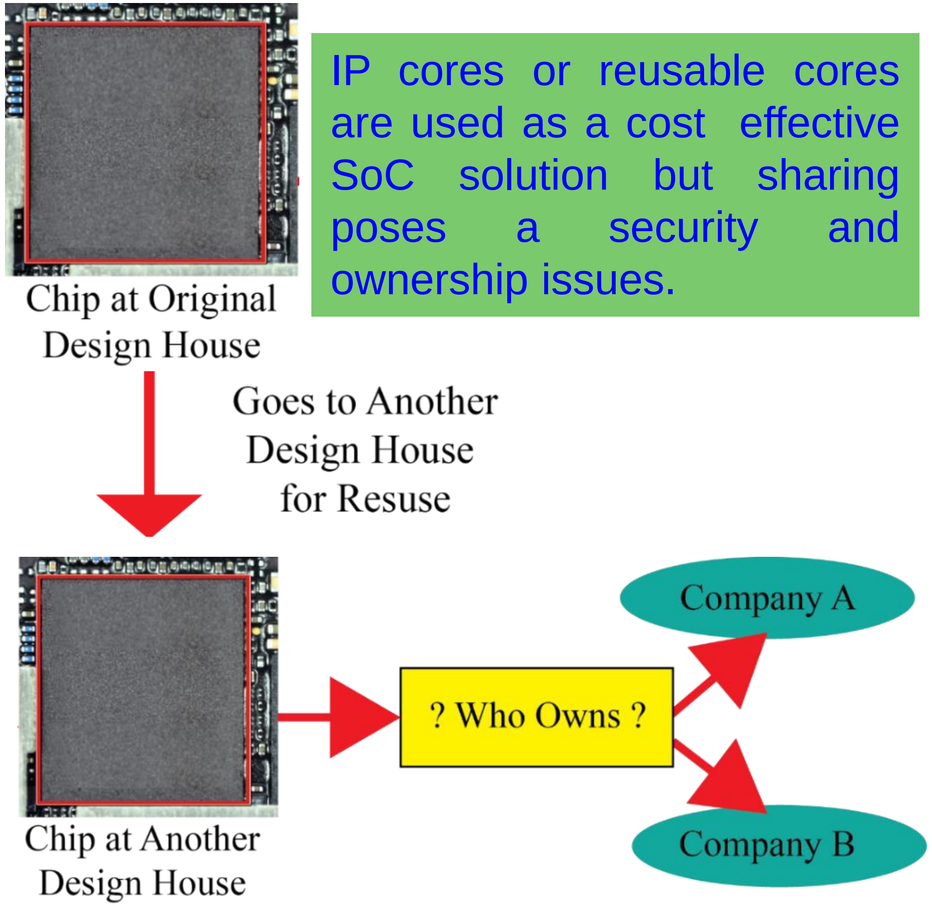
Copyright or Intellectual Property (IP) Protection

Media Ownership



Hardware Ownership

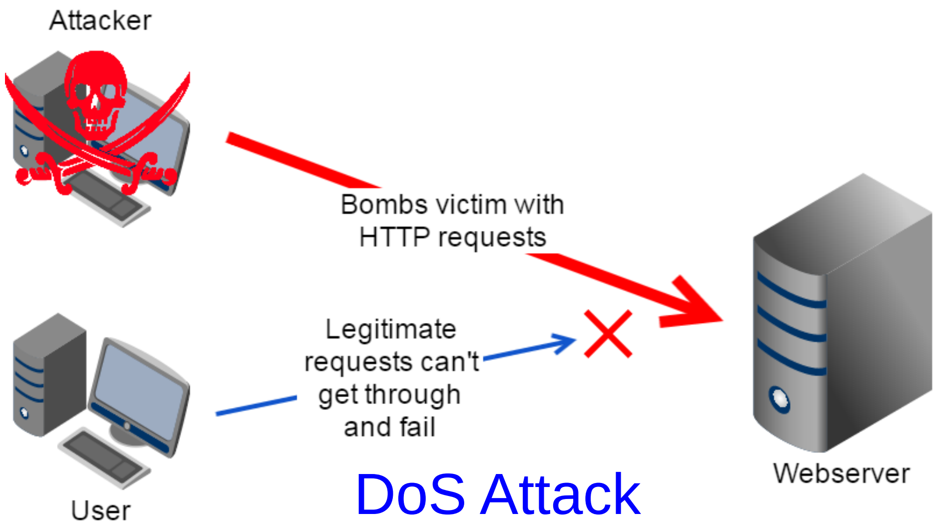
IP cores or reusable cores are used as a cost effective SoC solution but sharing poses a security and ownership issues.



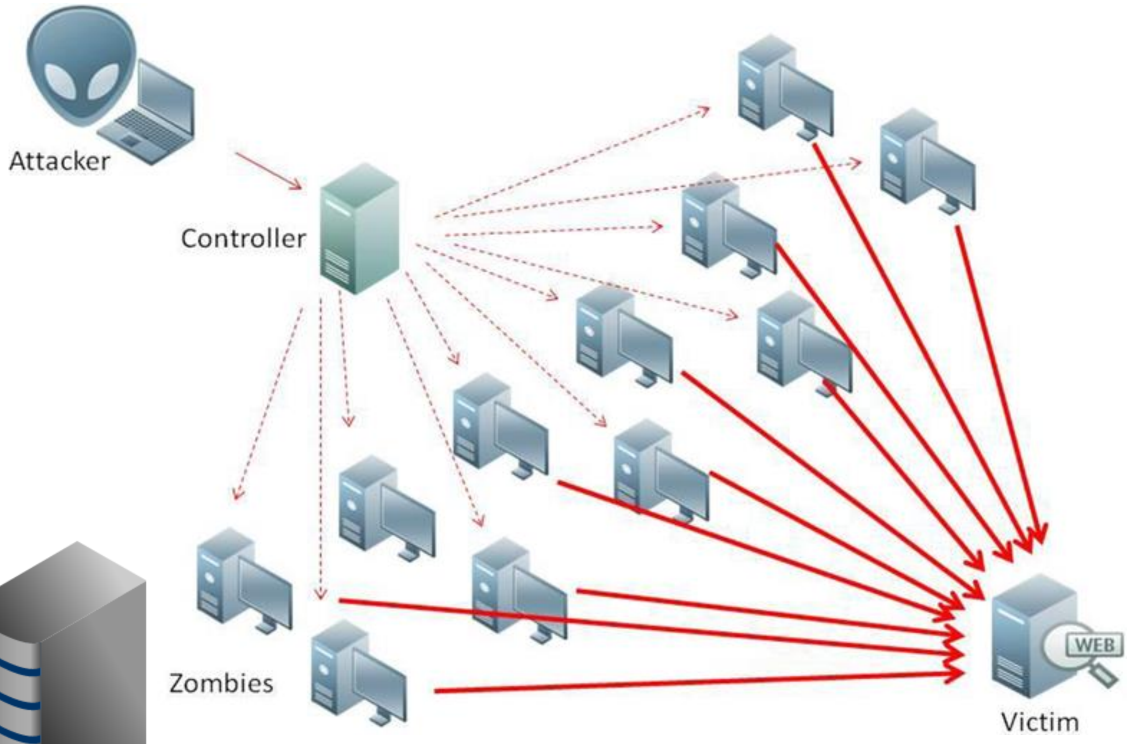
Source: Mohanty 2015, McGraw-Hill 2015

Security in Communications Technology

Denial-of-Service (DoS) Attacks



DoS Attack

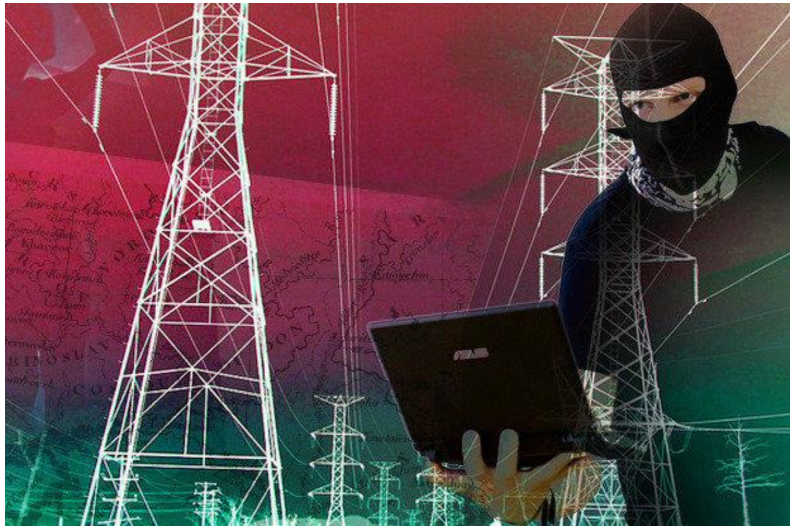


Distributed DoS (DDoS) Attack

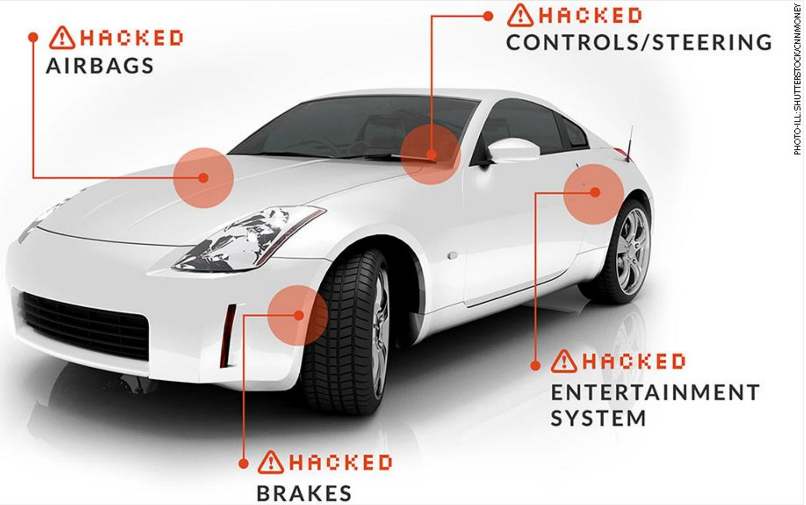
Source: https://bogner.sh/2015/05/analysing-a-denial-of-service-attack-tool/

Security - Systems …

Power Grid Attack



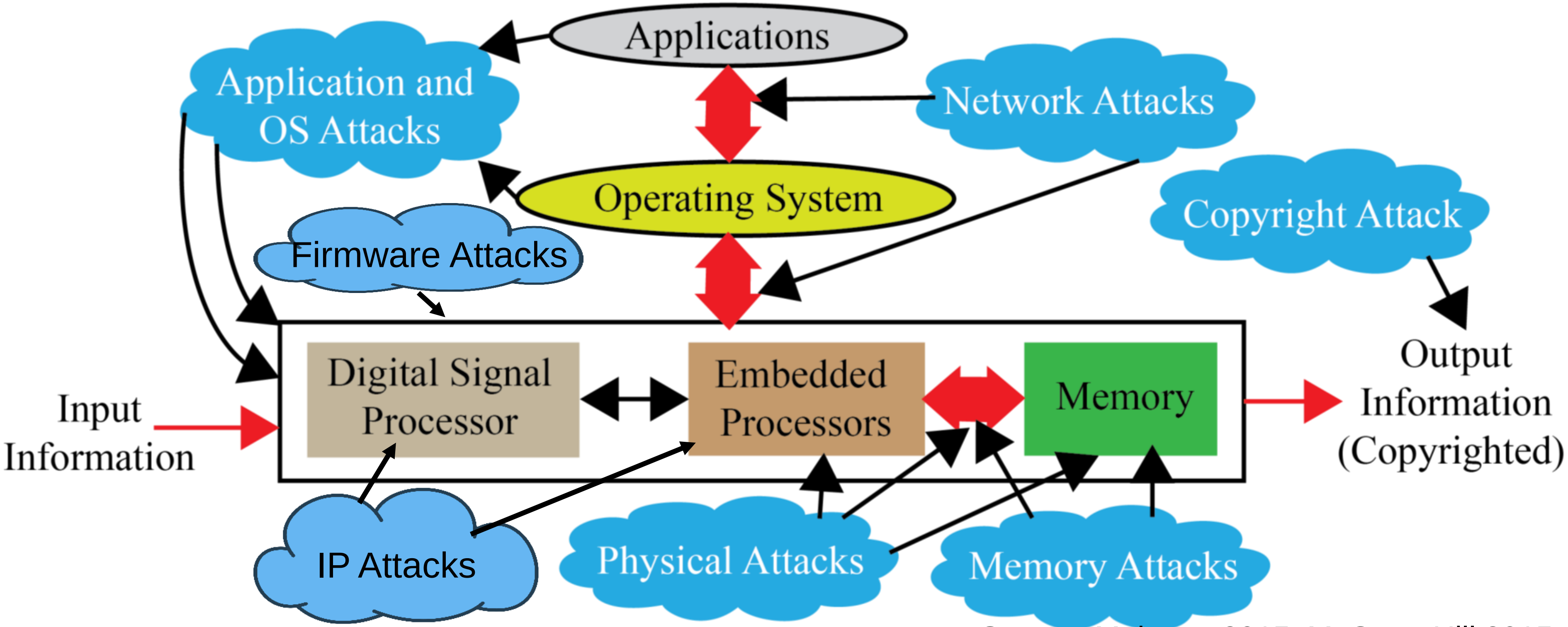
Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html



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

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

Selected Attacks on a Typical CE System – Security, Privacy, IP Right



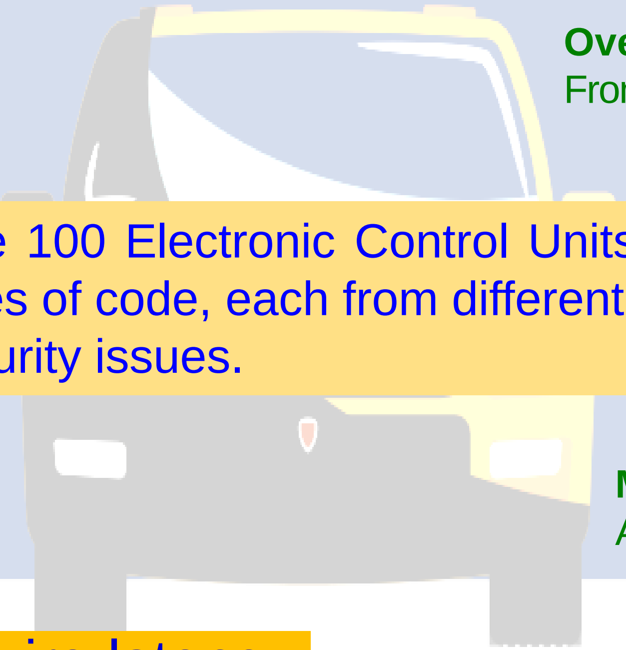
Source: Mohanty 2015, McGraw-Hill 2015

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

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)

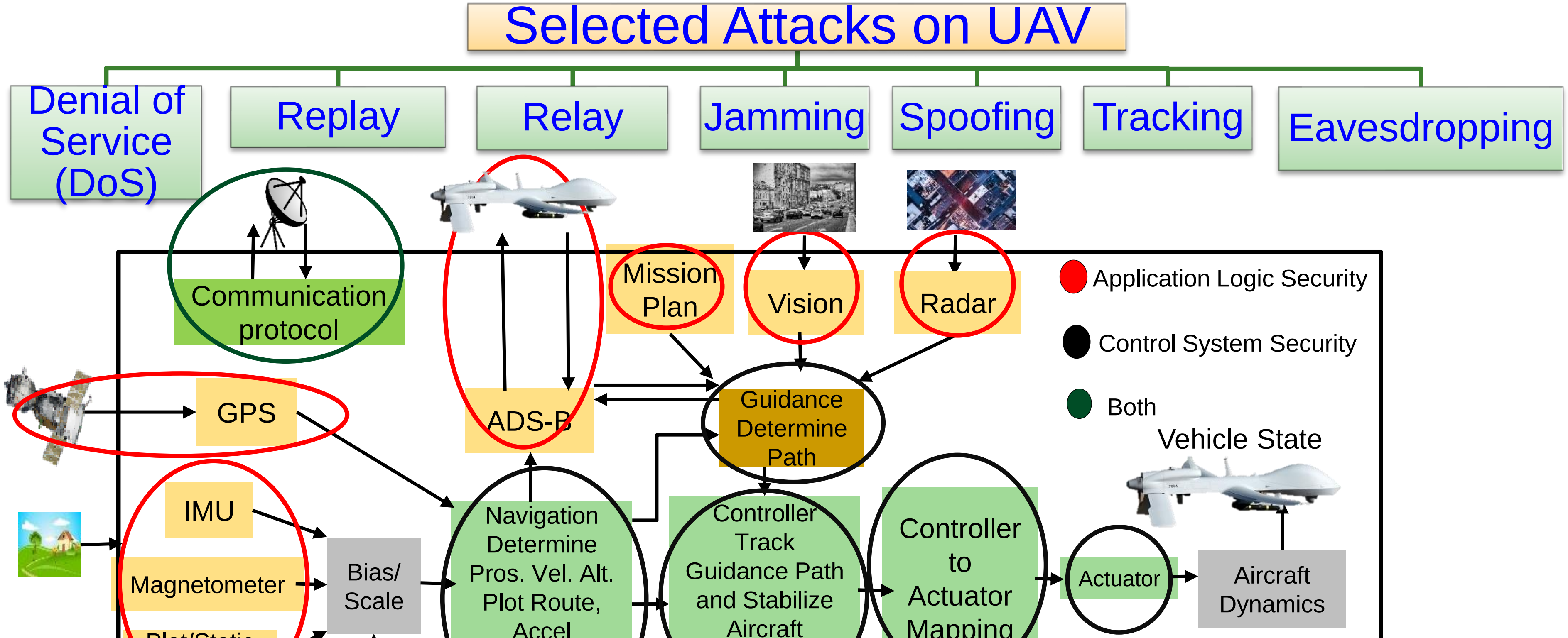
Mitigating Advanced Threats
Analytics in the Car and in the Cloud

- 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

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.

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 the 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.
  - It is projected that 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 CE system.

Hardware Assisted Security

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

  (1) information being processed,

  (2) hardware itself,

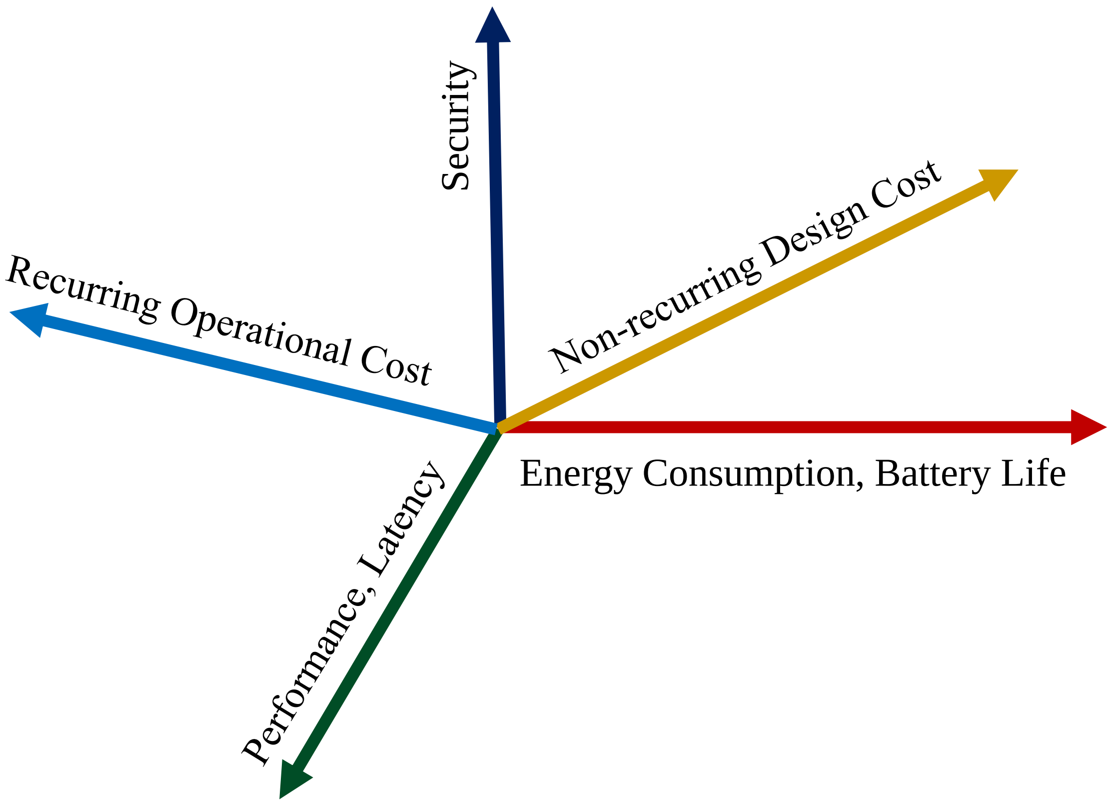
  (3) overall system
- Additional hardware components used for security.
- Hardware design modification is performed.
- System design modification is performed.

RF Hardware Security | Digital Hardware Security – Side Channel

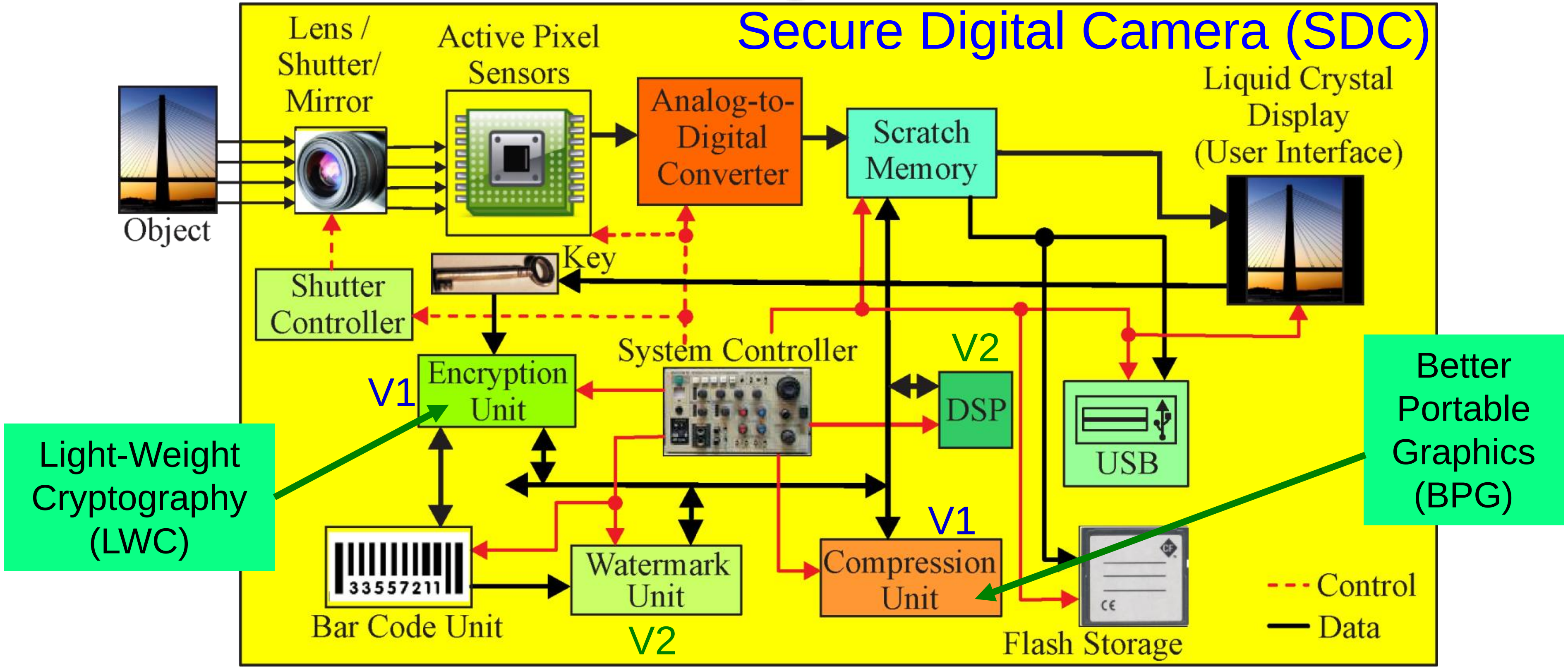
Hardware Trojan Protection | Information Security, Privacy, Protection

IR Hardware Security | Memory Protection | Digital Core IP Protection

CE System Design and Operation Tradeoffs



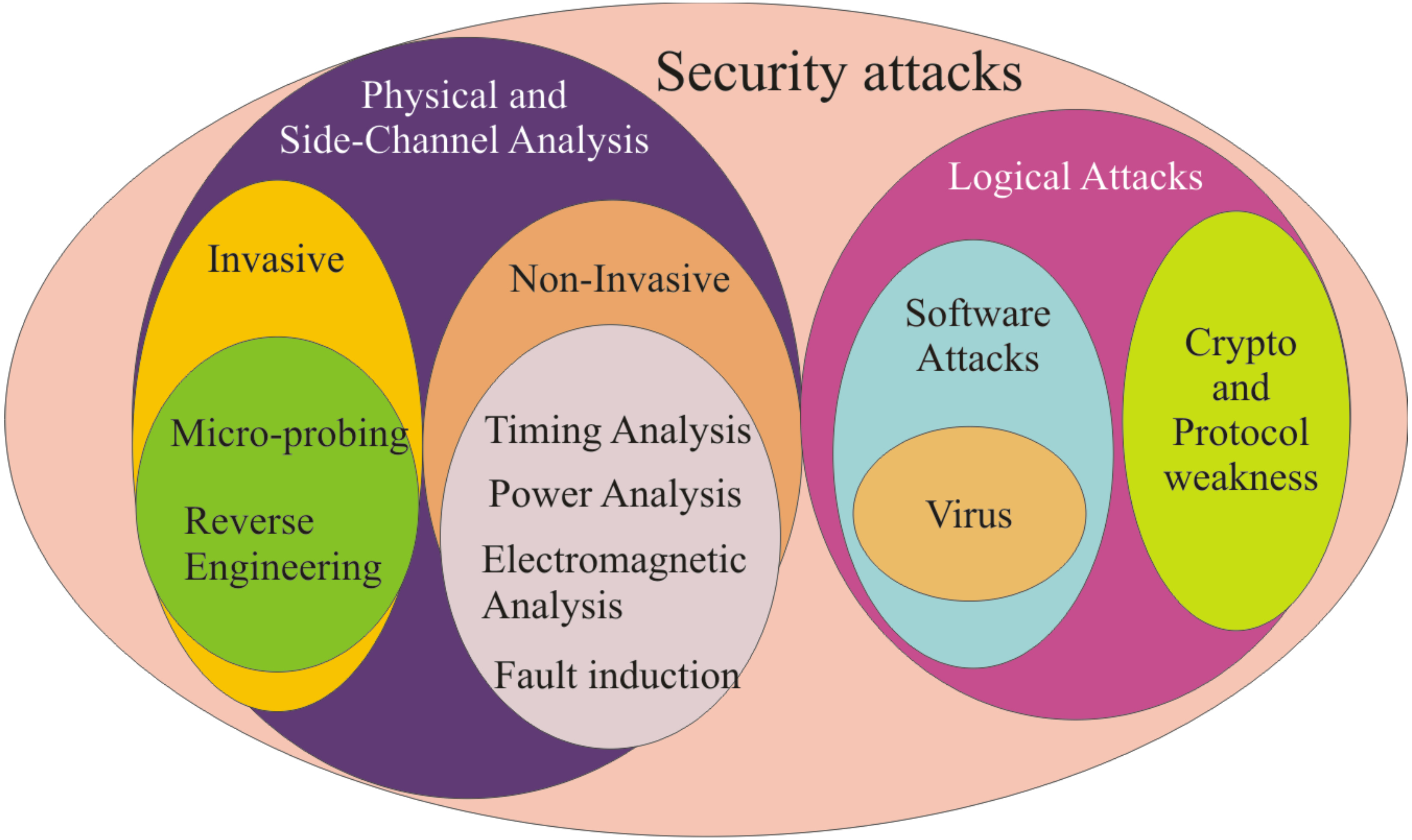
CE System Energy & Security Tradeoff – System Level



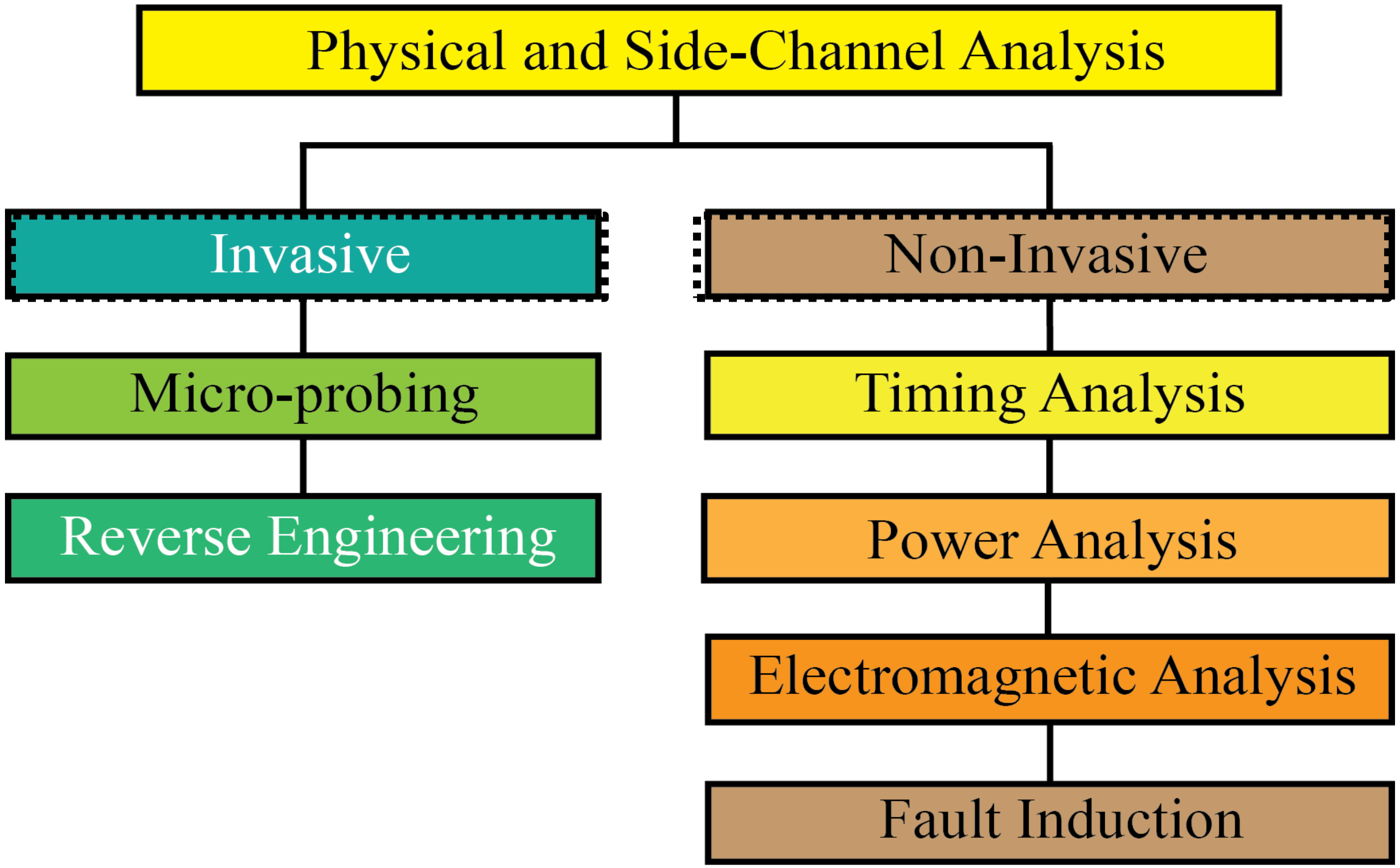
Include additional hardware components, but perform DVFS like technology for security, energy and performance optimization.

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

Different Attacks on a Typical CE System



Physical Attacks on Hardware



Source: Mohanty 2015, McGraw-Hill 2015

Physical Attacks on Hardware

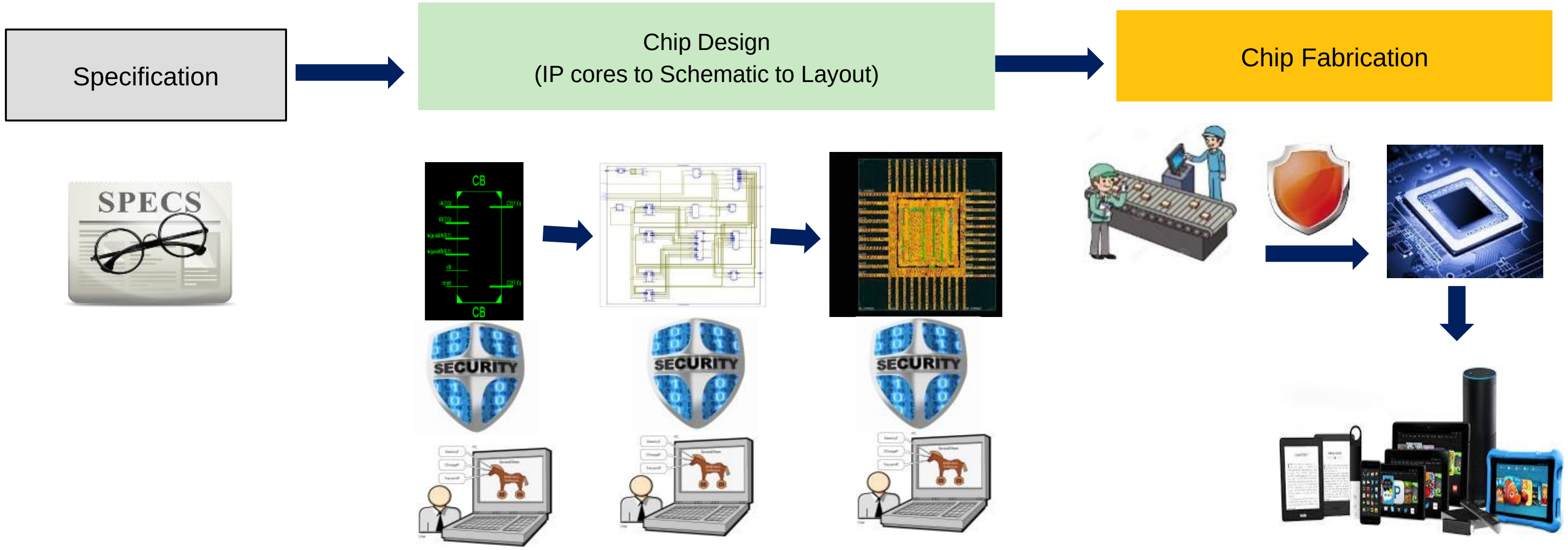


Fig.2a Chip design flow indicating possible hardware vulnerabilities in each step

Source: Sengupta 2017: CE Magazine July 2017

Physical Attacks on Hardware

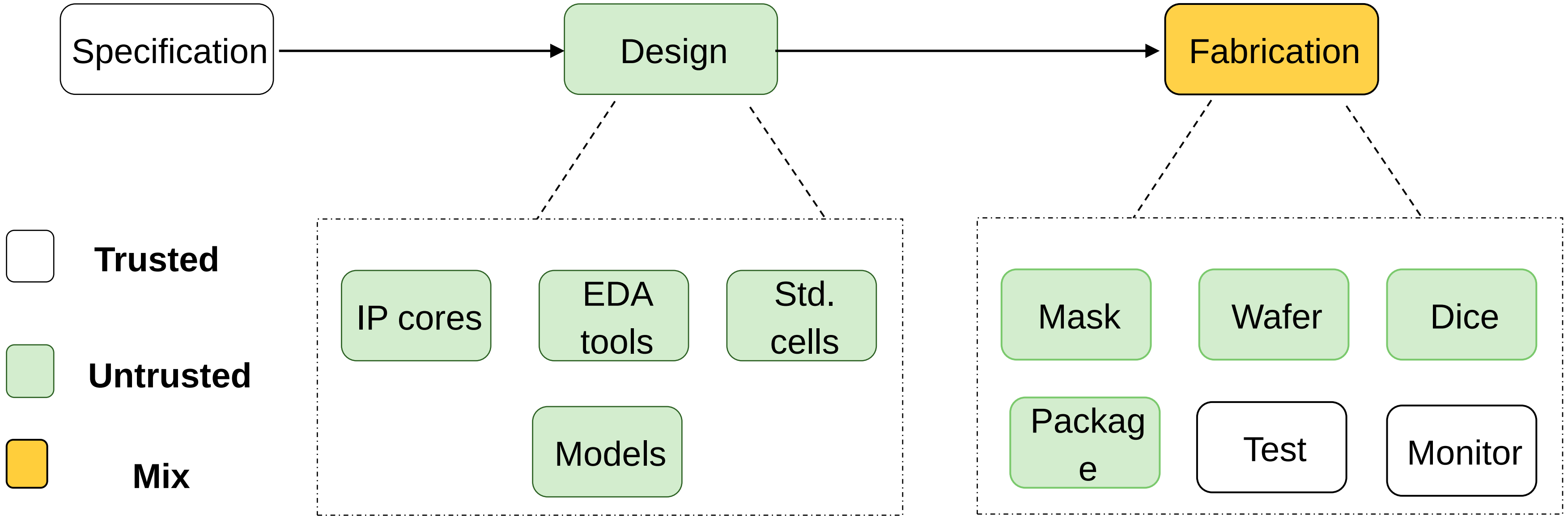


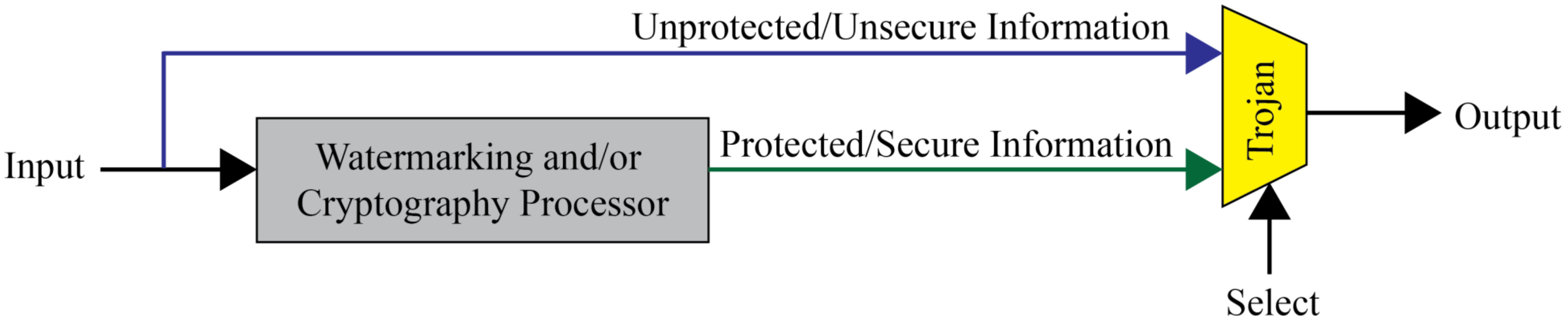
Fig.2b Life-cycle of a chip used in CE product indicating possibilities of hardware vulnerabilities

Source: Sengupta 2017: CE Magazine July 2017

Malicious Design Modifications Issue

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

Hardware Trojans



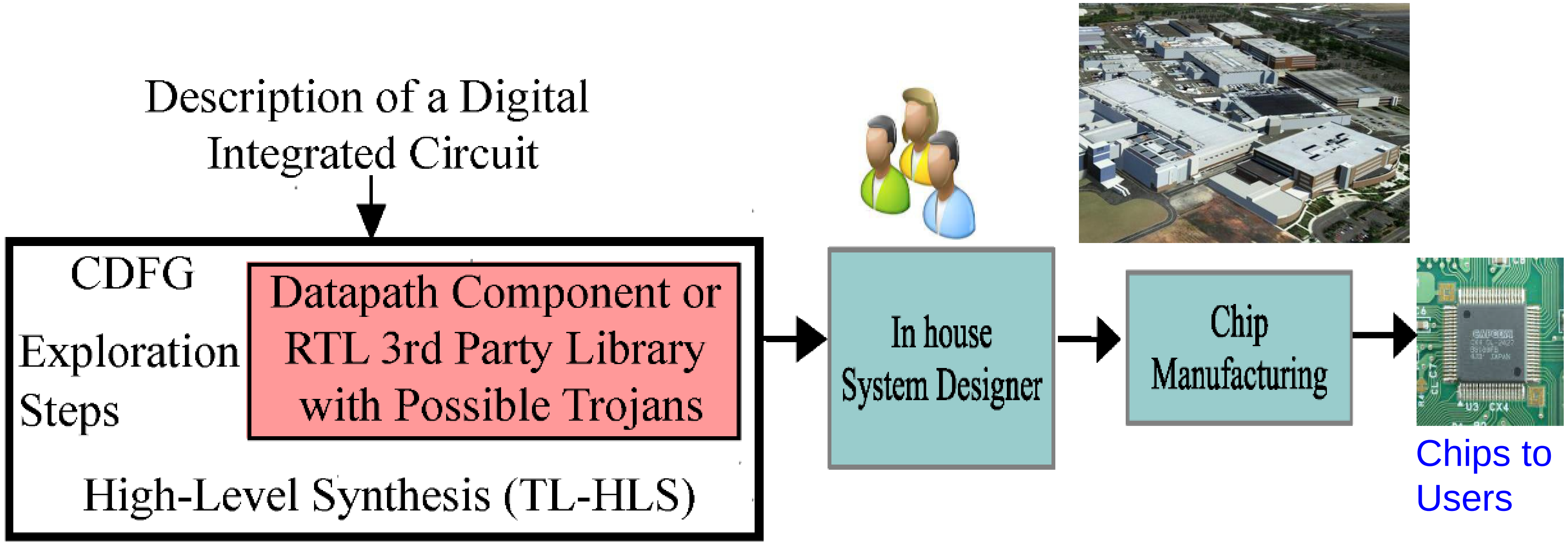
Source: Mohanty 2015, McGraw-Hill 2015

Provide backdoor to adversary.
Chip fails during critical needs.

Malicious Design Modifications Issue

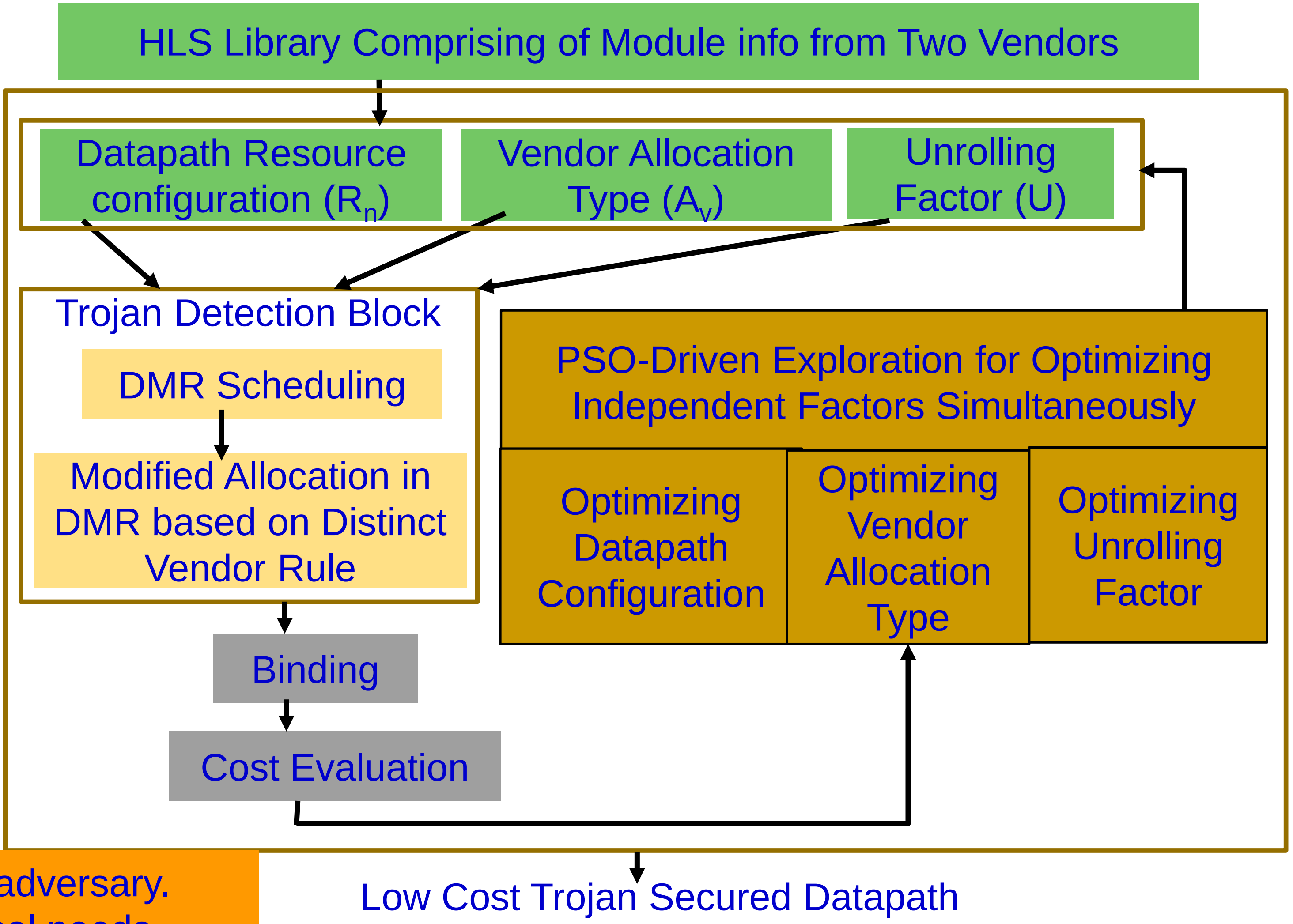
- Malicious modifications of designs becomes an issue when chips manufactured in unauthentic fabrication plants are used in critical applications, such as military and power grid.
- Such unauthentic plants might have deliberately introduced additional components in the chip so that the chip fails to work during critical needs.
- The term “Hardware Trojans” explains such additional components and when it is present in watermarking or cryptography chip, some or all of the steps in watermarking and encryption may be bypassed giving a non-watermarked or non-encrypted output.

Trojans Secure Digital Hardware Synthesis



Source: Sengupta and Mohanty 2017, TCAD April 2017

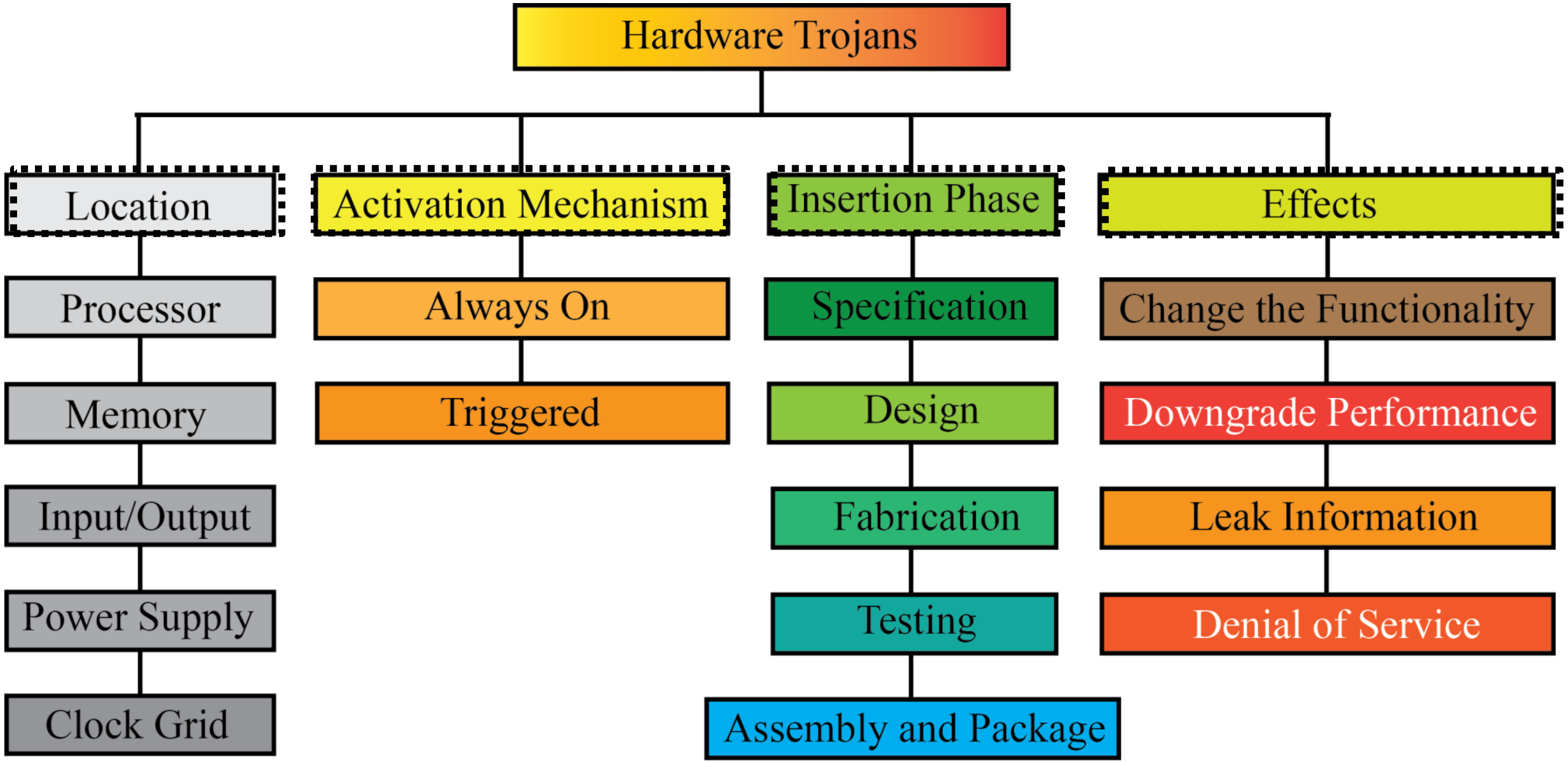
Trojan Secure Digital Hardware Synthesis



Provide backdoor to adversary.
Chip fails during critical needs.

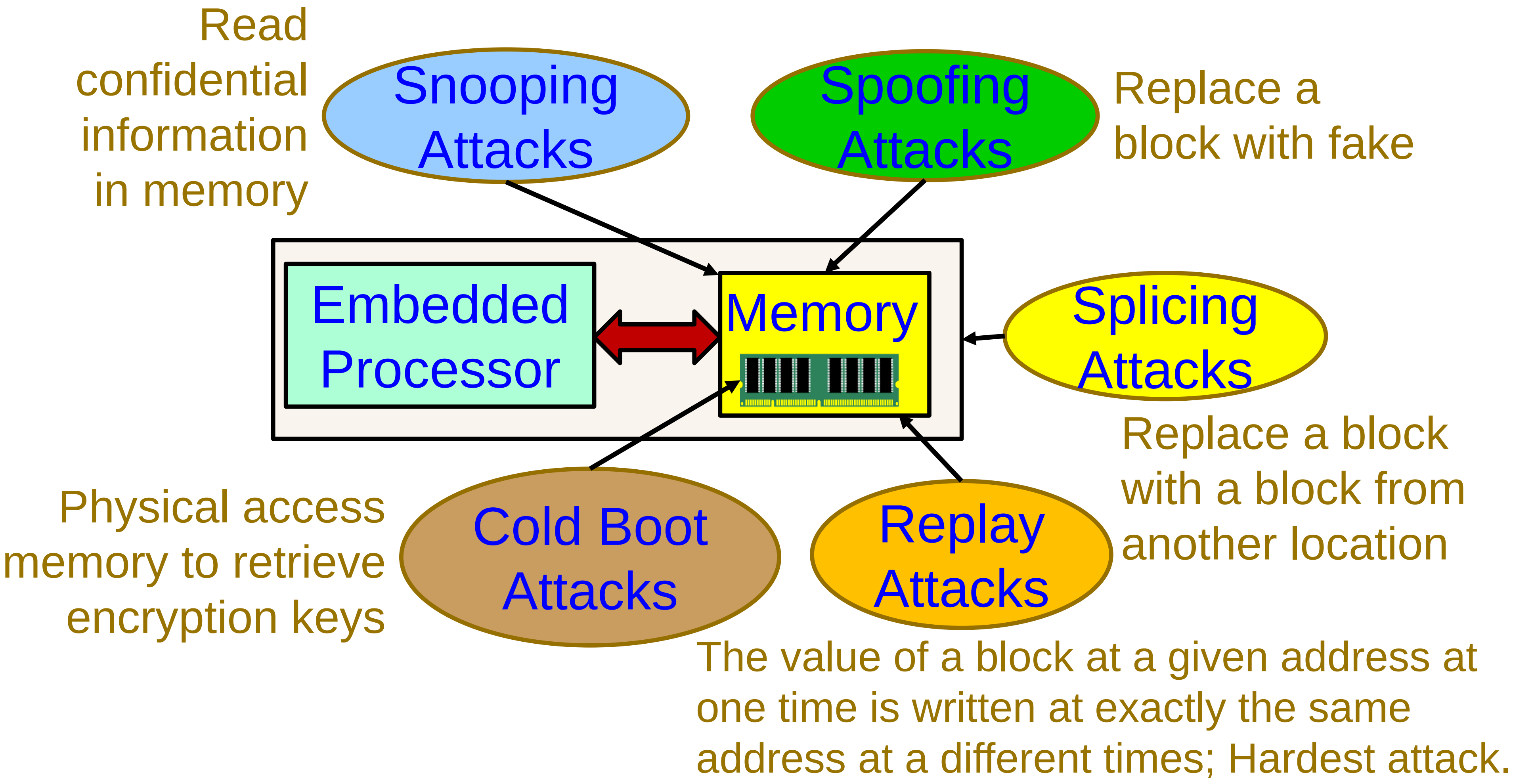
Source: Sengupta, Mohanty 2017: TCAD April 2017

Different Types of Hardware Trojans



Source: Mohanty 2015, McGraw-Hill 2015

Memory Attacks

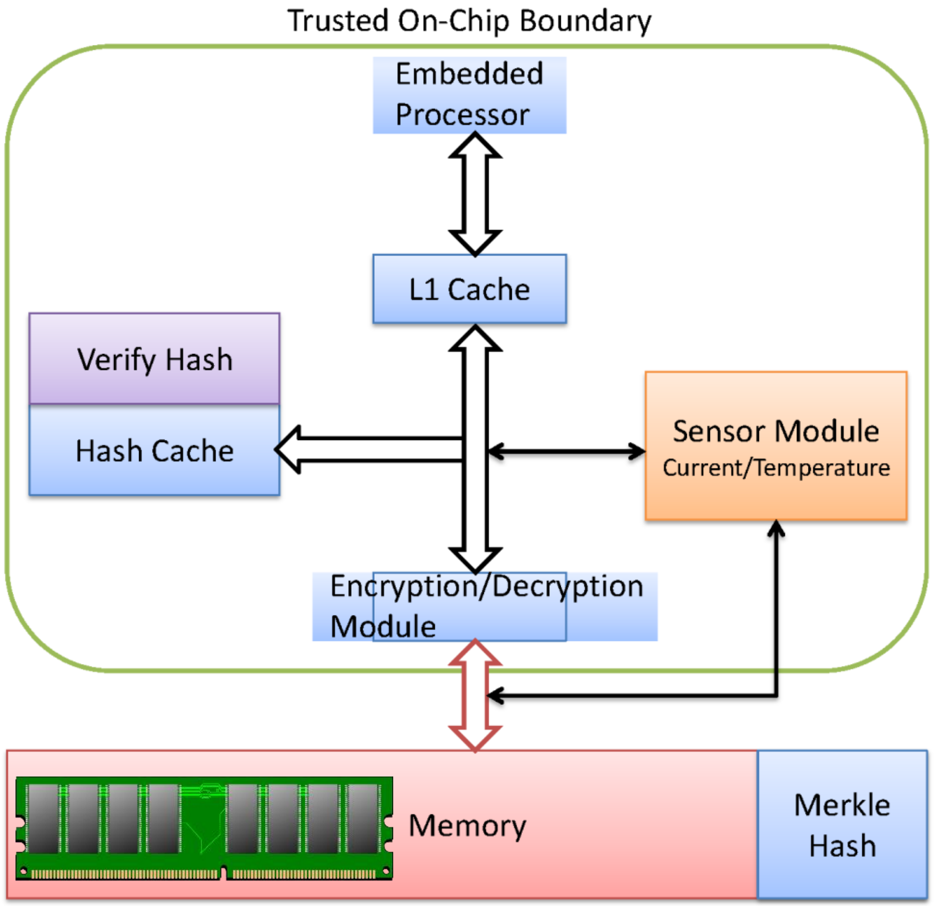


Source: Mohanty 2013, Springer CSSP Dec 2013

Memory Security and Protection

Nonvolatile Storage

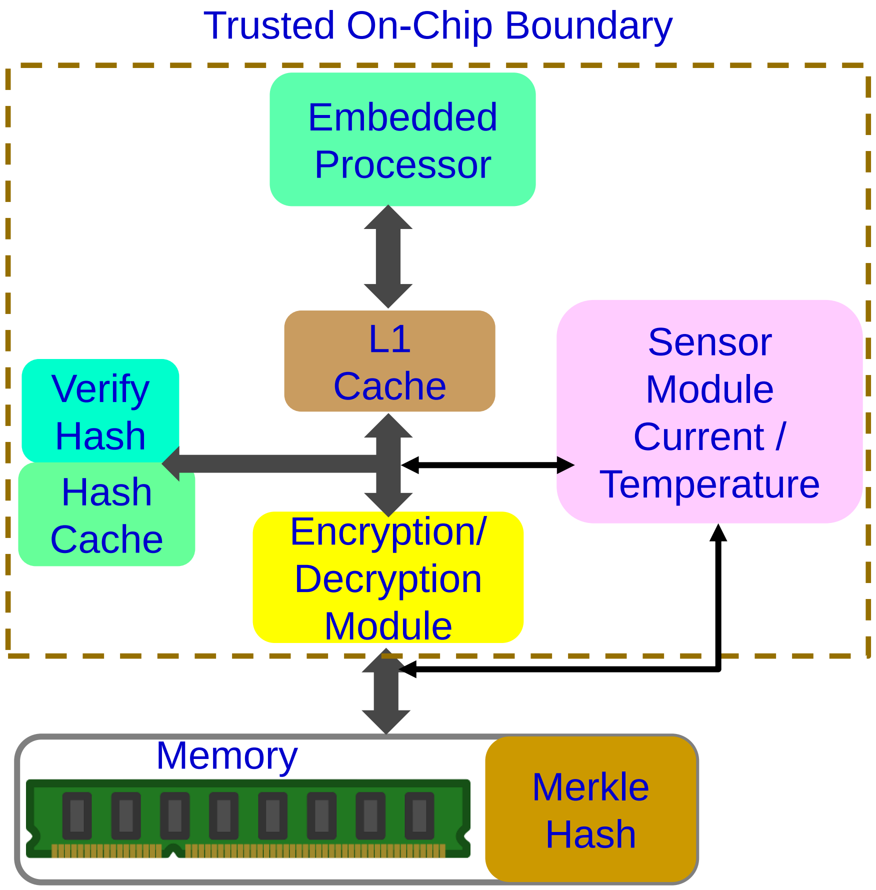
Source: http://datalocker.com



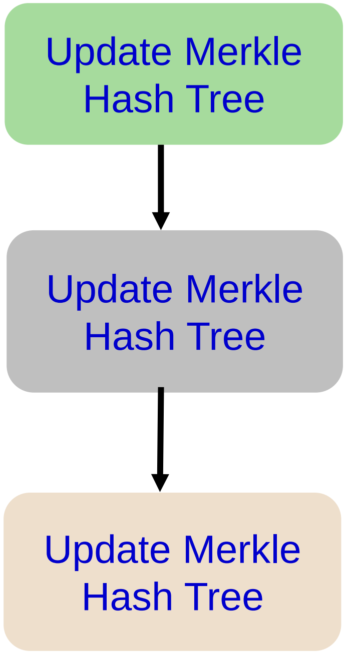
On-Chip/On-Board Memory Protection

Source: Mohanty 2013, Springer CSSP Dec 2013

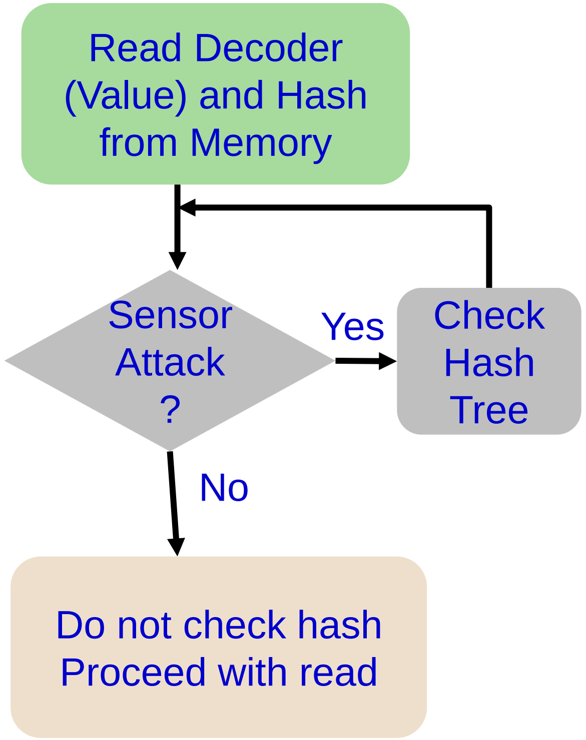
Embedded Memory Security and Protection



On-Chip/On-Board Memory Protection



Write Operation



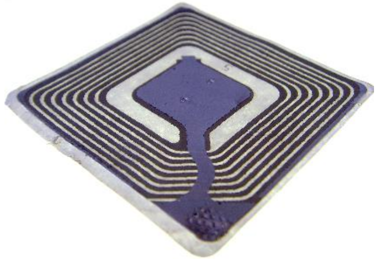
Read Operation

Source: Mohanty 2013 and Springer CSSP Aug 2013

RFID Security - Attacks

Selected RFID Attacks

- **Physical RFID Threats**
  - Disabling Tags
  - Tag Modification
  - Cloning Tags
  - Reverse Engineering and Physical Exploration
- **RFID Channel Threats**
  - Eavesdropping
  - Snooping
  - Skimming
  - Replay Attack
  - Relay Attacks
  - Electromagnetic Interference
- **System Threats**
  - Counterfeiting and Spoofing Attacks
  - Tracing and Tracking
  - Password Decoding
  - Denial of Service (DoS) Attacks



Numerous Applications

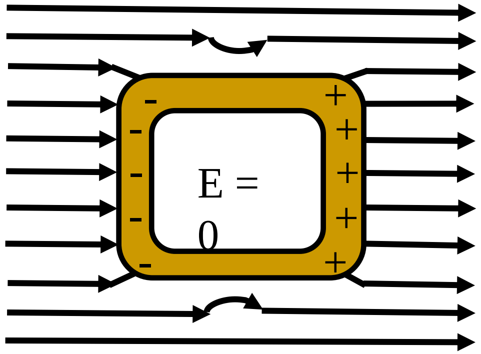
Source: Khattab 2017: Springer 2017 RFID Security

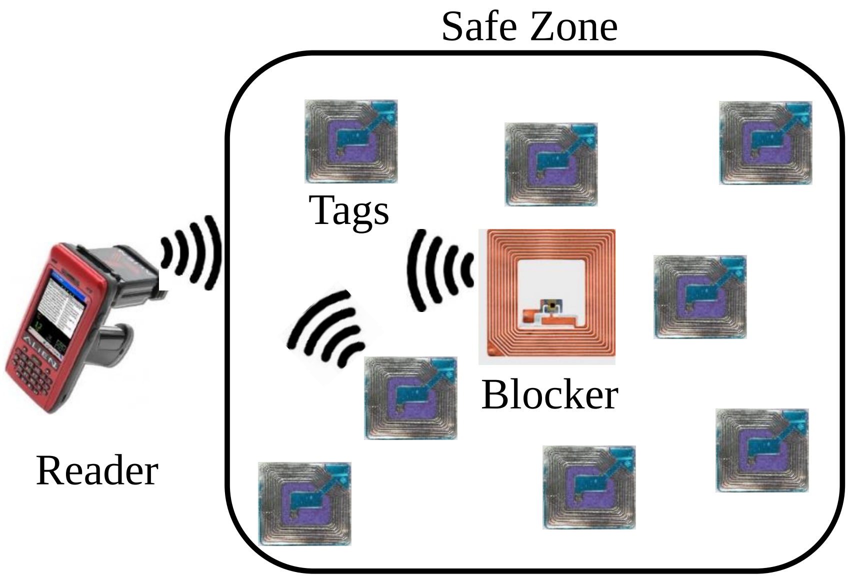
RFID Security - Solutions

Selected RFID Security Methods

- Killing Tags
- Sleeping Tags
- Faraday Cage
- Blocker Tags
- Tag Relabeling
- Minimalist Cryptography
- Proxy Privacy Devices

Faraday Cage





Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

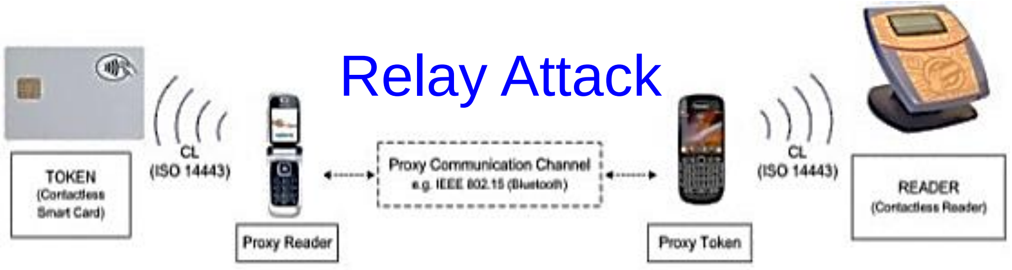
NFC Security - Attacks

Selected NFC Attacks
- Eavesdropping
- Data Modification
- Relay Attacks
- Data Corruption
- Spoofing
- Interception Attacks
- Theft

Source: http://www.idigitaltimes.com/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497

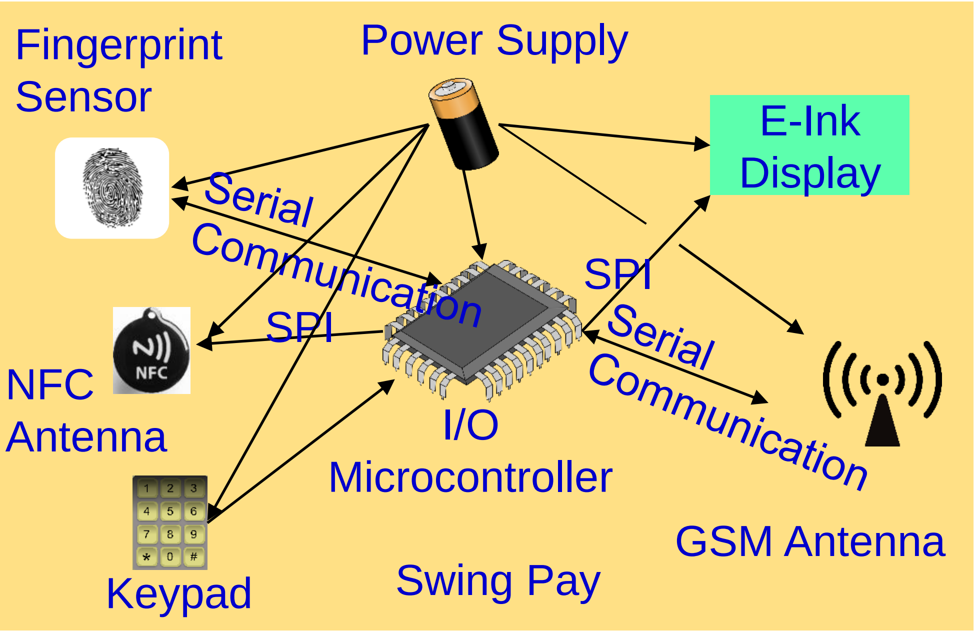
Eavesdropping

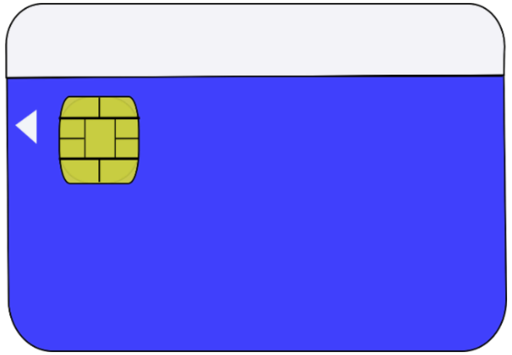
Source: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

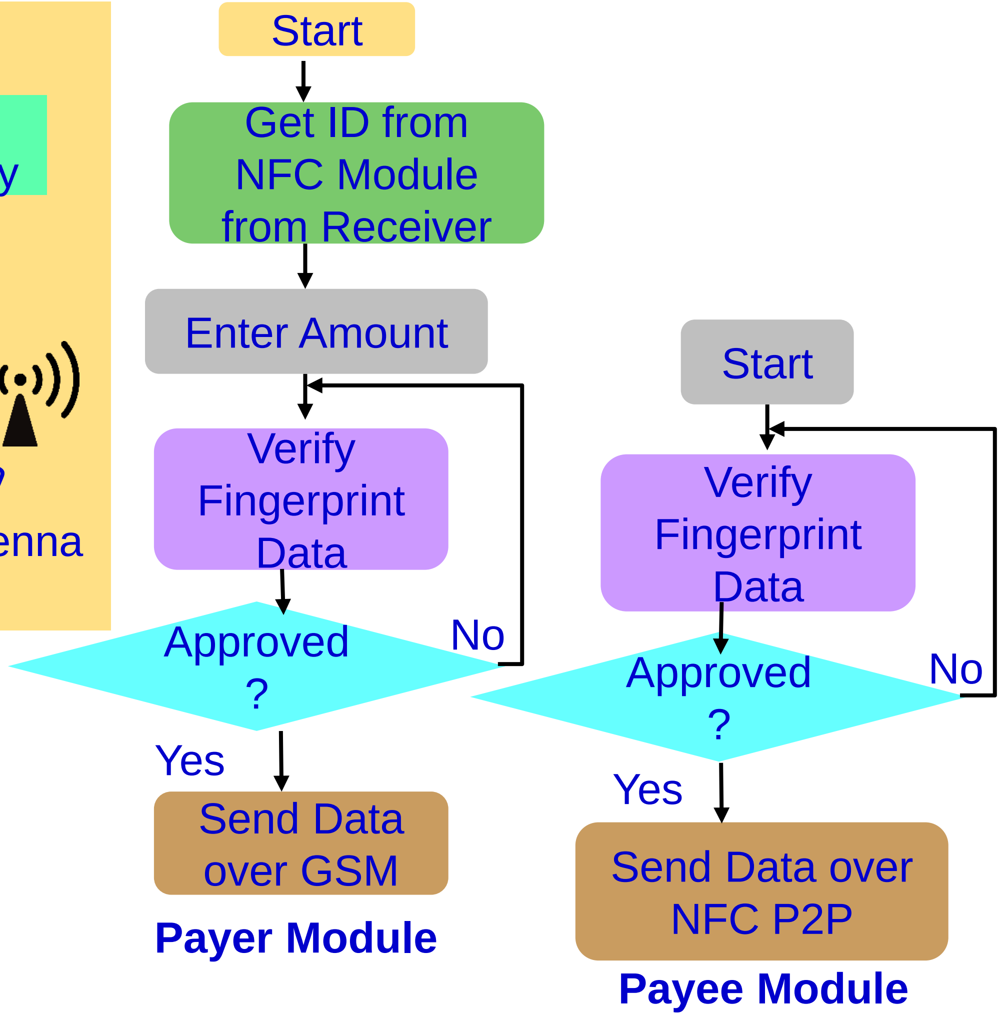


Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

NFC Security - Solution

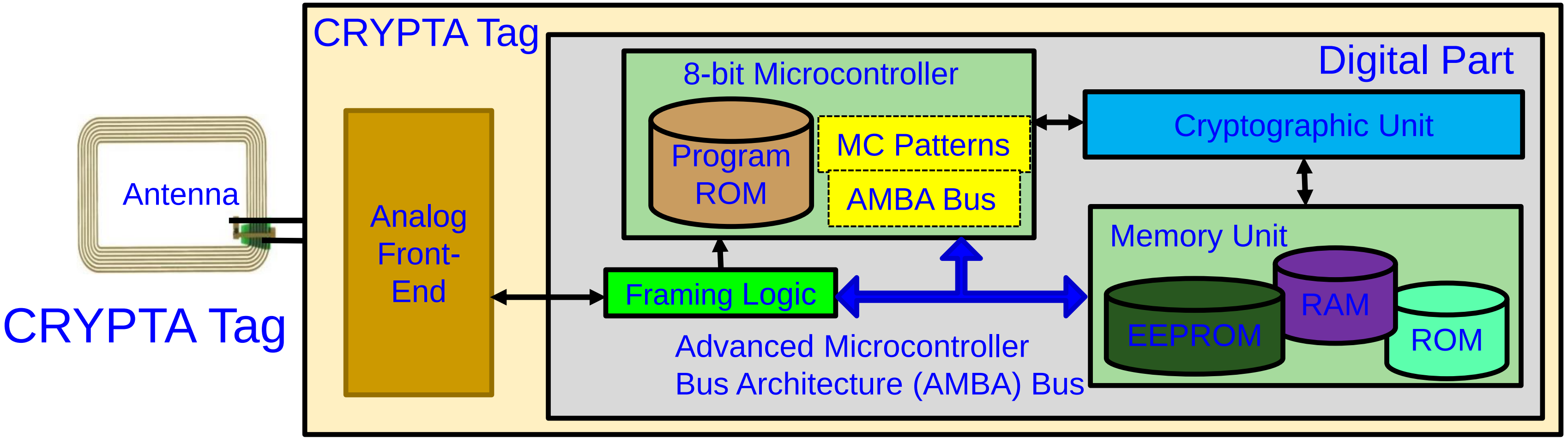






Source: Mohanty 2017, CE Magazine Jan 2017

NFC Security - Solutions

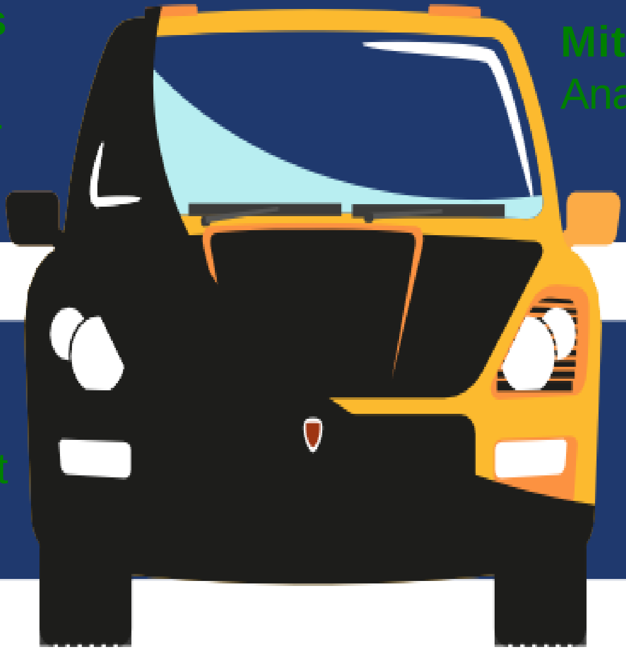


Source: Plos 2013, TVLSI Nov 2013

Autonomous Car Security – Key Aspects

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

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

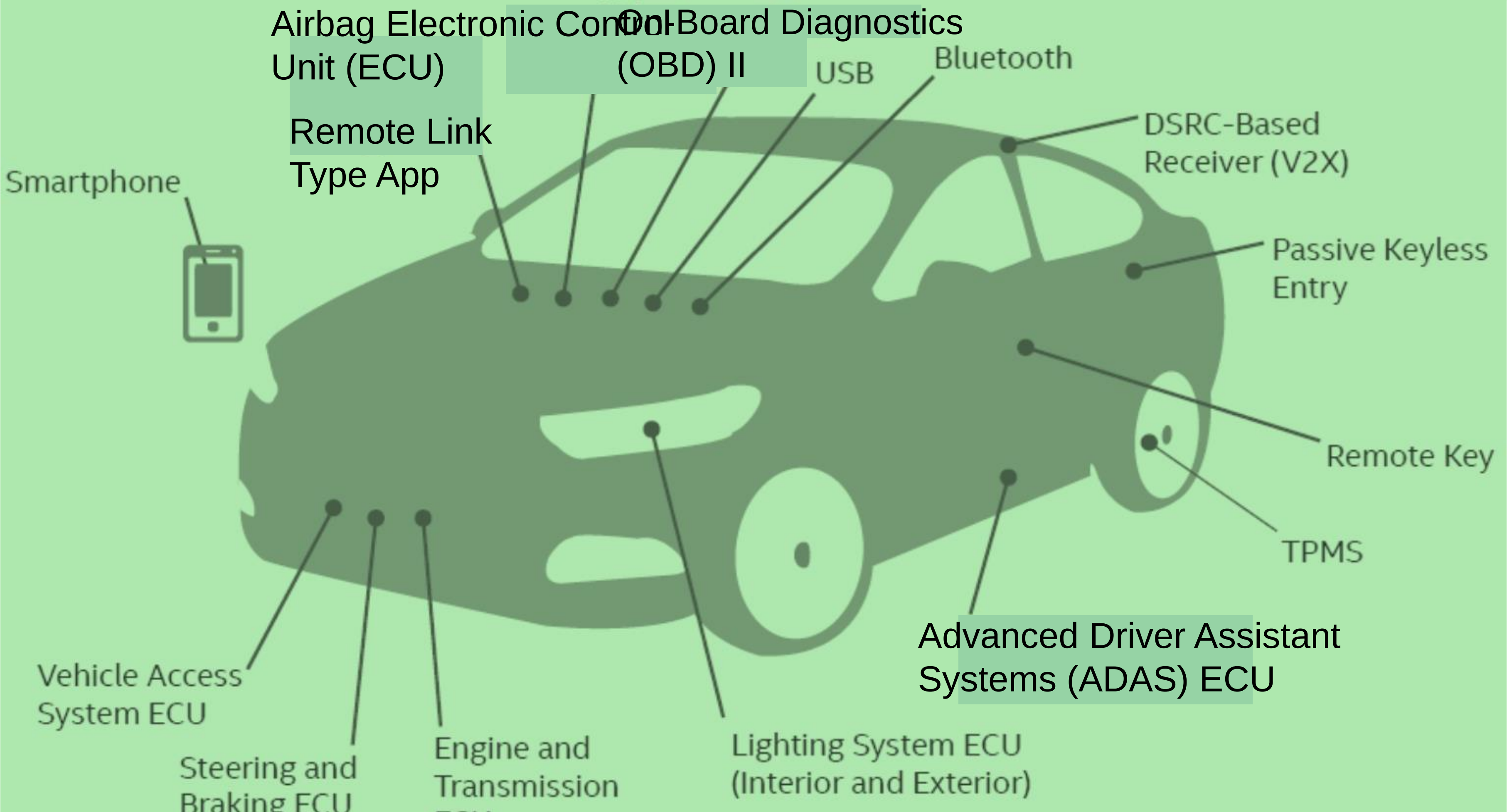


Protecting Each Module
Sensors, Actuators, and Anything with an Microcontroller Unit (MCU)

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

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

Next-Generation Car – Security Venerability



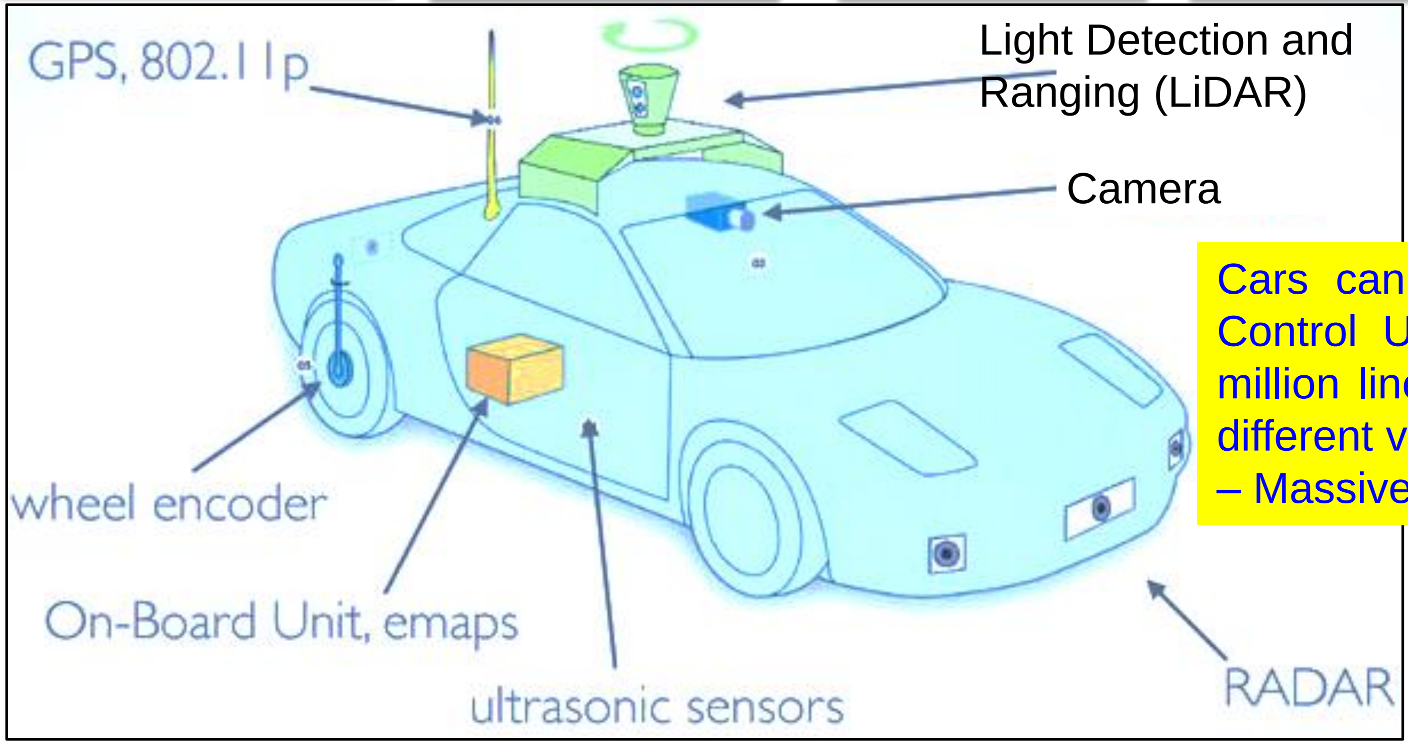
Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

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

Autonomous Car – Security Venerability

Selected Attacks on Autonomous Cars

- Replay
- Relay
- Jamming
- Spoofing
- Tracking



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

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

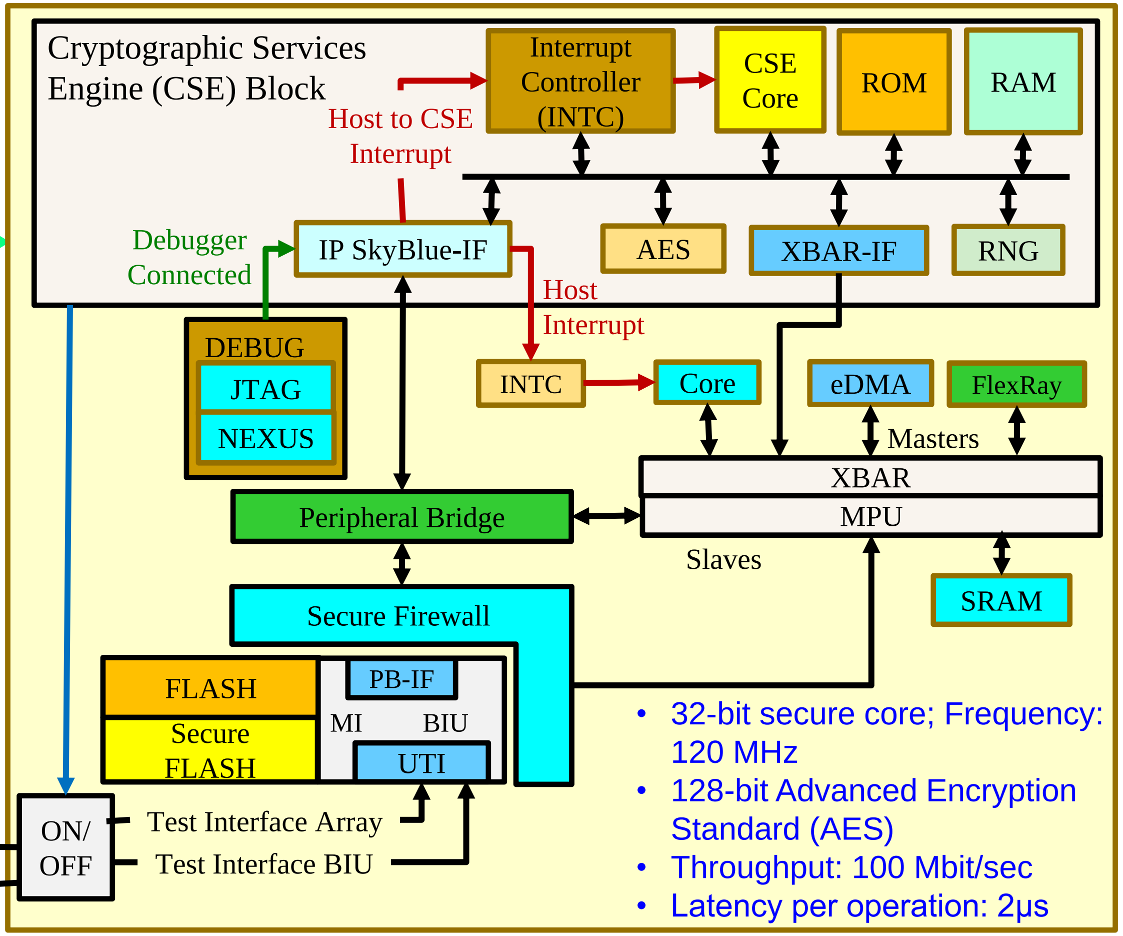
Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

Source: Petit 2015: IEEE-TITS Apr 2015

Autonomous Car Security – Cryptographic Hardware

Cryptographic Services Engine (CSE) Block

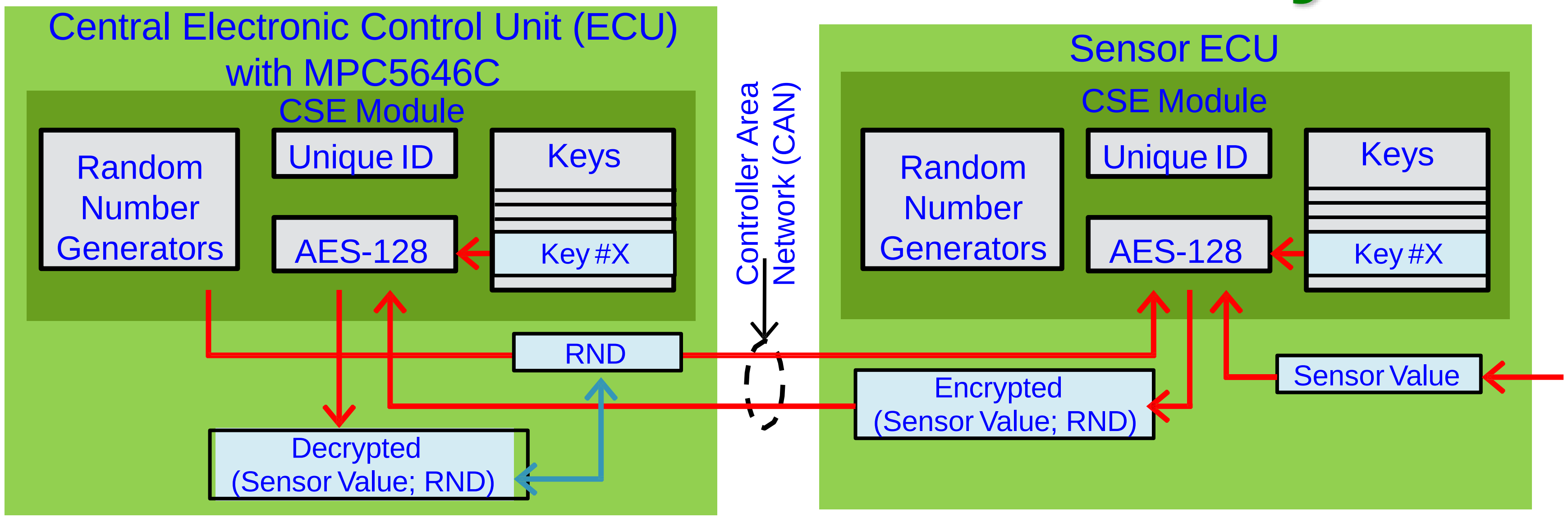
Qorivva MPC564xB/C Family from NXP/Freescale



- 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

Autonomous Car Security



Step 1: Central ECU obtains random number and sends it to sensors ECU (after power-on of car).

Step 2: Sensor ECU reads sensor value and asks CSE module to encrypt it and the received random number (using key #X).

Step 3: Sensor ECU sends encrypted message to central ECU.

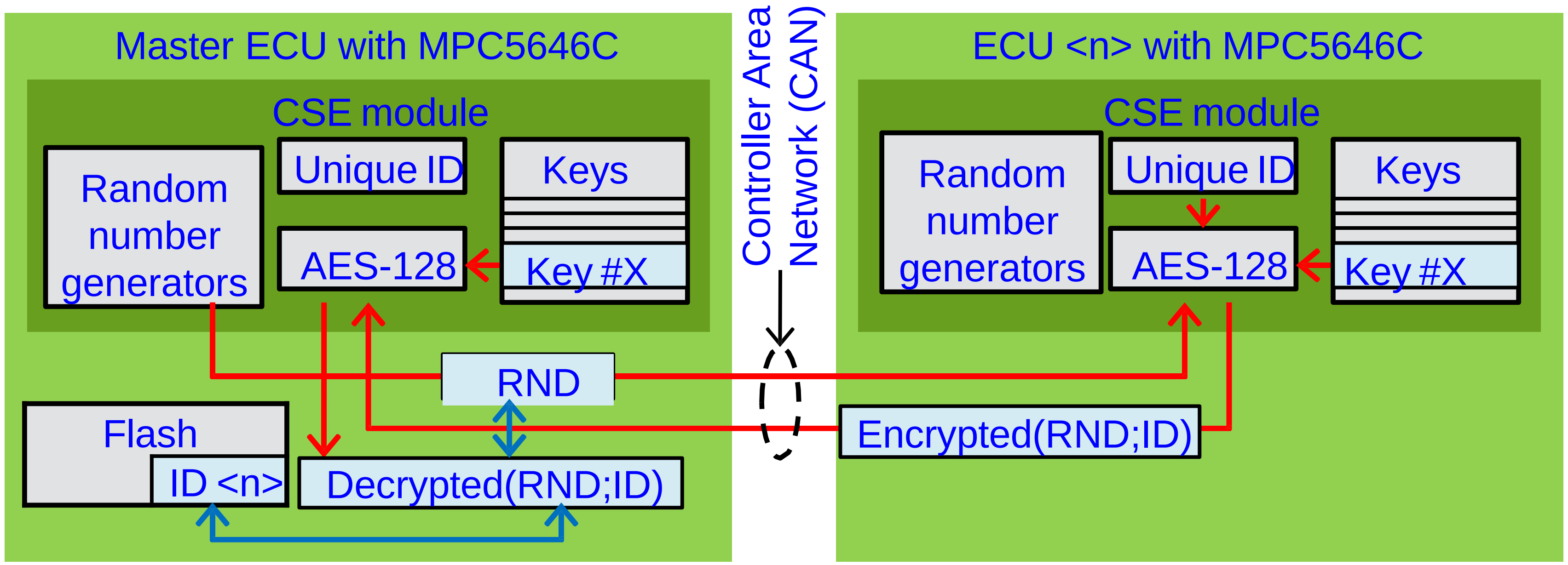
Step 4: Central ECU asks CSE module to decrypt received message (using key #X).

Step 5: Central ECU checks sent random number versus received/decrypted random number.

- Random number: Protects against replay attacks.
- Encryption: Protects against eavesdropping.
- Random number and encryption: Ensures data integrity and authenticity.

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

Autonomous Car Security



Step 1: Master ECU obtains random number and sends it to ECU <n>.

Step 2: ECU <n> appends its unique ID to received RND, encrypts this message with key #X, and sends encrypted message to master ECU.

Step 3: Master ECU decrypts received message with key #X.

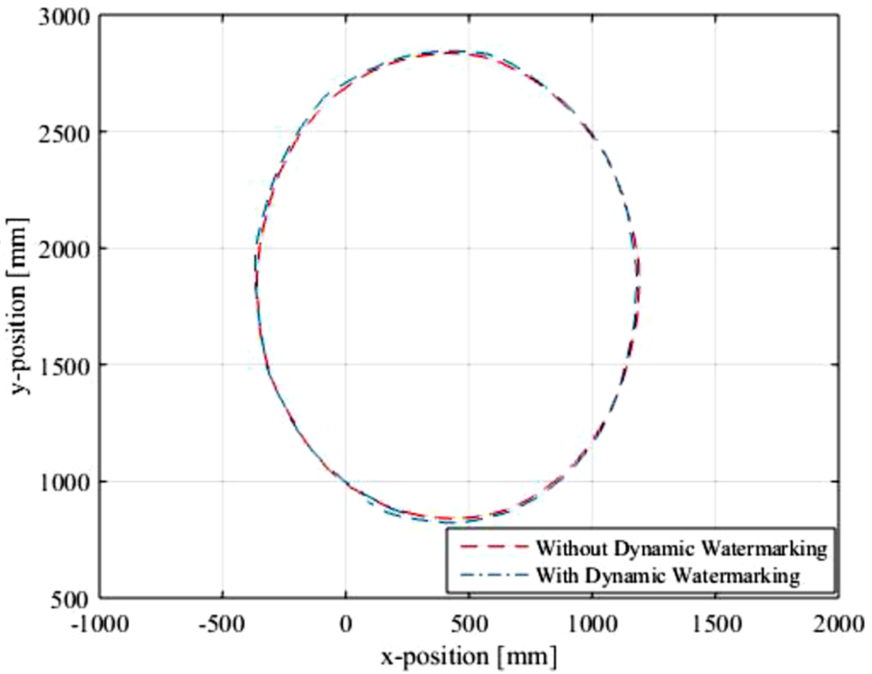
Step 4: Master ECU checks decrypted RND and ID with sent RND and with stored ID <n>. If match: ECU <n> is ok.

- Replacement or modification of ECU <n> will change its unique ID and/or keys. Both will be detected with this proposal for component protection.

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

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 with a random signal $e_i[t]$ (watermark) on control policy-specified input.

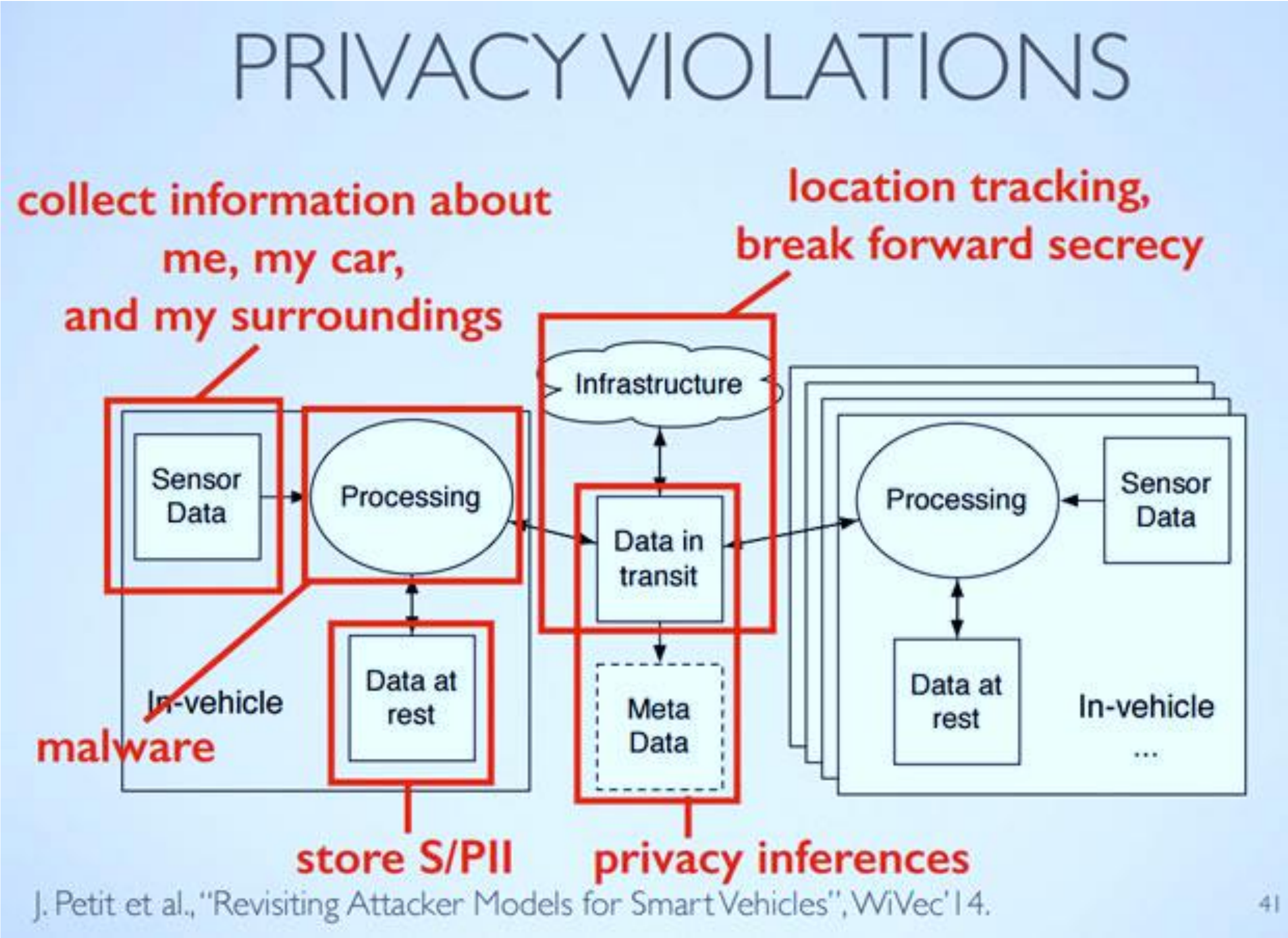


Source: Ko 2016, CPS-Sec 2016

Trajectories of a vehicle:

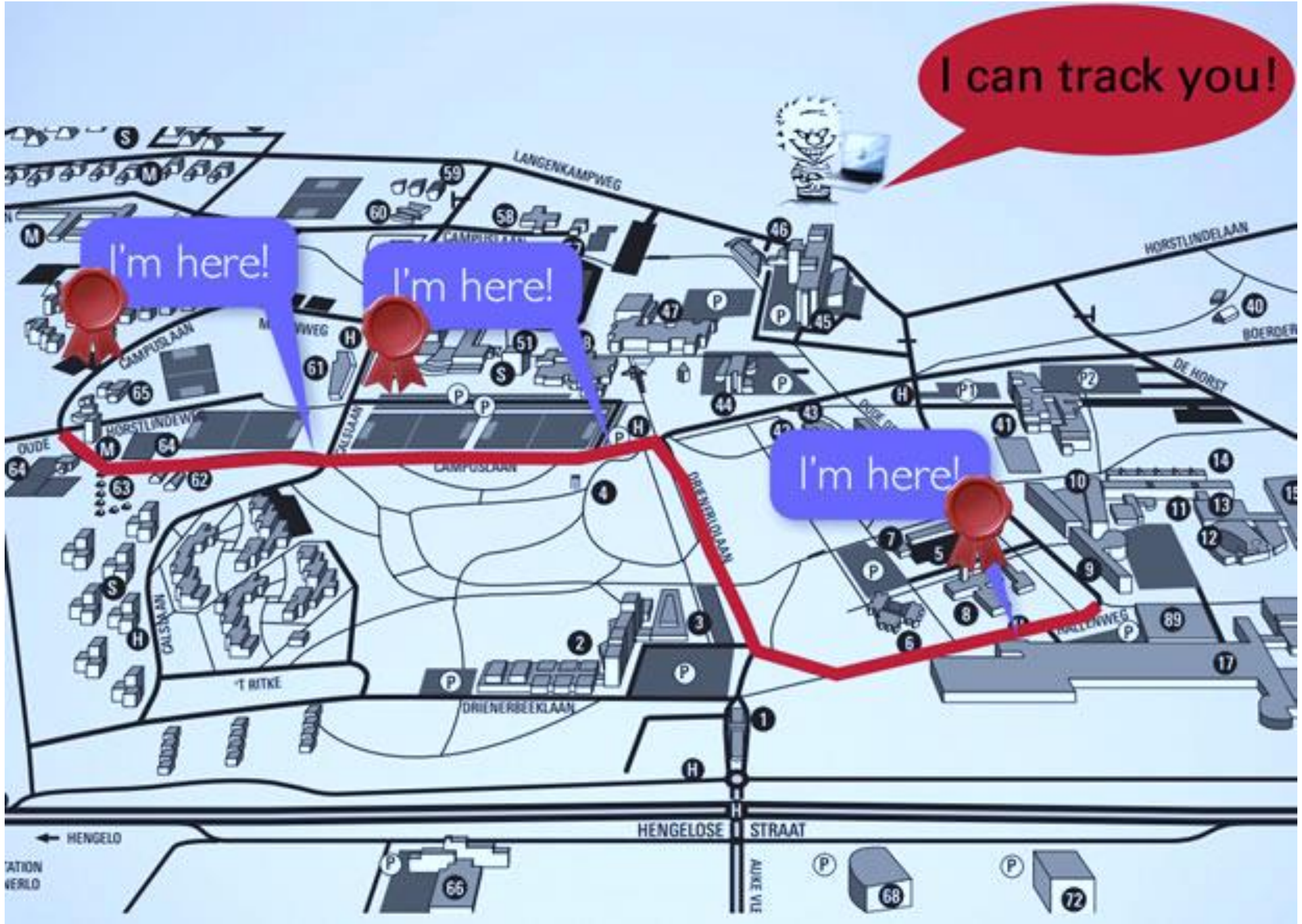
Negligible mismatch -> No significant performance degradation due to watermarking

Autonomous Car – Privacy Venerability



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

Autonomous Car – Privacy Venerability



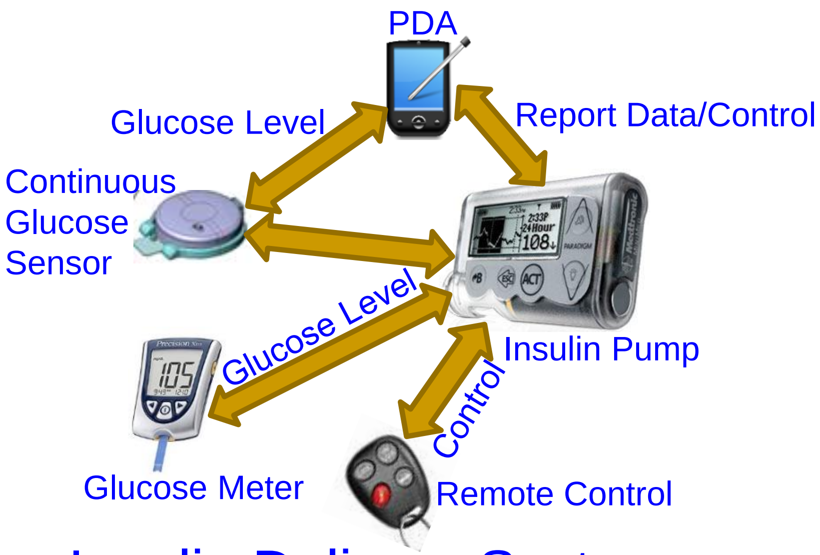
Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

Smart Healthcare - Security and Privacy Issue

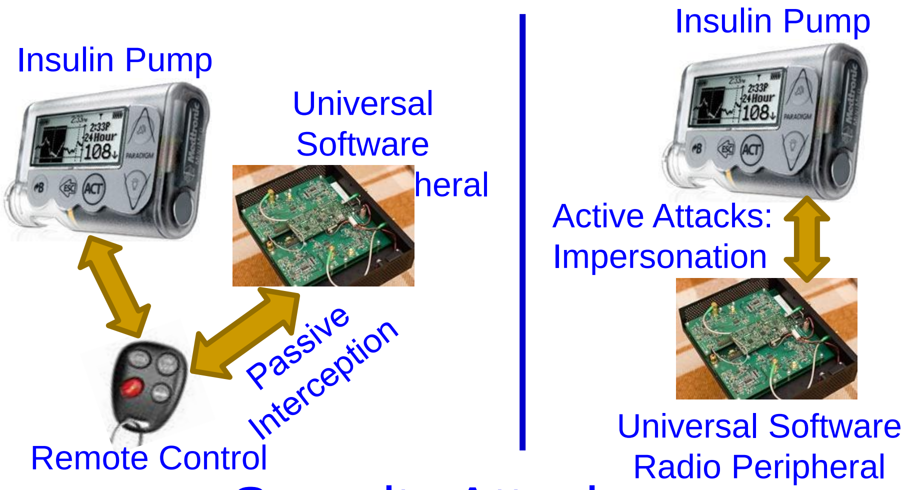
Selected Smart Healthcare Security/Privacy Challenges

- Data Eavesdropping
- Data Confidentiality
- Data Privacy
- Location Privacy
- Identity Threats
- Access Control
- Unique Identification
- Data Integrity

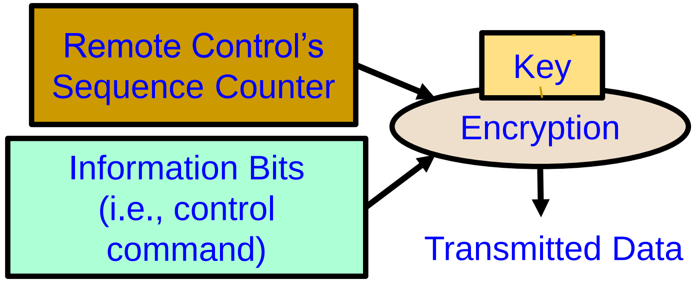
Smart Healthcare Security



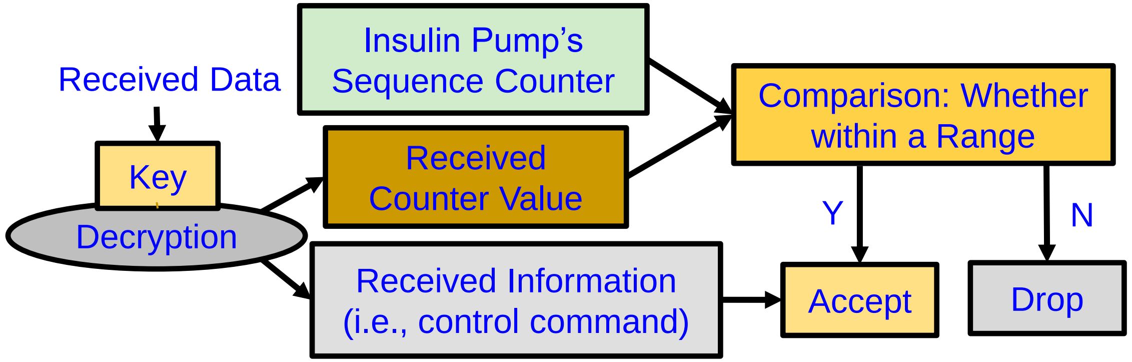
Insulin Delivery System



Security Attacks



Rolling Code Encoder in Remote Control

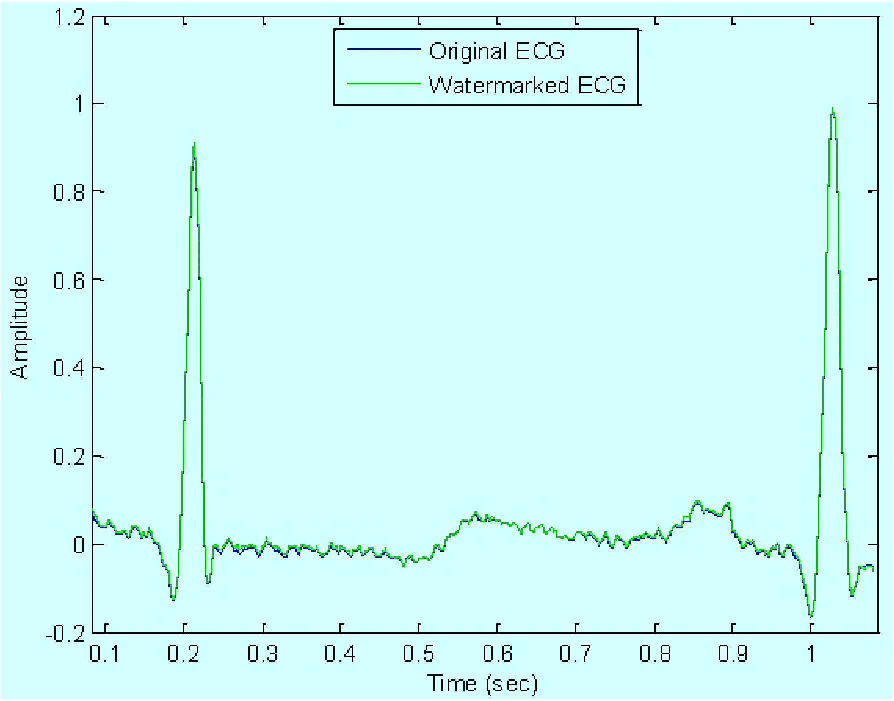


Rolling Code Decoder in Insulin Pump

Source: Li 2011, e-Health 2011

Smart Healthcare Security – 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

Side Channel Leakage

- Cryptography and watermarking hardwares provide low-power consumption, real-time performance, higher reliability and low-cost along with easy integration in multimedia hardware.
- Cryptography and watermarking hardware which are implemented using CMOS technology are susceptible to side channel attacks which collects information from physical implementation rather than software weakness.
- DFX targeted for information leakage proof is very in the current information driven society.

History of Side Channel Attacks

- During WWII, one engineer observed a spike in the oscilloscope

  during a key press of a secure typewriter Model 131-B2 (Python) at

  Bell lab in 1943
- First publicly acknowledged side-channel attack was reported in 1965. MI5 break the ciphers used by the Egyptian Embassy in London using microphones
- Van Eck phreaking – 1985 : eavesdropping on the contents of a CRT by detecting electromagnetic emissions (NSA tempest)

Source: Parameswaran Keynote iNIS-2017

Mechanical Cryptography

Jefferson Wheel [1]

was used by the United States Army from 1923 until 1942

Enigma Machine [2]

Theoretical number of possible configurations the machine could generate : 3x10114

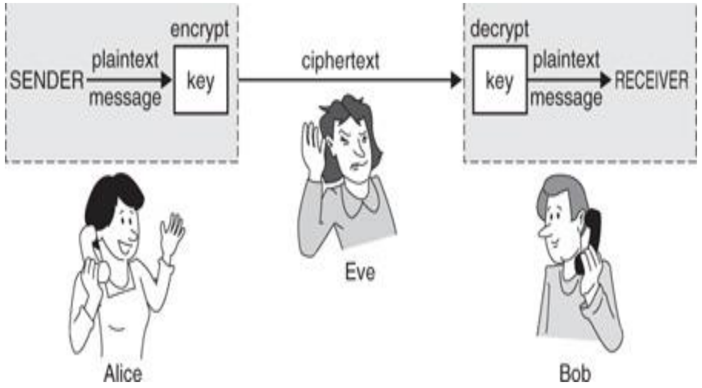
The total number of atoms in the universe : 1083

[1]. https://en.wikipedia.org/wiki/Jefferson_disk
[2]. https://en.wikipedia.org/wiki/Enigma_machine

Source: Parameswaran Keynote iNIS-2017

Modern Cryptography

- Built based on mathematical equations/ properties
- Symmetric-key algorithm
  - Same key must be used for decrypting the message
  - AES, DES and T-DES
- Asymmetric-key algorithm
  - Private key and public key
  - Public key : Encrypt
  - Private key : Decrypt
  - RSA, Elliptic Curve



Courtesy: www.powayusd.com

Source: Parameswaran Keynote iNIS-2017

Advanced Encryption Standard - AES

- Block cipher algorithm
- Plaintext 128 bits ; Key 128, 192 or 256 bits

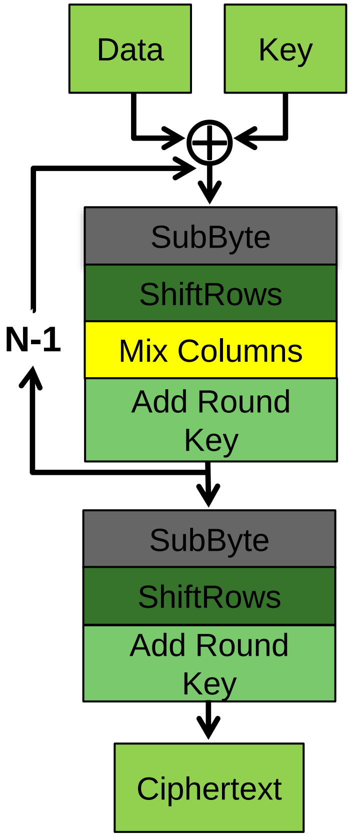
Based on the key size, number of rounds will change

AES - 128 N=10

AES - 192 N=12

AES - 256 N=14

  - Initial round
  - (N – 1) rounds
  - Final round



Source: Parameswaran Keynote iNIS-2017

How Secure is it?

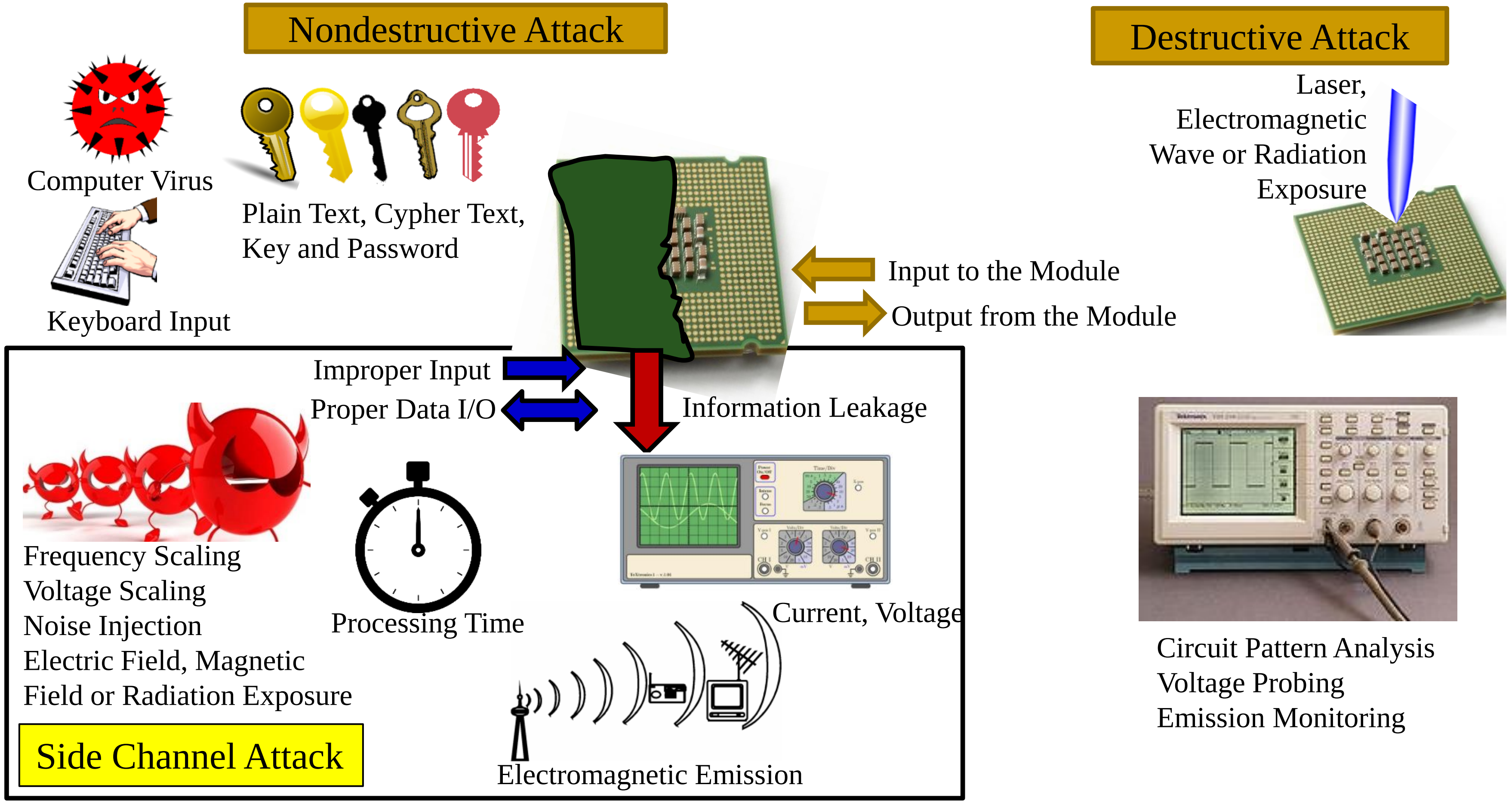
- Brute force a 128 bit key ?
- If you assume
  - Every person on the planet owns 10 computers
  - Each of these computers can test 1 billion key combinations per second
  - There are 7 billion people on the planet
  - On average, you can crack the key after testing 50% of the possibilities
  - Then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

Age of the Earth 4.54 ± 0.05 billion years

Age of the Universe 13.799 ± 0.021 billion years

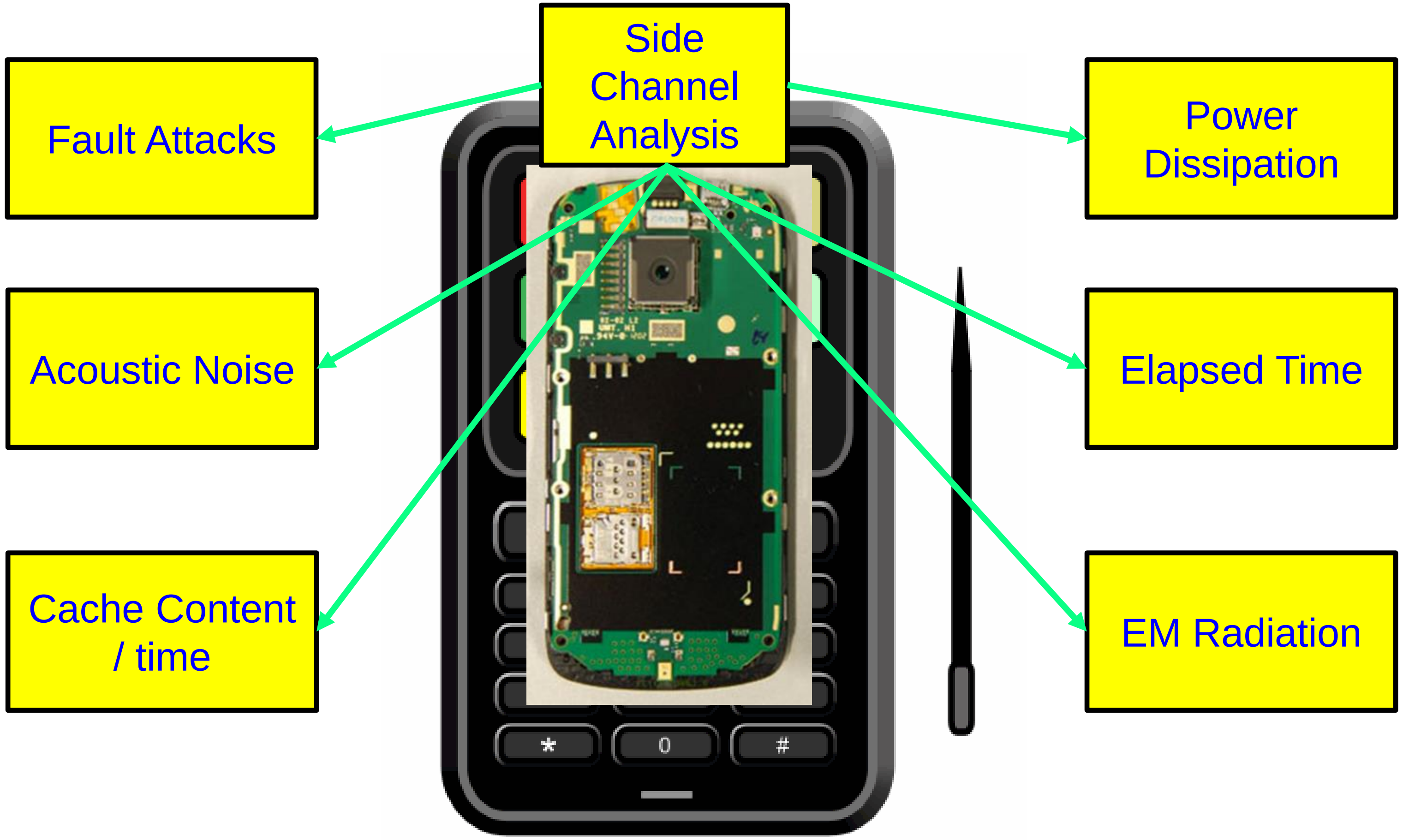
Source: Parameswaran Keynote iNIS-2017

Side Channel Attacks



Source: http://www.keirex.com/e/Kti072_SecurityMeasure_e.html

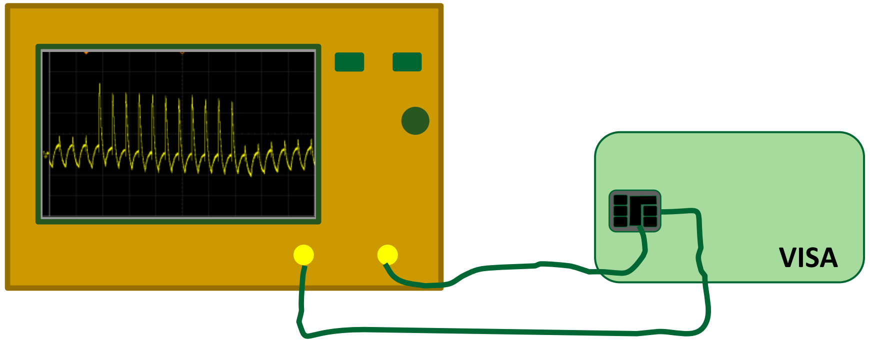
What are Side Channel Analysis Attacks?



Source: Parameswaran Keynote iNIS-2017

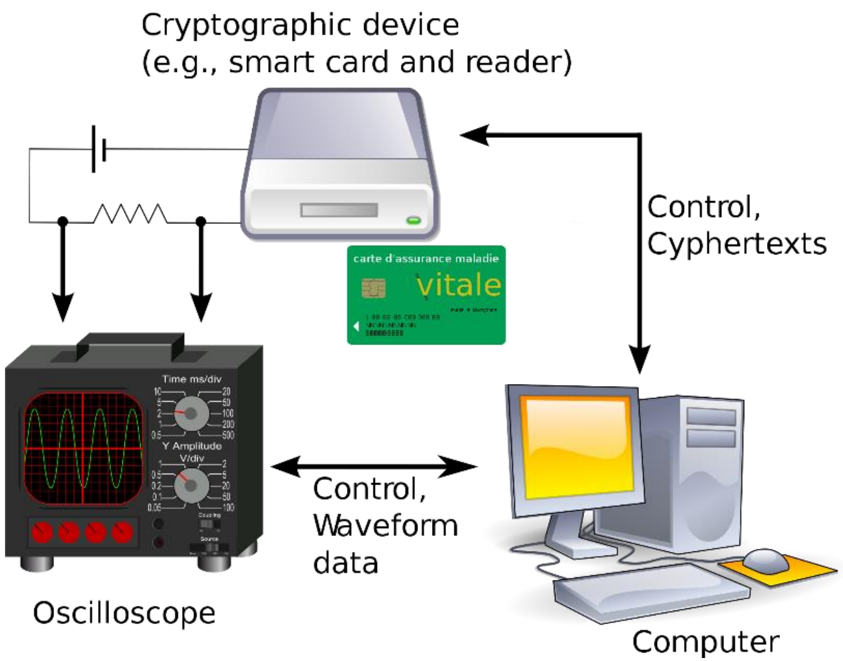
Power Analysis Attacks

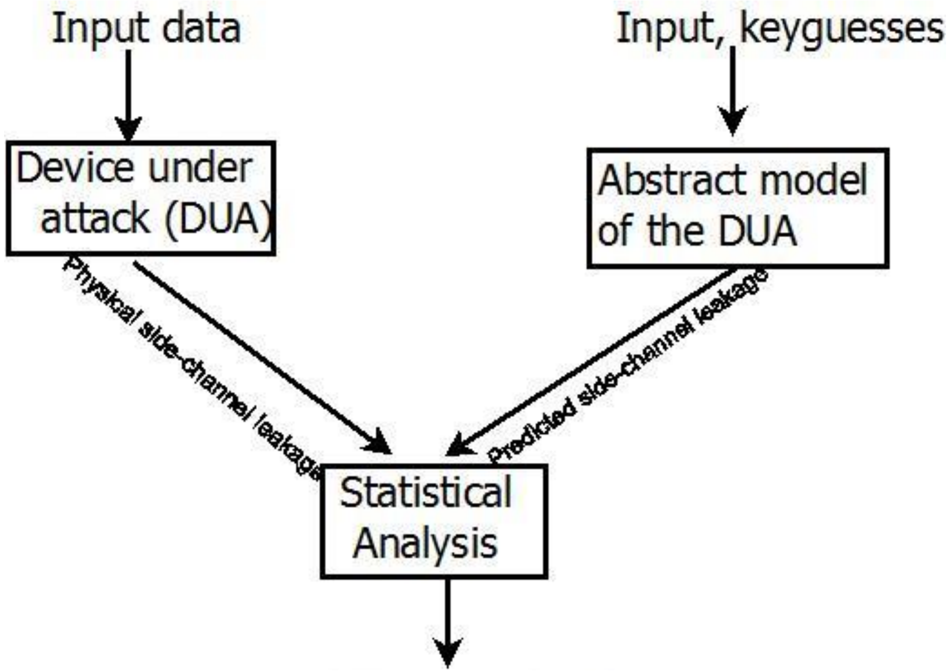
- Revealing the secret information via the power dissipation of the device
- Why?
  - CMOS gates are the most popular building blocks of IC manufacturing
  - Power dissipation of CMOS gates depend on inputs
  - The power consumption of a 0-1 transition is different to a 1-0 transition



Source: Parameswaran Keynote iNIS-2017

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





Decision on key guess

Side Channel Attacks - Correlation Power Analysis (CPA)

- CPA analyzes the correlative relationship between the plaintext/ cipher-text and instantaneous power consumption of the cryptographic device.
- CPA is a more effective attacking method compared with DPA.

Differential Power Analysis (DPA)

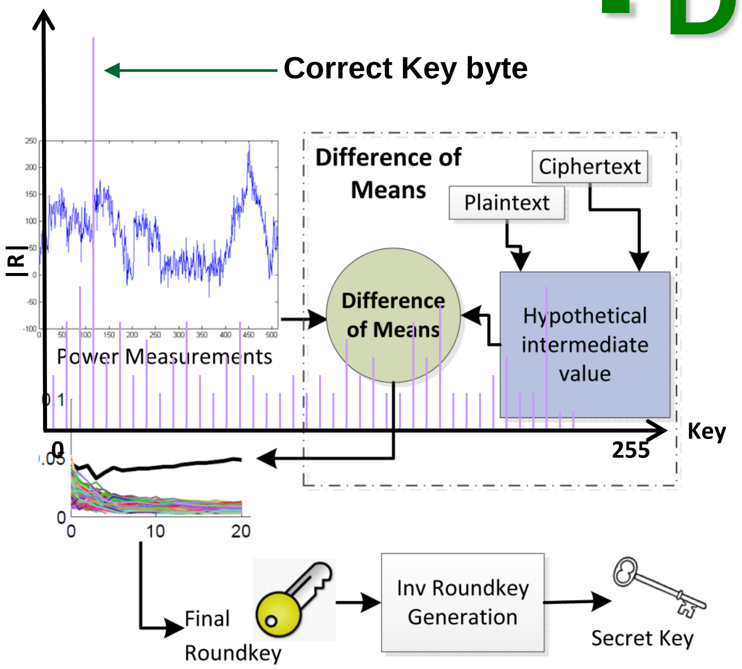
- Attacks using relationship between data and power.
- Looks at difference of category averages for all key guess.
- Requires more power traces than CPA.
- Slower and less efficient than CPA.

Correlation Power Analysis (CPA)

- Attacks using relationship between data and power.
- Looks at correlation between all key guesses.
- Requires less power traces than DPA.
- Faster, more accurate than DPA.

Source: Zhang and Shi ITNG 2011

Differential Power Analysis Attacks - DPA



M_0 = 34 + 32 + 27 = 93

M_1 = 50 + 36 + 25 + 20 = 131

$R = \left|\frac{93}{3} - \frac{131}{4}\right|$

R = 1.75

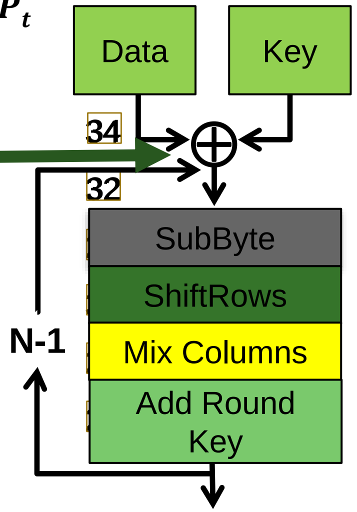
Difference of Means

If b_0=0; $M_0 = \sum_{n=1}^{N} P_n$

If b_0=1; $M_1 = \sum_{t=1}^{T} P_t$

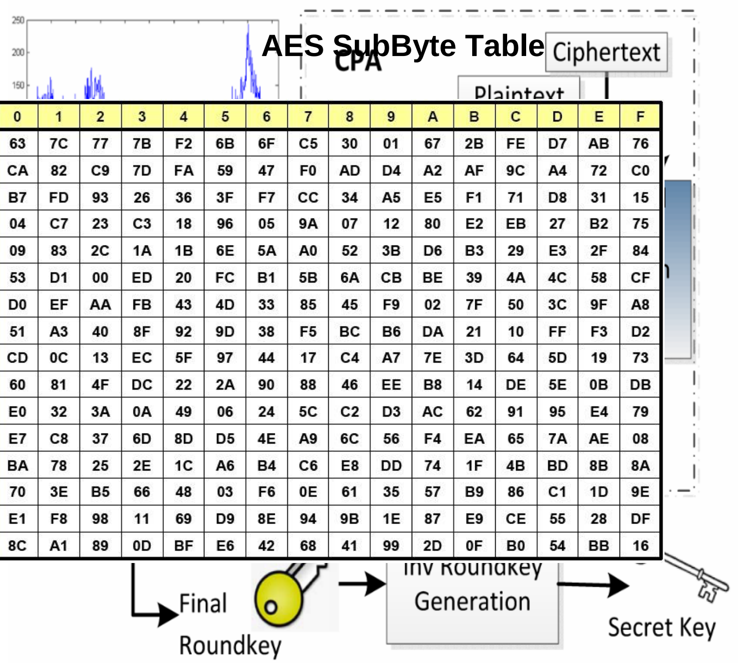
Pt	Key	Pt⊕key	Binary	μW
3F	00	[illegible]	[illegible]	
6E	00		[illegible]	34
07	00		[illegible]	32
48	00	48	01001000	
29	00	29	00101000	
B3	00	B3	10110010	
83	00	83	10000010	

Exploit this operation



Source: Parameswaran Keynote iNIS-2017

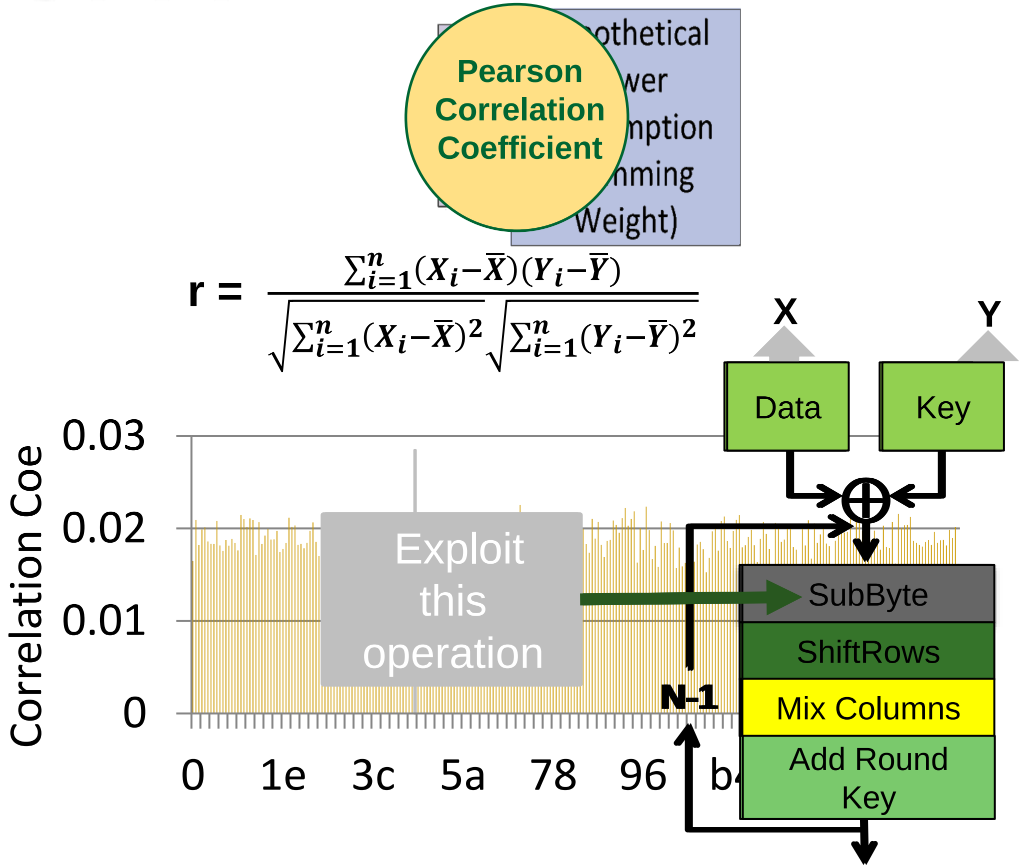
Correlation Power Analysis Attacks - CPA



AES SubByte Table

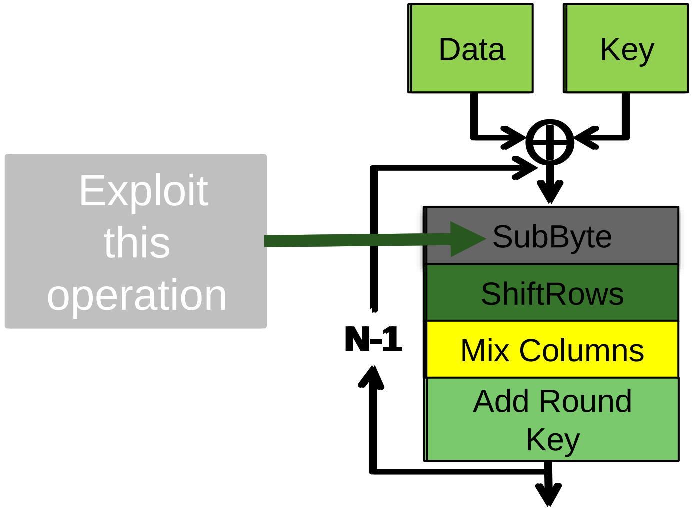
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

$$r = \frac{\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i-\bar{Y})^2}}$$



Source: Parameswaran Keynote iNIS-2017

Correlation Power Analysis (CPA)



SubByte Table

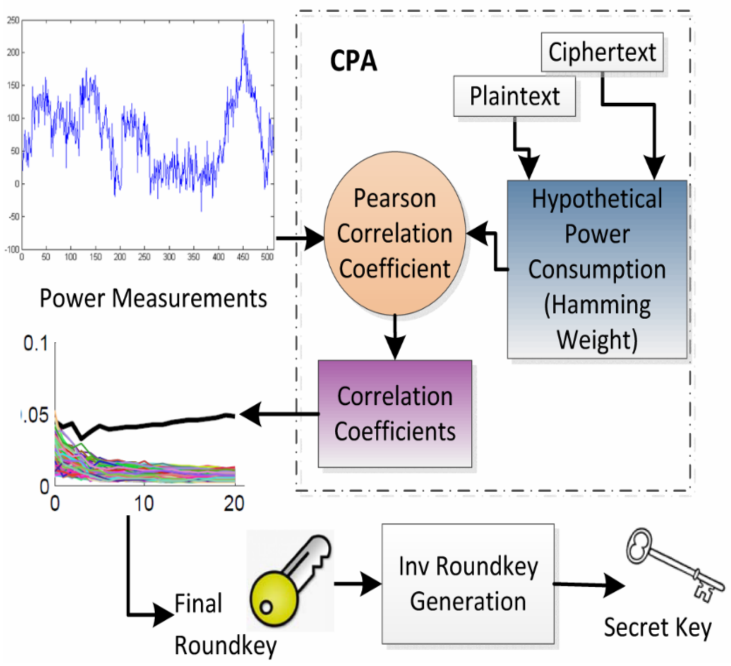
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

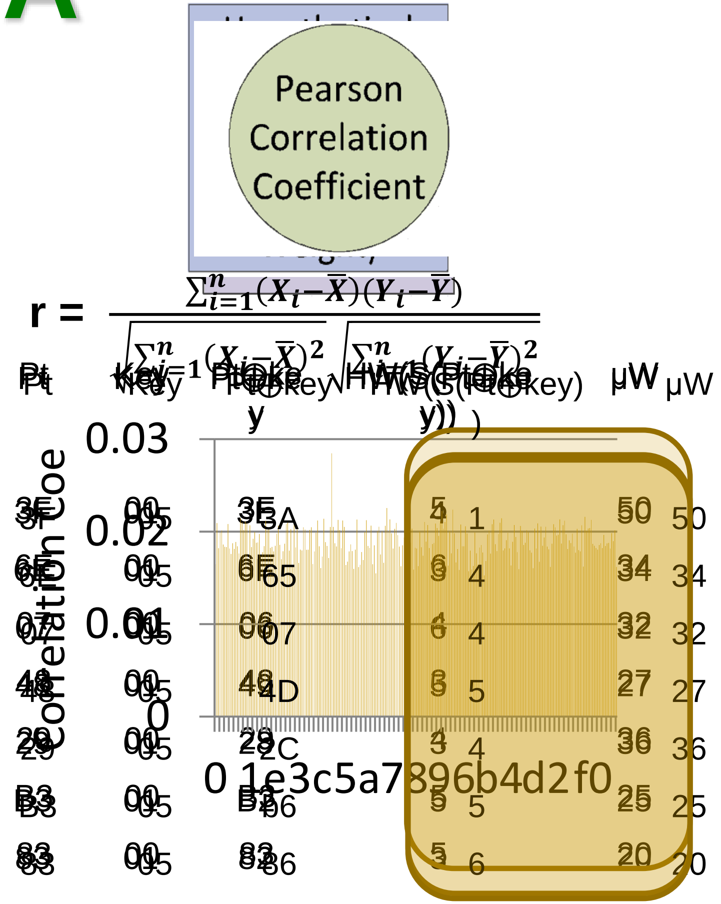
Source: Parameswaran Keynote iNIS-2017

Pt	Key	Pt⊕key	S(Pt⊕key)	Binary	HW(S(Pt⊕key))	µW
3F	01	3F	B2	10110010	4	50
6E	01	6E	A8	10101000	3	34
07	01	07	6F	01101111	6	32
48	01	48	3B	00111011	5	27
29	01	29	34	00110100	3	36
B3	01	B3	37	00110111	5	25
83	01	83	13	00010011	3	20

Source: Parameswaran Keynote iNIS-2017

Correlation Power Analysis Attacks - CPA

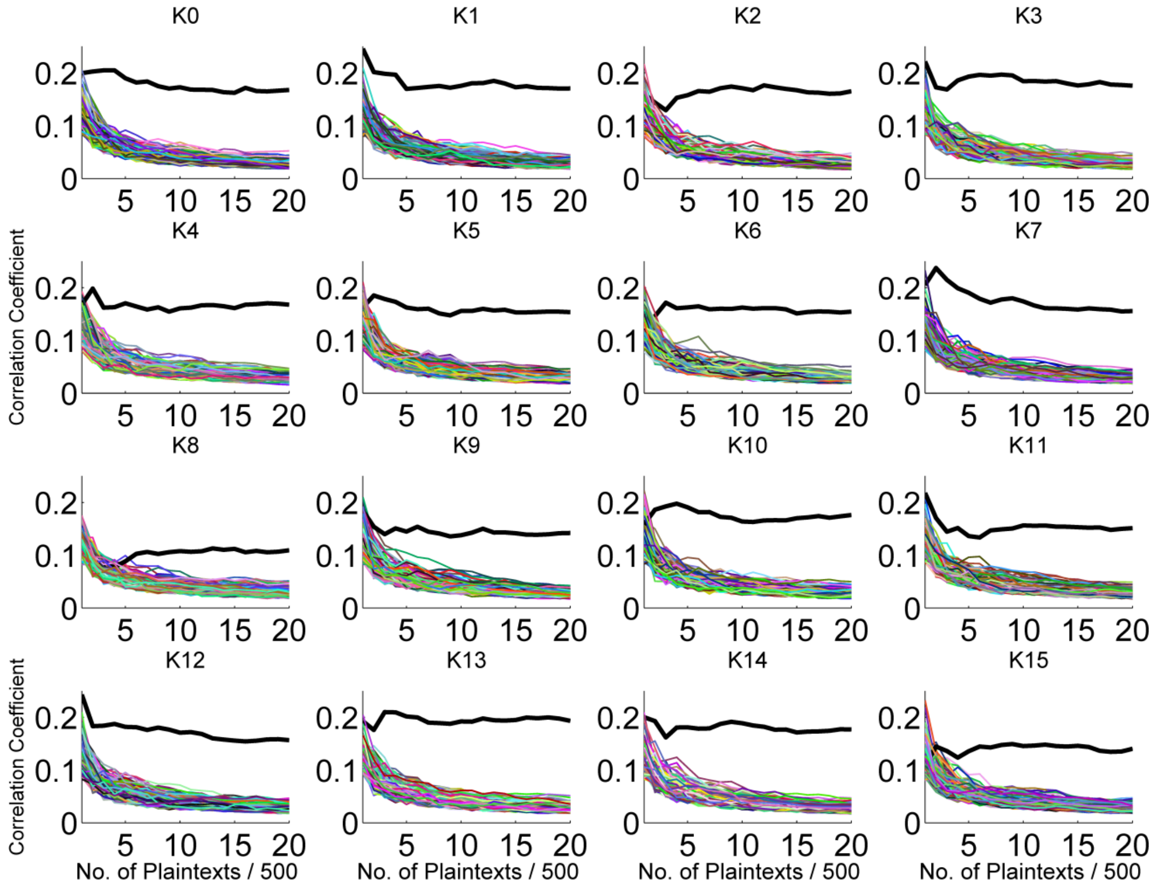




$$r = \frac{\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i-\bar{Y})^2}}$$

Source: Parameswaran Keynote iNIS-2017

Attack on Standard AES Circuit



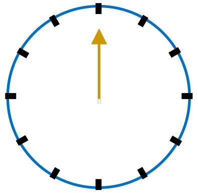
Source: Parameswaran Keynote iNIS-2017

Timing Attacks

- Elapsed time for some functions is input dependent
- E.g. linux/lib/string.c
  - Function will terminate when c1 not equal to c2
- C, Java, Python or assembly
- Attack password checking

```
int strncmp(const char *cs, const char *ct, size_t count)
{
        unsigned char c1, c2;

        while (count) {
                c1 = *cs++;
                c2 = *ct++;
                if (c1 != c2)
                        return c1 < c2 ? -1 : 1;
                if (!c1)
                        break;
                count--;
        }
        return 0;
}
```



Let us assume

s1= "To be Or not to be"

s2= "To be or not to be"

cs	T	o		b	e		O	r		n	o	t		t	o		b	e	\0
ct	T	o		b	e		o	r		n	o	t		t	o		b	e	\0

Source: Parameswaran Keynote iNIS-2017

Cache Content / Timing

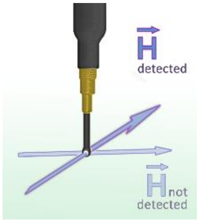
- Processor needs data RAM
- RAM is slow compared to the CPU
- Processor needs data Cache RAM
- Access time of Cache <<<< Access time of RAM
- Size of Cache <<< size of RAM
- Most of the cryptographic algorithms use pre-calculated values (tables)
- Therefore, time taken for execute such cryptographic algorithms take varying number of time (clock cycles)

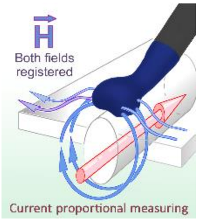
Source: Parameswaran Keynote iNIS-2017

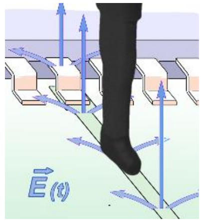
EM Radiation

- When current flow through a wire, an EM field is generated
- Unlike power dissipation, EM can be localized
- Different probes for different EM leakages

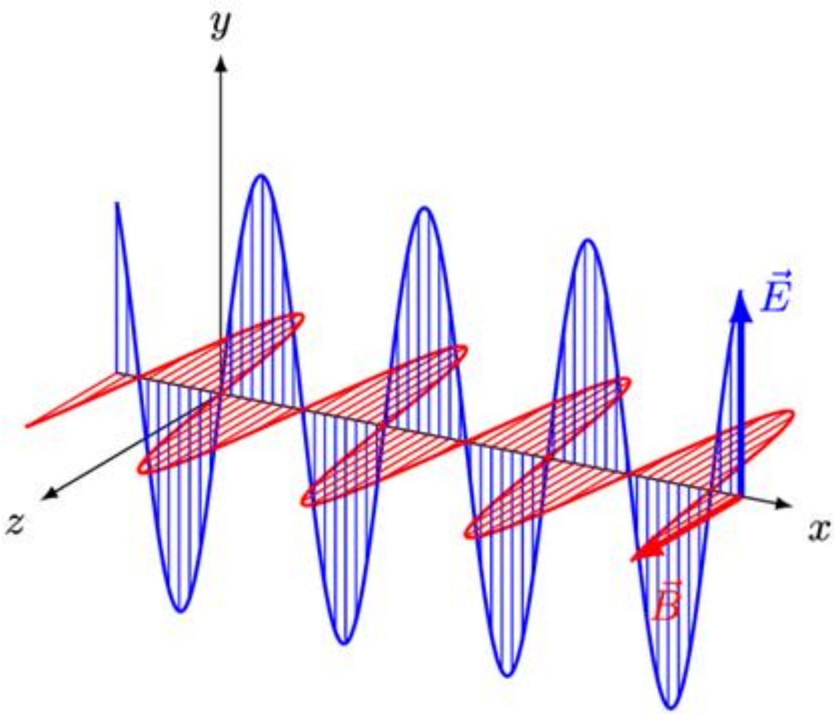
H probes H probes E probes







www.langer-emv.de

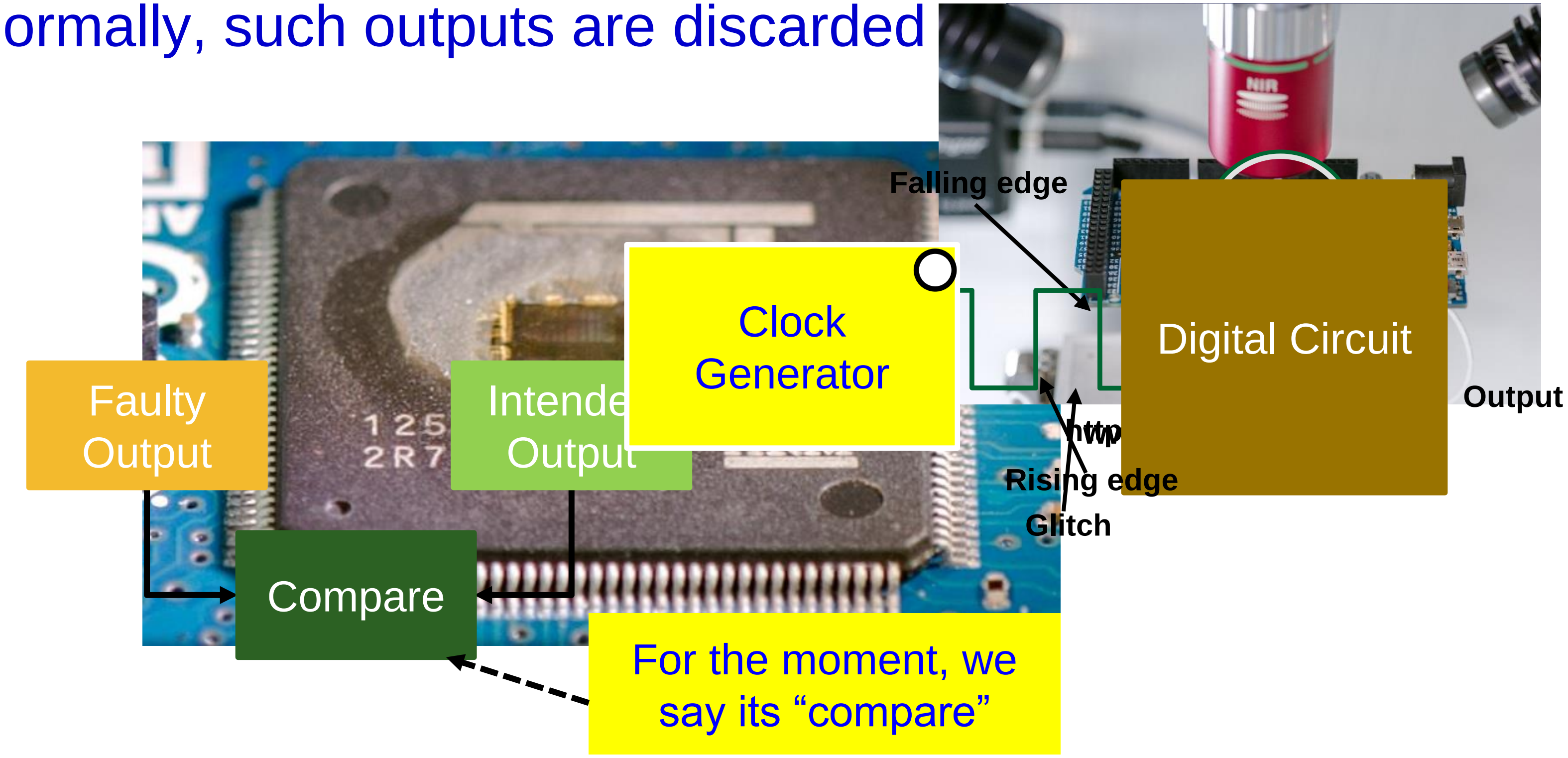


Wikipedia

Source: Parameswaran Keynote iNIS-2017

Fault Attacks

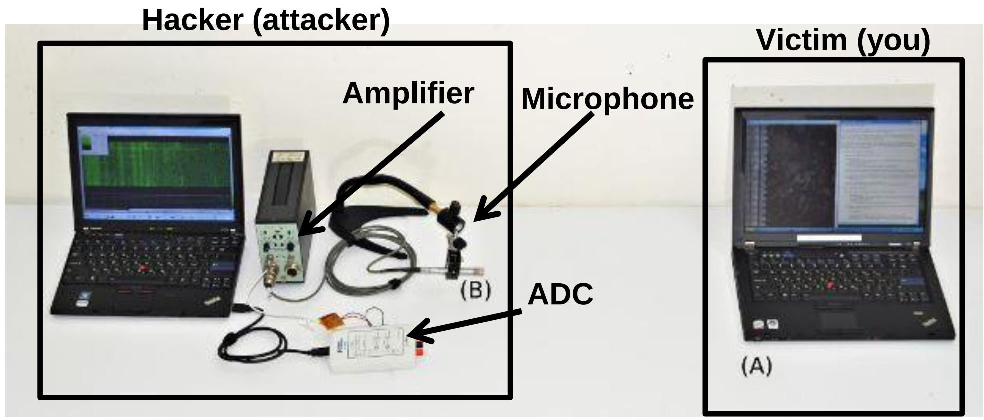
- Faults can be intentional or non-intentional (natural or human made)
- Due to faults, the outputs of the circuit/operation can be faulty
- Normally, such outputs are discarded



Source: Parameswaran Keynote iNIS-2017

Acoustic Noise

- Opening safe based on the clicking sound of the lock
- Acoustic attacks on keyboards
- Logic gates emit high frequency sounds ...



Adi Shamir

Mirror.co.uk

Source: Parameswaran Keynote iNIS-2017

How to Prevent These Attacks

Countermeasures Against Side Channel Attacks

- Each countermeasure is independent

e.g. countermeasures against timing attacks will not protect the device against power analysis attacks.

Power Analysis Attacks

- Adding noise
- Random execution
- Balancing
- Masking

Cache Timing Attacks

- Disable/ lock the cache
- Prefetch the table lookups

Acoustic attacks

- Masking
- Balancing number of transitions

Source: Parameswaran Keynote iNIS-2017

How to Prevent These Attacks

Countermeasures Against Side Channel Attacks

EM Attacks

- Adding noise
- Random execution
- Balancing
- Masking
- Adding detectors

Timing Attacks

- Write the code for constant time
- Add noise (random loop)
- Wait for the worst case elapsed time

Source: Parameswaran Keynote iNIS-2017

Differential Power Analysis (DPA) Attack Countermeasures

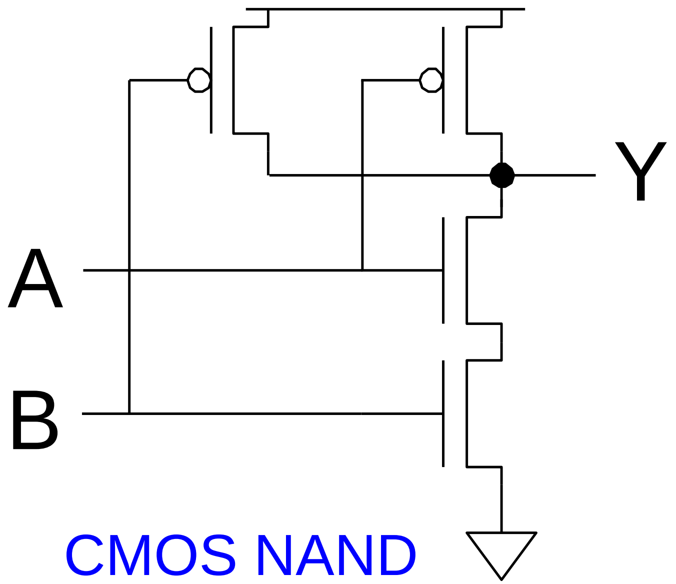
- DPA Attack Countermeasures
  - Hardware Measures
    - Power Randomization
    - Power Process Interrupts
    - Detached Power Supplies
    - Nondeterministic Execution
  - Software Measures
    - Desynchronization
    - Software Balancing
    - The Duplication Method
    - Random Masking
    - Secret-Sharing

Selected DPA and Correlation Power Analysis (CPA) Attack Resilience Methods

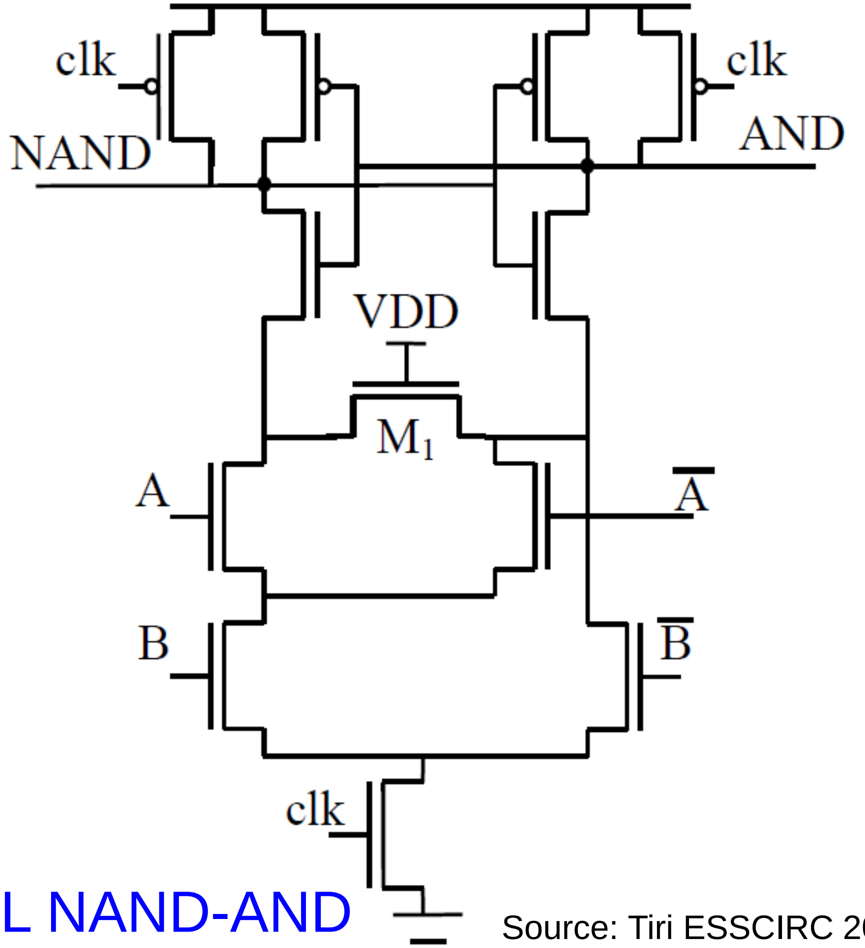
DPA and CPA Attack Resilience Methods

- Sense Amplifier Basic Logic (SABL)
- Wave Dynamic Differential Logic (WDDL)
- Two-Spacer Alternating Dual Rail Circuit
- Dynamic Voltage & Frequency Switching Approach
- Random Switching Logic (RSL)
- Return To Zero Protocols (RTZ)
- Masked Dual-Rail Pre-charged Logic (MDPL)

DPA Resilience Hardware:
Sense Amplifier Basic Logic (SABL)



CMOS NAND

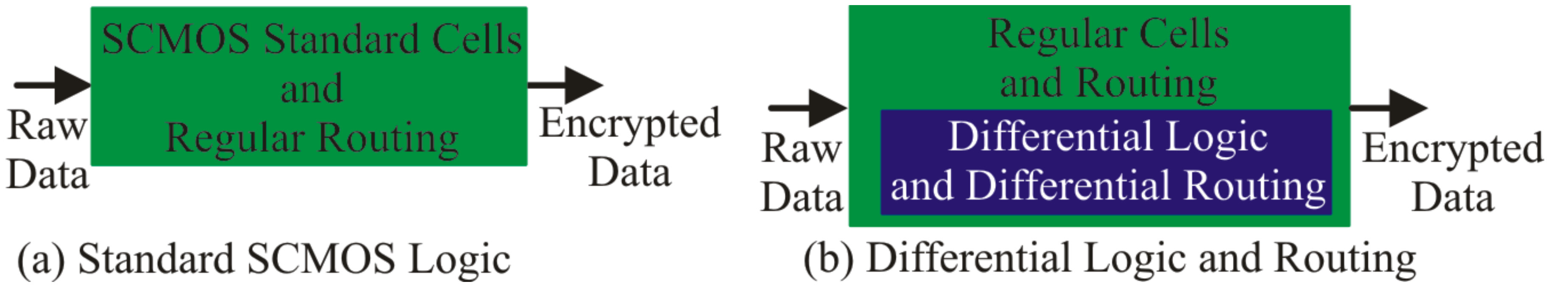


SABL NAND-AND

Source: Tiri ESSCIRC 2002

DPA Resilience Hardware - Differential Logic and Routing

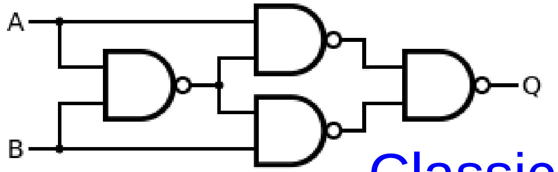
- Develop logic styles and routing techniques such that power consumption per cycle is constant and capacitance charged at a node is constant.



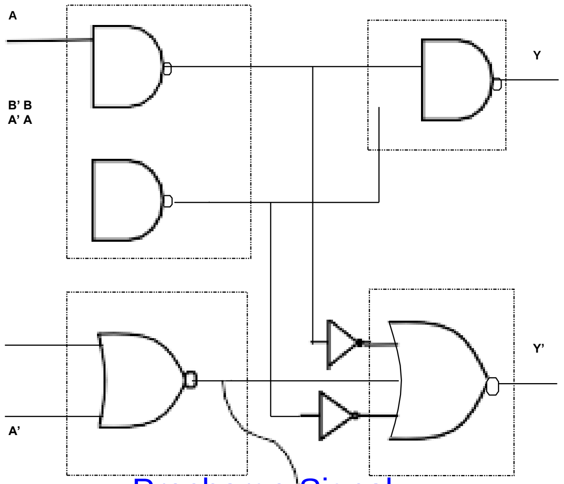
Vulnerable to side channel attack.

May abstract switching activity and reduce information leaking.

DPA Resilience Hardware - Differential Logic and Routing

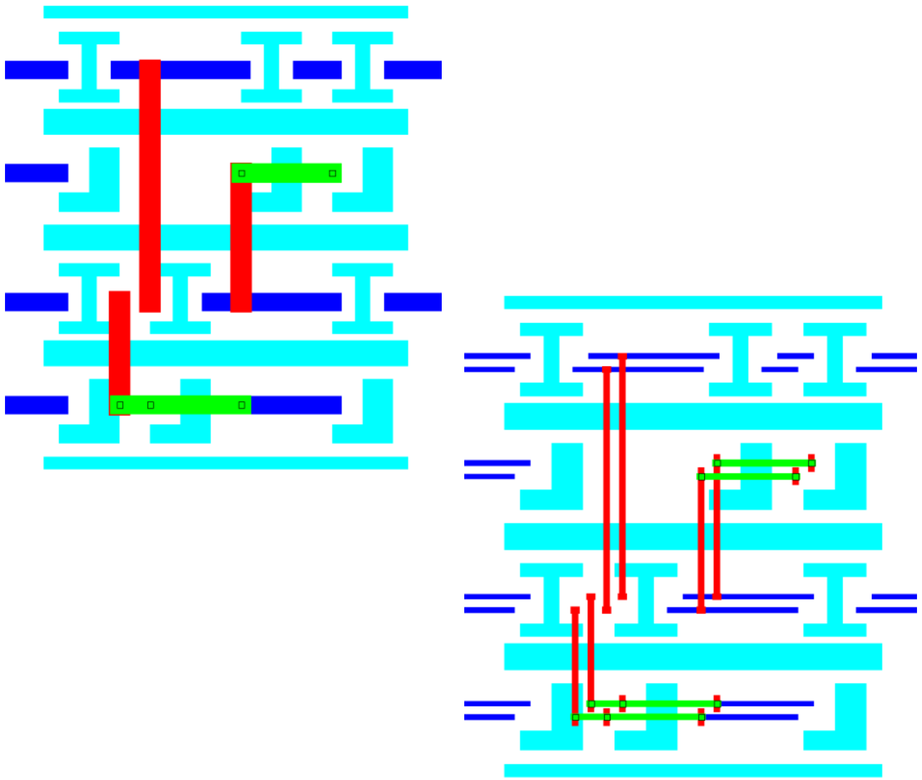


Classic XOR



Reduced Complementary Dynamic and Differential Logic (RCDDL) XOR

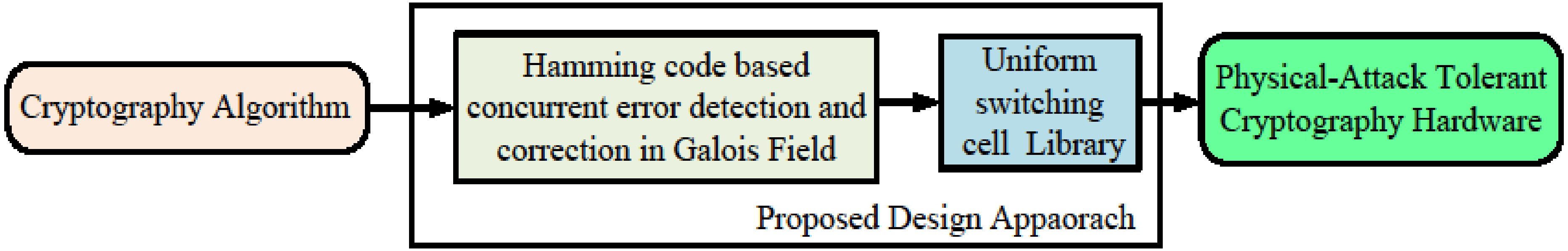
Source: Rammohan VLSID 2008

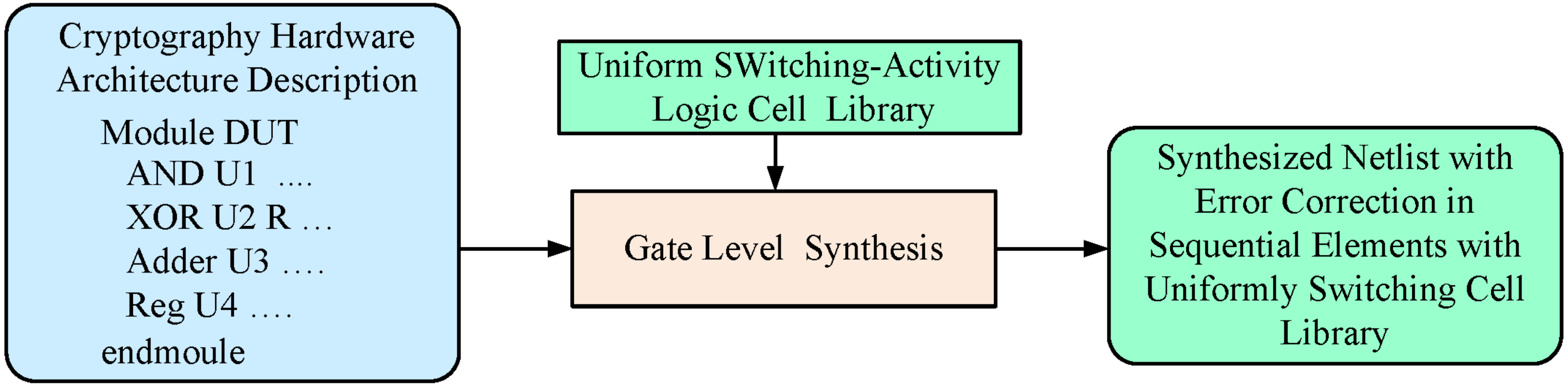


Differential Routing

Source: Schaumont IWLS 2005

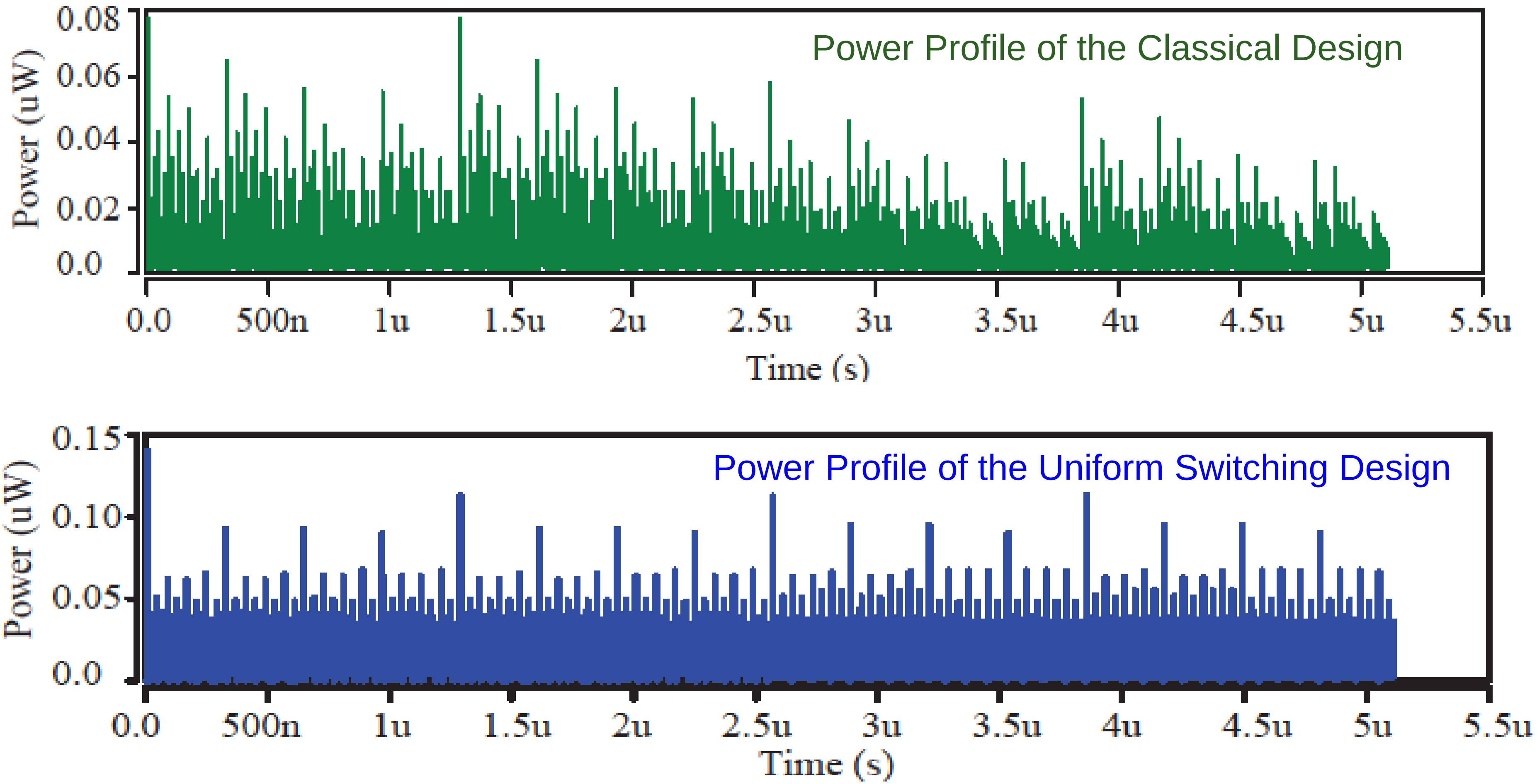
DPA Resilience Hardware - Synthesis Flow





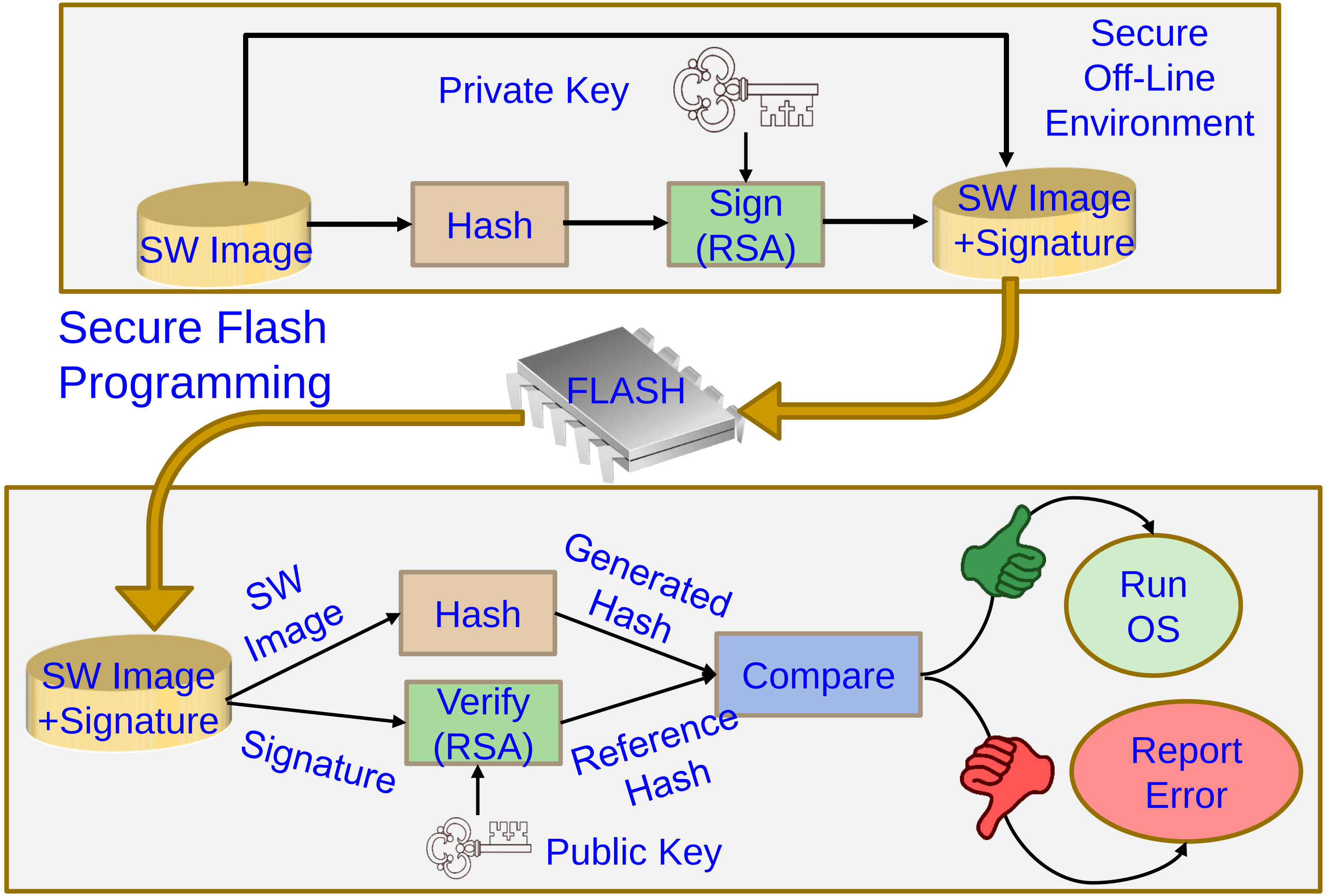
Source: Mohanty 2013, Elsevier CEE 2013

DPA Resilience Hardware



Source: Mohanty 2013, Elsevier CEE 2013

Firmware Security



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

Multimedia Piracy – Movie/Video

Piracy Threat Level: High → Low

- Studio
- Cinema
- On-line
- Video on Demand
- DVD/Blu-ray
- Pay-TV Broadcasting
- Free-to-Air Broadcasting

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

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

Multimedia Piracy – Music/Audio

"The U.S. economy loses $12.5 billion in total output annually as a consequence of music theft."

Source: https://www.riaa.com/reports/the-true-cost-of-sound-recording-piracy-to-the-u-s-economy/

DRM - Definition

- Digital Rights Management (DRM) is a generic term that refers to any of several technologies used by publishers, creators, or owners to control access and usage of digital data.
- Typically a DRM system:
  - Protects intellectual property by encrypting the data so that it can only be accessed by authorized users.

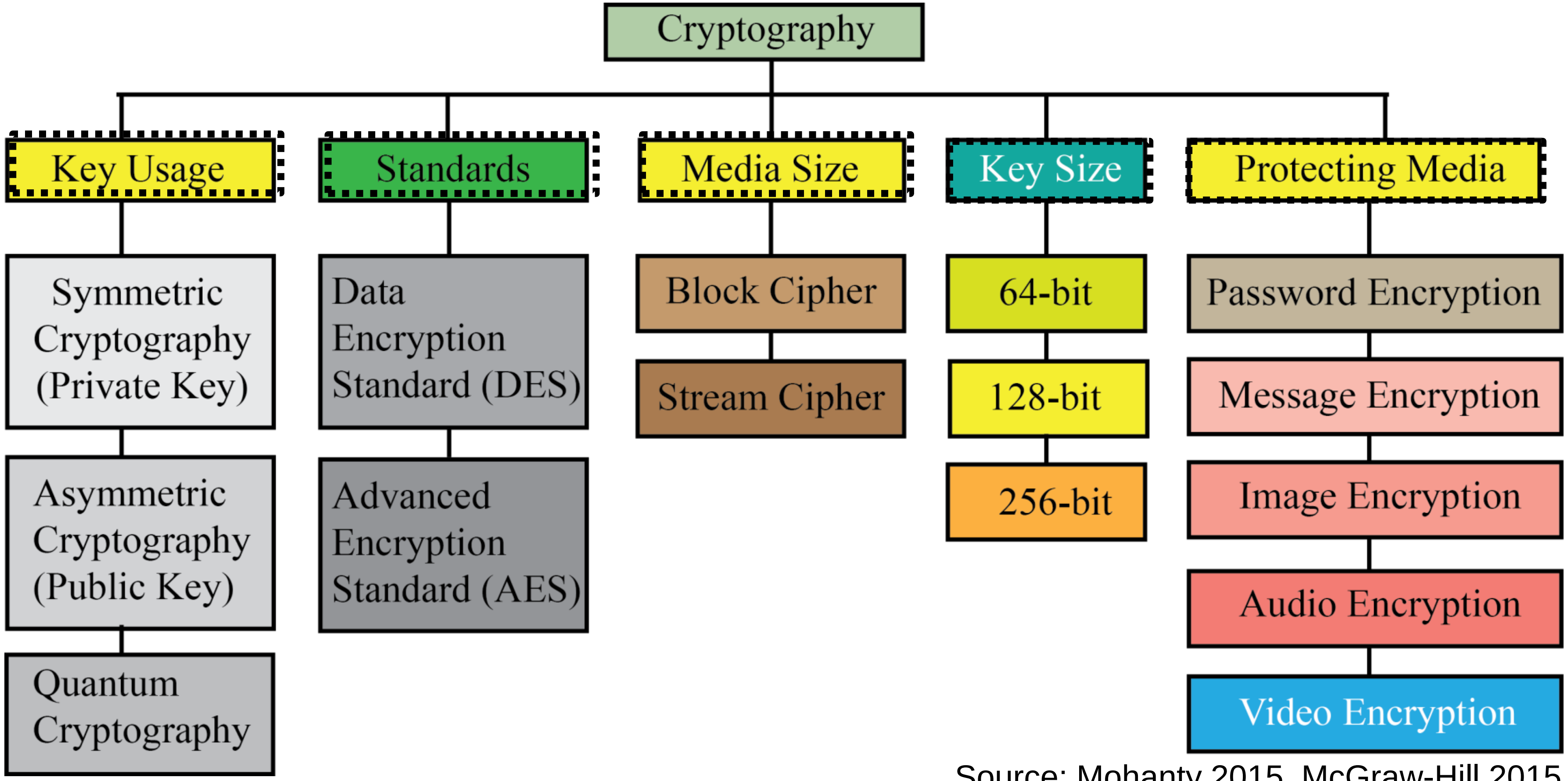
    and/or

  - Marks the content with a digital watermark so that the content can not be freely distributed.

DRM - Techniques

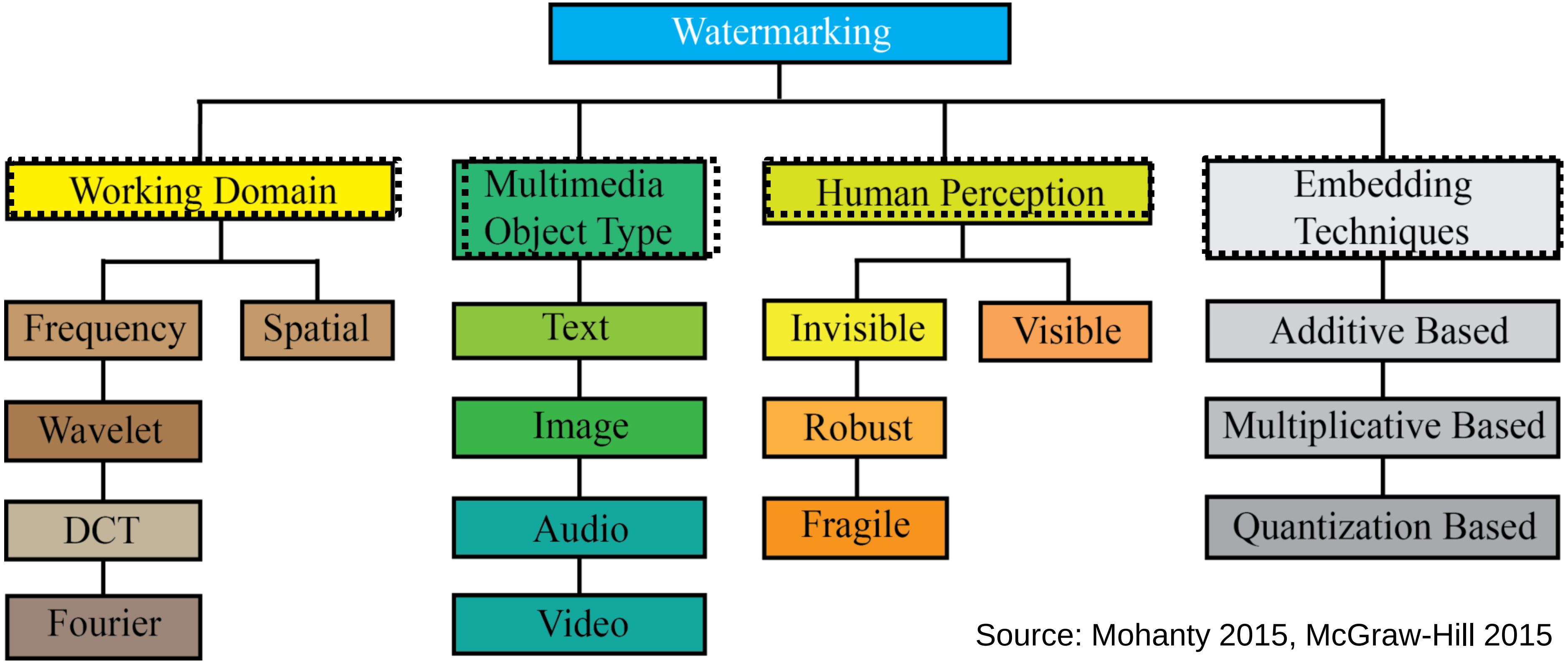
- Encryption
- Watermarking
- Scrambling
- Digital certificates
- Secure communications protocols
- Fingerprinting
- Hashing
- …… and more

Information Protection - Cryptography



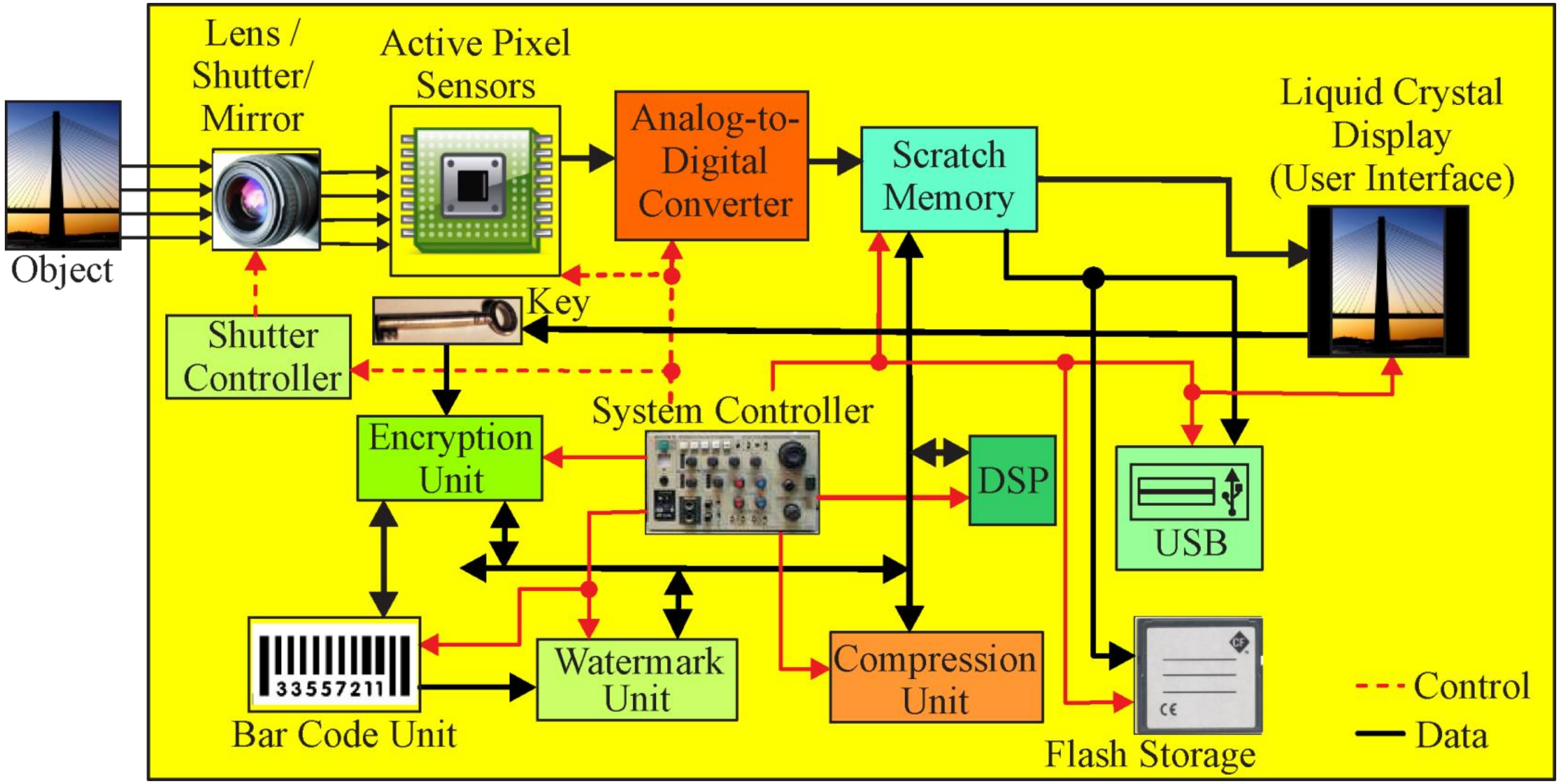
Source: Mohanty 2015, McGraw-Hill 2015

Copyright Protection - Watermarking



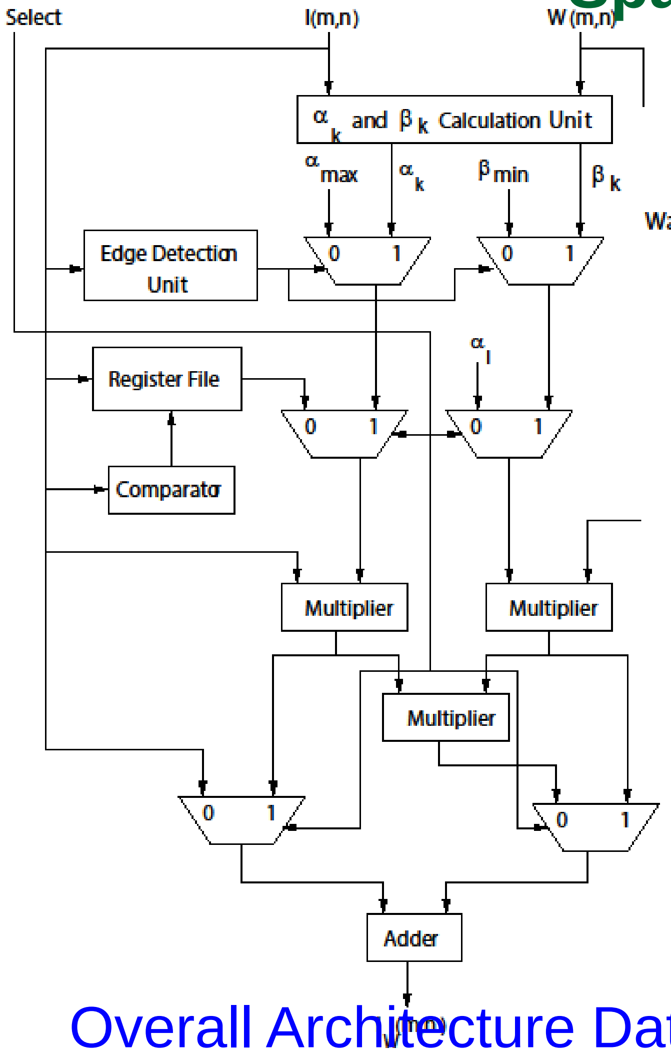
Source: Mohanty 2015, McGraw-Hill 2015

A DRM Hardware Integrated CE System – Secure Digital Camera (SDC) Example

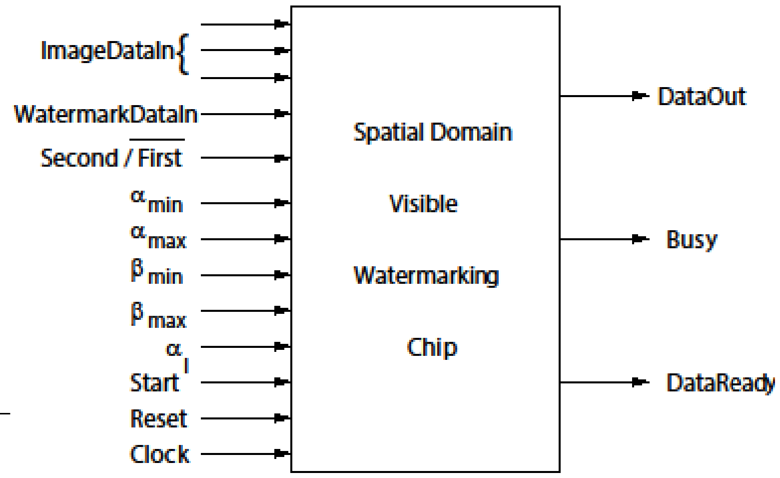


Source: Mohanty 2017, CE Magazine July 2017; Mohanty 2009, JSA Oct 2009

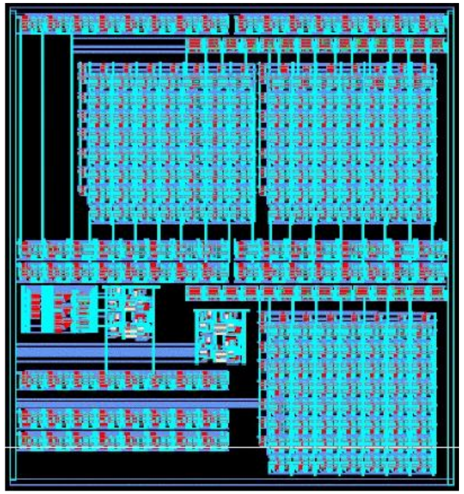
Copyright Protection Hardwares – Spatial Domain Watermarking



Overall Architecture Datapath



Chip Pin Diagram



Hardware Layout

Physical Design Data

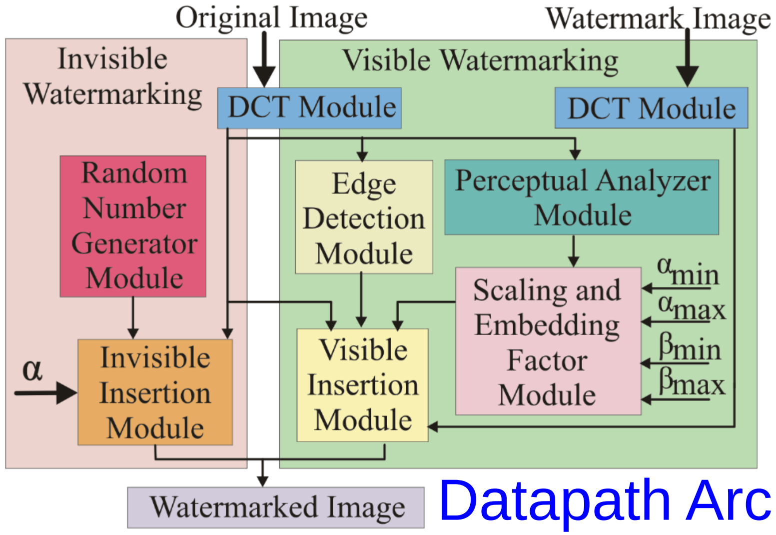
Total Area : 9.65 sq mm

No. of Gates: 28469

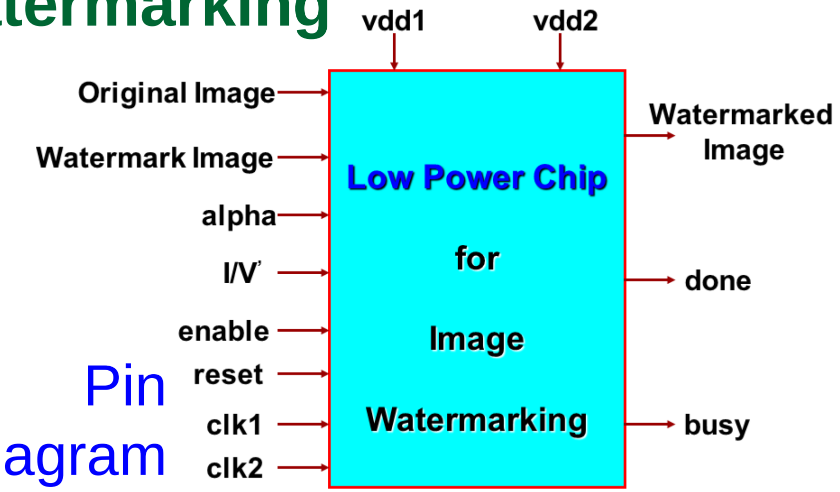
Power consumption: 6.92 mW

Source: Mohanty 2005, TVLSI Aug 2005

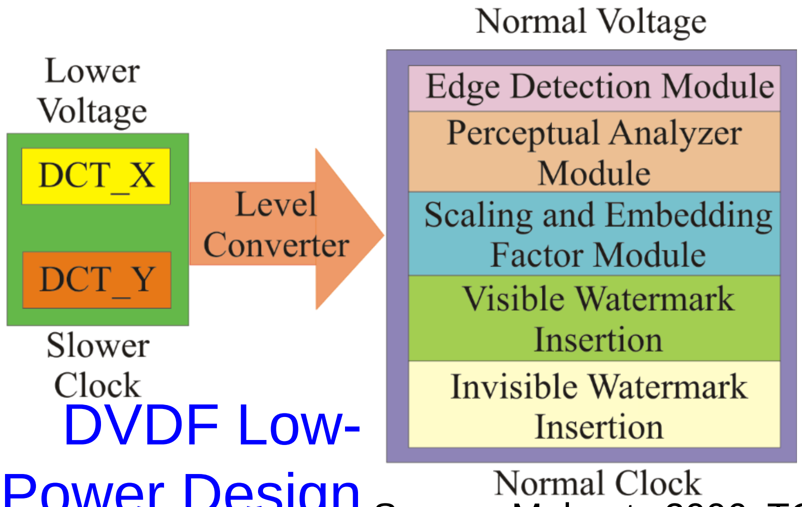
Copyright Protection Hardwares – DCT Domain Watermarking



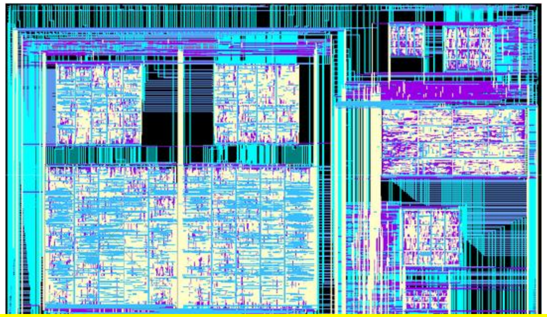
Datapath Architecture



Pin Diagram



DVDF Low-Power Design

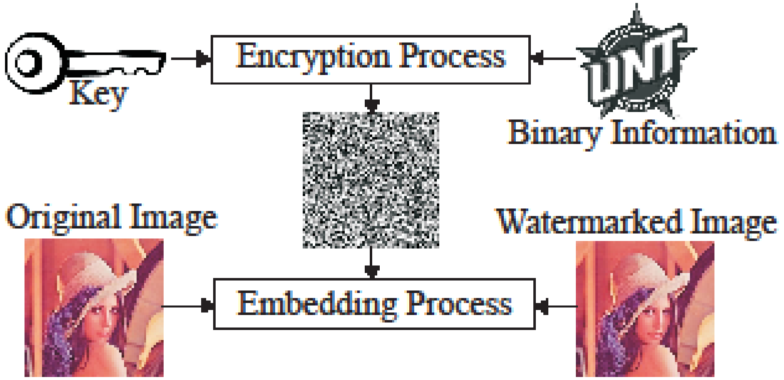


Hardware Layout

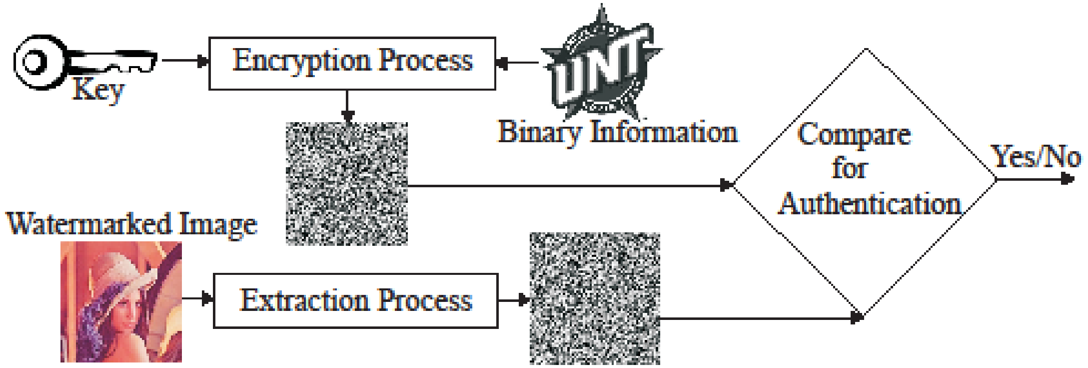
Physical Design Data
Total Area : 16.2 sq mm
No. of Transistors: 1.4 million
Power Consumption: 0.3 mW

Source: Mohanty 2006, TCASII May 2006

DRM Hardwares – CyptMark: Encryption + Watermarking

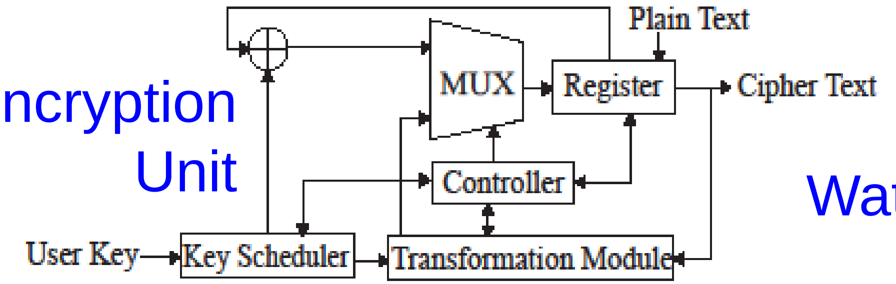


CryptMark: Embedding

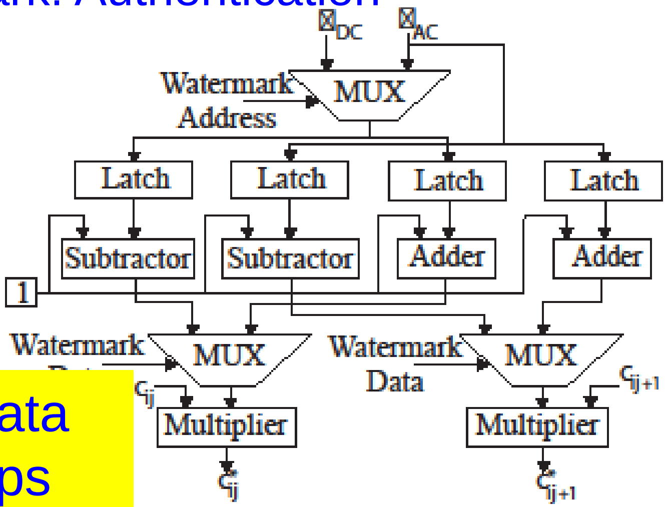


CryptMark: Authentication

Encryption Unit



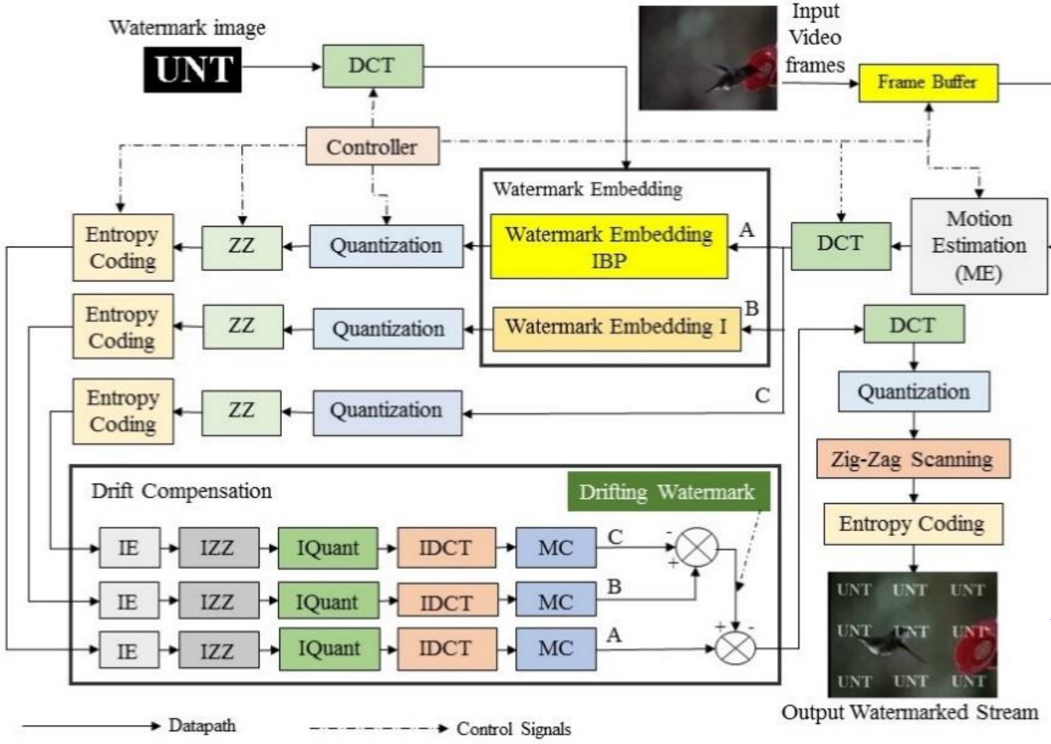
Watermarking Unit



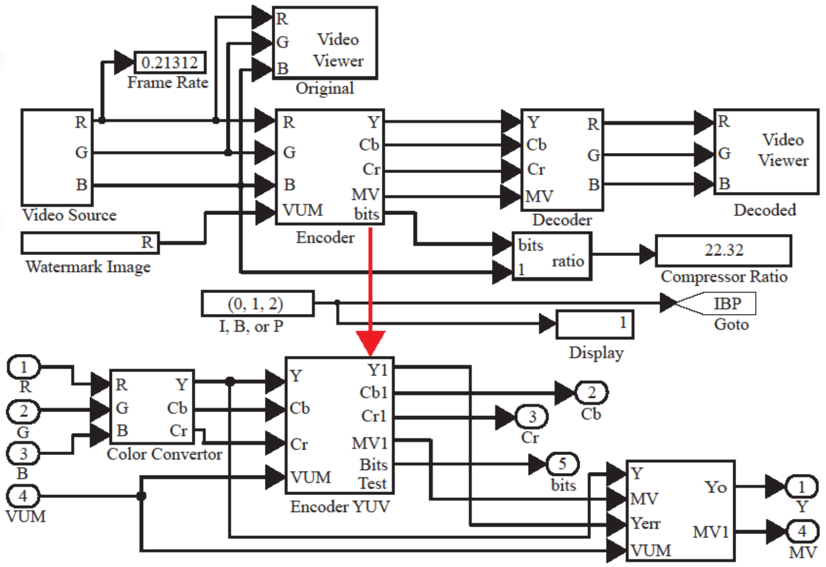
FPGA Prototyping Data
Throughput: 2.48 Gbps
Power Dissipation: 39.8 mW

FPGA Prototyping Data
hroughput: 544.2 Mbps
ower Dissipation: 3.7 mW

Copyright Protection Hardware –
MPEG-4 Video Watermarking



Video Watermarking Architecture Datapath

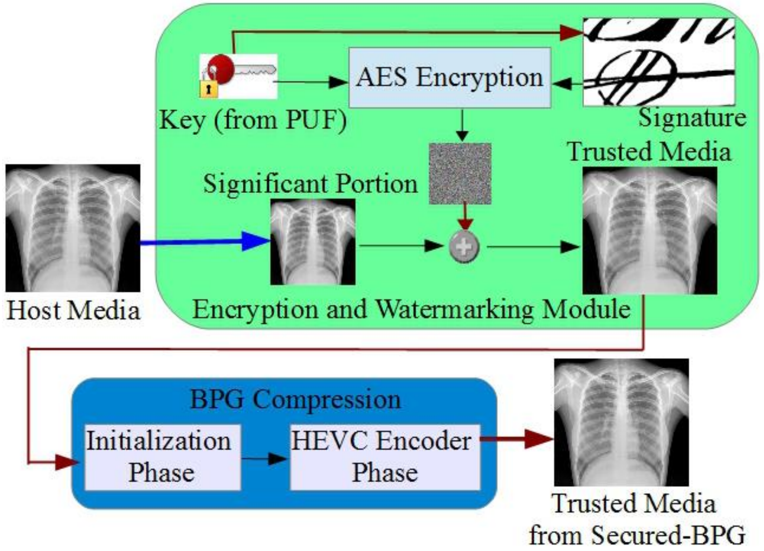


Video Watermarking Architecture: Simulink Model

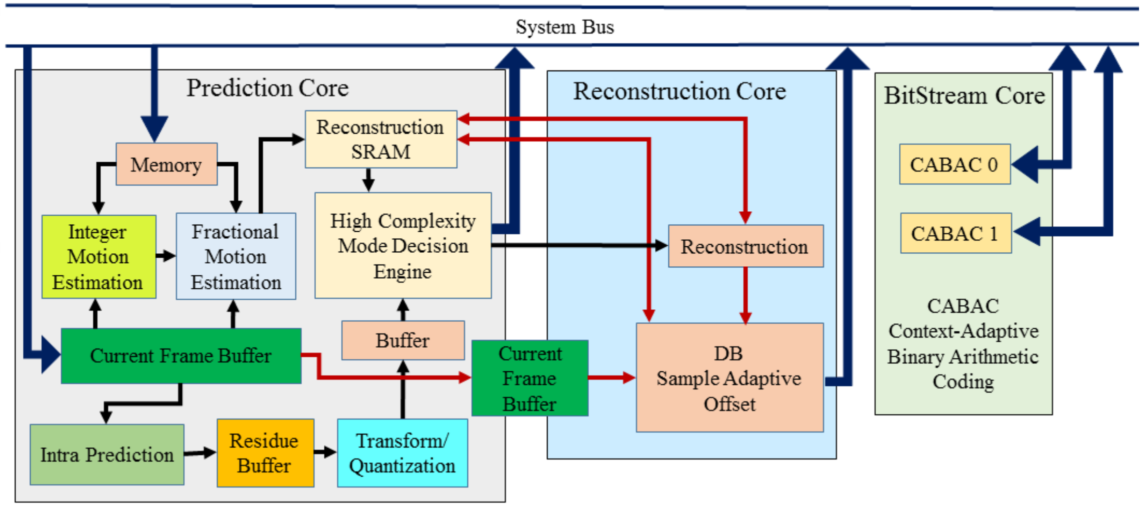
FPGA Prototyping
Throughput: 44 frames/sec
Logic Elements in FPGA Prototyping : 28322

Source: Mohanty 2011, JSS May 2011

DRM Hardware - Secure Better Portable Graphics (SBPG)



Idea of Secure BPG (SBPG)

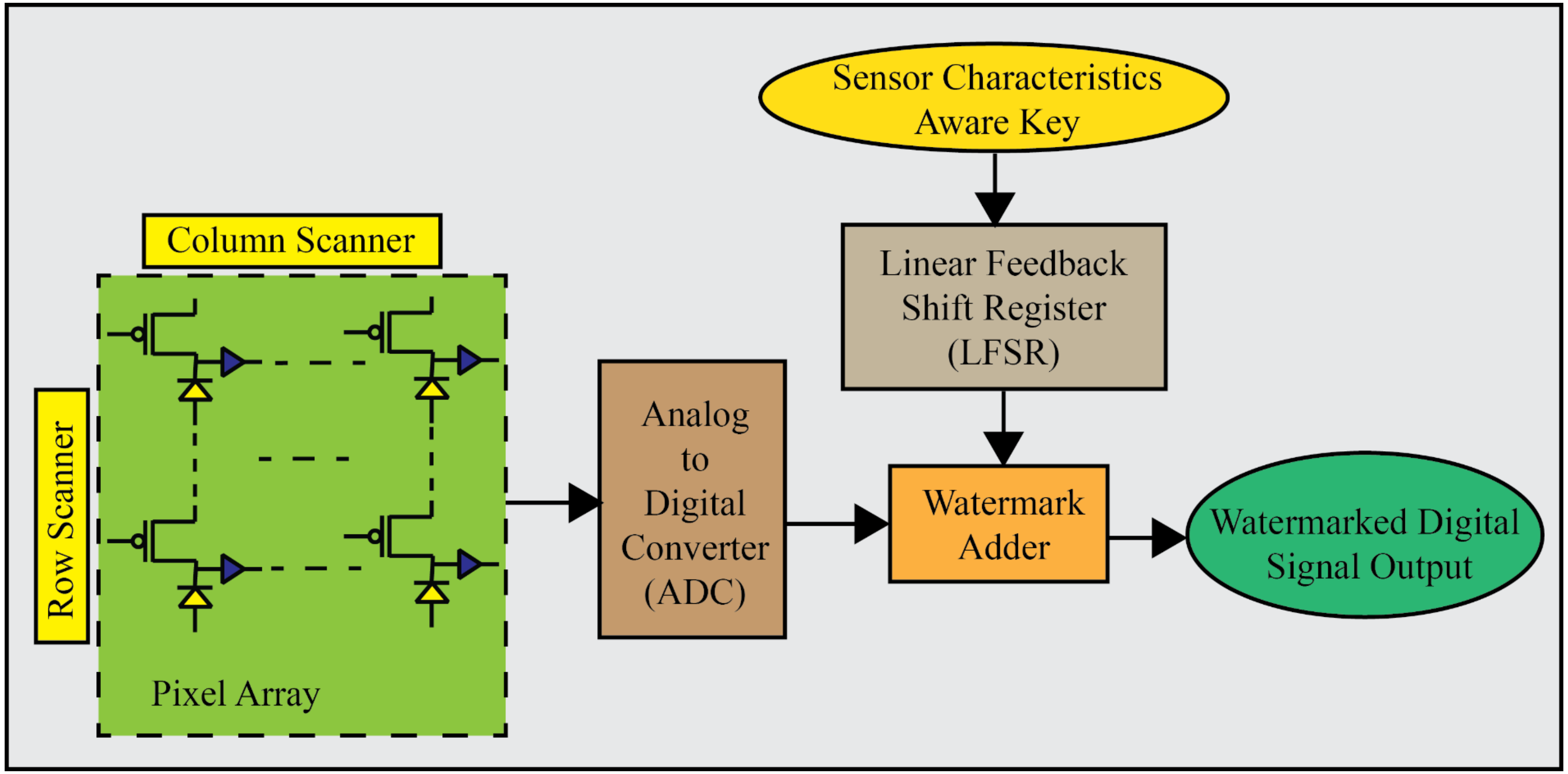


High-Efficiency Video Coding Architecture

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

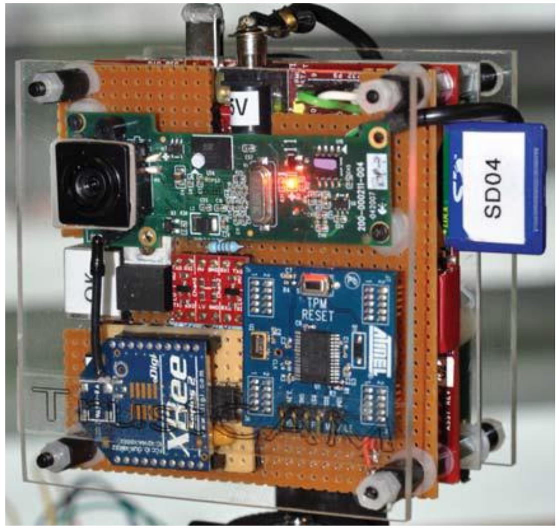
Source: Mohanty 2016, ISVLSI 2016 and EuroSimE 2016

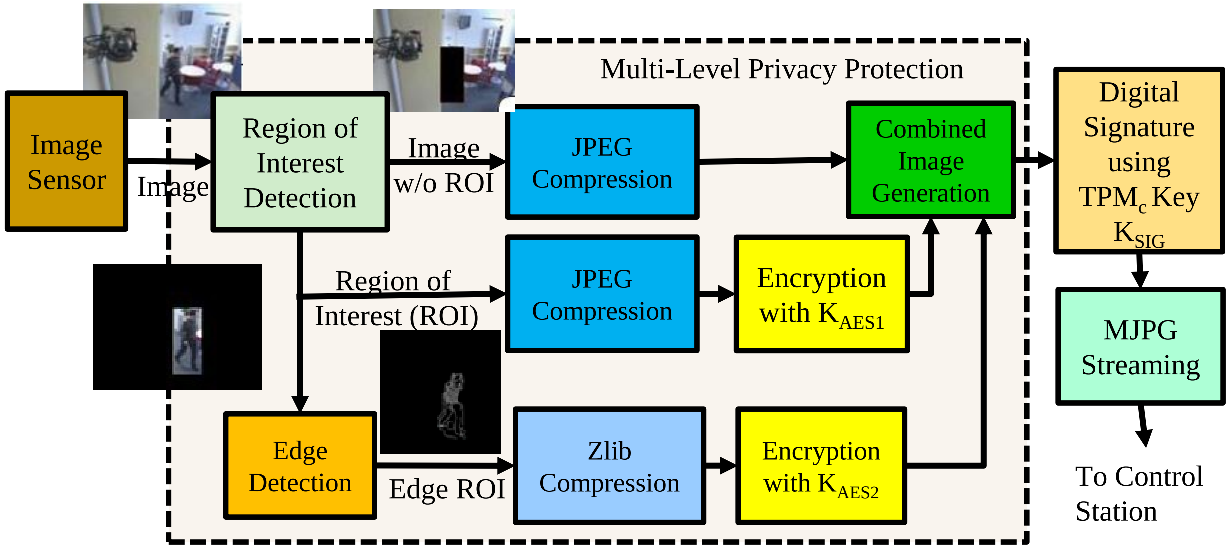
Secure Image Sensors



Source: Mohanty 2015, McGraw-Hill 2015

TrustCAM - Security and Privacy





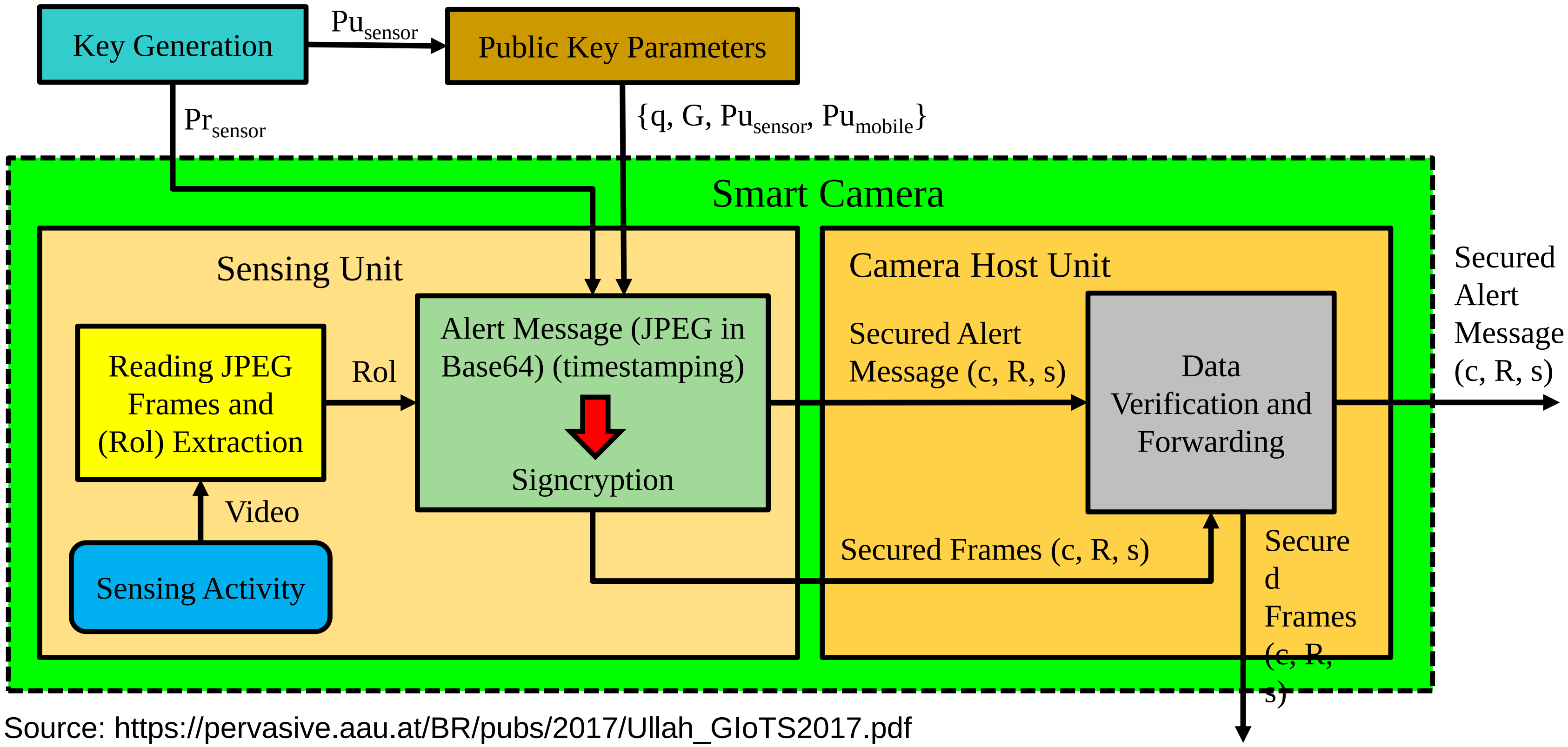
For integrity protection, authenticity and confidentiality of image data.

- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

Source: https://pervasive.aau.at/BR/pubs/2010/Winkler_AVSS2010.pdf

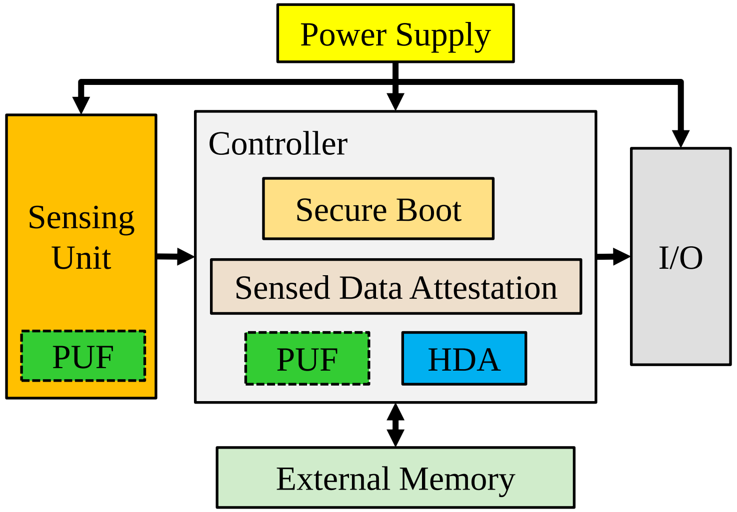
Smart Cameras with Signcryption

- Signcryption is a resource-efficient technique which implements signature and encryption in a single step for lower computational and communications overhead.

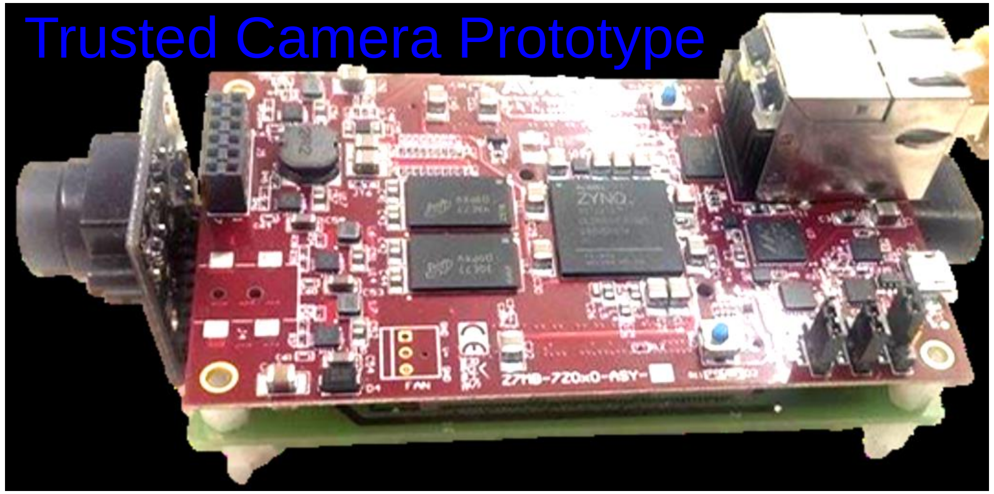


Source: https://pervasive.aau.at/BR/pubs/2017/Ullah_GIoTS2017.pdf

PUF-based Trusted Sensor



PUF-based Trusted Sensor



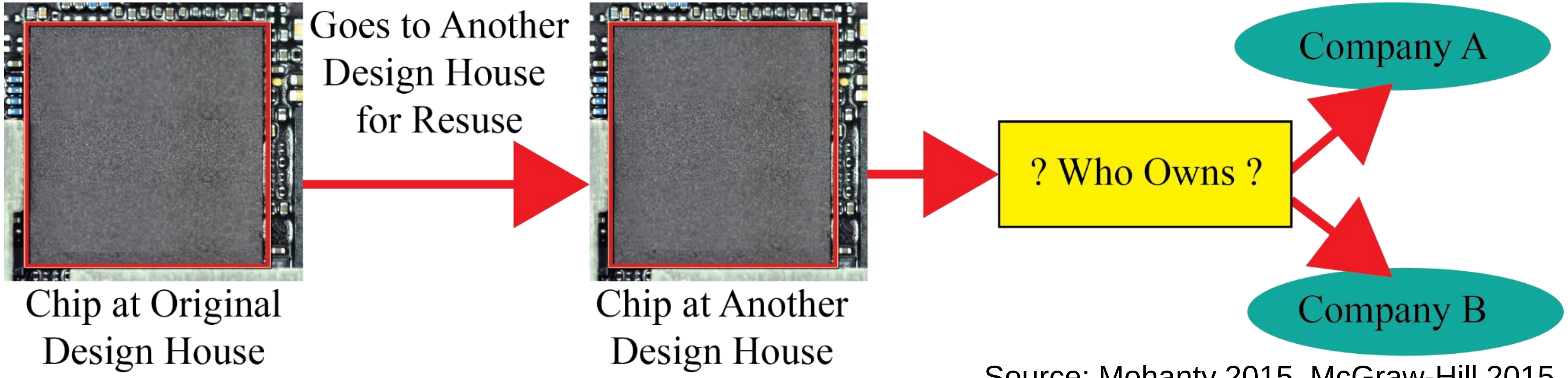
Source: https://pervasive.aau.at/BR/pubs/2016/Haider_IOTPTS2016.pdf

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.
  - 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)

Hardware Intellectual Property Issue

- Intellectual property blocks or reusable virtual components are used as a cost effective solution but sharing of such blocks for SoC design poses a severe security and ownership issues.
- DFX needs to consider this important issue for the protection of circuit for which watermarking is considered as a solution.
- In this case, watermarking is an identification code, imperceptible to human or machine analysis that is permanently embedded as an integral part within a design.

Hardware Reverse Engineering

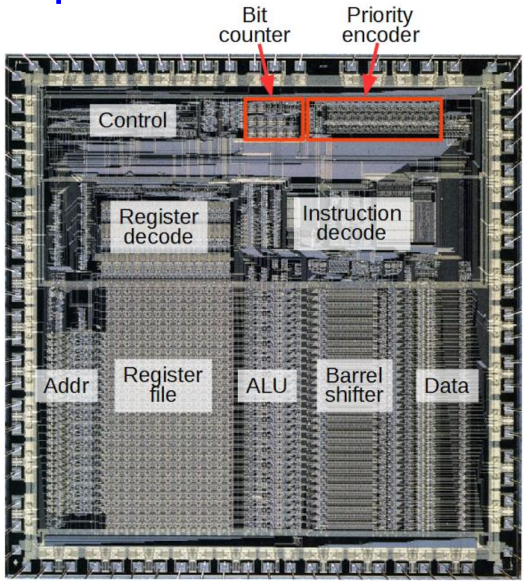
Source: http://legacy.lincolninteractive.org/html/CES%20Introduction%20to%20Engineering/Unit%203/u3l7.html

CE System disassembly Subsystem identification, modification

Source: https://www.slideshare.net/SOURCEConference/slicing-into-apple-iphone-reverse-engineering

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

Chip-Level Modification



Source: http://pic-microcontroller.com/counting-bits-hardware-reverse-engineering-silicon-arm1-processor/

Counterfeit Hardware

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%)

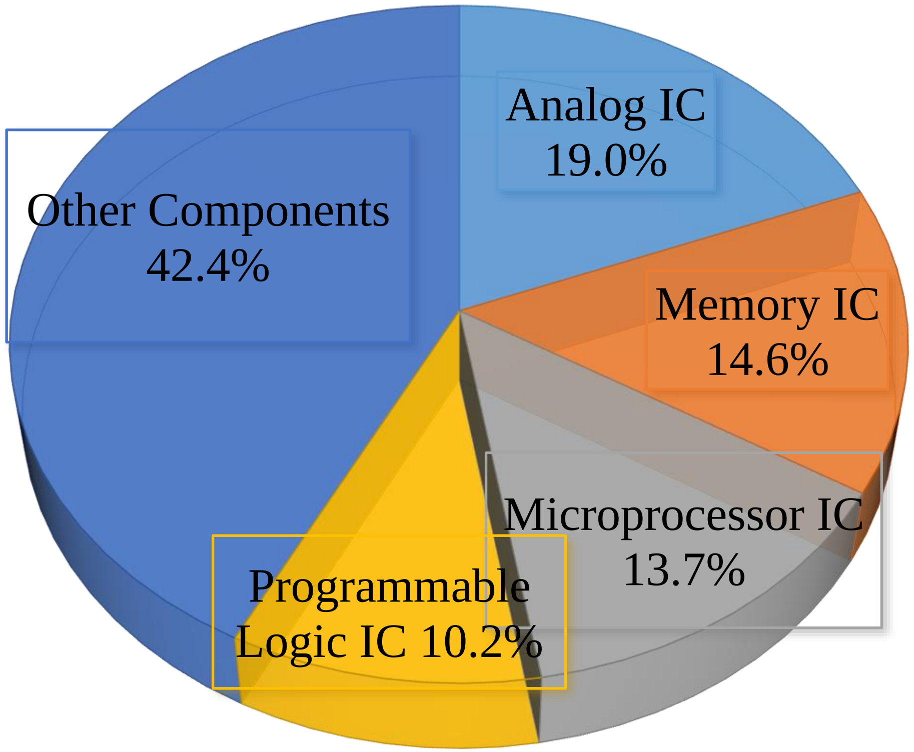
Data Processing
$6.0 billion (11%)

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.

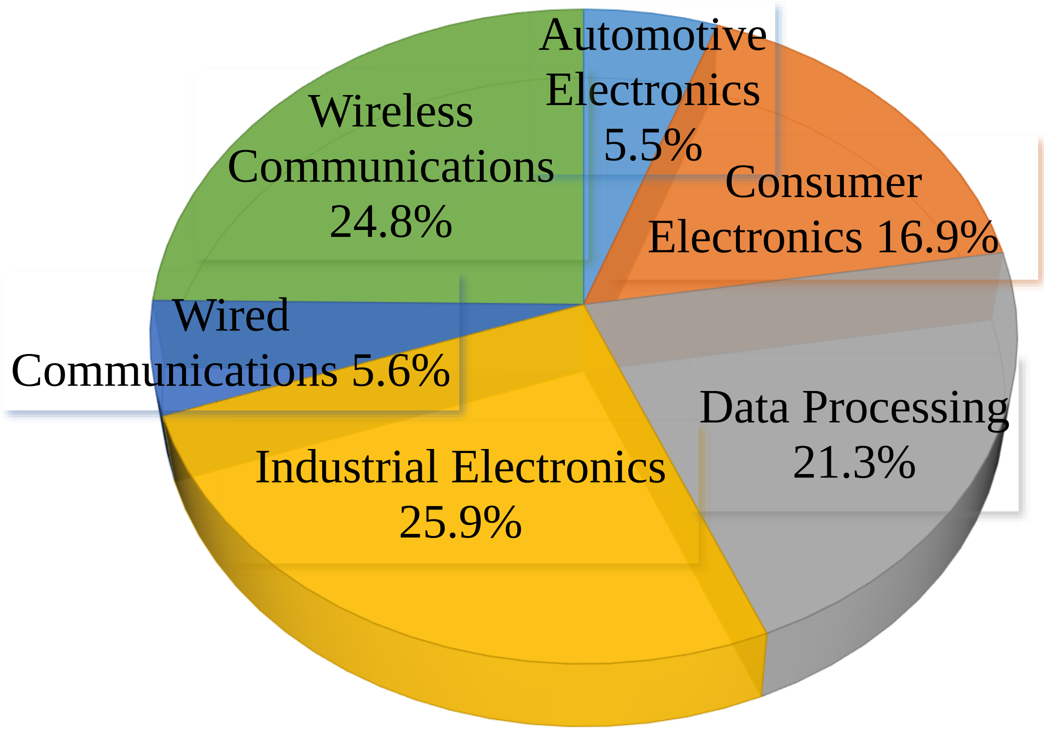
Counterfeit Hardware



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

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

Worldwide Electronics Revenue



- Worldwide OEM factory revenue is more than 2 trillion dollars currently.

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

Cloned/Fake Electronics Hardware – Example - 1

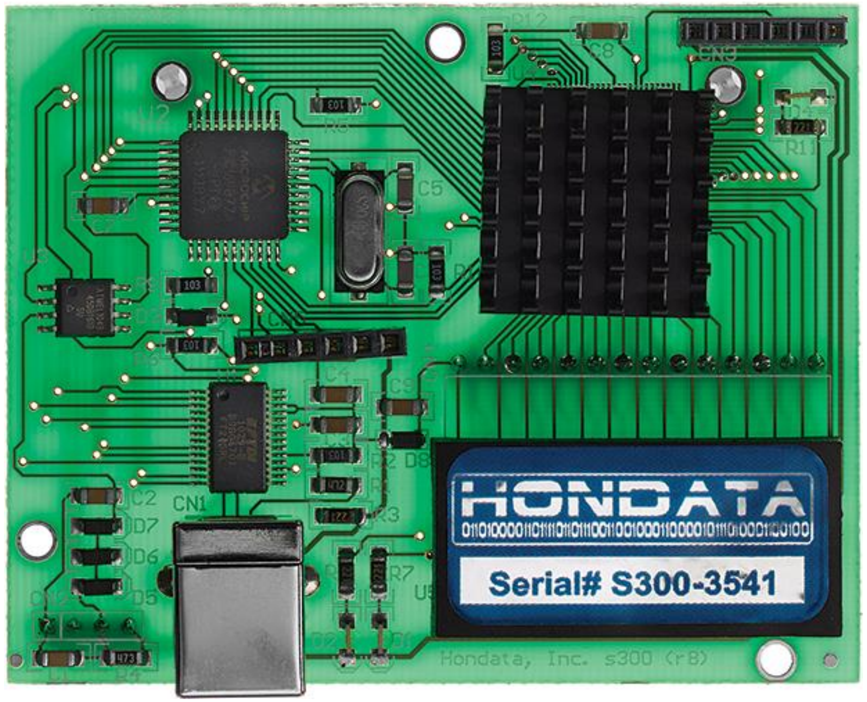
Source: https://petapixel.com/2015/08/14/i-bought-a-fake-nikon-dslr-my-experience-with-gray-market-imports/

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

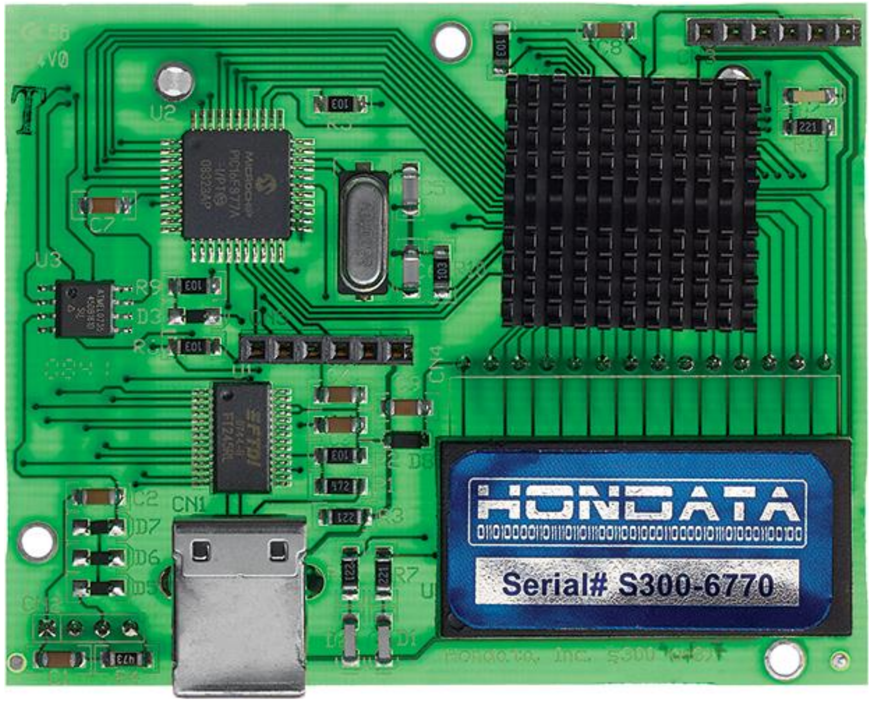
Source: http://www.cbs.cc/fake-capacity-usb-drives/

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

Cloned/Fake Electronics Hardware – Example - 3

Fake Authentic

A typical rechargeable battery in a typical CE

Source: https://www.premiumbeat.com/blog/how-to-spot-counterfeit-camera-gear/

Cloned/Fake/Counterfeit Electronics

- Consumer Electronics is the 2nd most counterfeit product in USA.
- Between November 2007 and May 2010, U.S. Customs officials seized 5.6 million counterfeit microprocessors.
- The market value of the 2016 seized counterfeit goods, had they been genuine, amounted to $1.4 billion.

Source: https://www.scientificamerican.com/article/electronic-chip-counterfeit-china/

Source: http://247wallst.com/special-report/2017/04/29/10-most-counterfeited-products-in-america/

Cloned/Fake Electronics Hardware - What is the Problem? It is cheaper!

- Installing cloned hardware into networks can open door to hackers: man-in-the-middle attacks or secretly alter a secure communication path between two systems to bypass security mechanisms.
- Cloned hardware may lack the security modules intended to protect IoT devices, and so it opens up the user to cyberattack.
- If a hacker embeds a malicious hardware in a drone then he could shut it down or retarget it when it reached preset GPS coordinates.

Source: https://www.scientificamerican.com/article/electronic-chip-counterfeit-china/

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

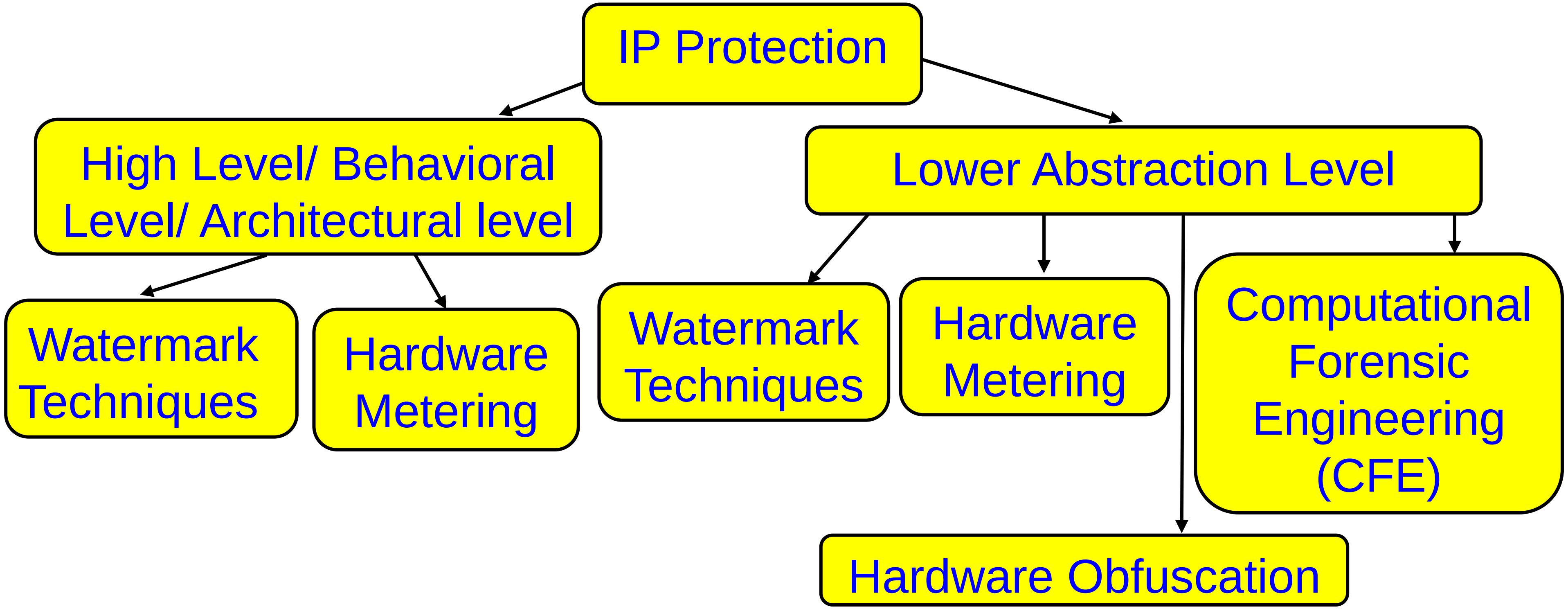
Cloned/Fake Electronics Hardware - What is the Problem? It is cheaper!

- Counterfeit battery can cause safety hazards.
- Counterfeit electronics embedded in missile guidance systems and aircrafts can have serious problems for the defense systems.
- According to the International AntiCounterfeiting Coalition, lost profits due to counterfeiting has resulted in the loss of more than 750,000 jobs in the United States.

Source: https://www.scientificamerican.com/article/electronic-chip-counterfeit-china/

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

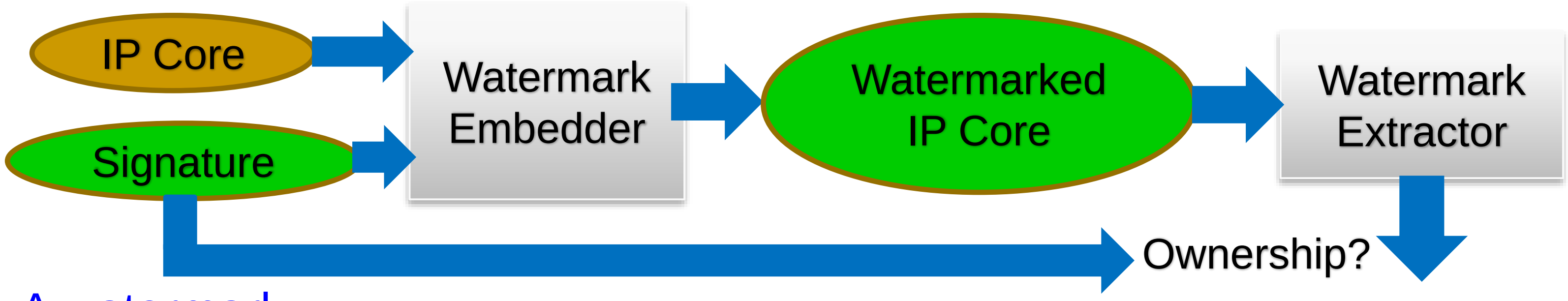
Selected Solutions for IP Protection



Source: Sengupta, Mohanty 2016, ISCAS 2016

Watermarking for Hardware IP Protection

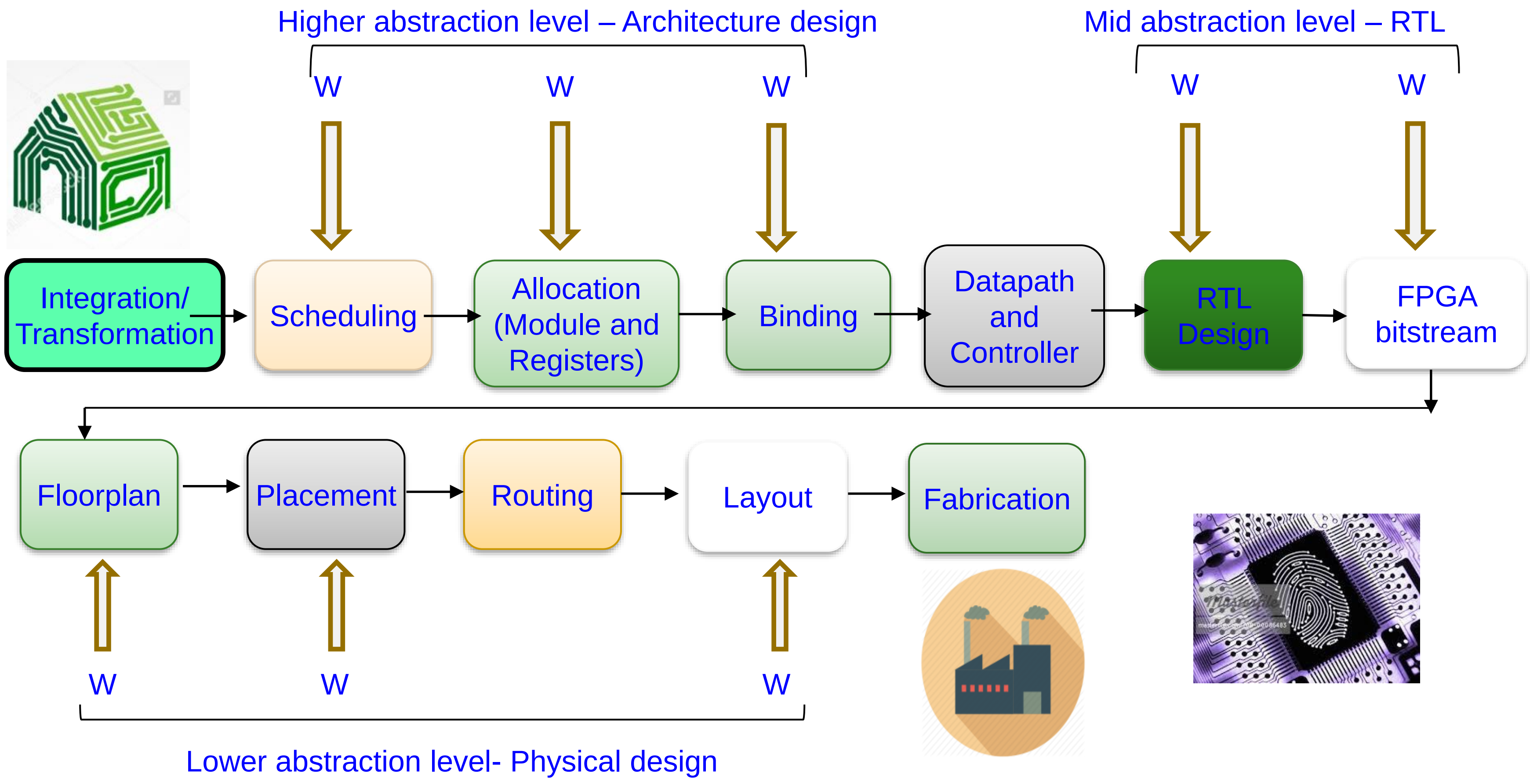
- A watermark is a signature of the owner embedded in a IP core.



- A watermark:
  - should be capable to identify the owner/creator of the design
  - should be robust and difficult to remove
  - should be resilient against attacks like: ghost signature and tampering
  - should have minimal embedding cost to obtain the watermarked design
  - should be embedded in the IP design with minimal computation effort
  - should be easy to detect signature at the genuine receivers end for the receiver who has full knowledge of the signature encoding rule

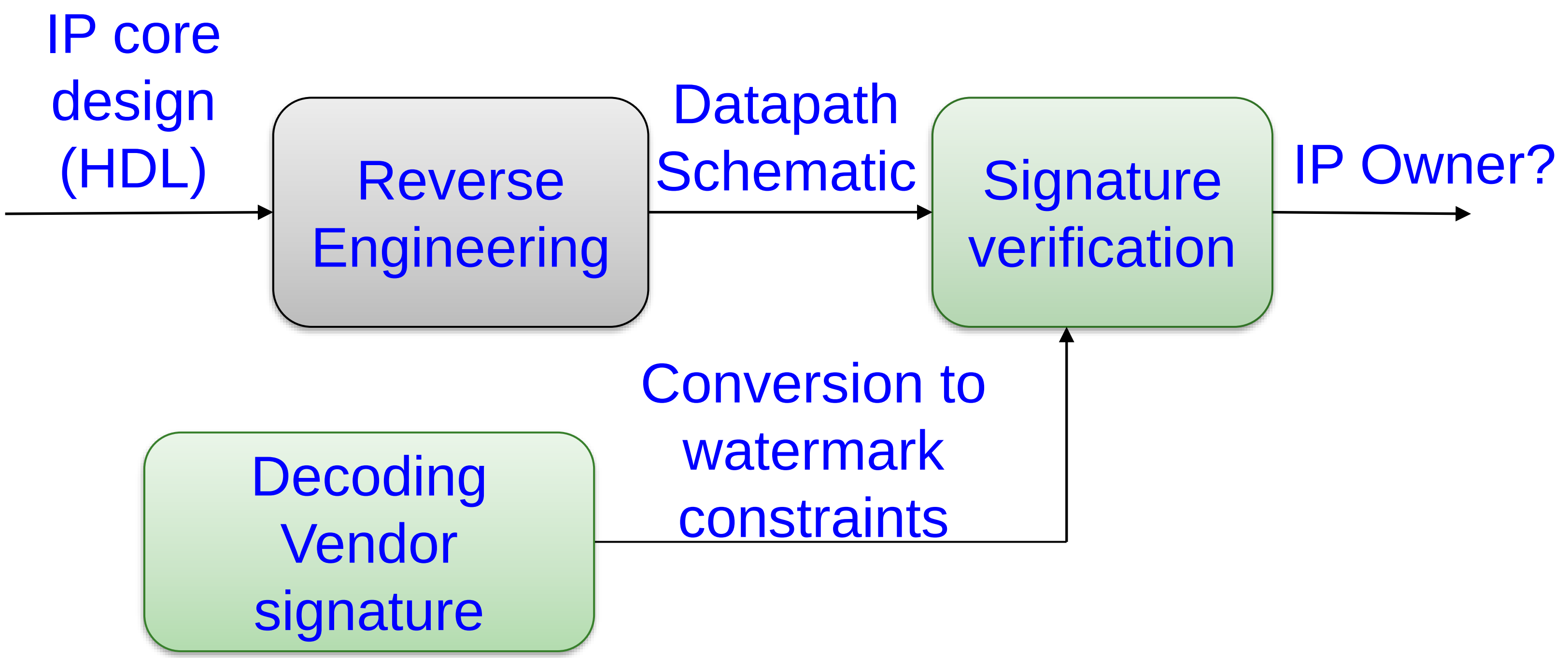
Source: Sengupta, Mohanty 2016, ISCAS 2016

Digital Hardware - Watermark



Source: Mohanty 2017: CE Magazine October 2017

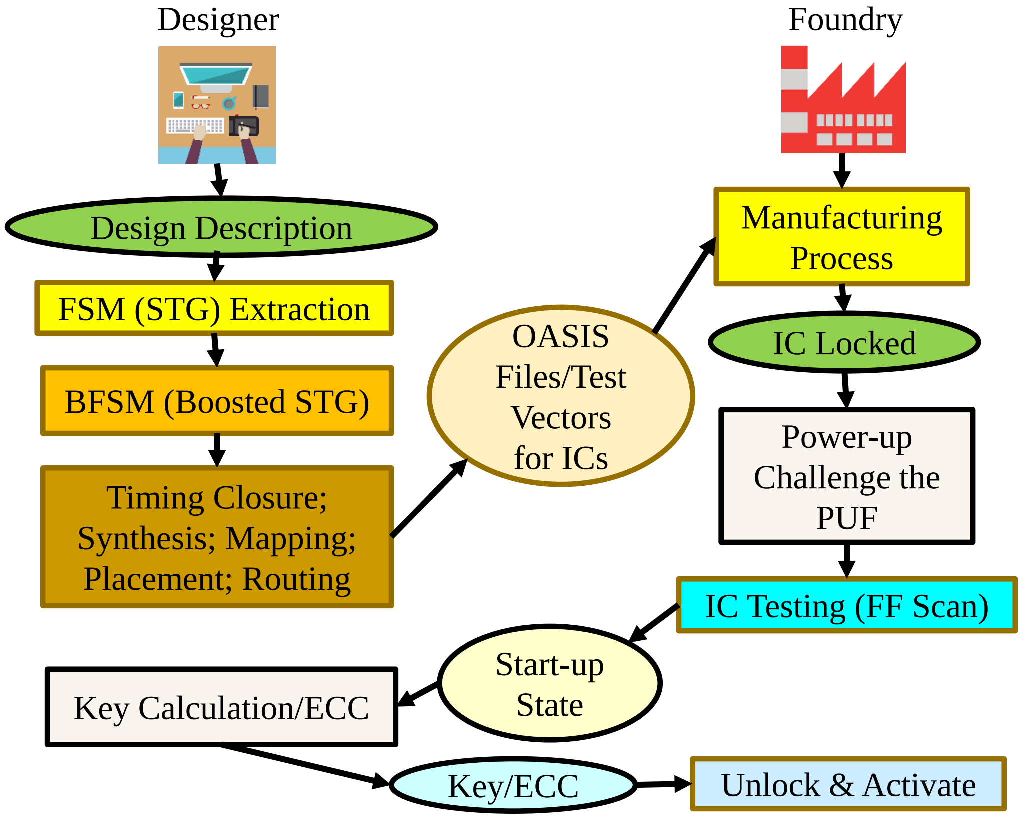
Watermark (W) Detection Process



Source: Mohanty 2017: CE Magazine October 2017

Digital Hardware – IP Metering

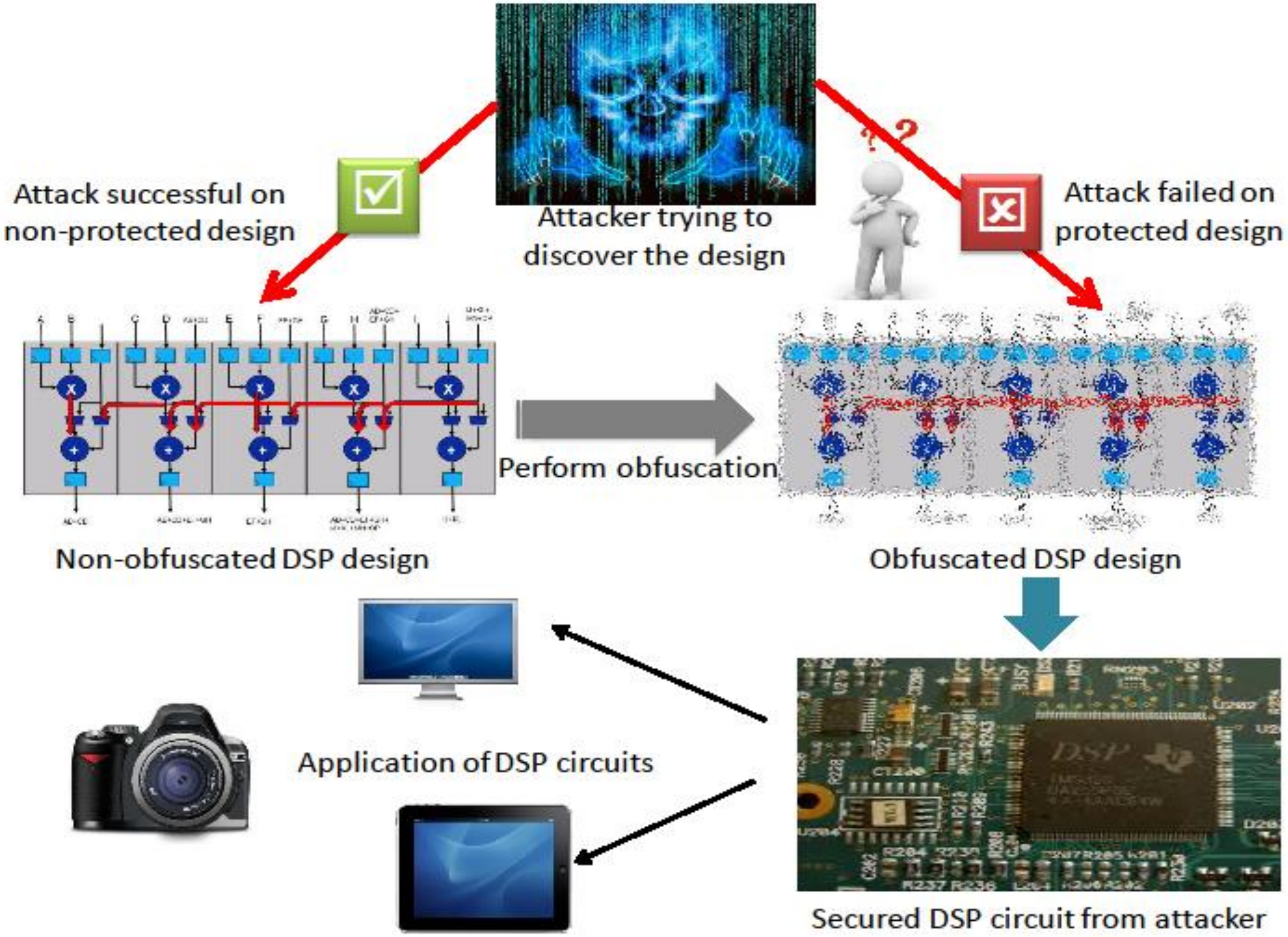
- Hardware metering enables the design house to gain post-fabrication control by:
  - Passive or active control of the number of manufactured ICs from one design
  - The properties of IC and its usage
  - Remote runtime monitoring and disabling



A global flow for active hardware metering.

Source: http://www.glsvlsi.org/archive/glsvlsi11/Koushanfar_MeteringGLS-VLSI.pdf

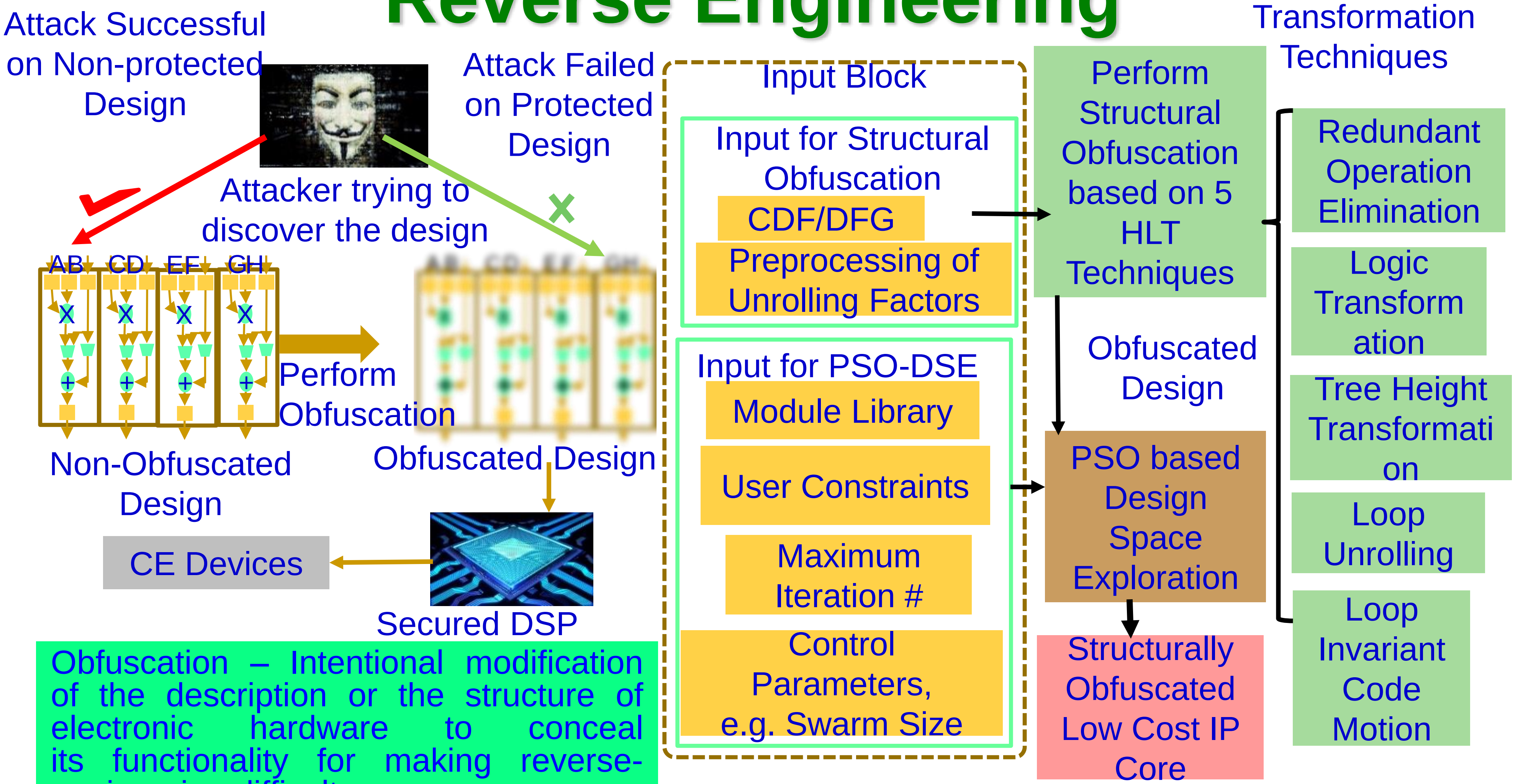
Digital Hardware – Obfuscation



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

Source: Sengupta, Mohanty 2017, TCE November 2017

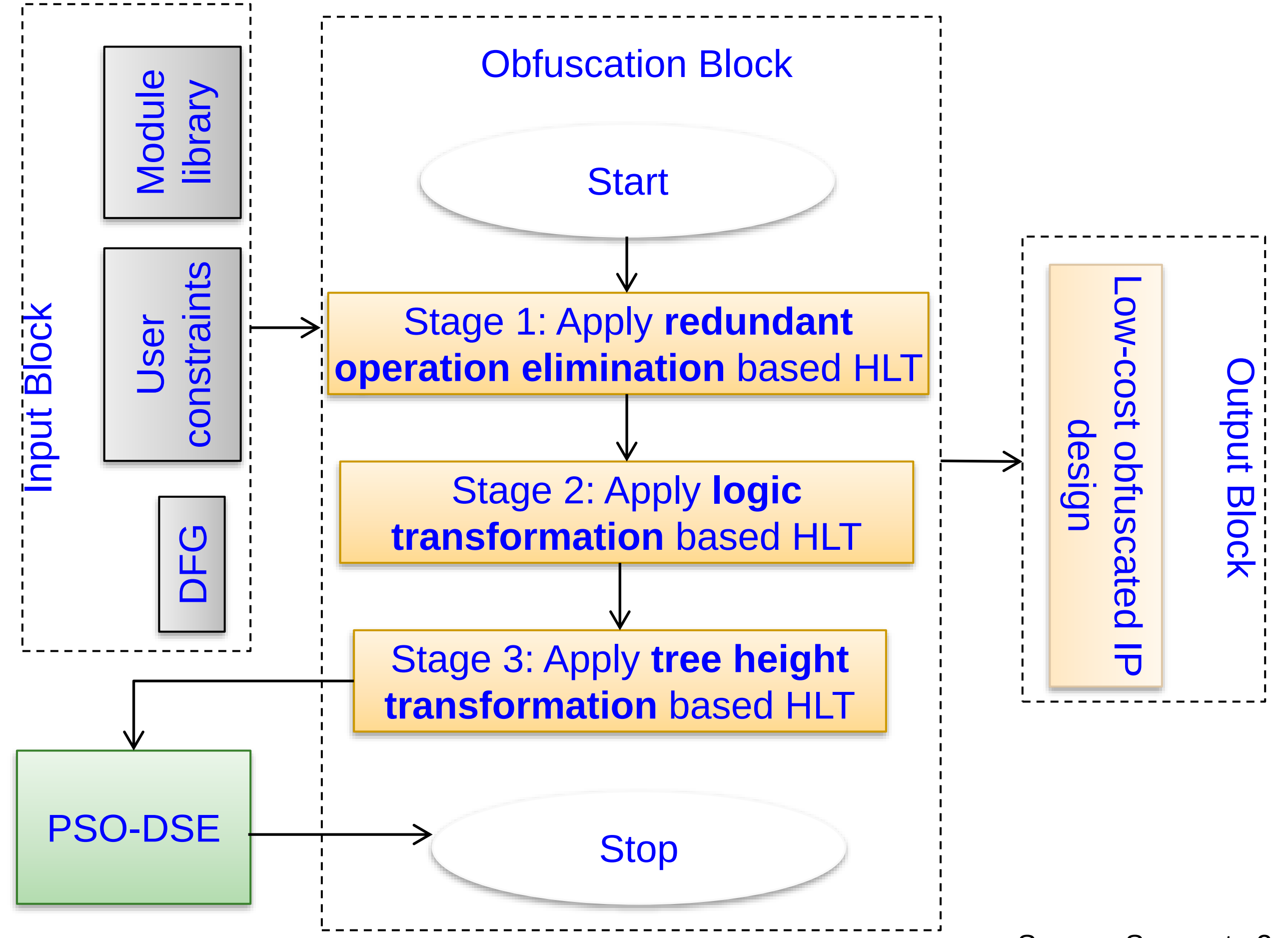
Digital Hardware Synthesis to Prevent Reverse Engineering



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

Source: Sengupta, Mohanty 2017, TCE November 2017

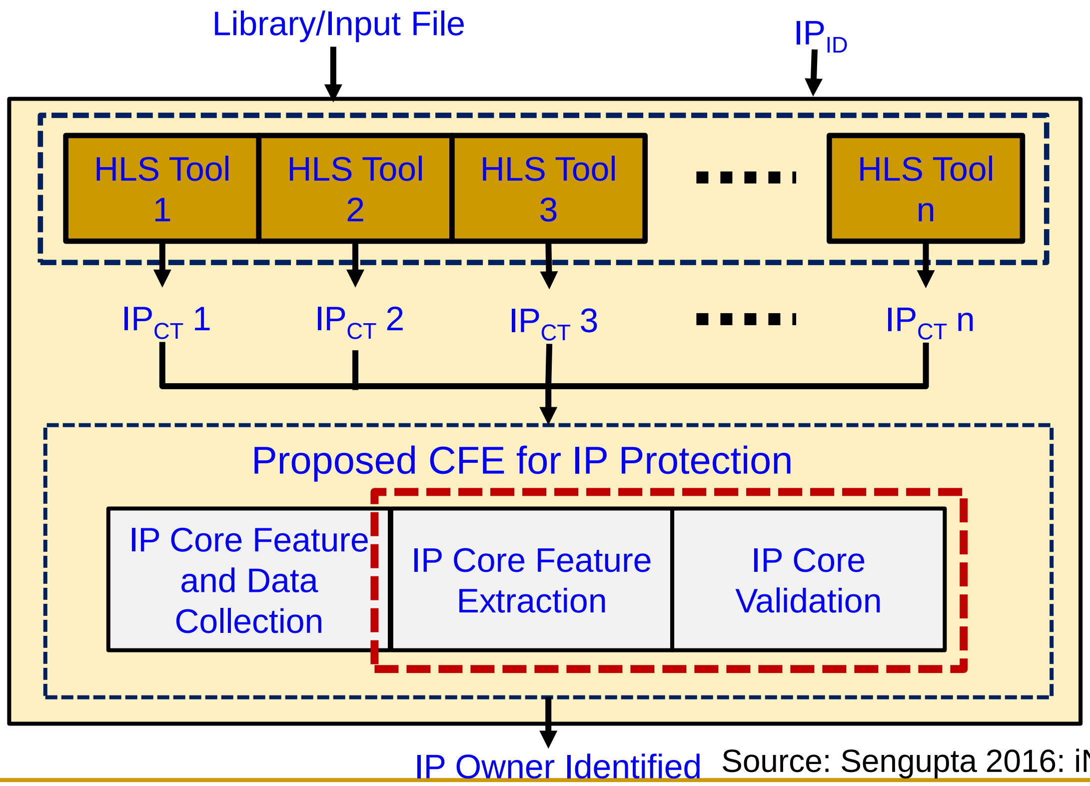
Digital Hardware – Architecture Level Obfuscation Method



Source: Sengupta 2017: IET EL 2017

Digital Hardware – Computational Forensic Engineering (CFE)

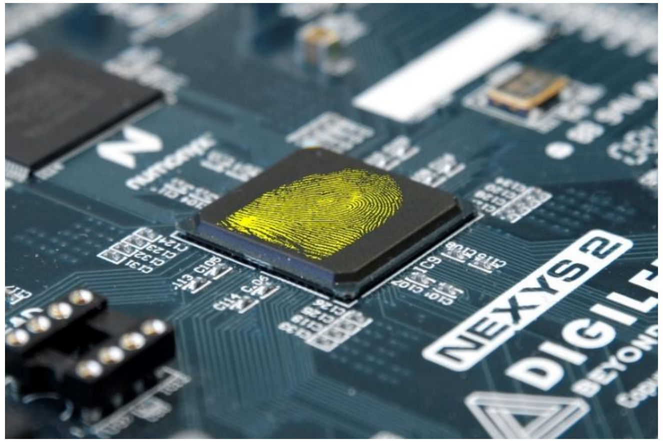
CFE aims to identify the entity that created the IP by analyzing certain features of a given IP and quantizes the likelihood that a specific entity has created it.



Source: Sengupta 2016: iNIS 2016

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.”

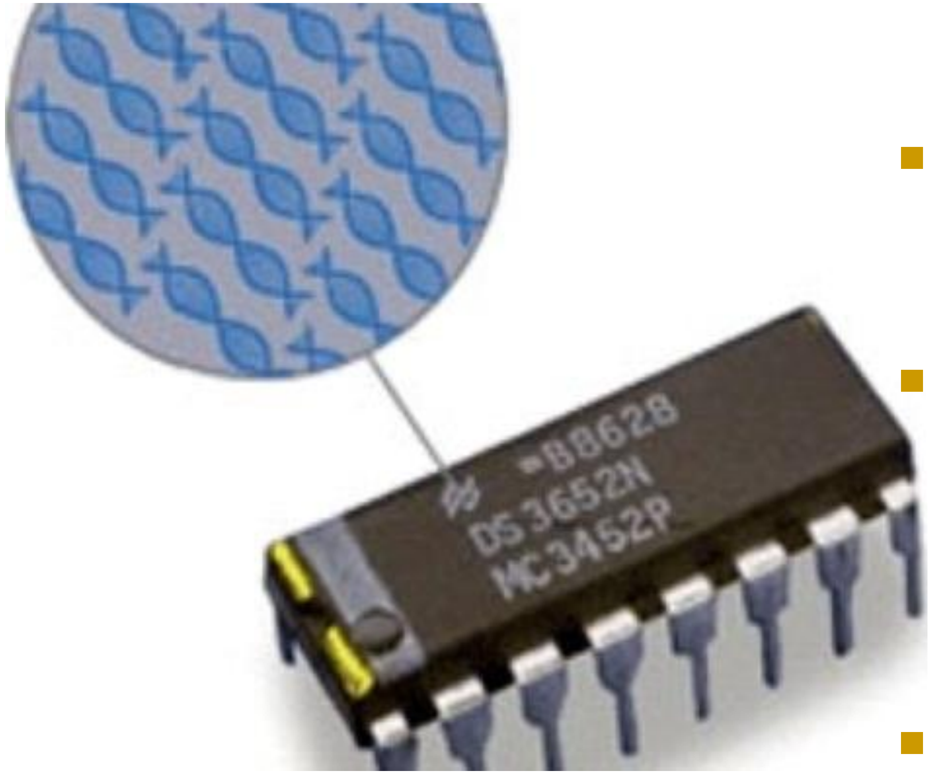


Source: https://phys.org/news/2011-02-fingerprint-chips-counterfeit-proof.html

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

Protecting Hardware by DNA Tagging



- Tagging chips and PCBs with special materials, such as plant DNA.
- Plat DNA sequences are scrambled to create unique patterns to be used as a signature.
- DNA is mixed with selected fluorophores (which are chemicals that glow under specific wavelengths of light) and tag the electronics with this DNA ink.
- A chip is authentic if the fluorescent signature exists.

Source: https://www.scientificamerican.com/article/electronic-chip-counterfeit-china/

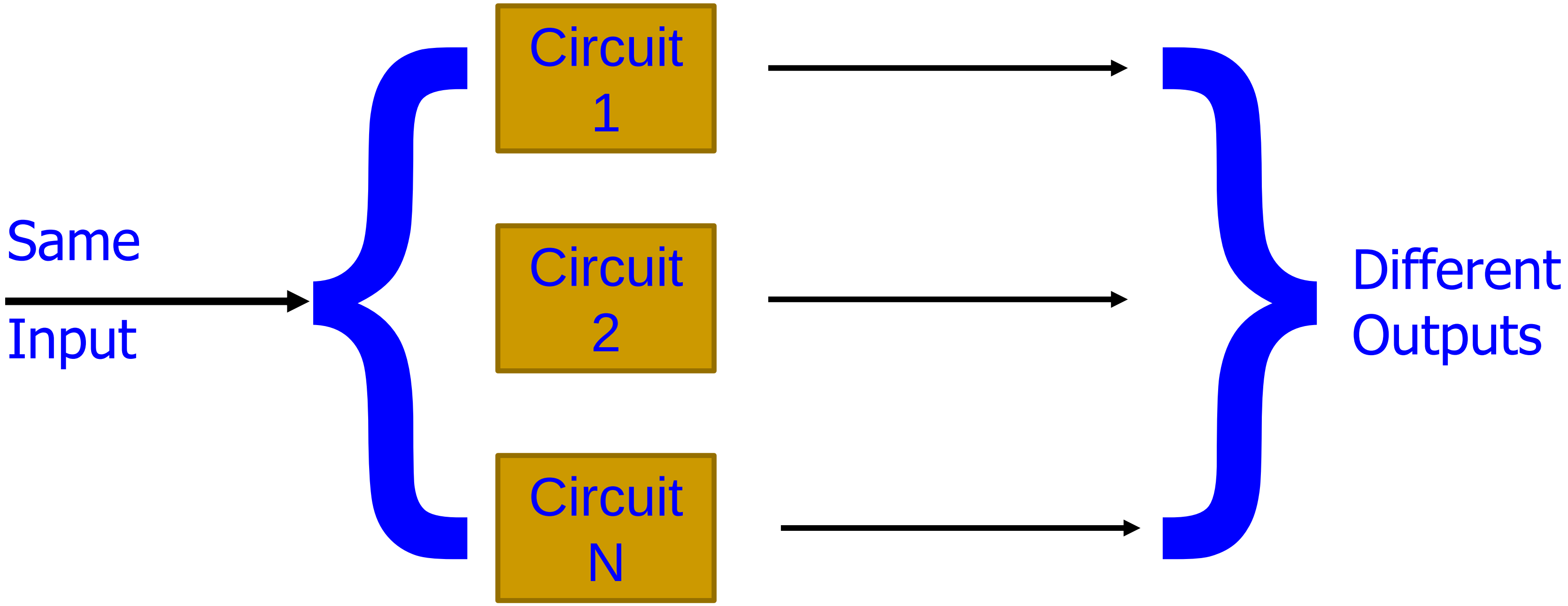
Physical Unclonable Function (PUF)

- Physical Unclonable Functions are simple primitives for security.
- PUFs are easy to build and impossible to duplicate (Theoretically).
- Input and Output are called Challenge Response Pair (CRP).

Only an authentic hardware can produce a correct Response for a Challenge.

Source: Mohanty 2017, Springer ALOG Dec 2017

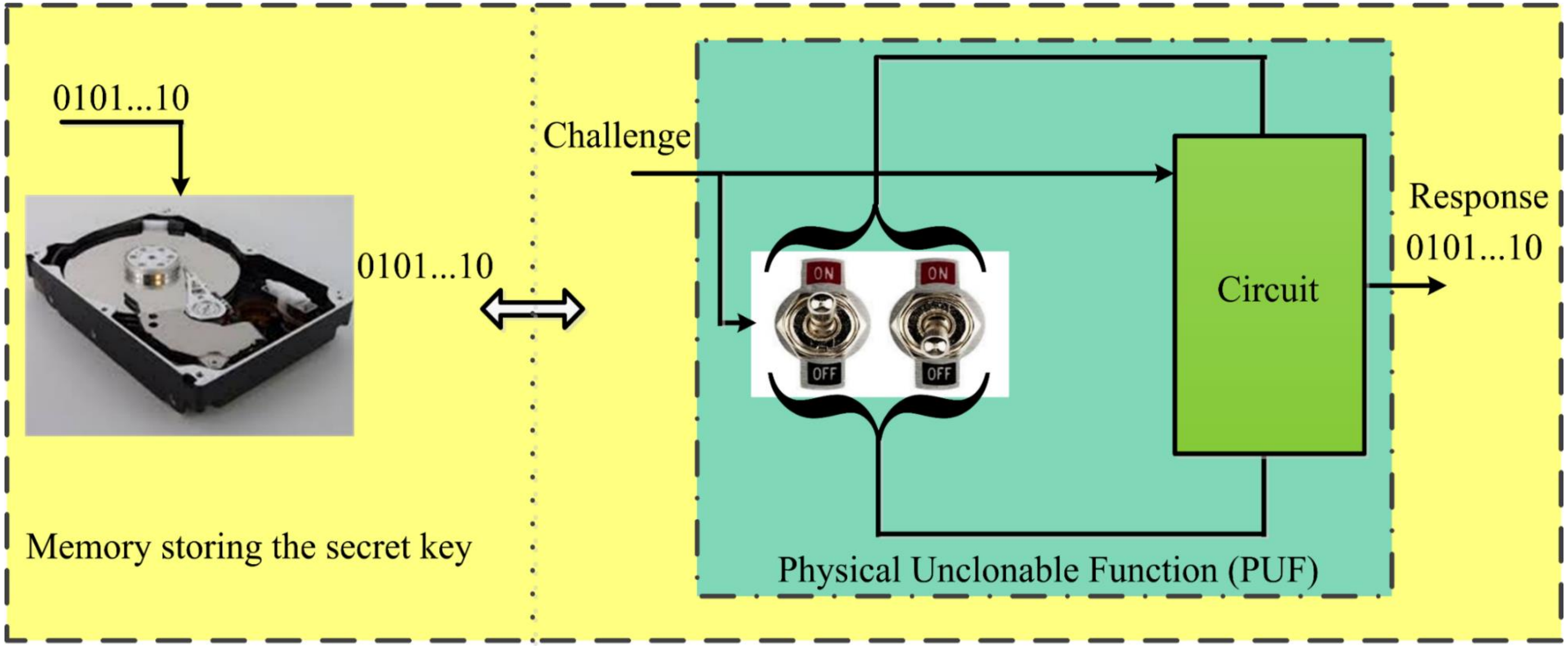
PUF - Principle



- With the same input to different copies of the same circuit, different outputs are obtained, each unique to each circuit.

Source: http://rijndael.ece.vt.edu/puf/background.html

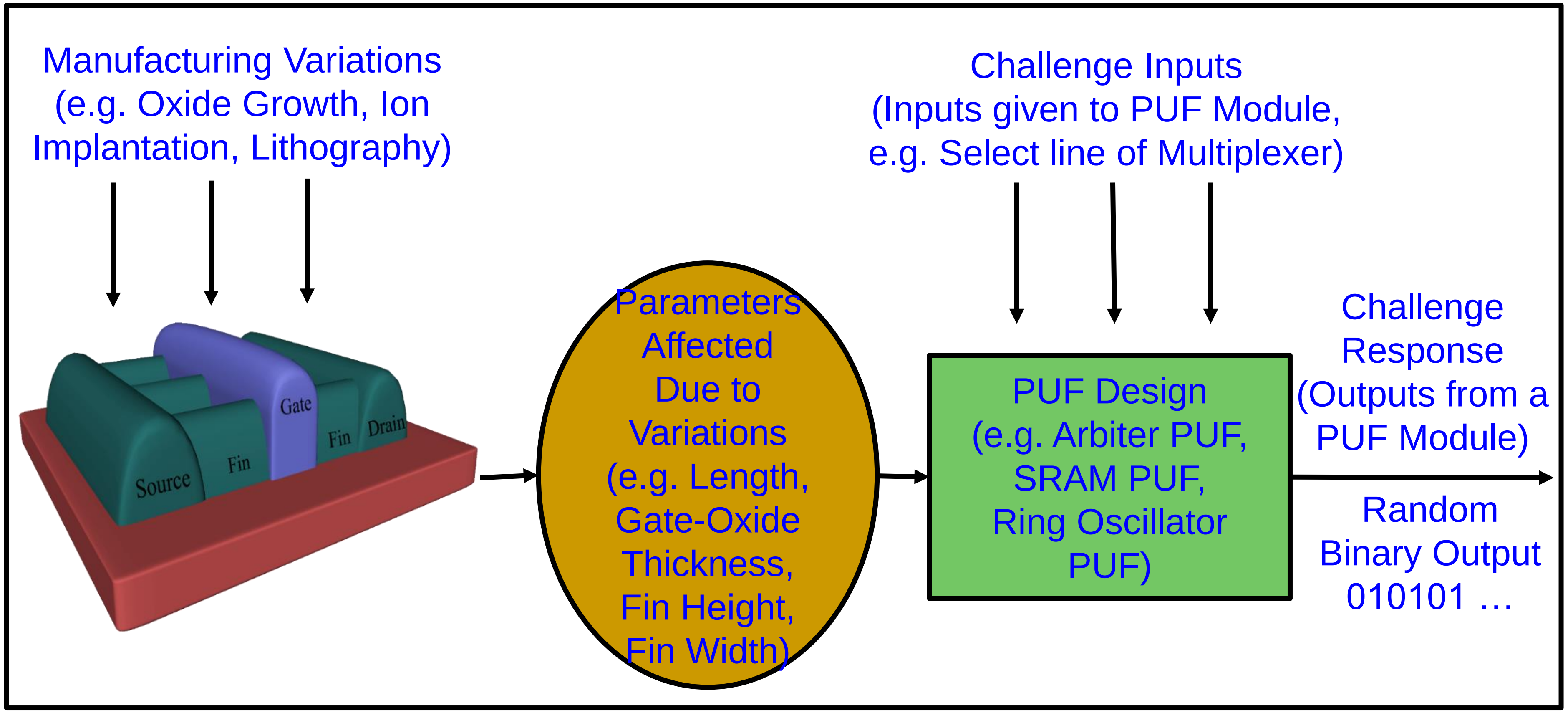
PUF - Principle



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



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

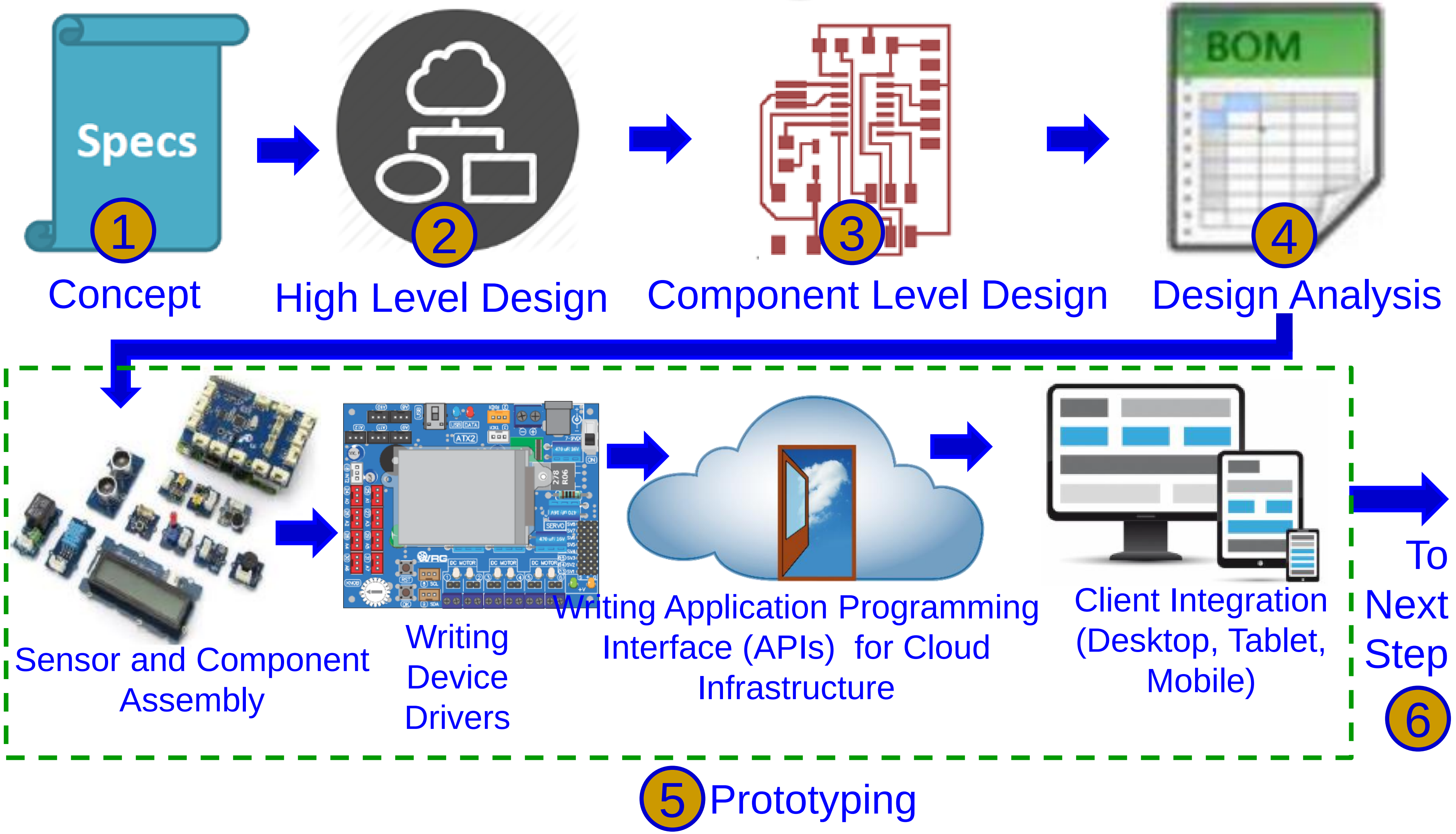
Source: Mohanty 2017, Springer ALOG 2017

PUF Vs Encryption

- In classic encryption, decryption key is stored in memory.
- If memory gets attacked, key is compromised.
- Key generated by PUF is not permanently stored in memory.
- If needed, it is not stored in temporary memory.

Design Flow

IoT – Design Flow



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

IoT – Design Flow

6 Field Testing

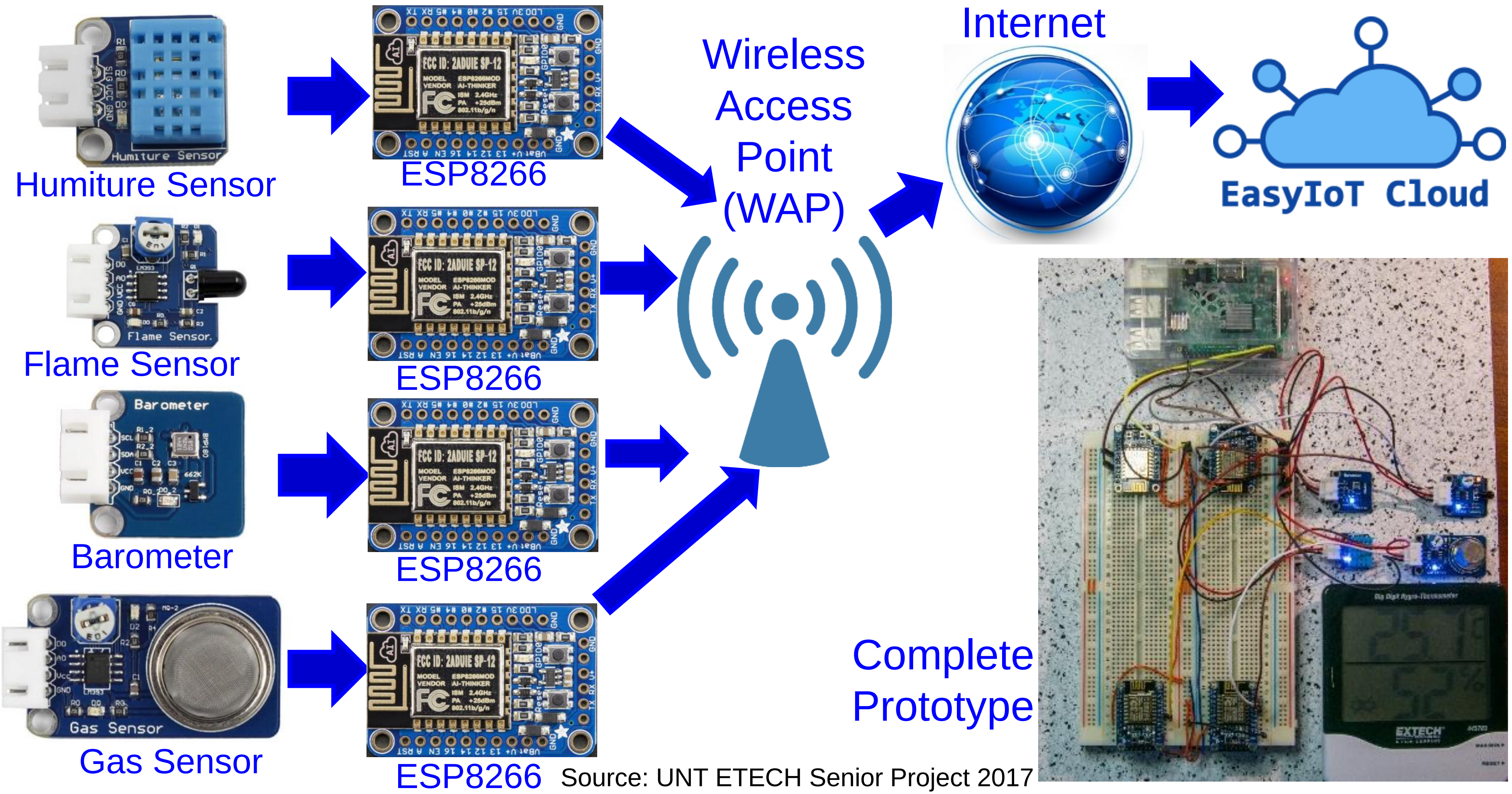
7 Release of Beta Version

8 Production

9 Release and Documentation

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

IoT Design – Case Study – Indoor Air Quality Monitoring



Source: UNT ETECH Senior Project 2017

Hardware for IoT

IoT Hardware Domains
- Embedded Systems and Boards (e.g. Arduino Yun, Raspberry Pi, BeagleBone, Samsung ARTIK)
- Wearable Devices and Gadgets (e.g. Samsung Gear 2, FitBit Flex, FLORA, iWallet)

Features	Processor/Microcontroller	Graphics Processing Unit	Clock Speed	Size	Memory	RAM	Supply Voltage	Listed Price
SparkFun Blynk Board	Tensilica L106 32-b	No	26 MHz	51 mm x 42 mm	4 MB	128 KB	5 V via micro-USB/ Li-Po connector and charging circuit	US$29.95
Arduino Yun	ATmega32u4 and Atheros AR9331 (for Linux)	No	16 MHz and 400 MHz	73 mm x 53 mm	32 KB and 16 MB + micro-SD	64 MB DDR2	5 V via micro-USB	US$58
Raspberry Pi 3	Broadcom BCM2837 and ARM Cortex-A53 64-b Quad Core	VideoCore IV @ 300/400 MHz	1.2 GHz	85 mm x 56 mm	Micro-SD	1 GB LPDDR2	5 V via micro-USB	US$35
cloudBit	Freescale i.MX233 (ARM926EJ-S core)	No	454 MHz	55 mm x 19 mm	Micro-SD slot with 4-GB micro-SD	64 MB	5 V via micro-USB	US$59.95
Photon	STM32F205 120Mhz ARM Cortex M3	No	120 MHz	36.5 mm x 20.3 mm	1 MB	128 KB	5 V via micro-USB	US$19
BeagleBone Black	AM335x ARM Cortex-A8	PowerVR SGX530	1 GHz	86 mm x 56 mm	4 GB 8-b eMMC, micro-SD	512 MB DDR3	5 V via mini-USB	US$49
Pinoccio	ATmega256RFR2	No	16 MHz	70 mm x 25 mm	256 KB	32 KB	5 V via micro-USB/ Li-Po connector and charging circuit	US$109
UDOO	Freescale i.MX 6 ARM Cortex-A9 and Atmel SAM3X8E ARM Cortex-M3	Vivante GC 2000 for 3-D + GC 355 for 2-D (vector graphics) + GC 320 for 2-D	1 GHz	110 mm x 85 mm	Micro-SD	1 GB DDR3	12 V	US$135
Samsung Artik 10	ARM A15x4 and A7x4	Mali-T628 MP6 core	1.3 GHz and 1.0 GHz	39 mm x 29 mm	16 GB	2 GB LPDDR3	3.4–5 V	US$100

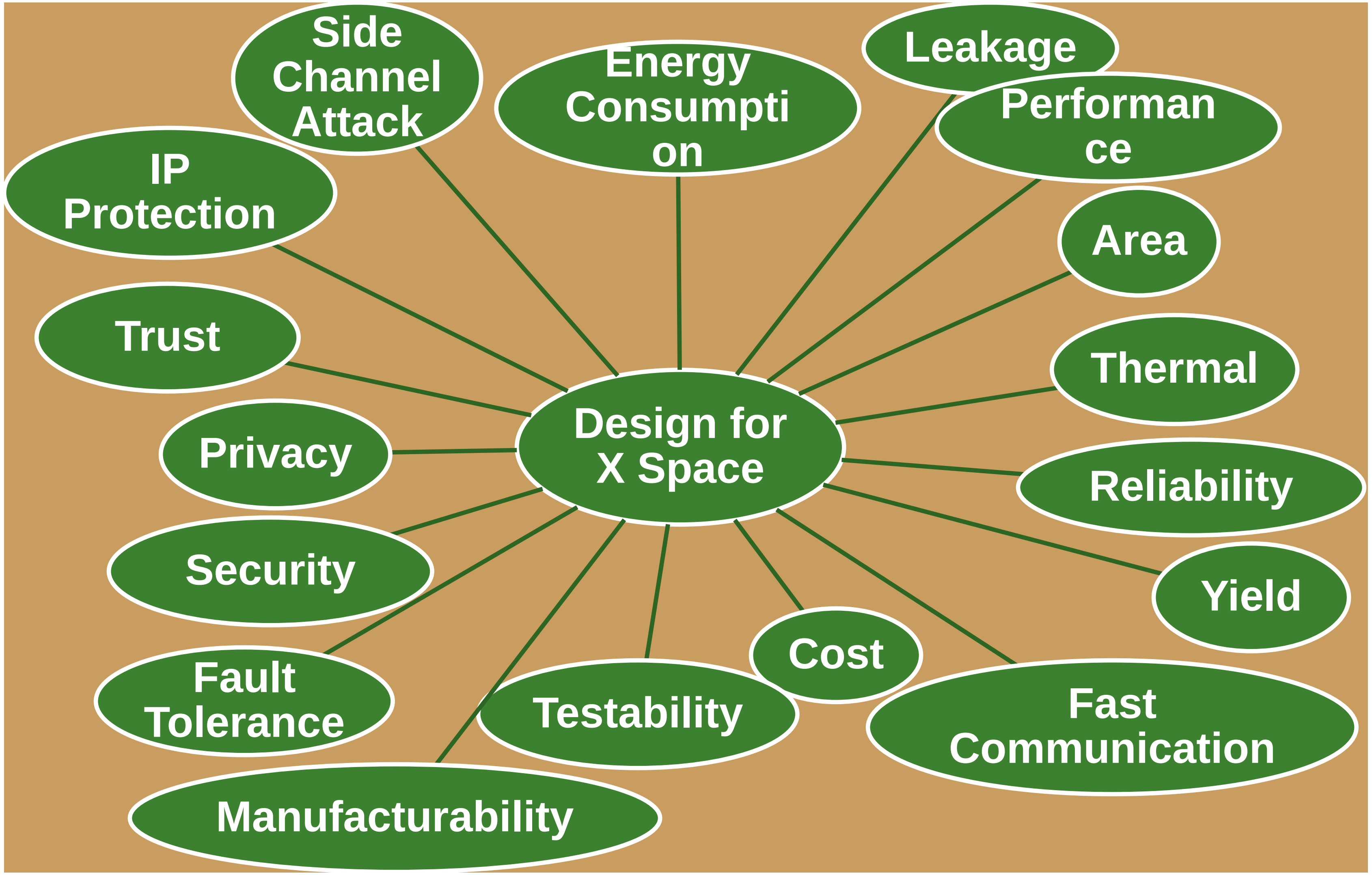
Source: Singh 2017, CE Magazine, April 2017

Software for IoT

- IoT Software Domains
  - Platforms
    - Temboo
    - Kaa
    - Carriots
    - Ubidots
    - ThingSpeak
    - Artik Cloud
    - Pinoccio
    - Smartliving
    - Samsung ARTIK
  - Languages
    - C/C++
    - Java
    - HTML5
    - Javascript
    - Python

Source: Singh 2017, CE Magazine, April 2017

How to Handle DfX in IoT Design?



Tools and Solutions

IoT - Design & Simulation Challenges

- Traditional controllers and processors do not meet IoT requirements, such as multiple sensor, communication protocol, and security requirements.
- Existing tools are not enough to meet challenges such as time-to-market, complexity, cost of IoT.
- Can a framework be developed for simulation, verification, and optimization:
  - of individual (multidiscipline) “Things”
  - of IoT Components
  - of IoT Architecture

IoT Simulators

Selected IoT Simulators

- Bevywise IoT Simulator
- CupCarbon
- IoTIFY
- Meshify
- Node-RED
- NetSim
- SimpleIoTSimulator

IoT Simulator - CUPCARBON

- **About**
  - CUPCARBON is a smart city and Internet of Things Wireless sensor network simulator (SCI-WSN)
- **Objective**
  - Design, Visualize, Debug
  - Validate distributed algorithms
  - Create environmental scenarios
- **Environments**
  - Design of mobility scenarios and the generation of natural events such as fires and gas as well as the simulation of mobiles such as vehicles and flying objects (e.g. UAVs, insects, etc.).
  - A discrete event simulation of WSNs which takes into account the scenario designed on the basis of the first environment.

Source: http://www.cupcarbon.com/

CUPCARBON

- **About:**
  - CUPCARBON is a smart city and Internet of Things Wireless sensor network simulator (SCI-WSN).

✓ **Objective**
- Design
- Visualize
- Debug
- Validate distributed algorithms
- Create environmental scenarios

CUPCARBON

- ***SenScript***

1. It is the script used to program sensor nodes of the CupCarbon Simulator.
2. In this script variables are not declared but can be initialized(set command).
3. A variable is used by its name and its value is determined by $.
4. SenScript-Source

- **Editor:**

Notepad ++ (for Windows) and CotEditor (for MAC).

Example:

- ✓ Sen: Set x abcd

Java: String x= “abcd”

- ✓ Sen: set y $x

Java: String y = x;

- ✓ Sen: set y x

Java: String y = “x”

IoT Simulators - Node-RED

- **About**:
  - Node-RED is a flow-based IoT Simulator.
  - It is a programming tool for wiring together hardware devices, APIs and online services in new ways.
  - The light-weight runtime is built on Node.js, taking full advantage of its event-driven, non-blocking model.
- **Editor**:
  - Browser-based editor.
  - The flows created in Node-RED are stored using JSON which can be easily imported and exported for sharing with others.
- **Advantages**:
  - Available for smaller computing devices such as Raspberry Pi.
  - It takes moments to create cloud applications that combine services from across the platform.

IoT Simulators - SimpleIoTSimulator

- About:
  - SimpleIoTSimulator is an IoT Sensor/device simulator that quickly creates test environments made up of thousands of sensors and gateways, all on just one computer.

IoT Simulators - Meshify

- About:
  - Meshify offers industrial IoT solutions. It helps to monitor, analyze, control, & track your devices.
  - It was founded in 2011 with the goal of making IoT more accessible.
- Services:
  - Hardware Selection & Implementation
  - UI/UX Design & development
  - Seasoned Integrations Team
  - End-to-end Architecture design
  - Professional Project Management

IoT Simulators – Observations

- IoT does not have a one-size-fits-all solution.
- IoT solutions often require pulling together different device APIs and online services in new and interesting ways.
- It is a multi-disciplinary domain and everyone cannot master everything.
- Tools that make it easier for developers at all levels, are always in demand.

Metamodel based Simulation?

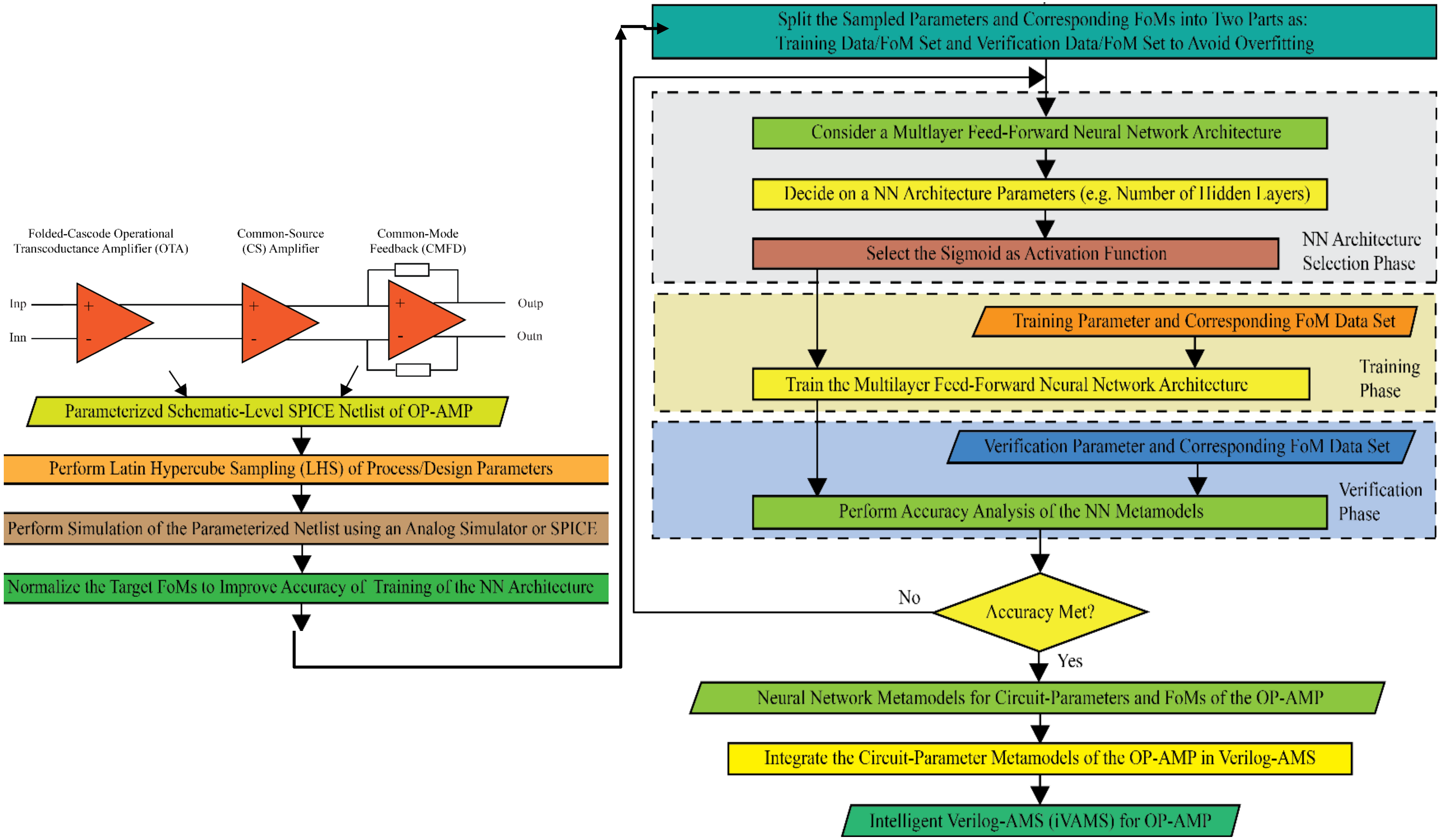
- "Model of a model" -- Metamodels are mathematical function (s) used to represent computer simulation models – e.g. polynomial functions, DOE predictive functions, neural networks, and Kriging interpolation:

$$\hat{F}(x_n) = F(x_n) + \varepsilon \approx F(x_n)$$

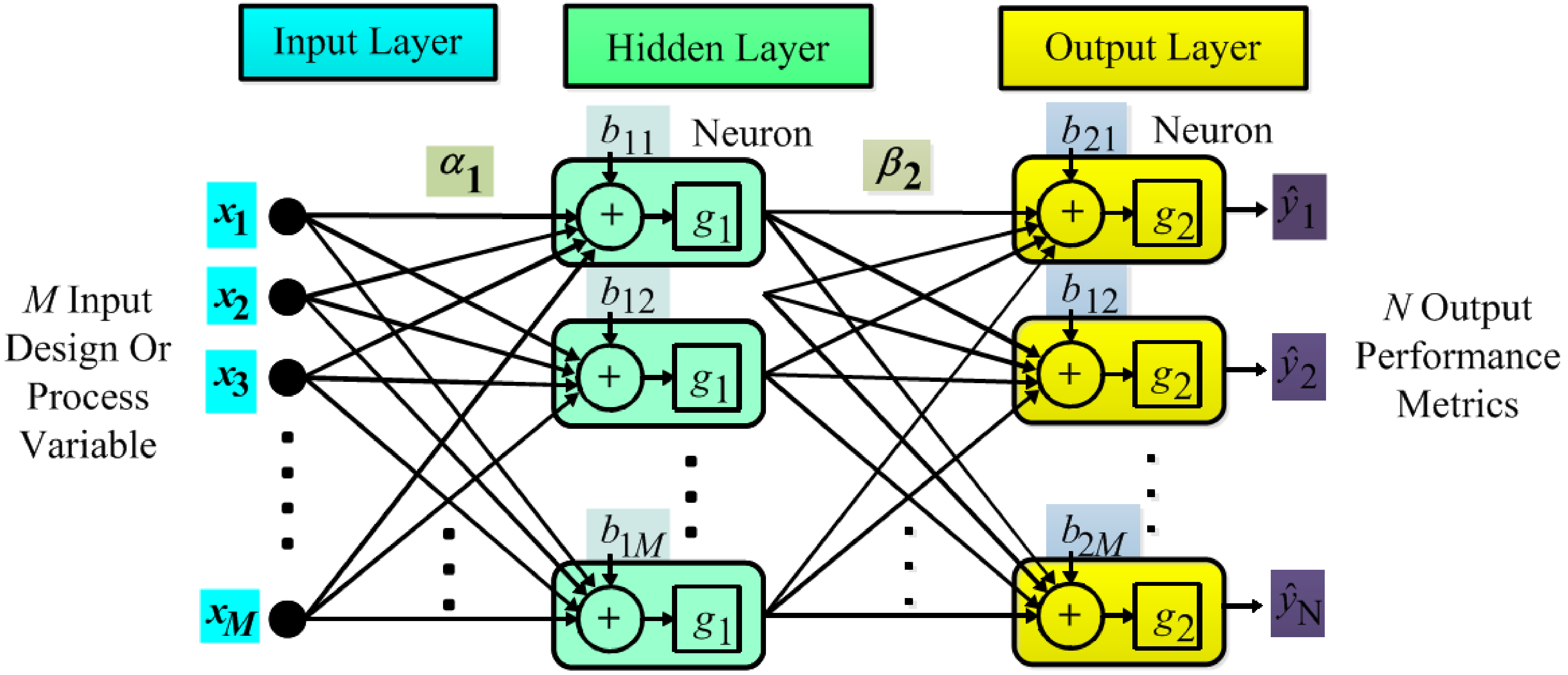
Some Metamodels

- **Polynomial**
- **Neural-Networks**
- **Kriging Methods**

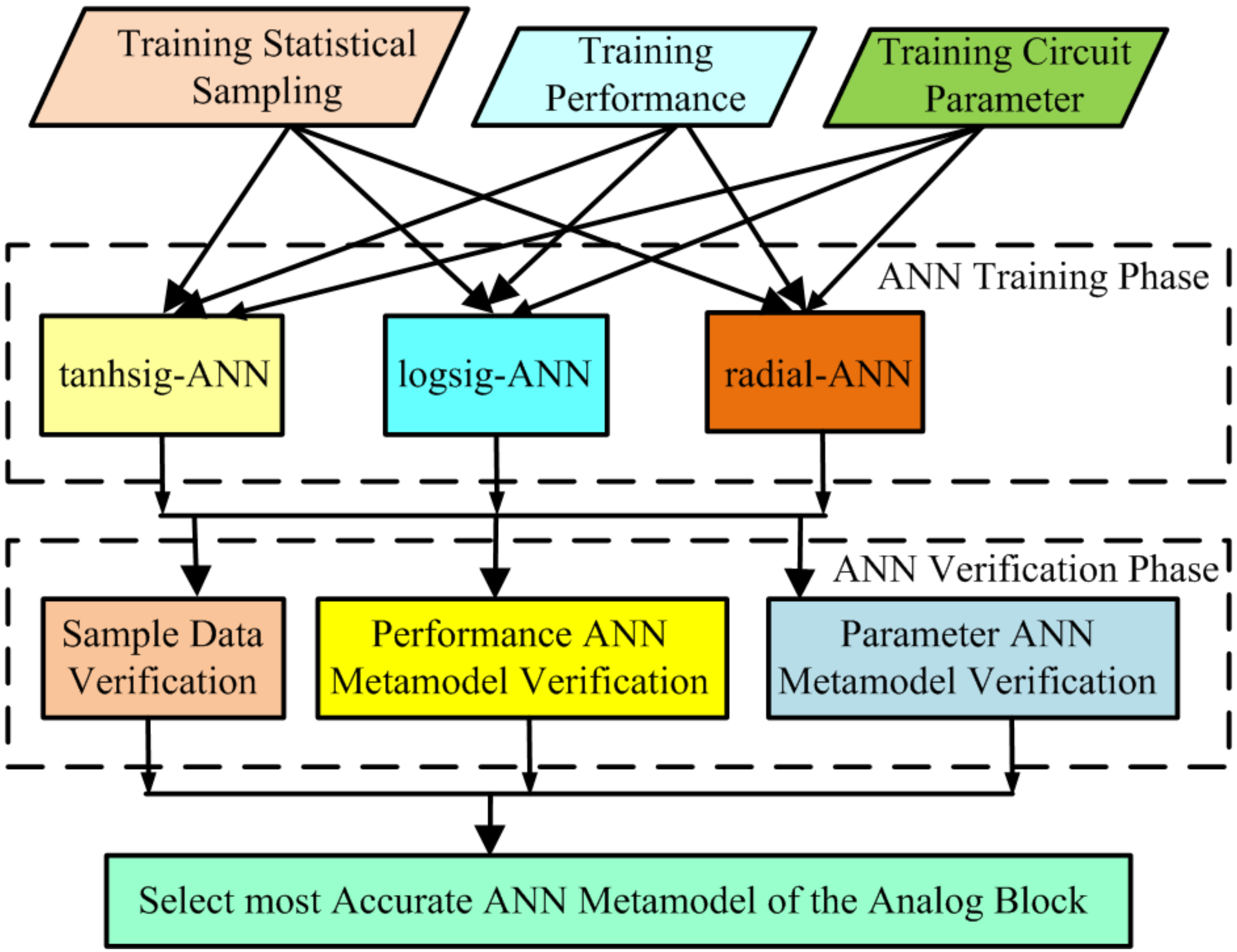
iVAMS - ANN Metamodel Generation



iVAMS - ANN Metamodeling

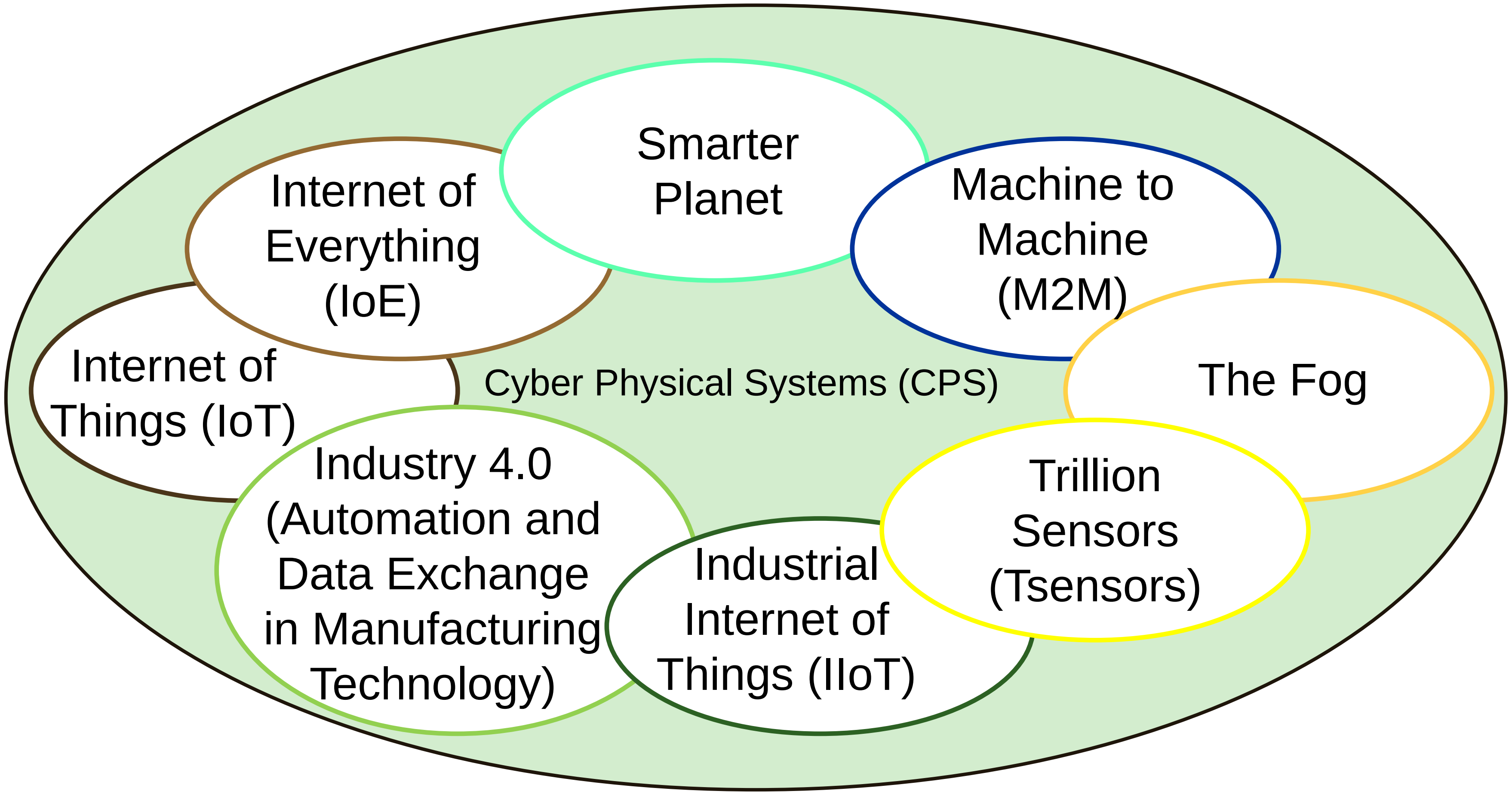


iVAMS - ANN Metamodel Architecture Selection



Related Buzzwords

Some related Buzzwords



Source: Sangiovanni-Vincentelli 2016, ISC2 2016

IoT Vs Sensor Networks

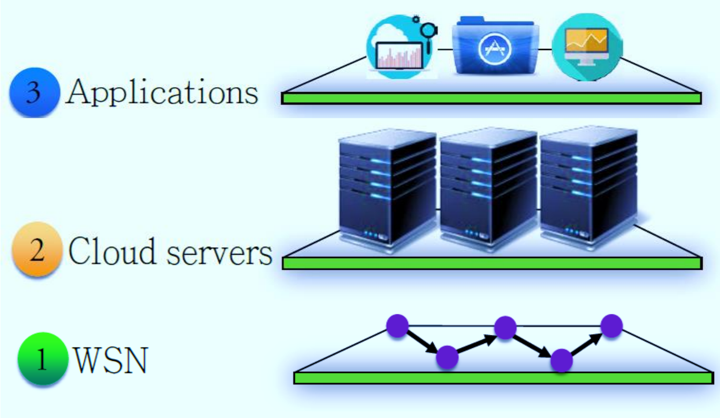
Wireless Sensor Networks (WSN)

- WSN is like the eyes and ears of the IoT.
- Anetwork of small wireless electronic nodes which consists of different sensors.
- The purpose is to collect data from the environment.

IoT adds value to data!

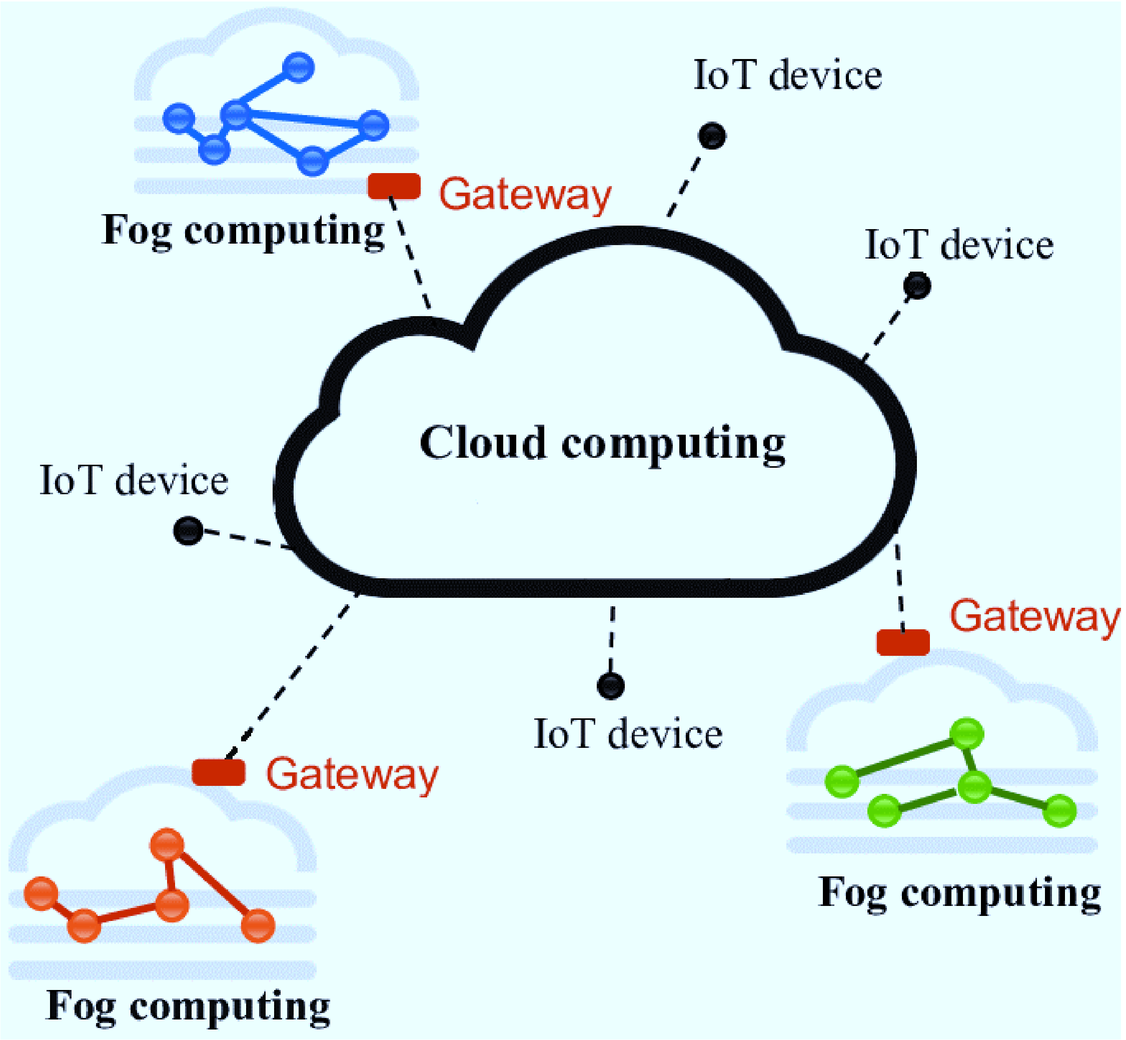
IoT

- IoT in a broad sense is like a brain.
- Store both real world data and can also be used to monitor the real world parameters and give meaningful interpretation.



Source: Nia 2017, IEEE TETC 2017

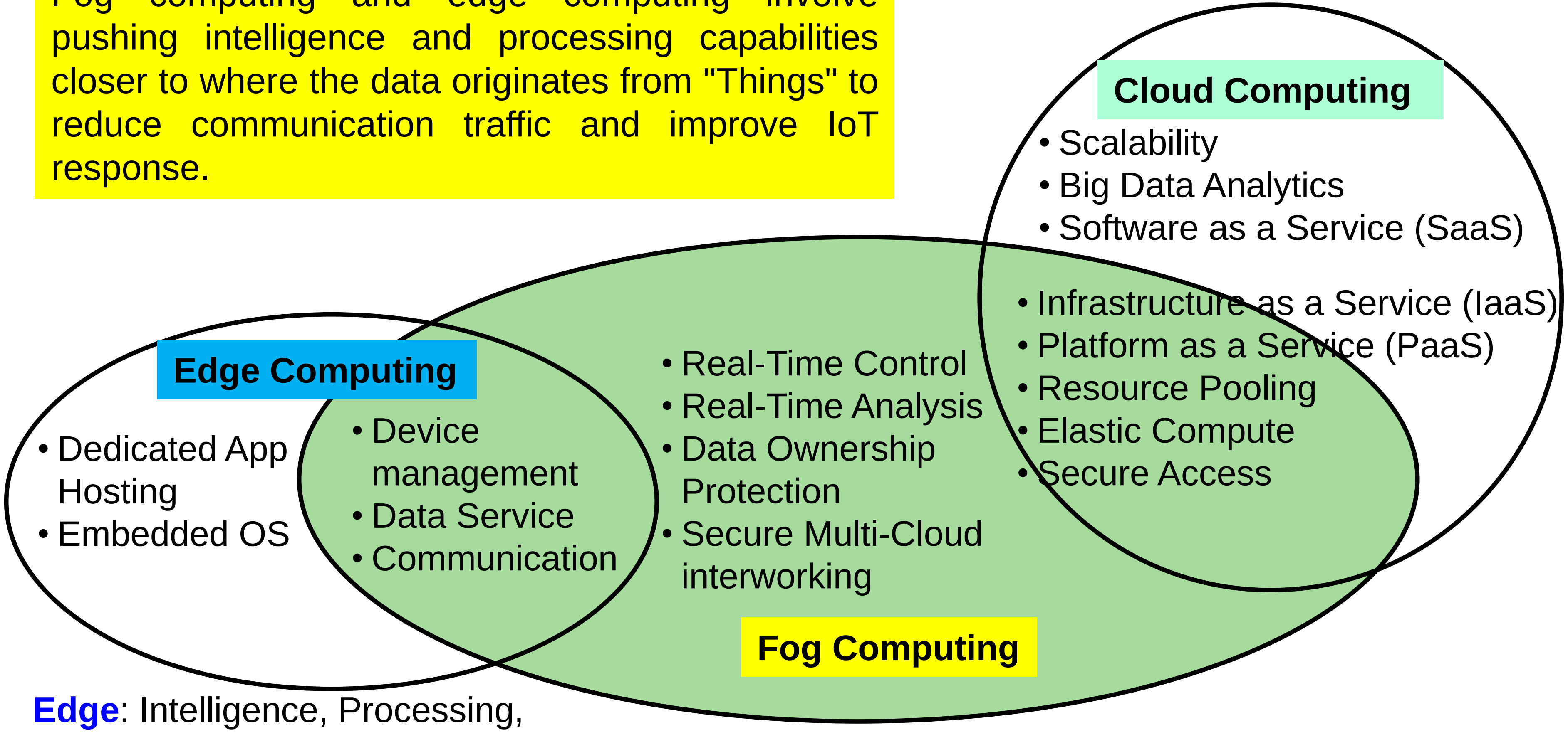
IoT Vs Fog Computing



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

Fog Vs Edge Vs Cloud Computing

Fog computing and edge computing involve pushing intelligence and processing capabilities closer to where the data originates from "Things" to reduce communication traffic and improve IoT response.



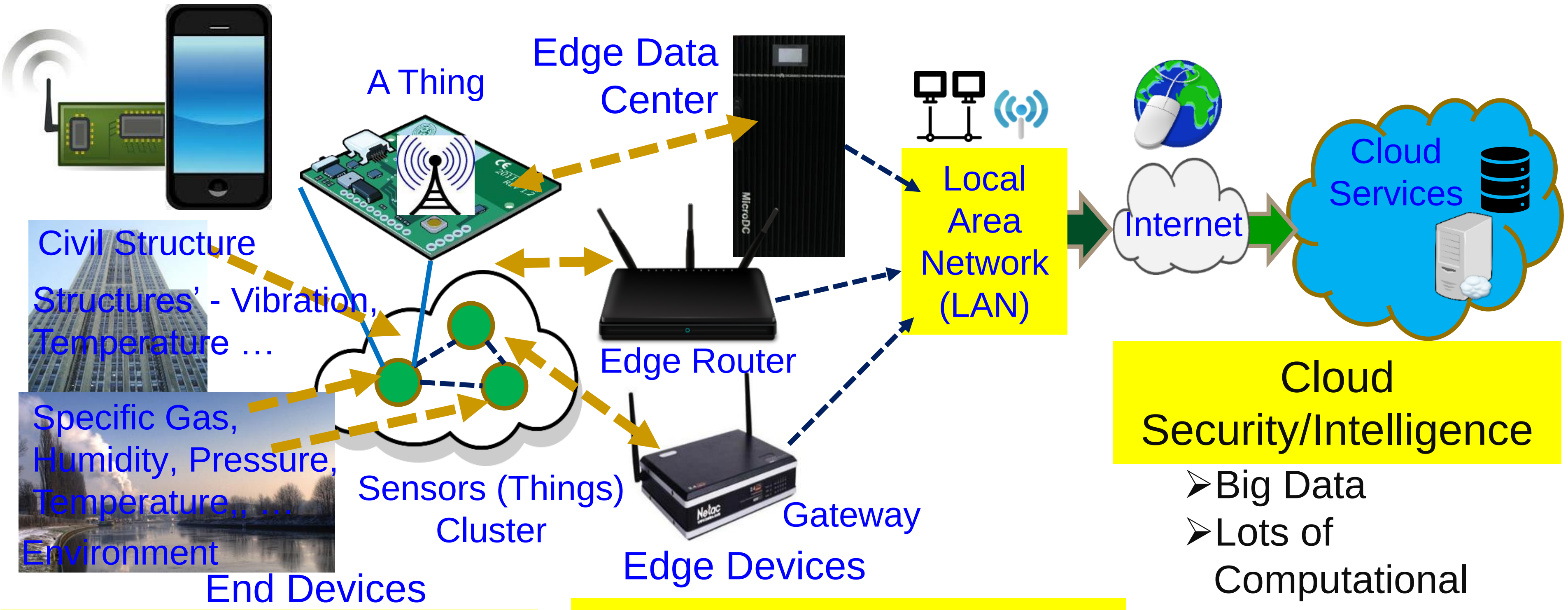
Edge: Intelligence, Processing, and Communication - Devices like Programmable Automation Controllers (PACs)

Fog: Intelligence - LAN, Processing - fog node or IoT gateway.

Source: https://www.automationworld.com/fog-computing-vs-edge-computing-whats-difference

Source: https://www.nebbiolo.tech/wp-content/uploads/whitepaper-fog-vs-edge.pdf

End, Edge Vs Cloud Security, Intelligence …



Cloud Security/Intelligence

- Big Data
- Lots of Computational Resource
- Accurate Data Analytics
- Latency in Network
- Energy overhead in Communications

End Security/Intelligence

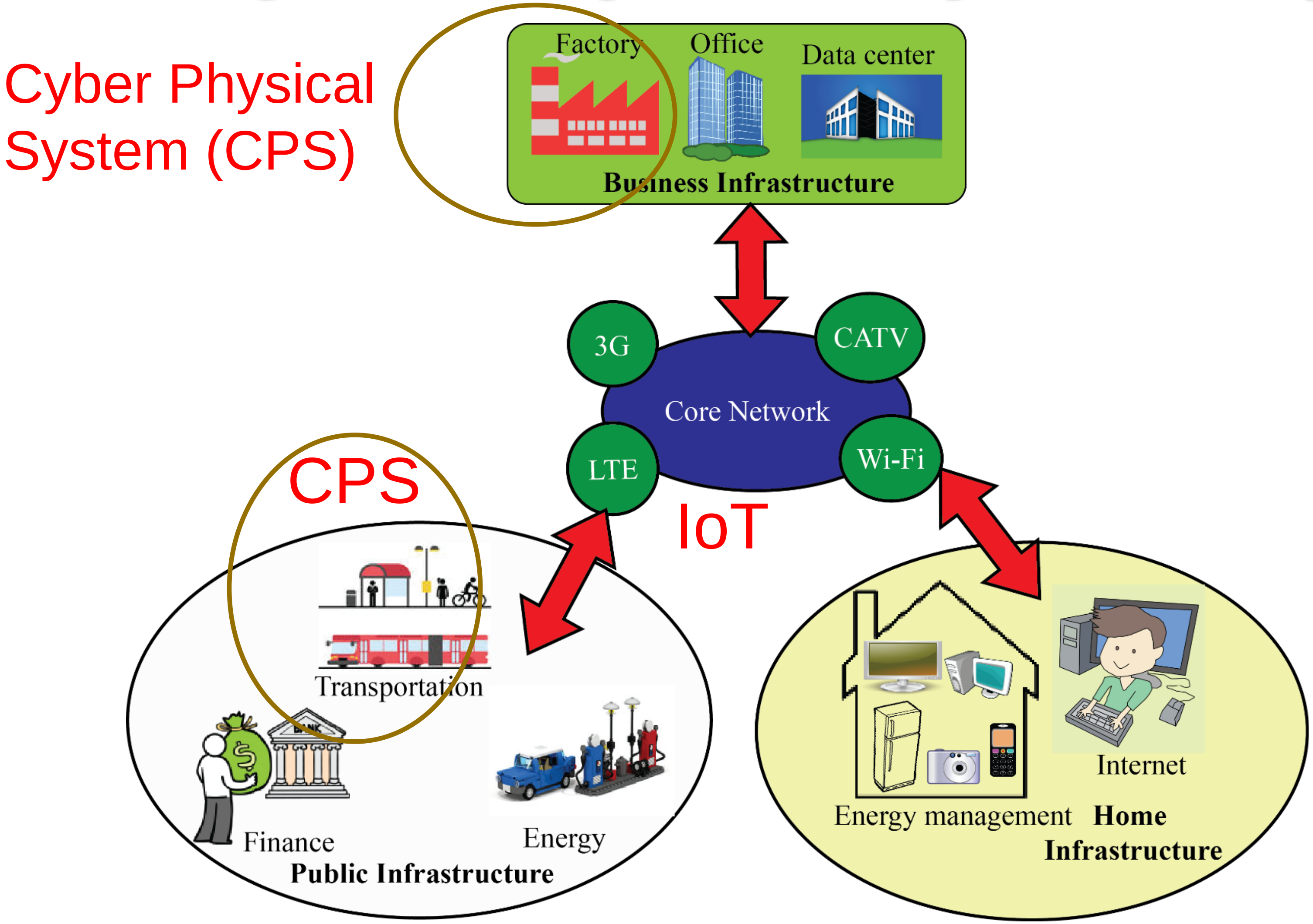
- Minimal Data
- Minimal Computational Resource
- Least Accurate Data Analytics
- Very Rapid Response

Edge Security/Intelligence

- Less Data
- Less Computational Resource
- Less Accurate Data Analytics
- Rapid Response

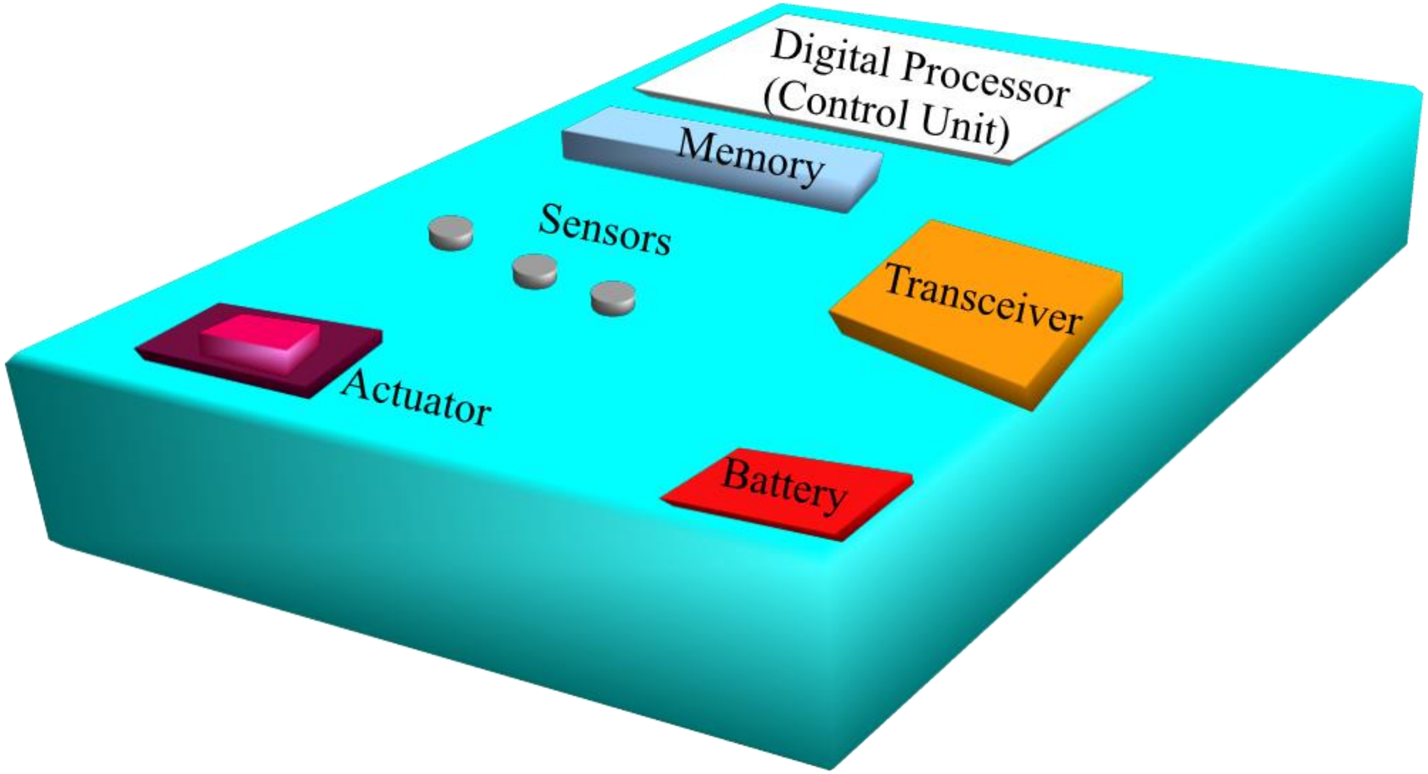
Source: Mohanty iSES Keynote 2018 and ICCE 2019 Panel

IoT Vs Cyber Physical Systems (CPS)



Source: Mohanty 2016, CE Magazine July 2016

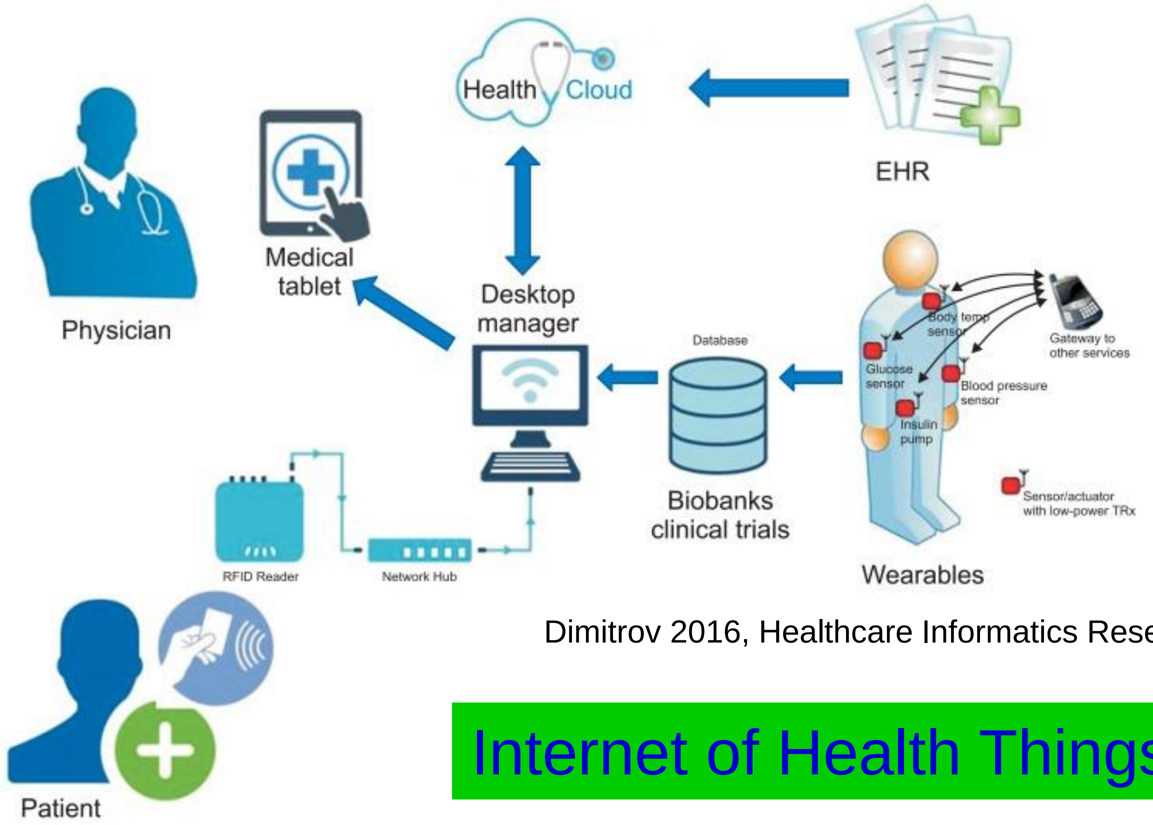
Internet of NanoThings (IoNT)



Akyildiz_IEEE-Wireless-Communications_Magazine_2015-Mar

Akyildiz_IEEE-Wireless-Communications_Magazine_2010-Dec

Internet of MedicalThings (IoMT)



Dimitrov 2016, Healthcare Informatics Research. July 2016

Internet of Health Things (IoHT)

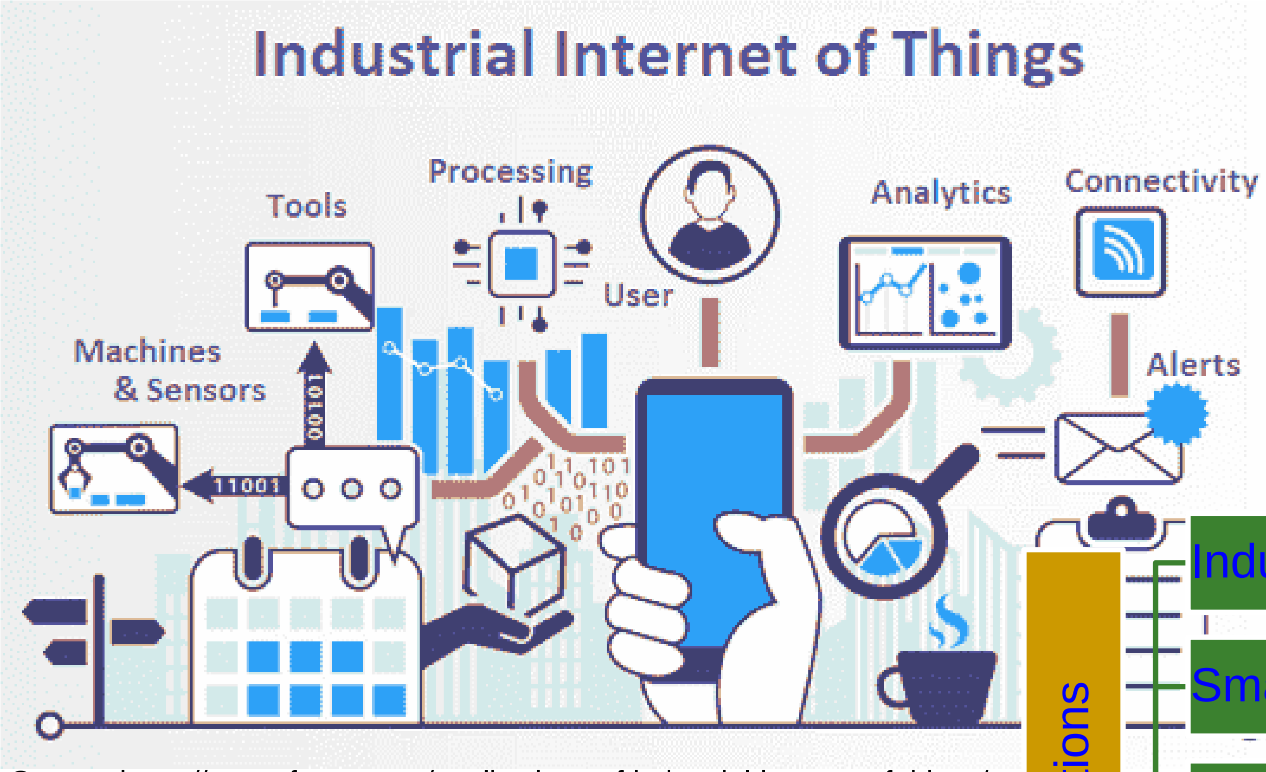
IoMT is a collection of medical devices and applications that connect to healthcare IT systems through Internet.

Source: http://www.icemiller.com/ice-on-fire-insights/publications/the-internet-of-health-things-privacy-and-security/

Source: http://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things

Internet of Agro Things (IoAT)

Industrial Internet of Things (IIoT)

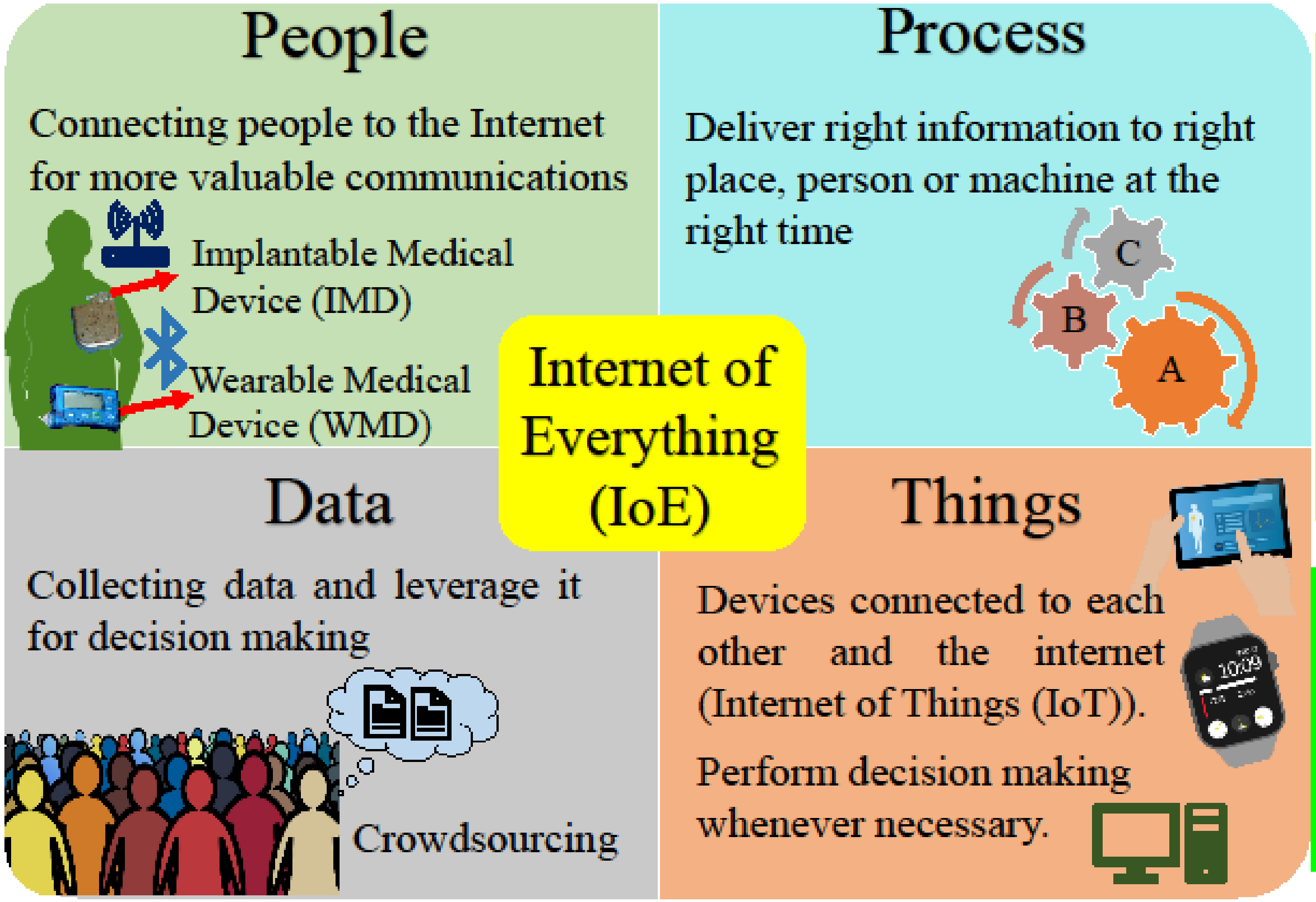


Source: https://www.rfpage.com/applications-of-industrial-internet-of-things/

Applications

- Industrial Automation
- Smart Robotics
- Predictive Maintenance
- Integration of Tools / Wearables
- Smart Logistics

Internet of Every Things (IoE)



Requires:
- Data, Device, and System Security
- Data, Location, and System Privacy

Need of the Hour:
- Security/Secure by Design (SbD)
- Privacy by Design (PbD)

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)", *arXiv Computer Science*, arXiv:1909.06496, September 2019, 37-pages.

Conclusion

Conclusion

- IoT has following components: Things, LAN, Cloud, Internet.
- IoT is backbone of smart cities.
- Scalability, Cost, Energy-consumption, Security are some important challenges of IoT.
- Security, Privacy, and Ownership Rights are critical for trustworthy IoT design.
- Physical Unclonable Functions (PUF) emerging as a good security solution.
- Coordination among the various researchers and design engineers is a challenge as IoT is multidisciplinary.

Future Directions

- Energy-Efficient "Thing" design is needed.
- Security and Privacy of Information need more research.
- Security of the CE systems (e.g. UAV, Smart Cars) needs research.
- Safer and efficient battery need research.
- IoT automatic design tool needs research.
- Some IoT simulators exist, but more needed for efficient, accurate, scalable, multi-discipline simulations.