ELEC 5970/6970
Hardware Security-I
Fall 2020

Lecture 1: Introduction

Ujjwal Guin, Assistant Professor
Department of Electrical and Computer Engineering
Auburn University, Auburn, AL 36849
http://www.eng.auburn.edu/~uguin

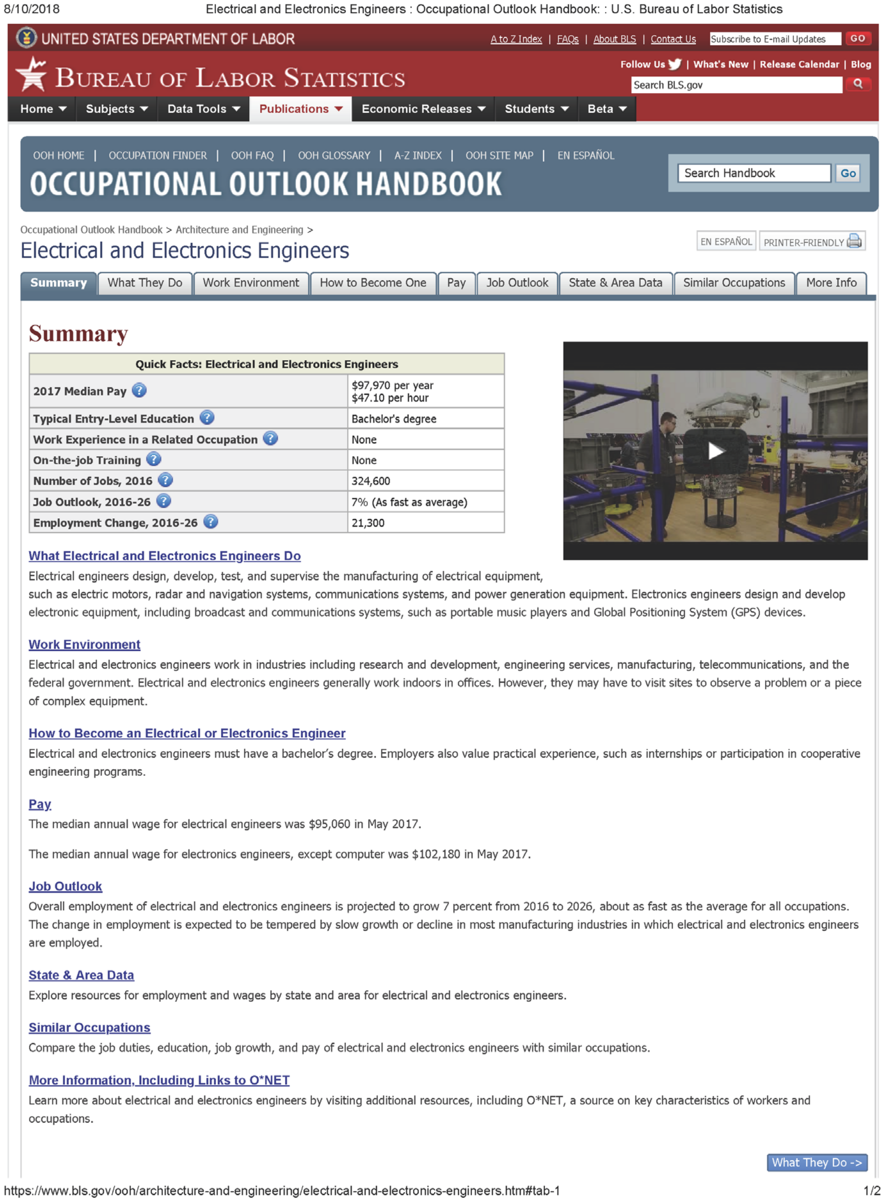
Course Details

- Presentations will be uploaded in Canvas
- https://www.eng.auburn.edu/~uguin/teaching.html
  - ELEC 5210/ELEC 6210 - Hardware Security I Fall 2021
- Methods for evaluating performance

	Undergraduate Students	Graduate Students
Homework	25%	20%
Class tests (2)	25%	20%
Design Project	25%	20%
Open Hardware Security Problem	-	20%
Final Examination	25%	20%

- Grading Scale
  - 90-100:A; 80-89: B; 70-79: C; 60-69:D; <60:F

Motivation


UNITED STATES DEPARTMENT OF LABOR
A to Z Index | FAQs | About BLS | Contact Us
Subscribe to E-mail Updates
GO
Follow Us | What's New | Release Calendar | Blog
BUREAU OF LABOR STATISTICS
Search BLS.gov
Home
Subjects
Data Tools
Publications
Economic Releases
Students
Beta
OOH HOME | OCCUPATION FINDER | OOH FAQ | OOH GLOSSARY | A-Z INDEX | OOH SITE MAP | EN ESPAÑOL
OCCUPATIONAL OUTLOOK HANDBOOK
Search Handbook
Go
EN ESPAÑOL
PRINTER-FRIENDLY
Summary
What They Do
Work Environment
How to Become One
Pay
Job Outlook
State & Area Data
Similar Occupations
More Info
What They Do ->

8/10/2018 Electrical and Electronics Engineers : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics

Occupational Outlook Handbook > Architecture and Engineering >

Electrical and Electronics Engineers

Summary

Quick Facts: Electrical and Electronics Engineers	
2017 Median Pay	$97,970 per year $47.10 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	None
On-the-job Training	None
Number of Jobs, 2016	324,600
Job Outlook, 2016-26	7% (As fast as average)
Employment Change, 2016-26	21,300

What Electrical and Electronics Engineers Do

Electrical engineers design, develop, test, and supervise the manufacturing of electrical equipment, such as electric motors, radar and navigation systems, communications systems, and power generation equipment. Electronics engineers design and develop electronic equipment, including broadcast and communications systems, such as portable music players and Global Positioning System (GPS) devices.

Work Environment

Electrical and electronics engineers work in industries including research and development, engineering services, manufacturing, telecommunications, and the federal government. Electrical and electronics engineers generally work indoors in offices. However, they may have to visit sites to observe a problem or a piece of complex equipment.

How to Become an Electrical or Electronics Engineer

Electrical and electronics engineers must have a bachelor's degree. Employers also value practical experience, such as internships or participation in cooperative engineering programs.

Pay

The median annual wage for electrical engineers was $95,060 in May 2017.

The median annual wage for electronics engineers, except computer was $102,180 in May 2017.

Job Outlook

Overall employment of electrical and electronics engineers is projected to grow 7 percent from 2016 to 2026, about as fast as the average for all occupations. The change in employment is expected to be tempered by slow growth or decline in most manufacturing industries in which electrical and electronics engineers are employed.

State & Area Data

Explore resources for employment and wages by state and area for electrical and electronics engineers.

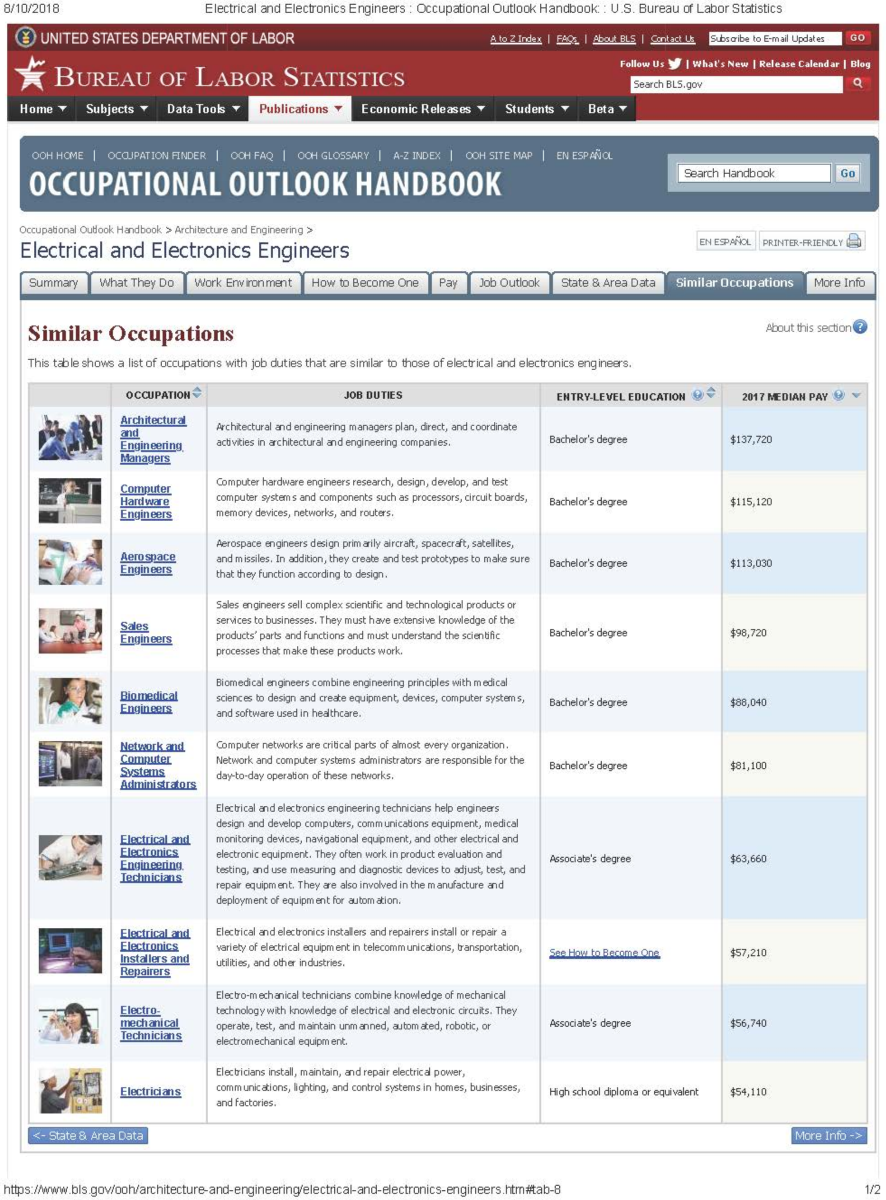
Similar Occupations

Compare the job duties, education, job growth, and pay of electrical and electronics engineers with similar occupations.

More Information, Including Links to O*NET

Learn more about electrical and electronics engineers by visiting additional resources, including O*NET, a source on key characteristics of workers and occupations.

https://www.bls.gov/ooh/architecture-and-engineering/electrical-and-electronics-engineers.htm#tab-1 1/2


UNITED STATES DEPARTMENT OF LABOR
A to Z Index | FAQs | About BLS | Contact Us
Subscribe to E-mail Updates
GO
Follow Us | What's New | Release Calendar | Blog
BUREAU OF LABOR STATISTICS
Search BLS.gov
Home
Subjects
Data Tools
Publications
Economic Releases
Students
Beta
OOH HOME | OCCUPATION FINDER | OOH FAQ | OOH GLOSSARY | A-Z INDEX | OOH SITE MAP | EN ESPAÑOL
OCCUPATIONAL OUTLOOK HANDBOOK
Search Handbook
Go
EN ESPAÑOL
PRINTER-FRIENDLY
Summary
What They Do
Work Environment
How to Become One
Pay
Job Outlook
State & Area Data
Similar Occupations
More Info
About this section
<- State & Area Data
More Info ->

8/10/2018 Electrical and Electronics Engineers : Occupational Outlook Handbook : U.S. Bureau of Labor Statistics

Occupational Outlook Handbook > Architecture and Engineering >

Electrical and Electronics Engineers

Similar Occupations

This table shows a list of occupations with job duties that are similar to those of electrical and electronics engineers.

	OCCUPATION	JOB DUTIES	ENTRY-LEVEL EDUCATION	2017 MEDIAN PAY
	Architectural and Engineering Managers	Architectural and engineering managers plan, direct, and coordinate activities in architectural and engineering companies.	Bachelor's degree	$137,720
	Computer Hardware Engineers	Computer hardware engineers research, design, develop, and test computer systems and components such as processors, circuit boards, memory devices, networks, and routers.	Bachelor's degree	$115,120
	Aerospace Engineers	Aerospace engineers design primarily aircraft, spacecraft, satellites, and missiles. In addition, they create and test prototypes to make sure that they function according to design.	Bachelor's degree	$113,030
	Sales Engineers	Sales engineers sell complex scientific and technological products or services to businesses. They must have extensive knowledge of the products' parts and functions and must understand the scientific processes that make these products work.	Bachelor's degree	$98,720
	Biomedical Engineers	Biomedical engineers combine engineering principles with medical sciences to design and create equipment, devices, computer systems, and software used in healthcare.	Bachelor's degree	$88,040
	Network and Computer Systems Administrators	Computer networks are critical parts of almost every organization. Network and computer systems administrators are responsible for the day-to-day operation of these networks.	Bachelor's degree	$81,100
	Electrical and Electronics Engineering Technicians	Electrical and electronics engineering technicians help engineers design and develop computers, communications equipment, medical monitoring devices, navigational equipment, and other electrical and electronic equipment. They often work in product evaluation and testing, and use measuring and diagnostic devices to adjust, test, and repair equipment. They are also involved in the manufacture and deployment of equipment for automation.	Associate's degree	$63,660
	Electrical and Electronics Installers and Repairers	Electrical and electronics installers and repairers install or repair a variety of electrical equipment in telecommunications, transportation, utilities, and other industries.	See How to Become One	$57,210
	Electro-mechanical Technicians	Electro-mechanical technicians combine knowledge of mechanical technology with knowledge of electrical and electronic circuits. They operate, test, and maintain unmanned, automated, robotic, or electromechanical equipment.	Associate's degree	$56,740
	Electricians	Electricians install, maintain, and repair electrical power, communications, lighting, and control systems in homes, businesses, and factories.	High school diploma or equivalent	$54,110

https://www.bls.gov/ooh/architecture-and-engineering/electrical-and-electronics-engineers.htm#tab-8 1/2

Goals

- Learning emerging technologies and security trends.
- Learning state-of-the-art security measures.
- Integration of security measures at the design stage.
- Solid understanding of different hardware attacks and their countermeasures.
    - Electronics supply chain.
    - Vulnerabilities in manufacturing/production process.
    - Integration of the countermeasures.

Course Organization

- References Books
  - ***Understanding Cryptography: A Textbook for Students and Practitioners,*** C. Paar, and Jan Pelz, Springer-Verlag Berlin Heidelberg, 2010, ISBN 978-3-642-04100-6
  - ***Counterfeit Integrated Circuits: Detection and Avoidance***, M. M. Tehranipoor, U. Guin, and D. Forte, Springer International Publishing, 2015, ISBN: 978-3-319-11823-9
  - ***Introduction to Hardware Security and Trust***, M. Tehranipoor, C. Wang, Springer-Verlag New York, 2012, ISBN 978-1-4419-8079-3
- Instructor: Ujjwal Guin, Broun 325, (334) 844-1835, *ujjwal.guin@auburn.edu*
- Classroom: MWF 10:00 a.m. - 10:50 a.m., Broun 113

Student Performance Evaluation

- Homework (25%,20%)
- Two Class Tests (25%,20%)
  - Test 1, TBD, 10:00 a.m. - 10:50 a.m., Broun 113
  - Test 2, TBD, 10:00 a.m. - 10:50 a.m., Broun 113
- Design Project (25%,20%)
  - Demonstration: TBD
- Open Hardware Security Problem (-,20%)
- Final Exam (25%,20%)
  - http://www.auburn.edu/administration/registrar/calendars.html
- Participation in class discussion and attendance of lectures are strongly encouraged.

Course Outline

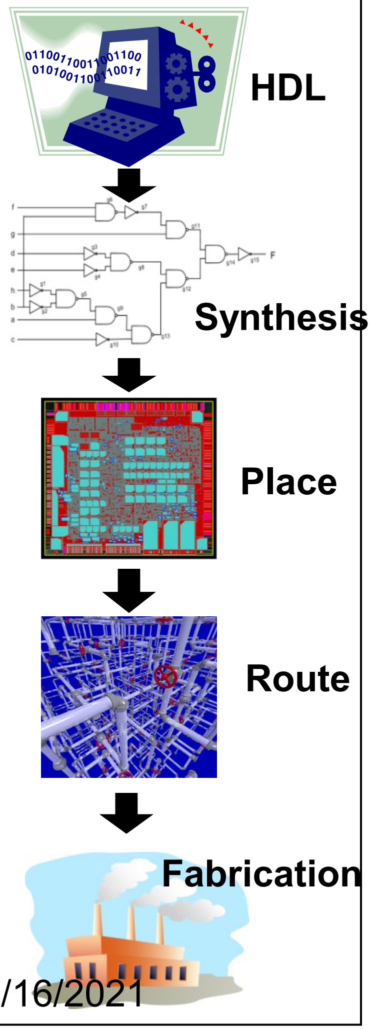
- Cryptography
  - Symmetric and Asymmetric Ciphers
    - DES, AES, Diffie-Hellman, and RSA
  - Message Authentication Codes (MAC)
    - Secure Hash Function
    - Keyed-hash message authentication code (HMAC)
  - Digital Signatures
- Hardware Security
  - Semiconductor Supply Chain
  - Counterfeit Integrated Circuits
  - Detection of Counterfeit ICs
    - Recycled and Remarked ICs
  - Avoidance of Counterfeit ICs
    - IC Overproduction, Cloning, Manufacturing Rejection
  - Physically Unclonable Functions (PUFs)
  - True Random Number Generators (TRNGs)

Motivation for Hardware Security

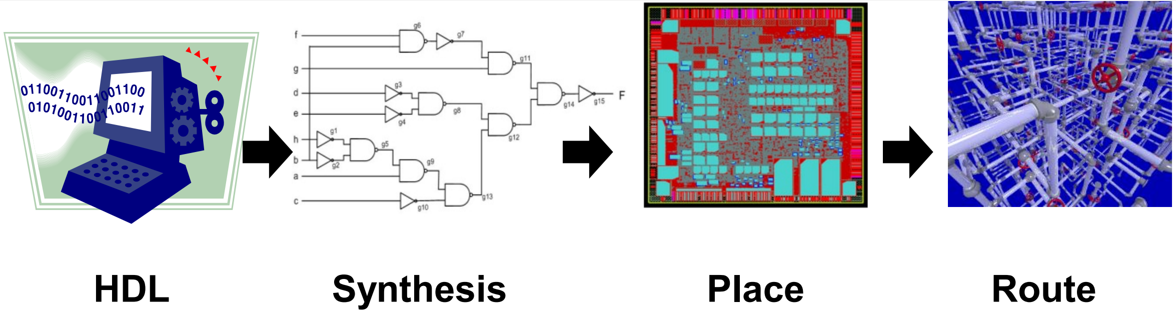
- Shift in the Semiconductor Industries Business Model
- E-waste Management
- The Rise of Internet of Things (IoT) and Cyber Physical Systems (CPS)
- Autonomous Vehicles
- Many more!

Shift in the Semiconductor Industries’ Business Model

Vertical - One Company

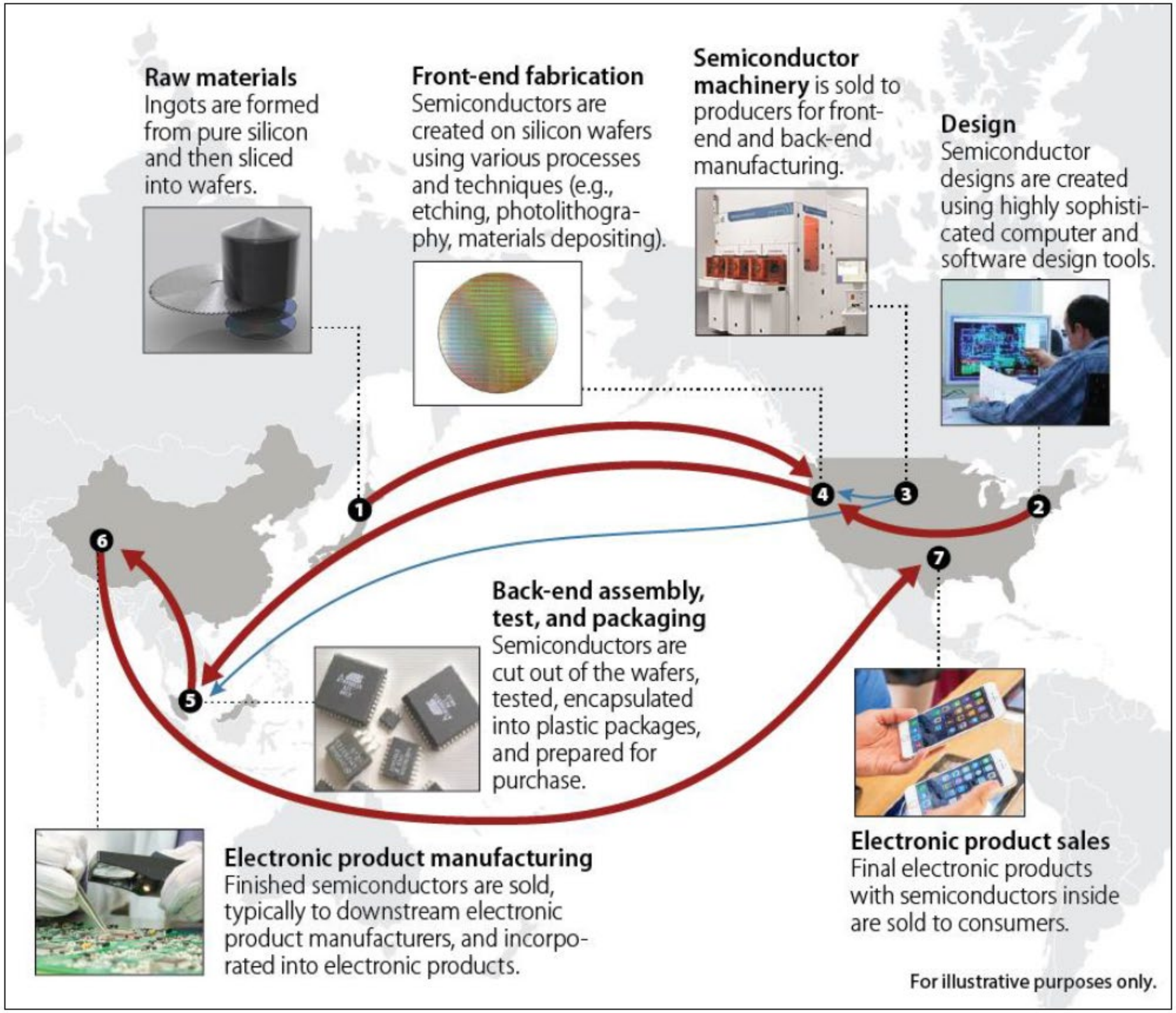


Horizontal (Dominant) – Two or more Companies



Economy of scale: The same fabrication facility serves many fabless companies

Typical Global Semiconductor Production Pattern



Raw materials Ingots are formed from pure silicon and then sliced into wafers.

Front-end fabrication Semiconductors are created on silicon wafers using various processes and techniques (e.g., etching, photolithography, materials depositing).

Semiconductor machinery is sold to producers for front-end and back-end manufacturing.

Design Semiconductor designs are created using highly sophisticated computer and software design tools.

Back-end assembly, test, and packaging Semiconductors are cut out of the wafers, tested, encapsulated into plastic packages, and prepared for purchase.

Electronic product manufacturing Finished semiconductors are sold, typically to downstream electronic product manufacturers, and incorporated into electronic products.

Electronic product sales Final electronic products with semiconductors inside are sold to consumers.

For illustrative purposes only.

Source: CRS, adapted from information provided by SIA.

Notes: This diagram is for illustrative purposes only. Numbered circles do not necessarily reflect where specific production, services, or sales take place.

Electronic Waste Management

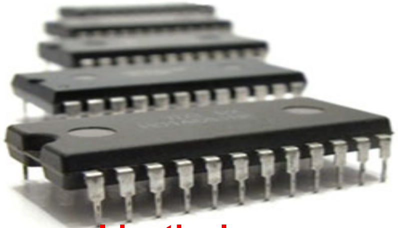
A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new

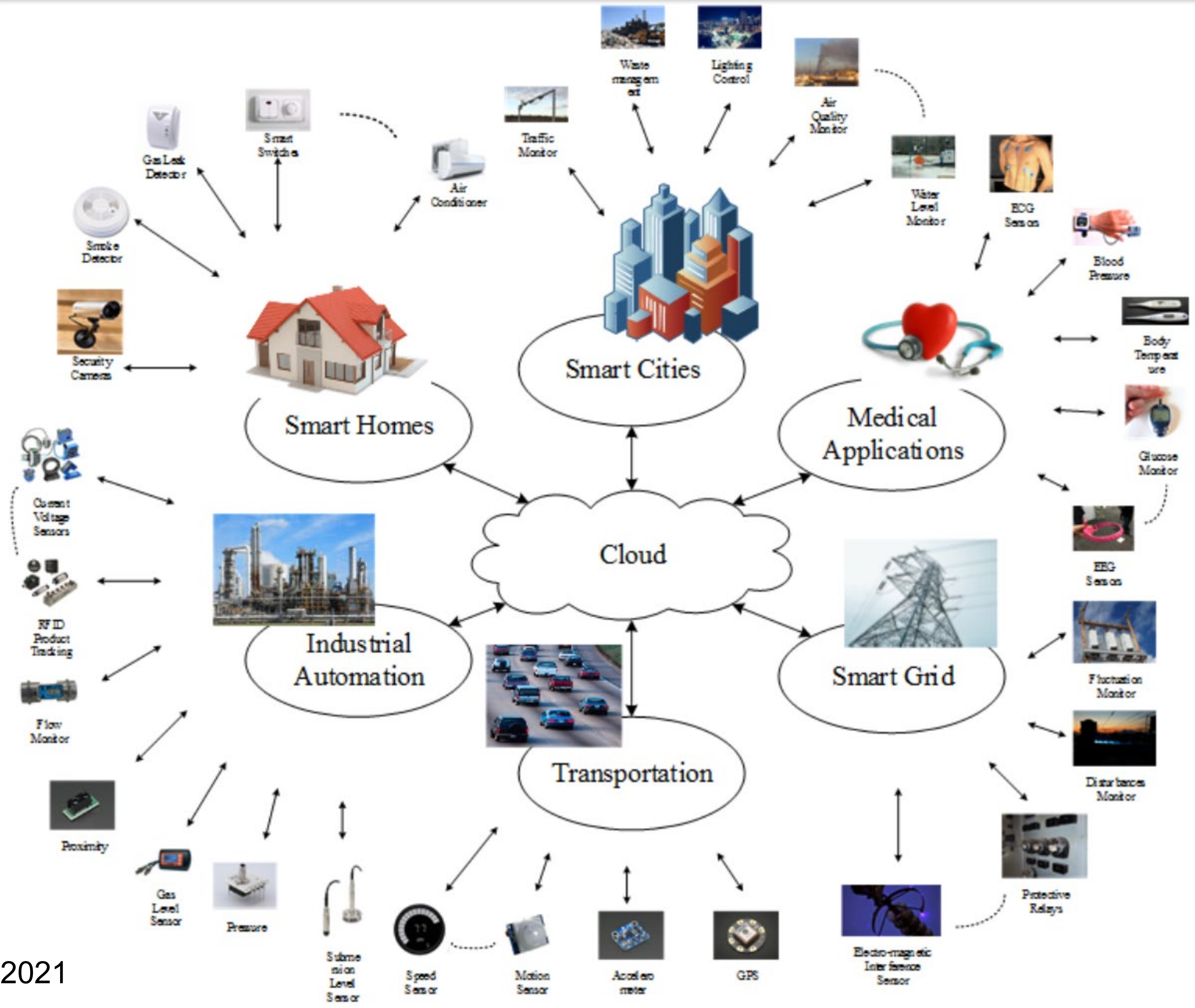


Identical:
Appearance, Function, Specification

Critical Application

Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Internet of Things and Cyber Physical Systems



Definitions

- **Intellectual property** represents the property of your mind or intellect - proprietary knowledge
- The four legally defined forms of IP
  - **Patents** When you register your invention with the government, you gain the legal right to exclude anyone else from manufacturing or marketing it
  - **Trademarks** A trademark is a name, phrase, sound or symbol used in association with services or products
  - **Copyrights** Copyright laws protect written or artistic expressions fixed in a tangible medium
  - **Trade secrets** A formula, pattern, device or compilation of data that grants the user an advantage over competitors

Definitions – Cont.

- **Vulnerability**: Weakness in the secure system
- **Threat**: set of circumstances that has the potential to cause loss or harm
- **Attack**: The act of a human exploiting the vulnerability in the system
- Computer security aspects
  - **Confidentiality**: the related assets are only accessed by authorized parties
  - **Integrity**: the asset is only modified by authorized parties
  - **Availability**: the asset is accessible to authorized parties at appropriate times

Piracy – Some True Stories

- In 2000, Chen Jin, finished Ph.D. in computer engineering at UT Austin
- He went back to China, first to Motorola research and then to Jiaotong University as a faculty
- In 2003, he supervised a team that created one of China's first homegrown DSP IC
- Chen was named one of China’s brightest young scientists, funded his own lab, got a huge grant from the government
- In 2006, it was revealed that he faked the chip, stealing the design from Texas Instruments!

The Athens Affair

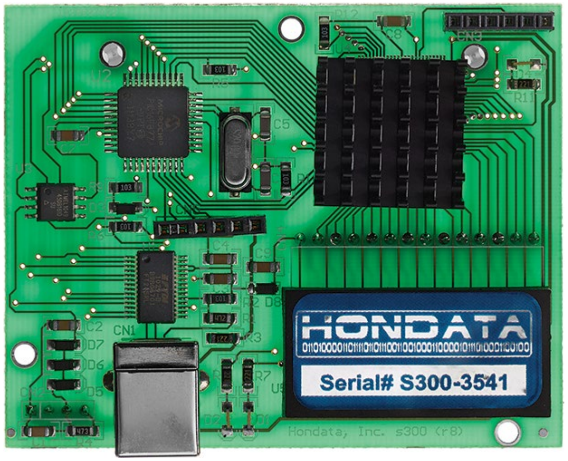
- In March 8, 2005, Costas Tsalikidis, a 38-year-old Engineer working for Vodafone Greece committed suicide – linked to the scandal!
- The next day, the prime minister got notified that his cell phone – and those of many other high-rank officials – were hacked!
- Earlier in Jan, investigators had found rogue software installed on the Vodafone Greece by parties unknown
- The scheme did not depend on the wireless nature
- A breach in keeping keys in a file – Vodafone was fined €76 million December 2006!

Cisco Clones

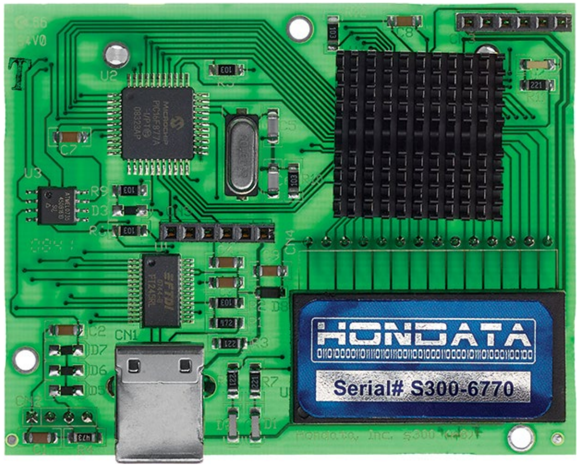
- Ehab Ashoor, Sugarland, Texas, was sentenced in the Southern District of Texas to 51 months in prison and ordered to pay $119,400 in restitution to Cisco Systems.
- Ashoor purchased counterfeit Cisco Gigabit Interface Converters (GBICs) from an online vendor in China with the intention of selling them to the U.S. Department of Defense for use by U.S. Marine Corps personnel operating in Iraq.
- As of 2010, more than $143 Million in Seizures and 30 felony cases from Initiative Targeting Traffickers in Counterfeit Network Hardware (Operation Network Raider)

Clones - Cont.

- FBI charged a Florida man, Marc Heera, with selling a cloned version of the Hondata s300, a plug-in module for the engine computer that reads data from sensors in Honda cars and automatically adjusts the air-fuel mixture, idle speed, and other factors to improve performance (February 2014).



Fake



Genuine

Interesting Articles

- **Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market**, IEEE Spectrum, Apr. 2017.
- J. Villasenor and M. Tehranipoor, “**The Hidden Dangers of Chop Shop Electronics**” IEEE Spectrum, Sep. 2013.
- **The Hunt for the Kill Switch**, IEEE Spectrum, May 2008.

- Next few classes
  - Cryptography