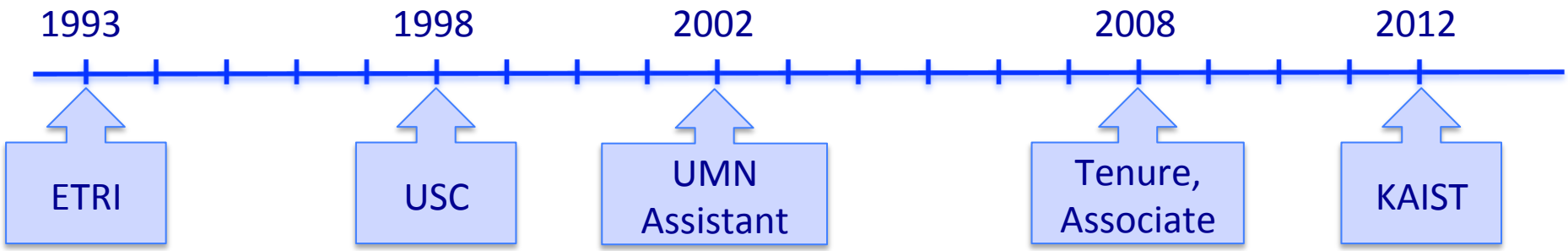
# Hacking Sensors with EMI

Yongdae Kim

KAIST

With D. Foo Kune, J. Backes, S. Clark, D. Kramer, M. Reynolds, K. Fu, W. Xu




- KAIST chaired Professor at EE and GSIS, KAIST (2012. 9 ~)

- 20 year career in security research
  - Applied cryptography, Group key agreement, Storage, P2P, Mobile/Sensor/ Ad-hoc/cellular Networks, Social networks, Internet, Anonymity, censorship, Medical devices, smart meters, Embedded devices, cyber Physical Systems

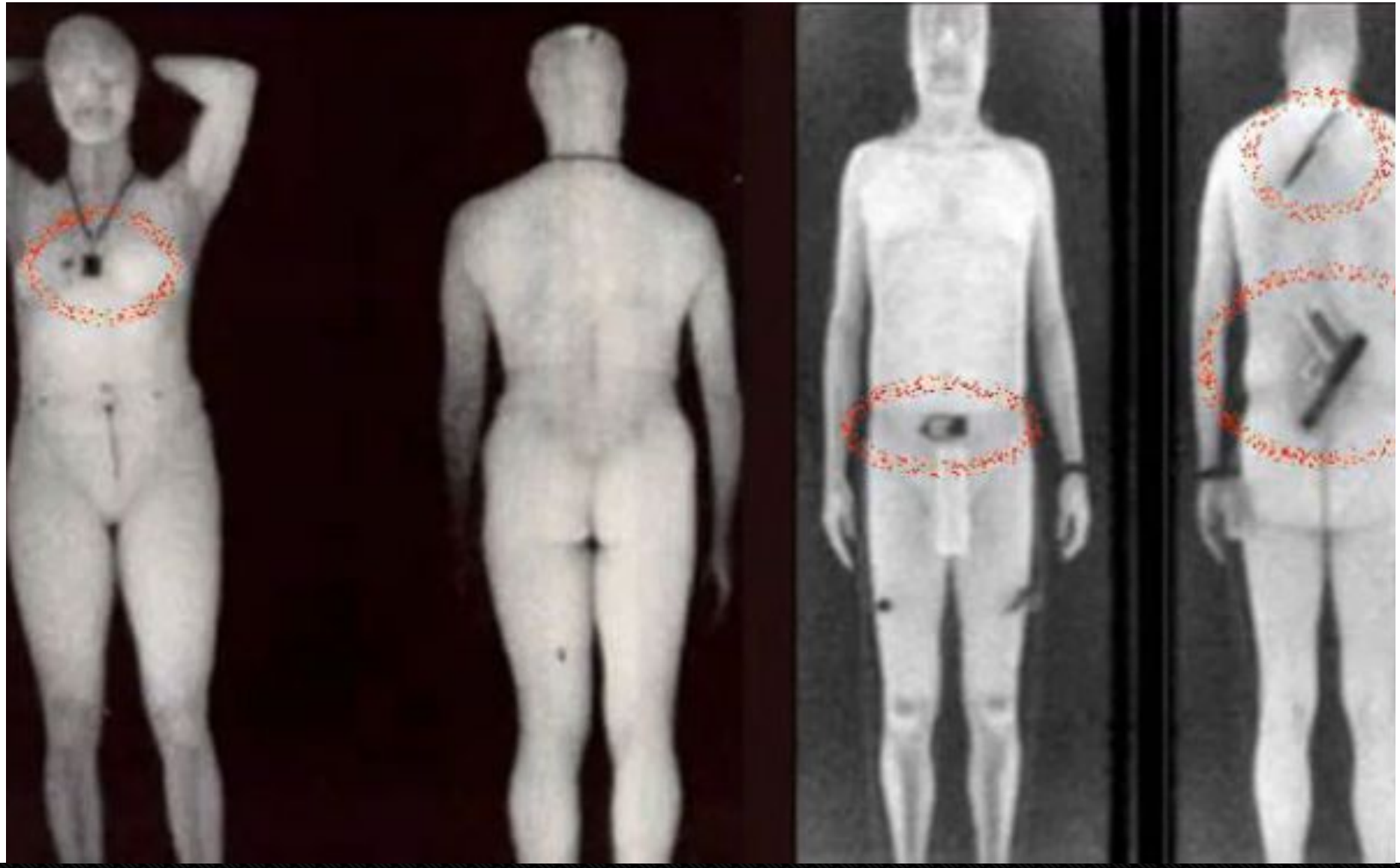
- Some hacking experience
  - Shutdown whole eMule DHT using a single Pc with 100MBps link
  - controlling Network coordinate systems
  - Membership-hiding Botnet (Overlay networks)
  - Remote location tracking on GSM
  - Shutting down the Internet control Plane using Botnet

# Security 101: Think like an Adversary

- Introduction (2 wks)
  - Introduction
  - Attack Model, Security Economics, Legal Issues, Ethics
- common Failures (3 wks)
  - User Interface/Psychological Failures
  - Software Engineering Failures and Malpractices
  - Data mining/Machine Learning Failures
- case Study (10 wks)
  - Peer-to-Peer System Security
  - Social Network Security and Privacy
  - Botnet/Malware
  - cloud computing Security
  - Internet control Plane Security
  - cellular Network Security
  - Mobile Phone Security
  - Security of Automobiles
  - Smart Grid/Meter Security
  - Medical Device Security

http://security101.kr

# TSA Body Scanner



# BMW Stealer

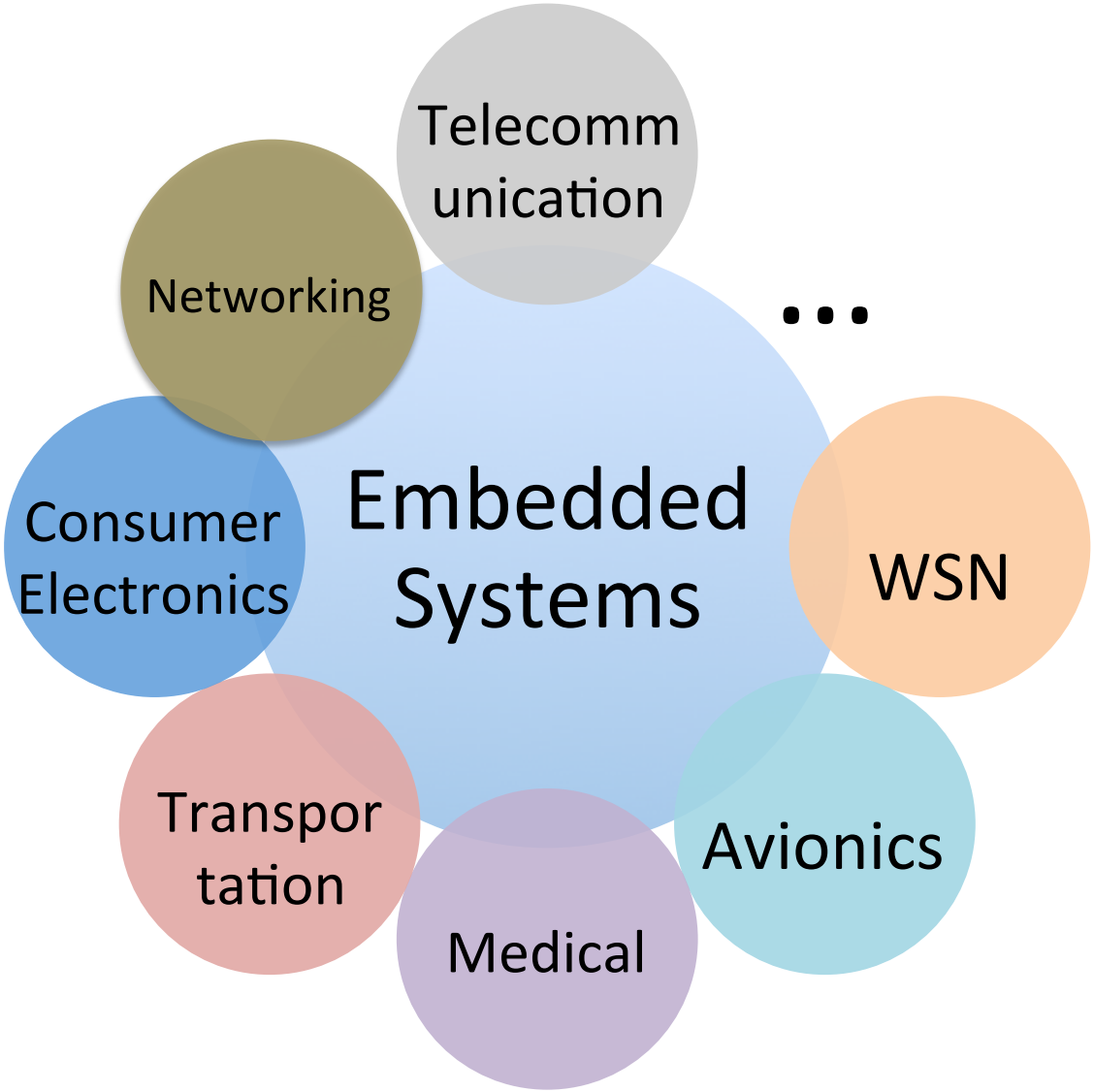
- First, the car is entered
  - nearby RF jammers that block the lock signal
  - breaking a window
    - » exploiting a gap in the car's internal ultrasonic sensor system to avoid tripping the alarm.
- connect a device to the car's OBD-II connector
  - Access to the cars' unique key fob digital ID,
  - program a blank key fob to work with the car

http://www.youtube.com/watch?v=DshK4ZXPU90

# Embedded Systems

- a computer system with a dedicated function within a larger mechanical or electrical system
  - often with real-time computing constraints
- embedded as part of a complete device often including hardware and mechanical parts
- optimize it to reduce the size and cost of the product and increase the reliability and performance

# Applications



# Infusion Pump Safety

- During 2005 and 2009, FDA received approximately 56,000 reports of adverse events associated with the use of infusion pumps
  - 1% deaths, 34% serious injuries
  - 87 infusion pump recalls to address safety problems
- The most common types of problems
  - Software Defect
  - User Interface Issues
  - Mechanical or Electrical Failure

# Smart Pump Attack

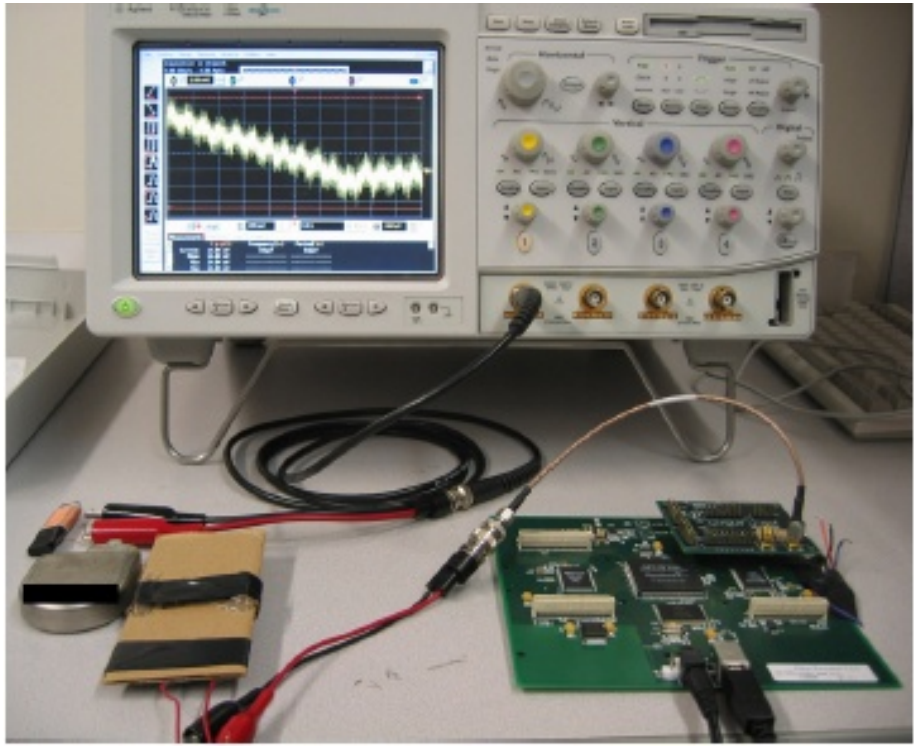
- Barnaby Jack
  - influence any pump within a 91m
  - dispense its entire 300 unit

- A few more details known
  - wirelessly send and receive data over the 900 MHz frequency.
  - custom-built antenna
  - no encryption
  - overrides restrictions that normally prevent the pump from receiving wireless commands to increase dosages.
  - Disable a vibration or loud tone when dispensing a dosage

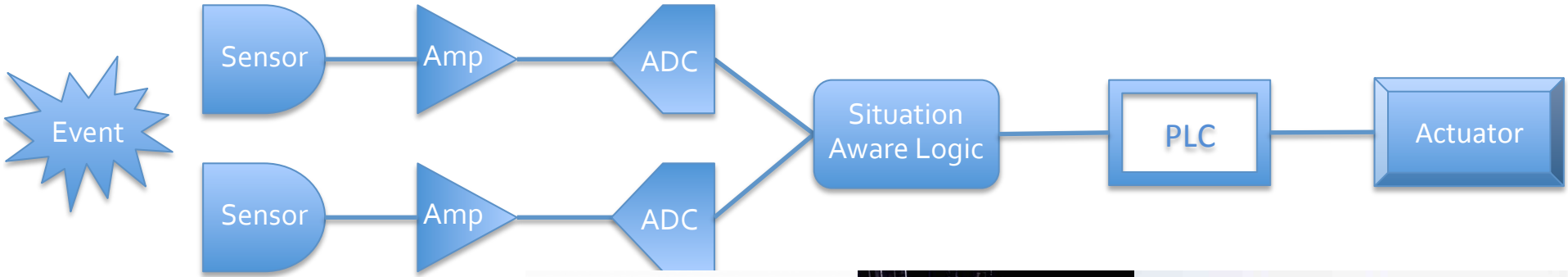
Warning over medical implant attacks, BBC, http://www.bbc.com/news/technology-17623948

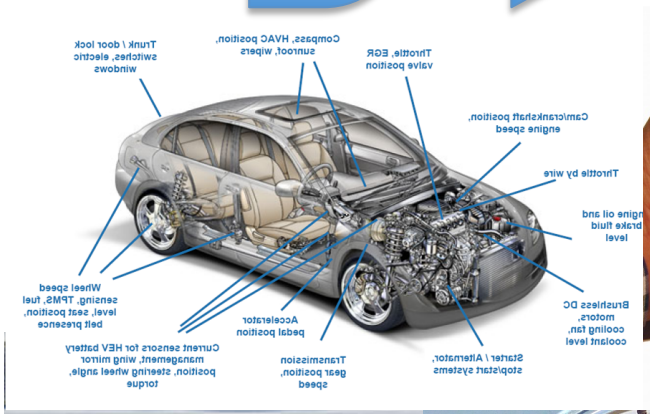
# Intercept communication

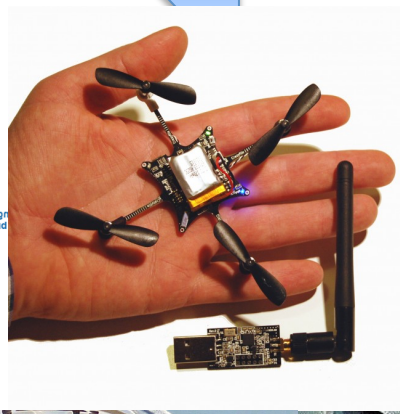
- Observed a timeline and probable data flow model for ICD communication
  - Found clear text representations of private patient data. (Names, numbers and histories)
- Observed telemetry
- Performed attacks using a software radio

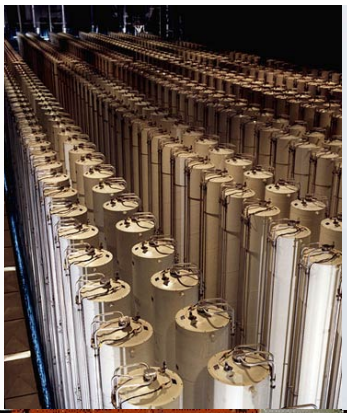


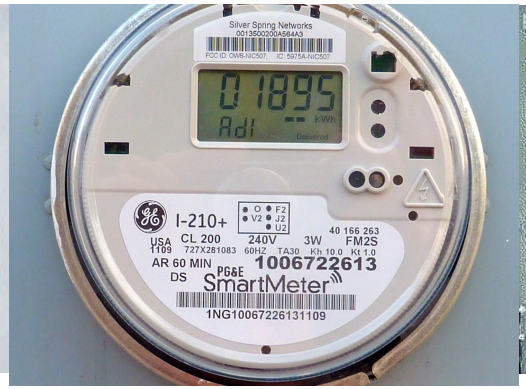
# Sensing-and-Actuation System

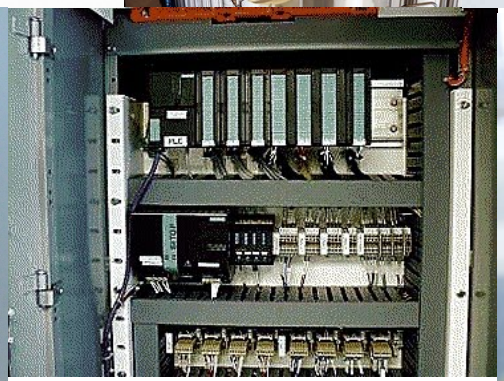


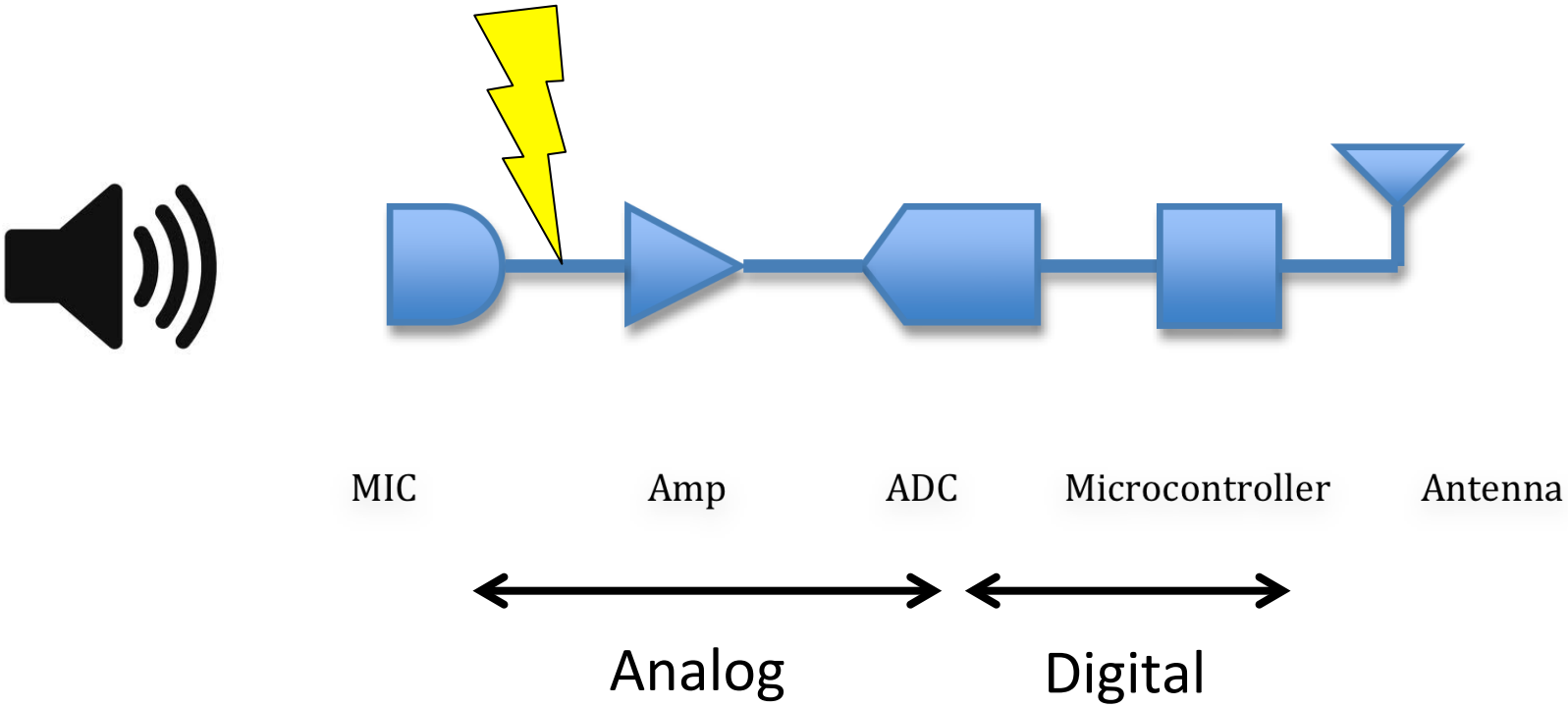






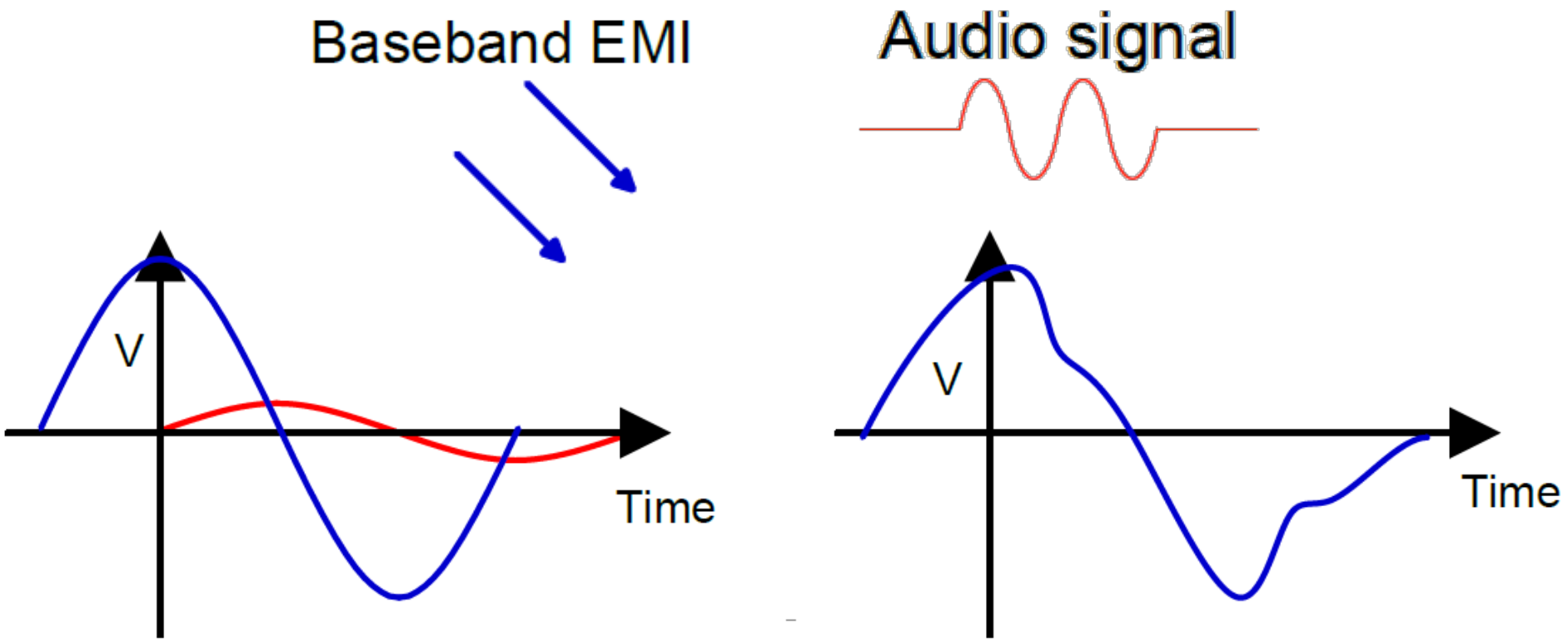
# EMI on analog inputs



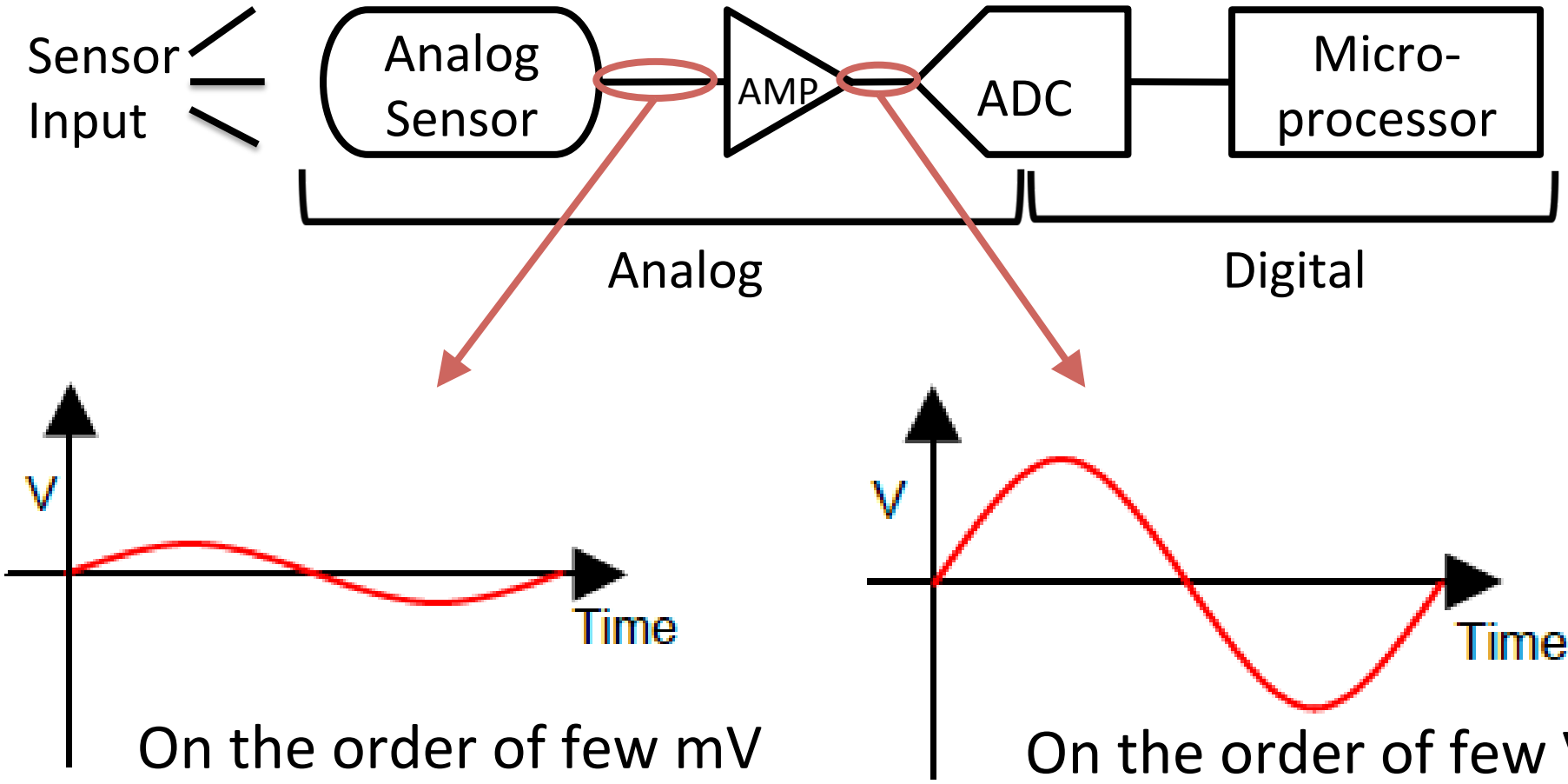
# classification on EMI

| | Intensional | Unintentional |
|---|---|---|
| Low Power | Yet to be explored | Circuit design issue |
| High Power | Can disable circuits | A lot of work |

# Voltage Induction



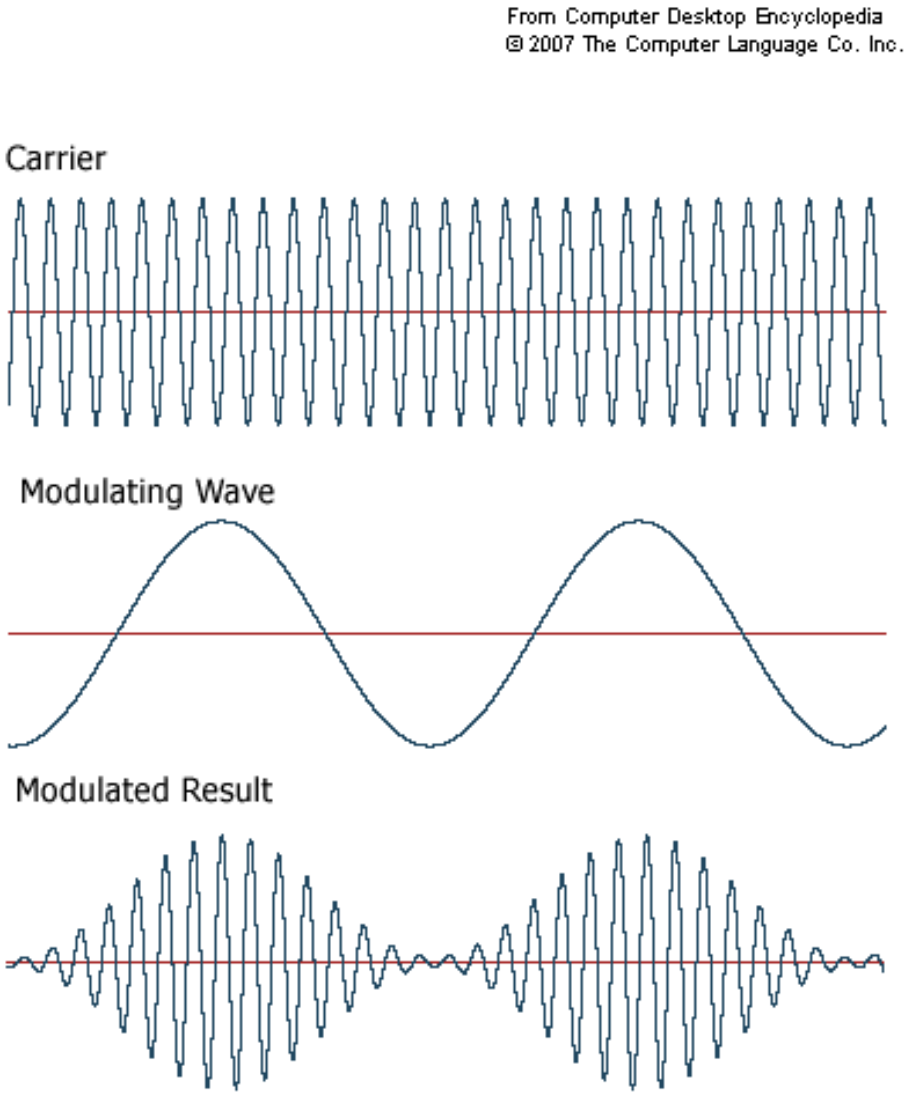
# Between Sensor and Amp?



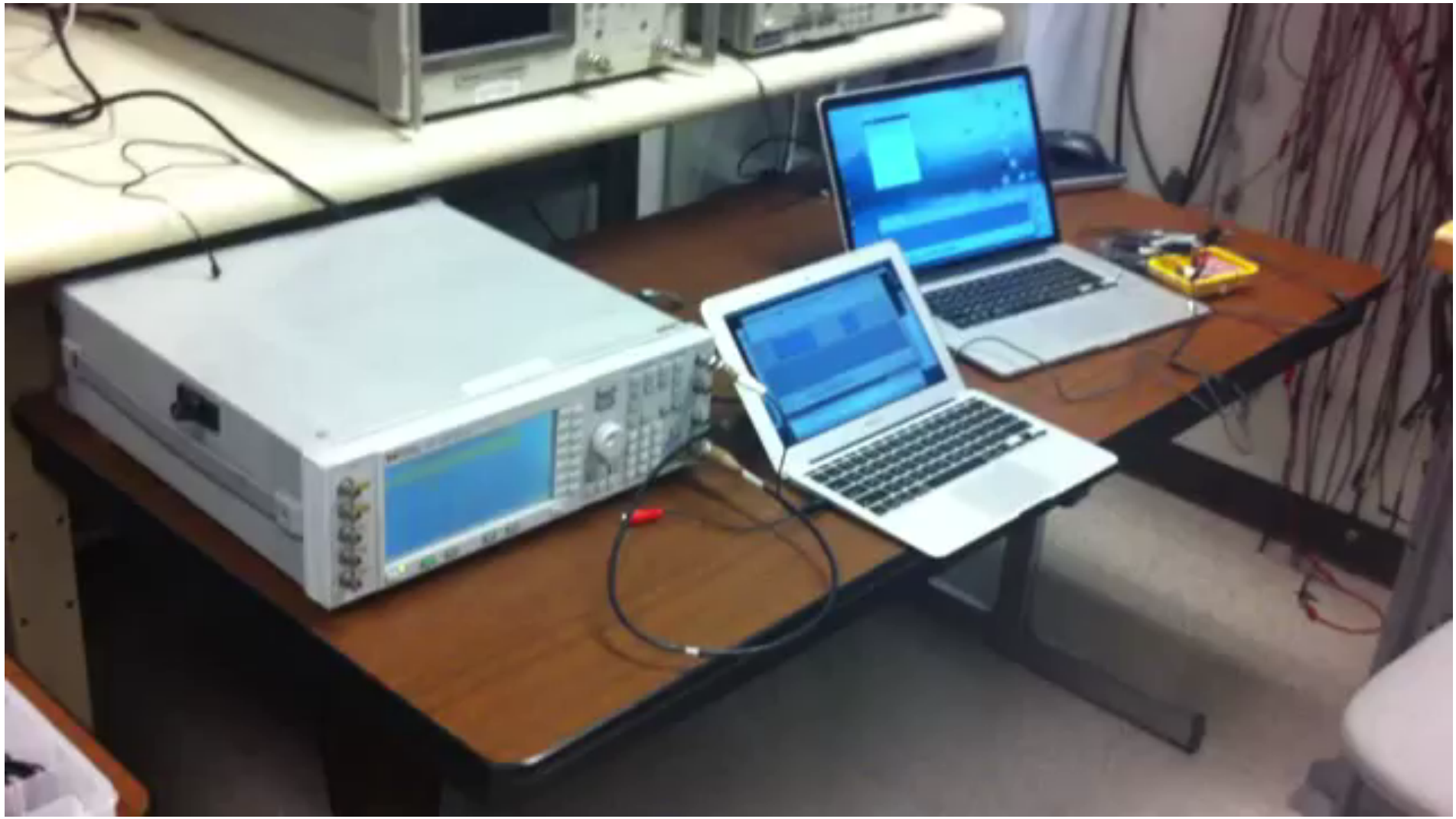
# Modulated EMI Attack

- Signals in high frequency range can be injected well compared to low frequency signals

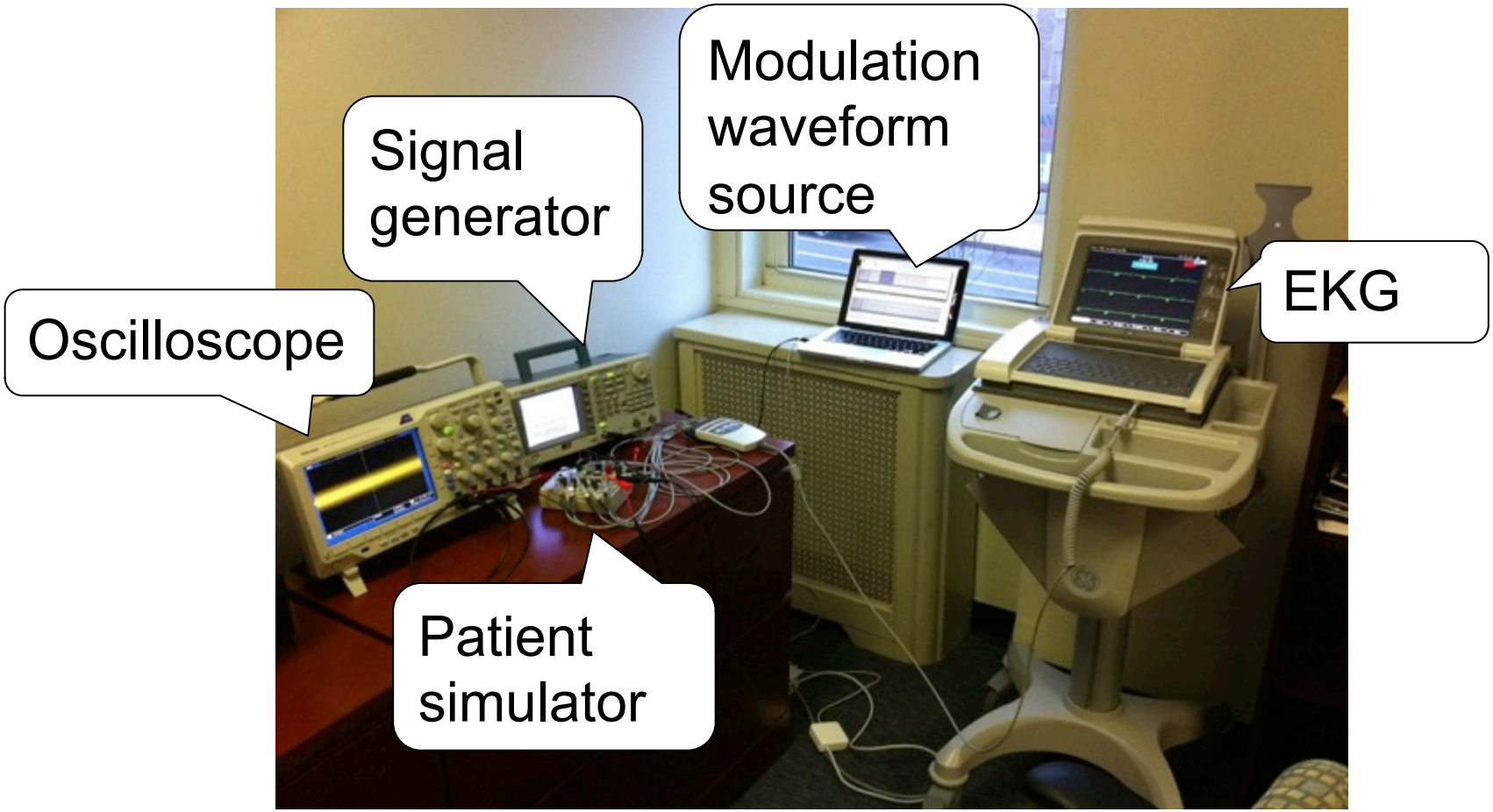
- Demodulation due to
  - Nonlinear components
  - Analog-Digital convertor (ADC)
  - capacitor & Diode



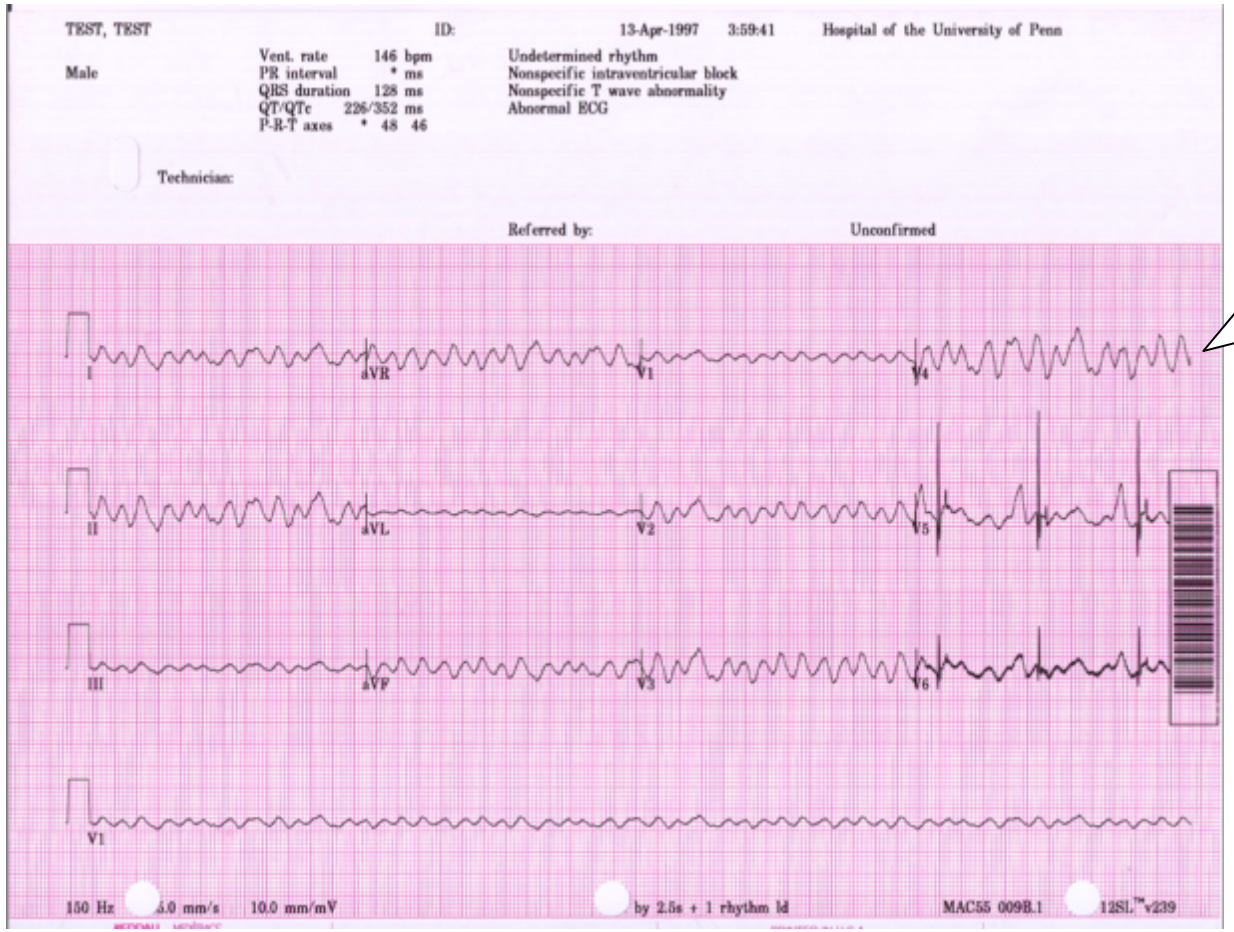
# use case



# Inducing waveforms on EKG



# EKG - v-fib patient




Ventricular fibrillation

Induced 66 bpm signal

# Standard Lead Design

# Application to medical devices

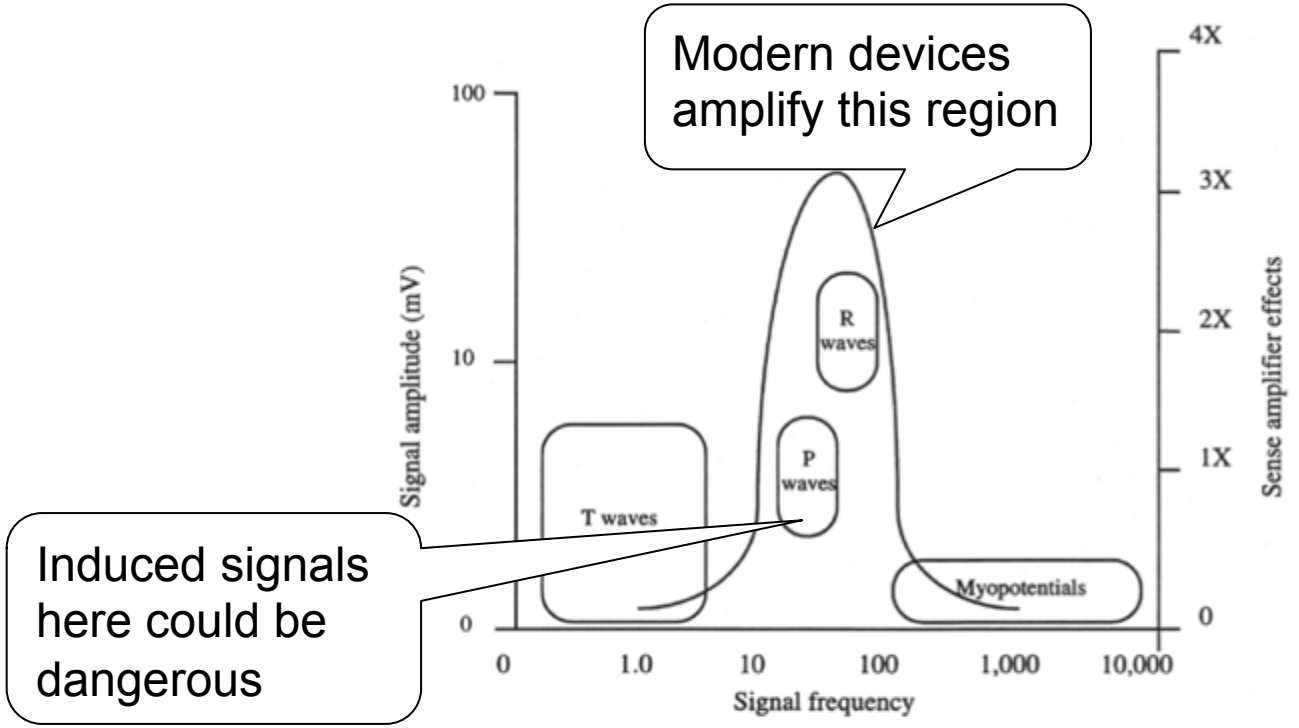
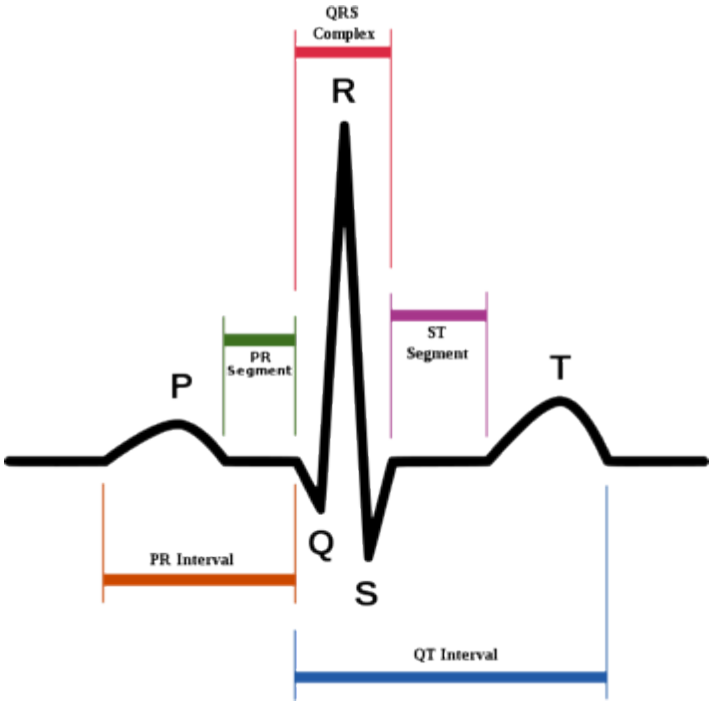



**Fig 17.1** Signal amplitude and frequency from various sources. Modern sense amplifiers employ bell-shaped response curves that amplify signals within the 10–100 Hz range while attenuating signals below and above these frequencies. In this way signals from ventricular depolarization (R waves) and atrial depolarization (P waves) can be amplified and the effects from spurious signals, such as T waves and myopotentials, can be minimized.

# Sensing algorithm

- Assuming bipolar configuration
- QRS complex and detection



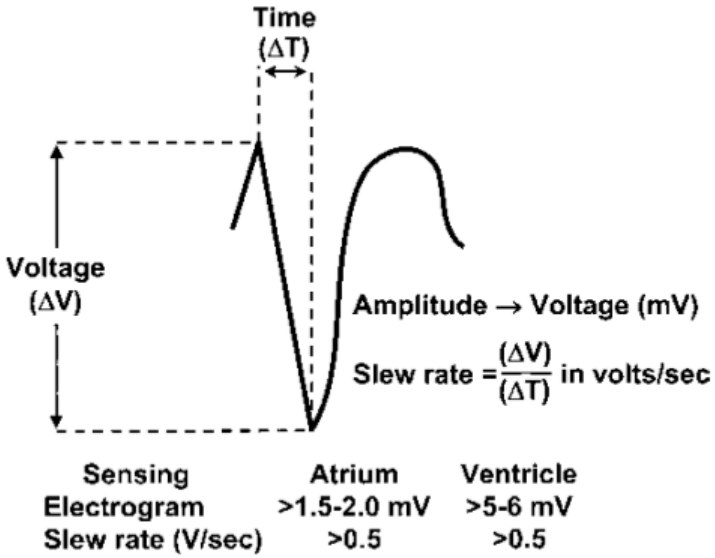
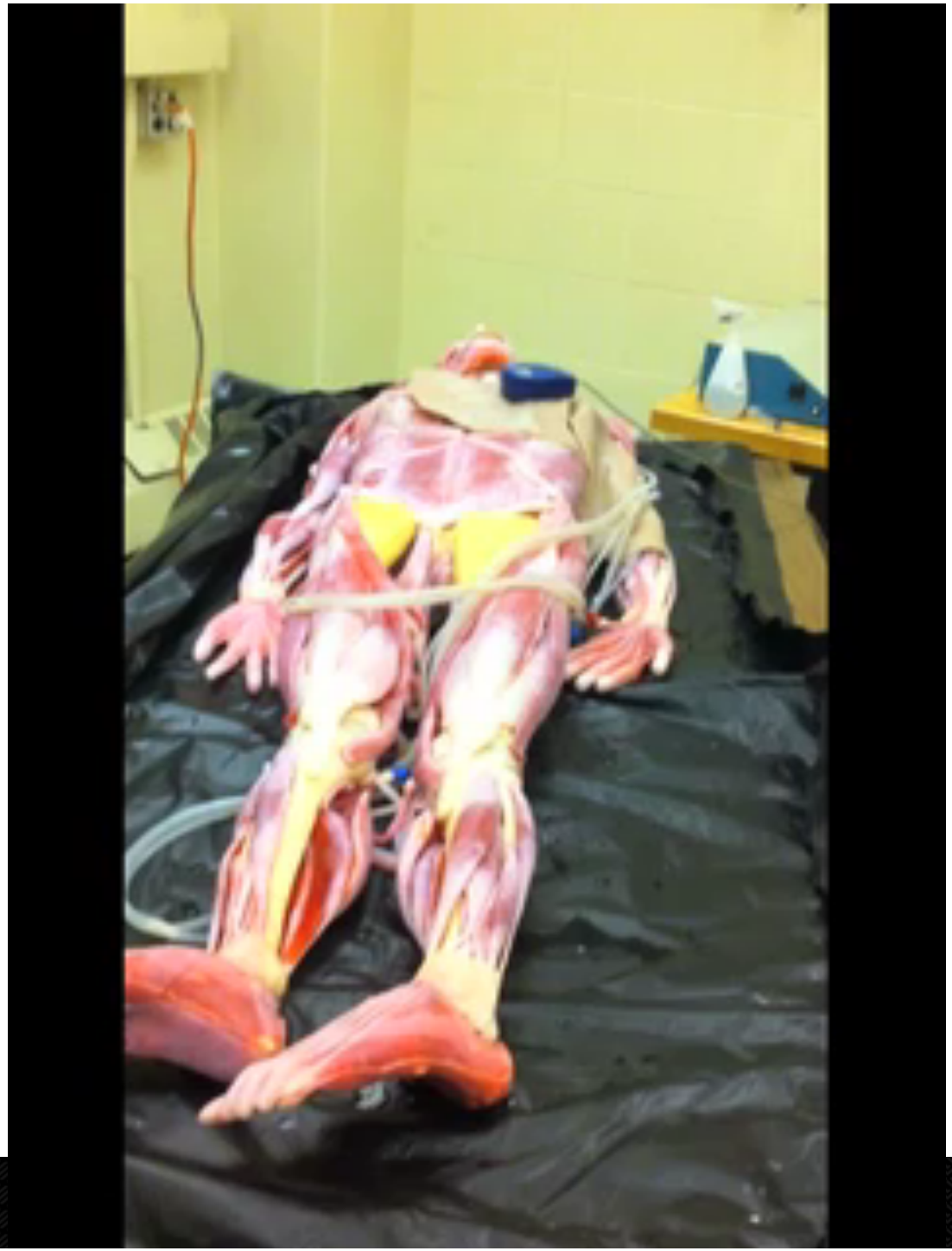



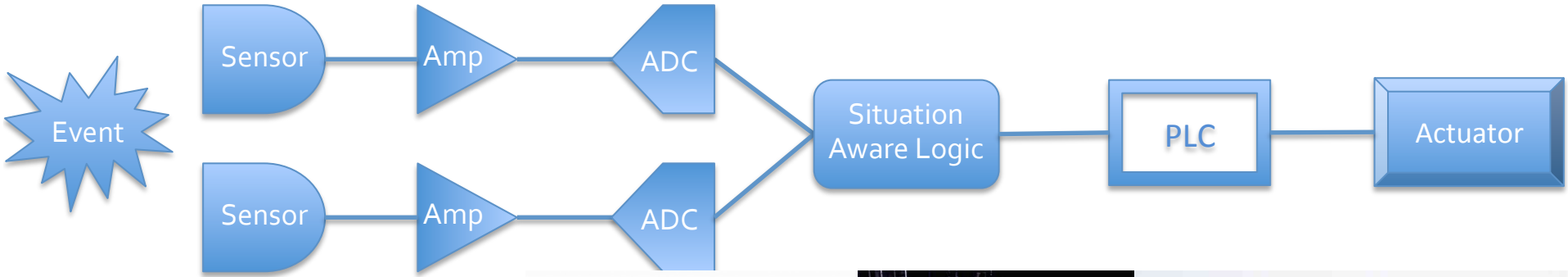

**Fig. 1.9** In the intracardiac electrogram, the difference in voltage recorded between two electrodes is the amplitude, which is measured in millivolts. The slew rate is volts per second and should be at least 0.5.

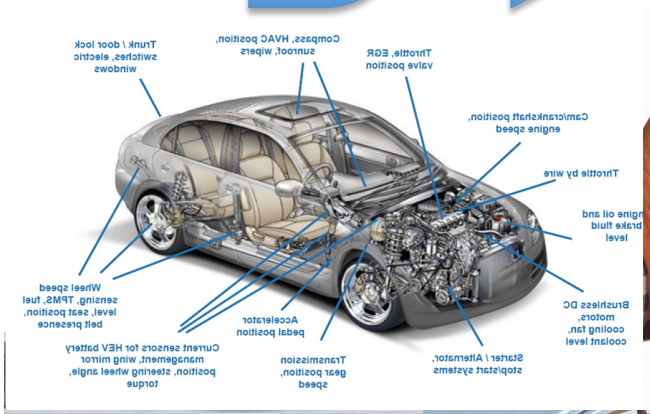
# Results

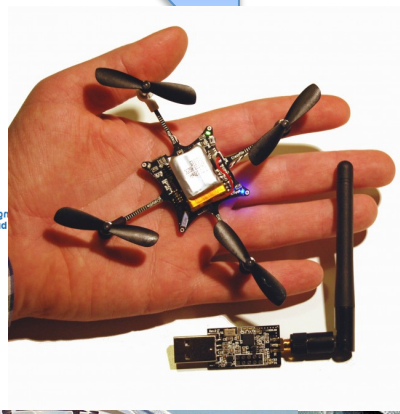
| Device | Open air | Saline | SynDaver |
|---|---|---|---|
| A Inc. Device 1 | 1.36m | 0.03m | Unknown |
| A Inc. Device 2 | 1.57m | 0.05m | 0.08m |
| B Inc. Device | No response | Unknown | Unknown |
| C Inc. Device | 0.76m | Unknown | Unknown |

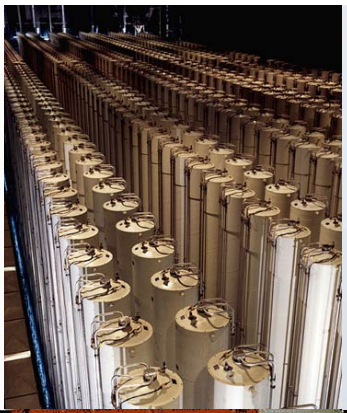


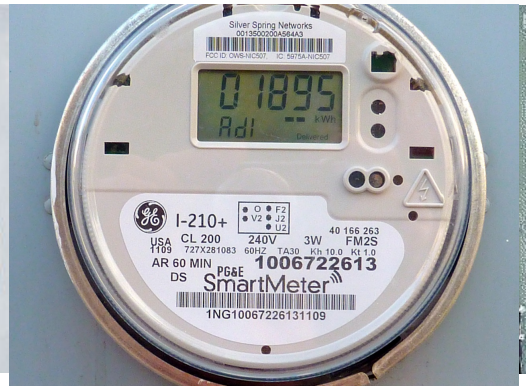
# Sensing-and-Actuation System

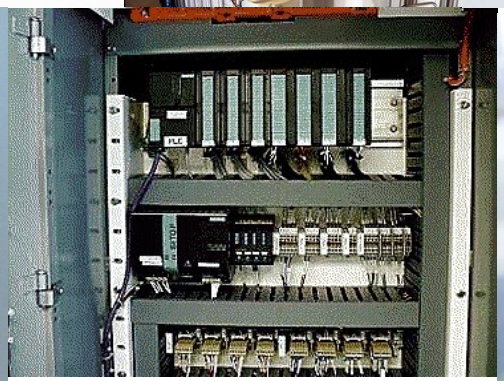








# Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"