Medical Device Cyber Physical Systems - Security

Denis Foo Kune, Yongdae Kim, Nick Hopper
University of Minnesota

NSF Program Review, Jan 31, 2012

UNIVERSITY OF MINNESOTA
Driven to Discover℠

Is the data trustworthy?

- Can we trust data in the network?
  - Untrustworthy data in CPS can be catastrophic
    - Pacing inhibition
  - Problem magnified in Medical Device context
    - Stuxnet, in a clinical environment
- Broad problem
  - Maintain safety and reliability under adversarial conditions
    - Trusted nodes and trusted data paths
  - Previous work done in securing
    - Communication protocols stacks
    - Infrastructure
  - Limited material available on analog input circuitry

UNIVERSITY OF MINNESOTA
Driven to Discover℠

Analog input interference

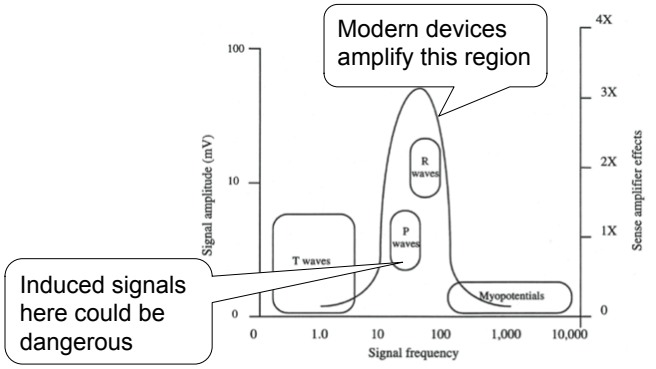
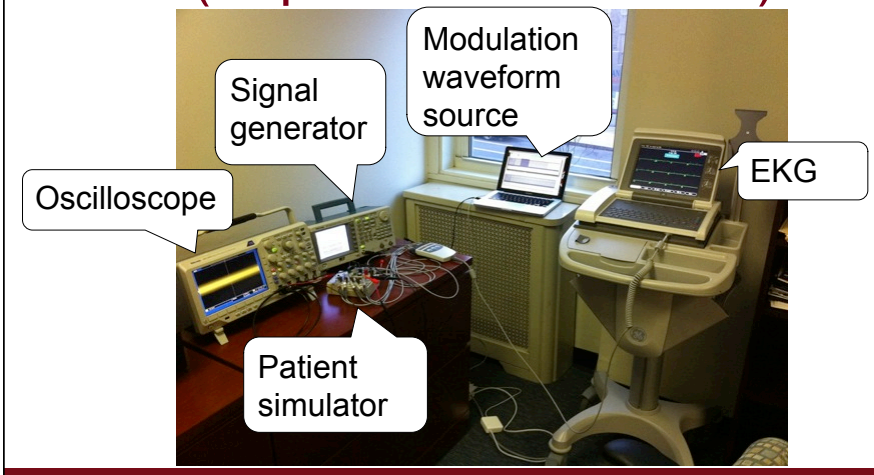
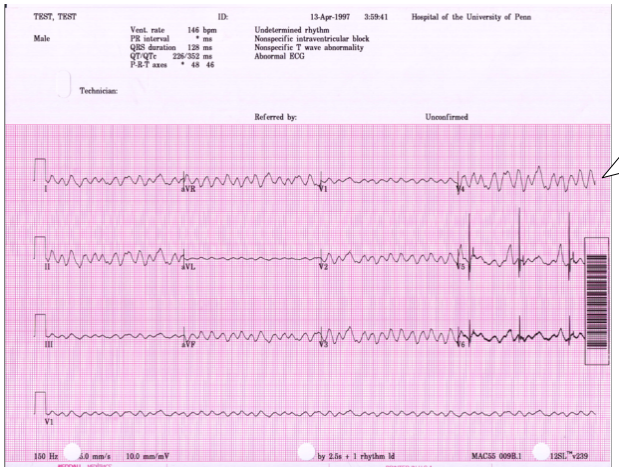


Fig 17.1 Signal amplitude and frequency from various sources. Modern sense amplifiers employ bell-shaped response curves that amplify signals within the 10–100 Hz range while attenuating signals below and above these frequencies. In this way signals from ventricular depolarization (R waves) and atrial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

Inducing waveforms on EKG (Experiments at Penn)

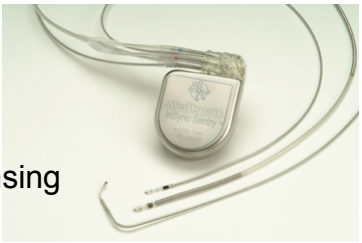


EKG – V-fib patient



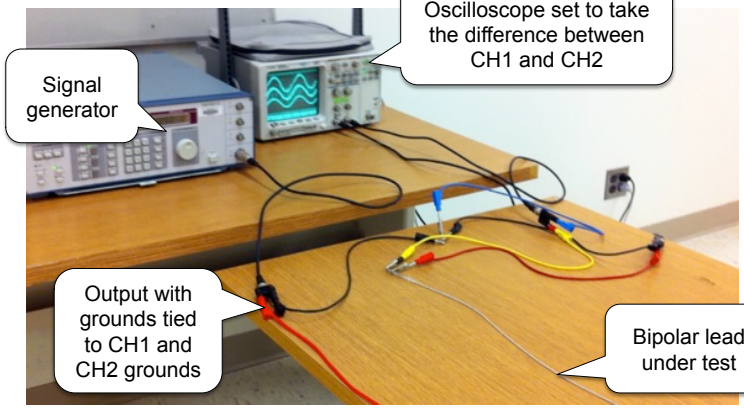
Inducing waveforms on ICD

- Implantable devices
  - Pacing inhibition
  - Inductive properties of leads
  - Understand the physical sensing process of devices
  - Help from
    - University of Massachusetts, Amherst
    - University of South Carolina



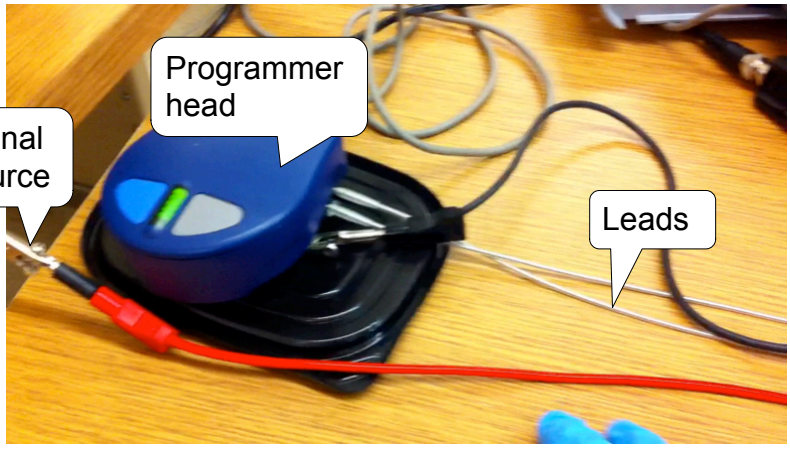
UNIVERSITY OF MINNESOTA
Driven to Discover℠

Setup



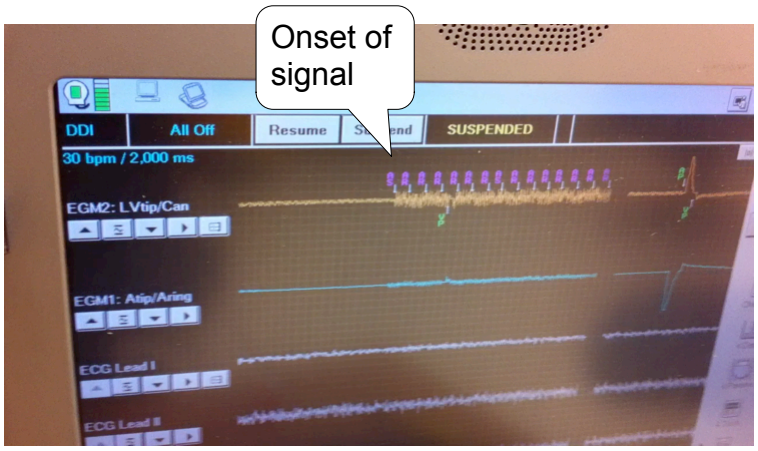
UNIVERSITY OF MINNESOTA
Driven to Discover℠

Setup

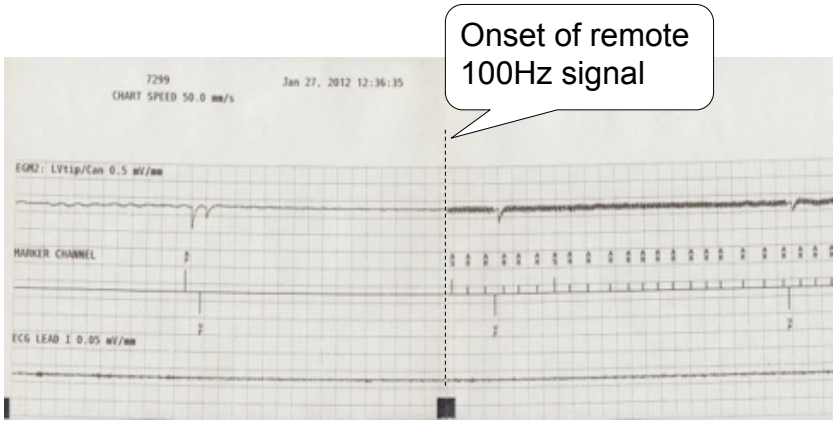


UNIVERSITY OF MINNESOTA
Driven to Discover℠

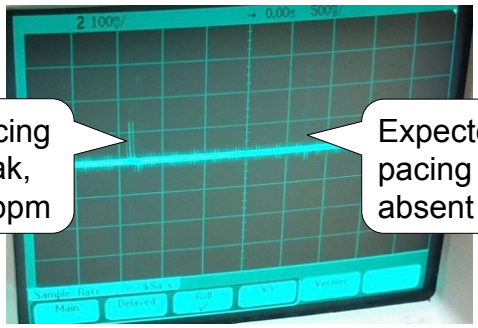
Pacing inhibition



ICD – pacing inhibition



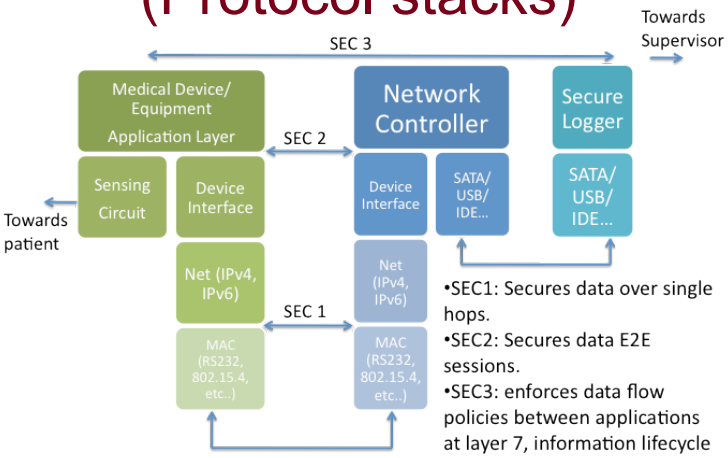
ICD – pacing inhibition



Improving current design

- Effective analog and digital defenses
  - Improve discrimination between induced and measured voltages
  - Improve detection algorithms in devices
- Noise removal as early as possible
  - Improve leads, matching antennas
    - Current designs focus on the electrical and mechanical properties.
    - We look at inductive properties as well
- Collaboration with St Jude Medical, Medtronic, Adventium
  - Review of our findings and solutions
  - Boston Scientific putting us in contact with appropriate team

Securing the data path (Protocol stacks)



- SEC1: Secures data over single hops.
- SEC2: Secures data E2E sessions.
- SEC3: enforces data flow policies between applications at layer 7, information lifecycle and patch management

Broad intellectual impact

- Clinical environments are a special case of constrained devices
- Improving security of analog sensing circuitry
  - Applicable to CPS and beyond
  - Ex. flow, temperature and pressure sensors in industrial applications
- Secure architecture
  - Applicable to
    - Cyber Physical Systems
    - Industrial sensing and control
  - Centralized management
  - Heterogeneous nodes
  - Connection to external “business” network
  - Diversity of protocols, some of which are unsecured legacy protocols

Collaboration

Secure architecture, heterogeneous protocol stacks, secure logging
Analysis of analog EMI on external devices (EKG)

Wireless signal propagation and impact on ICD analog sensing circuitry
Equipment support including SynDaver and standard procedures

Solutions to vulnerabilities in implantable medical device analog circuits
Advise on impact of vulnerabilities and practicality solutions

Conclusion and direction

- Better understanding of problem space in analog inputs
  - Red Team exercise to quantify parameters of problem
  - Investigation of areas that didn't receive as much attention
- Improve design of devices and systems
  - Develop secure architecture for Integrated Clinical Environments
  - Improve security of analog sensing circuitry
- Ensure practical applicability of results
  - Collaboration with industry