Embedded Security

EECE 5698-08: Special Topics: Cyber-Physical Security of IoT Systems in the Age of AI

Lecture 5: Sound and Sensors

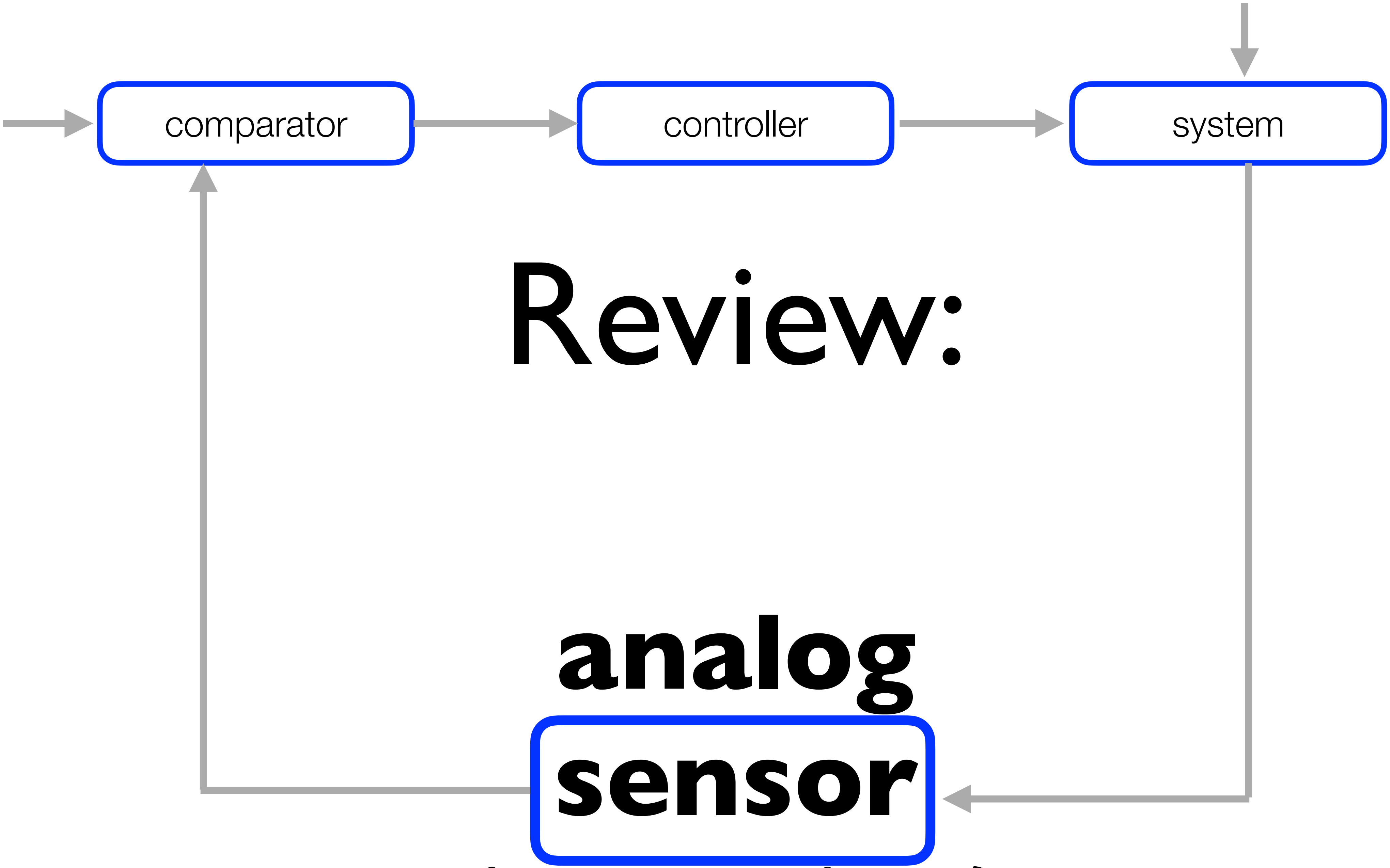
Prof. Kevin Fu

September 22, 2025

https://spqrlab1.github.io/emsec/

1991 Apple IIGS

https://oldcomputers.net/appleiigs.html



Review:

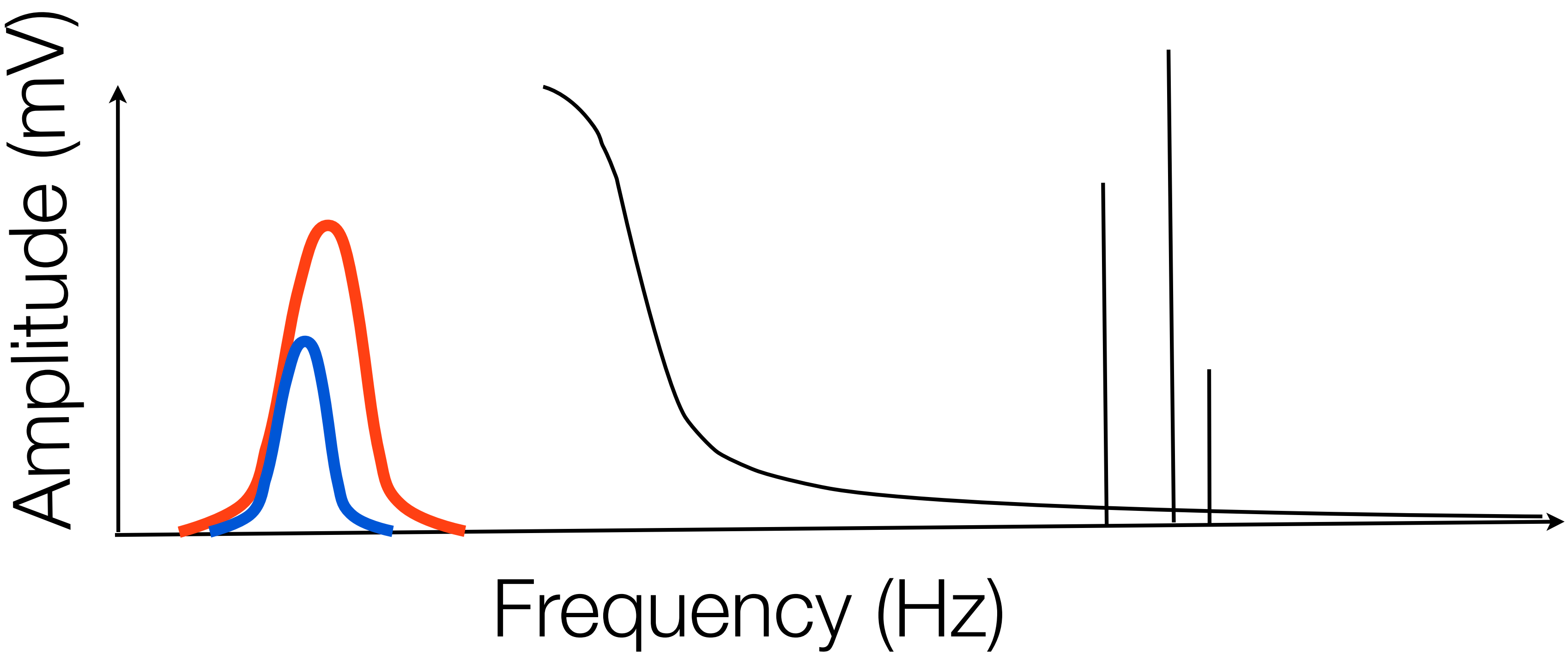
analog sensor integrity?

Last Time: Transduction attacks

- Side channels
  - “Read” side channels violate confidentiality
  - “Write” side channels violate integrity
  - Can use for good to detect malware with power
- **Transduction attacks** exploit the physics of sensors to fool sensors into seeing a false, coherent reality
- **Signal conditioning path:** Transducer, Amplifier, Filter, ADC, microprocessor
- Examples: EMI for thermocouples, microphones, pacemakers

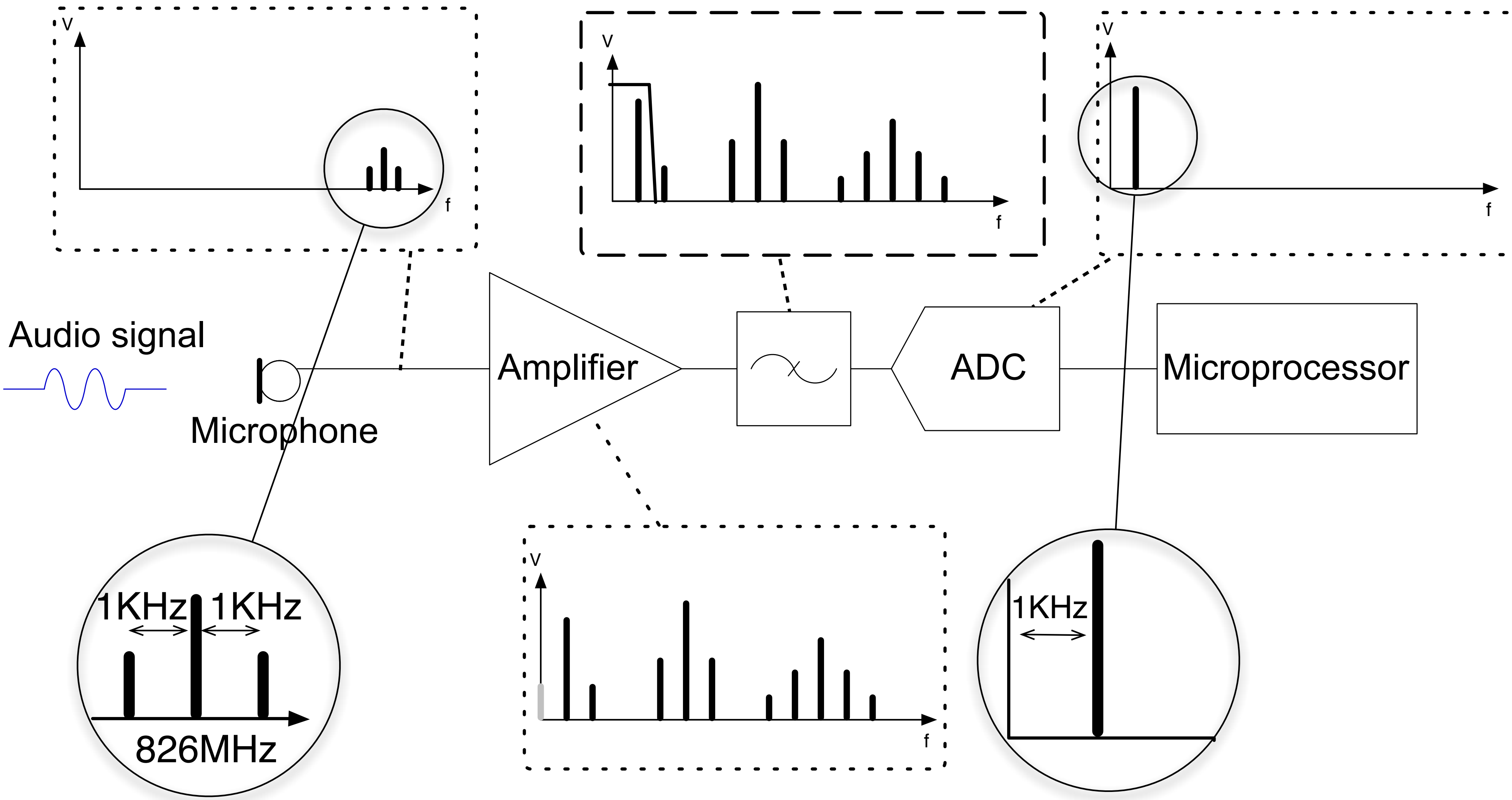
Review: Baseband Injection

- Baseband: frequency range of desired signals.
- Interference outside the baseband is easy to filter.
- Interference in the baseband is hard to remove.



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Review: Self Demodulation



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

intermodulation distortion…

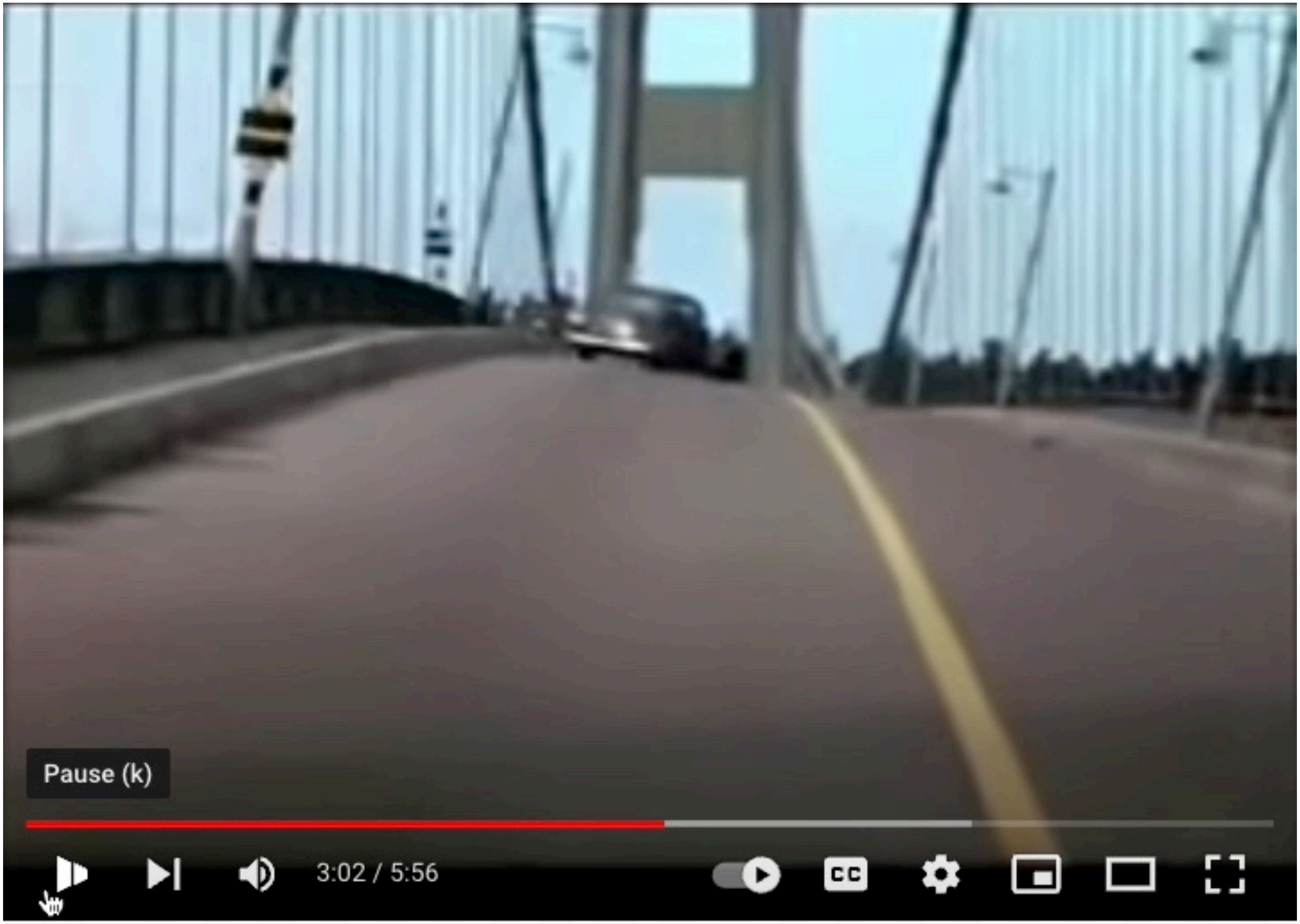
Pop Quiz #3

- Write your name on paper

Today's Learning Goal

- How to use intentional acoustic interference to control MEMS accelerometers
- Gain understanding of the underlying physics necessary for testing attacks for real in lab

Resonant vibrations can damage bridges



Tacoma Narrows Bridge Collapse "Gallopin' Gertie"

14,344,818 views Dec 9, 2006 Watch the amazing "Gallopin' Gertie" November 7, 1940 film clip.
1940 Tacoma Narrows Bridge ...more

Resonant vibrations
can damage ~~bridges~~
MEMS semiconductors

Z-axis of MEMS gyroscopes

- 8 kHz acoustic tone hits resonant frequency of MEMS gyroscope
- Disturbs PID feedback control
- Drone falls from sky

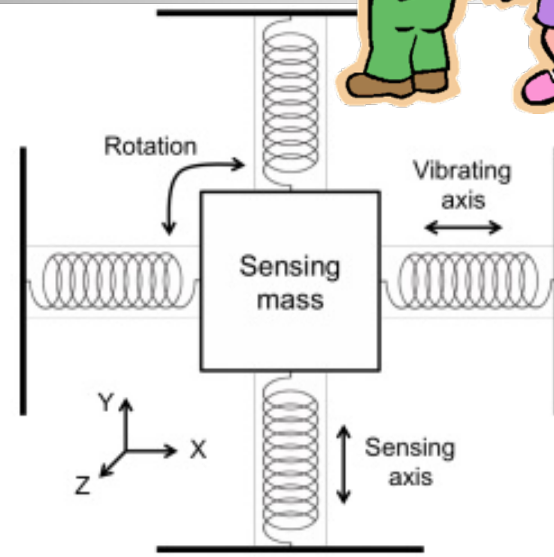


Figure 2: Concept of MEMS gyroscope structure for one axis

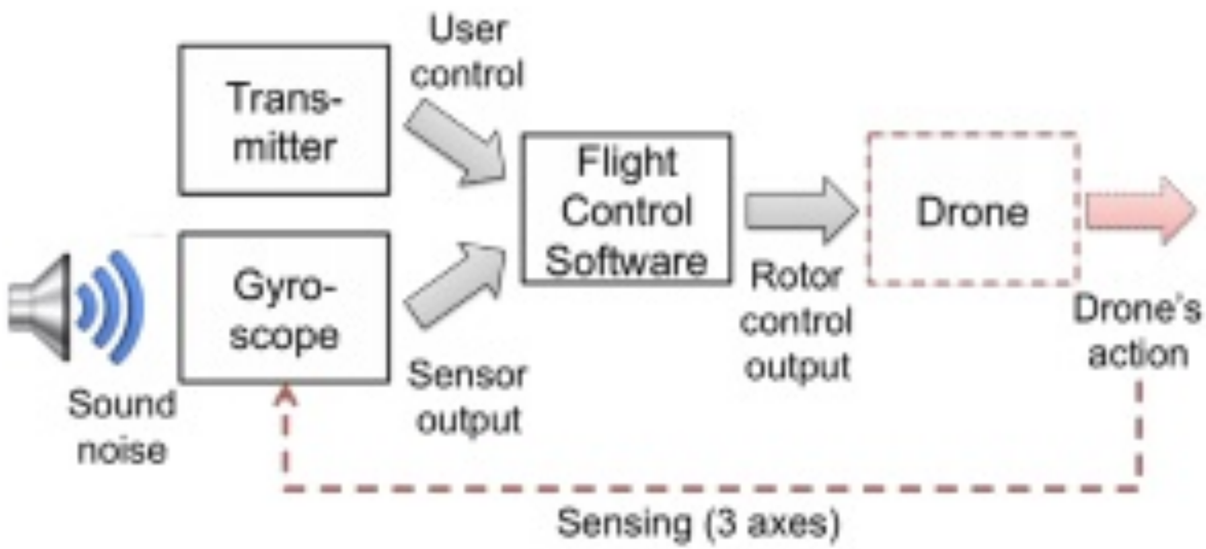


Figure 8: Propagation of the effect of sound noise

[Son et al., USENIX Security' 15]

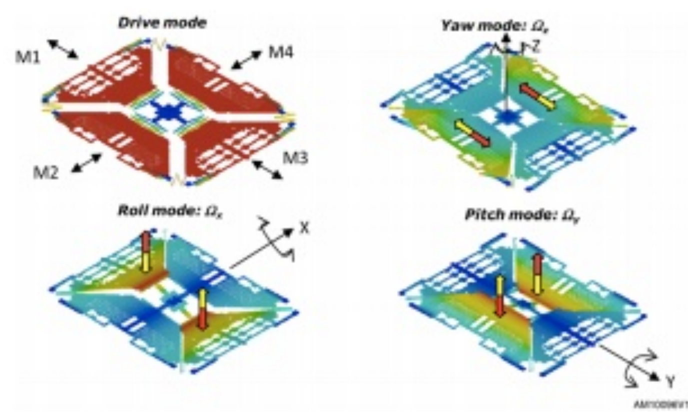
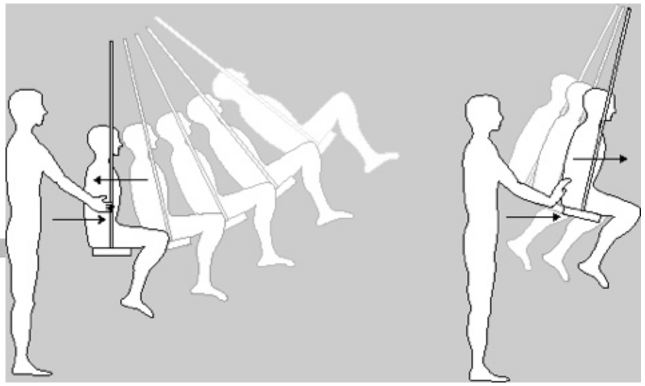
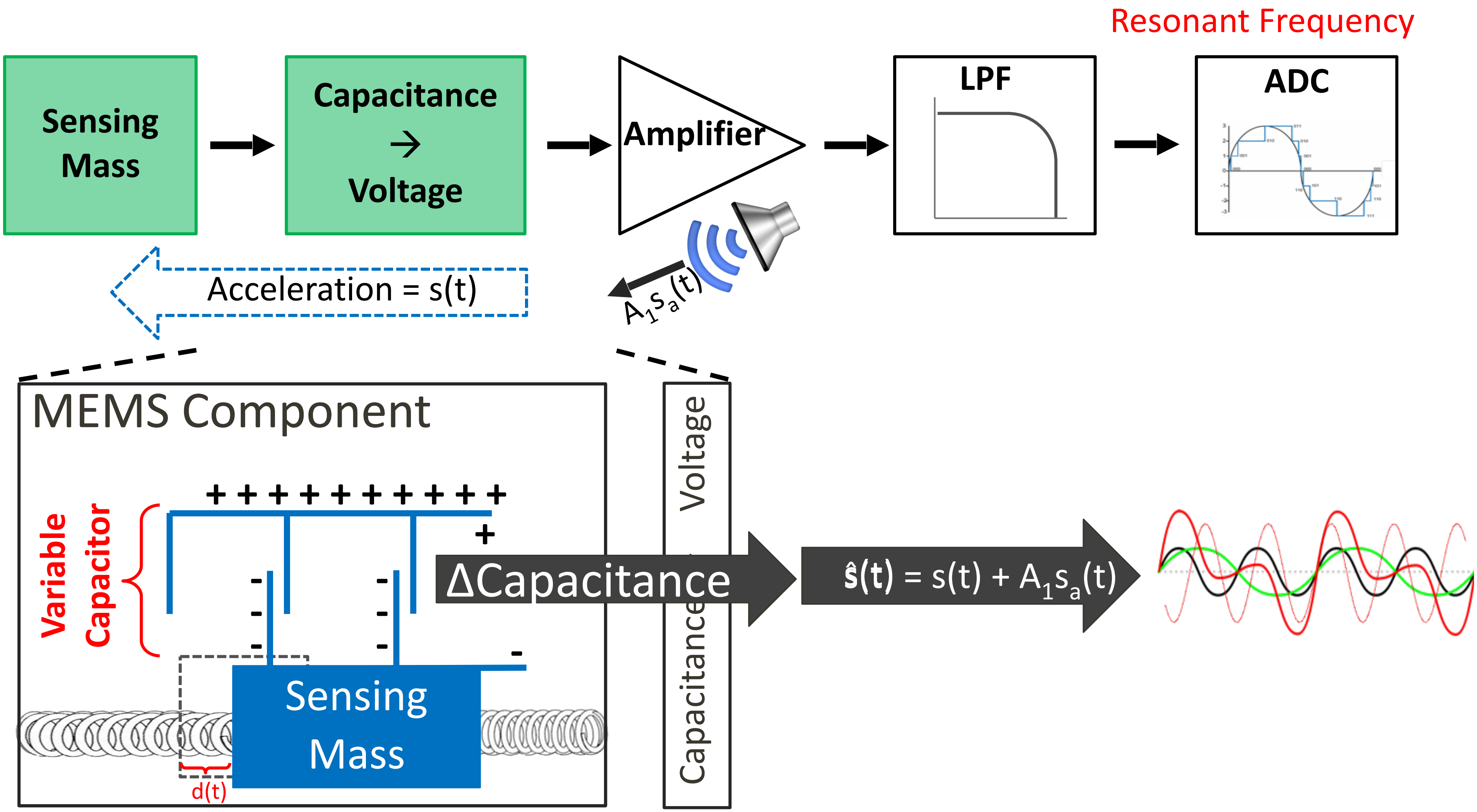
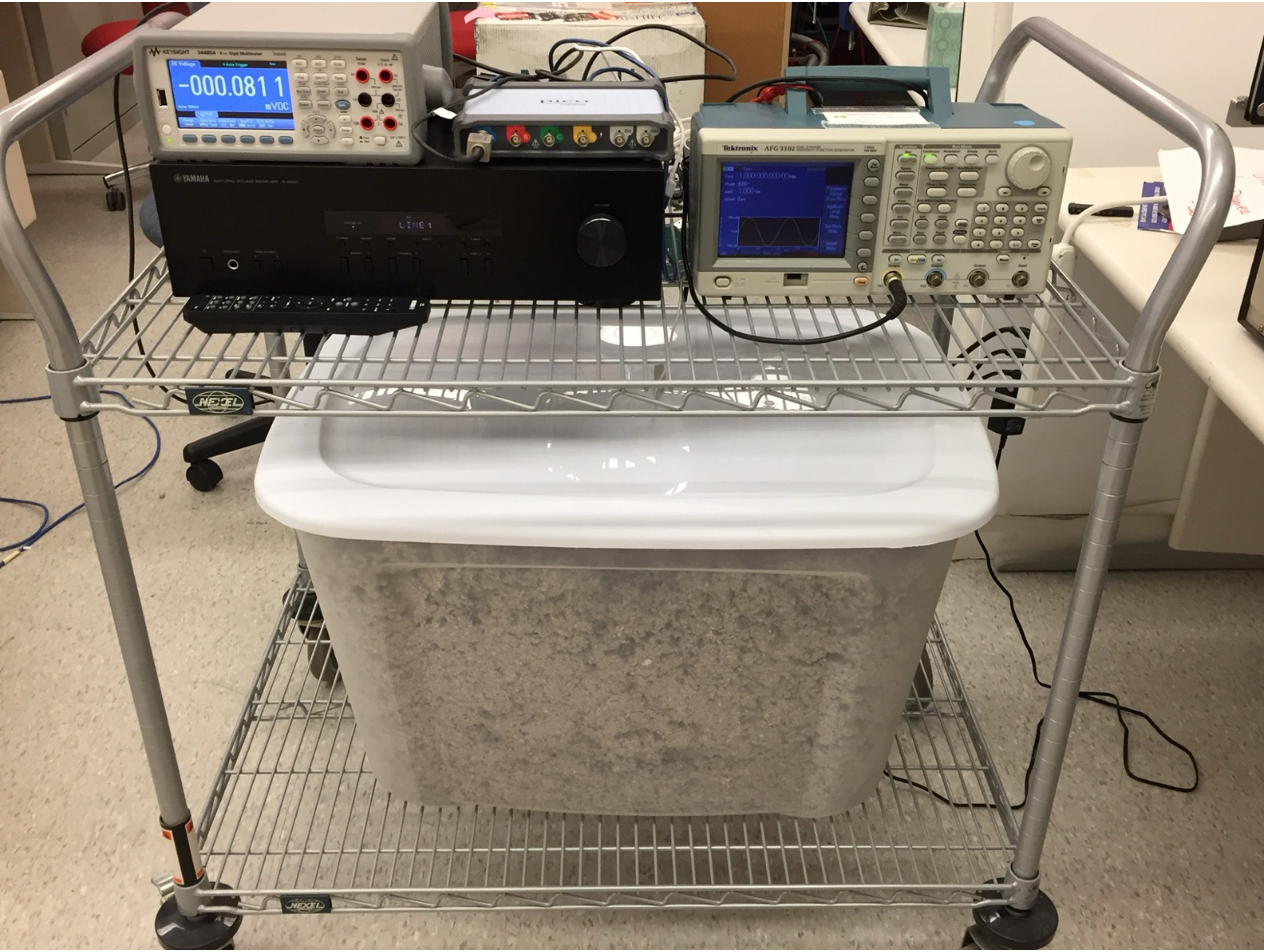


Figure 3: Operation of a three-axis MEMS gyroscope [10] (the X-, Y-, and Z-axes are defined as the pitch, roll, and yaw, respectively.)

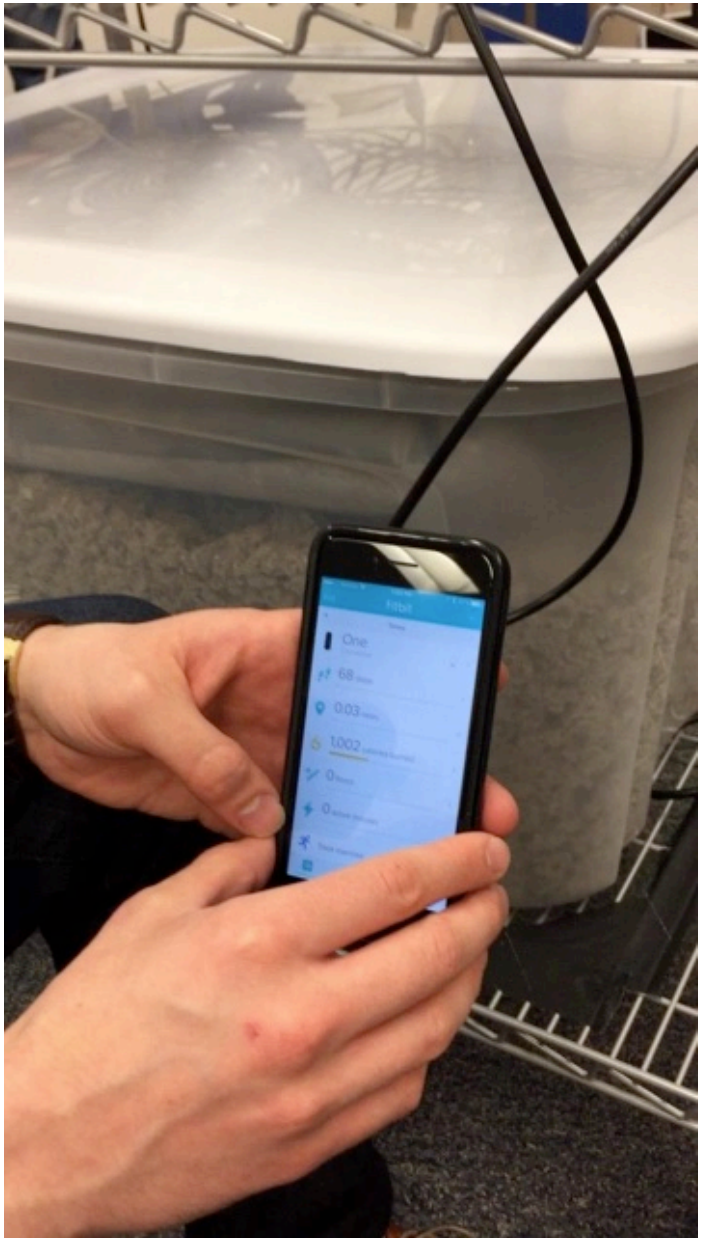
Signal Generation



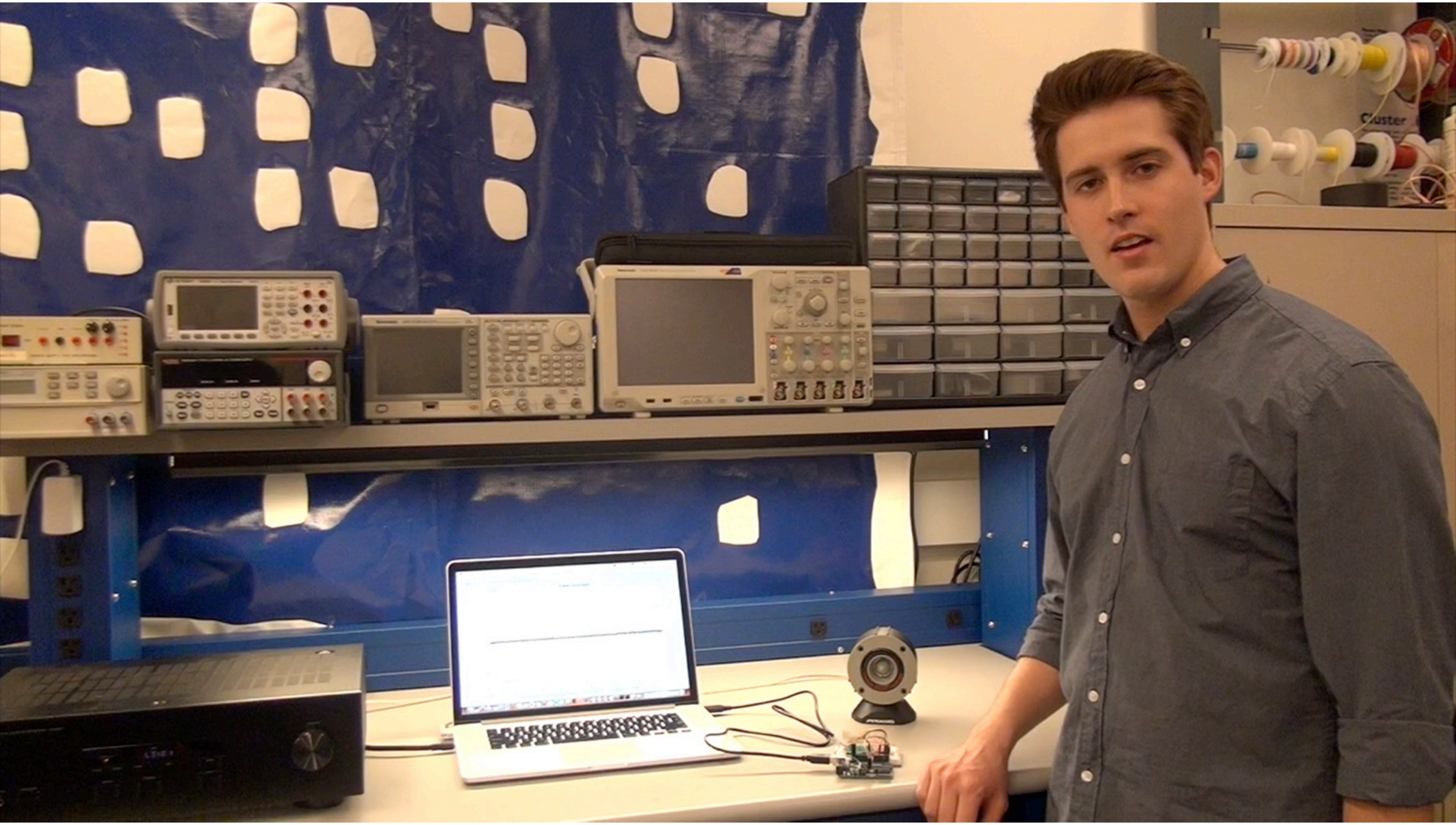



KEYSIGHT
34465A
DC Voltage
-000.081 1
mVDC
YAMAHA
LINE 1
Tektronix AFG 3102
NEXEL
NEXEL

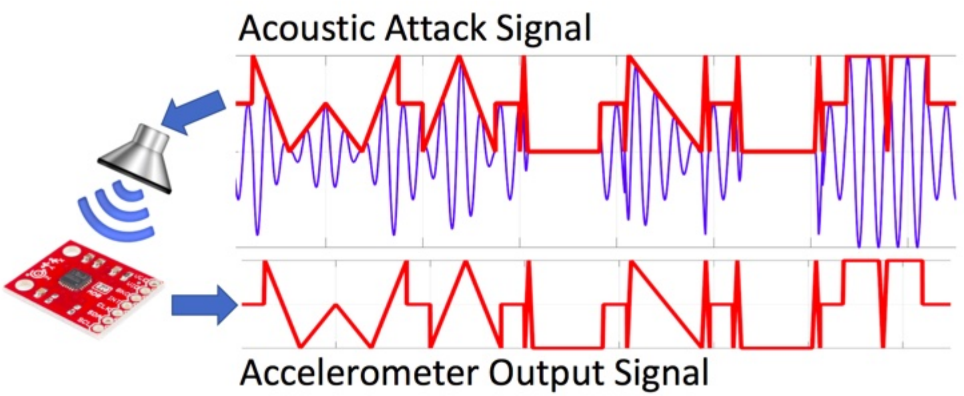
Sound and MEMS Sensor Security



[“WALNUT” by Trippel et al., IEEE Euro S&P 2017]



Unintentional Demodulation



VS.

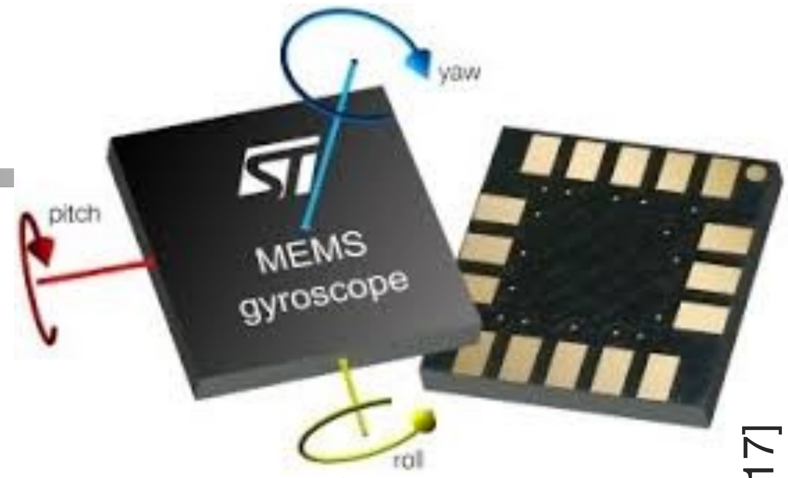
Both: Intentional signal modulation

Intentional
signal demodulation

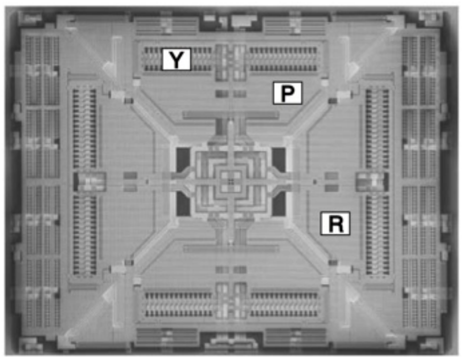
<u>Unintentional</u>
signal demodulation

MEMS Sensors

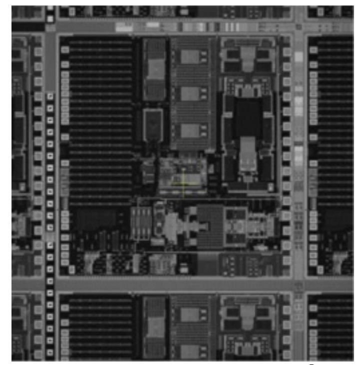
- Micro-Electro-Mechanical Systems
  - **Accelerometers**
  - **Gyroscopes**
  - **Clocks**



IC Package



Mechanical*

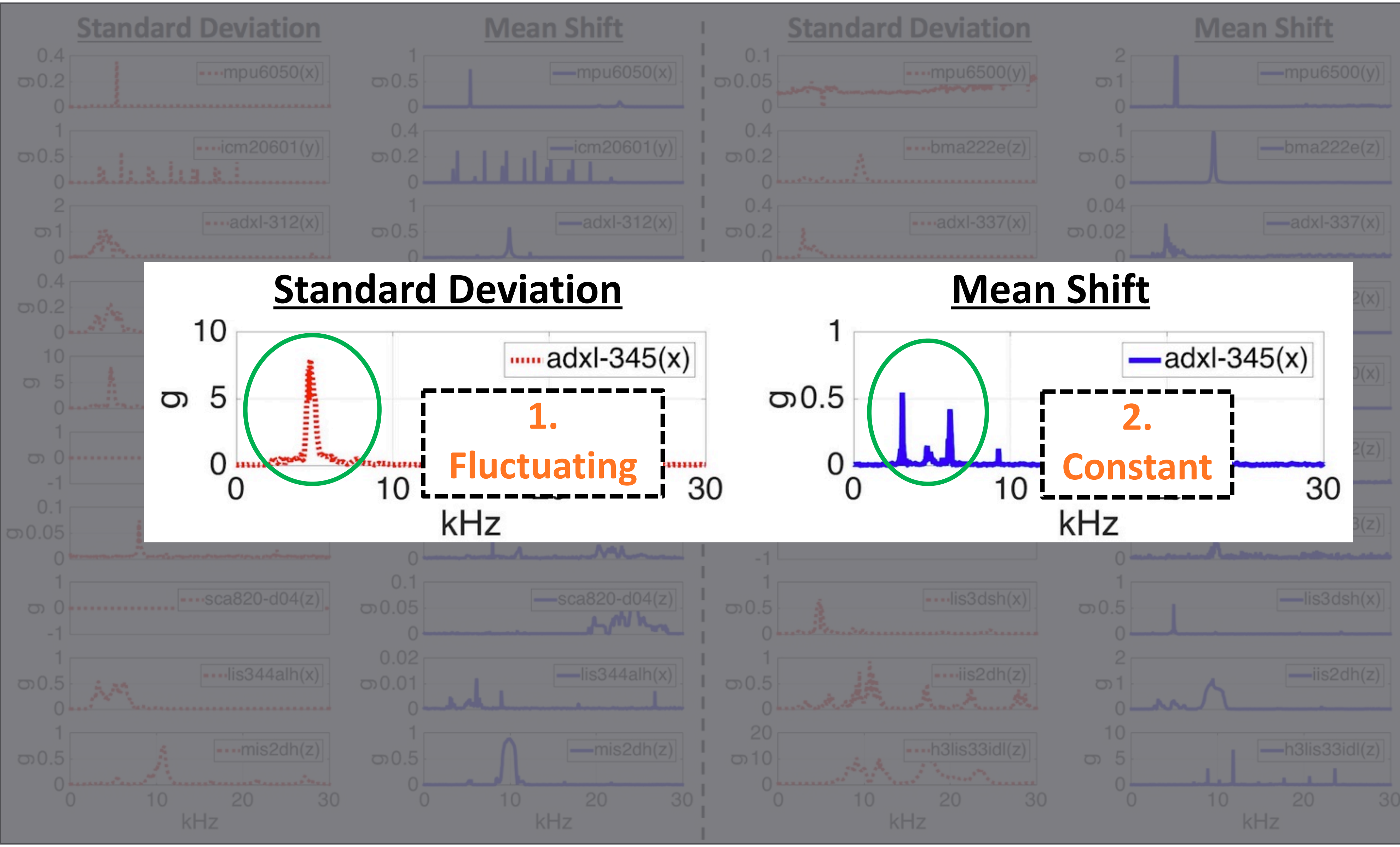


Electrical*

- Advantages
  - Low cost
  - Low power
    some < 1 mA
  - Small integrated circuit

*Photos courtesy of "*Everything about STMicroelectronics' 3-axis digital MEMS gyroscopes – Technical Report*", by STMicroelectronics.

["WALNUT" by Trippel et al., IEEE Euro S&P 2017]

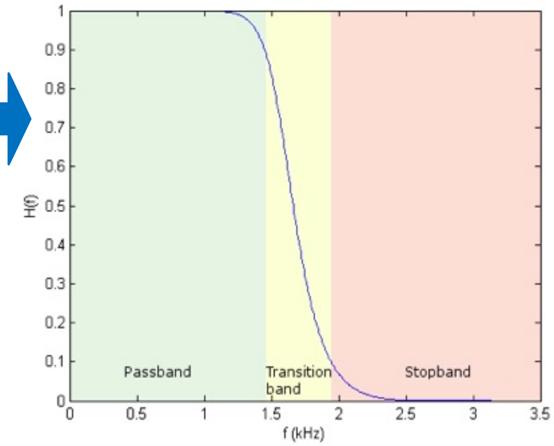


[“WALNUT” by Trippel et al., IEEE Euro S&P 2017]

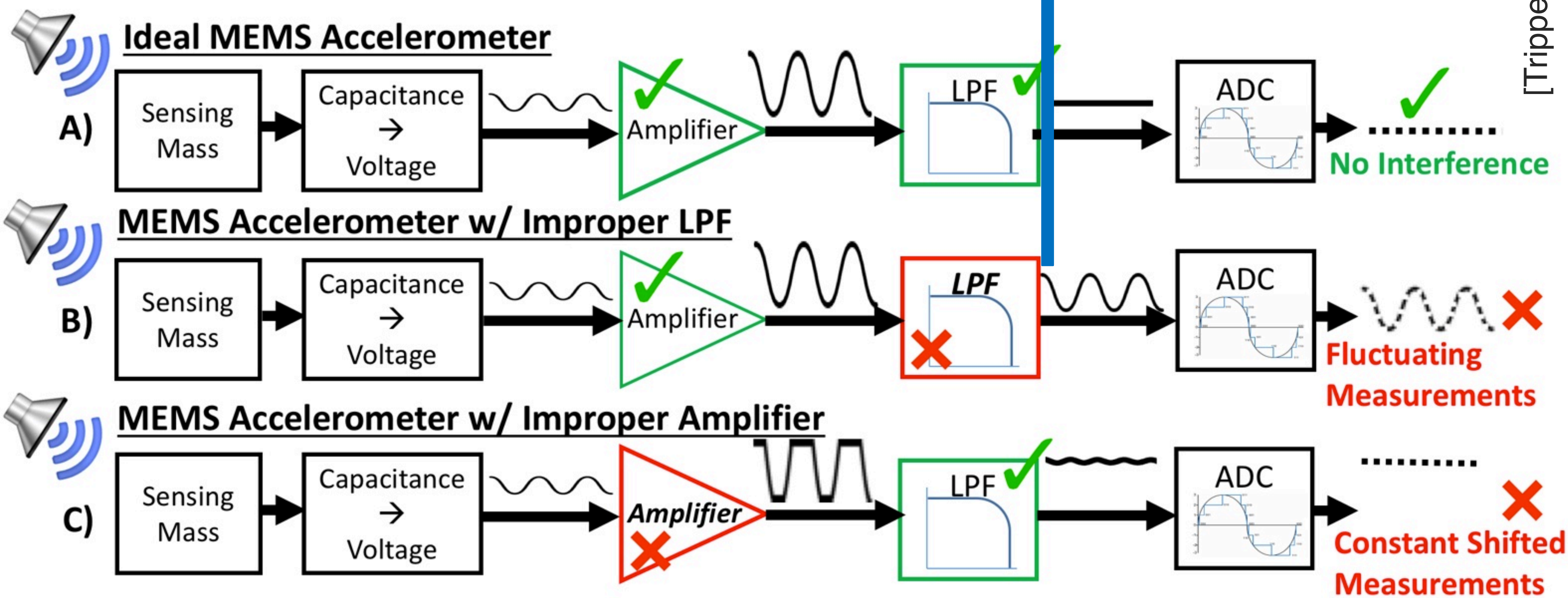
Signal Distortion

Two types of spoofed acceleration

- Fluctuating accelerometer output
- Constant accelerometer output



[Trippel et al., IEEE Euro S&P 2017]



asymmetric clipping

Output Control Modulation

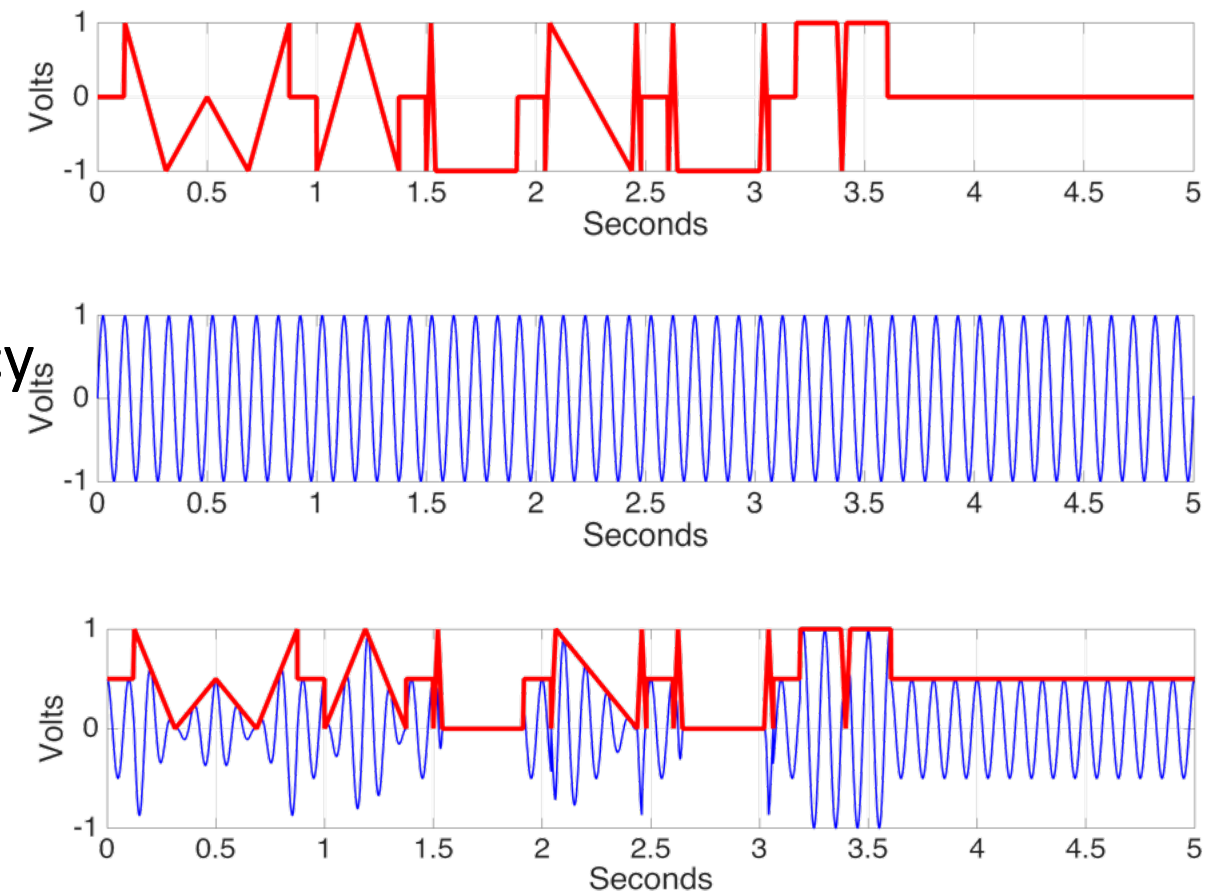
Desired Accelerometer Output Signal

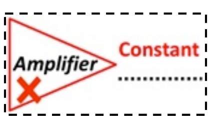
+

MEMS Resonant Frequency (Carrier Signal)

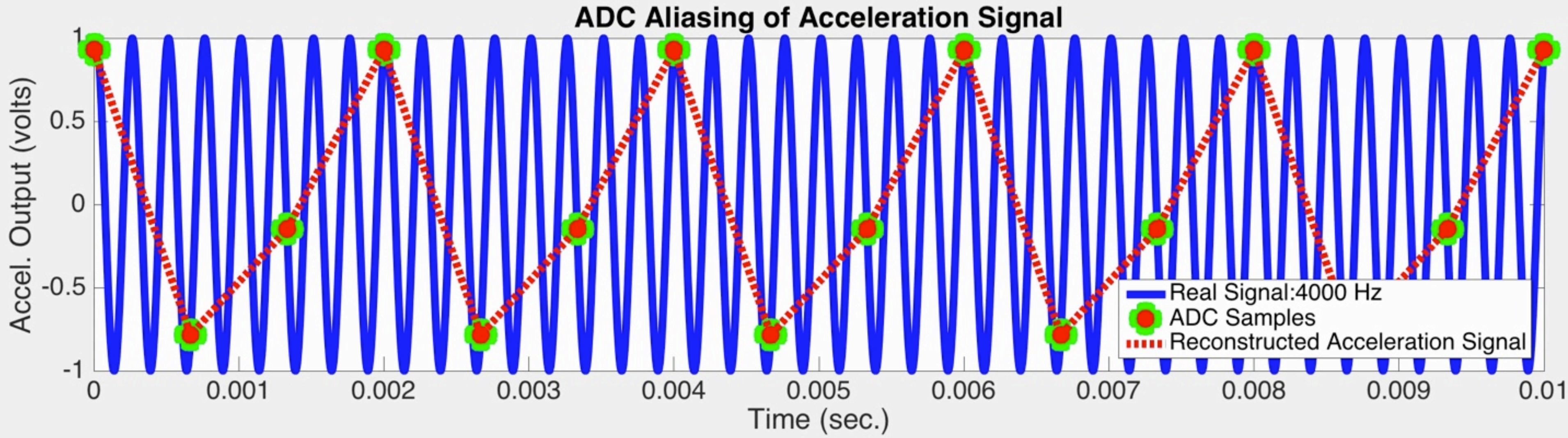
=

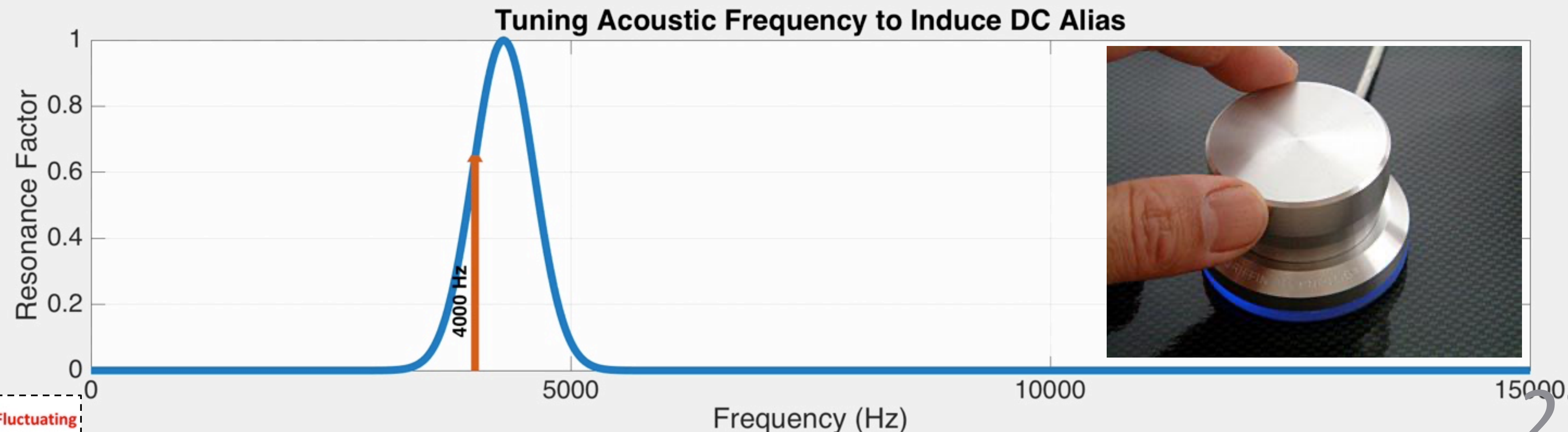
Modulated Acoustic Attack Signal

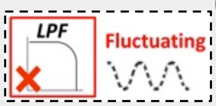


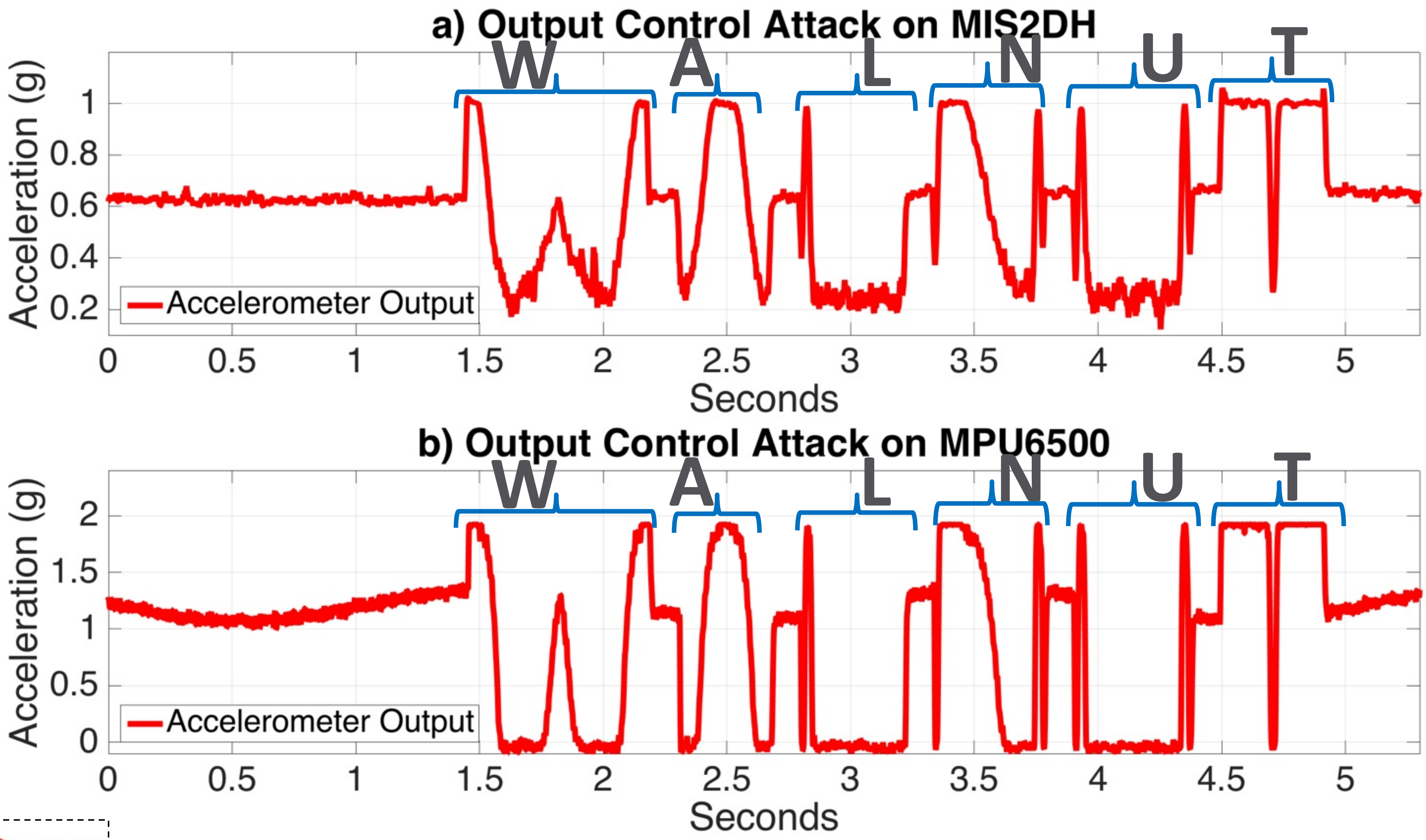


[“WALNUT” by Trippel et al., IEEE Euro S&P 2017]


ADC Aliasing of Acceleration Signal
Accel. Output (volts)
1
0.5
0
-0.5
-1
0
0.001
0.002
0.003
0.004
0.005
0.006
0.007
0.008
0.009
0.01
Time (sec.)
Real Signal:4000 Hz
ADC Samples
Reconstructed Acceleration Signal

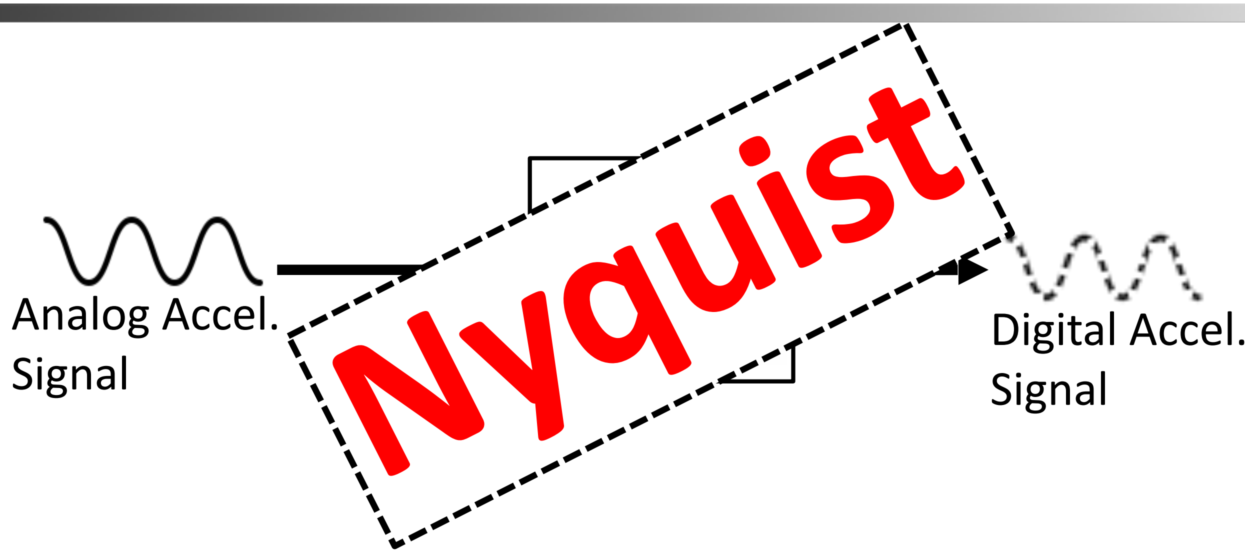

Tuning Acoustic Frequency to Induce DC Alias
Resonance Factor
1
0.8
0.6
0.4
0.2
0
4000 Hz
0
5000
10000
15000
Frequency (Hz)

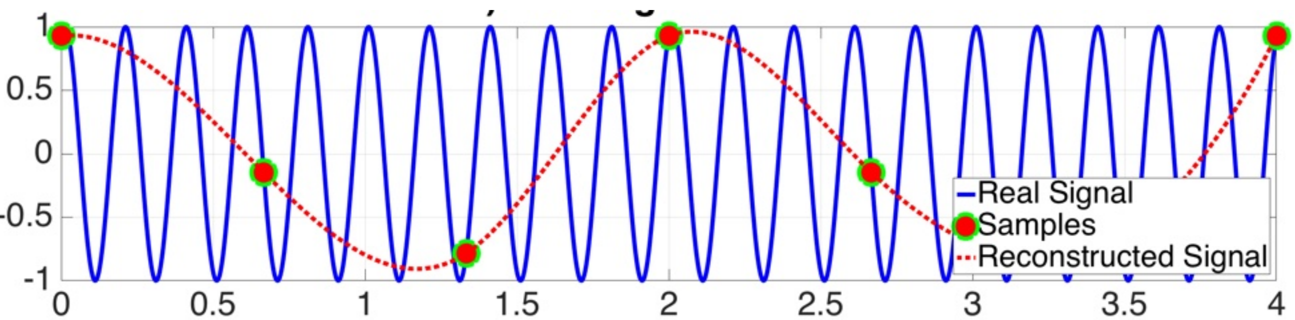

LPF
Fluctuating

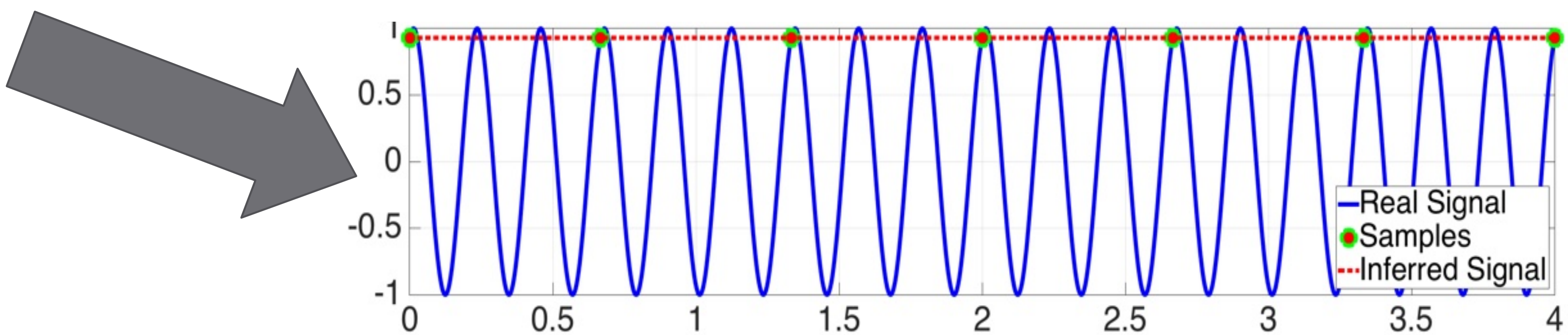


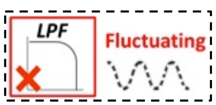
[“WALNUT” by Trippel et al., IEEE Euro S&P 2017]

Output Biasing via Aliasing









["WALNUT" by Trippel et al., IEEE Euro S&P 2017]

Altering System Behavior through its Accelerometer

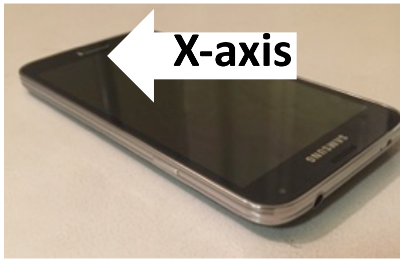
Samsung Galaxy S5

- *Smartphone is ideal target → both speaker and accelerometer COLOCATED!*
- Phone runs application that uses accelerometer to maneuver an RC car
  - Application: iSpy Toys
  - Accelerometer: MPU6500
- Phone simultaneously plays malicious audio file

Orientation of Phone X-axis vs. Car Actions

1g = Backward

0.3g = Stop

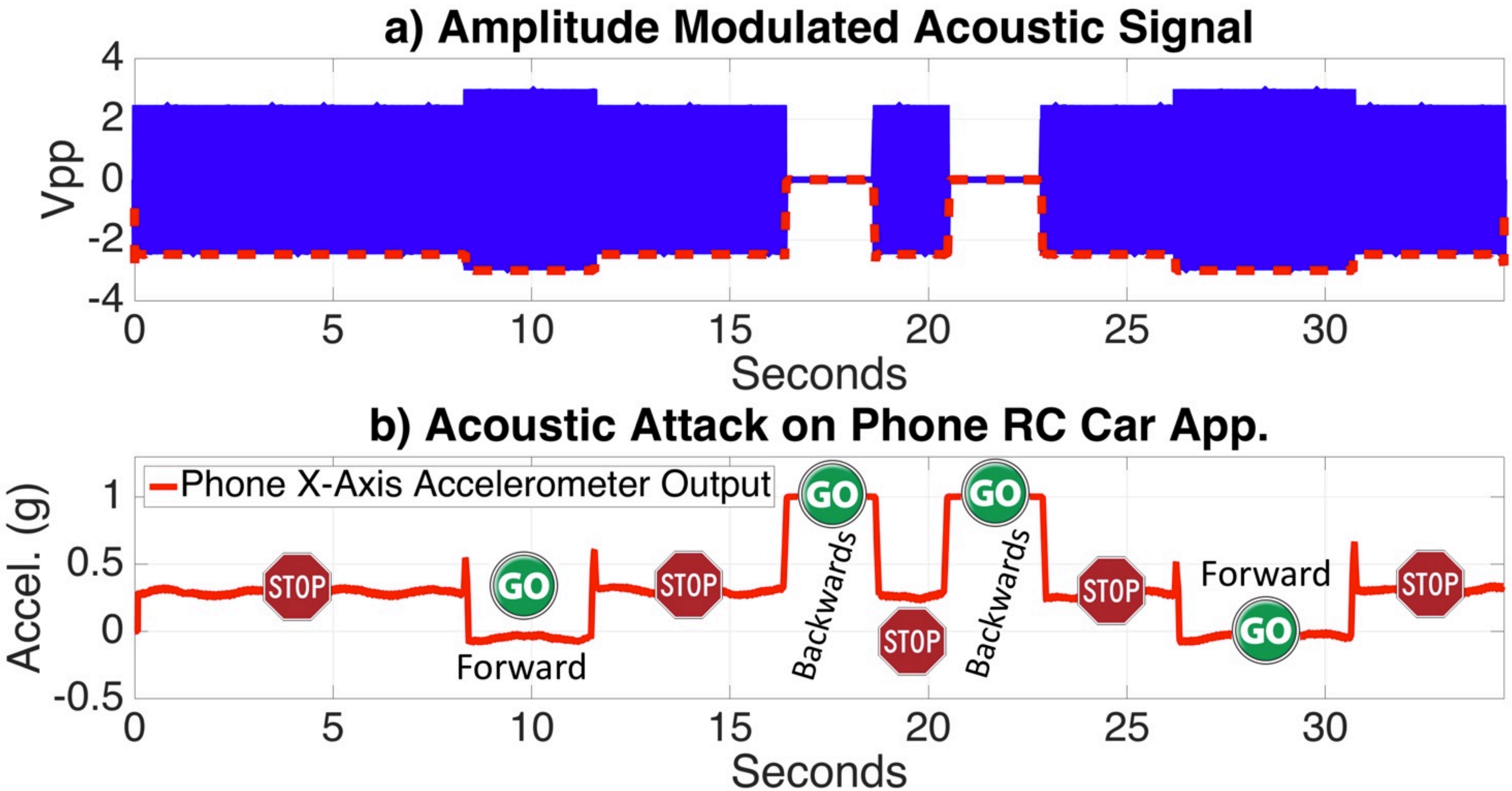


0g = Forward

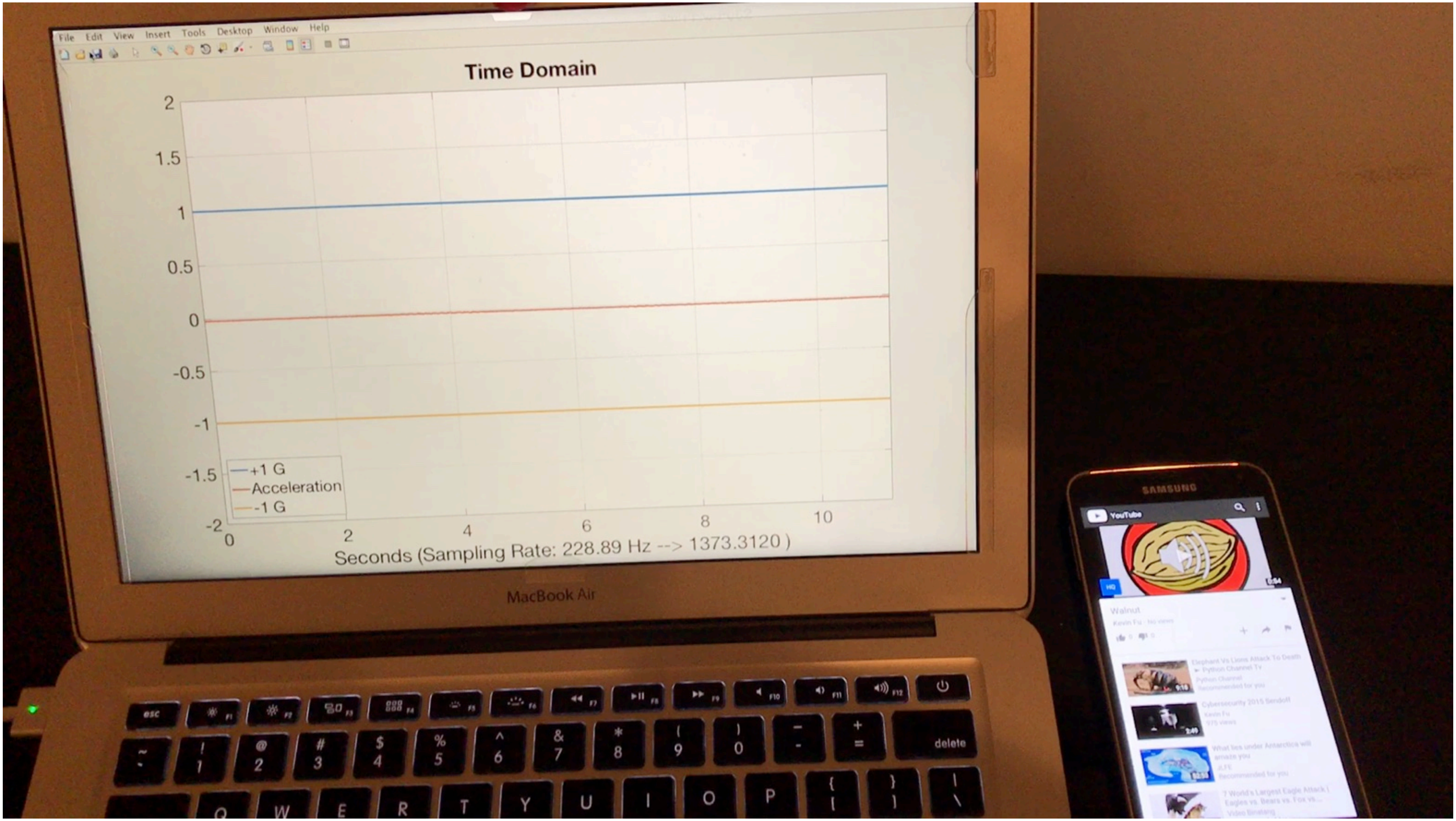
Car Commands

Samsung Galaxy S5

Samsung Galaxy S5



Potential Delivery Mechanisms



ANALOG DEVICES ADVISORY TO ICS ALERT-17-073-01

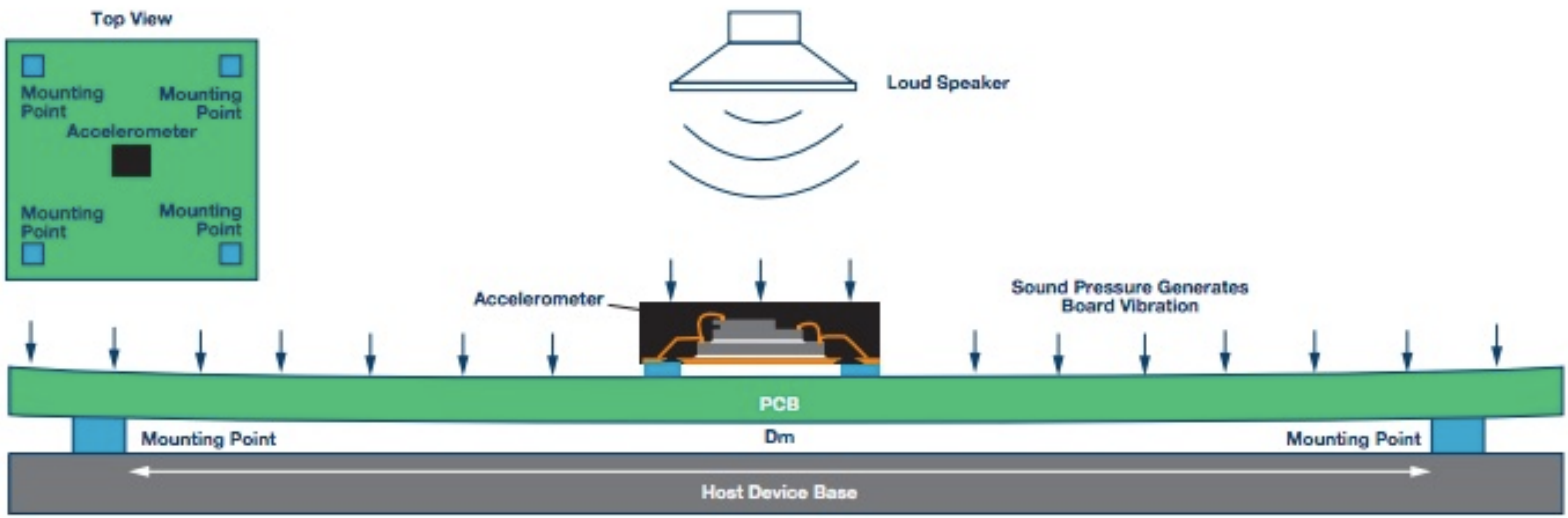


Figure 1. MEMS accelerometer board and mounting with acoustic vibration from off-board speaker.

ANALOG DEVICES ADVISORY TO ICS ALERT-17-073-01

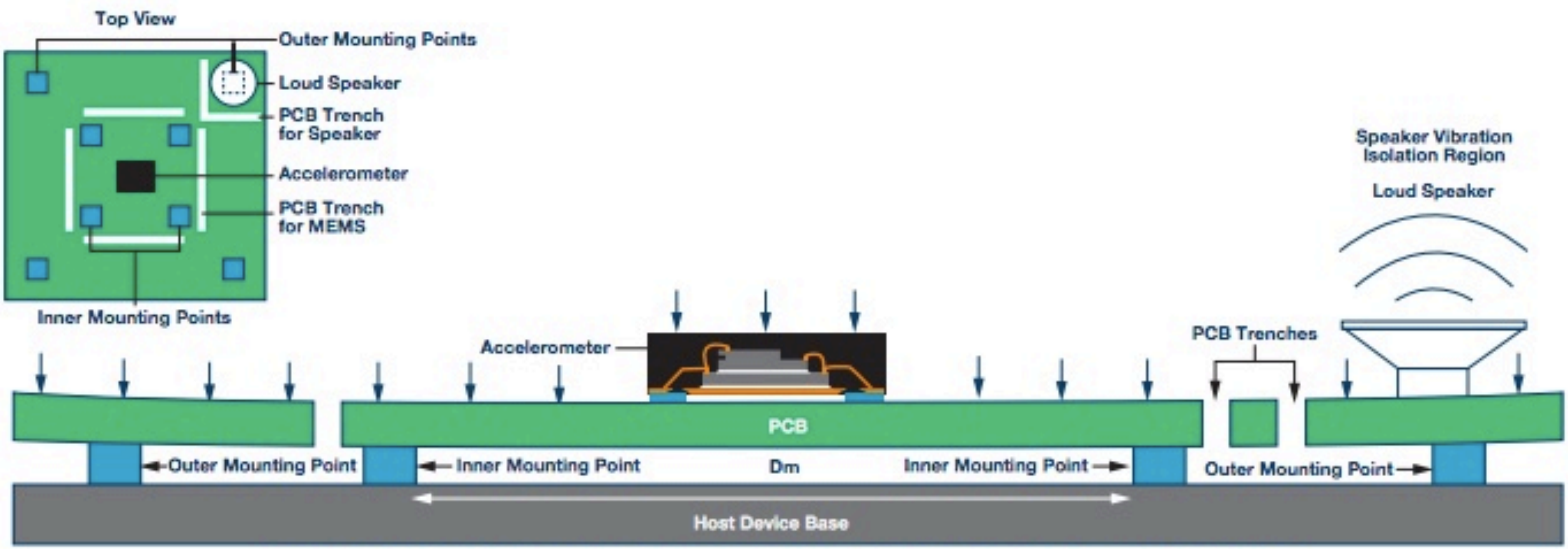


Figure 2. MEMS accelerometer board and mounting with acoustic and mechanical vibration from on-board speaker.

ICS-CERT is also working with several of the cooperative vendors to identify a list of affected devices that contain vulnerable capacitive MEMS accelerometer sensors.

The following MEMS Accelerometer sensors may be affected:

- Bosch BMA222E,
- STMicroelectronics MIS2DH,
- STMicroelectronics IIS2DH,
- STMicroelectronics LIS3DSH,
- STMicroelectronics LIS344ALH,
- STMicroelectronics H3LIS331DL,
- InvenSense MPU6050,
- InvenSense MPU6500,
- InvenSense ICM20601,
- Analog Devices ADXL312,
- Analog Devices ADXL337,
- Analog Devices ADXL345,
- Analog Devices ADXL346,
- Analog Devices ADXL350,
- Analog Devices ADXL362,
- Murata SCA610,
- Murata SCA820,
- Murata SCA1000,
- Murata SCA2100, and
- Murata SCA3100.

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ANALOG DEVICES ADVISORY TO ICS ALERT-17-073-01

The following derivations based on a single periodic sound frequency can be used to relate the board deflection to acceleration level.

The board harmonic deflection can be defined as:

$$deflection = d_{bd} \times \sin(\omega \times t) \qquad (1)$$

where d_{bd} is the amplitude of the board deflection under the sound pressure and ω is the frequency of the sound.

The acceleration produced by the harmonic deflection is:

$$acceleration = d_{bd} \times \omega^2 \times \sin(\omega \times t) \qquad (2)$$

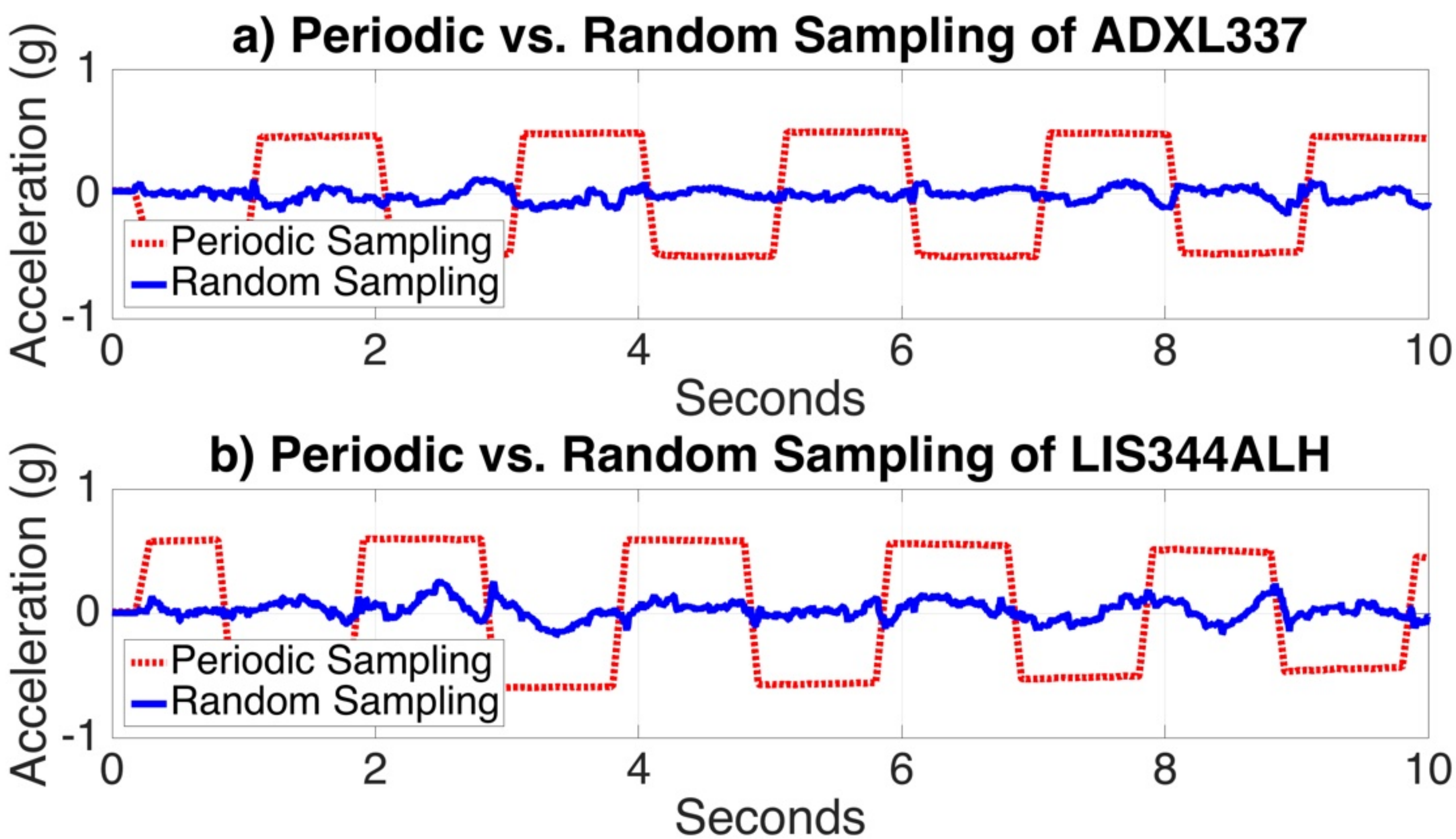
In the case where the sound frequency matches the board resonant frequency, the deflection will be amplified by the qualify factor (Q_{bd}) of the board and Equation 2 will be modified as:

$$acceleration \text{ at } board\ resonance = Q_{bd} \times d_{bd} \times \omega^2 \times \sin(\omega \times t) \qquad (3)$$

By inspecting Equation 3, one can find the following methods to mitigate the board acceleration effect. These methods have been either implemented in Analog Devices' accelerometer products or advised to the customers for system design considerations, whichever is applicable.

Randomized Sampling

- Destroy predictability of sampling regime
- Randomize delay at each sampling interval

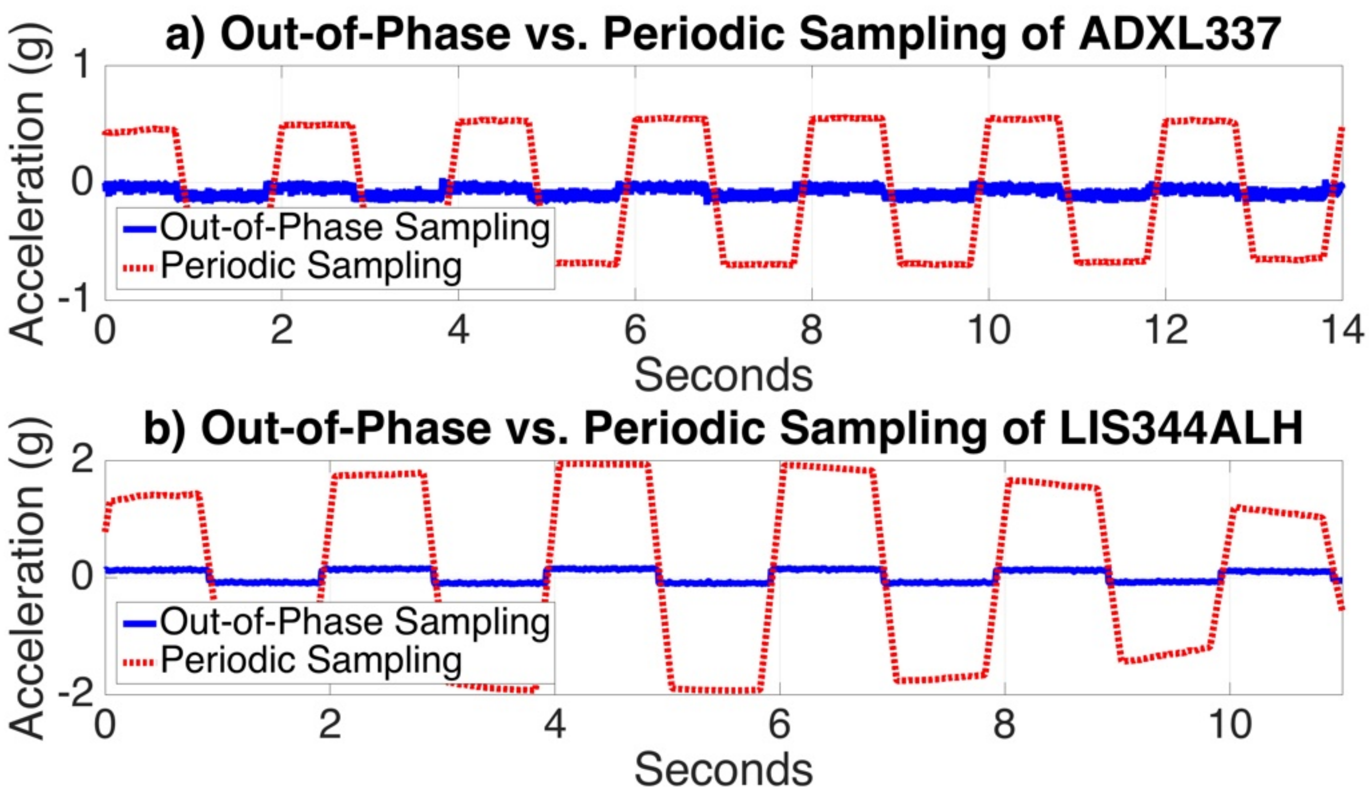


[“WALNUT” by Trippel et al., IEEE Euro S&P 2017]

180° Out-of-Phase Sampling

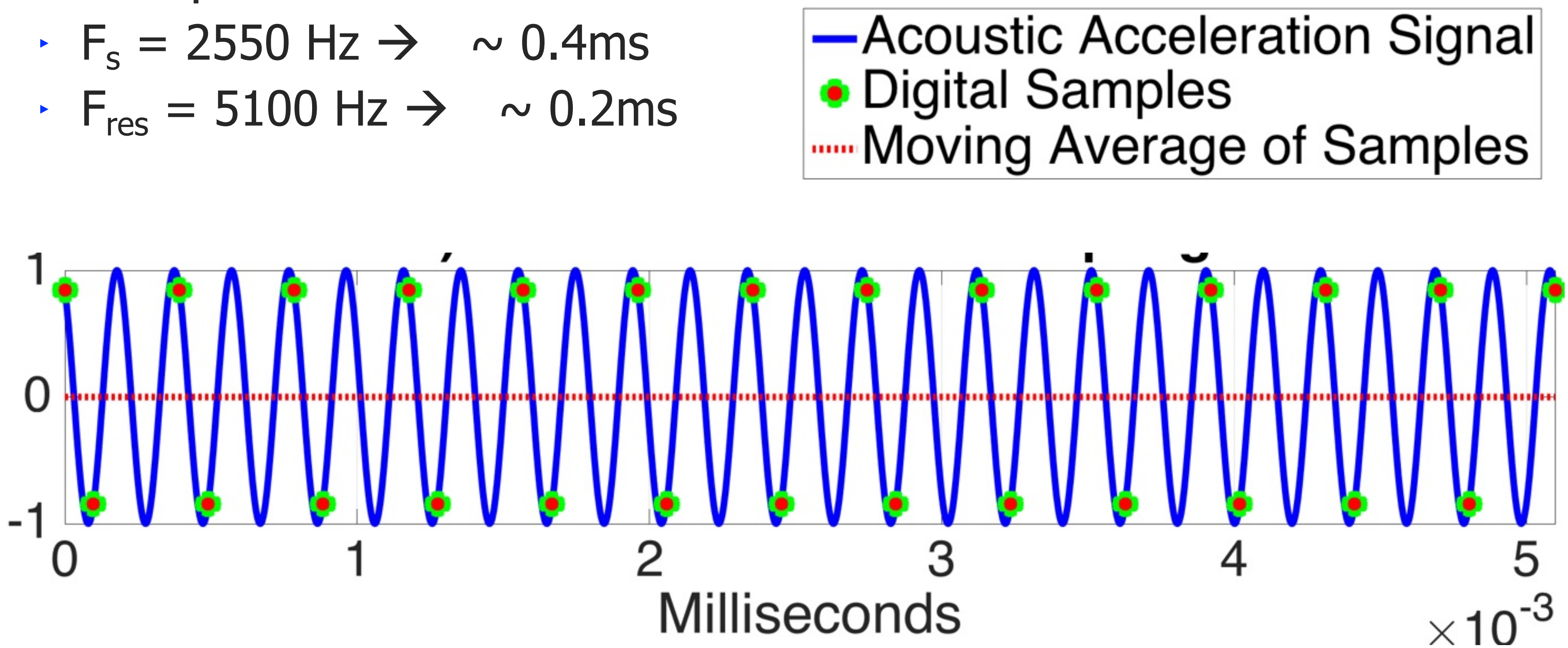
Un-aliased acoustic acceleration is sinusoidal

- Symmetrically distributed around zero
- Averaging attenuates acoustic acceleration



180° Out-of-Phase Sampling

- Un-aliased acoustic acceleration is sinusoidal
  - Symmetrically distributed around zero
  - Averaging two consecutive acceleration samples attenuates acoustic acceleration
- Example:
  - F_s = 2550 Hz → ~ 0.4ms
  - F_{res} = 5100 Hz → ~ 0.2ms



Consequences of Intentional EMI on Sensors

Internet of Everything
What could possibly go wrong?

"Runs on a Chip"

How LED Lights Can Cause Problems With Your Garage Door Opener

NOVEMBER 4, 2013 BY TOMMY MELLO

If you've been experiencing problems with your garage door opener remote unit – sometimes it works, sometimes it doesn't – and can't track the problem down, you might look to the type of lights you're using in and around your garage for the culprit.

http://www.phoenixazgaragedoorrepair.com/garage-door-repair/1786/how-led-lights-can-cause-problems-with-your-garage-door-opener/garage-door-blog/

“Runs on a Chip”

Can LED lights interfere with your garage door opener?

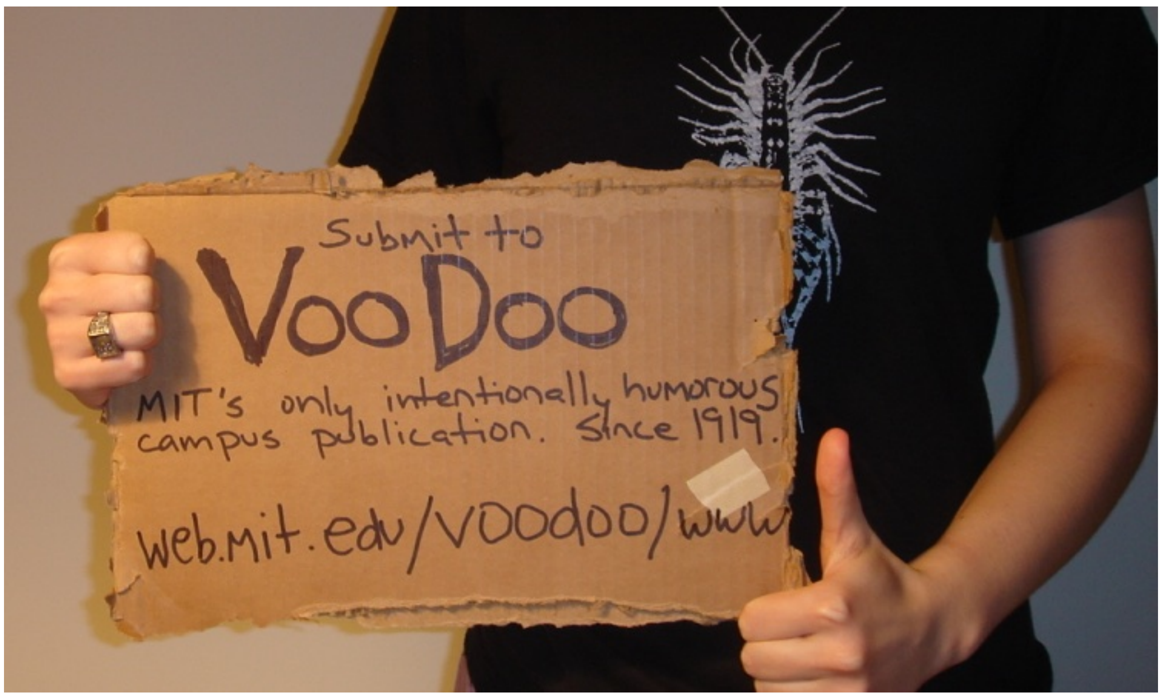
By Deni Hawkins | Published: Apr 17, 2014 at 5:39 PM MDT | Last Updated: Apr 17, 2014 at 7:04 PM MDT

Recommend 0 G+1 0 Tweet 0 Print Email

NAMPA, Idaho (KBOI) - A local man makes strides to conserve energy, but believes it may have caused problems for him and his neighbors in the process.

http://www.phoenixazgaragedoorrepair.com/garage-door-repair/1786/how-led-lights-can-cause-problems-with-your-garage-door-opener/garage-door-blog/

MIT Humor Magazine Predicts IoT Light Bulbs Fall 1995



Voo Doo Magazine, Late Fall '95

IP Address Shortage Spurs Black Market

by Alyssa P. Hacker

Although M.I.T. owns one of the few Class A Internet Protocol (IP) address spaces in the world, the now famous "Net 18", there is a campus shortage of available addresses. Not a real shortage, mind you, but an artificial shortage created by Information Systems controlling and rationing the available subnets. I/S claims that proactive measures are prudent and necessary, but critics point out that out of the sixteen million possible addresses of the form 18.*.*.*, there are only about thirteen thousand hosts on MITnet.

Jeffrey Schiller, M.I.T.'s Network Manager, seems rational enough. "We must plan for the future," he explains. "The number of hosts at M.I.T. has been rising exponentially for years, and will for years to come. We are just starting to see some of the technologies that will burden our IP address space in the future. If we didn't charge $2000 a month for a Class C subnet (with space for 255 hosts of the form 18.n.n.*), people would be just throwing away useful address space."

IP Addressable Light Fixtures

Schiller's favorite examples of future technology that will be IP-address hungry are Networked Light Fixtures. "Imagine an office filled with light fixtures on the network: their status could be queried from any point on the network, energy usage could be centrally or remotely tracked, and authorized managers could turn them on and off. You could literally finger and telnet to your lights! Imagine this with all the thousands of light fixtures at M.I.T.; this kind of technology requires that we plan for a great future need."

But there are other, more realistic needs, he adds. The next wave of computing might very well be desktop symmetric multiprocessing machines, computers with more than one computer inside. Machines are available now with anywhere between 2 to 65,000 processors. In some configurations, administrators may wish to assign an IP address to each processor. "A Connection Machine could occupy an entire Class B subnet [using 65,535 IP-addresses of the form 18.n.*.*]!"

Current developments at M.I.T. are also putting a drain of the address space. Under the Residential Networking Initiative, or "ResNet", dormitories, fraternities, and other independent living groups are given access to MITnet. With this access goes a huge chunk of MIT's IP address space. "Just to make the routing simpler, each fraternity is assigned a Class B network. That's nuts!" says Ward Lesser, Network Administrator for the Department of Electrical Engineering. "That's as much as the Media Lab! No frat is going to have thousands of machines."

Departments, Users Suffering

Many departments are suffering due to this shortage, especially those that rely heavily on computers in their curriculum, namely the Media Laboratory, the Artificial Intelligence Laboratory, the Laboratory for Computer Science, and the Department of Electrical Engineering. "We've only been assigned a Class B network," sighs Matt Knudsen, Network Manager at L.C.S., "While that seems like a lot, it only allows us around 200 subnets. Do you know how many computers there are in this department, and in this building? We don't want 200 machines on every subnet."

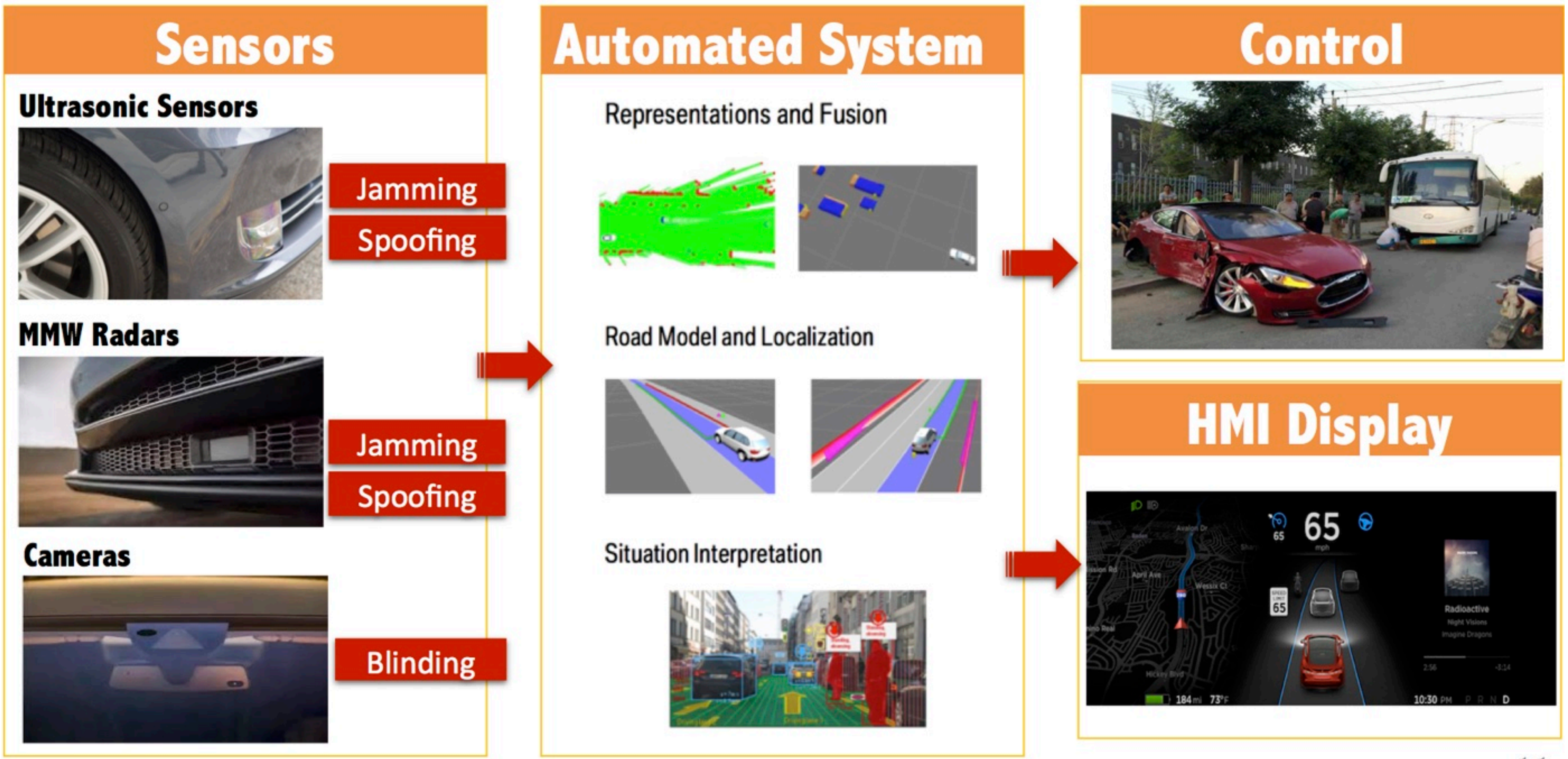
Due to this shortage, some departments have had to implement IP saving measures of their own. "Jeff Schiller is right, IP addressable equipment is on its way, but it's happening now, not five years from now," explains Lesser. "FDDI hubs now require their own IP address for management, so I have to decommission X-terminals in the labs to deploy one because of the Schiller iron grip. The ultimate victims of this are students. I want to deploy more X-terminals in the teaching labs and electronic classrooms, not less, but whenever I mention it to Network Services, I get Jeff talking out of his hairy ass about FTP-lightbulbs."

George Maxwell, researcher with the Research Laboratory for Electronics, has another view. "IP addressable appliances are coming, but who is going to develop them? M.I.T. can't do it unless Network Services gives us the address space to play with!" He concedes that running out of available address space could be a grave problem, "but it's happening in the

- 22 -

http://web.mit.edu/voodoo/www/archive/pdfs/1995-Fall.pdf

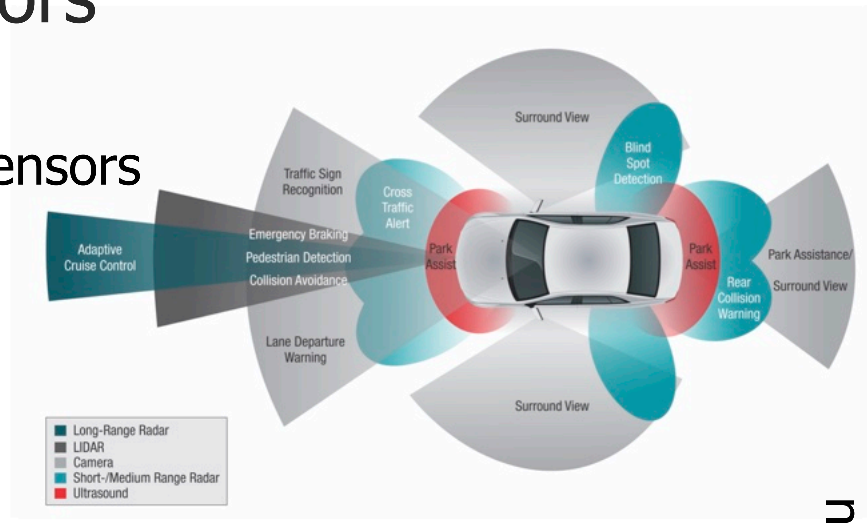
What About Automotive Sensors?



Source: TI & ZHU

Protecting Auto Sensor Security

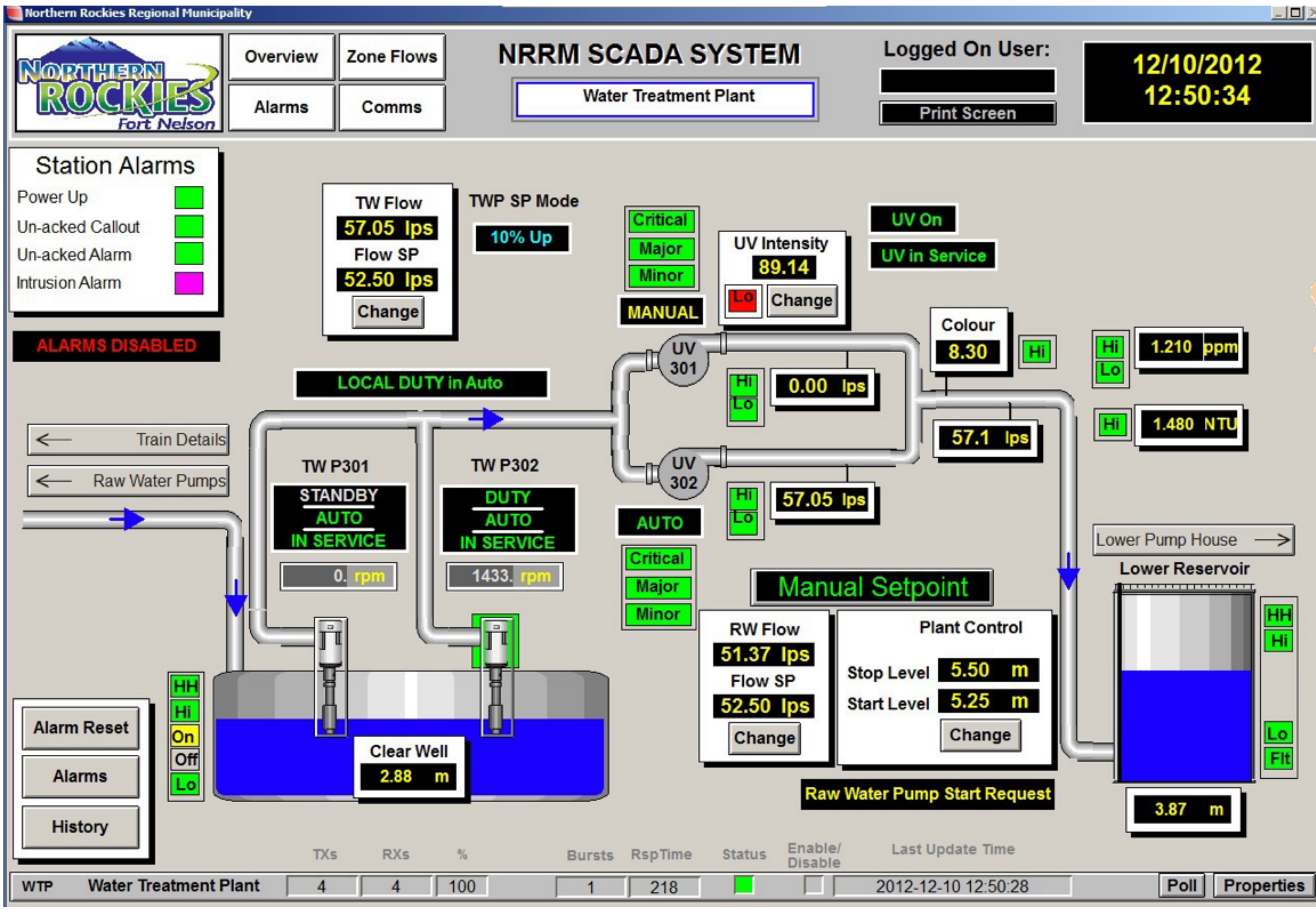
- Vehicles need trustworthy sensors
  - Level 0: airbags, traction control
  - Levels 1-3: inertial measurement, prox sensors
  - Levels 4-5: closed-loop feedback control



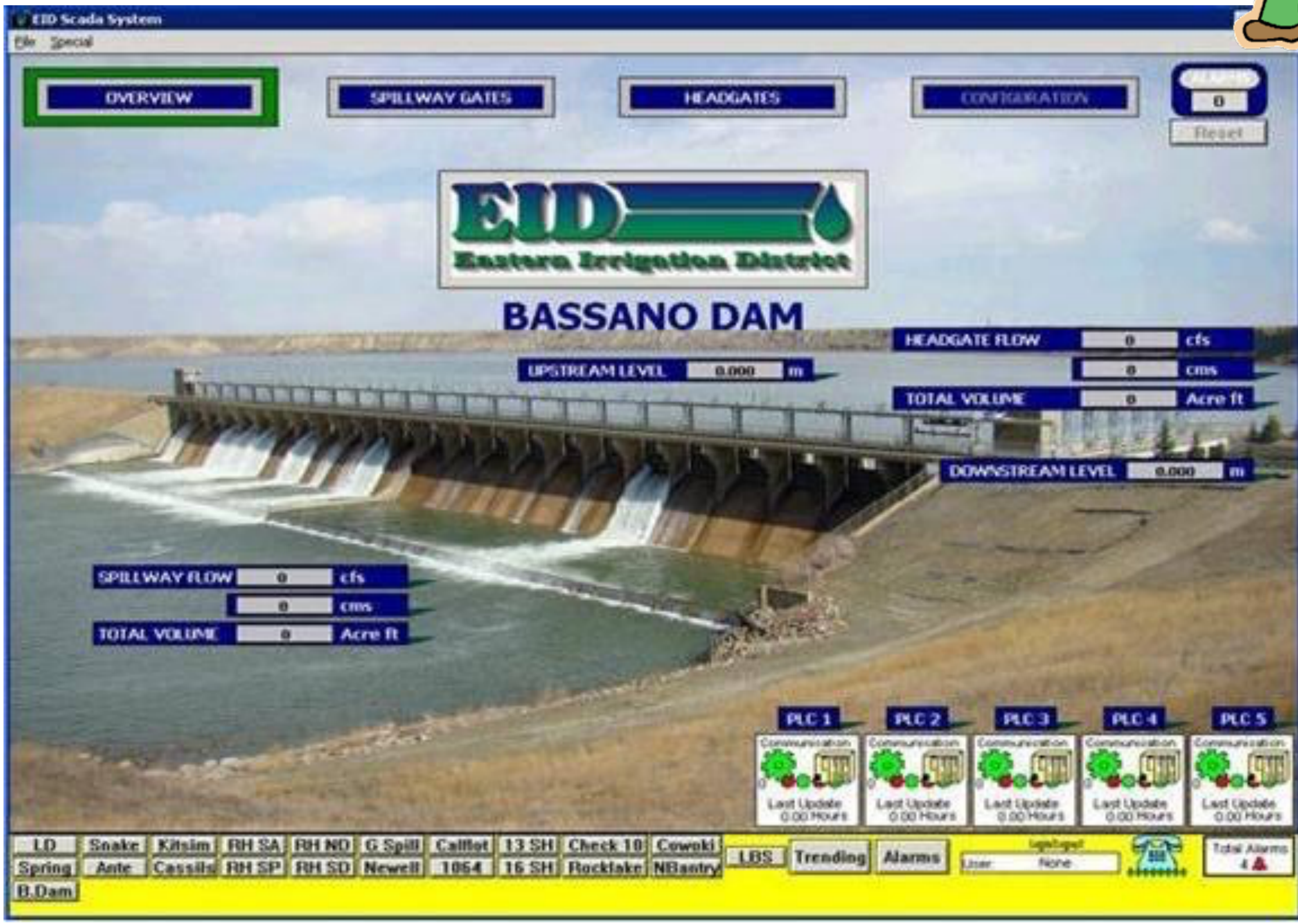
- Meaningful threat models
  - Should be based on science, not hope
  - Cannot be valid unless refutable
  - Requires identification of non-trivial limits & failure
- Red herrings
  - Key size, software only, signals only, HW only

Source: TI & Wenyuan Xu

Sensors: Water Treatment Plant

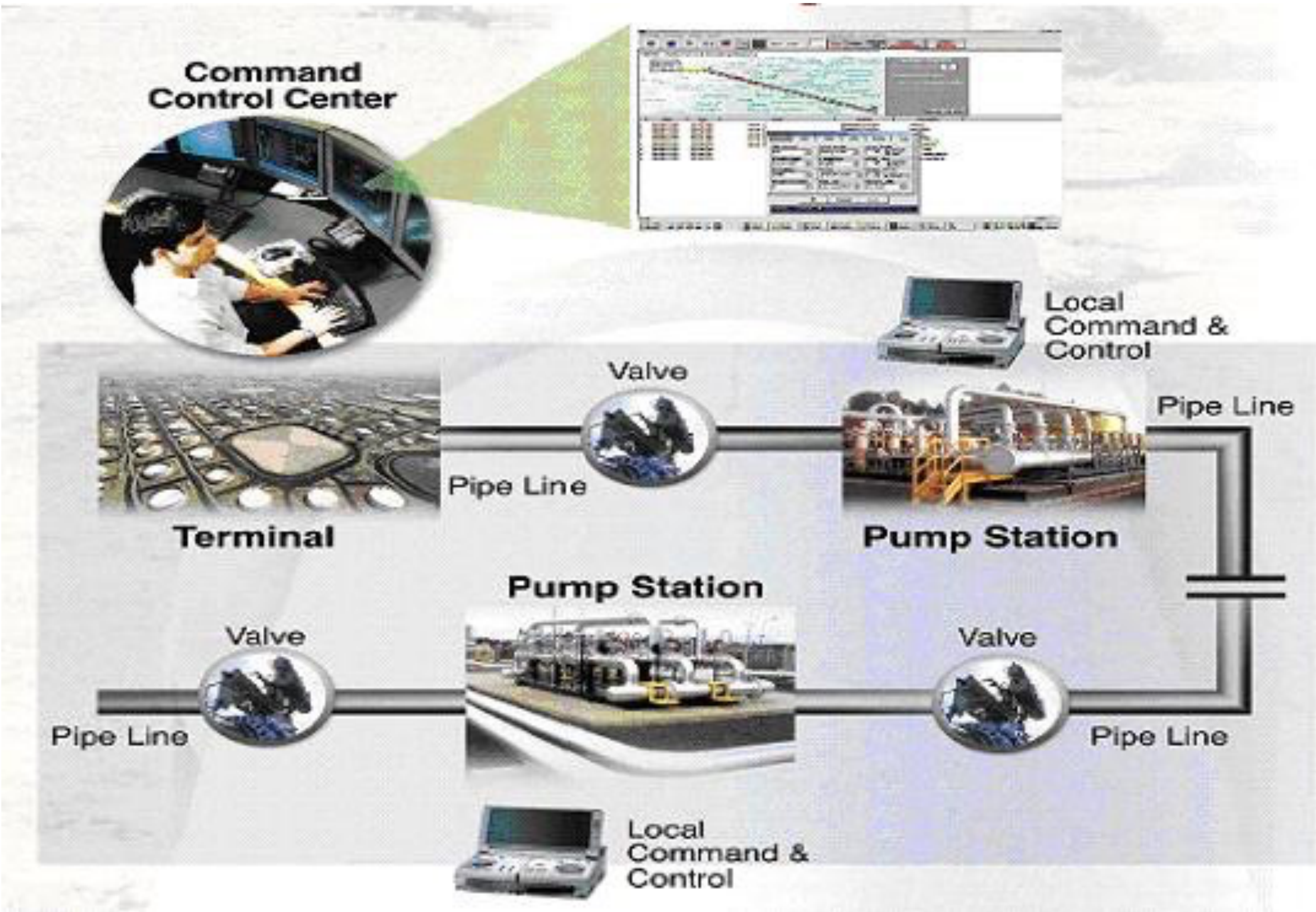


Sensors: Dams



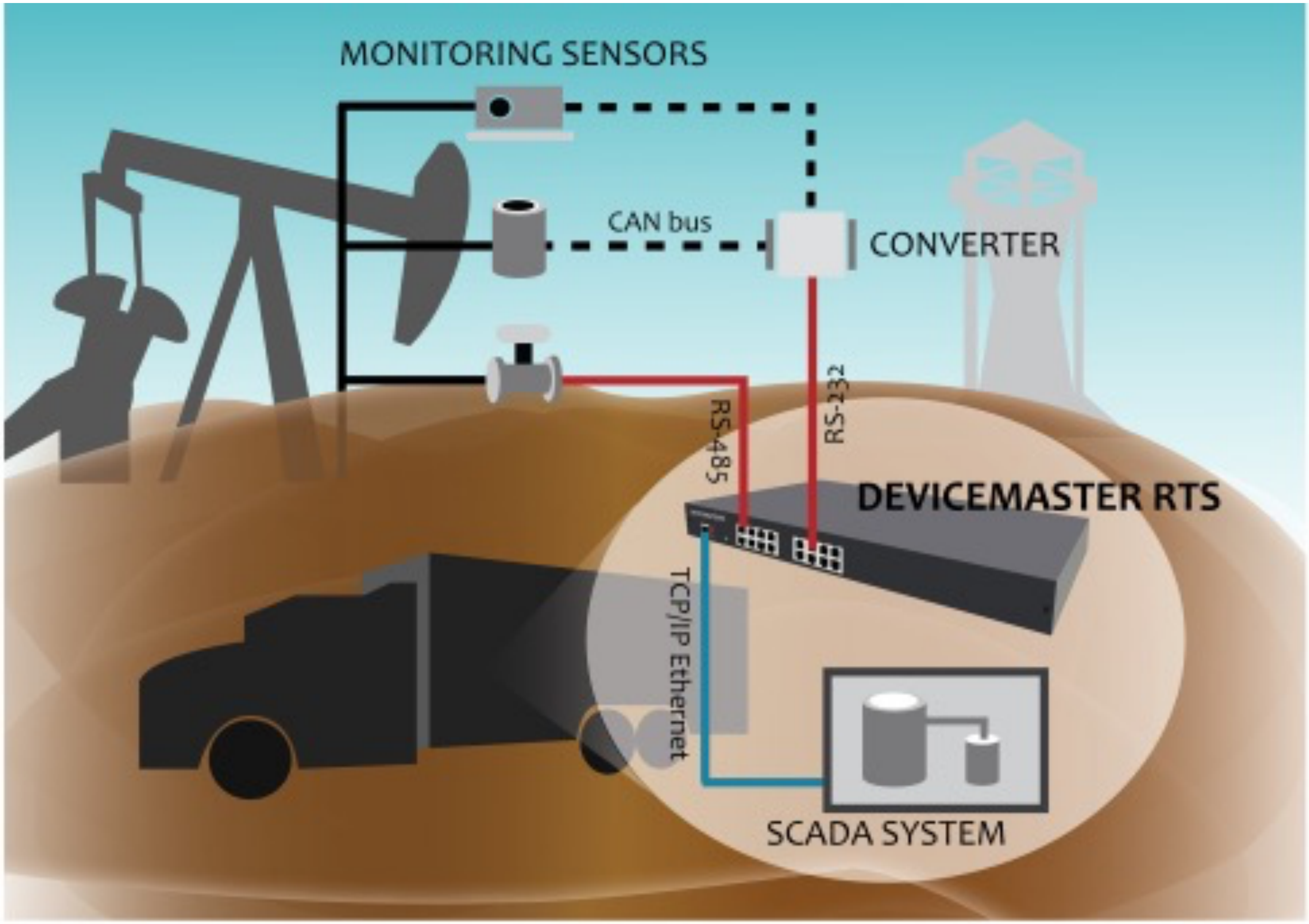
http://www.mpe.ca/project_experience/projects.php?view=28

Sensors: Oil Pipelines



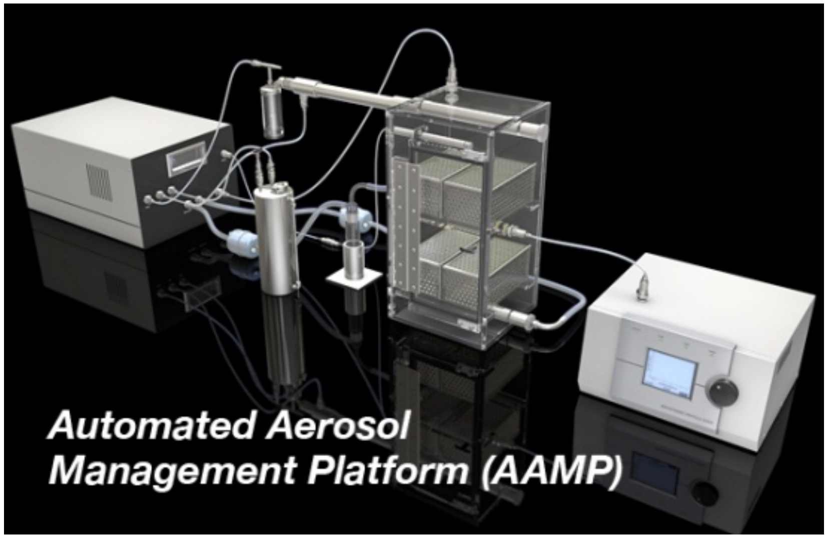
http://www.modcon-systems.com/applications/pipelines/pipeline-scada-security/

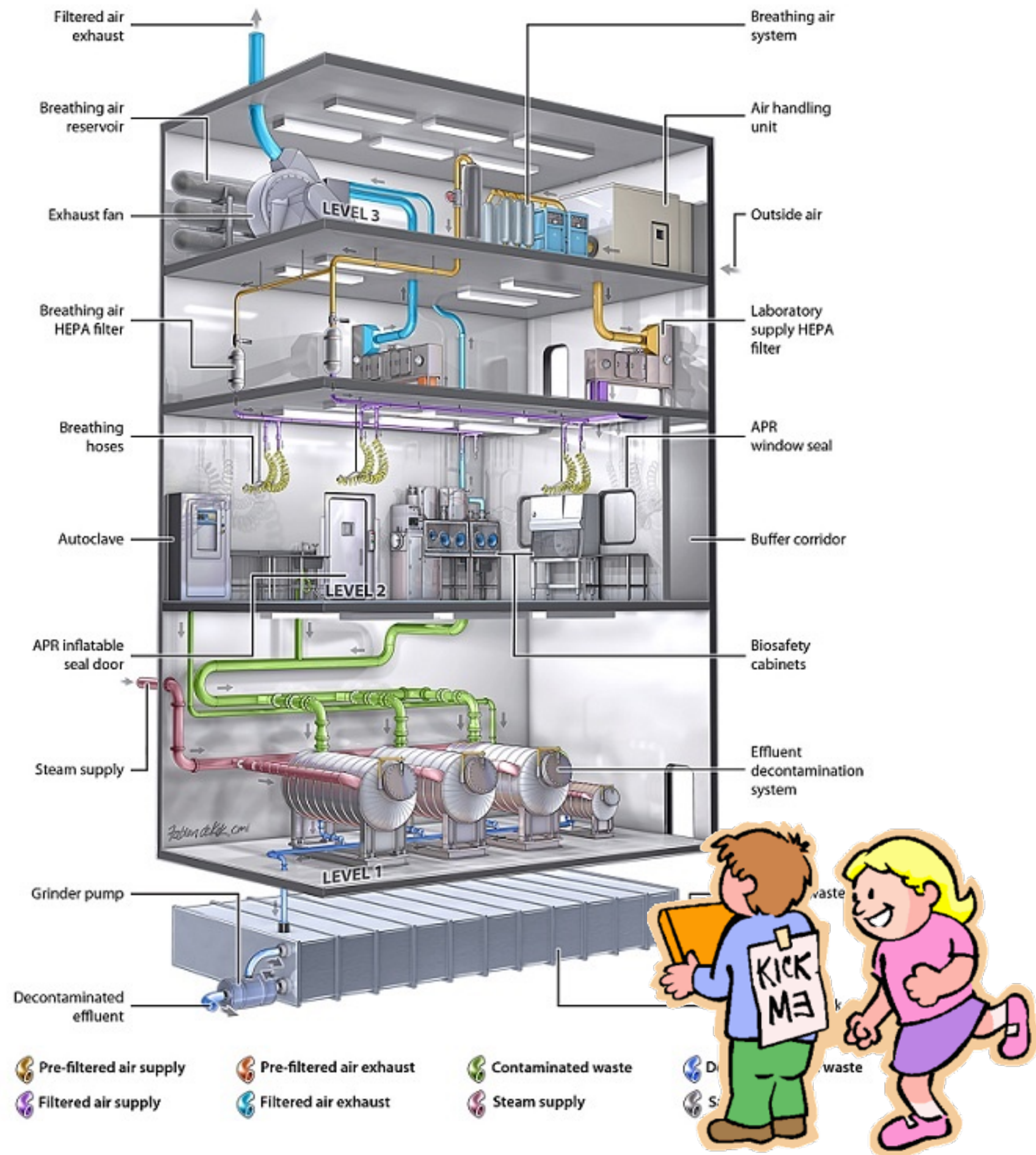
Sensors: Hydraulic Fracturing



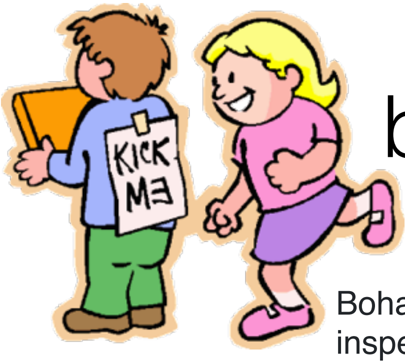
http://blog.comtrol.com/2013/04/03/hydraulic-fracturing-process-monitoring/

Sensors: BSL-4 Negative Pressure





IAEA sensors for treaty



"Nuclear inspectors must learn to trust their colleagues, but during their training they must learn not to trust others…you never know who might be siphoning off nuclear material to build a bomb or sell on the black market…."

Bohannon, J. (2006). Staying one step ahead: An IAEA inspector fits the picture. IAEA Bulletin, 48(1), 31-32.

Baconian Corollary:

IoT Makes Everything Better?

[Photos: uncyclopedia.wikia.com/wiki/Bacon & bacondujour.blogspot.com http://www.digitaltrends.com/home/heck-internet-things-dont-yet/]

No Worries As Long As No Antenna...

GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies

Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky[1], Yuval Elovici[1]

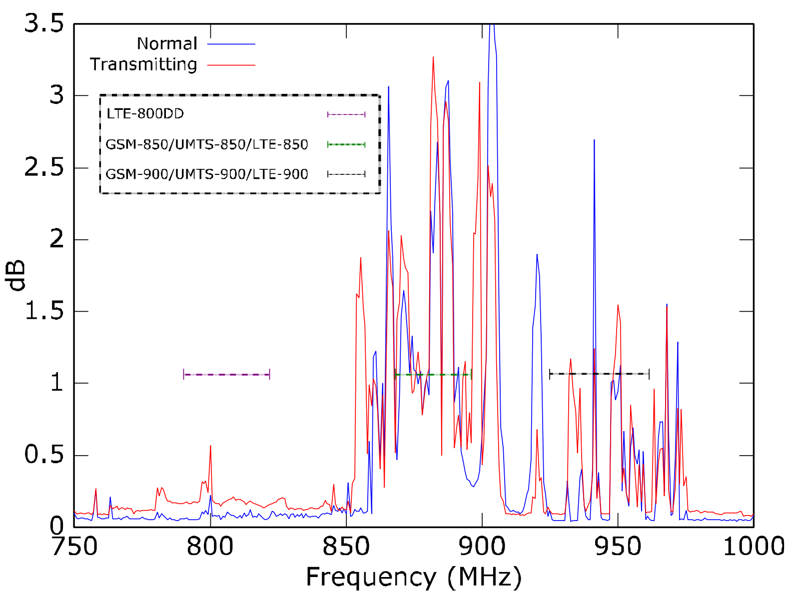


Figure 3: A plot of the amplitude of the radio waves emitted from a motherboard with an 800MHz I/O bus using DDR3-1600 RAM. Blue: casual use of the computer. Red: our transmission algorithm while using the dual channel data paths.

[USENIX Security 2015]

We propose that a computer's memory bus can be exploited to act as an antenna capable of transmitting information wirelessly to a remote location. When data is exchanged between the CPU and the RAM, radio waves are emitted from the bus's long parallel circuits. The emission frequency is loosely wraps around the frequency of the RAM's I/O bus clock with a marginal span of +/-200MHz. The casual use of a computer does not generate these radio waves at significant amplitude, since it requires a major buildup of voltage in the circuitry. Therefore, we have found that by generating a continuous stream of data over the multi-channel memory buses, it is possible to raise the amplitude of the emitted radio waves. Using this observation, we are able to modulate binary data over these carrier waves by deterministically starting and stopping multi-channel transfers using special CPU instructions.

Analog Cybersecurity: Row

```
codela:
  mov (X), %eax  // read from address X
  mov (Y), %ebx  // read from address Y
  clflush (X)    // flush cache for address X
  clflush (Y)    // flush cache for address Y
  jmp codela
```

A snippet of x86 assembly code that induces the row hammer effect (memory addresses `X` and `Y` must map to different DRAM rows in the same memory bank)[1]:3[4][14]:13–15

https://en.wikipedia.org/wiki/Row_hammer

So, you depend on sensors?

https://www.pinterest.com/pin/499547783640216987/

Creating Trustworthy Sensors

- 🌈 Demystify analog sensor attack surface
  - 👉 Test to security **FAILURE**, not test to ¯_(ツ)_/¯
  - 👉 **Unwrap abstractions** of electrical engineering, mechanical engineering, materials science
- 🌈 Ad-hoc security ⇒ measurable science
  - 👉 Physically de-risk **intentional interference** with more deliberate HW specs & design (e.g., resonance)
- 🌈 Rethink ICs and hardware-software APIs
  - 👉 Convey to SW stack **WHY** trust sensor output
  - 👉 HW should expose **HINTS** of trustworthiness

Analog Cybersecurity Risks

- Computers have always been vulnerable to analog cybersecurity threats

- What's changing?
  - Degree of connectedness and dependence
  - From human-in-the-loop to automated consequences
  - Increased risks to availability and integrity

- Maybe it's a not a good idea to put a computer in everything unless there's a good reason

https://onemomentonly.files.wordpress.com/2013/06/boiling-frog1.jpg

Homework and Next

- Homework
  - ✓ Lab #1: Due Mon, Sep 22
  - ➡ Prelab #2: Due Thu, Sep 25
  - ➡ Essay #1: Due Mon, Sep 29
- Next
  - Thursday: Lab #2 time in class