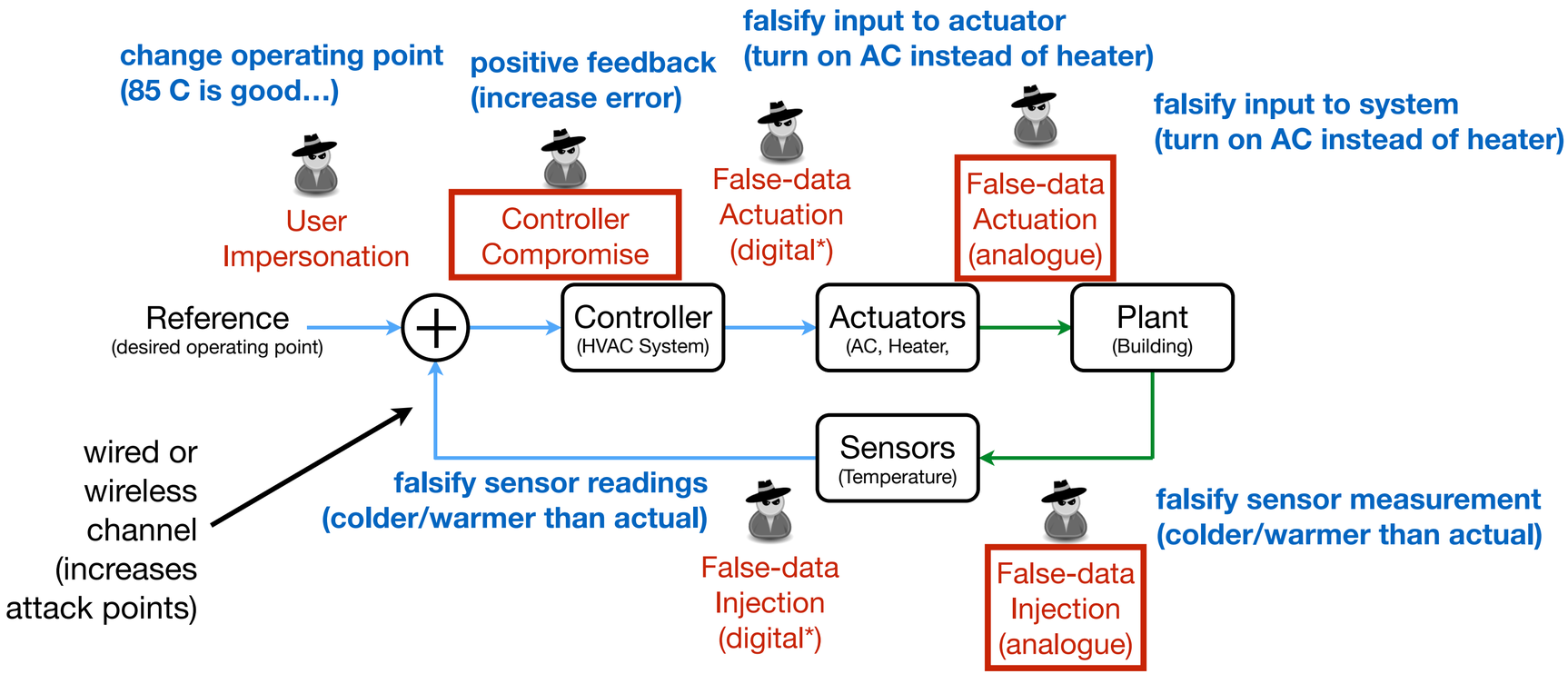
I Intended That: Using EMI to Control Digital Systems

Ryan M. Gerdes
Bradley Department of Electrical and Computer Engineering
Virginia Tech

EECE 5698-008: Special Topics: Cyber-Physical Security of IoT Systems in the Age of AI
Fall 2025
Northeastern University
November 10, 2025

cyber-physical systems threats

(a building HVAC)



non-comprehensive: controls centric

(e.g., system timing)

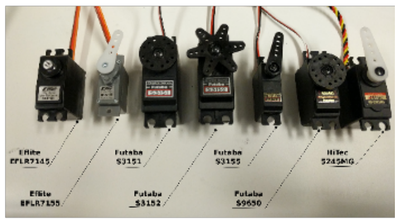
intentional electromagnetic interference

(related work)

IEMI on Analog Signals
- Light Sensors
- Microphones
- Cardiac Devices (CIED and ECG)
- Voltage/current Sensors
- Temperature Sensors
- Speed Sensors
- CCD Cameras

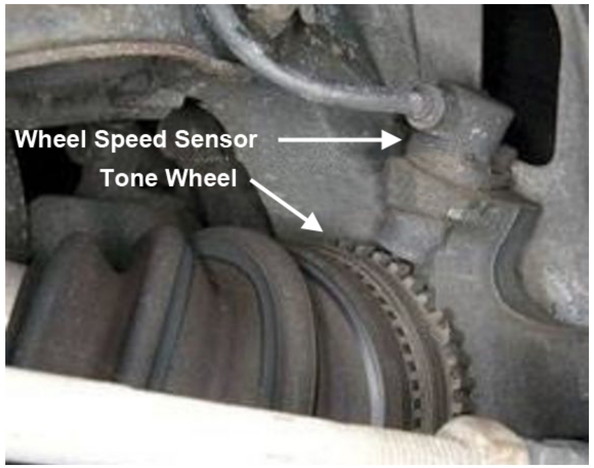
IEMI on Actuation Signals
- Servos and DC motors
- Transistors/Current Switches

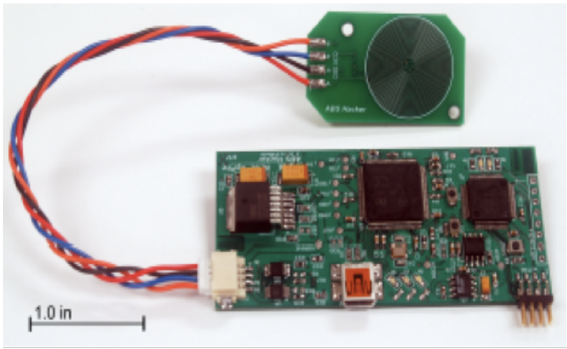


Sensors and actuators attacked in the literature

Shoukry et al. report an IEMI attack that manipulates the speed data in an anti-lock braking system (ABS)



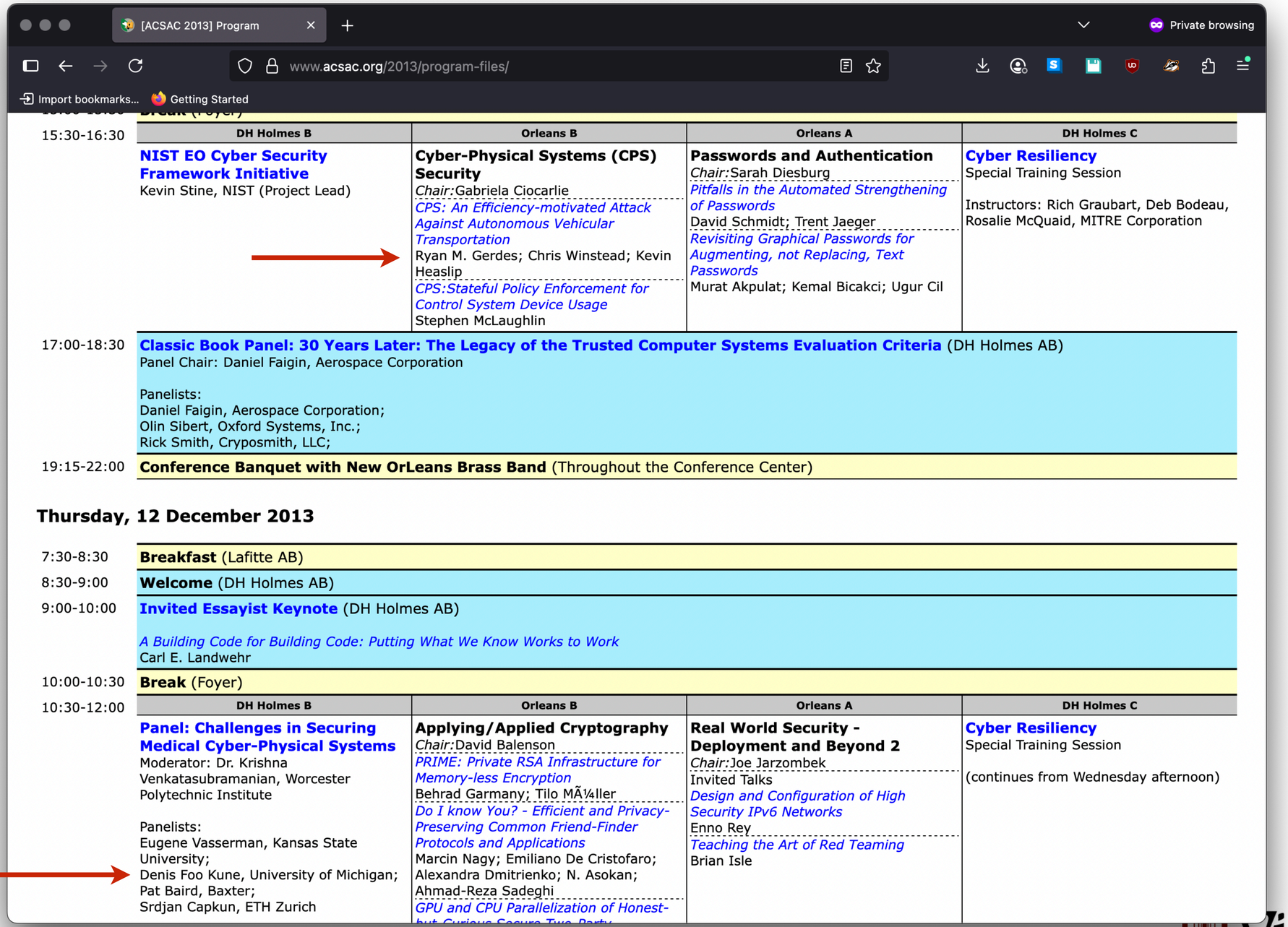


ABS Hacker

Challenges:

The required induced voltage for the digital and actuation signals is high, e.g., 5 V

The induced voltage for the analog signals is relatively low, e.g., 100-200 mV



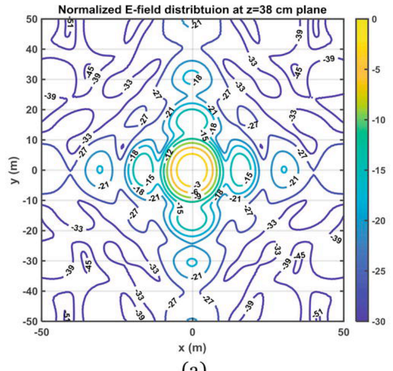
	DH Holmes B	Orleans B	Orleans A	DH Holmes C
15:30-16:30	**NIST EO Cyber Security Framework Initiative** Kevin Stine, NIST (Project Lead)	**Cyber-Physical Systems (CPS) Security** *Chair:*Gabriela Ciocarlie *CPS: An Efficiency-motivated Attack Against Autonomous Vehicular Transportation* Ryan M. Gerdes; Chris Winstead; Kevin Heaslip *CPS:Stateful Policy Enforcement for Control System Device Usage* Stephen McLaughlin	**Passwords and Authentication** *Chair:*Sarah Diesburg *Pitfalls in the Automated Strengthening of Passwords* David Schmidt; Trent Jaeger *Revisiting Graphical Passwords for Augmenting, not Replacing, Text Passwords* Murat Akpulat; Kemal Bicakci; Ugur Cil	**Cyber Resiliency** Special Training Session Instructors: Rich Graubart, Deb Bodeau, Rosalie McQuaid, MITRE Corporation
17:00-18:30	**Classic Book Panel: 30 Years Later: The Legacy of the Trusted Computer Systems Evaluation Criteria** (DH Holmes AB) Panel Chair: Daniel Faigin, Aerospace Corporation Panelists: Daniel Faigin, Aerospace Corporation; Olin Sibert, Oxford Systems, Inc.; Rick Smith, Cryposmith, LLC;			
19:15-22:00	**Conference Banquet with New OrLeans Brass Band** (Throughout the Conference Center)			

Thursday, 12 December 2013

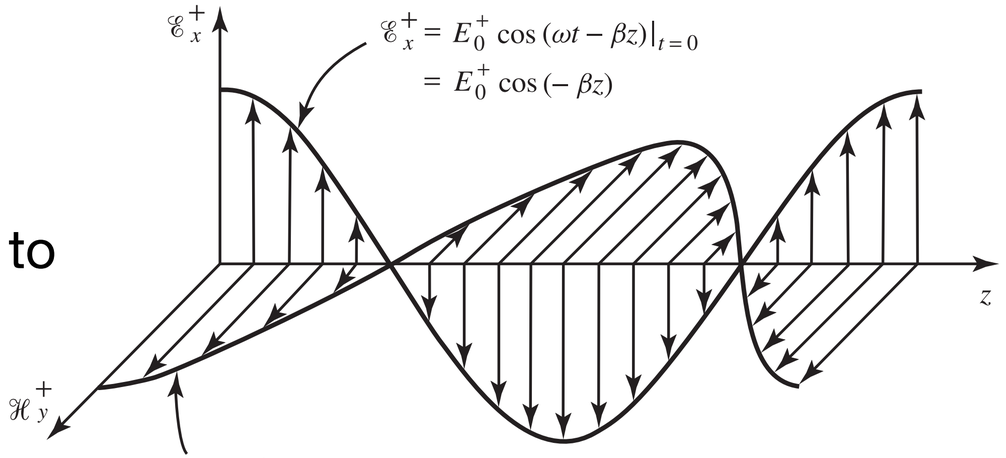
7:30-8:30	**Breakfast** (Lafitte AB)			
8:30-9:00	**Welcome** (DH Holmes AB)			
9:00-10:00	**Invited Essayist Keynote** (DH Holmes AB) *A Building Code for Building Code: Putting What We Know Works to Work* Carl E. Landwehr			
10:00-10:30	**Break** (Foyer)			
10:30-12:00	**Panel: Challenges in Securing Medical Cyber-Physical Systems** Moderator: Dr. Krishna Venkatasubramanian, Worcester Polytechnic Institute Panelists: Eugene Vasserman, Kansas State University; Denis Foo Kune, University of Michigan; Pat Baird, Baxter; Srdjan Capkun, ETH Zurich	**Applying/Applied Cryptography** *Chair:*David Balenson *PRIME: Private RSA Infrastructure for Memory-less Encryption* Behrad Garmany; Tilo MÃ¼ller *Do I know You? - Efficient and Privacy-Preserving Common Friend-Finder Protocols and Applications* Marcin Nagy; Emiliano De Cristofaro; Alexandra Dmitrienko; N. Asokan; Ahmad-Reza Sadeghi *GPU and CPU Parallelization of Honest-but-Curious Secure Two-Party*	**Real World Security - Deployment and Beyond 2** *Chair:*Joe Jarzombek Invited Talks *Design and Configuration of High Security IPv6 Networks* Enno Rey *Teaching the Art of Red Teaming* Brian Isle	**Cyber Resiliency** Special Training Session (continues from Wednesday afternoon)

background

- high power (kW): destruction or disruption
- low power: influencing a measurement/signal
  - alter voltages/currents in a sensing circuit that correspond to the phenomenon being measured
  - the voltages that determine the amount and direction of actuation
  - electric field (capacitive coupling): **E**
  - magnetic field (inductive coupling): **H**
  - electromagnetic field (time varying E/H gives rise to)
- far field, near-field (sinusoidal sources, mainly)
  - far: E/H coupled, predictable pattern (analytical methods)
    - shielding via Faraday cage (wavelength/10)
  - near: E/H decoupled, unpredictable (computational)
    - electric: shielding effective
    - magnetic: difficult to shield against (low-frequency)



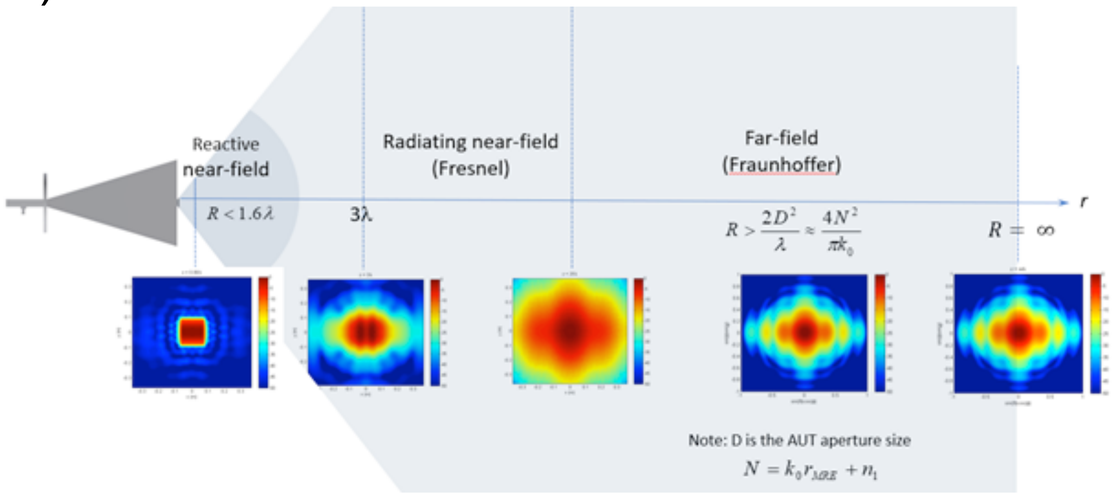
:E in the near field (this is an antenna, so actually good)



$$\mathscr{H}_y^+ = \frac{E_0^+}{\eta} \cos(\omega t - \beta z)|_{t=0} = \frac{E_0^+}{\eta} \cos(-\beta z)$$

what you imagine E/H look like

material properties dictate which dominates



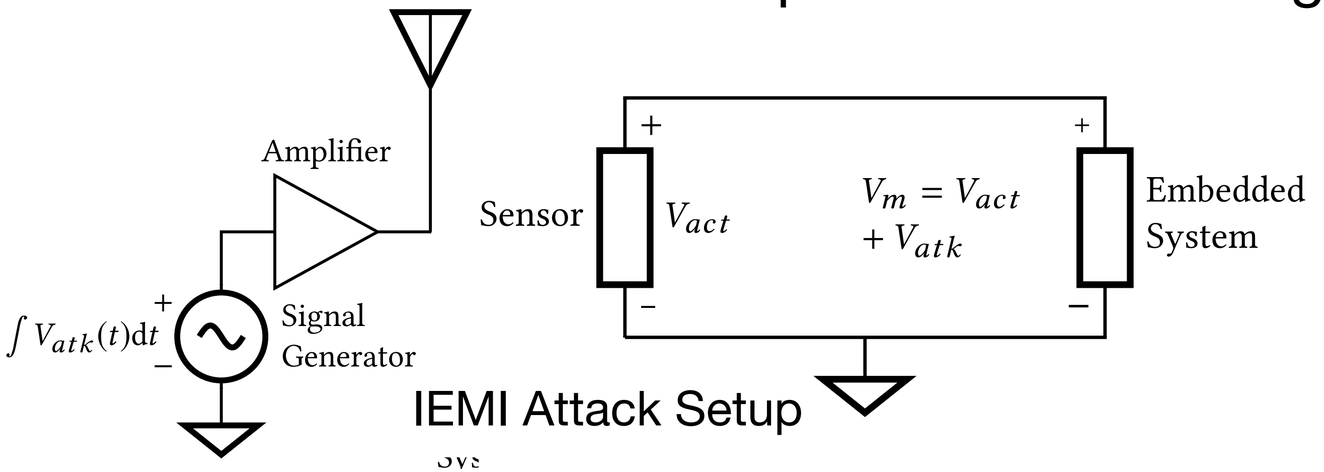
D aperture size, adjustable

Virginia Tech
College of Engineering

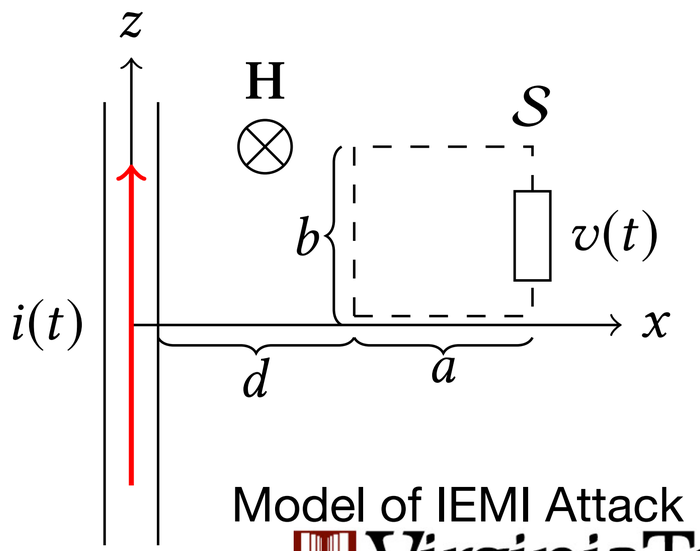
intentional electromagnetic interference

(inductive coupling)

- Example system: voltage transducer (sensor)
  - Attack model generic (applicable to any system relying on voltage/current measurement)
  - Attacker objective: alter voltages/currents in a sensing circuit that correspond to the phenomenon being measured (Figure, lower left)
  - Attack Vector: superimpose a voltage (V_{atk}) onto the true output of the sensor (V_{act})
  - Mechanism of attack: magnetic, near-field coupling (Figure, lower right)
    - Attacker generates current *i(t)* proportional to integral of V_{atk}, creates magnetic field, **H**, that induces V_{atk}
    - Near field: difficult and expensive to shield against



IEMI Attack Setup

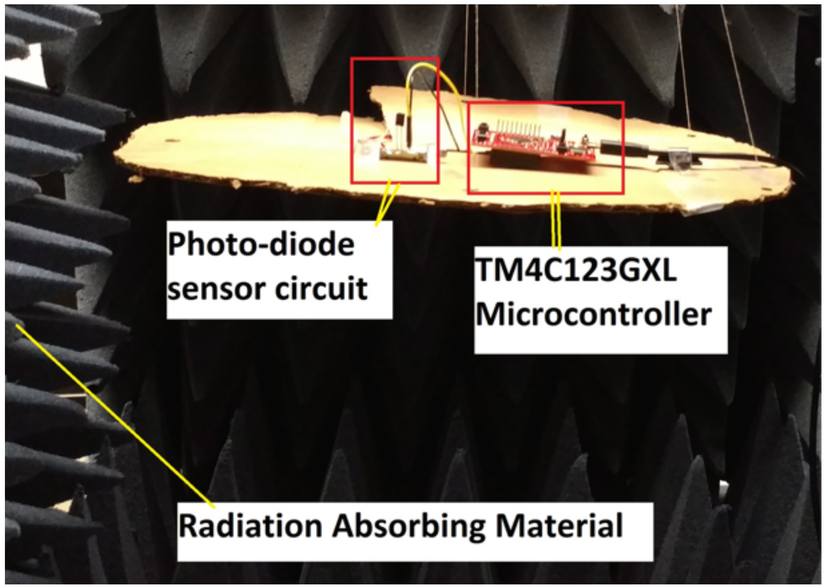


Model of IEMI Attack

Electromagnetic Induction Attacks Against Embedded Systems, Selvaraj et al., AsiaCCS, 2018

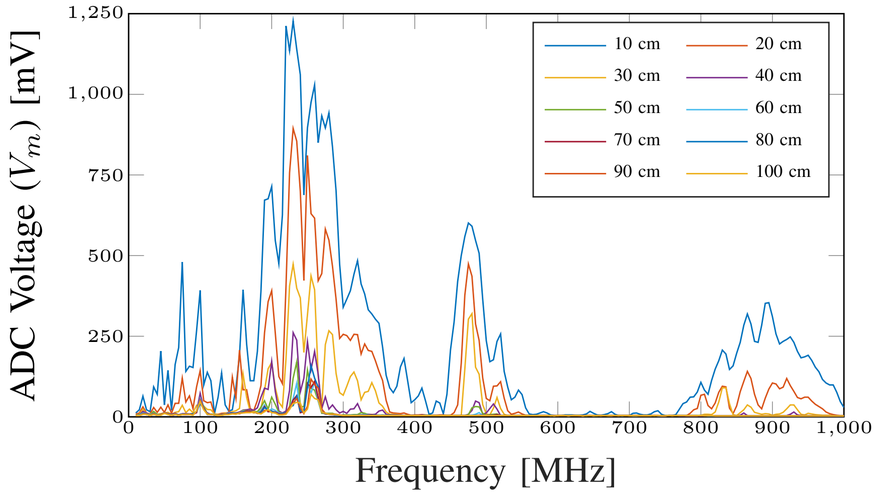
intentional electromagnetic interference

(anlog sensors)



Experimental setup for ADC-targeted (voltage output) Attacks

Voltage Induced in Attack vs. Frequency (0 V is nominal)



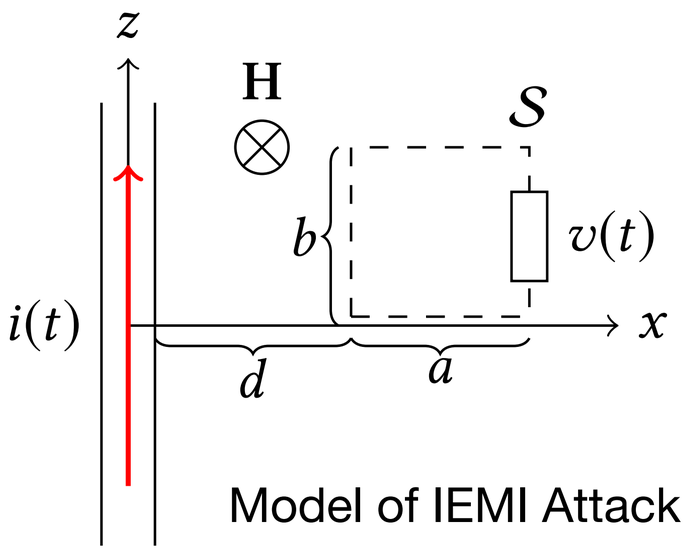
Q1: frequency dependence

Q2: DC offset

(EMI is zero mean)

Electromagnetic Induction Attacks Against Embedded Systems, Selvaraj et al., AsiaCCS, 2018

VirginiaTech
College of Engineering



Model of IEMI Attack

$$\mathbf{H} = \hat{y}\frac{i(t)}{2\pi x}$$

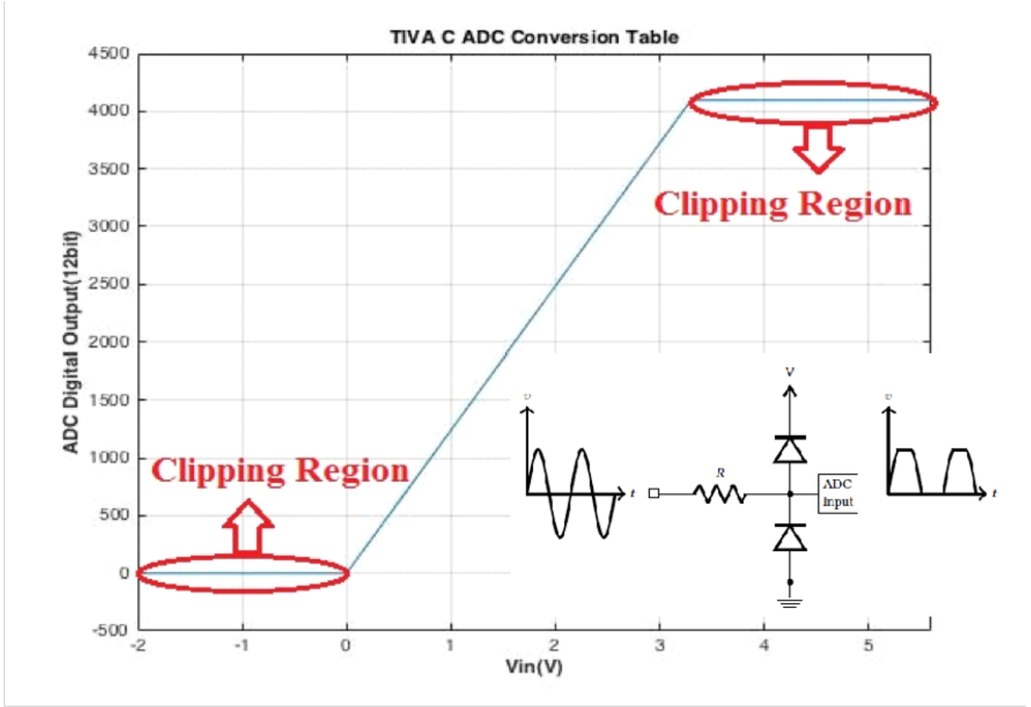
$$v(t) = \oint_{\partial S} \mathbf{E}.d\ell = -\frac{d}{dt}\iint_{S} \mu\mathbf{H}.d\mathbf{S}$$

$$v(t) = -\mu\frac{di(t)}{dt}\left[\frac{b}{2\pi}\ln\left(\frac{d+a}{d}\right)\right]$$

no DC component!

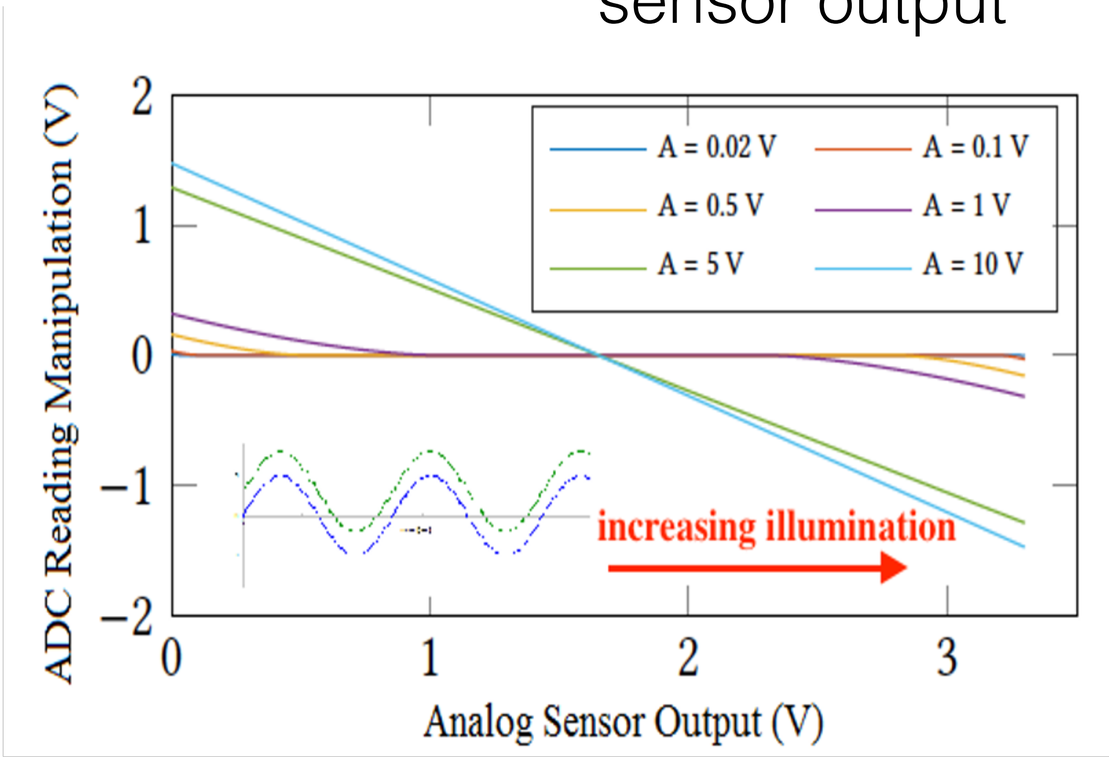
intentional electromagnetic interference

(attack theory)



analogue2digital: linear and nonlinear range

iemi amplitude effect on sensor output

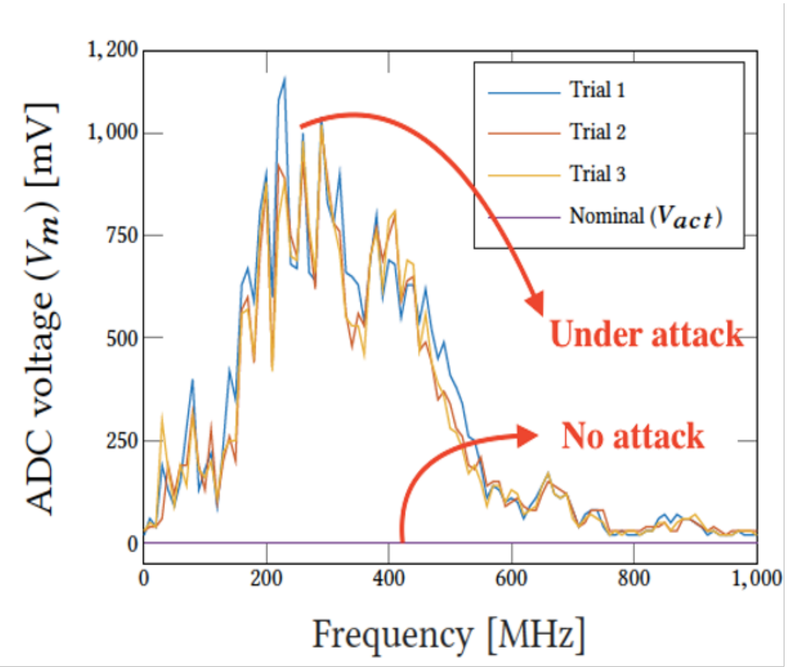


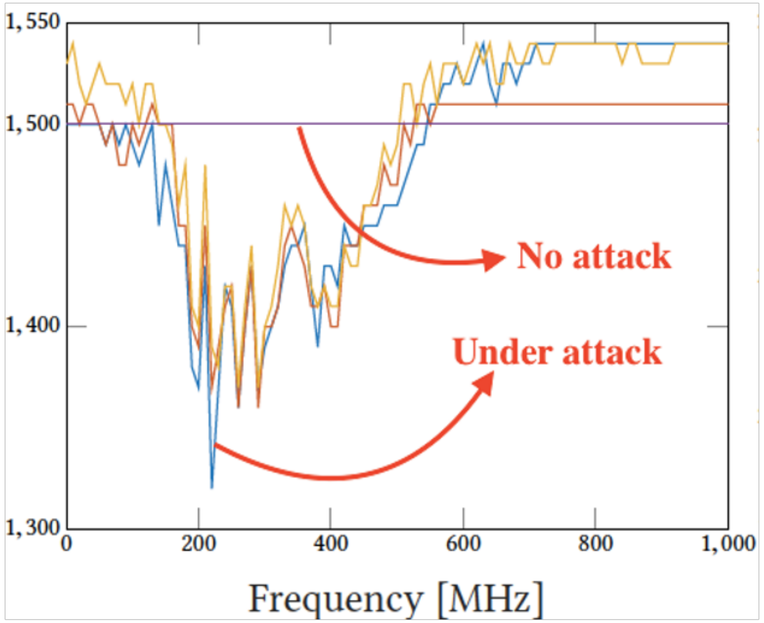
intentional electromagnetic interference

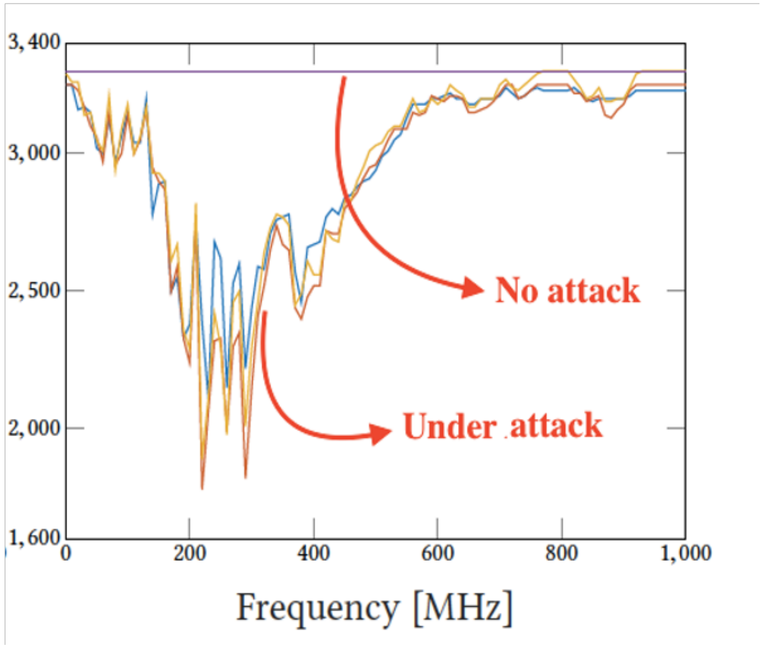
(attack theory)

clipping+diode nonlinearity(?)

(increasing/decreasing middle reading)







clipping

(increasing low reading)

clipping

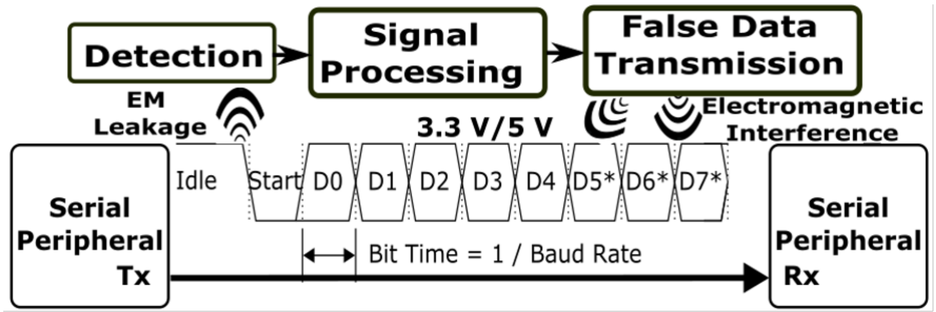
(decreasing high reading)

Q: asymmetry in l2h and h2l

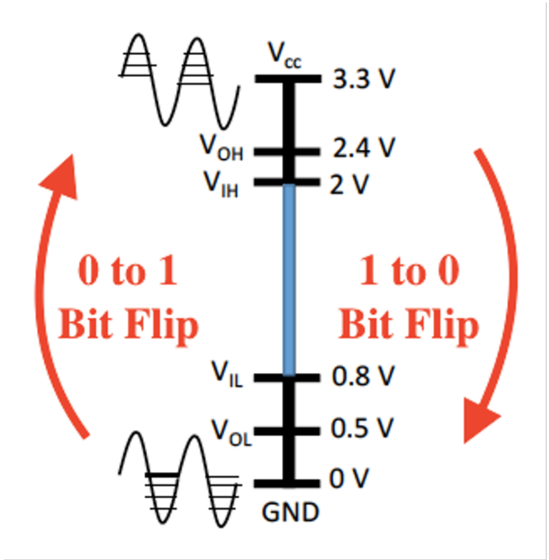
A: uC can sink more current than source(?)

intentional electromagnetic interference

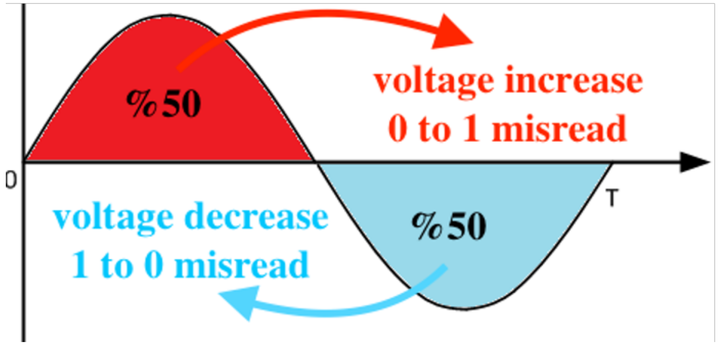
(digital sensors/actuators)



Attacks on serial communication (UART)



conditions for bit flips



50% of sine contributes 0 to 1 flip
50% of sine contributes 1 to 0 flip
whether a bit is flipped depends on bit and when read

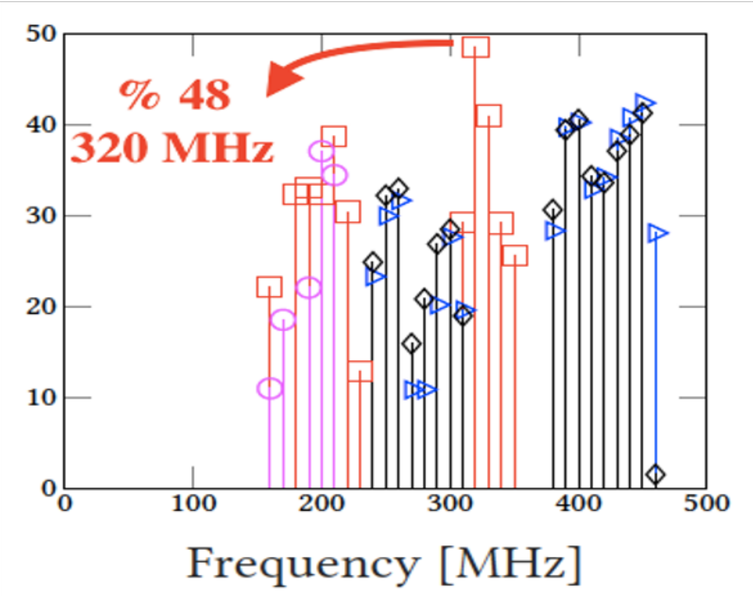
A typical vehicle will have an admixture of sensors:

1. digital interfaces (e.g., UART, SPI, I2C)
2. others output a voltage proportional to the phenomenon being measured

intentional electromagnetic interference

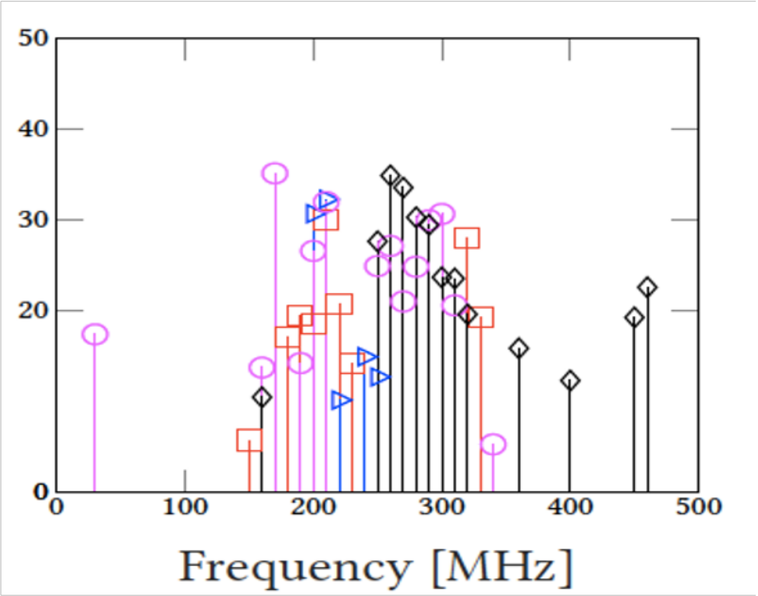
(digital sensors/actuators)

theoretically: 50% of bits flipped



0 to 1

1 to 0



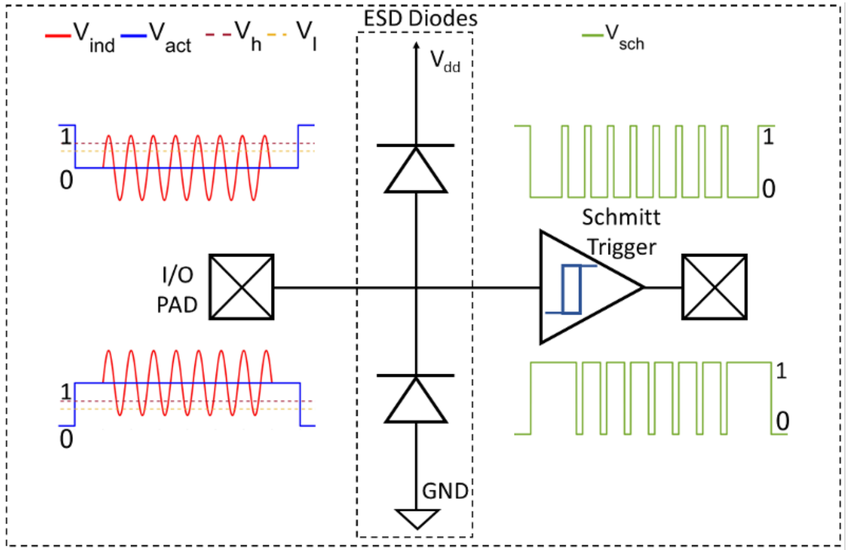
asymmetry: larger drop
for 1 to 0(?)

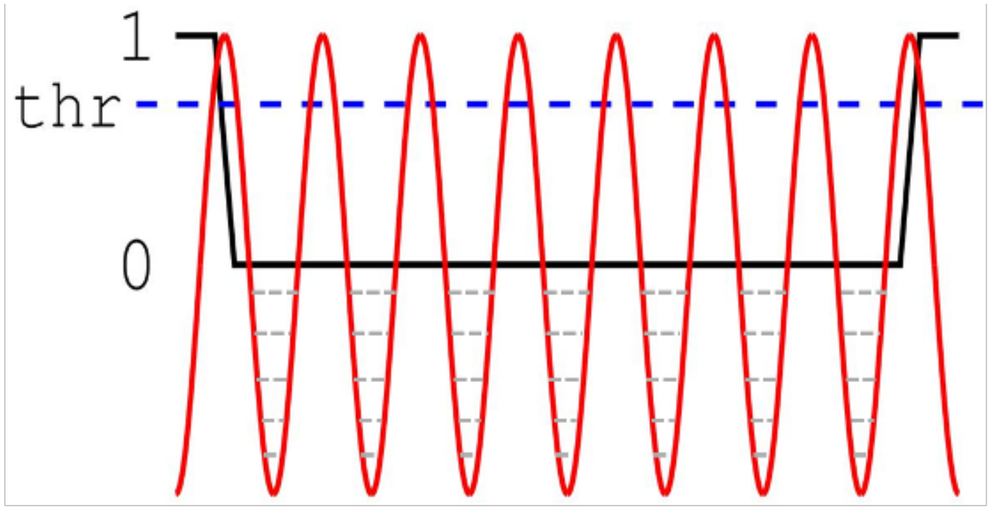
Q: targeted bit flips?

intentional electromagnetic interference

(digital sensors/actuators)

For the attack to be successful, sampling instant should be during one of the flips (unlikely)





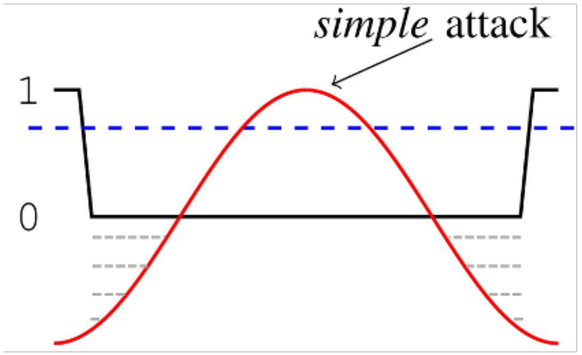
Schmitt trigger is a hysteresis comparator with two thresholds (Vh and Vl)

Wireless Manipulation of Serial Communication, Dayanikli et al., AsiaCCS, 2022

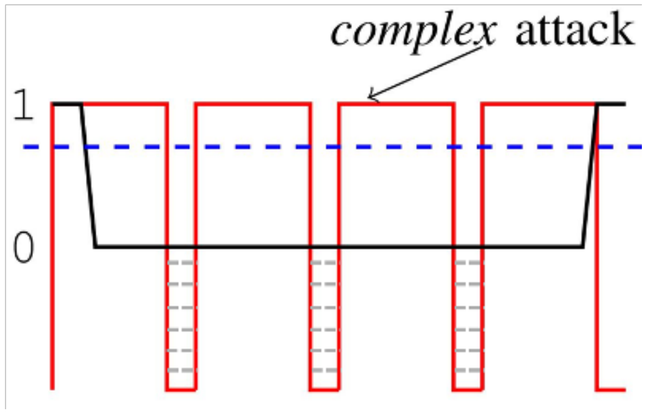
intentional electromagnetic interference

(digital sensors/actuators)

theory of attack:



half-period of attack waveform = bit duration



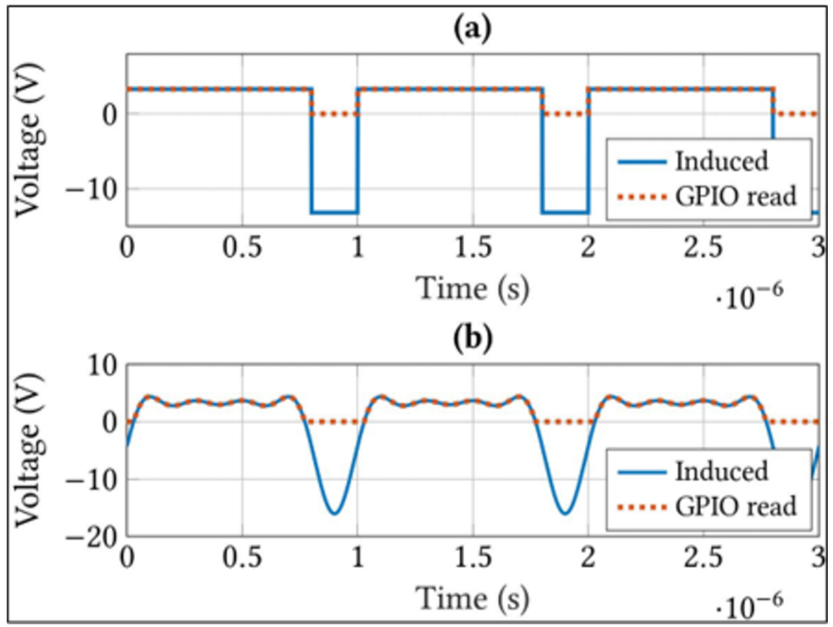
create DC signal

	Simple Waveform	Complex Waveform
Bandwidth	Narrowband	Wideband
Attack Frequency	Depends on baud rate (Low)	Doesn't depend on baud rate (High)
Timing	Fine synchronization with the start of frame.	Loosely synchronized.
Attacker knowledge about the victim	Limited	Detailed
Attack Distance	Low	High

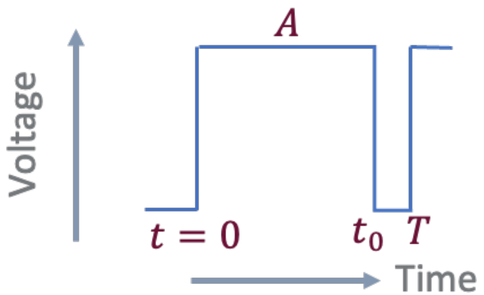
intentional electromagnetic interference

(digital sensors/actuators)

creating complex waveform:



(a) Ideal rectangular waveform, and (b) Fourier series approximation with 5 harmonics



we know how to transmit sinusoids!

$$v_a(t) = \sum_{i=-n}^{n} c_i \exp(j2\pi i f_0 t)$$

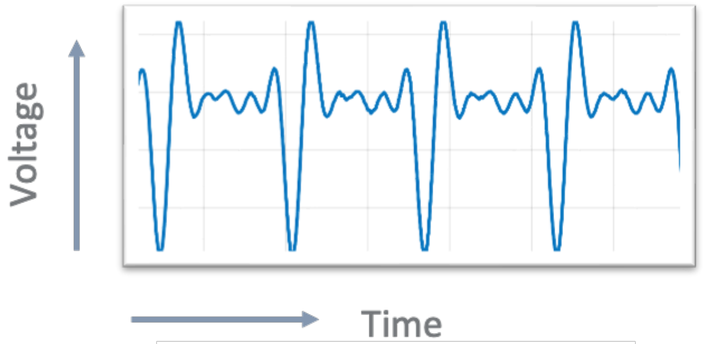
$$c_i = j\frac{A}{2\pi i}\frac{T}{T - t_0}[\exp(-j2\pi i\frac{t_0}{T}) - 1]$$

this seems unpleasant, though

intentional electromagnetic interference

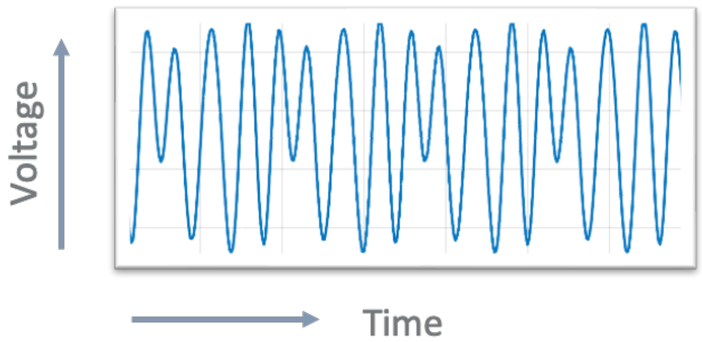
(digital sensors/actuators)

naive:



$$v_a(t) = \sum_{i=-n}^{n} c_i \exp(j2\pi i f_0 t)$$

$$v_a(t) = \sum_{i=-n}^{n} \frac{\mathbf{1}}{\mathbf{a_i}} c_i \exp(j(2\pi i f_0 t - \boldsymbol{\phi_i}))$$



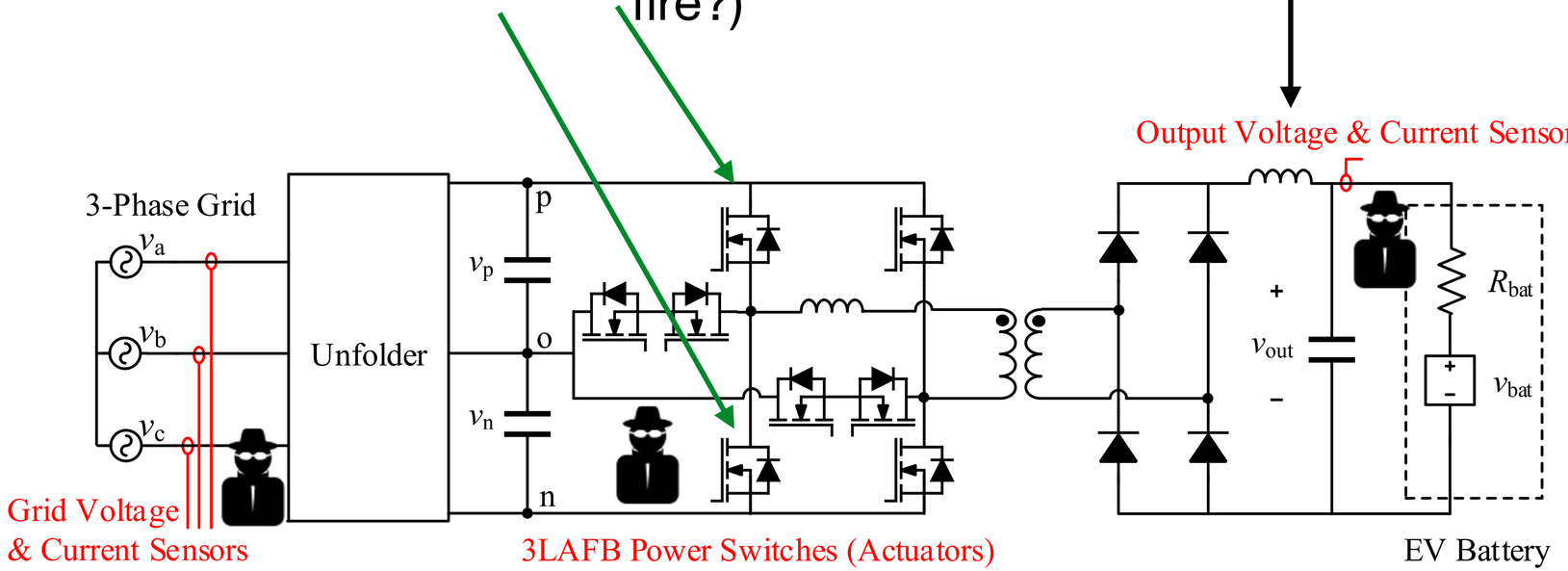
voltage at pin

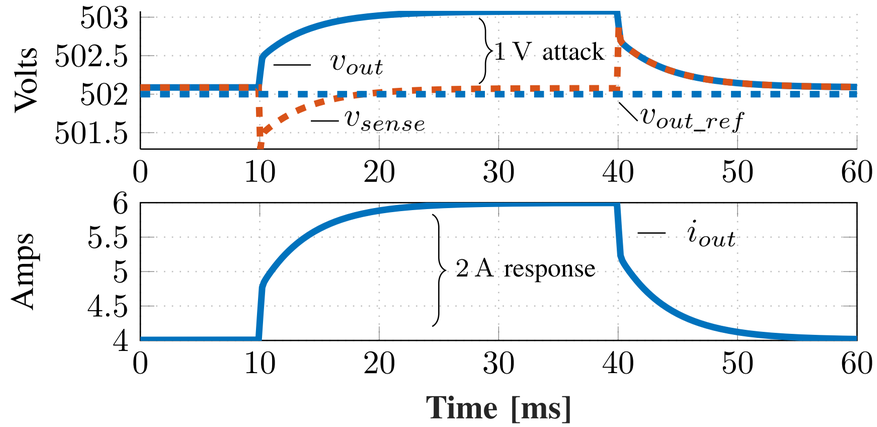
intentional electromagnetic interference

(actuator attacks)

if both switches closed, short (starts fire?)

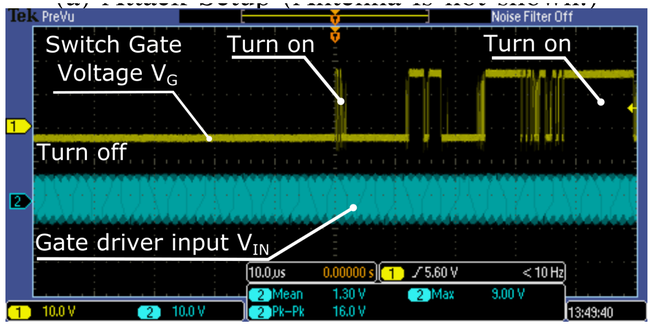
controls output current



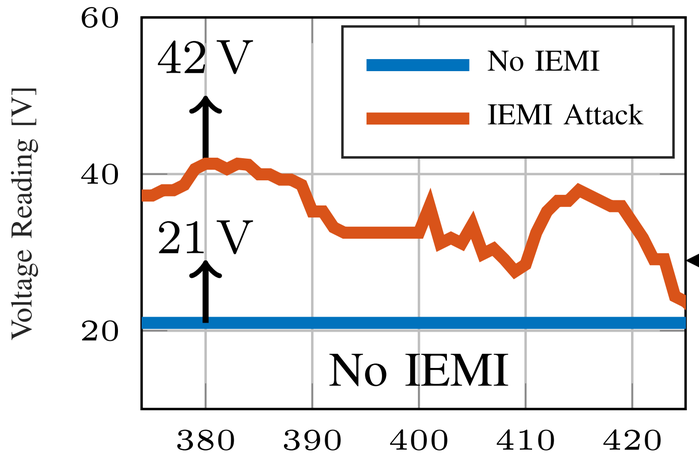


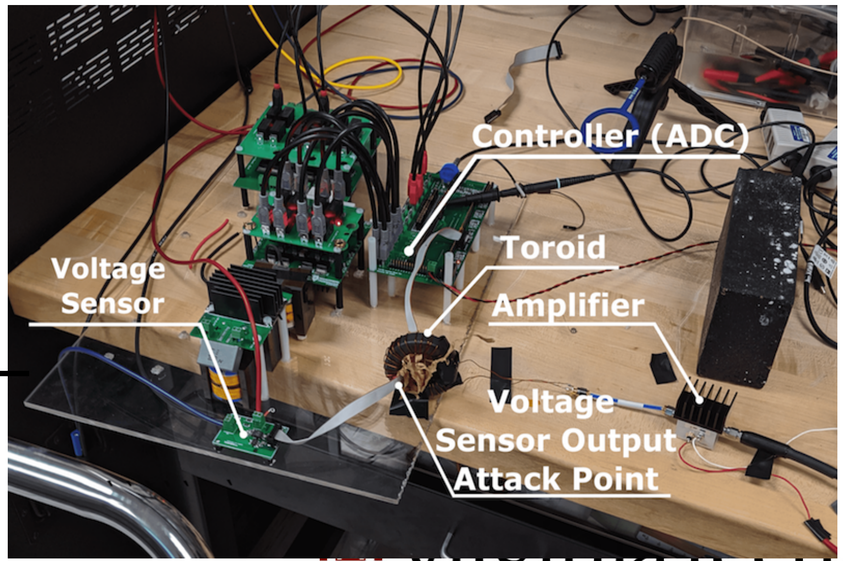
small change in voltage output results in large currents

Modern power converter design



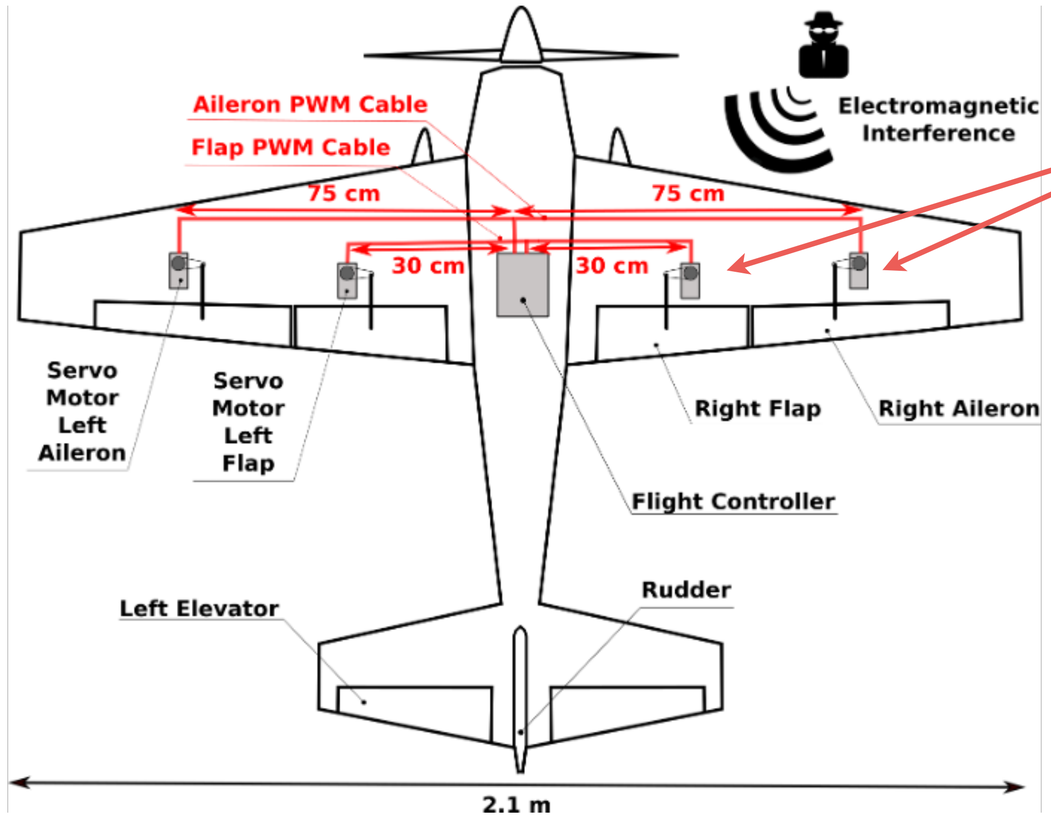
Turning on switches using IEMI

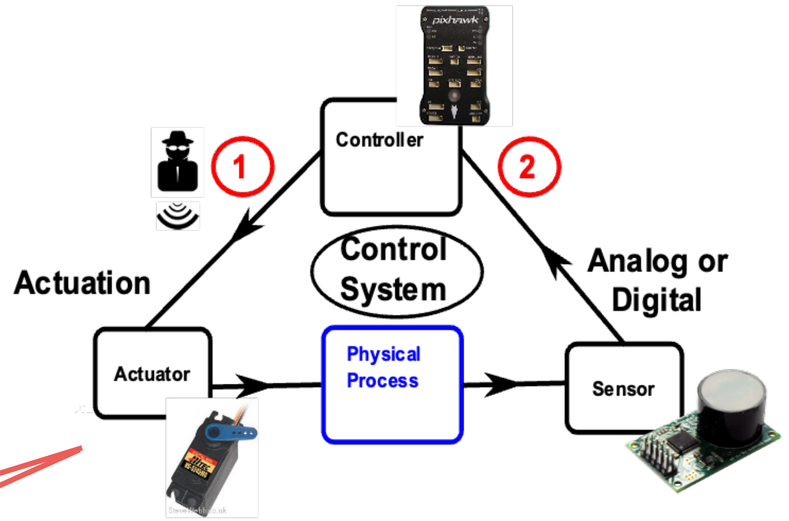




intentional electromagnetic interference

(actuator attacks)





our threat model:

1. indirect access to system
   (no direct connection)
2. white box knowledge
   (electrical dimensions of victim circuitry)
3. RF IEMI
4. manipulate/prevent the control of PWM-controlled actuators

intentional electromagnetic interference

(actuator attacks)

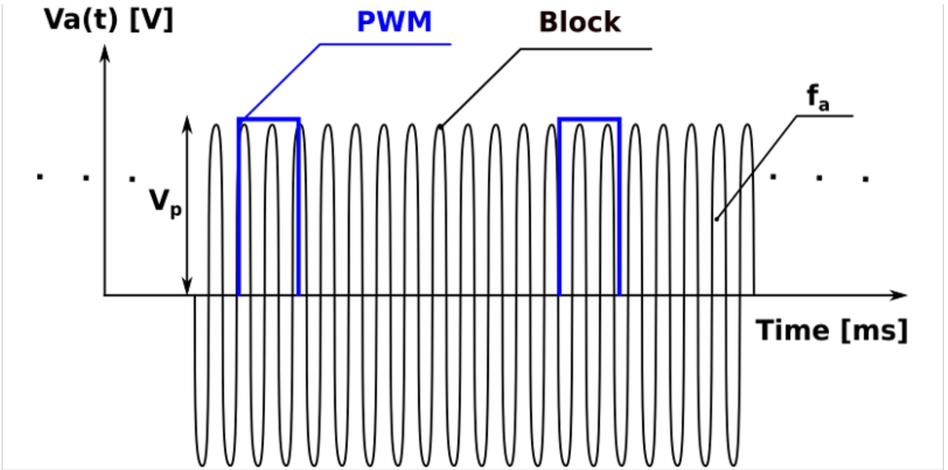
attack waveforms

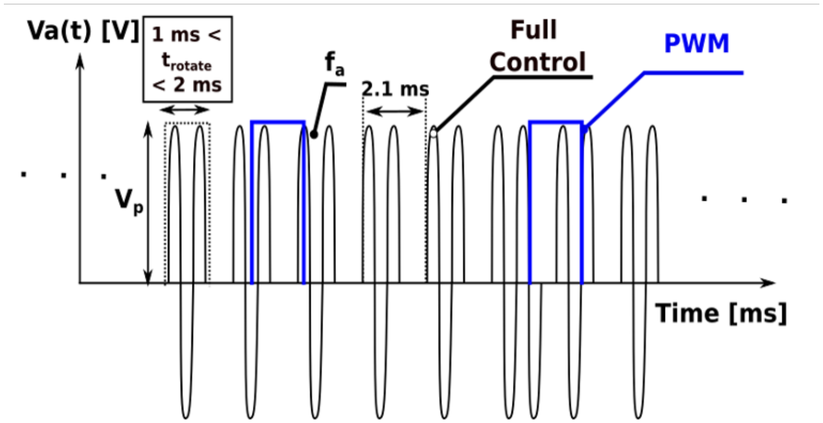
Block

Continuous wave signal at the victim resonance

The attacker can block the control of the actuators.

Applies to all tested servo and DC motors.





Full Control

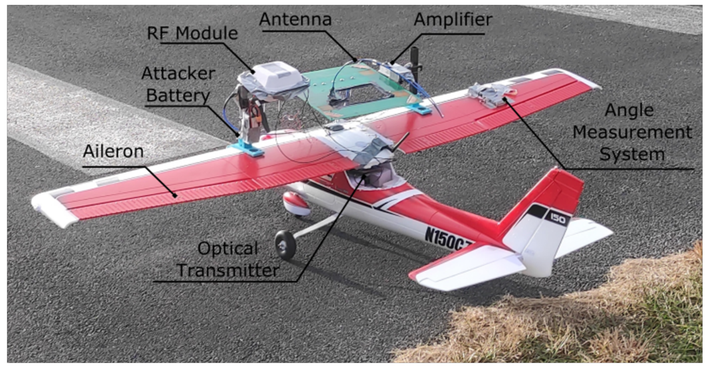
Frequent sinusoidal pulses at the victim resonance

The attacker can fully control the Futaba-make servo models.

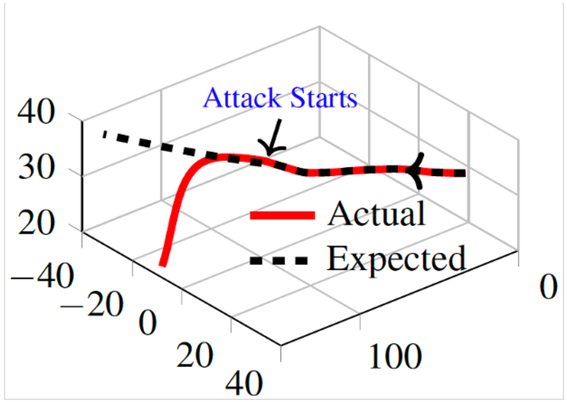
intentional electromagnetic interference

(actuator attacks)

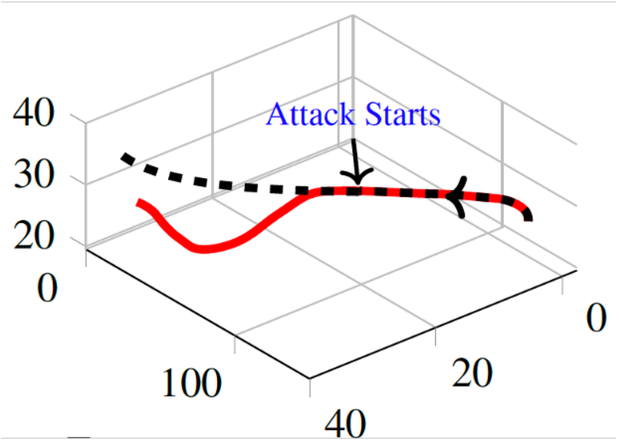
experimental results



block



full control



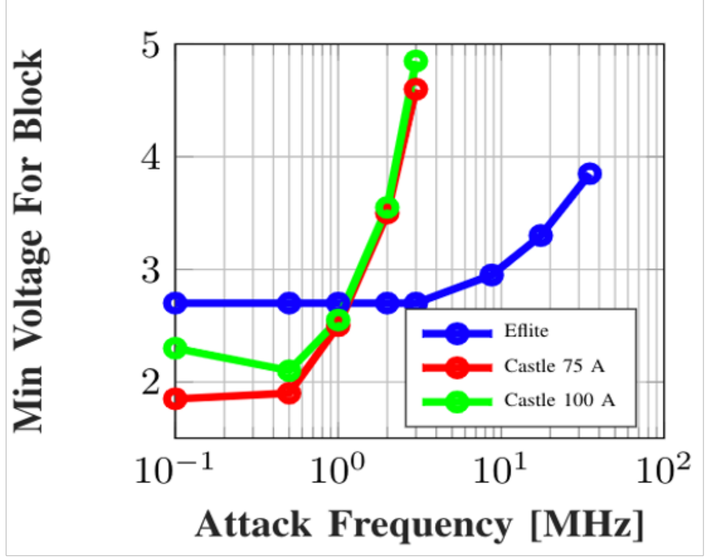
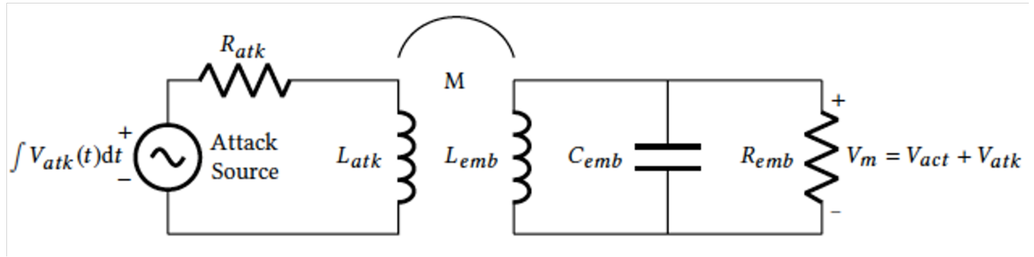
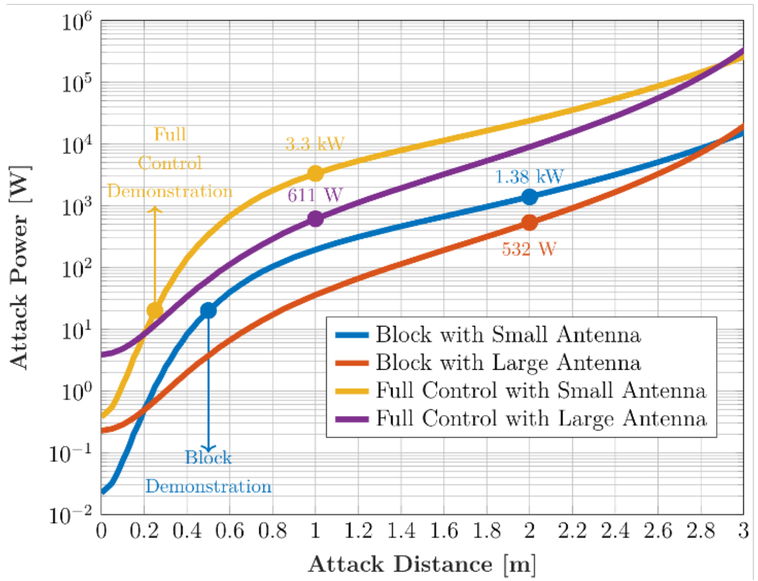
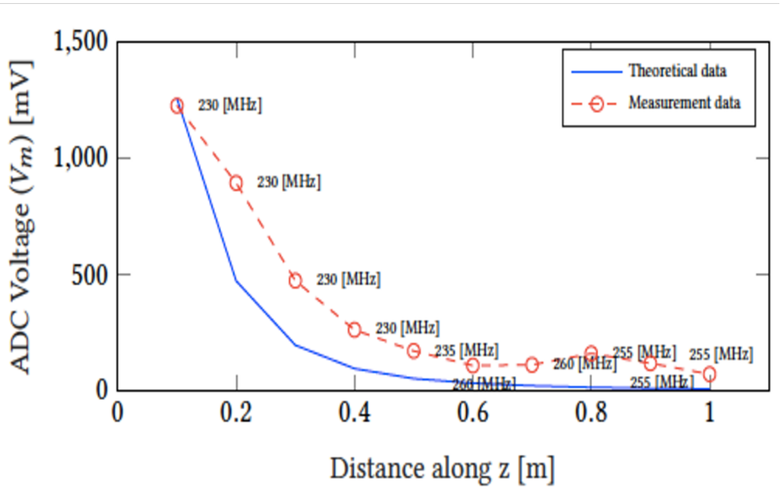


Figure 14: Attack distance and power relationship



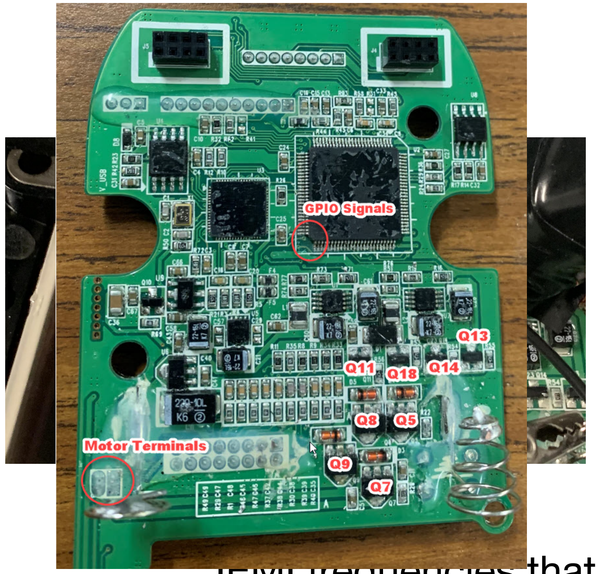
$$P_r = P_t \left(\frac{2\omega_o M}{(R_{atk})(R_{emb}) + (\omega_o M)^2} \right)^2 (R_{atk})(R_{emb})$$

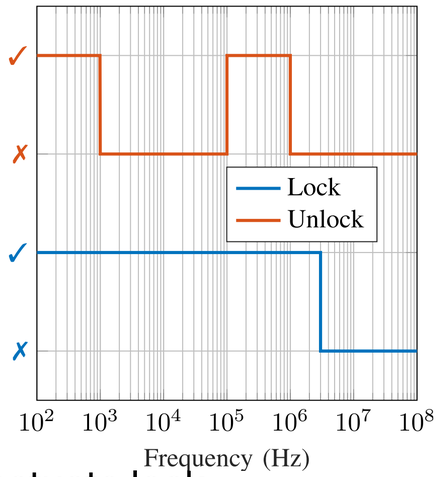




intentional electromagnetic interference

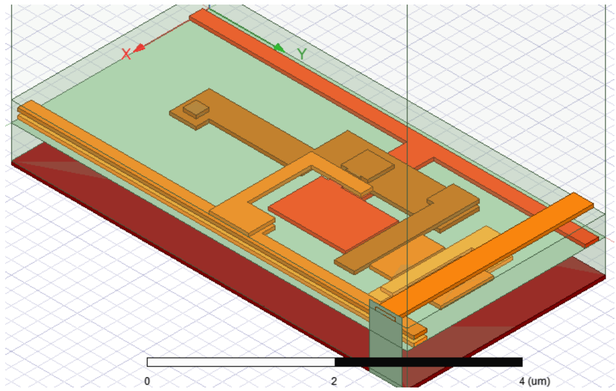
(vulnerability analysis)



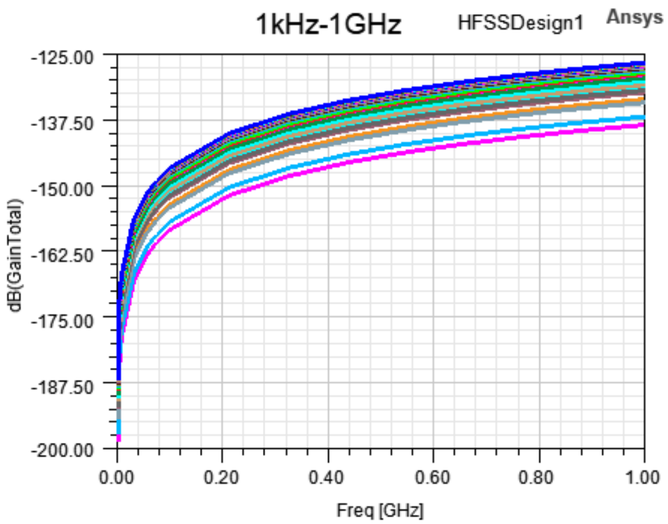


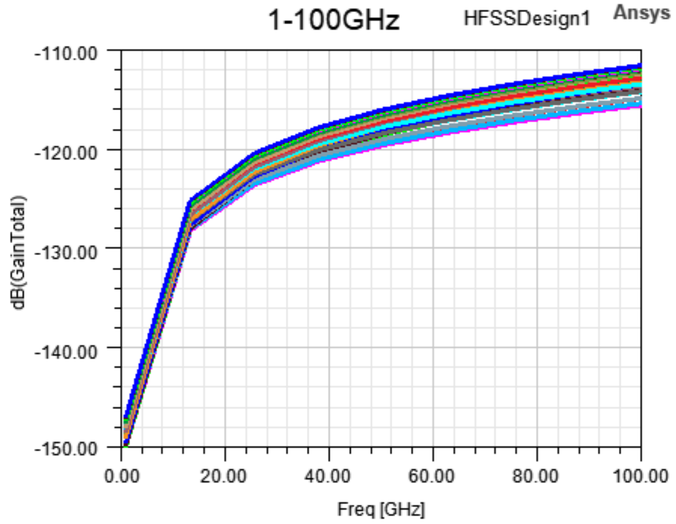
IEMI frequencies that actuate lock

PCB of popular smart lock

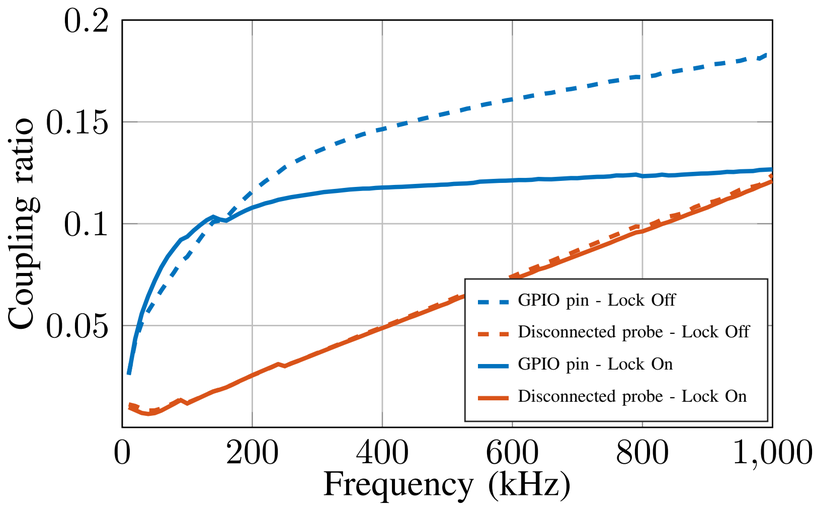


CMOS Pixel in ANSYS





Susceptibility of pixel to manipulation (higher better) vs. frequency



received power