USENIX Security Symposium 2015

Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

2015. 08. 14.

Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park,
Juhwan Noh, Kibum Choi, Jungwoo Choi, and **Yongdae Kim**
Electrical Engineering at KAIST
System Security Lab.

KAIST

Drones (Multi-coptors)

- ❖ Distribution delivery
- ❖ Search and rescue
- ❖ Aerial photography
- ❖ Private hobby

Drone, A New Threat

- Air terrorism using a weaponized drone

Drone, A New Threat

❖ Air terrorism using a weaponized drone

Teenager's video of gun-firing drone prompts investigations by aviation officials, police Jul. 2015

Drone, A New Threat

❖ Air terrorism using a weaponized drone

Teenager's video of gun-firing drone prompts investigations by aviation officials, police Jul. 2015

Man detained outside White House for trying to fly drone May. 2015

Drone, A New Threat

❖ Air terrorism using a weaponized drone

Teenager's video of gun-firing drone prompts investigations by aviation officials, police Jul. 2015

Man detained outside White House for trying to fly drone May. 2015

Arrest after drone with radioactive material lands on Japan PM's rooftop Apr. 2015

Drone, A New Threat

❖ Air terrorism using a weaponized drone

Teenager's video of gun-firing drone prompts investigations by aviation officials, police Jul. 2015

Man detained outside White House for trying to fly drone May. 2015

Arrest after drone with radioactive material lands on Japan PM's rooftop Apr. 2015

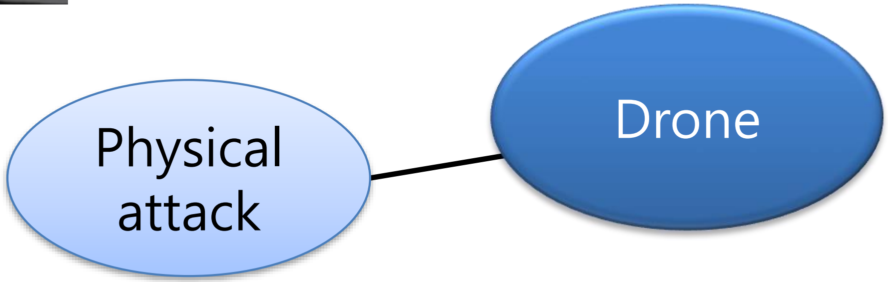
The Switch

Watch the Pirate Party fly a drone in front of Germany's chancellor Sep. 2013

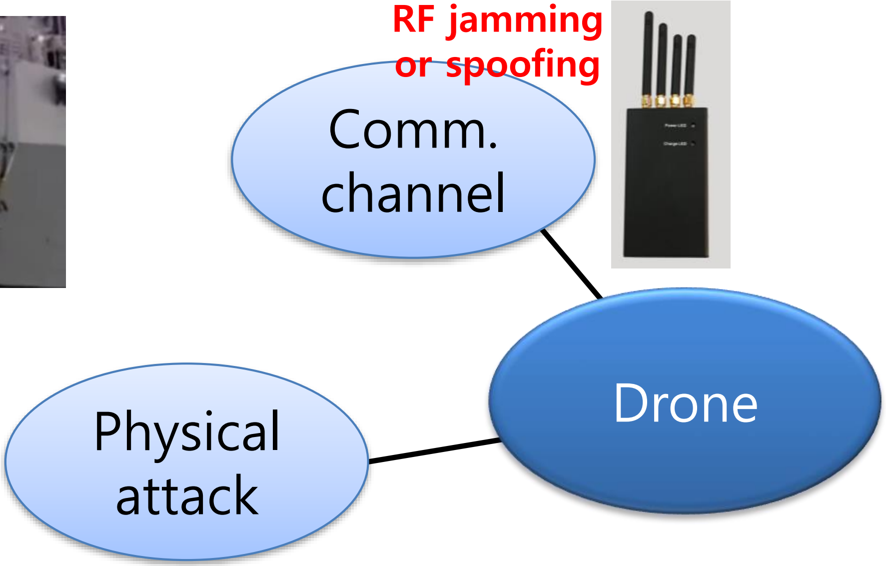
Attack Vectors of Drone

Drone

Attack Vectors of Drone



Attack Vectors of Drone



Attack Vectors of Drone

Physical attack

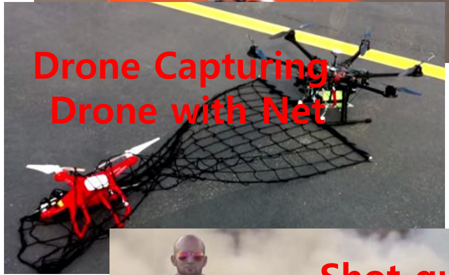
RF jamming or spoofing

Comm. channel

Drone

Software hacking

Attack Vectors of Drone



RF jamming
or spoofing

Comm. channel

Software hacking

Drone

Physical attack

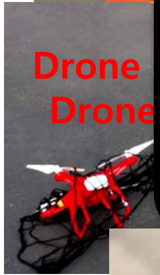
Positioning

Attack Vectors of Drone

Drone

- Comm. channel
- Software hacking
- Physical attack
- Positioning
- Sensing channel

Attack Vectors of Drone



RF jamming or spoofing

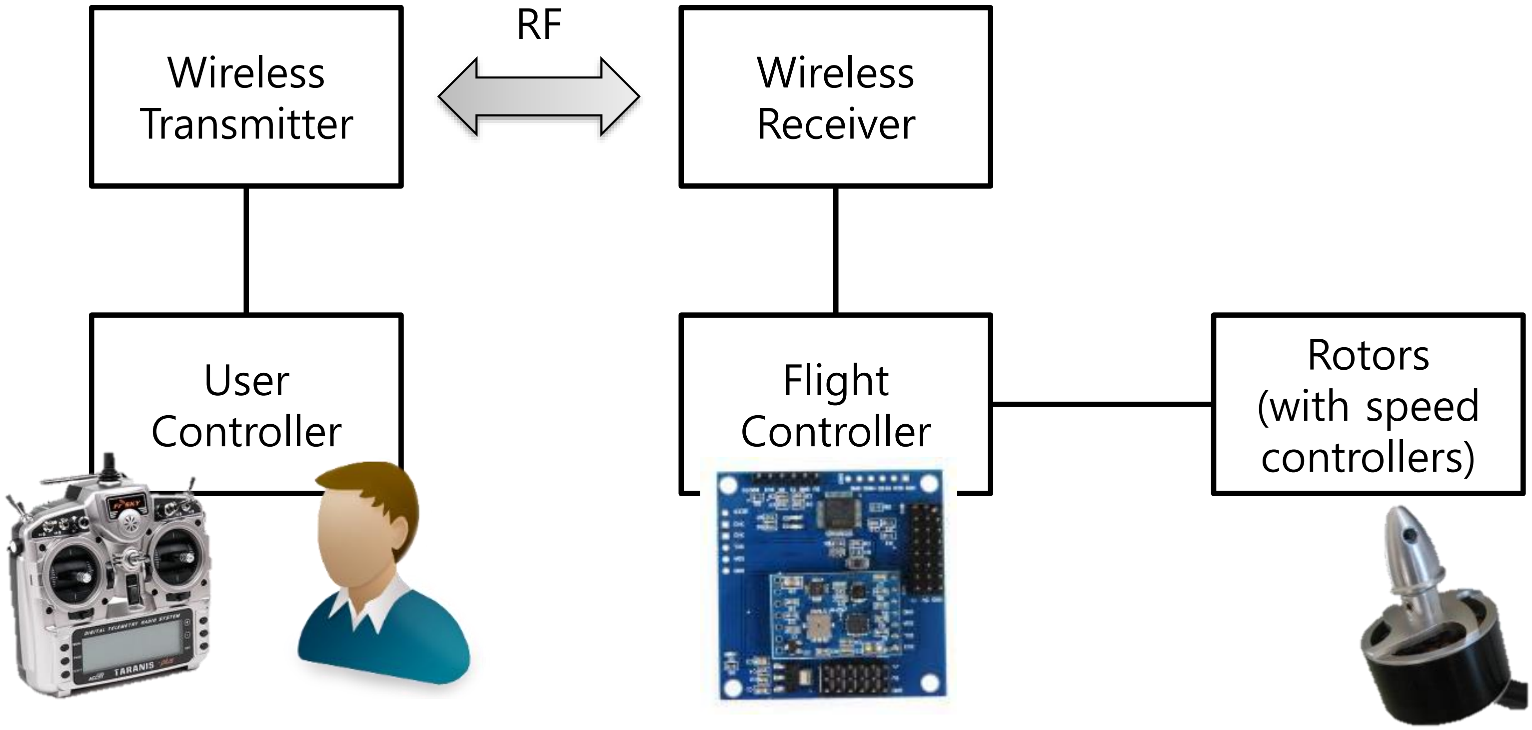
Comm. channel

Software hacking

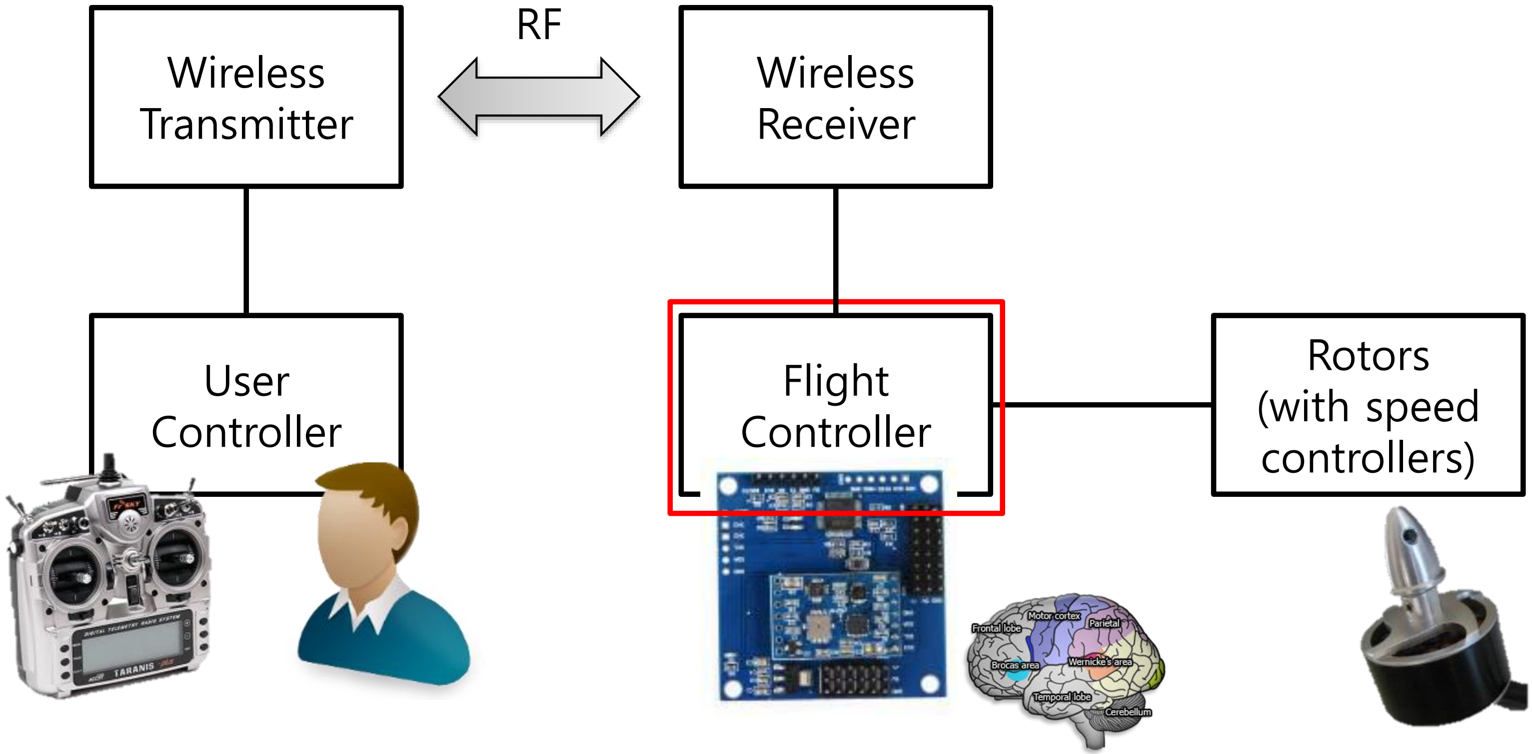
How secure is drone against interference on sensing channel?

Sensing channel

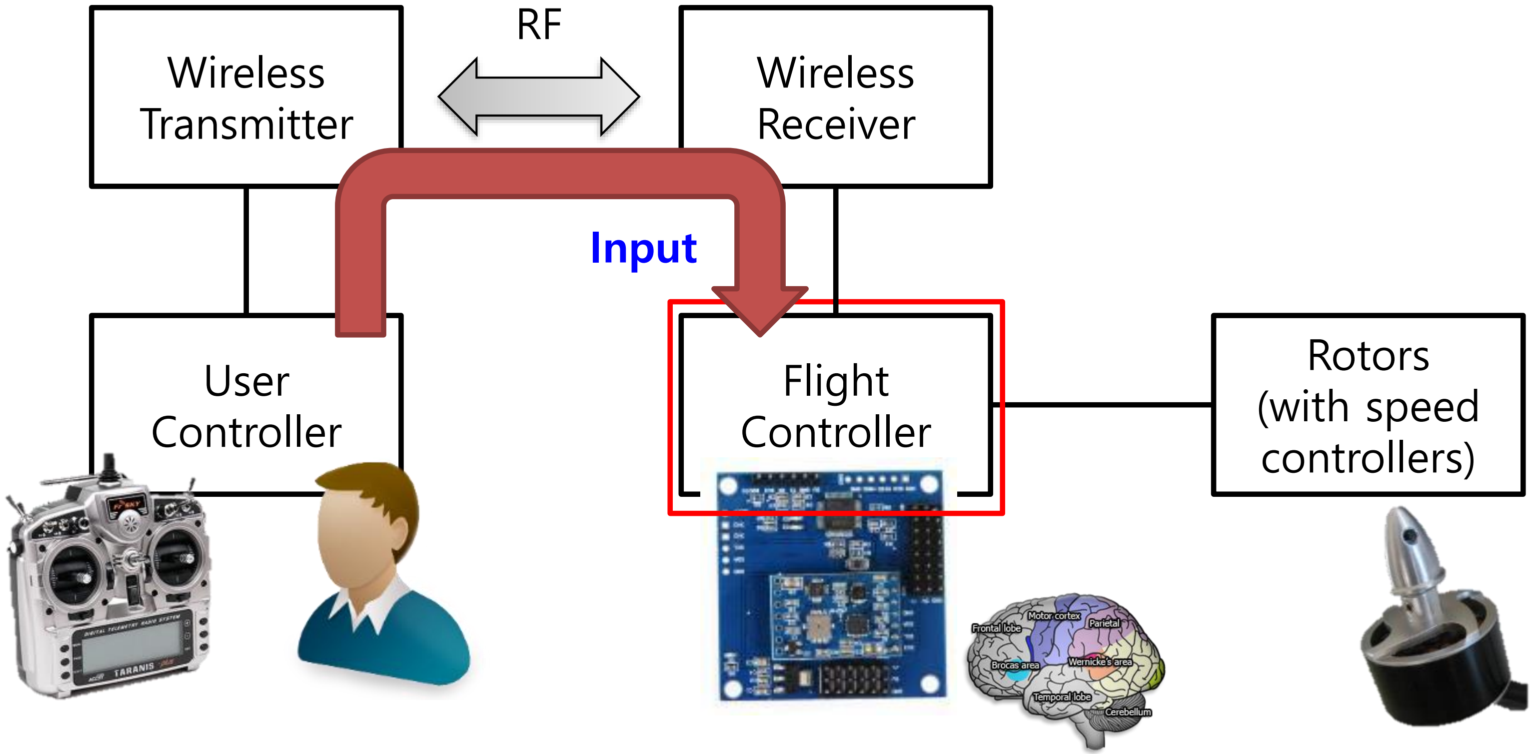
Drone System



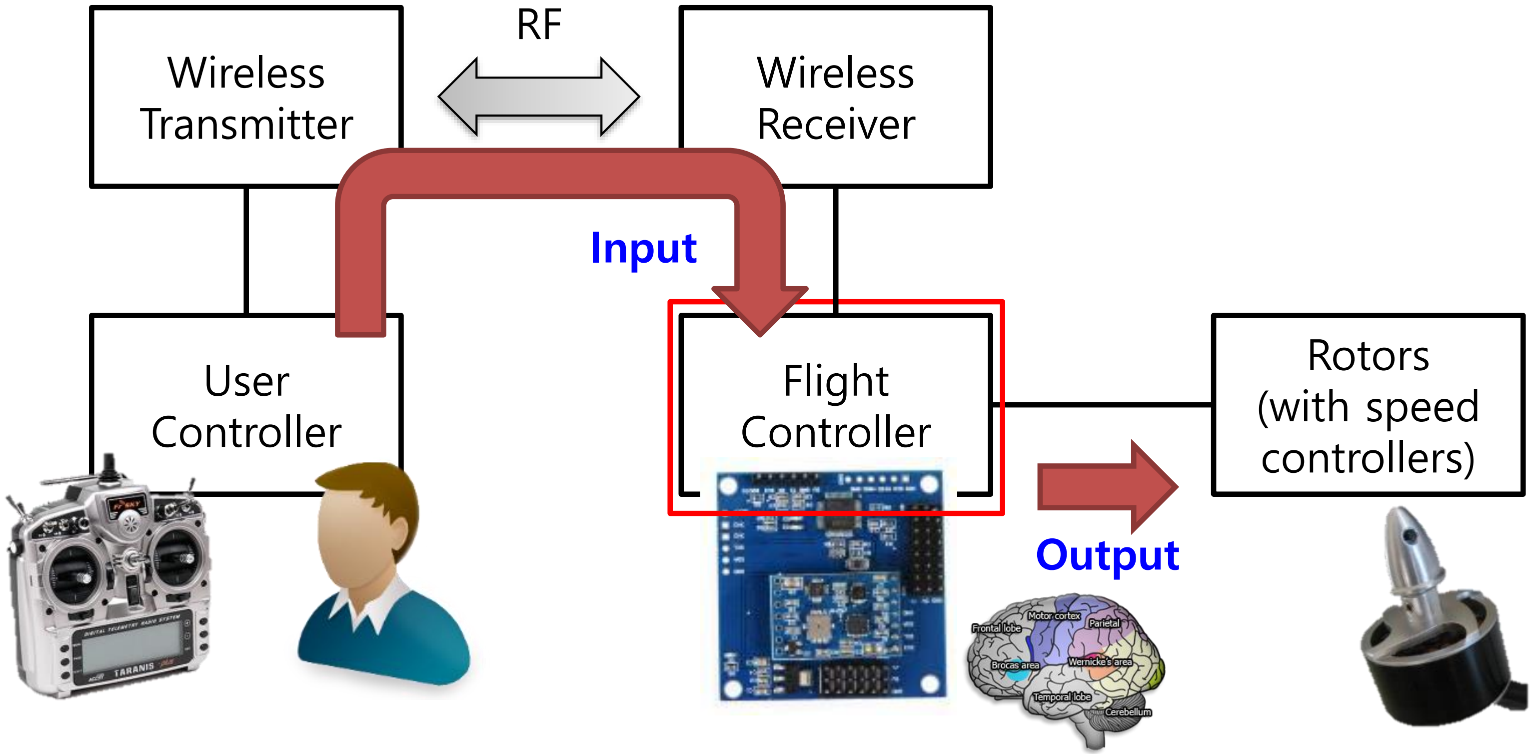
Drone System



Drone System

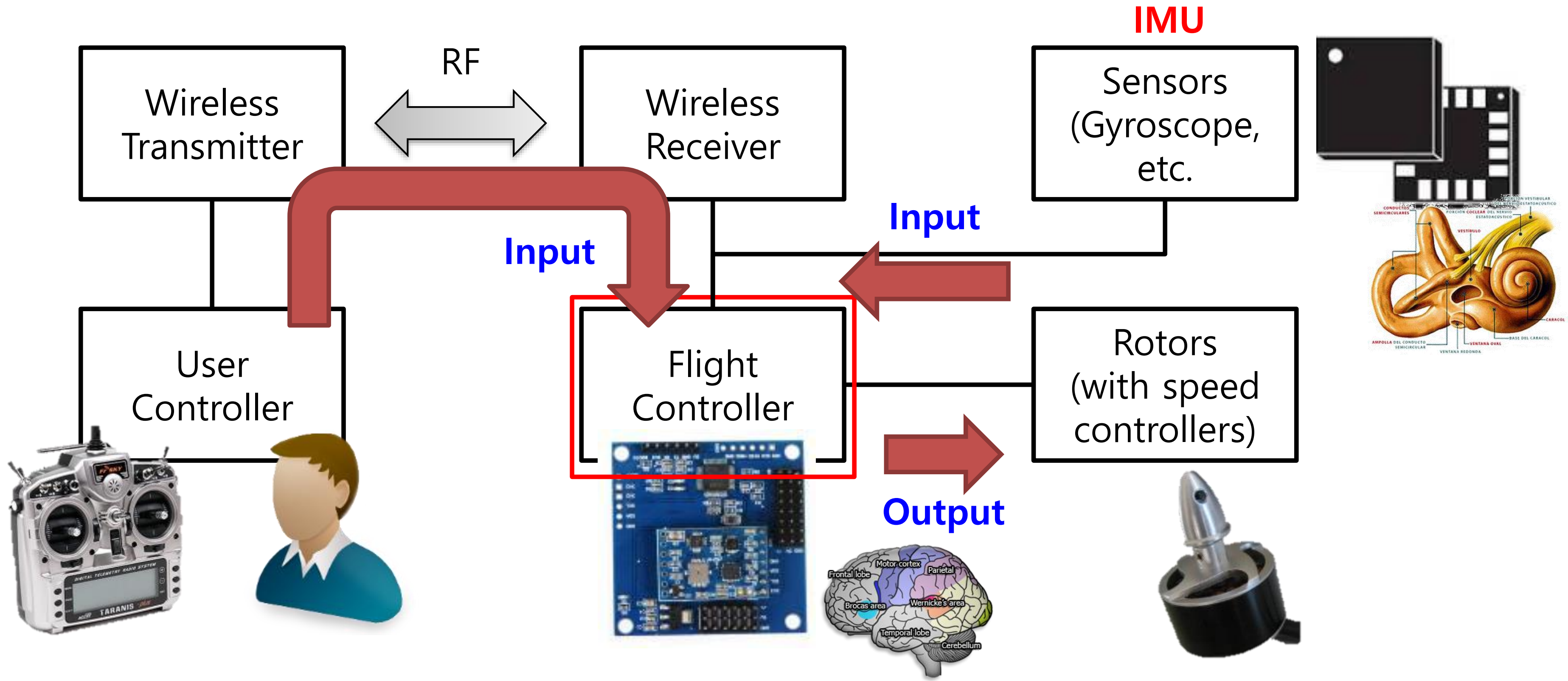


Drone System



Drone System

* IMU: Inertial Measurement Unit



Gyroscope on Drone

* MEMS: Micro-Electro-Mechanical Systems

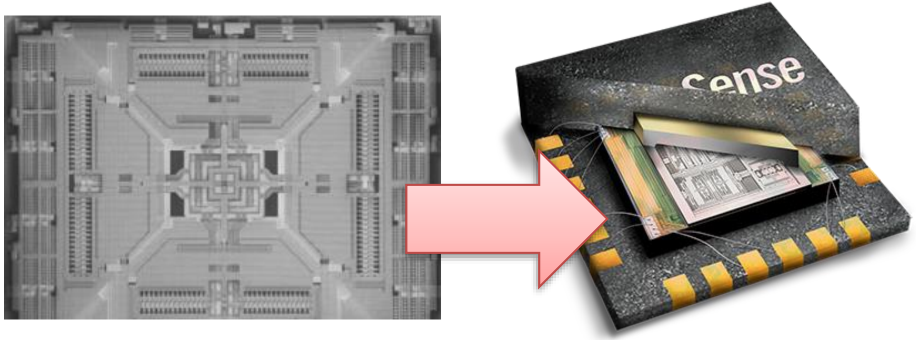
- Inertial Measurement Unit (IMU)
  - A device to measure velocity, orientation, or rotation
  - Using a combination of **MEMS gyroscopes** and accelerometers

Gyroscope on Drone

* MEMS: Micro-Electro-Mechanical Systems

- ❖ Inertial Measurement Unit (IMU)
  - A device to measure velocity, orientation, or rotation
  - Using a combination of **MEMS gyroscopes** and accelerometers

- ❖ MEMS gyroscope

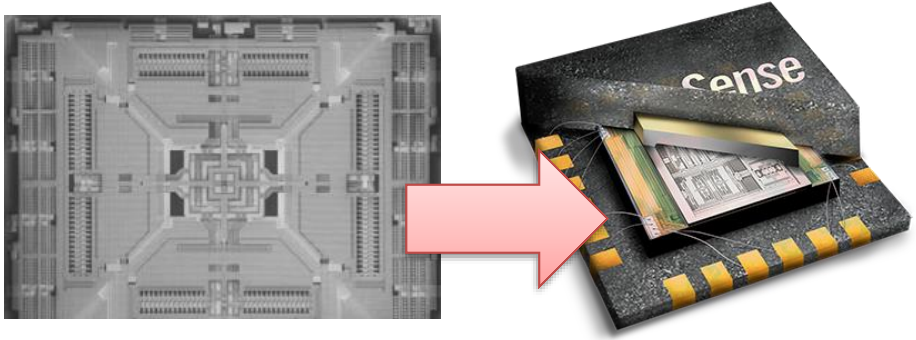


Gyroscope on Drone

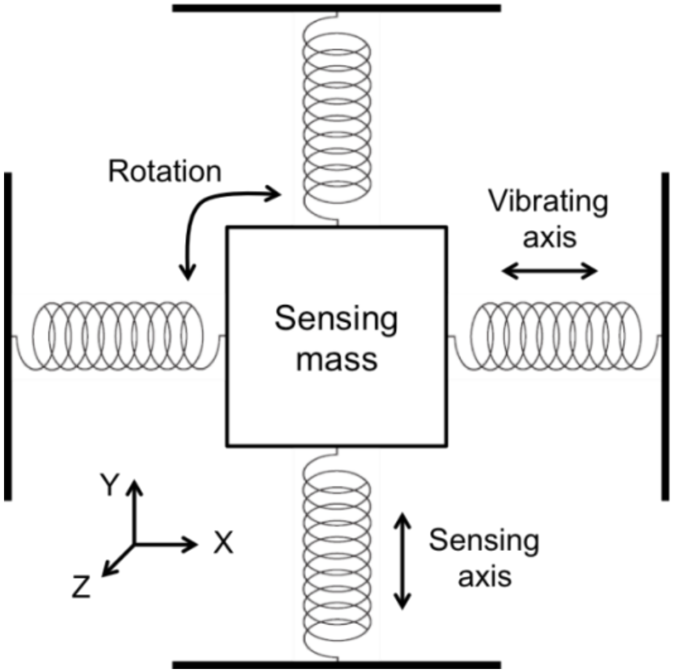
* MEMS: Micro-Electro-Mechanical Systems

- ❖ Inertial Measurement Unit (IMU)
  - A device to measure velocity, orientation, or rotation
  - Using a combination of **MEMS gyroscopes** and accelerometers

- ❖ MEMS gyroscope



<Conceptual structure of MEMS gyro.>



Gyroscope on Drone

* MEMS: Micro-Electro-Mechanical Systems

❖ Inerti

– A

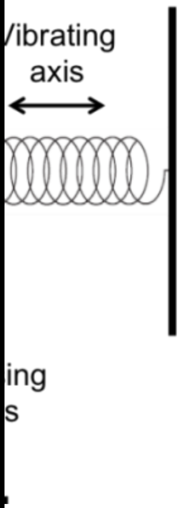
or

– U

gy

❖ MEM

MS gyro.>



(https://www.youtube.com/watch?v=joS6kfjuKQo, https://www.youtube.com/watch?t=45&v=sH7XSX10QkM)

Resonance in MEMS Gyroscope

- ❖ Mechanical resonance by sound noise
  - – Known fact in the MEMS community
  - – Degrades MEMS Gyro's accuracy
  - – With (resonant) frequencies of sound

Resonance in MEMS Gyroscope

- Mechanical resonance by sound noise
  - Known fact in the MEMS community
  - Degrades MEMS Gyro's accuracy
  - With (resonant) frequencies of sound

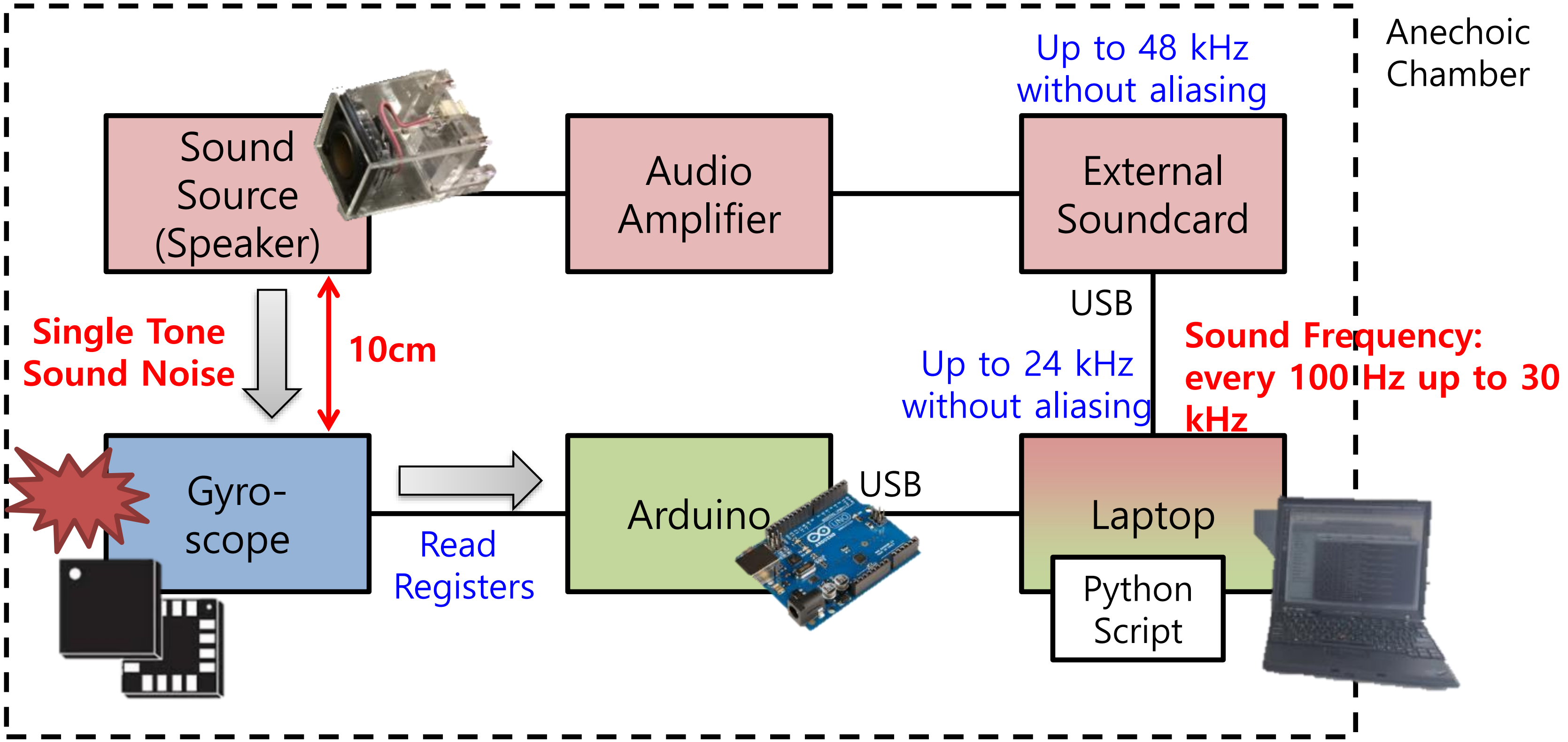
L3GD20

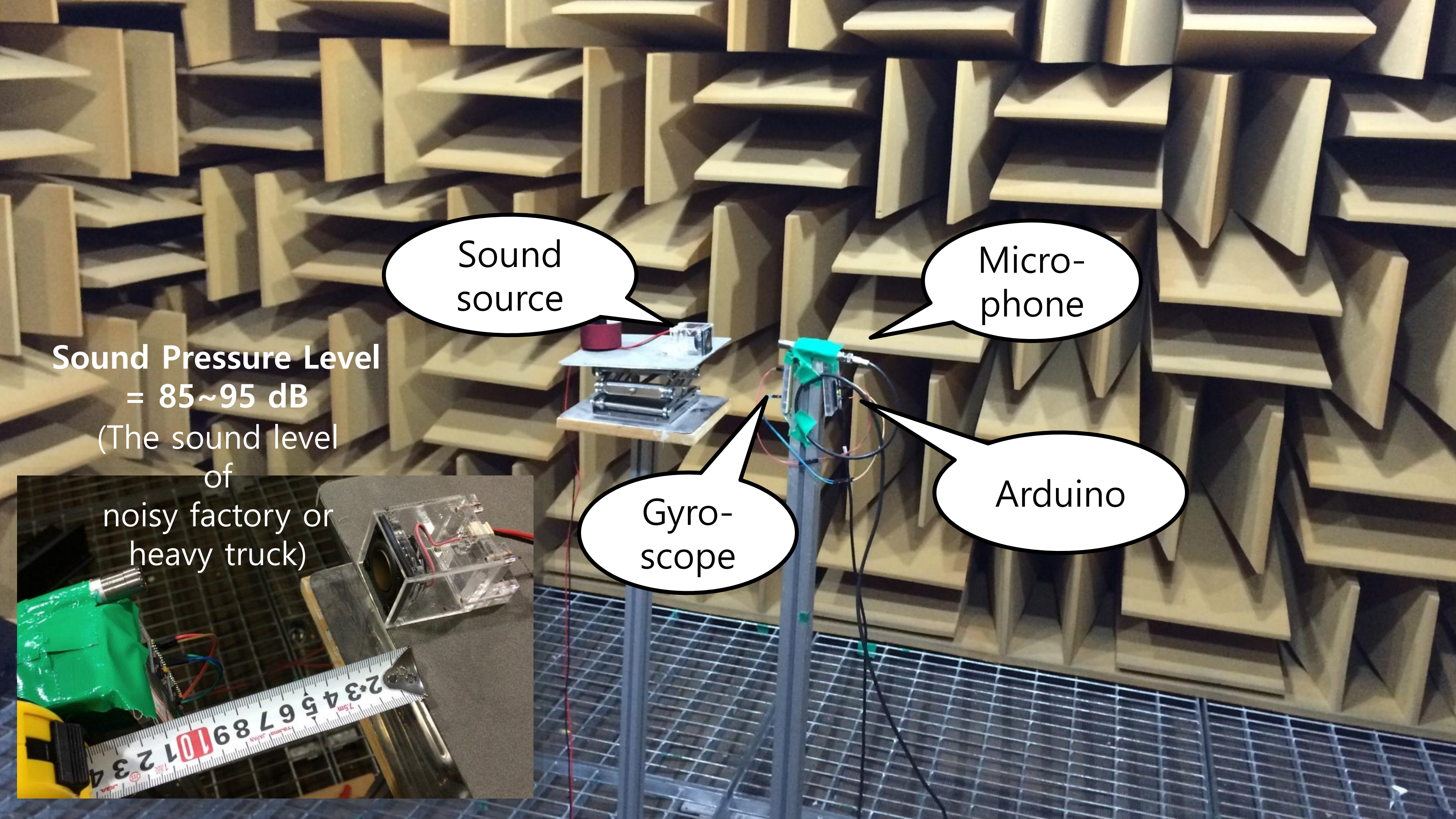
Features

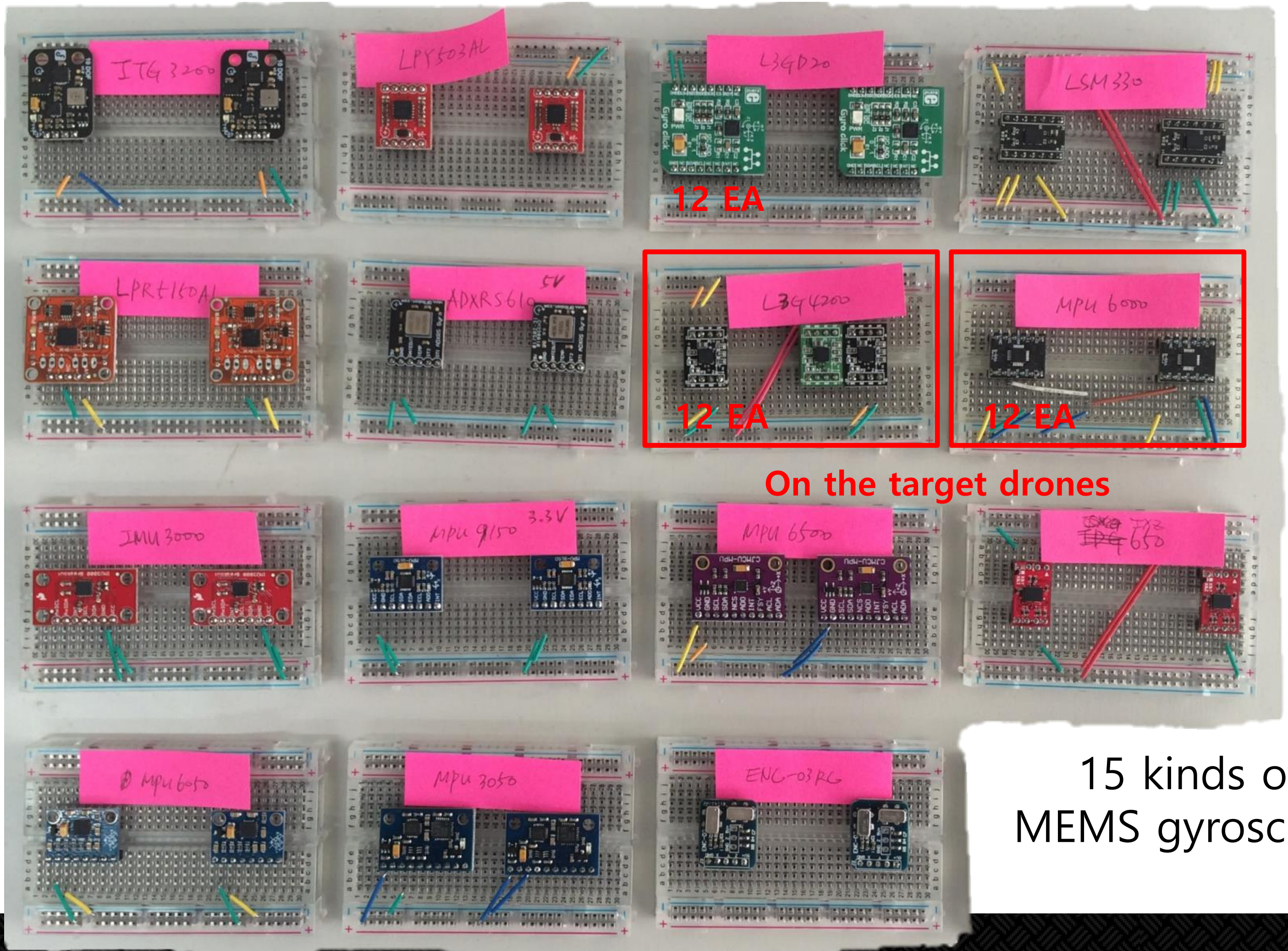
- Three selectable full scales (±250/500/2000 dps)
- 20+ kHz resonant frequency over the audio bandwidth

MEMS Gyro. with a high resonant frequency
to reduce the sound noise effect (above 20kHz)

Experiment Setup




Sound source
Micro-phone
Sound Pressure Level
= 85~95 dB
(The sound level of noisy factory or heavy truck)
Gyro-scope
Arduino



15 kinds of
MEMS gyroscopes

Experimental Results (1/3)

- Found the resonant frequencies of **7 MEMS gyroscopes**
- Not found for 8 MEMS gyroscopes

Sensor	Vender	Supporting Axis	Resonant freq. in the datasheet (axis)	Resonant freq. in our experiment (axis)
L3G4200D	STMicro.	X, Y, Z	No detailed information	**7,900 ~ 8,300 Hz (X, Y, Z)**
L3GD20	STMicro.	X, Y, Z		19,700 ~ 20,400Hz (X, Y, Z)
LSM330	STMicro.	X, Y, Z		19,900 ~ 20,000 Hz (X, Y, Z)
MPU6000	InvenSense	X, Y, Z	30 ~ 36 kHz (X) 27 ~ 33 kHz (Y) 24 ~ 30 kHz (Z)	**26,200 ~ 27,400 Hz (Z)**
MPU6050	InvenSense	X, Y, Z		25,800 ~ 27,700 Hz (Z)
MPU9150	InvenSense	X, Y, Z		27,400 ~ 28,600 Hz (Z)
MPU6500	InvenSense	X, Y, Z	25 ~ 29 kHz (X, Y, Z)	26,500 ~ 27,900 Hz (X, Y, Z)

Experimental Results (1/3)

- Found the resonant frequencies of **7 MEMS gyroscopes**
- Not found for 8 MEMS gyroscopes

Sensor	Vender	Supporting Axis	Resonant freq. in the datasheet (axis)	Resonant freq. in our experiment (axis)
L3G4200D	STMicro.	X, Y, Z	No detailed information	**7,900 ~ 8,300 Hz (X, Y, Z)**
L3GD20	STMicro.	X, Y, Z		19,700 ~ 20,400Hz (X, Y, Z)
LSM330	STMicro.	X, Y, Z		19,900 ~ 20,000 Hz (X, Y, Z)
MPU6000	InvenSense	X, Y, Z	30 ~ 36 kHz (X) 27 ~ 33 kHz (Y) 24 ~ 30 kHz (Z)	**26,200 ~ 27,400 Hz (Z)**
MPU6050	InvenSense	X, Y, Z		25,800 ~ 27,700 Hz (Z)
MPU9150	InvenSense	X, Y, Z		27,400 ~ 28,600 Hz (Z)
MPU6500	InvenSense	X, Y, Z	25 ~ 29 kHz (X, Y, Z)	26,500 ~ 27,900 Hz (X, Y, Z)

Experimental Results (1/3)

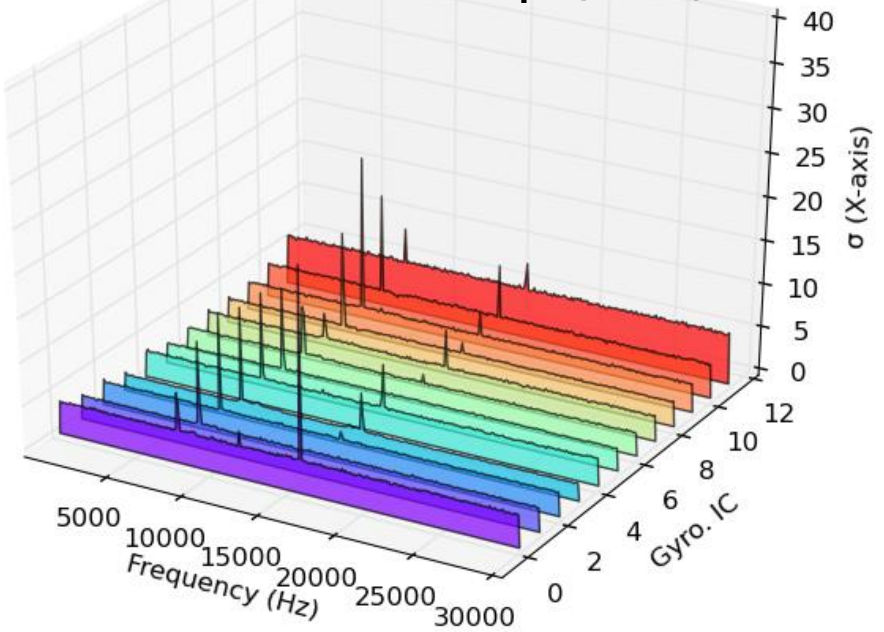
- Found the resonant frequencies of **7 MEMS gyroscopes**
- Not found for 8 MEMS gyroscopes

Sensor	Vender	Supporting Axis	Resonant freq. in the datasheet (axis)	Resonant freq. in our experiment (axis)
L3G4200D	STMicro.	X, Y, Z	No detailed information	**7,900 ~ 8,300 Hz (X, Y, Z)**
L3GD20	STMicro.	X, Y, Z		19,700 ~ 20,400Hz (X, Y, Z)
LSM330	STMicro.	X, Y, Z		19,900 ~ 20,000 Hz (X, Y, Z)
MPU6000	InvenSense	X, Y, Z	30 ~ 36 kHz (X) 27 ~ 33 kHz (Y) 24 ~ 30 kHz (Z)	**26,200 ~ 27,400 Hz (Z)**
MPU6050	InvenSense	X, Y, Z		25,800 ~ 27,700 Hz (Z)
MPU9150	InvenSense	X, Y, Z		27,400 ~ 28,600 Hz (Z)
MPU6500	InvenSense	X, Y, Z	25 ~ 29 kHz (X, Y, Z)	26,500 ~ 27,900 Hz (X, Y, Z)

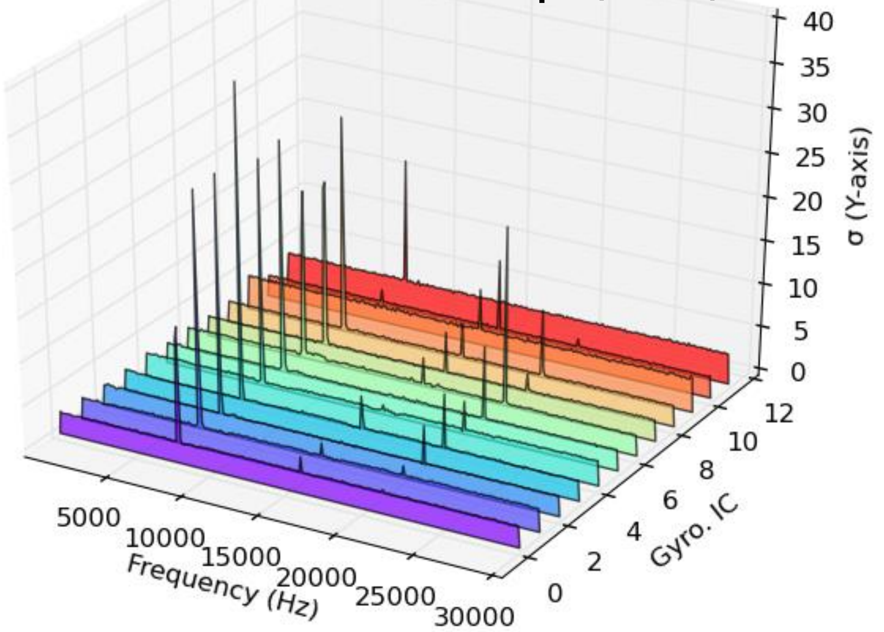
Experimental Results (2/3)

❖ Unexpected output by sound noise (for L3G4200D)

Standard deviation of raw data samples for 12 L3G4200D chips (X-axis)

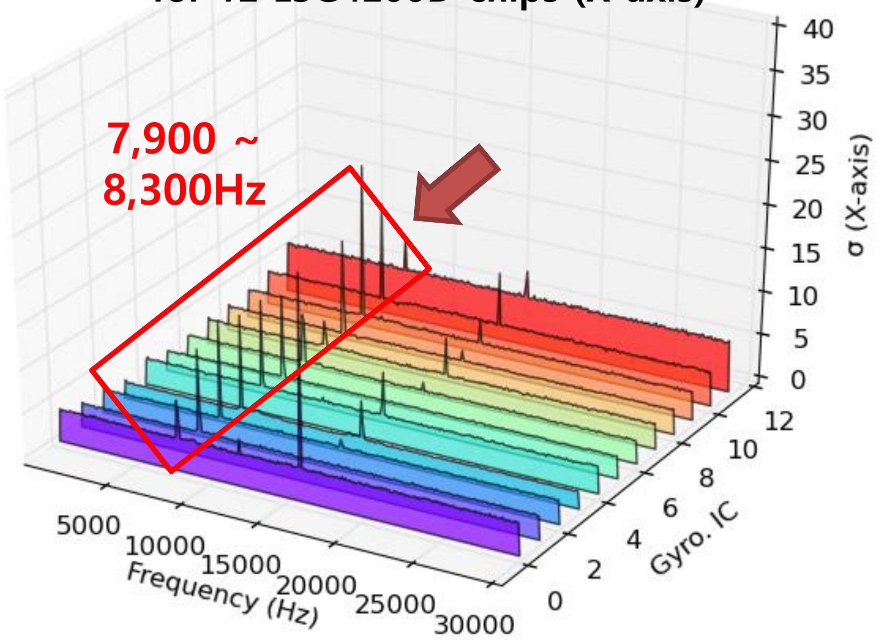


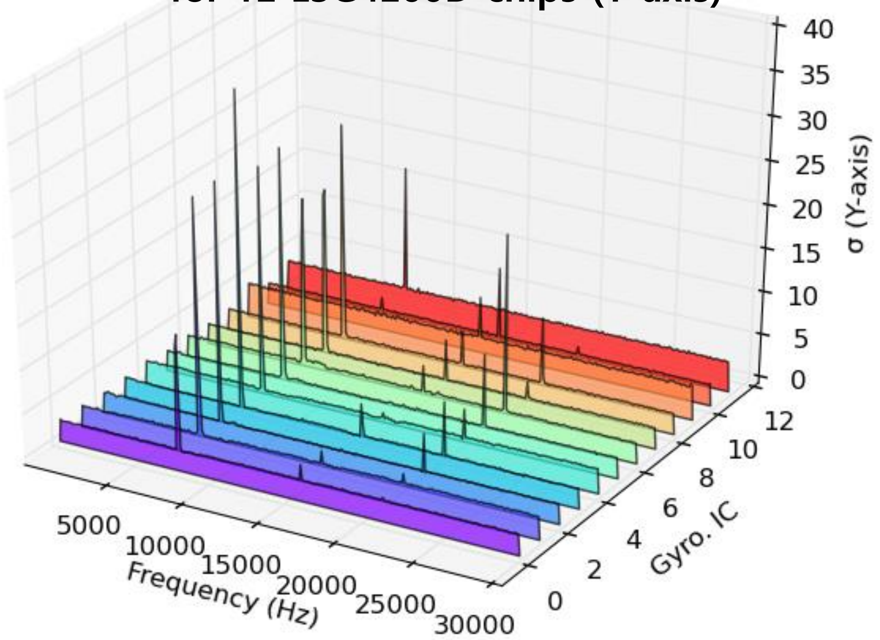
Standard deviation of raw data samples for 12 L3G4200D chips (Y-axis)



Experimental Results (2/3)

❖ Unexpected output by sound noise (for L3G4200D)

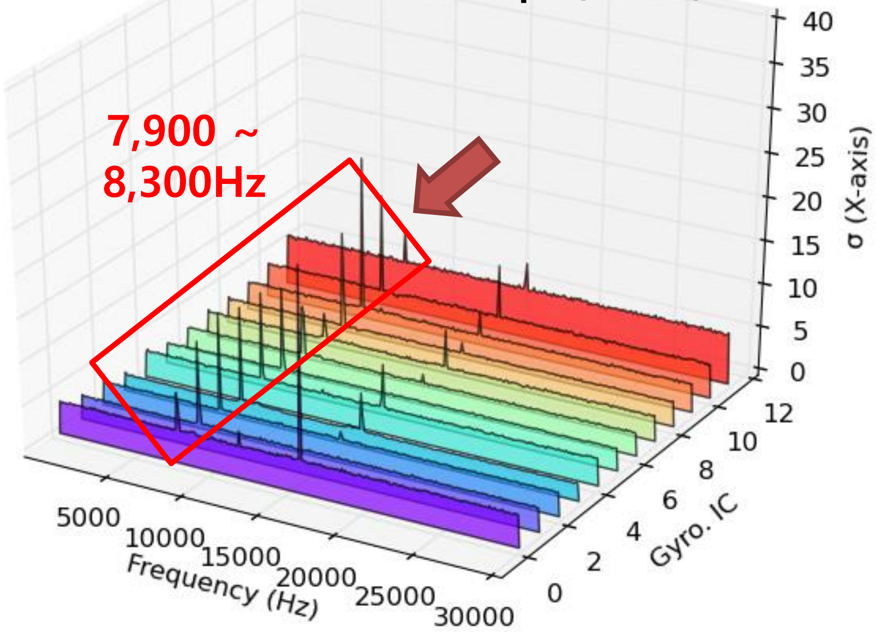




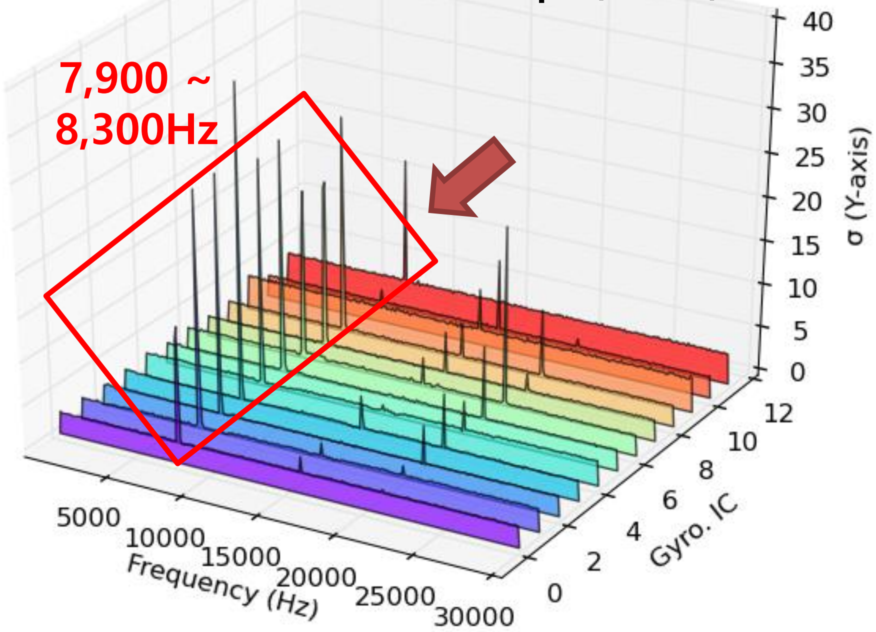
Experimental Results (2/3)

❖ Unexpected output by sound noise (for L3G4200D)

Standard deviation of raw data samples for 12 L3G4200D chips (X-axis)



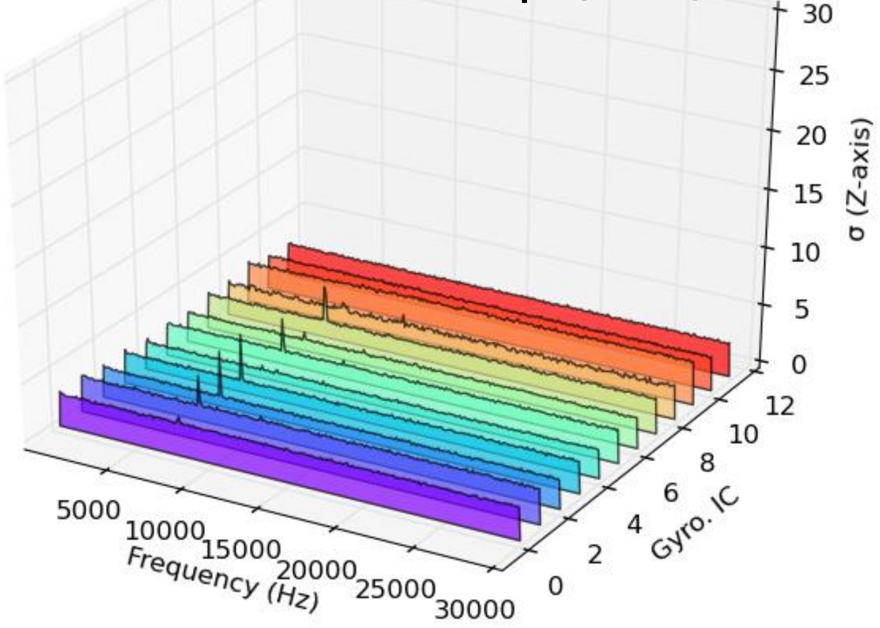
Standard deviation of raw data samples for 12 L3G4200D chips (Y-axis)



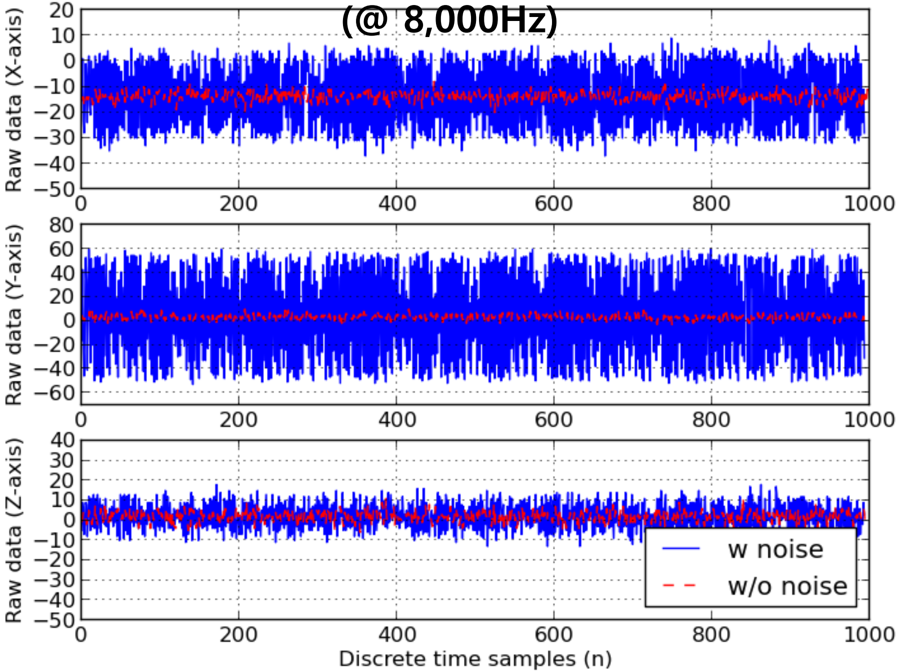
Experimental Results (3/3)

❖ Unexpected output by sound noise (for L3G4200D)

Standard deviation of raw data samples for 12 L3G4200D chips (Z-axis)



Raw data samples of one L3G4200D chip (@ 8,000Hz)

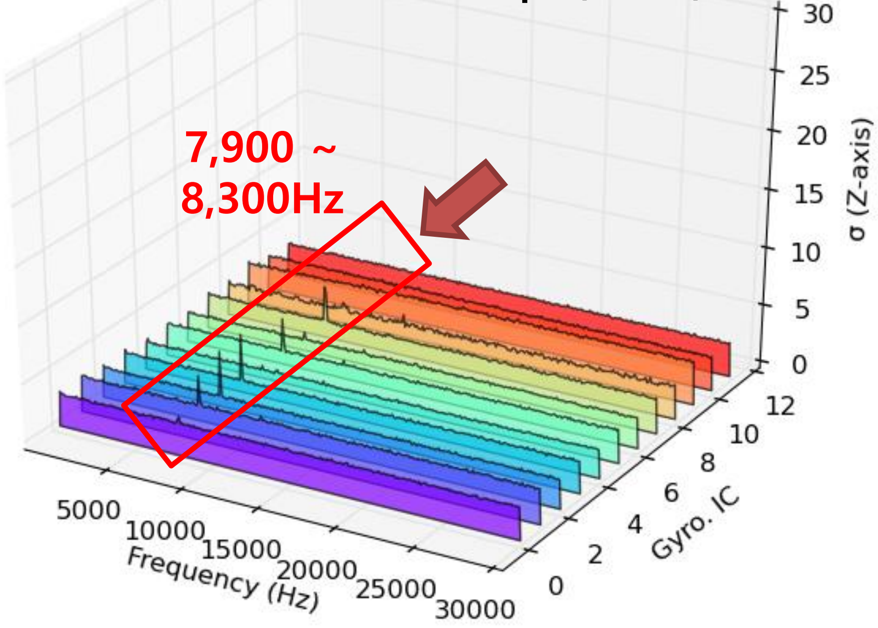


SysSec
System Security Lab

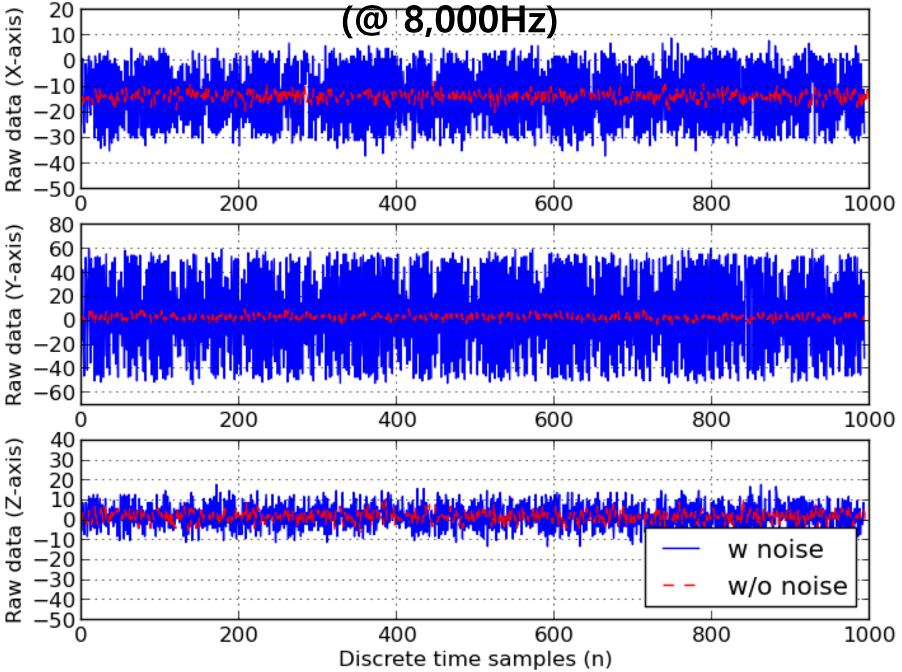
Experimental Results (3/3)

❖ Unexpected output by sound noise (for L3G4200D)

Standard deviation of raw data samples for 12 L3G4200D chips (Z-axis)



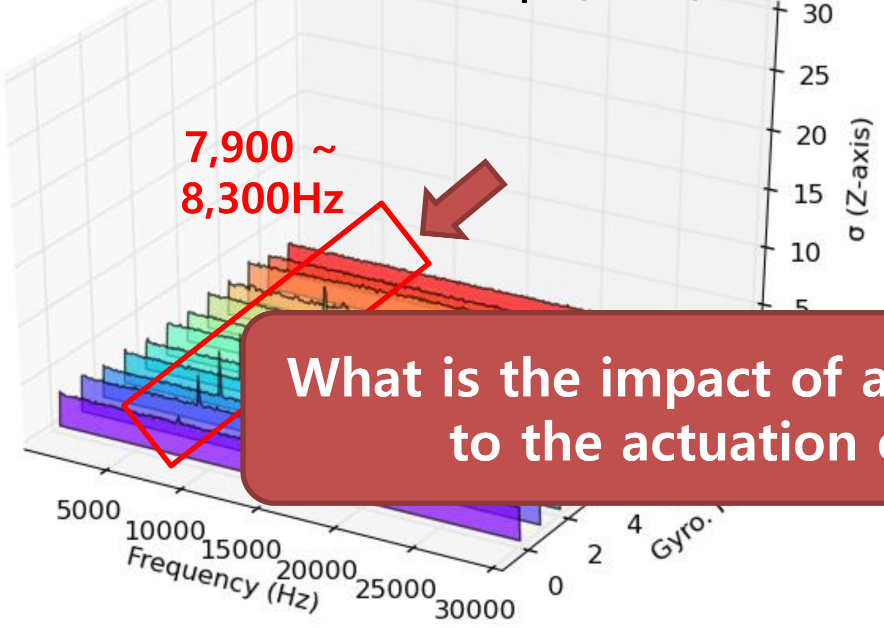
Raw data samples of one L3G4200D chip (@ 8,000Hz)



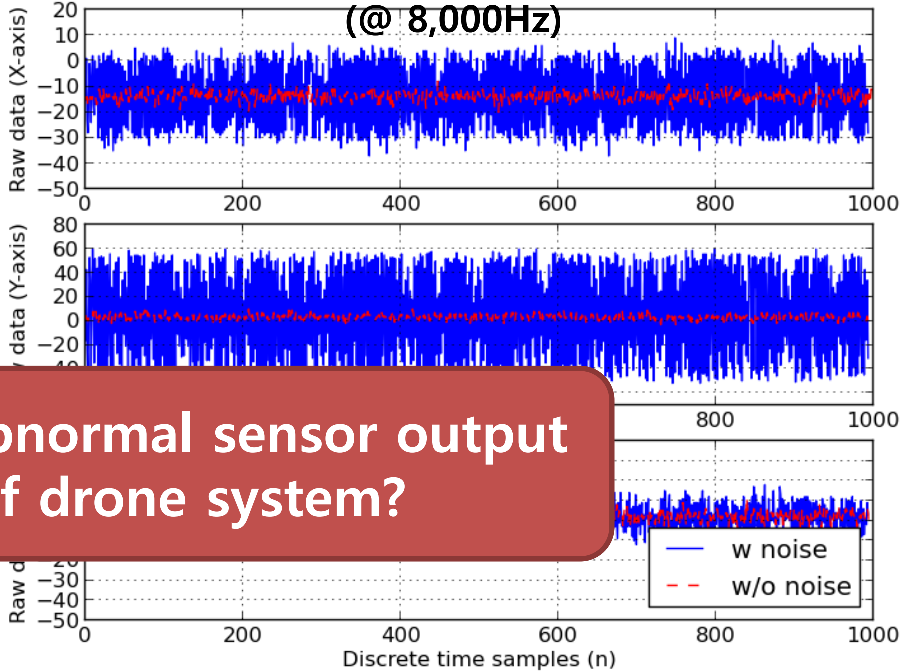
Experimental Results (3/3)

❖ Unexpected output by sound noise (for L3G4200D)

Standard deviation of raw data samples for 12 L3G4200D chips (Z-axis)



Raw data samples of one L3G4200D chip (@ 8,000Hz)



What is the impact of abnormal sensor output to the actuation of drone system?

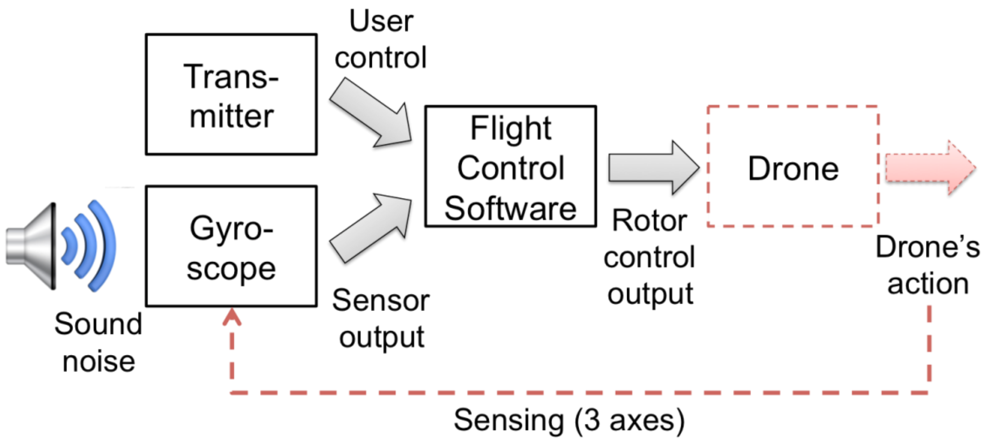
Software Analysis

- Two open-source firmware programs
  - Multiwii project
  - ArduPilot project

Software Analysis

- Two open-source firmware programs
  - Multiwii project
  - ArduPilot project

- Rotor control algorithm

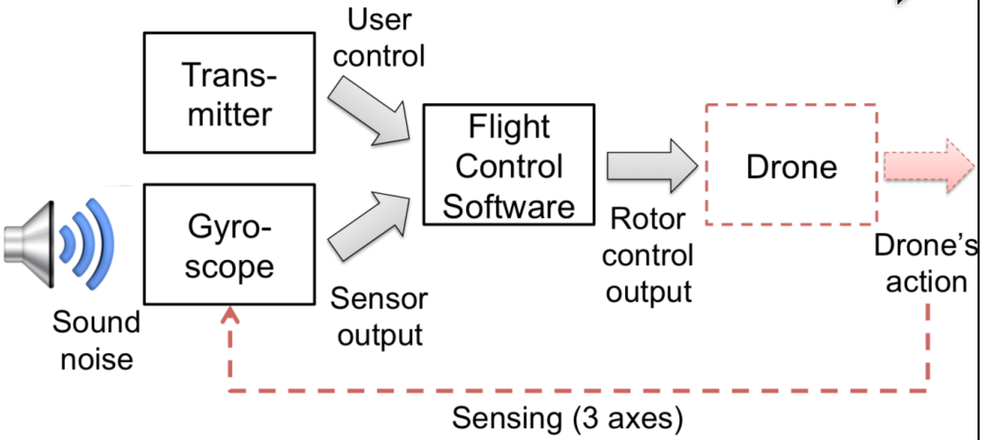


Software Analysis

- Two open-source firmware programs
  - Multiwii project
  - ArduPilot project

Proportional-Integral -Derivative control

- Rotor control algorithm



for *axis* **do**

$P = txCtrl[axis] - gyro[axis] \times G_P[axis];$

$error = txCtrl[axis]/G_P[axis] - gyro[axis];$

$error_{accumulated} = error_{accumulated} + error;$

$I = error_{accumulated} \times G_I[axis];$

$delta = gyro[axis] - gyro_{last}[axis];$

$delta_{sum}$ = sum of the last three delta values;

$D = delta_{sum} \times G_D[axis];$

$PIDCtrl[axis] = P + I - D;$

end

for *rotor* **do**

for *axis* **do**

$rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis];$

end

limit $rotorCtrl[rotor]$ within the pre-defined MIN (1,150) and MAX (1,850) values;

end

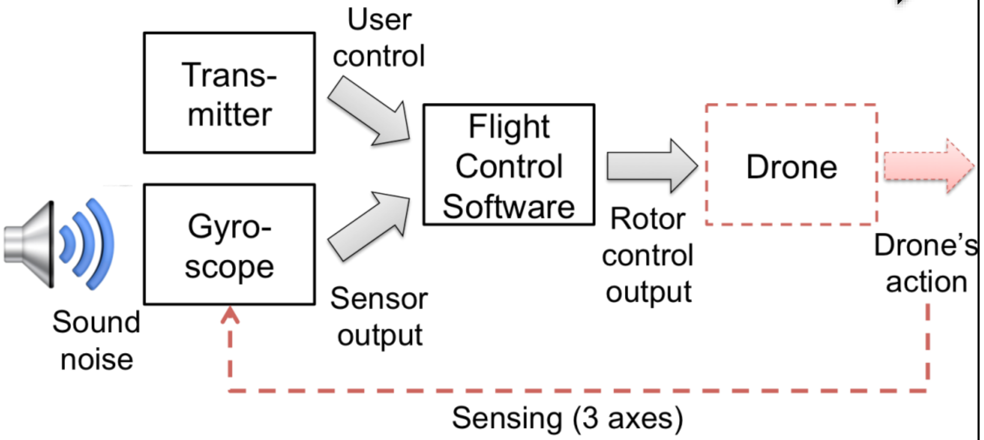
actuate rotors;

Software Analysis

- ❖ Two open-source firmware programs
  - – Multiwii project
  - – ArduPilot project

Proportional-Integral -Derivative control

- ❖ Rotor control algorithm



for *axis* **do**

$P = txCtrl[axis] - gyro[axis] \times G_P[axis]$;

$error = txCtrl[axis]/G_P[axis] - gyro[axis]$;

$error_{accumulated} = error_{accumulated} + error$;

$I = error_{accumulated} \times G_I[axis]$;

$delta = gyro[axis] - gyro_{last}[axis]$;

$delta_{sum}$ = sum of the last three delta values;

$D = delta_{sum} \times G_D[axis]$;

$PIDCtrl[axis] = P + I - D$;

end

for *rotor* **do**

for *axis* **do**

$rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis]$;

end

limit $rotorCtrl[rotor]$ within the pre-defined MIN (1,150) and MAX (1,850) values;

end

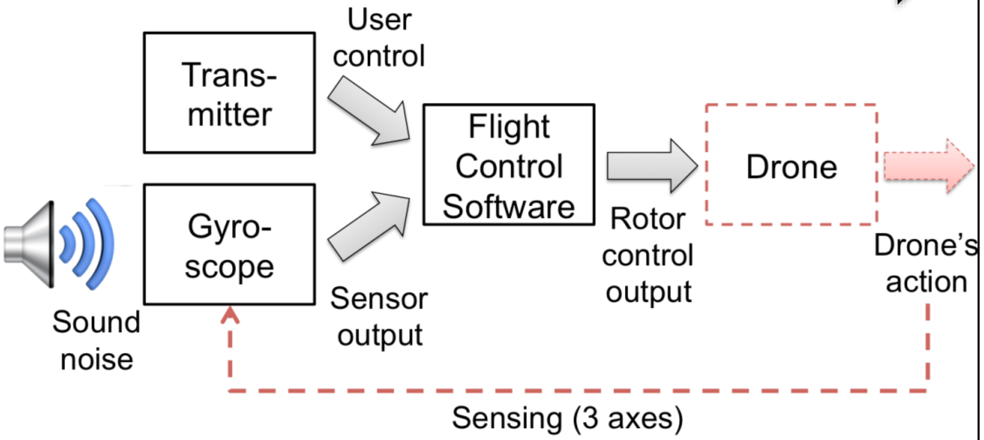
actuate rotors;

Software Analysis

- ❖ Two open-source firmware programs
  - Multiwii project
  - ArduPilot project

Proportional-Integral
-Derivative control

- ❖ Rotor control algorithm



for *axis* **do**

$P = txCtrl[axis] - gyro[axis] \times G_P[axis]$;

$error = txCtrl[axis] / G_P[axis] - gyro[axis]$;

$error_{accumulated} = error_{accumulated} + error$;

$I = error_{accumulated} \times G_I[axis]$;

$delta = gyro[axis] - gyro_{last}[axis]$;

$delta_{sum}$ = sum of the last three delta values;

$D = delta_{sum} \times G_D[axis]$;

$PIDCtrl[axis] = P + I - D$;

end

for *rotor* **do**

for *axis* **do**

$rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis]$;

end

limit $rotorCtrl[rotor]$ within the pre-defined MIN (1,150) and MAX (1,850) values;

end

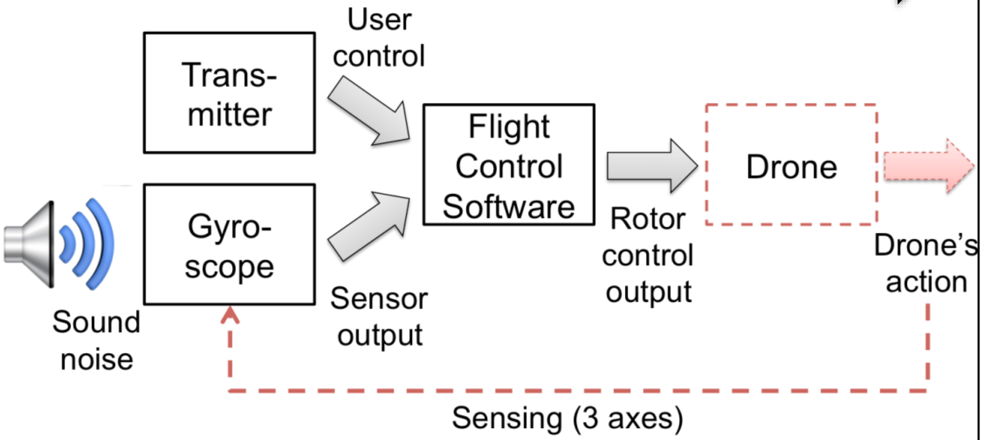
actuate rotors;

Software Analysis

- ❖ Two open-source firmware programs
  - Multiwii project
  - ArduPilot project

Proportional-Integral -Derivative control

- ❖ Rotor control algorithm



for *axis* **do**

$P = txCtrl[axis] - gyro[axis] \times G_P[axis];$

$error = txCtrl[axis]/G_P[axis] - gyro[axis];$

$error_{accumulated} = error_{accumulated} + error;$

$I = error_{accumulated} \times G_I[axis];$

$delta = gyro[axis] - gyro_{last}[axis];$

$delta_{sum}$ = sum of the last three delta values;

$D = delta_{sum} \times G_D[axis];$

$PIDCtrl[axis] = P + I - D;$

end

for *rotor* **do**

for *axis* **do**

$rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis];$

end

limit $rotorCtrl[rotor]$ within the pre-defined MIN (1,150) and MAX (1,850) values;

end

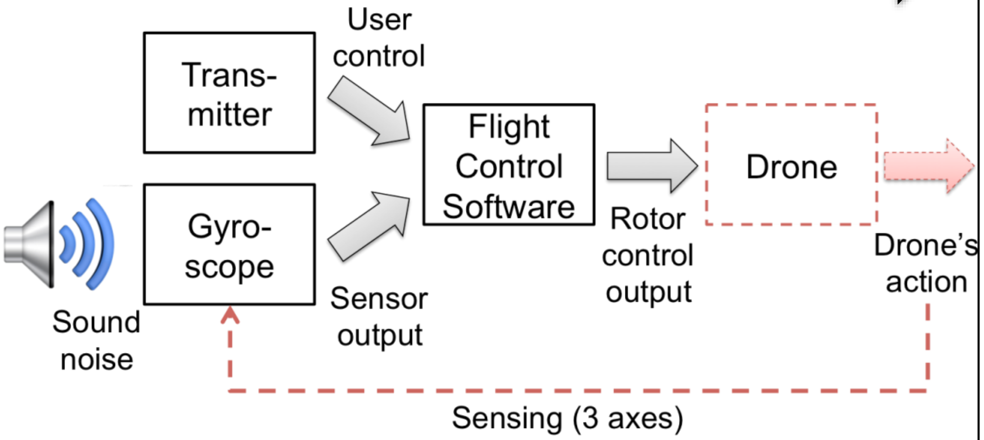
actuate rotors;

Software Analysis

- Two open-source firmware programs
  - Multiwii project
  - ArduPilot project

Proportional-Integral -Derivative control

- Rotor control algorithm



for *axis* **do**

$P = txCtrl[axis] - gyro[axis] \times G_P[axis];$

$error = txCtrl[axis]/G_P[axis] - gyro[axis];$

$error_{accumulated} = error_{accumulated} + error;$

$I = error_{accumulated} \times G_I[axis];$

$delta = gyro[axis] - gyro_{last}[axis];$

$delta_{sum}$ = sum of the last three delta values;

$D = delta_{sum} \times G_D[axis];$

$PIDCtrl[axis] = P + I - D;$

end

for *rotor* **do**

for *axis* **do**

$rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis];$

end

limit $rotorCtrl[rotor]$ within the pre-defined MIN (1,150) and MAX (1,850) values;

end

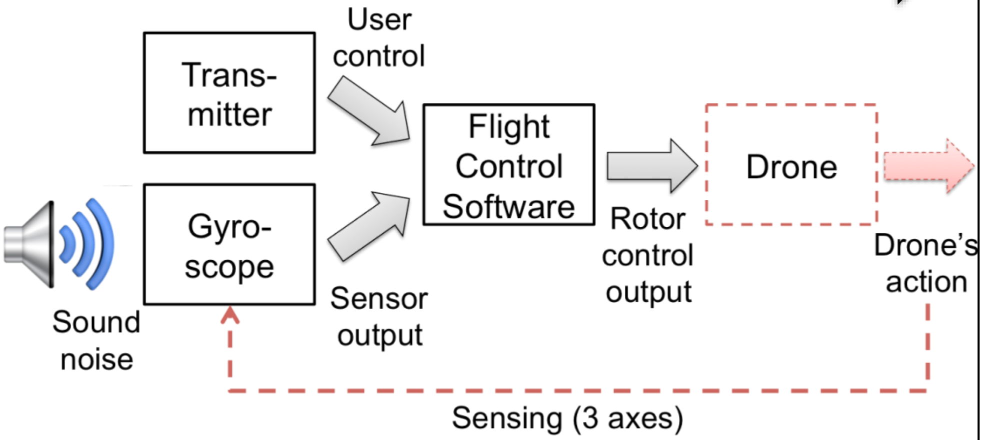
actuate rotors;

Software Analysis

- ❖ Two open-source firmware programs
  - – Multiwii project
  - – ArduPilot project

Proportional-Integral
-Derivative control

- ❖ Rotor control algorithm



for *axis* **do**
- $P = txCtrl[axis] - gyro[axis] \times G_P[axis]$;
- $error = txCtrl[axis]/G_P[axis] - gyro[axis]$;
- $error_{accumulated} = error_{accumulated} + error$;
- $I = error_{accumulated} \times G_I[axis]$;
- $delta = gyro[axis] - gyro_{last}[axis]$;
- $delta_{sum}$ = sum of the last three delta values;
- $D = delta_{sum} \times G_D[axis]$;
- $PIDCtrl[axis] = P + I - D$;

end

for *rotor* **do**
- **for** *axis* **do**
  - $rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis]$;
- **end**
- limit $rotorCtrl[rotor]$ within the pre-defined MIN (1,150) and MAX (1,850) values;

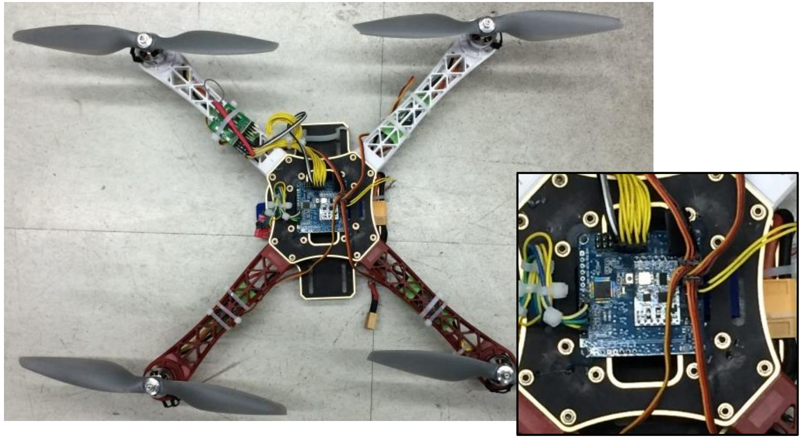
end

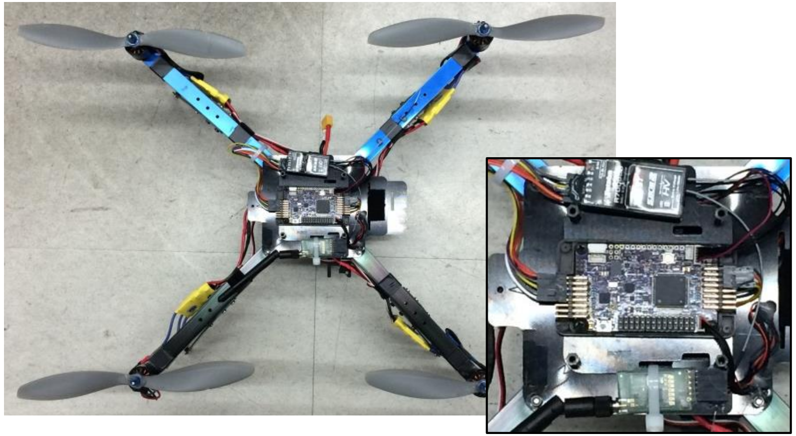
actuate rotors;

Target Drones

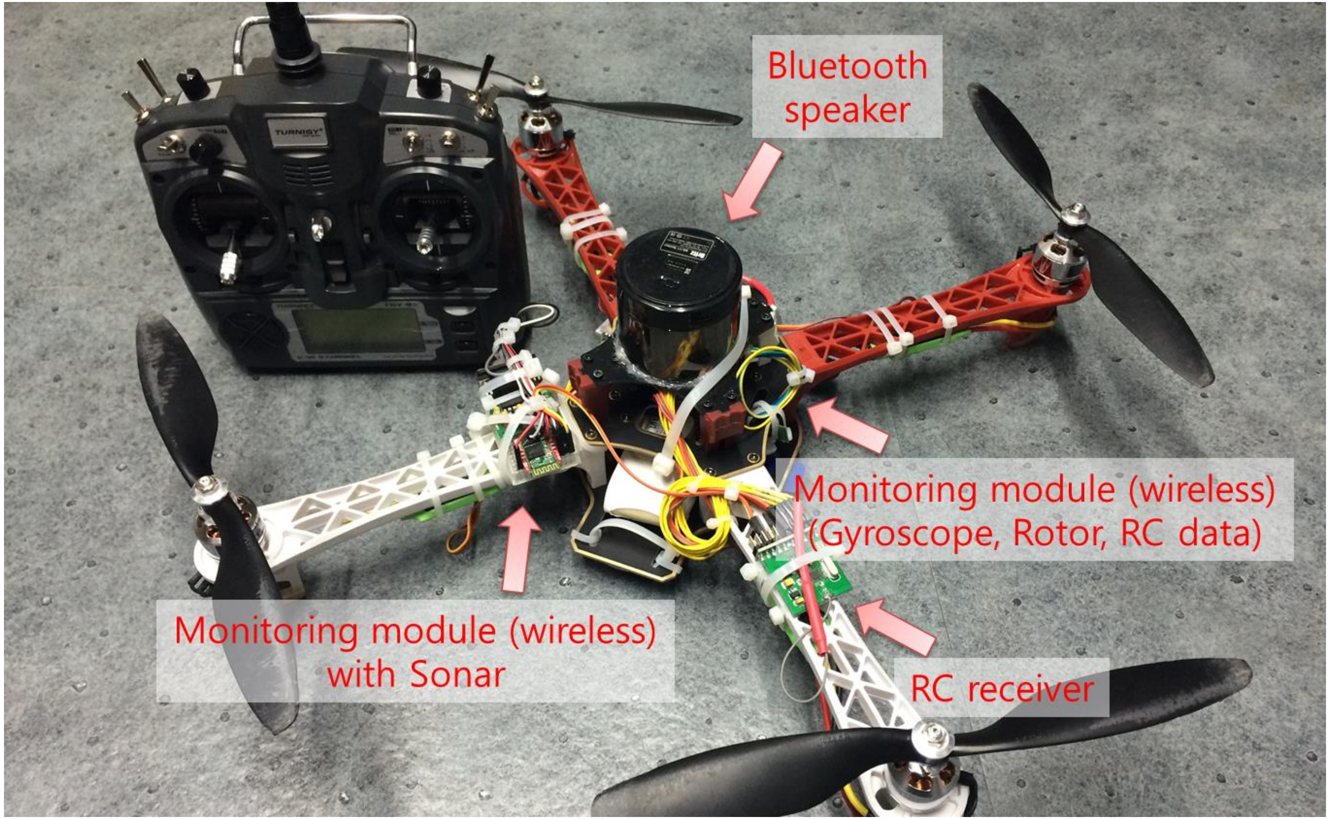
- Target drone A (DIY drone)
  - Gyroscope: L3G4200D
  - Resonant freq.: 8,200 Hz (Audible sound range)
  - Firmware: Multiwii

- Target drone B (DIY drone)
  - Gyroscope: MPU6000
  - Resonant freq.: 26,200 Hz (Ultra sound range)
  - Firmware: ArduPilot

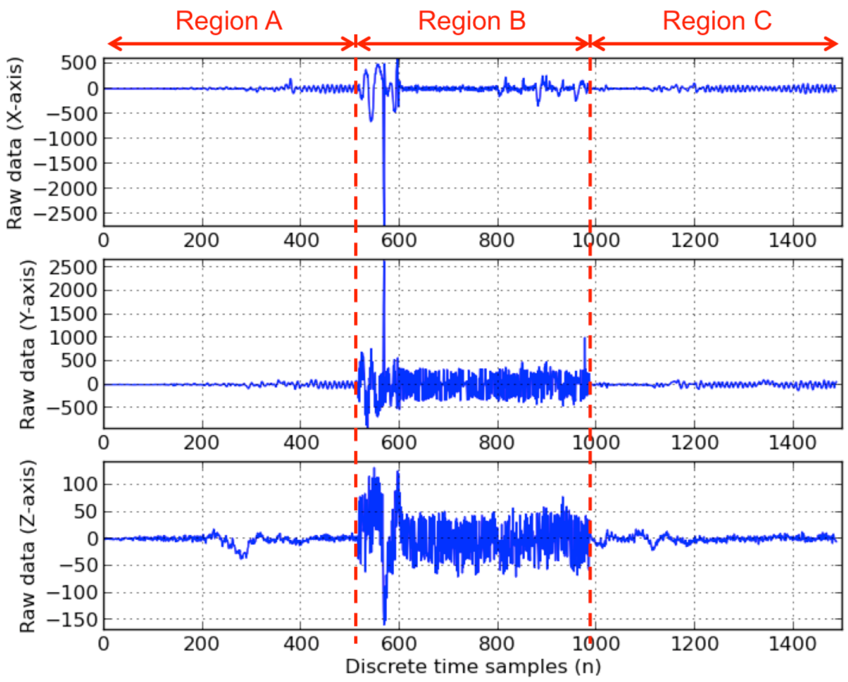




Attack DEMO


Bluetooth speaker
Monitoring module (wireless) (Gyroscope, Rotor, RC data)
Monitoring module (wireless) with Sonar
RC receiver

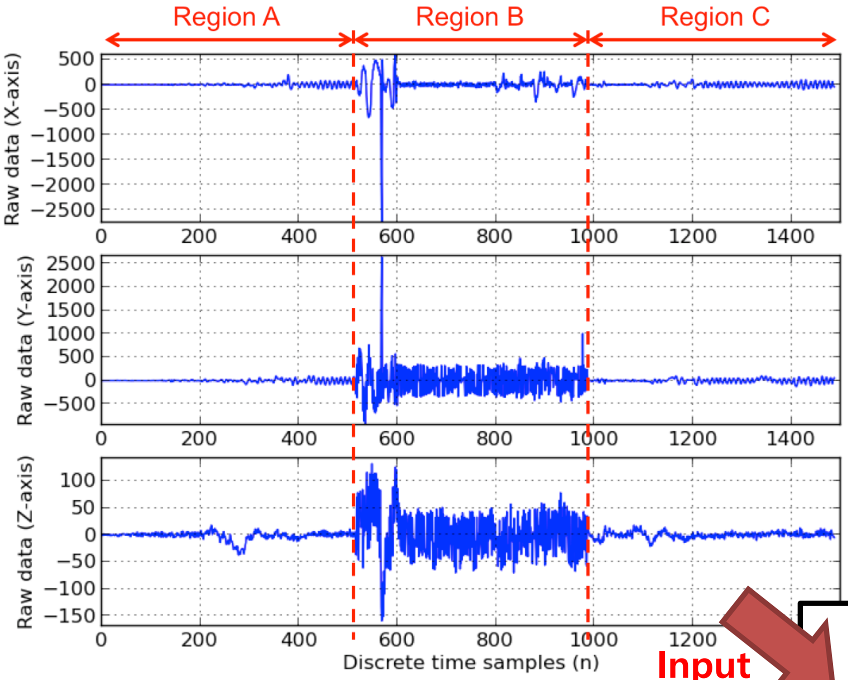
Attack DEMO (Target drone A)



Raw data samples of the gyroscope

SysSec System Security Lab

Attack DEMO (Target drone A)

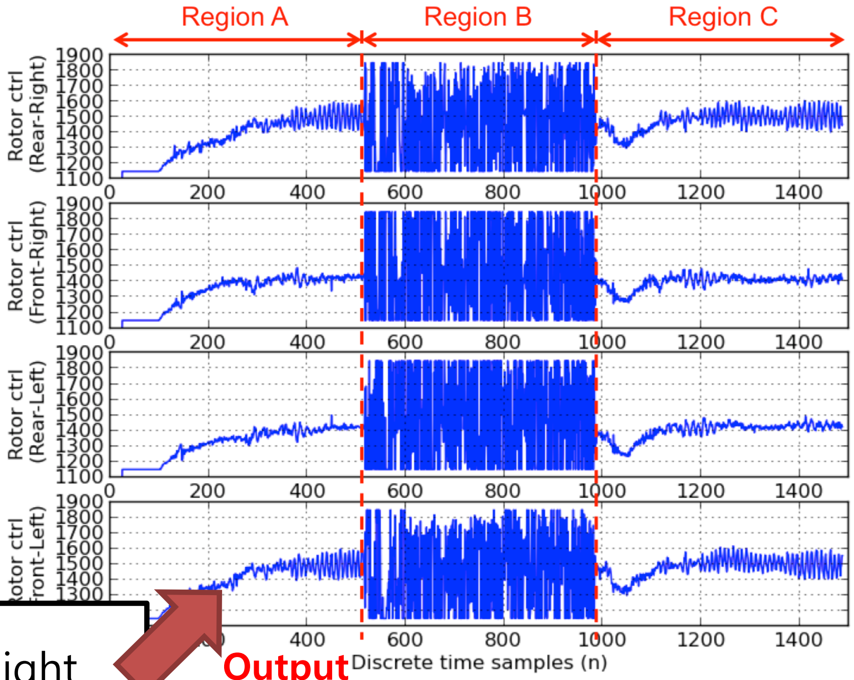


Raw data samples of the gyroscope

Input

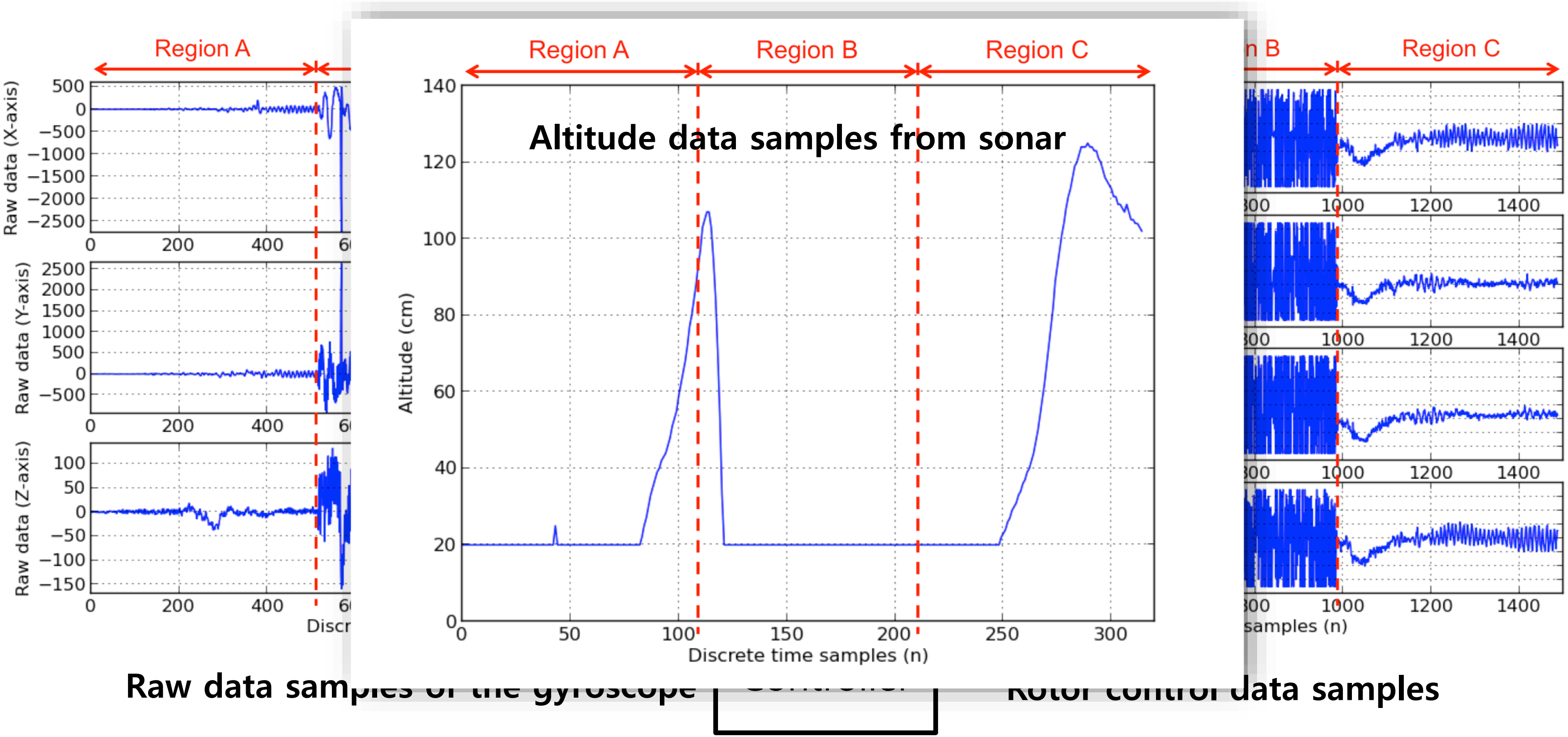
Flight Controller

Output



Rotor control data samples

Attack DEMO (Target drone A)



Attack Results

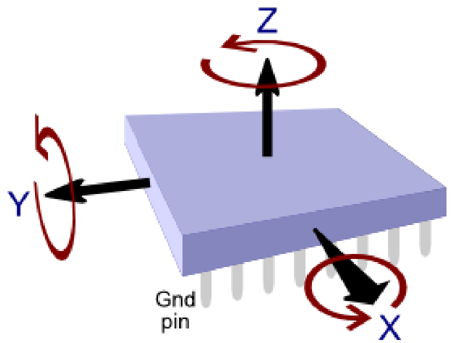
❖ Result of attacking two target drones

	Target Drone A	Target Drone B
Resonant Freq. (Gyro.)	8,200 Hz (L3G4200D)	26,200 Hz (MPU6000)
Affected Axes	X, Y, Z	Z
Attack Result	Fall down	-

Attack Results

❖ Result of attacking two target drones

	Target Drone A	Target Drone B
Resonant Freq. (Gyro.)	8,200 Hz (L3G4200D)	26,200 Hz (MPU6000)
Affected Axes	X, Y, Z	Z
Attack Result	Fall down	-



- X- and Y-axis = vertical rotation (more critical effect on stability)
- Z-axis = horizontal orientation

Attack Distance

- The minimum sound pressure level in our experiments
  - About 108.5 dB SPL (at 10cm)

$$SPL = SPL_{ref} - 20\log\left(\frac{d}{d_{ref}}\right)$$

Attack Distance

- The minimum sound pressure level in our experiments
  - About 108.5 dB SPL (at 10cm)

$$SPL = SPL_{ref} - 20\log\left(\frac{d}{d_{ref}}\right)$$

- Theoretically, 37.58m using a sound source that can generate 140 dB SPL at 1m

Attack Distance

- The minimum sound pressure level in our experiments
  - About 108.5 dB SPL (at 10cm)

$$SPL = SPL_{ref} - 20\log\left(\frac{d}{d_{ref}}\right)$$

- Theoretically, 37.58m using a sound source that can generate 140 dB SPL at 1m

<450XL of LRAD Corporation>

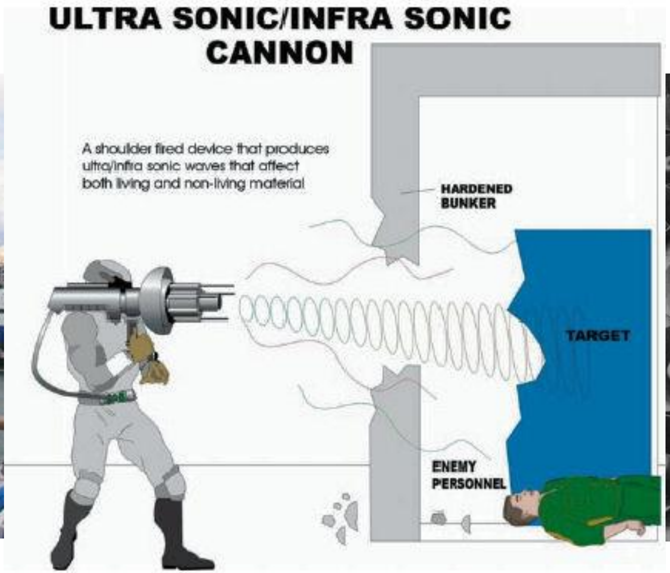
ACOUSTIC PERFORMANCE

Maximum Continuous Output	146dB SPL @ 1 meter, A-weighted
Sound Projection	+/- 15° at 1 kHz/-3dB
Communications Range	Highly intelligible voice messages over

(http://www.lradx.com/wp-content/uploads/2015/05/LRAD_Datasheet_450XL.pdf)

Attack Scenarios

- ❖ Drone to Drone Attack
- ❖ Sonic Weapons
- ❖ Sonic Wall/Zone



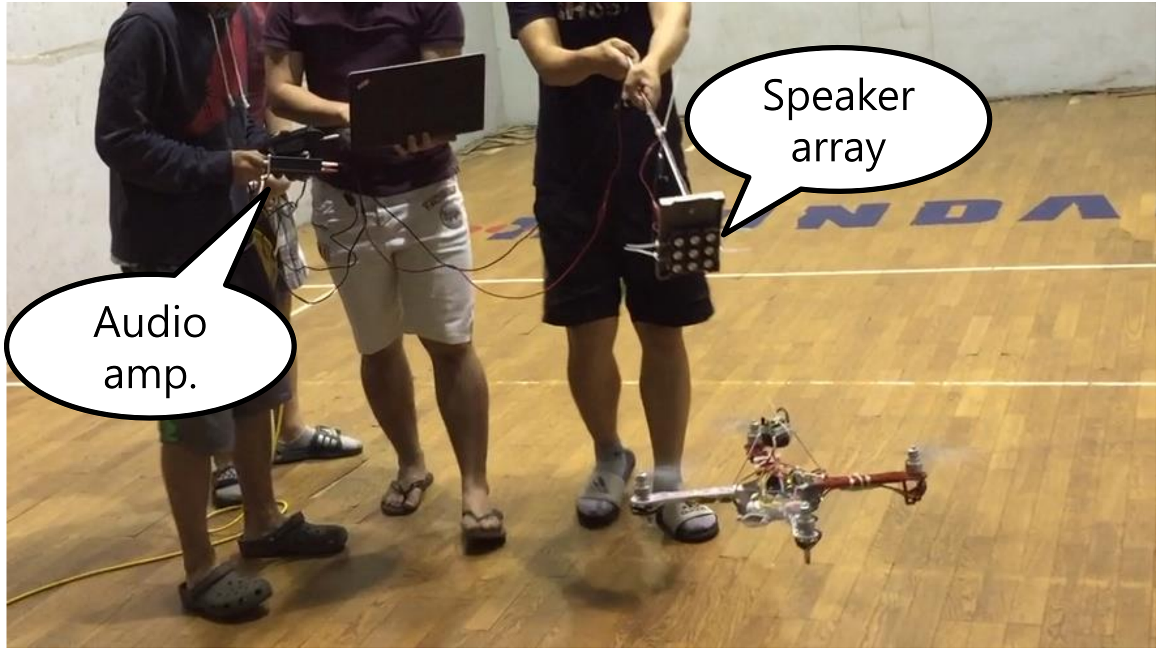
SysSec
System Security Lab

Limitations (1/2)

❖ Aiming at a 3- dimensional moving object

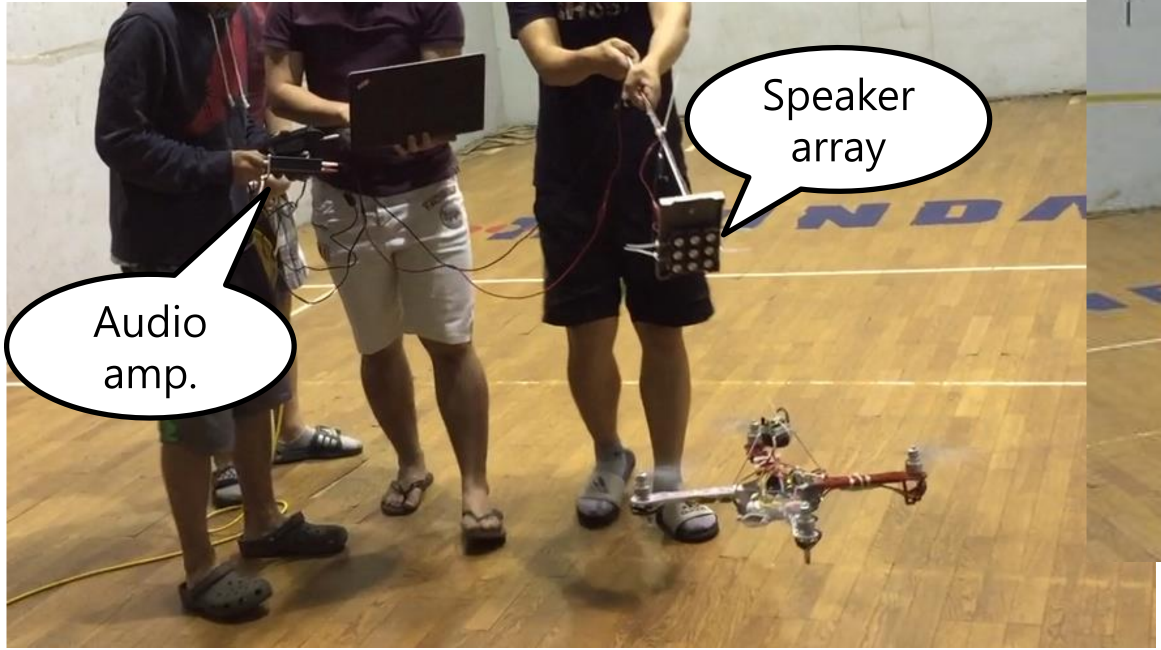
Limitations (1/2)

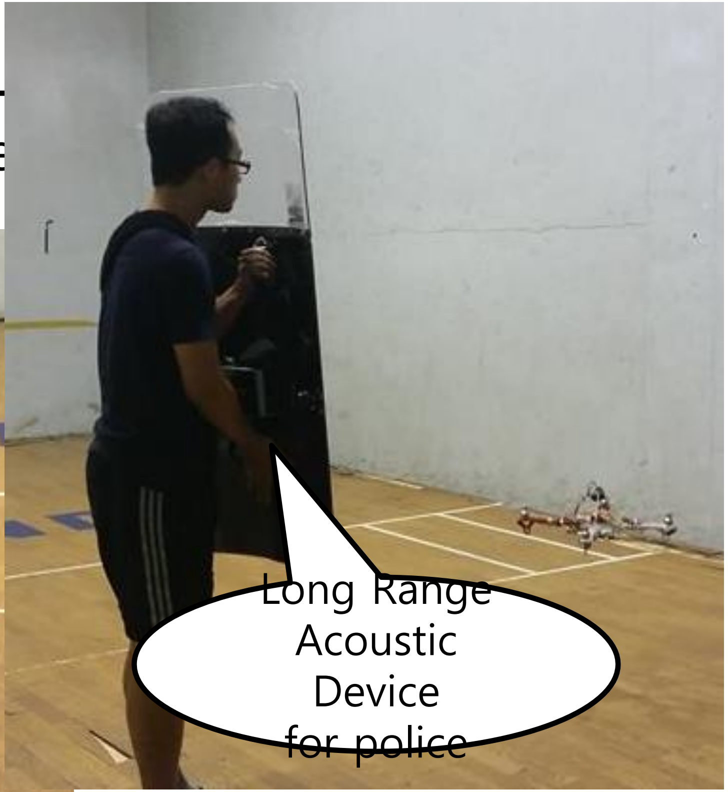
❖ Aiming at a 3- dimensional moving object



Limitations (1/2)

❖ Aiming at a 3- dimensional moving obje





Limitations (2/2)

❖ No accumulated effect or damage

Simple sonic wall
(3m-by-2m, 25 speakers)

Countermeasure

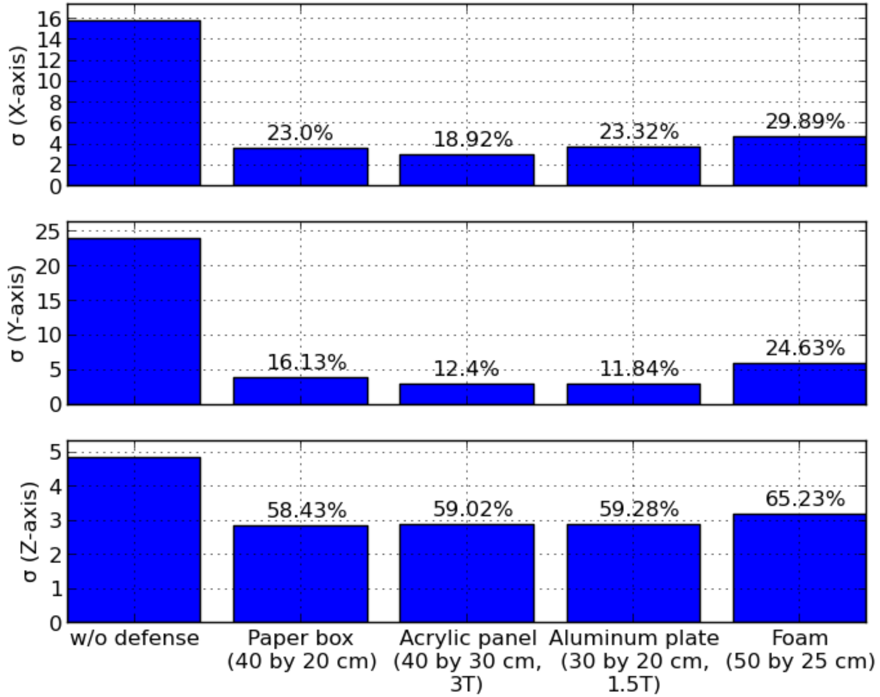
Countermeasure

- Physical isolation
  - Shielding from sound
  - Using four materials
    - Paper box
    - Acrylic panel
    - Aluminum plate
    - Foam

Countermeasure

- ❖ Physical isolation
  - Shielding from sound
  - Using four materials
    - Paper box
    - Acrylic panel
    - Aluminum plate
    - Foam

Standard deviation of raw data samples for one L3G4200D chip (averaged for 10 identical tests)



Conclusion

- A case study for a threat caused by sensor input
  - Finding mechanical resonant frequencies from 7 kinds of MEMS gyro.
  - Analyzing the effect of this resonance on the firmware of drones
  - Demonstrating to attack drones using sound noise in the real world
  - Suggesting several attack scenarios and defenses

Conclusion

- A case study for a threat caused by sensor input
  - Finding mechanical resonant frequencies from 7 kinds of MEMS gyro.
  - Analyzing the effect of this resonance on the firmware of drones
  - Demonstrating to attack drones using sound noise in the real world
  - Suggesting several attack scenarios and defenses

- Future work
  - Developing a software based defense (without hardware modifications)
  - Against sensing channel attacks for drones or embedded devices

Conclusion

- A case study for a threat caused by sensor input
  - Finding mechanical resonant frequencies from 7 kinds of MEMS gyro.
  - Analyzing the effect of this resonance on the firmware of drones
  - ld

Sensor output should not be fully trusted.

(Not only by natural errors, but also by attackers)

- Future work
  - Developing a software based defense (without hardware modifications)
  - Against sensing channel attacks for drones or embedded devices

Thank You!

yunmok00@kaist.ac.kr

APPENDIXES

Sensor

- Definition
  - To detect physical properties in nature
  - To convert them to quantitative values

Sensor

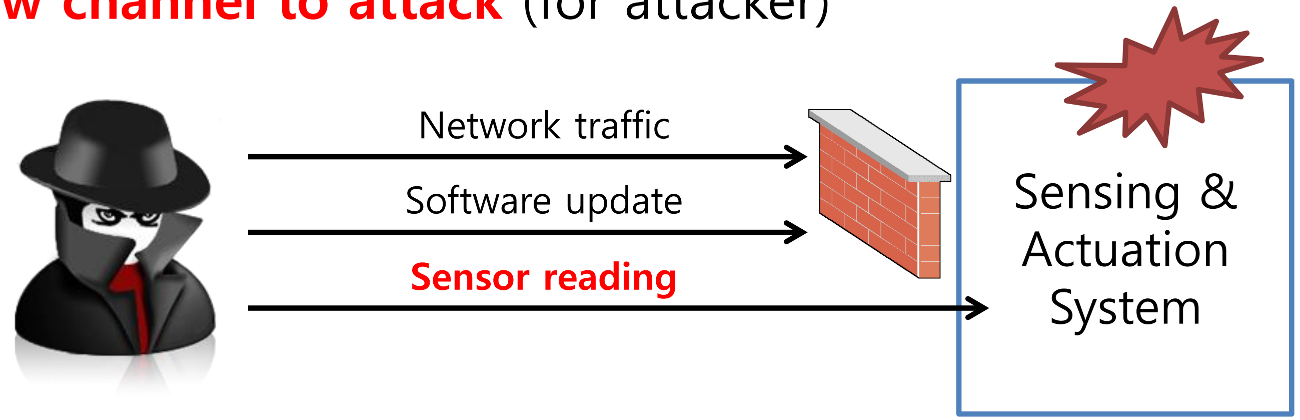
- Definition
  - To detect physical properties in nature
  - To convert them to quantitative values

- **New channel to attack** (for attacker)

Sensor

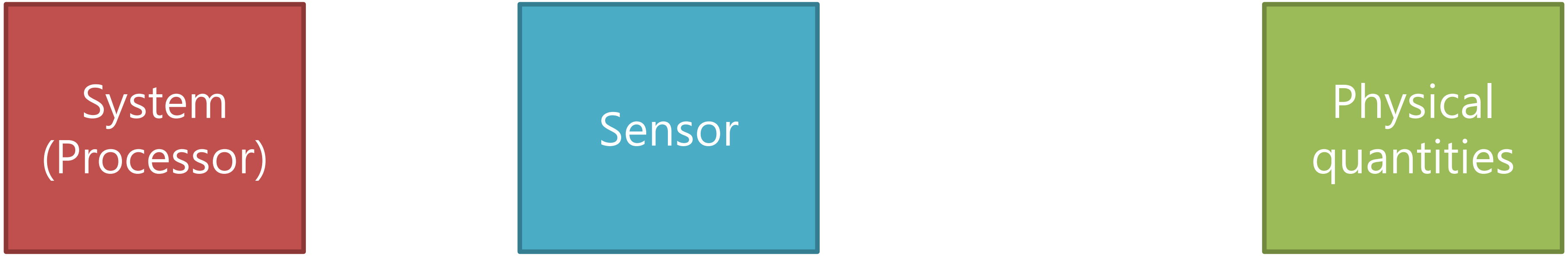
- ❖ Definition
  - To detect physical properties in nature
  - To convert them to quantitative values

- ❖ **New channel to attack** (for attacker)



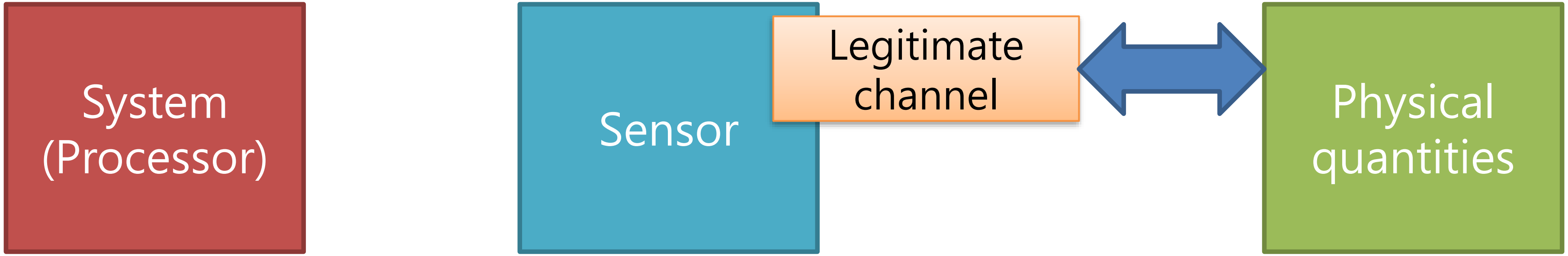
Attack Vectors of Sensor

- Three interfaces



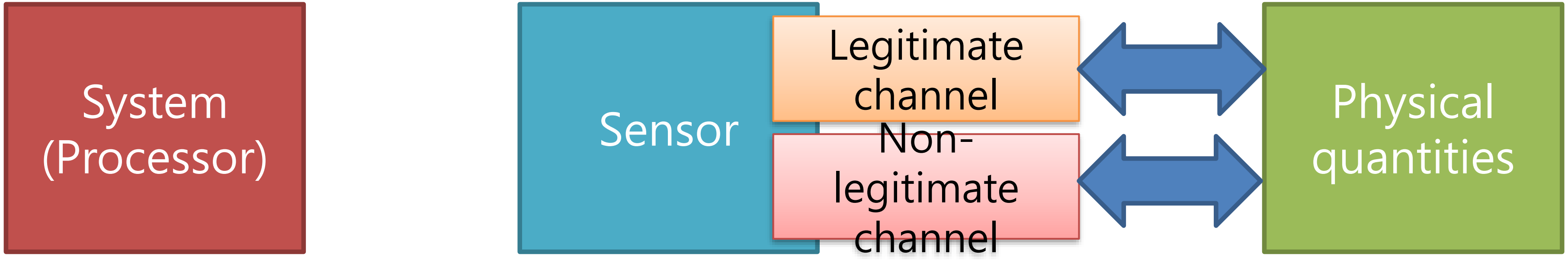
Attack Vectors of Sensor

- Three interfaces
  - Sensitive to legitimate (physical) quantities



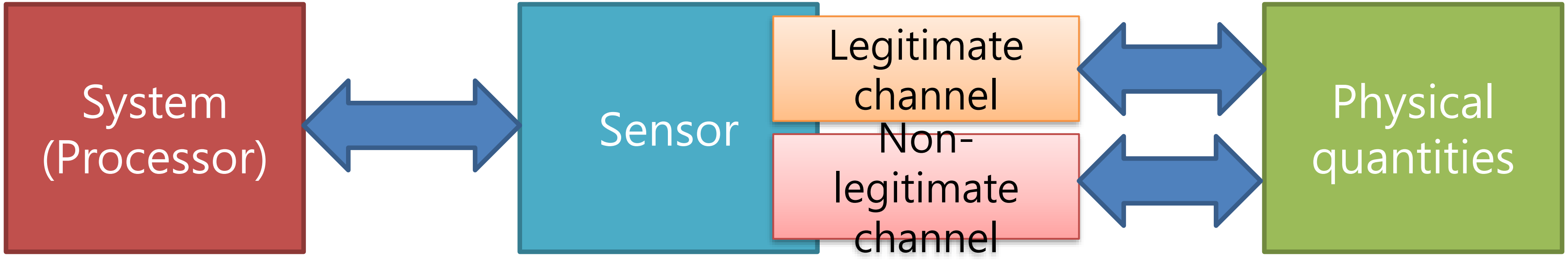
Attack Vectors of Sensor

- Three interfaces
  - Sensitive to legitimate (physical) quantities
  - Insensitive to other (physical) quantities



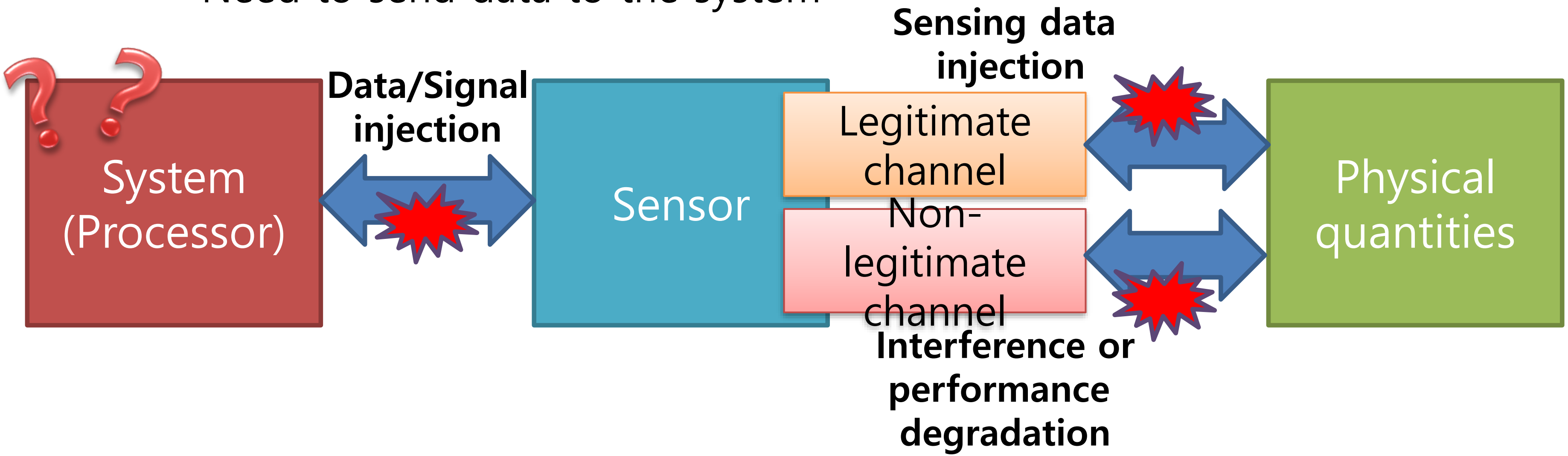
Attack Vectors of Sensor

- Three interfaces
  - Sensitive to legitimate (physical) quantities
  - Insensitive to other (physical) quantities
  - Need to send data to the system



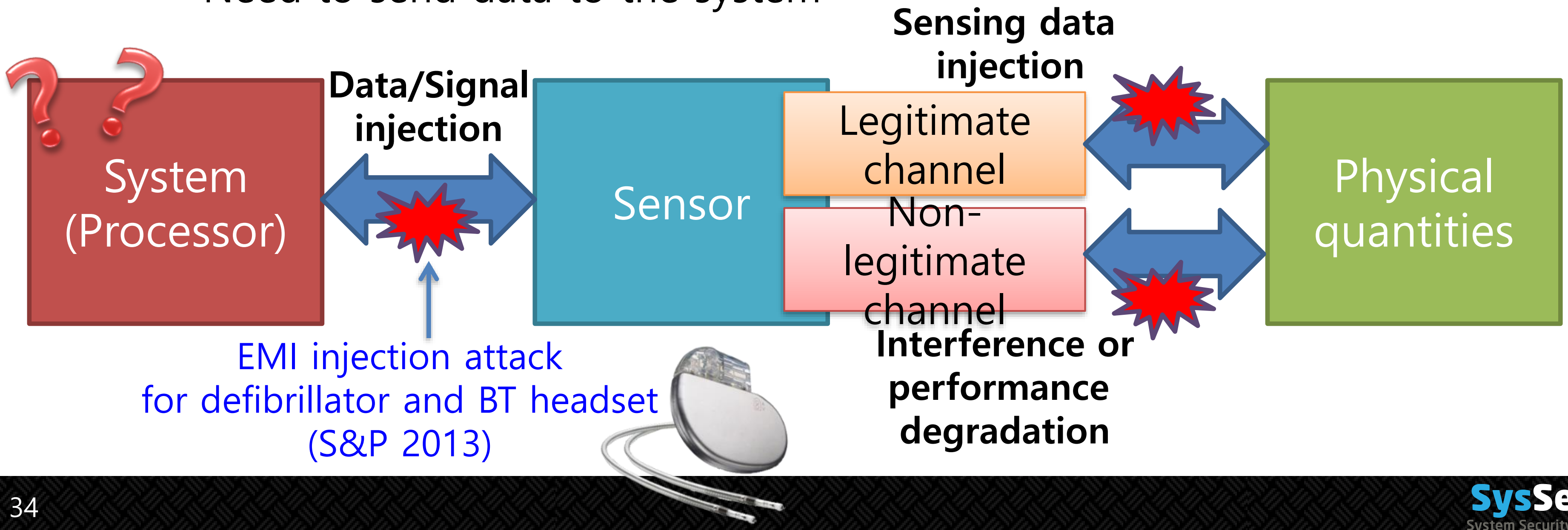
Attack Vectors of Sensor

- Three interfaces
  - Sensitive to legitimate (physical) quantities
  - Insensitive to other (physical) quantities
  - Need to send data to the system

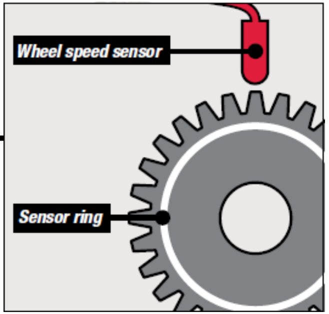


Attack Vectors of Sensor

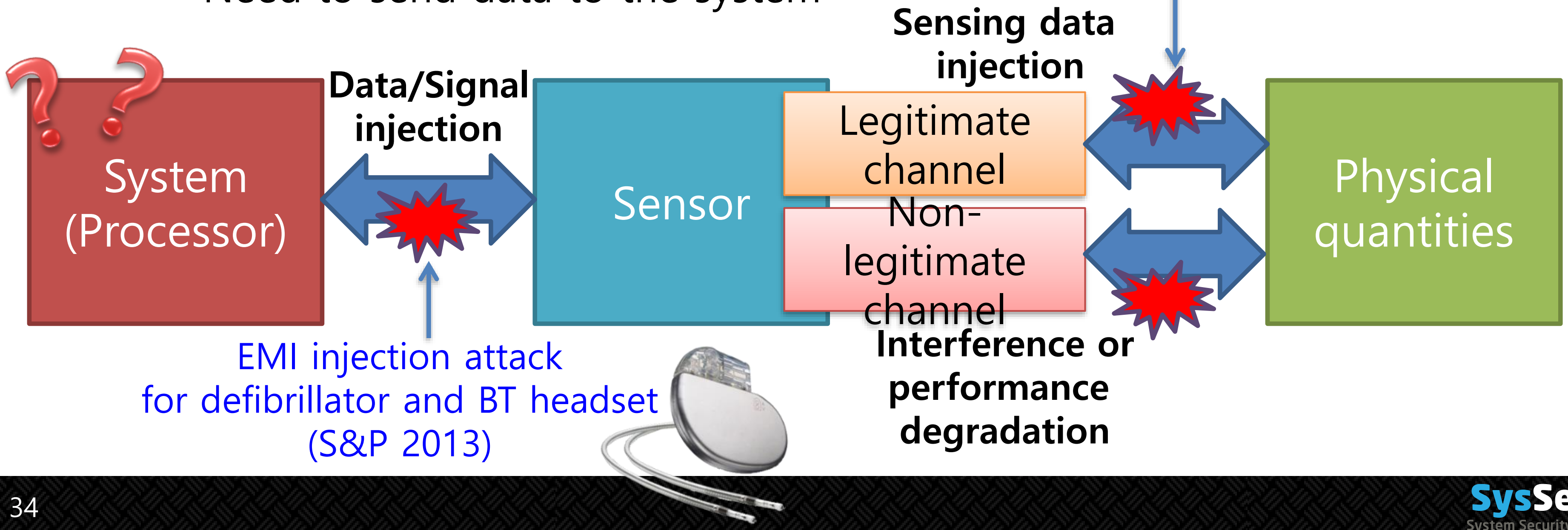
- Three interfaces
  - Sensitive to legitimate (physical) quantities
  - Insensitive to other (physical) quantities
  - Need to send data to the system



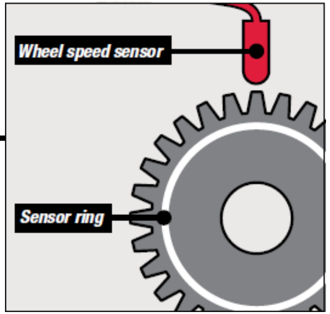
Attack Vectors of Sensor



- Three interfaces
  - Sensitive to legitimate (physical) quantities
  - Insensitive to other (physical) quantities
  - Need to send data to the system



Attack Vectors of Sensor

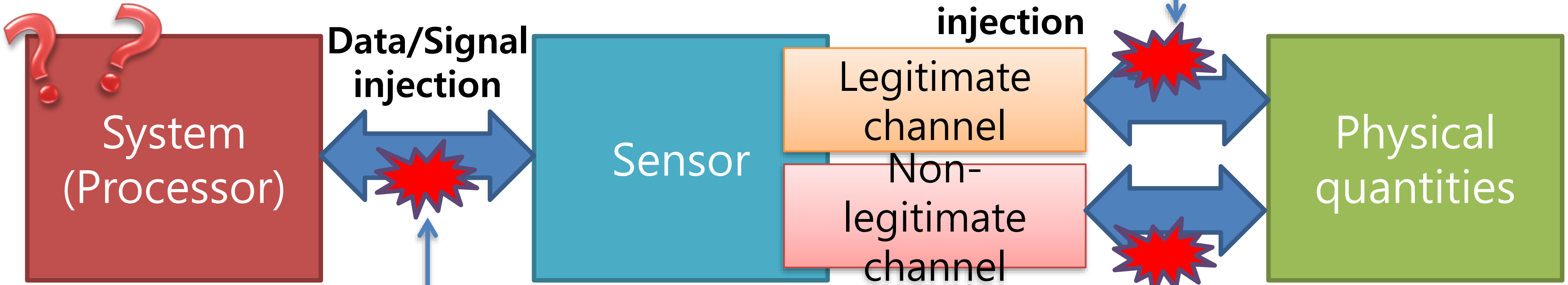


- Three interfaces
  - Sensitive to legitimate (physical) quantities
  - Insensitive to other (physical) quantities
  - Need to send data to the system

Spoofing attack for ABS in a car (CHES 2013)

Sensing data injection

Data/Signal injection



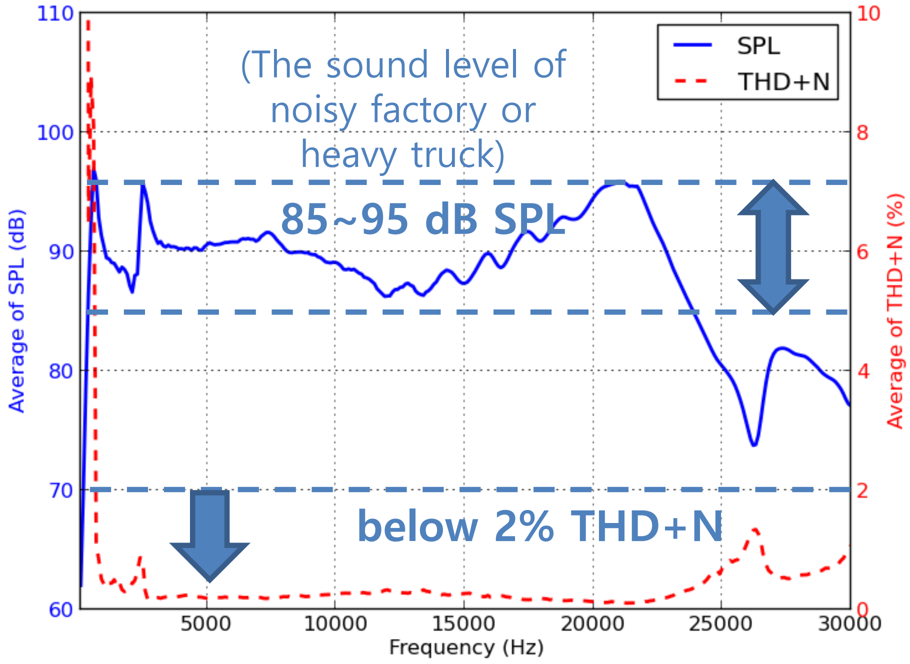
Interference or performance degradation

EMI injection attack for defibrillator and BT headset (S&P 2013)

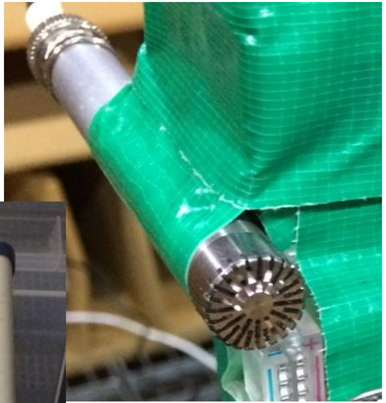
Our work

Sound Noise Source

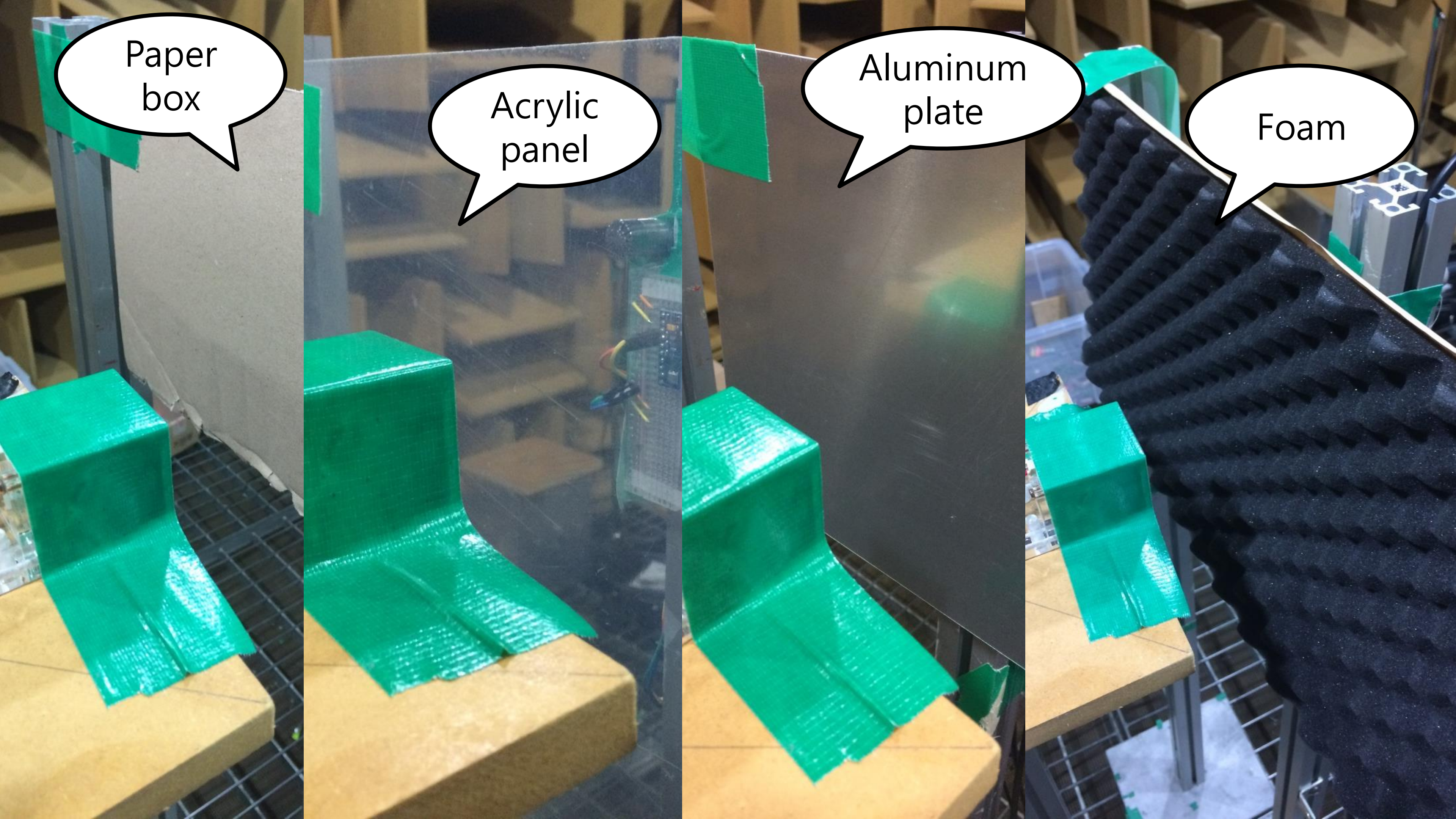
- Sound Pressure Level (SPL) and Total Harmonics Distortion plus Noise (THD+N) measurement



Microphone (Brüel & Kjær 4189-A-021)



Sound Measurement Instrument (NI USB-4431)


Paper box
Acrylic panel
Aluminum plate
Foam