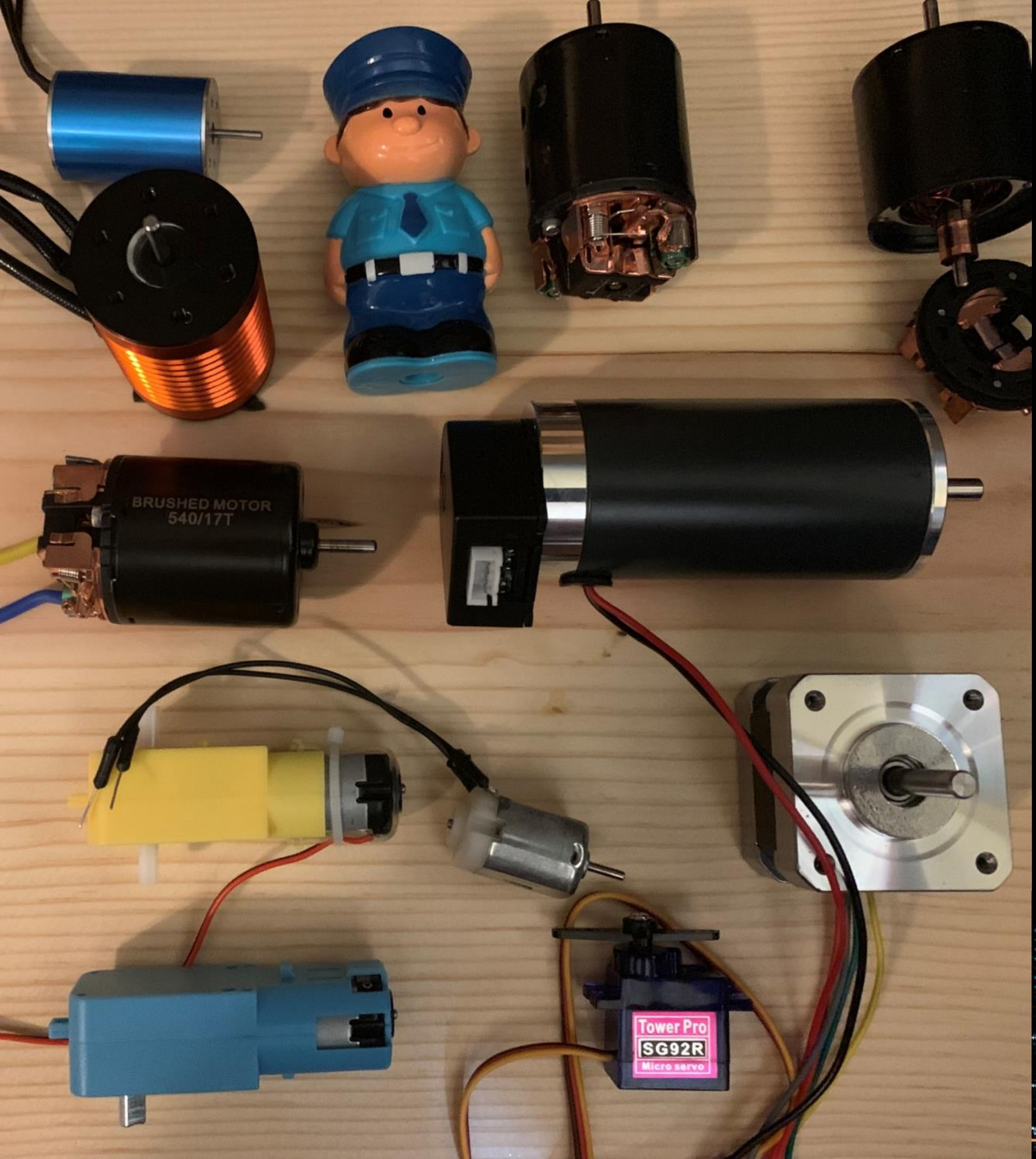


Attacking Electric Motors For Fun and Profit

Matthew Jablonski
Duminda Wijesekera, Ph.D.

black hat
USA 2019
AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS

About Us

GEORGE MASON UNIVERSITY

Matthew Jablonski

- Ph.D. Student in IT
- Engineer and penetration tester
- Safety and security of cyber-physical systems

Dr. Duminda Wijesekera

- Professor, CS
- 250+ Publications

RARE Lab

The Radar and Radio Engineering Lab ..

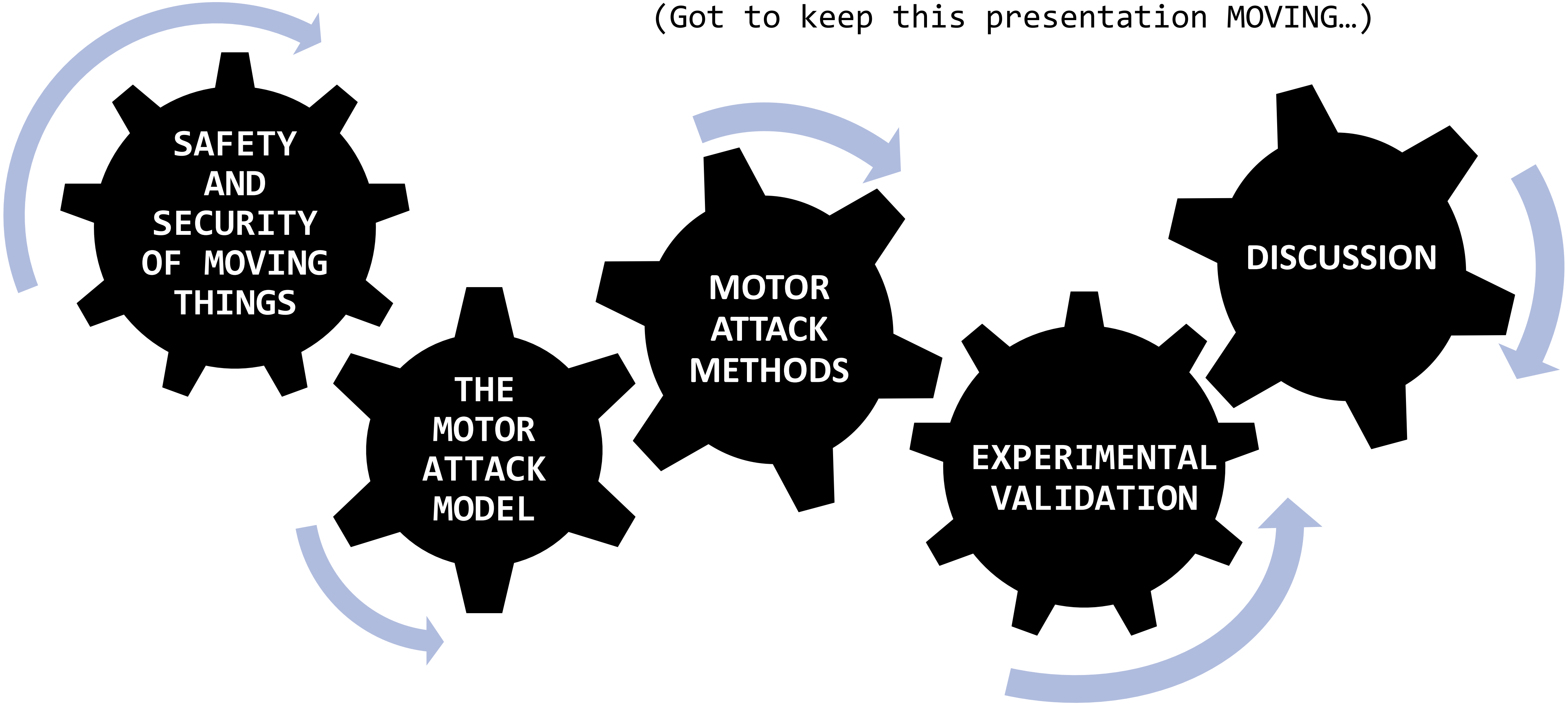
- Areas of Focus:
  - RF Off. and Def.
  - Cyber Physical Systems
  - Computer Vision
  - Risks in algorithms, HW/SW, etc.
- Collaborations:
  - Government
  - Transportation
  - Medical
  - Industrial

Abstract & Caveats

- Comprehensive technical evaluation of **attack objectives** and **offensive strategies** focused on **electric motor (EM) systems**
- Introducing the Motor Threat Model
- We do not:
  - target a specific product or endorse any products
  - follow safety warnings (but you should and we are not responsible for your actions)

Quick Overview

(Got to keep this presentation MOVING…)



Hypothetical Problem Scenario

- **Your next risk assessment target:**

  A Proprietary Drone System

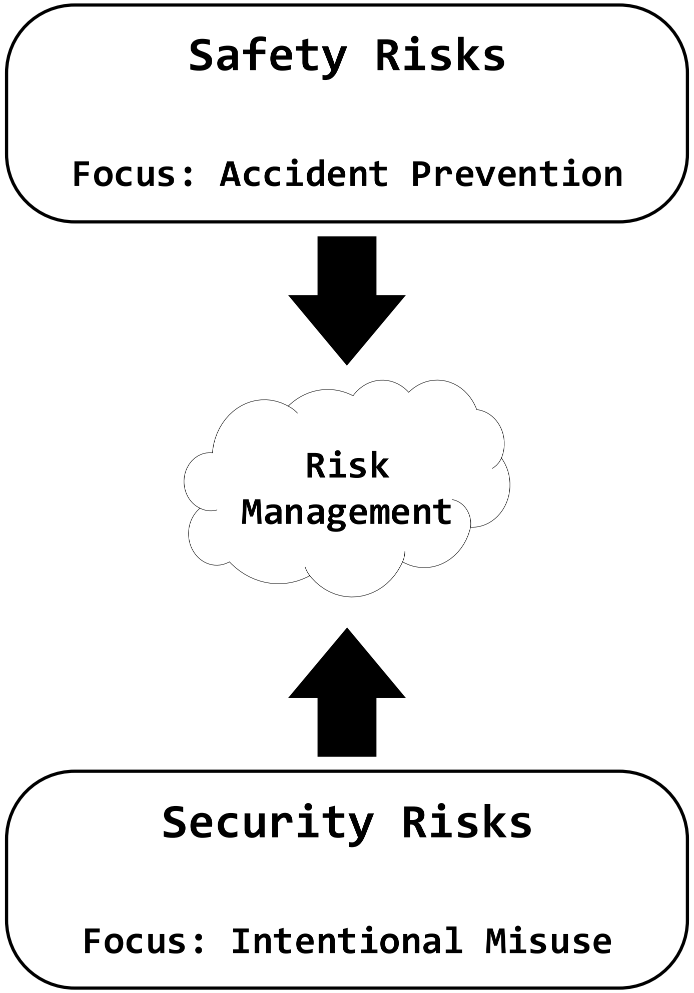
- Thousands deployed worldwide for package delivery
  - 30 different drone models were dev'ed
  - Hundreds of operators…
  - With physical and remote access…
  - And… background checks aren't required.
  - Over the Internet.
- **WHAT IS THE ATTACK SURFACE?**

  (and we need your response **NOW!**)

Safety First!

- Rules, Regulations, Standards
  - Designed to address **accidents**
- Protect against risks through:
  - Operational requirements
    - i.e. air traffic control
  - Power requirements
    - i.e. overcurrent, low voltage, etc.
  - System calibration requirements

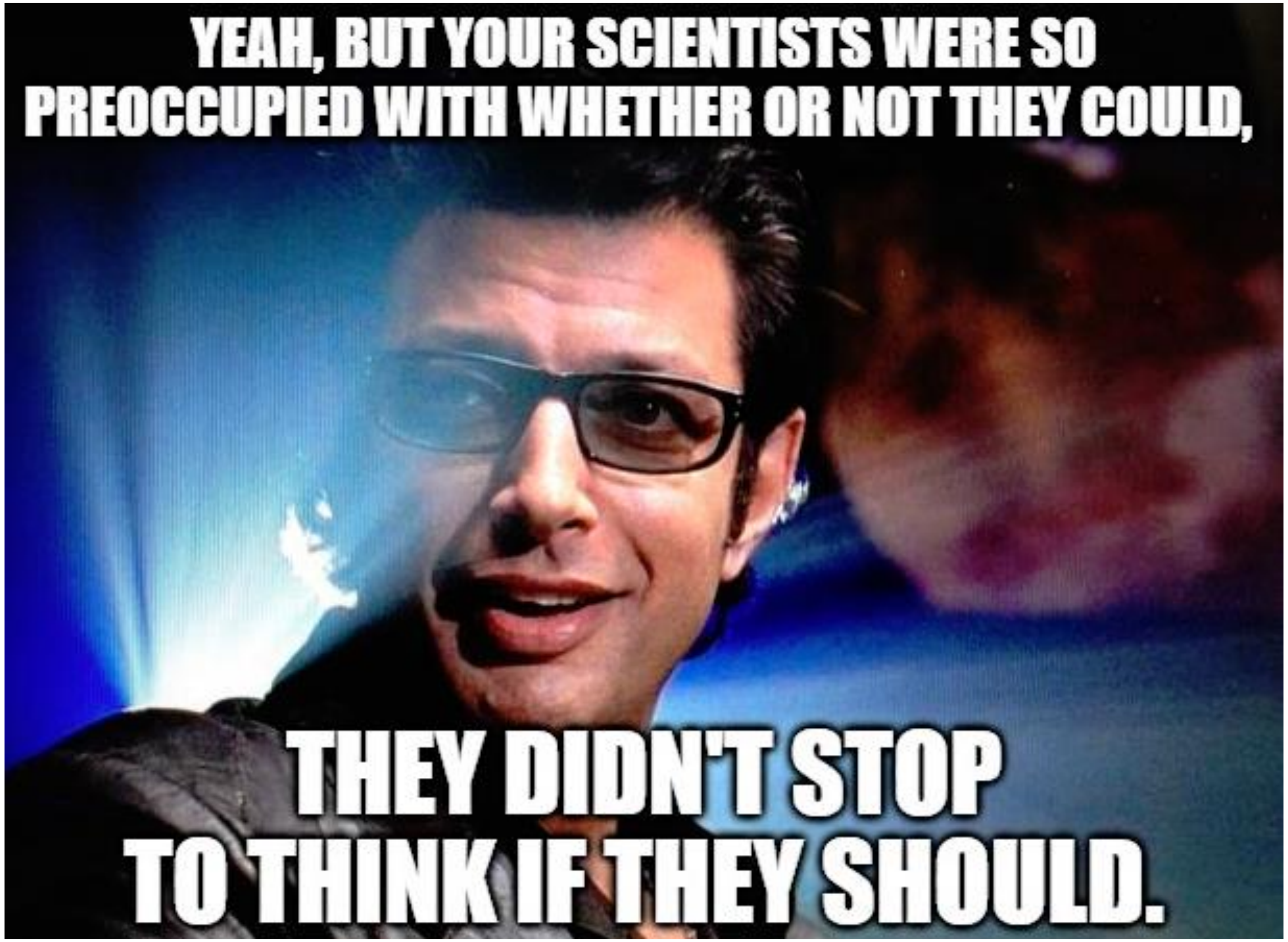
- Security… Second?
  - What about **intentional threats**?



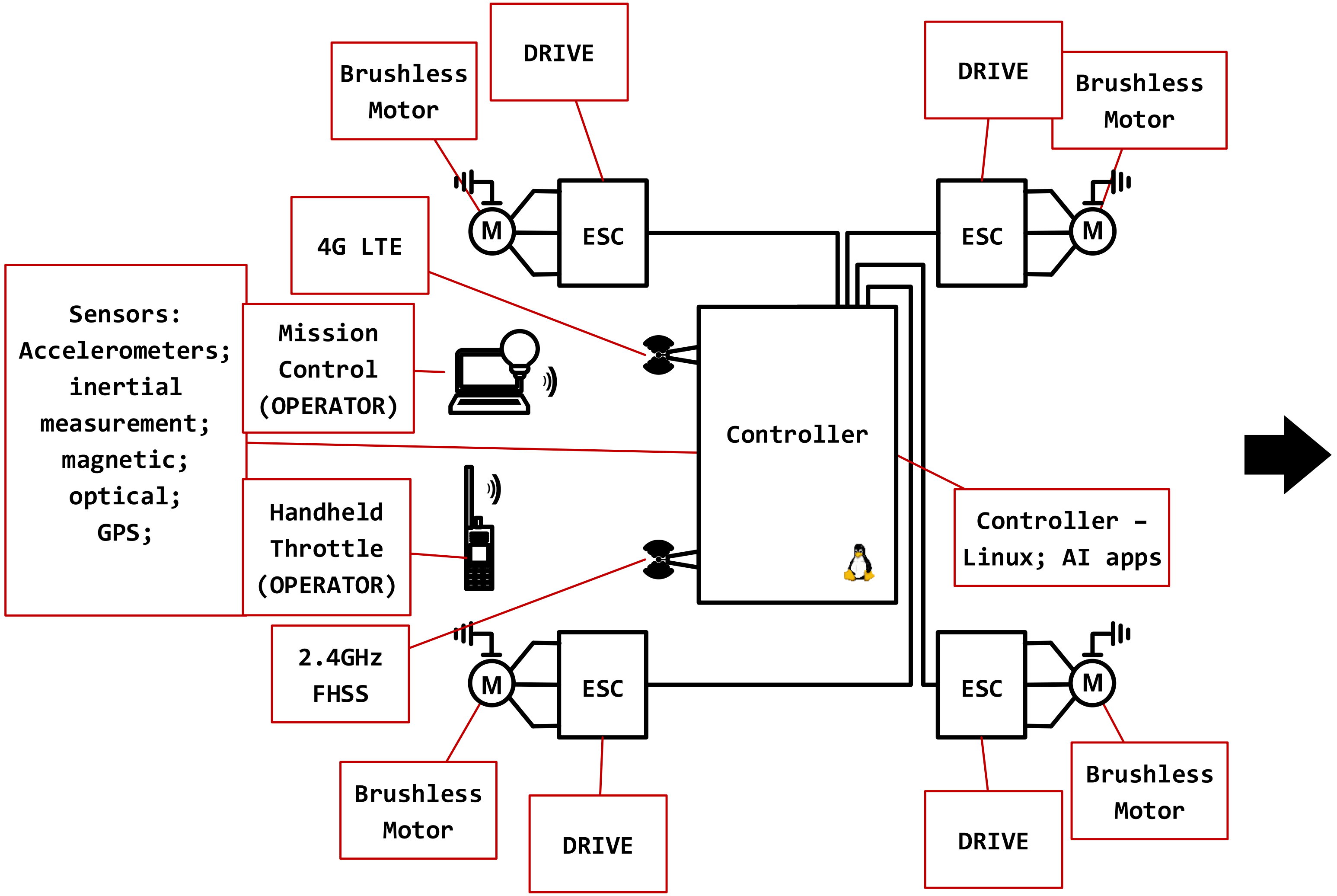
The First Security Problem…

- Possible nightmare scenario…

Unacceptable Security Recommendation



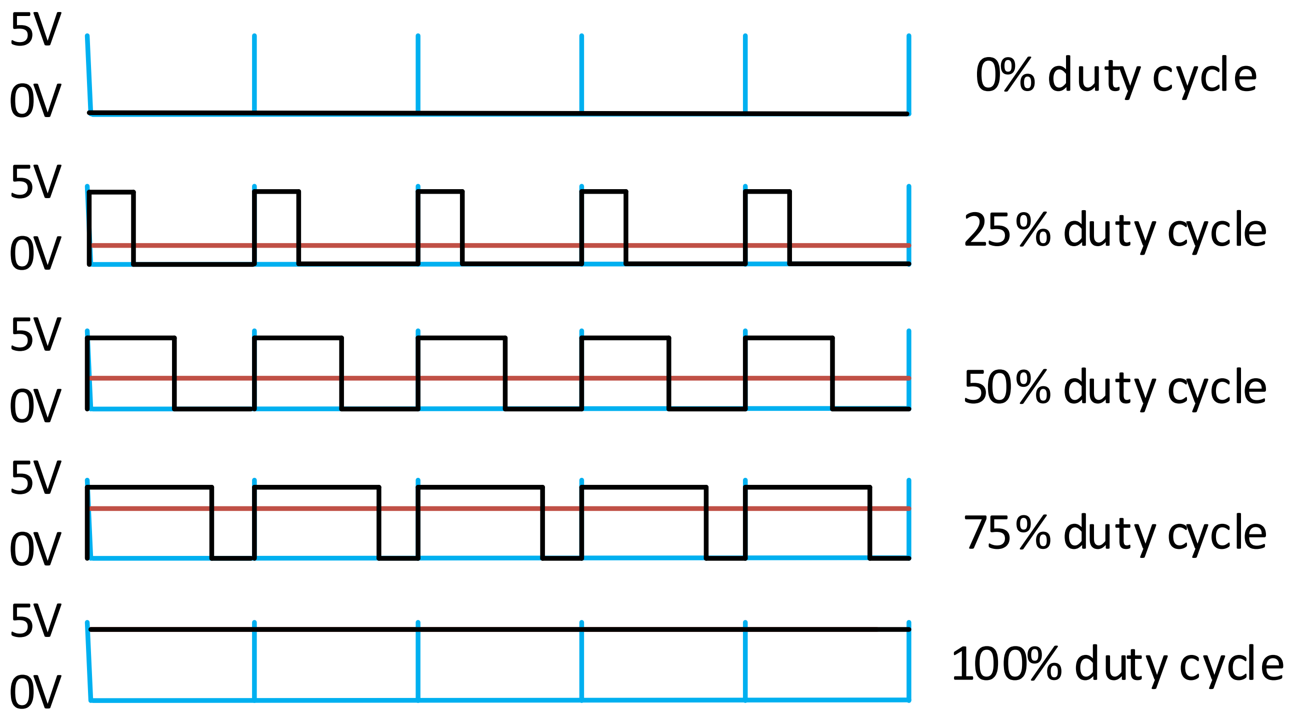
System Review: What’s Inside?



The Start: Find Similar Threat Models?

How do Electric Motors Work?

- Every motor connected to a **drive**
  - Embedded controller
  - ESC, VSD, VFB
- Voltage fluctuated at **pin** by HW switch
  - Current flows to motor when V>0
  - Pulse Width Modulation
- **Clock** and **duty cycle** controlled by HW & SW

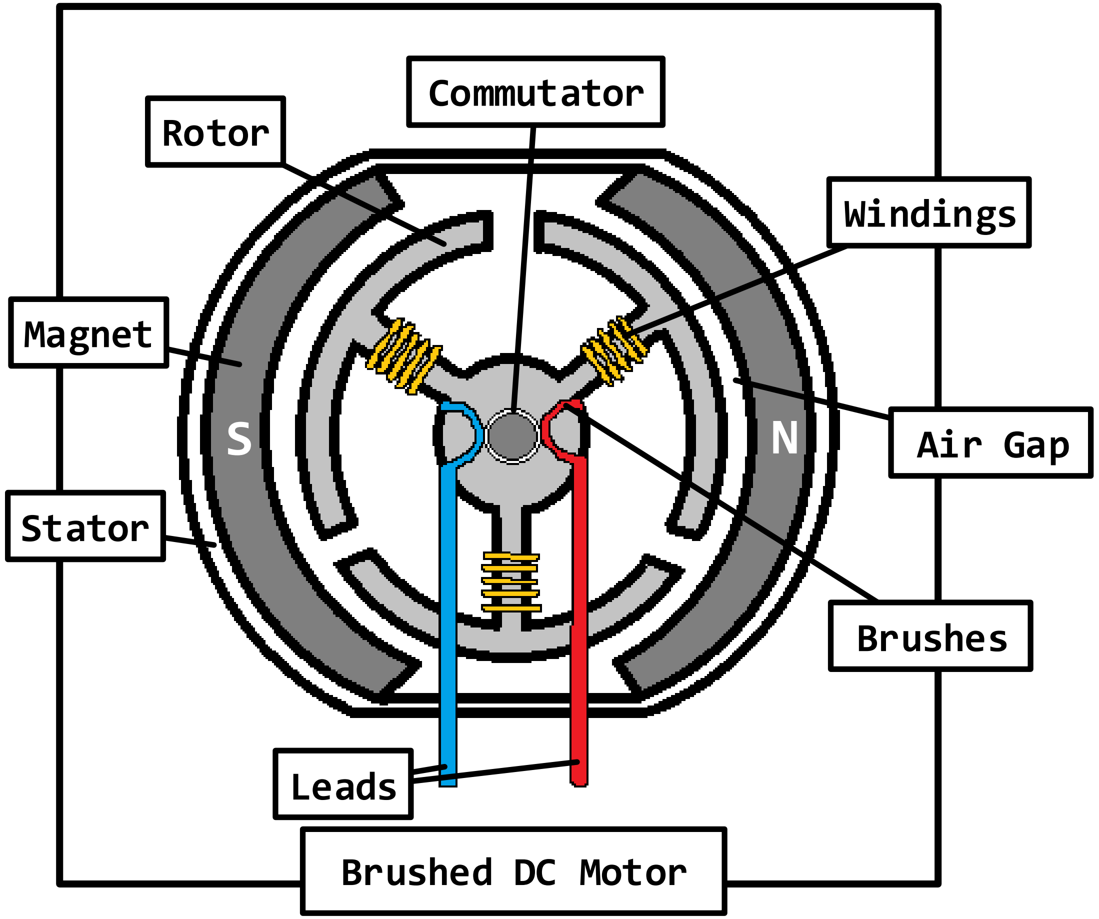


How do Electric Motors Work?

- **Input**: electrical energy
- **Output**: torque, speed, mechanical energy

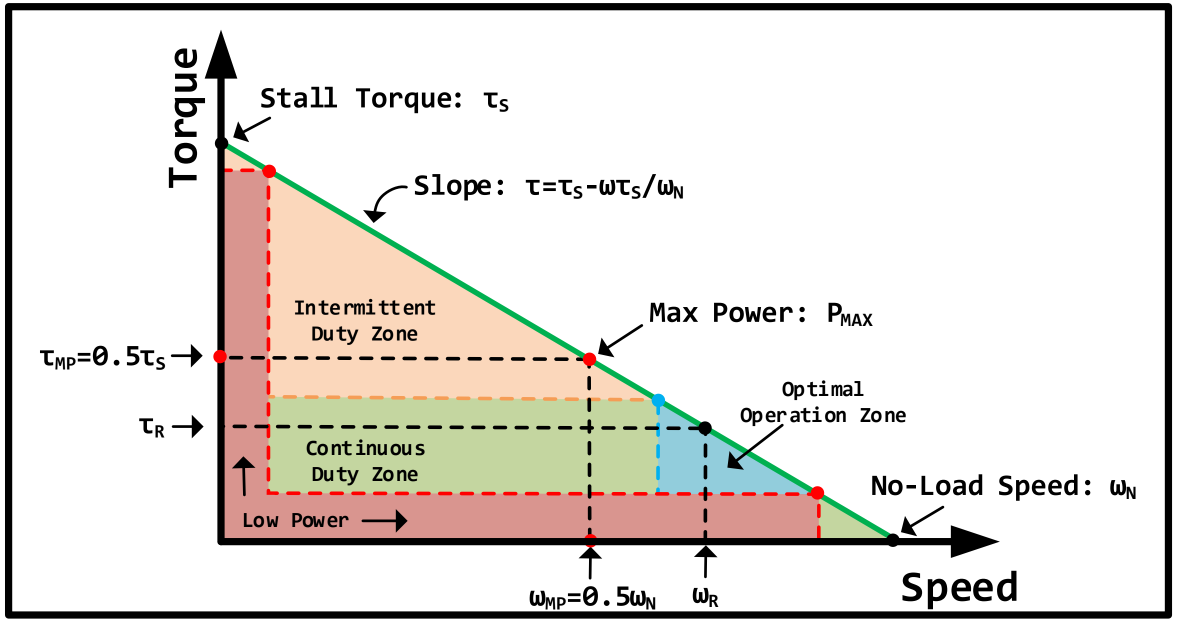
- **Rotor**: free-moving
- **Stator**: stationary

- **Many different types**:
  - DC vs. AC power
  - Rotary vs. linear
  - Selection based on LOAD

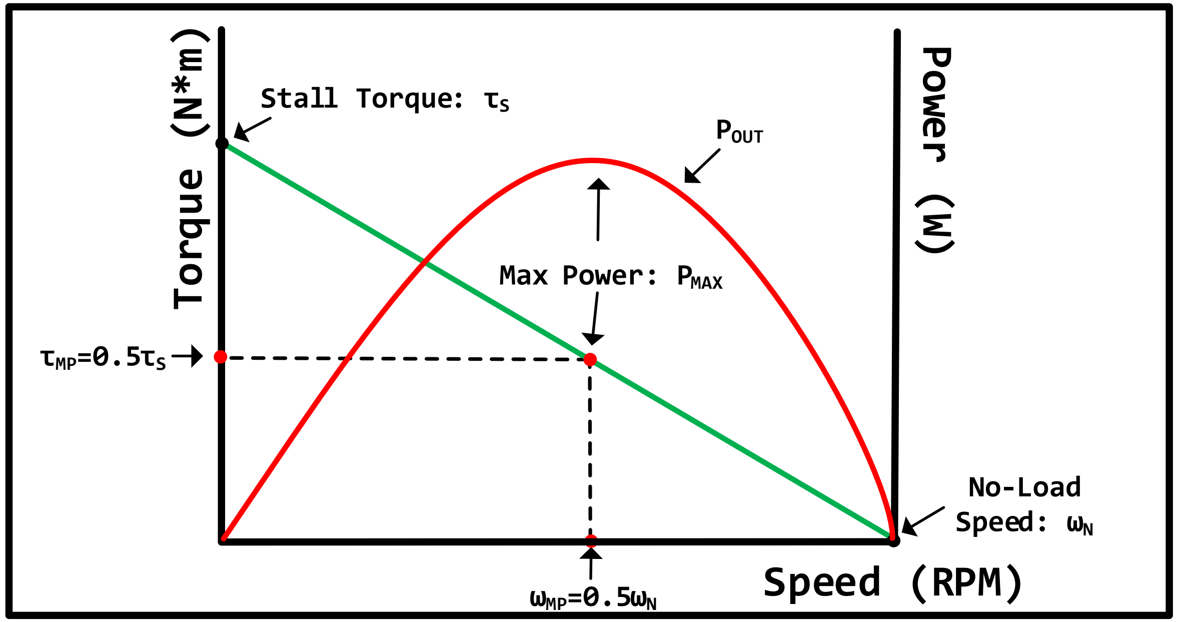


How do Electric Motors Work?

Torque vs. Speed

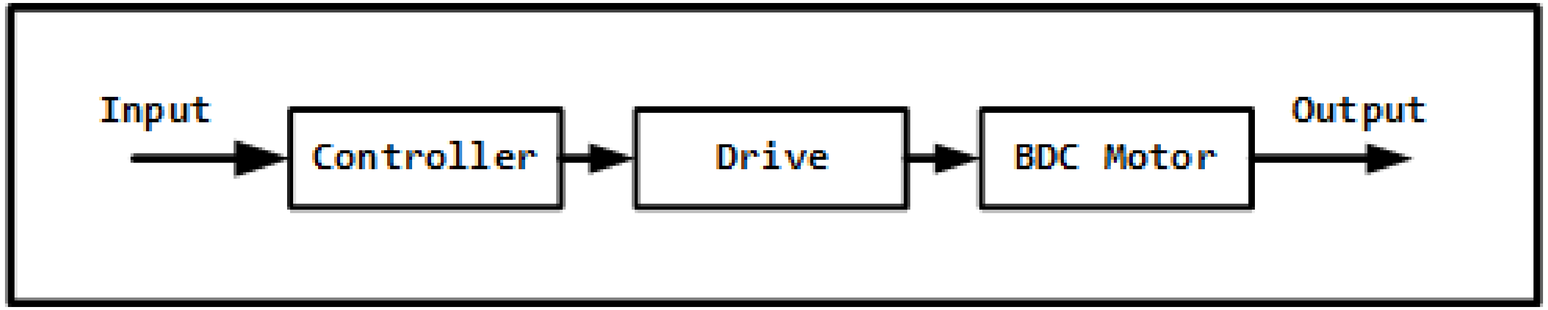


Effects on Power Output

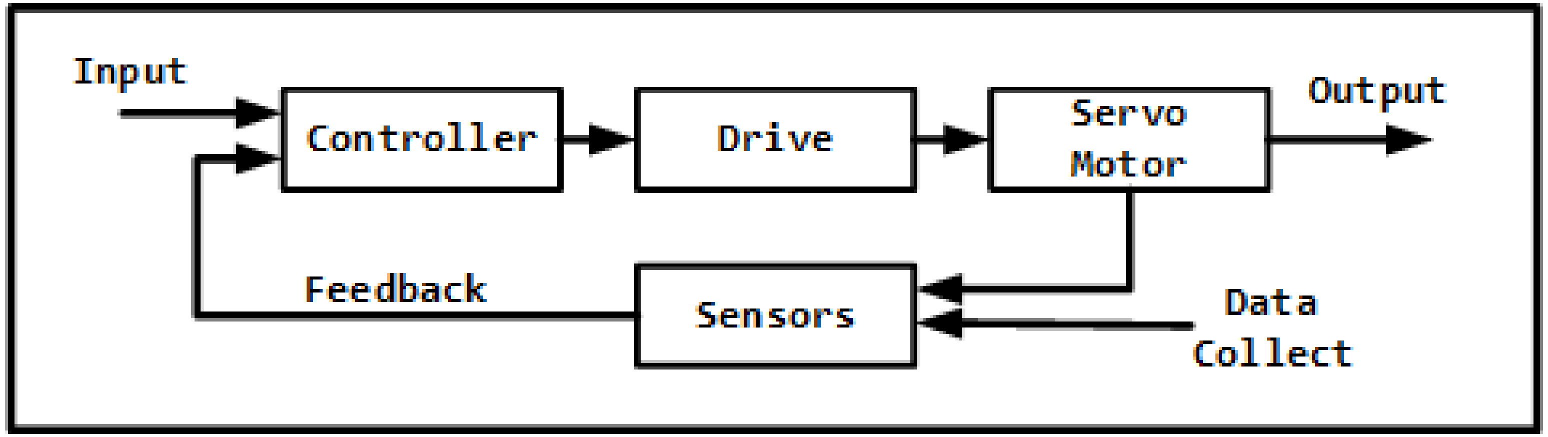


Control Theory:
The Recipe for Digital Movement Control

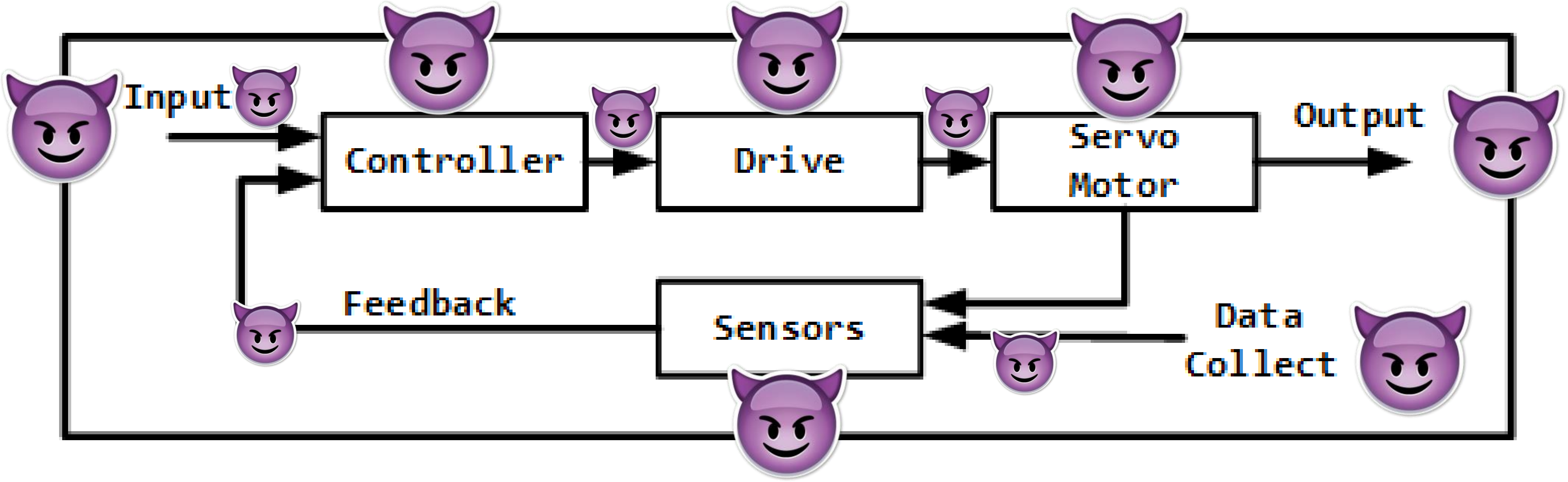
Open loop systems:



Closed loop systems:

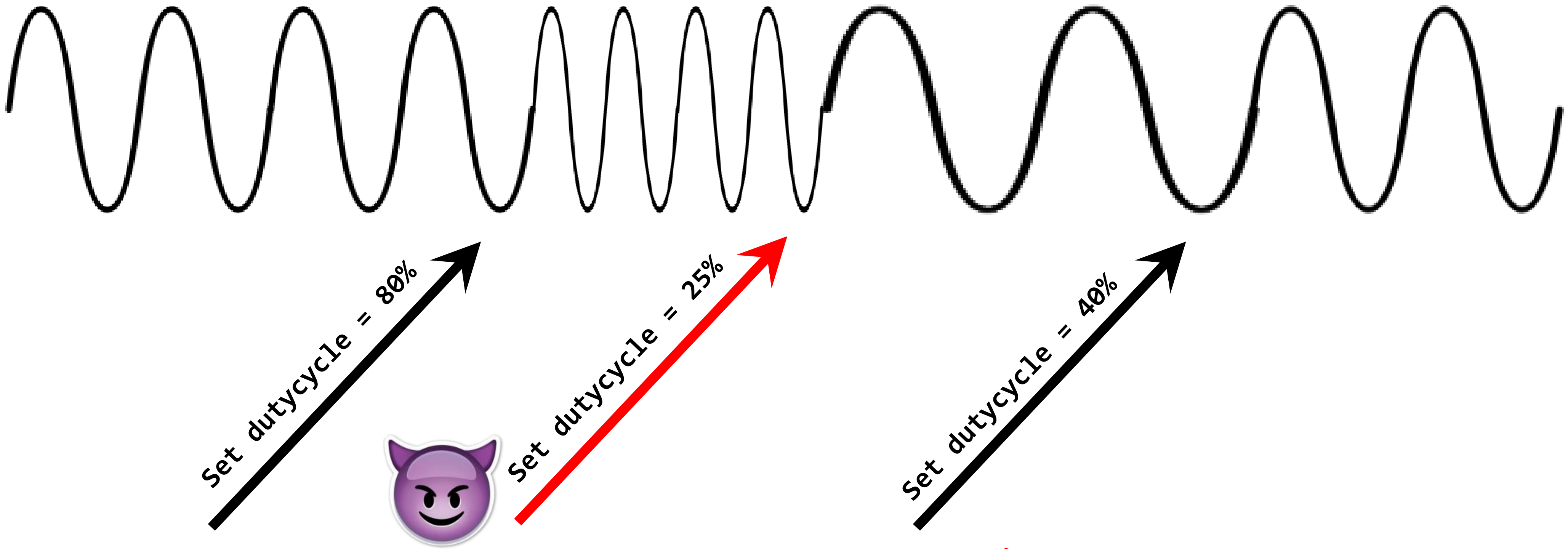


Another Security Problem…



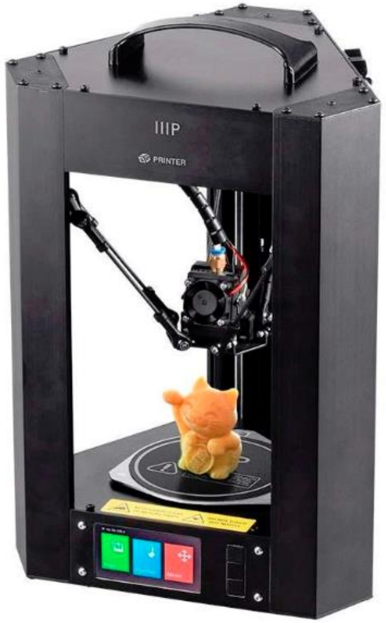
Yet Another Security Problem…

Movement is **continuous** (usually)



Digital control requires **discrete** commands

Maybe Similar Threat Models?

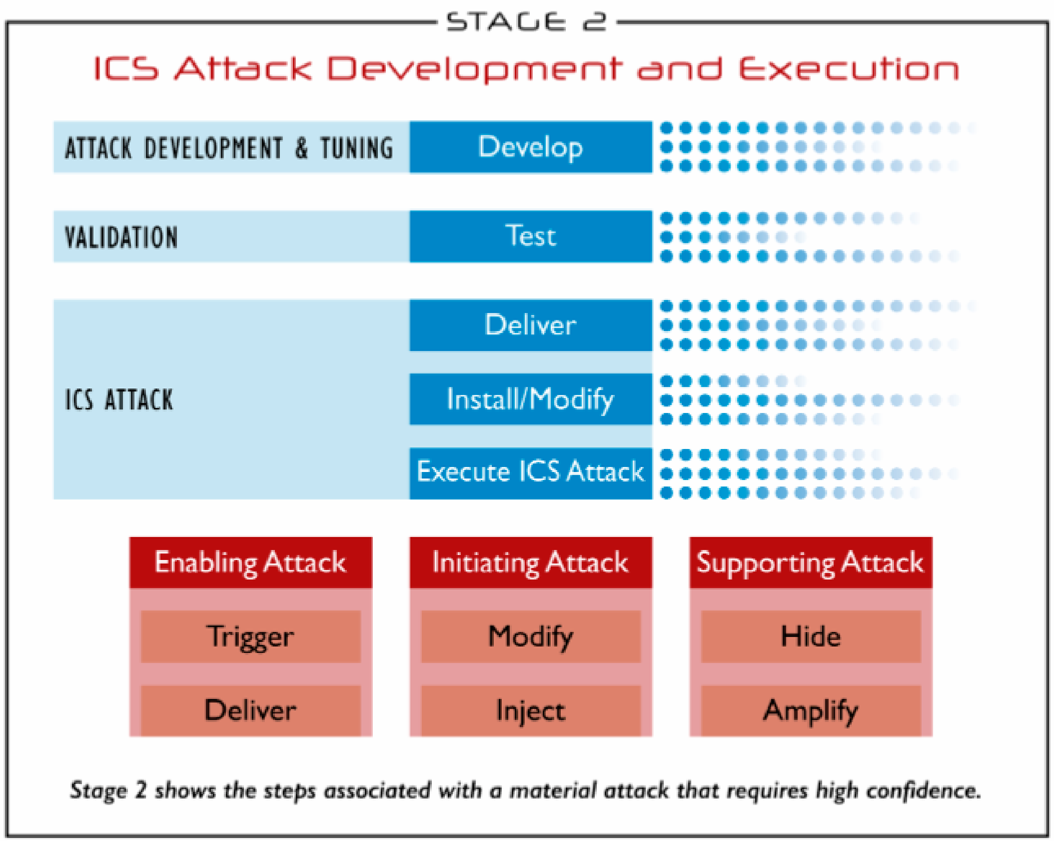


Threat Modeling… Gaps…

- Let’s get away from drones.

- **Common issues:**
  - Cyber vs. physical attacks
  - Physical attack outcomes
  - Multiple control layers
  - Digital commands are discrete

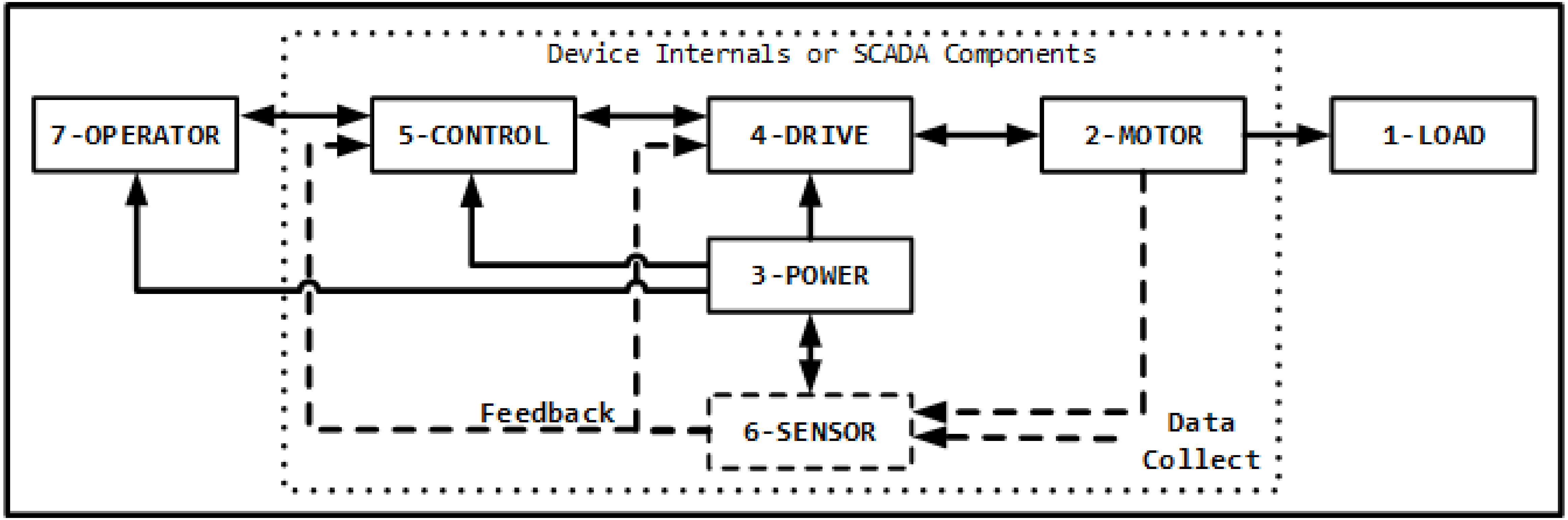
- **Possible models?**
  - ICS Cyber Kill Chain (Stage 2) [1]
  - Mitre’s ICS ATT&CK Framework [2]



[1] M. J. Assante and R. M. Lee, “The Industrial Control System Cyber Kill Chain,” Tech. Rep. 36297, SANS Institute, October 2015.
[2] O. Alexander, “ICS ATT&CK Framework: Adversary Tactics and Techniques (S4x19).” www.brighthubengineering.com/commercial-electrical-applications/78579-determining-causes-for-electric-motor-failure/, January 2019. Accessed: 2019-07-05.

The Motor Threat Model (MTM)

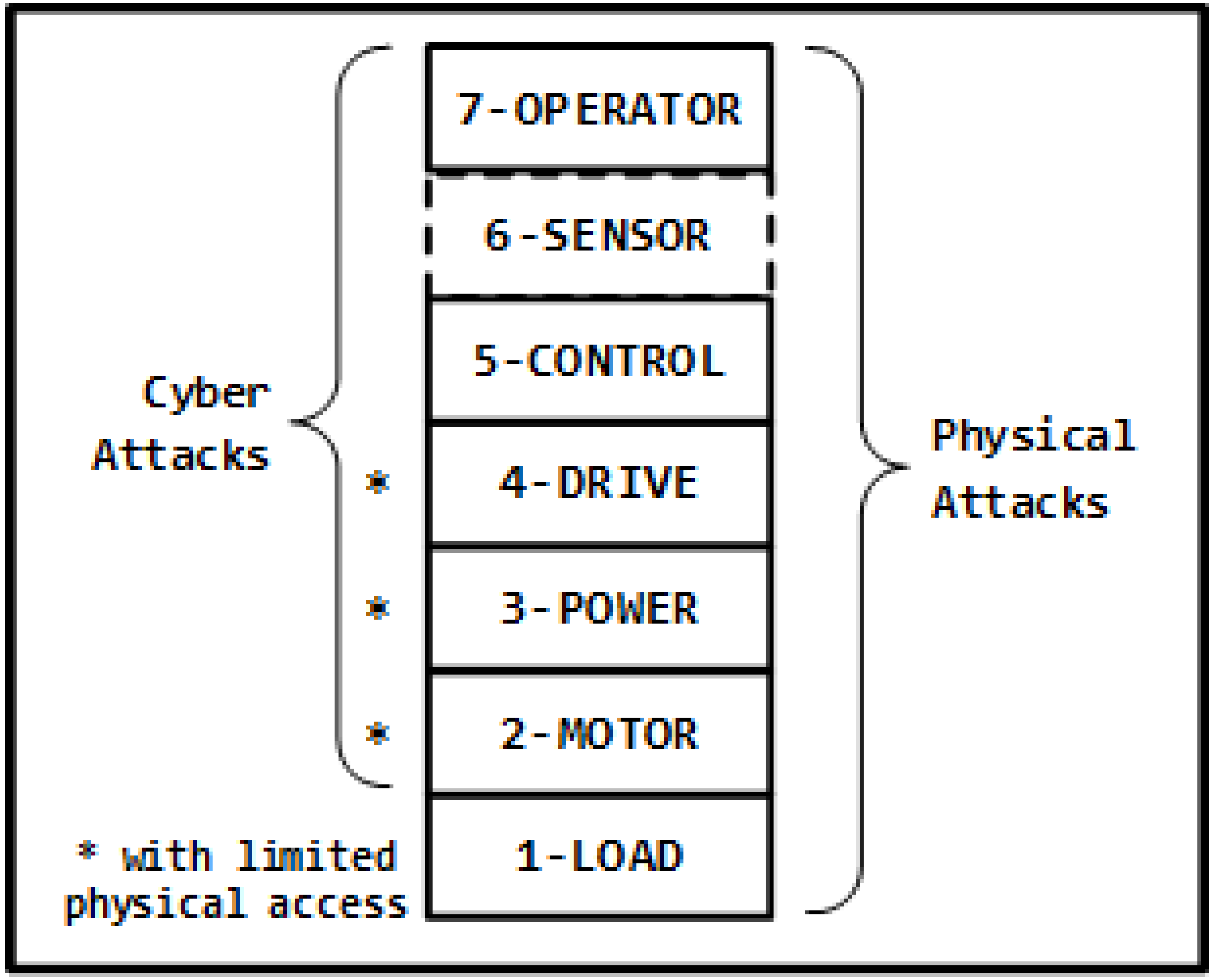
Our proposed model:



The MTM Stack

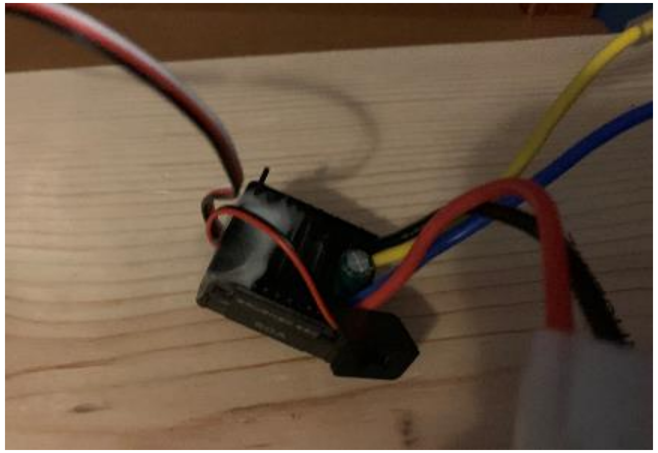
- Simplified 7-layer stack

- **Key takeaways:**
  - Attacks at **higher layers** allow better control for attacker
  - Attacks at **lower layers** take control of movement from higher layers
  - Can understand access needed for C v. P attacks



High Level Attack Objectives

- **Control**
  - Steal control to achieve some goal
  - Cyber attacks
  - Easiest at layers 4-7
- **Disrupt**
  - Stop movement or prevent operational controls
  - Cyber or physical attacks
  - All layers
- **Data Exfiltration**
  - IP or privacy theft by tracking movement data
  - Cyber attacks
  - Easiest at layers 5-7



Layer Descriptions

Name	Description	Level 1 Access Description	Level 2 Access Description	Types of Attacks (C, P)*	Attack Objectives (C, D, DE)**
7 – OPERATOR	Unprivileged motor control	Operator interface	OPERATOR-CONTROL channel	C, P	C, D, DE
6 – SENSOR	Feedback data on phys. env.	Sensors or Wireless Sensor Network (WSN)	Out-of-band safety system (if exists)	C, P	C, D, DE
5 – CONTROL	Root system control	System controller	CONTROL-DRIVE channel	C, P	C, D, DE
4 – DRIVE	Modify motor configuration	Motor drive controller	DRIVE-MOTOR channel	C, P	C, D

* Cyber (C) or Physical (P)
** Control (C), Disrupt (D) or Data Exfiltration (DE)

Layer Descriptions

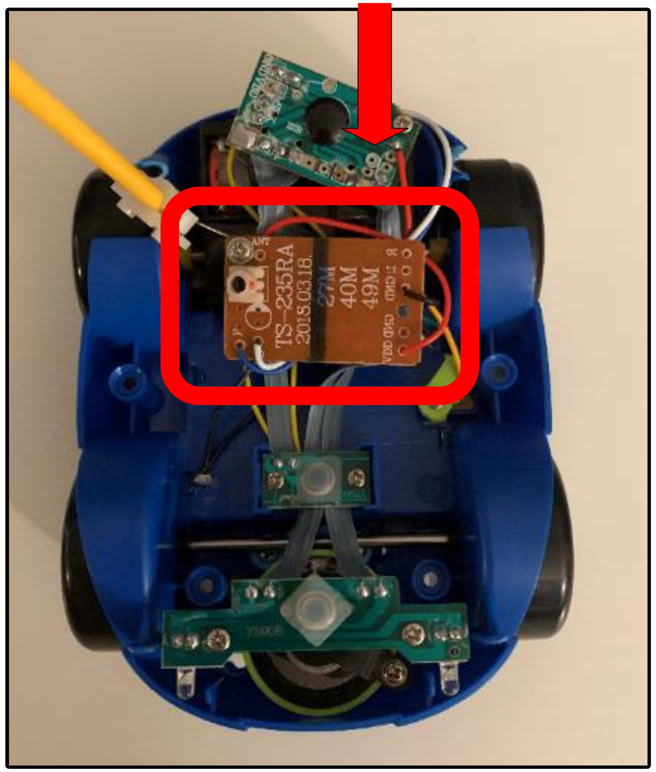
Name	Description	Level 1 Access Description	Level 2 Access Description	Types of Attacks (C, P)*	Attack Objectives (C, D, DE)**
3 - POWER	Prevent or degrade movement	Power system access	N/A	C, P	D
2 - MOTOR	Source of mechanical movement	Motor physical access	N/A	C, P	D
1 - LOAD	Prevent movement by overload	Output LOAD access	N/A	P	D

* Cyber (C) or Physical (P)
** Control (C), Disrupt (D) or Data Exfiltration (DE)

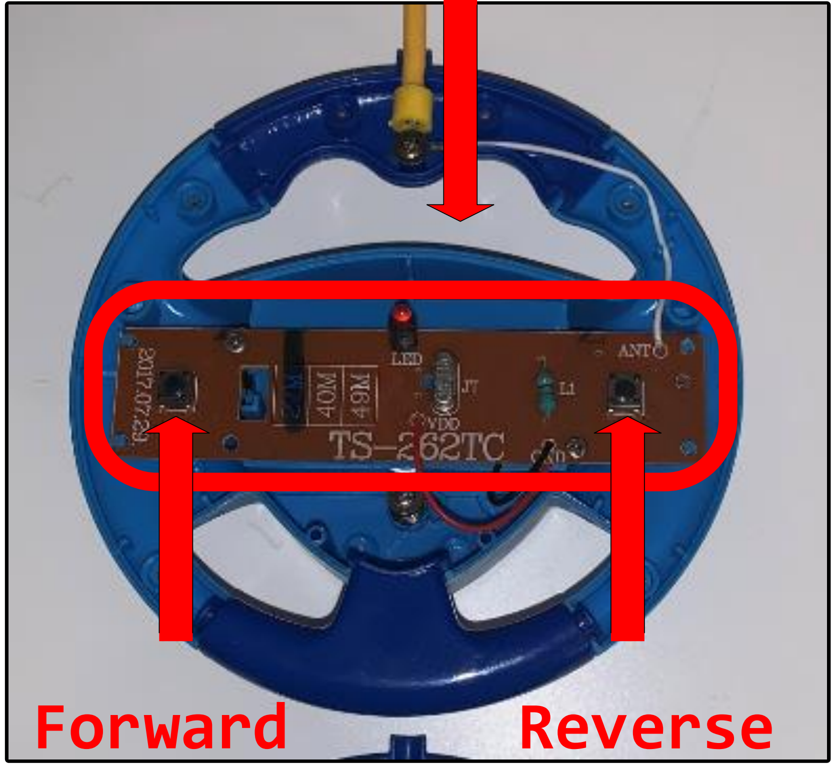
OPERATOR Attack Ex. 1
Wireless Control

Example Target:

Controller

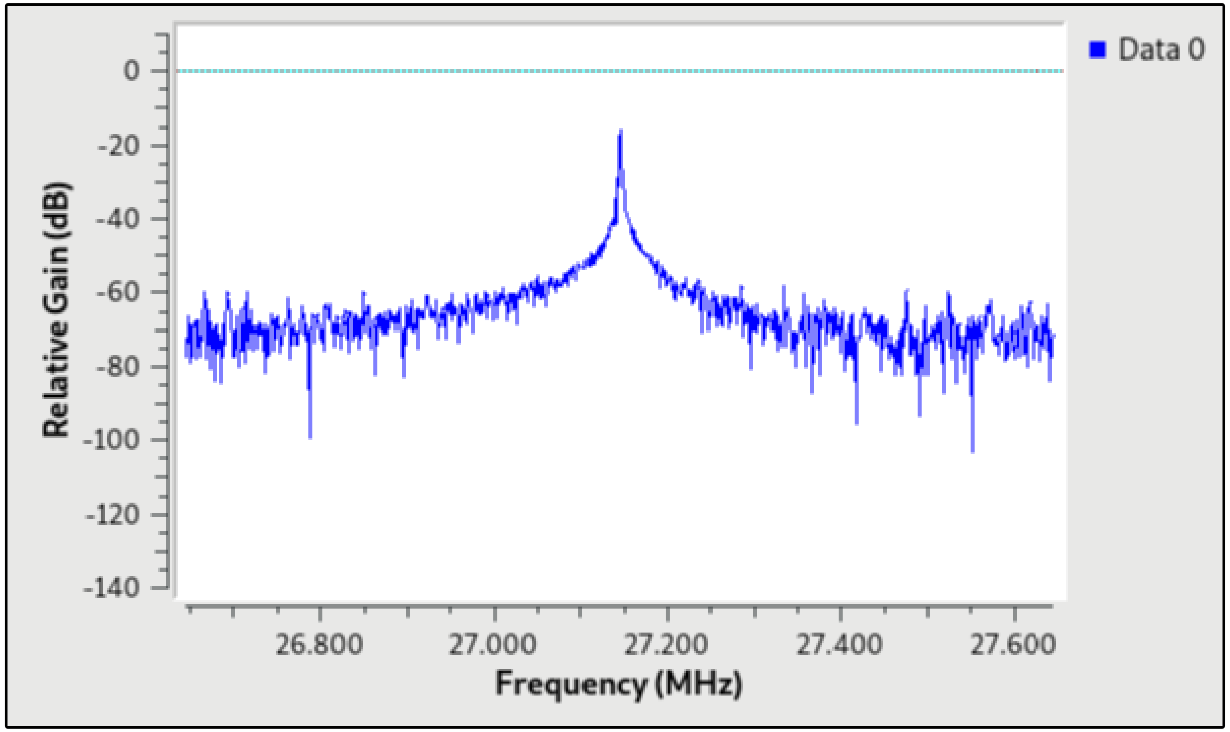


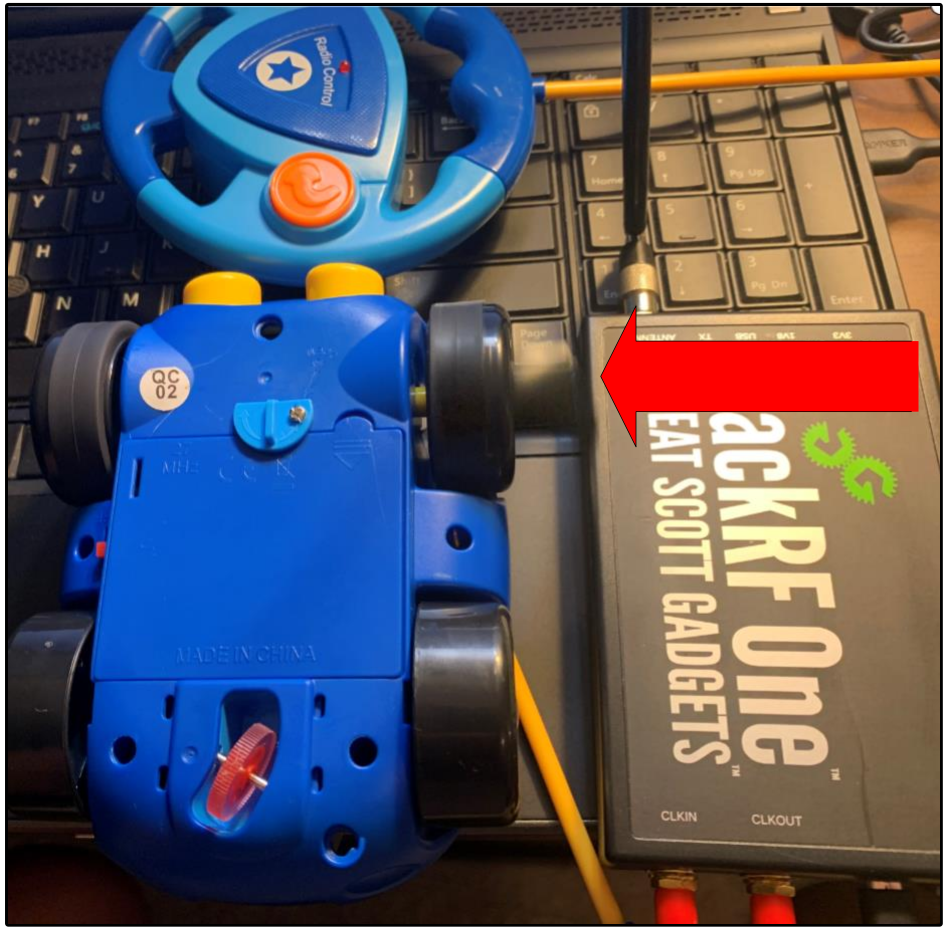
Operator



OPERATOR Attack Ex. 1
Wireless Control

Results: *Control and Disrupt*





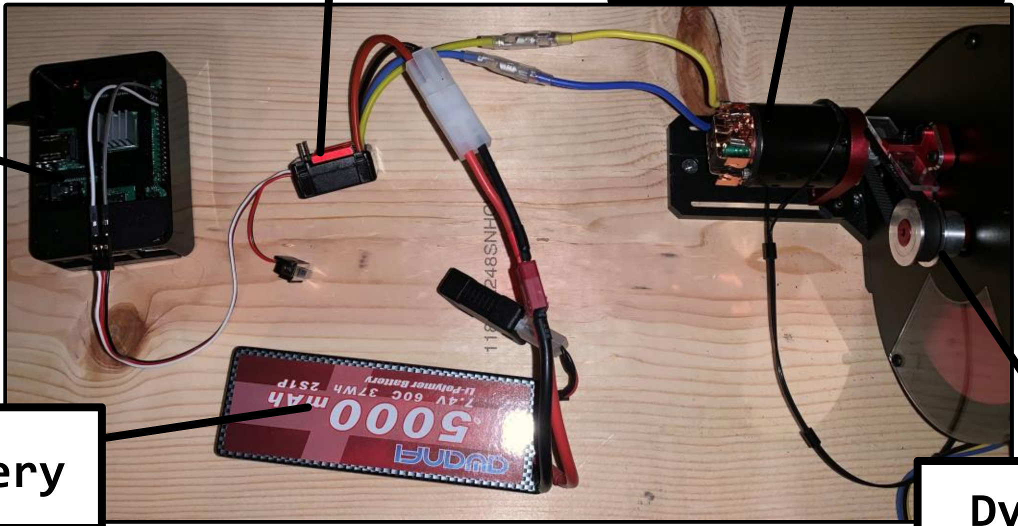
OPERATOR Attack Ex. 2
Remote Pin Control

Example Target:

RPi Controller; Raspbian; pigpiod with *Remote GPIO*

ESC

Brushed DC Motor



LiPO Battery

Dynanometer

This physical setup is used in most attack examples, unless noted.

OPERATOR Attack Ex. 2
Remote Pin Control

```
22/tcp   open  ssh              syn-ack (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_7.4p1 Raspbian-10+deb9u6
| ssh-hostkey:
|   2048 7e:87:cd:3e:a5:15:70:1a:e4:8b:53:d1:ff:61:b1:da (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDL6ll97ayXbg2N1+AWcH689TS5JDzuMj1w
X7MzmP48c1YUePU4pPc7rAuxyft4O9AO3on7E7XJ/RcBtos+EZCmTTeKtKs4+AuJ04dzDkG7iX
|   256 eb:ed:c8:df:84:36:5e:f7:a2:0b:22:f6:9b:40:97:e8 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABB
|   256 8c:bd:de:72:90:52:a6:b9:2c:0e:2b:95:56:60:e6:e8 (ED25519)
8888/tcp open  sun-answerbook? syn-ack
| fingerprint-strings:
|   NCP:
|_    DmdT
2 services unrecognized despite returning data. If you know the service/ve
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

Fingerprint on network

```python
from gpiozero import PWMOutputDevice
from time import sleep

motor = PWMOutputDevice(18)

motor.frequency = 250
while True:
    motor.value = 0.3
    sleep(3)
    motor.value = 0.4
    sleep(3)
```

Attack script

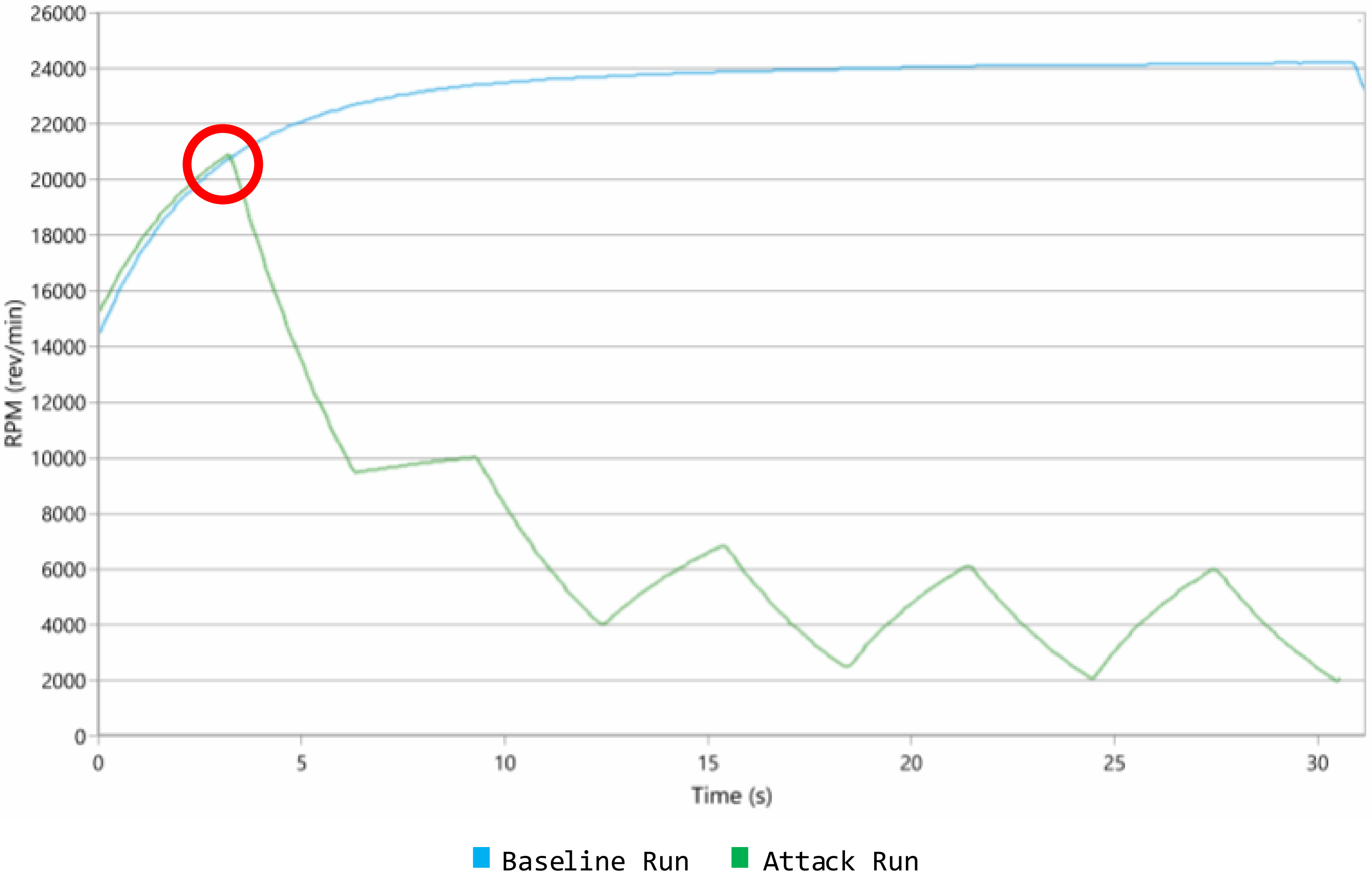
- Attacker has network access and observes remote GPIO
- Executes attack script: **PIGPIO_ADDR=192.168.1.4 python3 attack.py**

OPERATOR Attack Ex. 2
Remote Pin Control

Results:

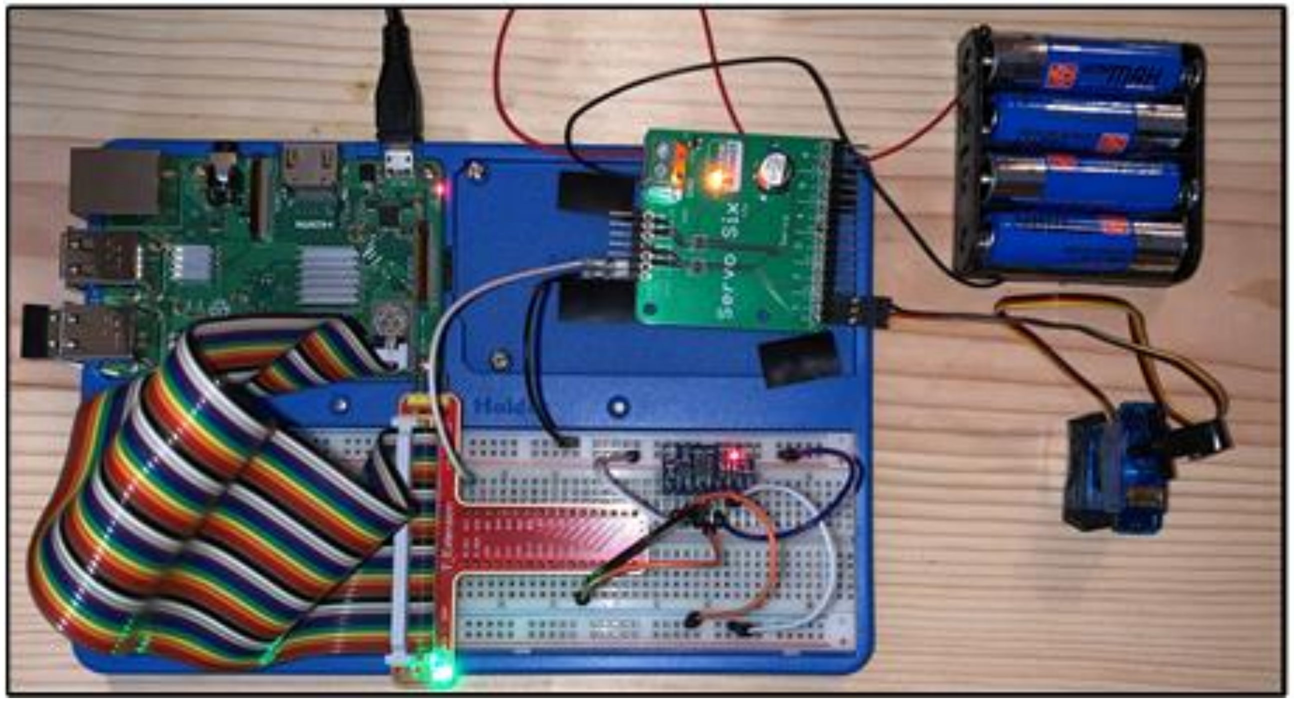
Control and Disrupt

RPM vs. Time

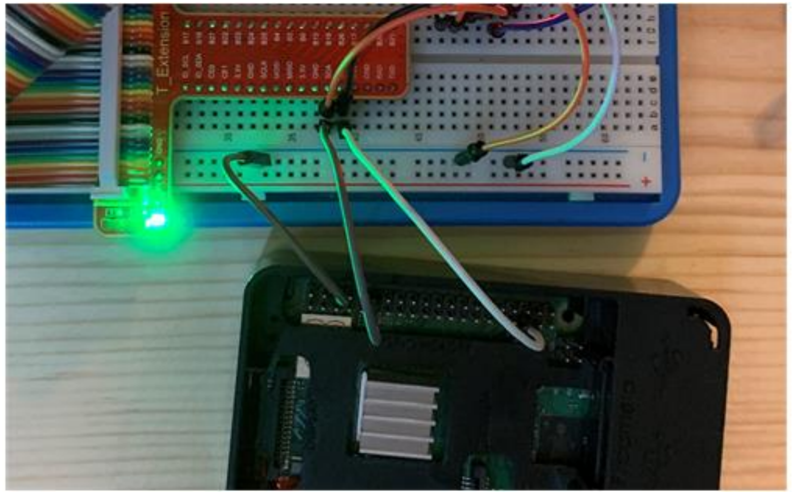


SENSOR Attack: Accelerometer Data Injection

Example Target: ADXL345 accelerometer used to control servo angle



SENSOR Attack:
Accelerometer Data Injection



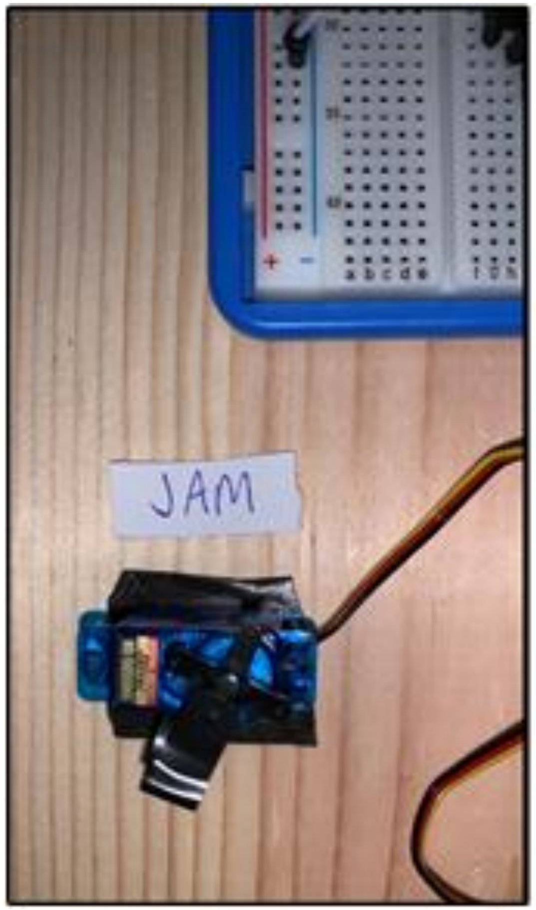
- Capture and decode I2C, 6 bytes sent for X, Y, Z
- Connecting attack Pi – observe I2C address 0x53

SENSOR Attack: Accelerometer Data Injection

- Set attack Pi as I2C slave
- Control bytes

Results:

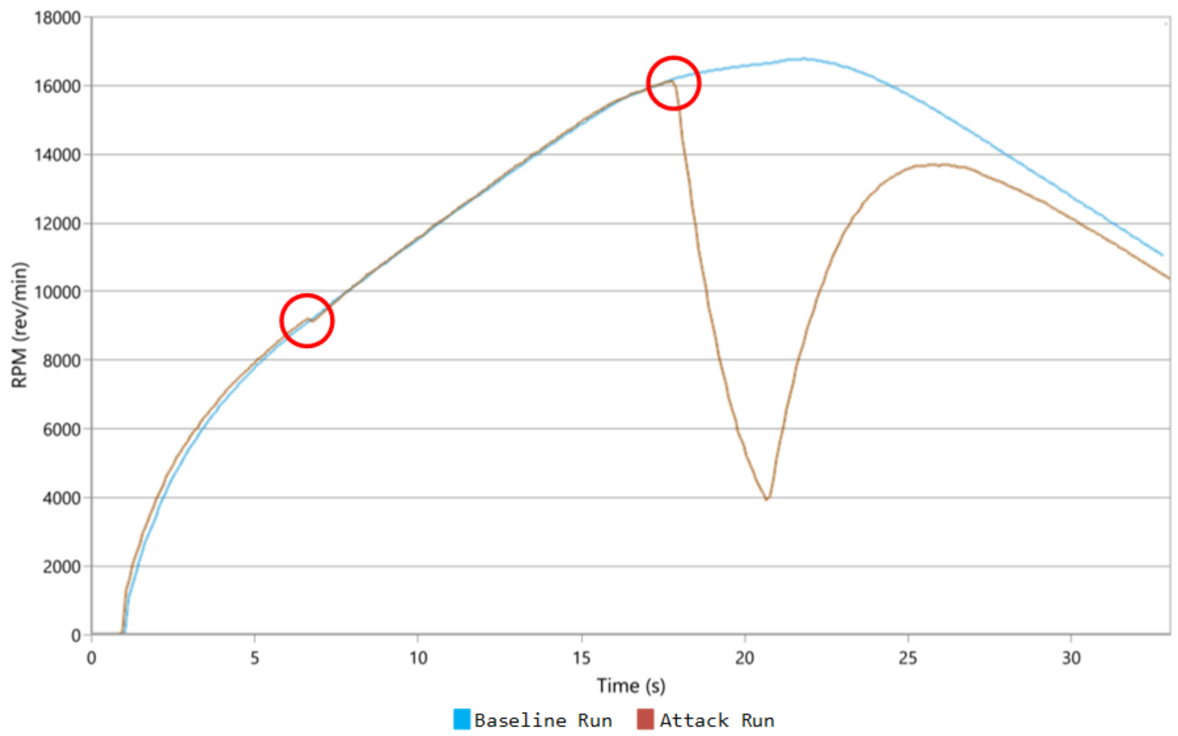
Control and Disrupt

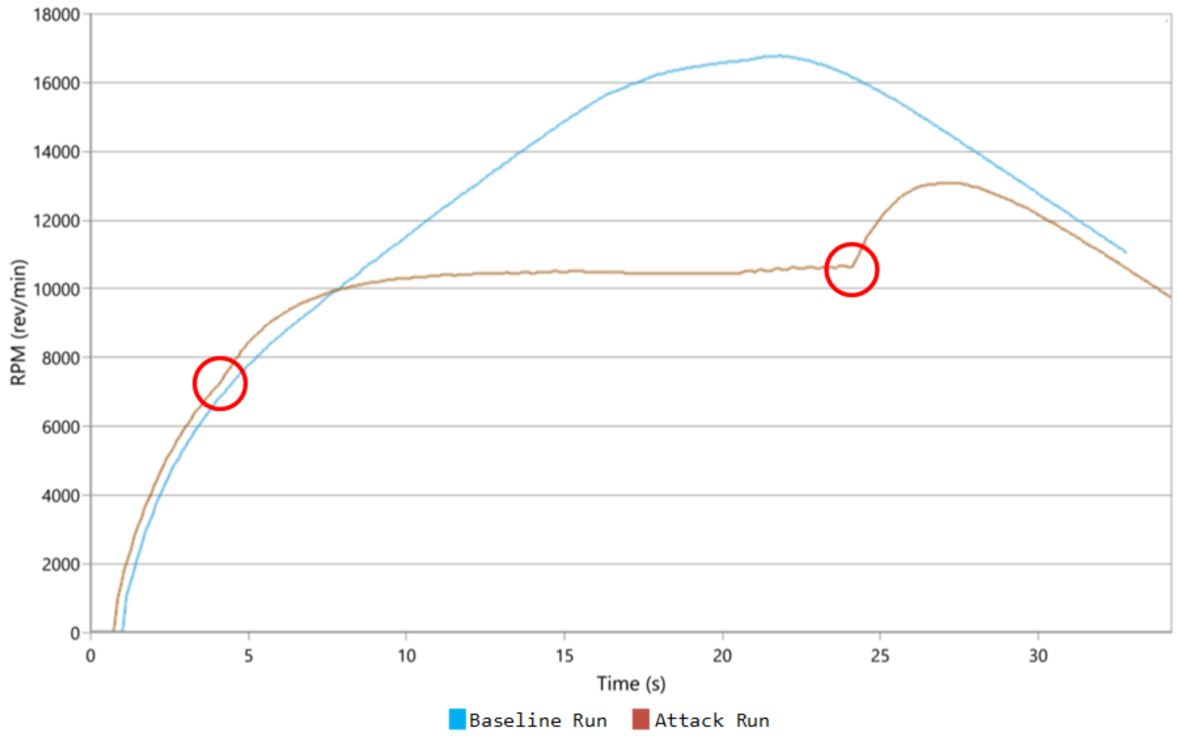


CONTROL Attack 1:
Timing Impacts of Discrete Command Injections on Motor Control

- Inject changes to duty cycle during operation

Results: Control and Disrupt; **RPM vs. Time**





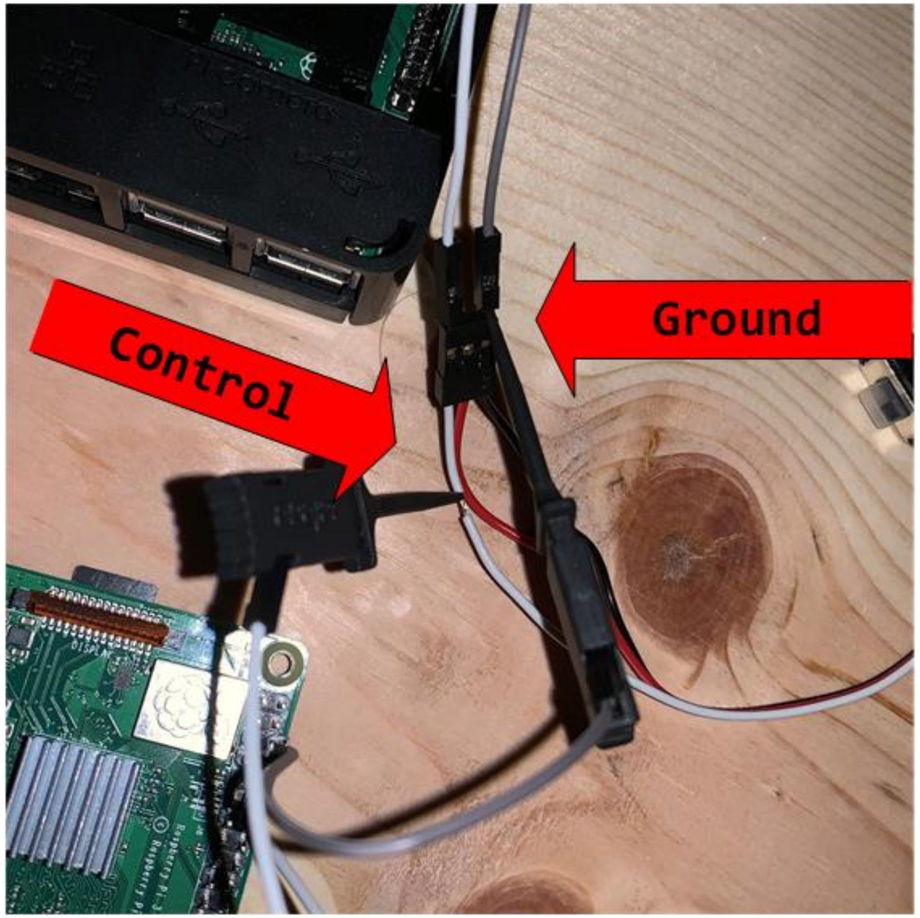
CONTROL Attack 2: Hardware Implant Targeting PWM Channel

Example Target:

CONTROL Attack 2:
Hardware Implant Targeting PWM Channel

- When PWM used as control signal, typically a 3-wire cable is used:

  - Black wire = ground
  - Red wire = current
  - White or yellow wire = control

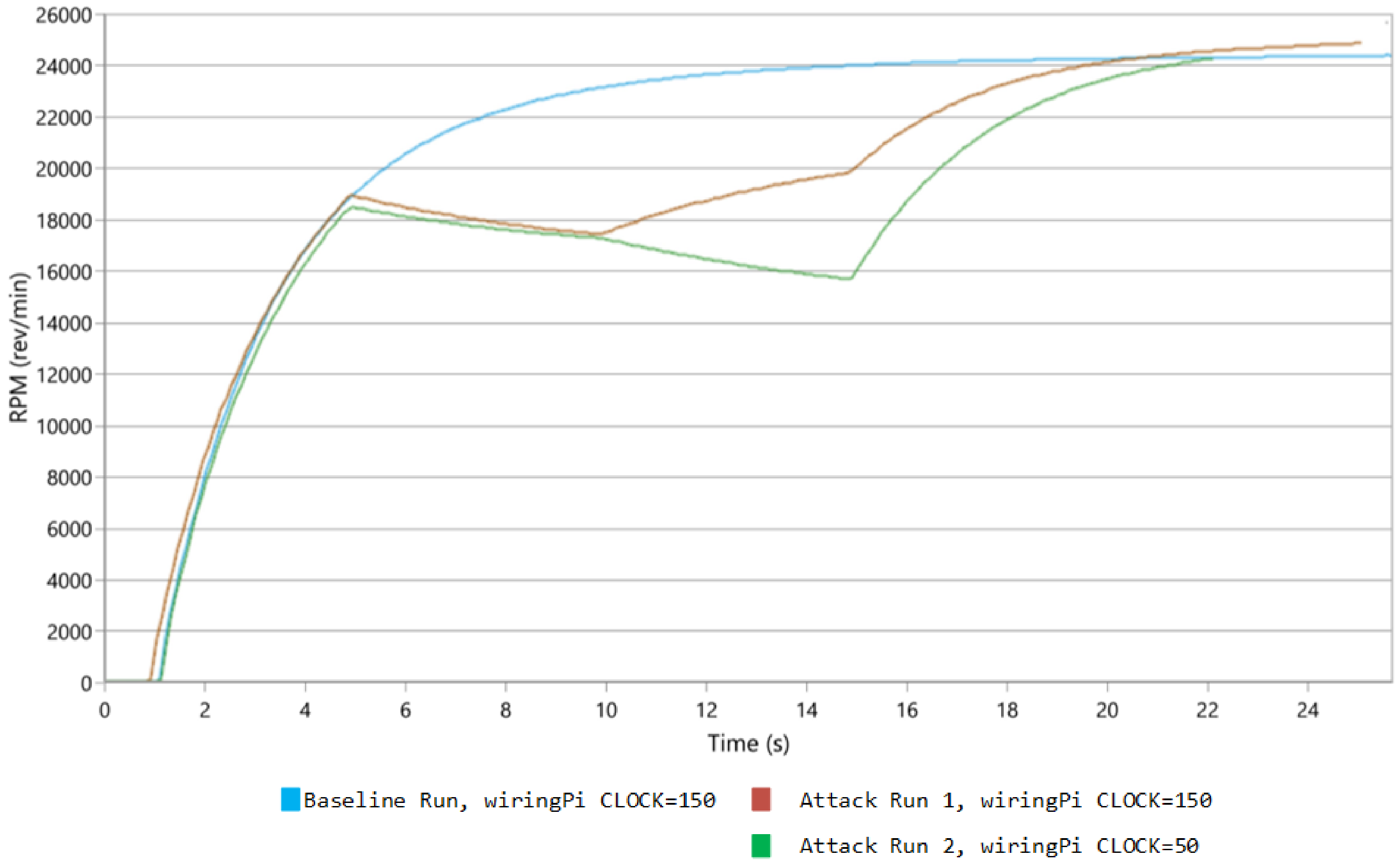


CONTROL Attack 2:
Hardware Implant Targeting PWM Channel

Results:

Control and Disrupt

RPM vs. Time



DRIVE Attacks: Pin Control and Configuration Attacks

- Attacks modify pin registers in Rpi 3 B+ SoC, Broadcom BCM2837
- Memory map physical memory locations using BCM2837 spec

```
#define PWM_CONTROL 0
#define PWM_STATUS  1
#define PWM0_RANGE  4
#define PWM0_DATA   5
#define PWM1_RANGE  8
#define PWM1_DATA   9
#define BLOCK_SIZE              (4*1024)

static volatile unsigned int piBase = 0x3F000000;
static volatile unsigned int *clk ;
static volatile unsigned int *gpio ;
static volatile unsigned int *pwm ;

GPIO_CLOCK_BASE = piBase + 0x00101000 ;
clk = (uint32_t *)mmap(0, BLOCK_SIZE, PROT_READ|PROT_WRITE, MAP_SHARED, fd, GPIO_CLOCK_BASE);

GPIO_BASE         = piBase + 0x00200000 ;
gpio = (uint32_t *)mmap(0, BLOCK_SIZE, PROT_READ|PROT_WRITE, MAP_SHARED, fd, GPIO_BASE);

GPIO_PWM          = piBase + 0x0020C000 ;
pwm = (uint32_t *)mmap(0, BLOCK_SIZE, PROT_READ|PROT_WRITE, MAP_SHARED, fd, GPIO_PWM);
```

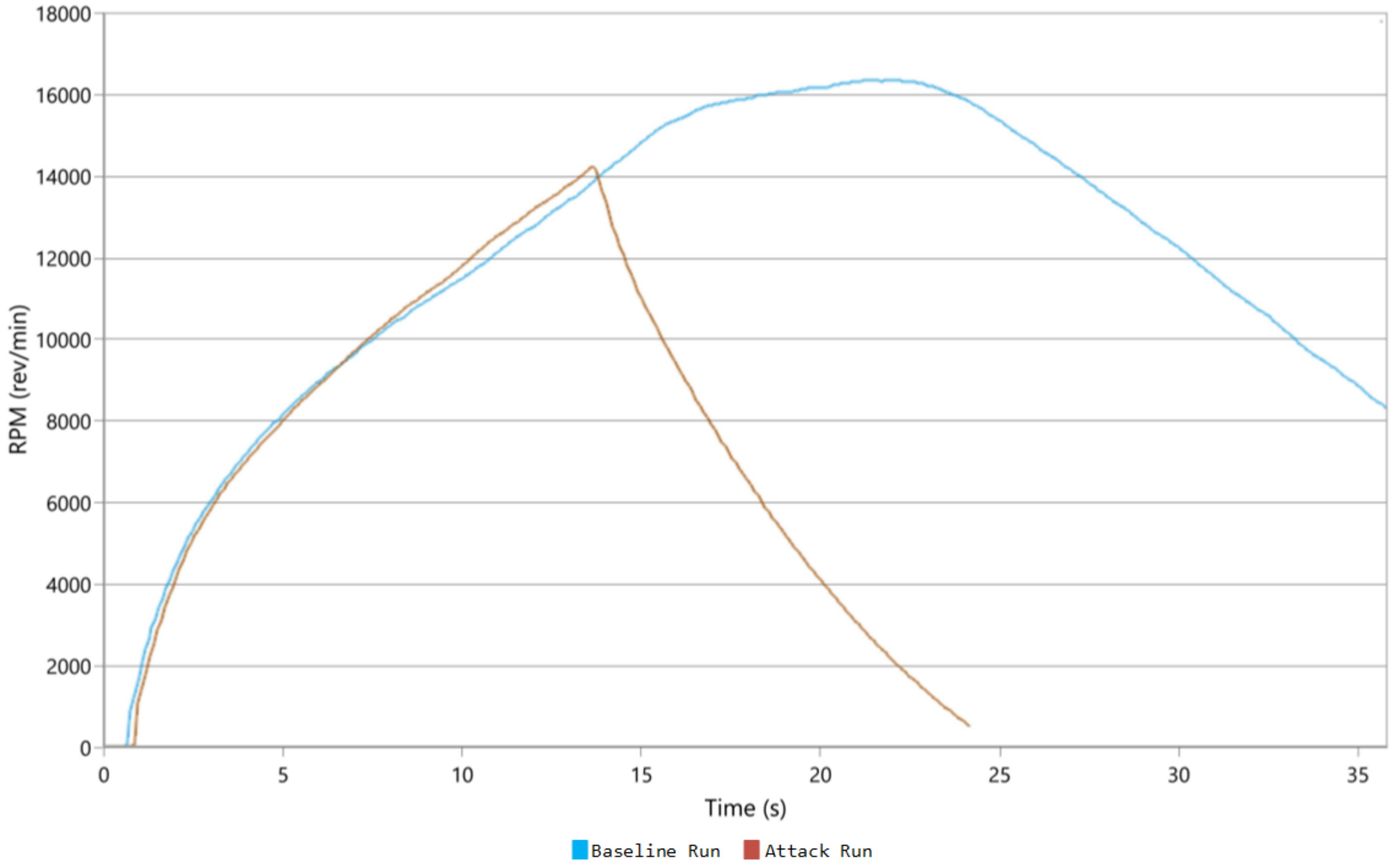
DRIVE Attacks:
Pin Control and Configuration Attacks

- Attack 1: Change pin to INPUT during operation

Results:

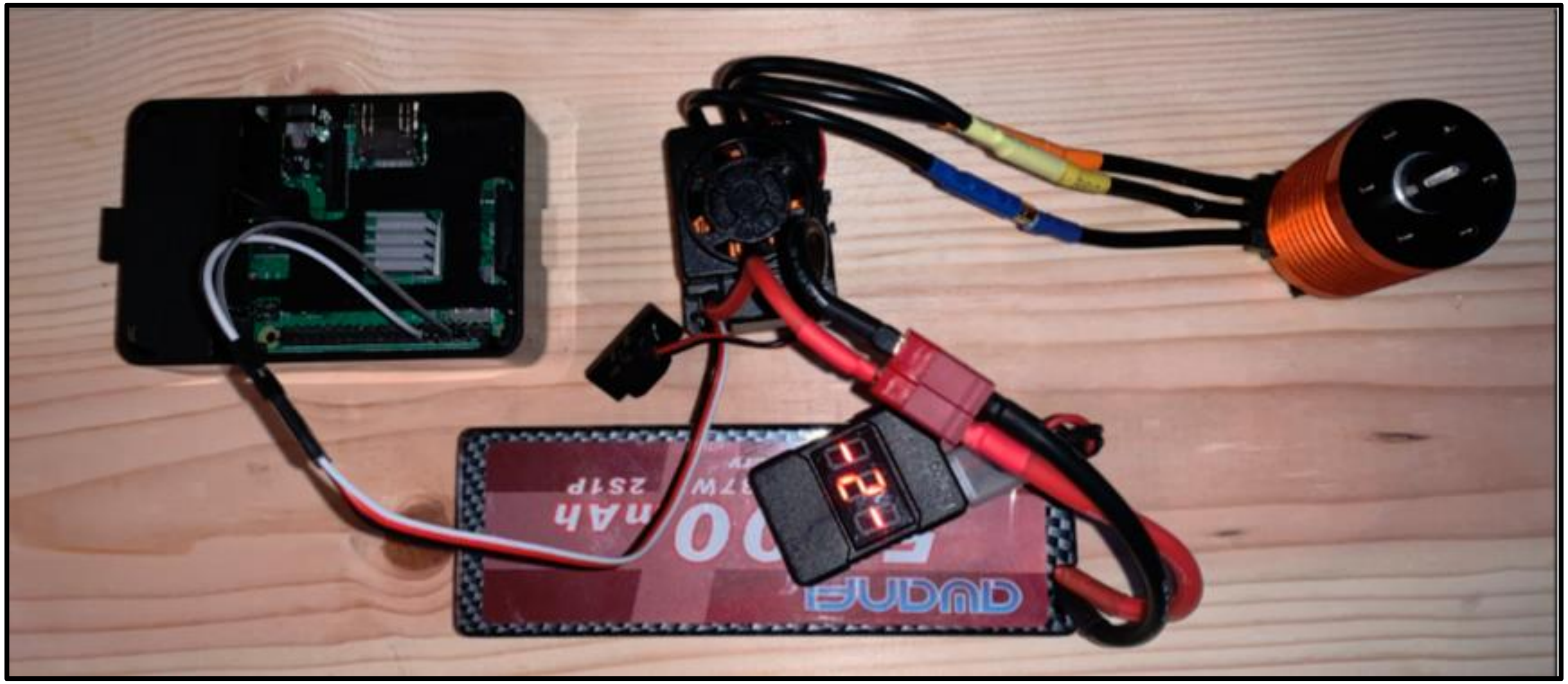
Control and Disrupt

RPM vs. Time



DRIVE Attacks:
Pin Control and Configuration Attacks

- Attack 2: Modify PWM CLOCK and DATA on BCM2837 to identify behavioral changes to motor
- Target:



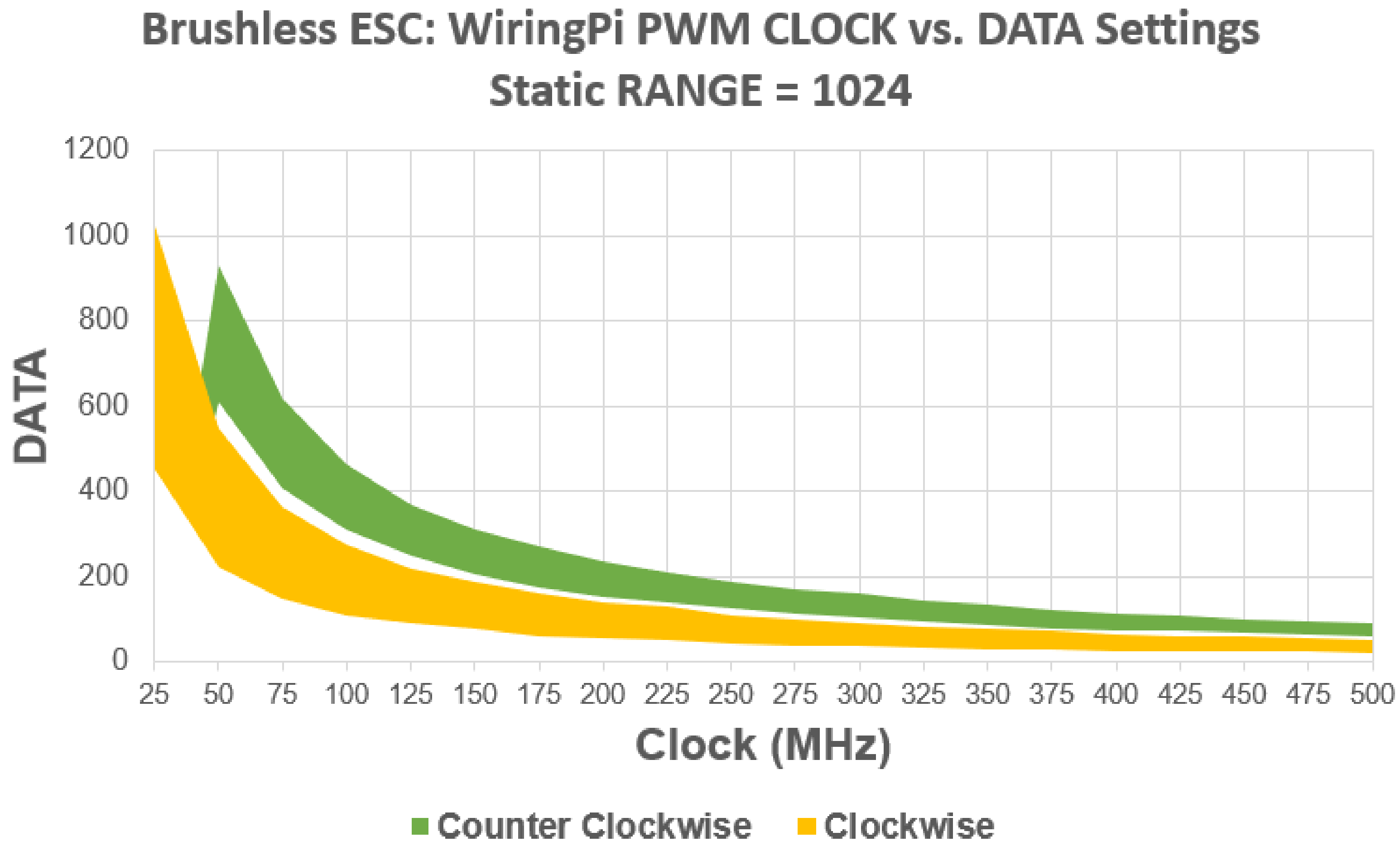
DRIVE Attacks:
Pin Control and Configuration Attacks

Results:

Control and Disrupt

DATA vs. CLOCK

w/ Static RANGE



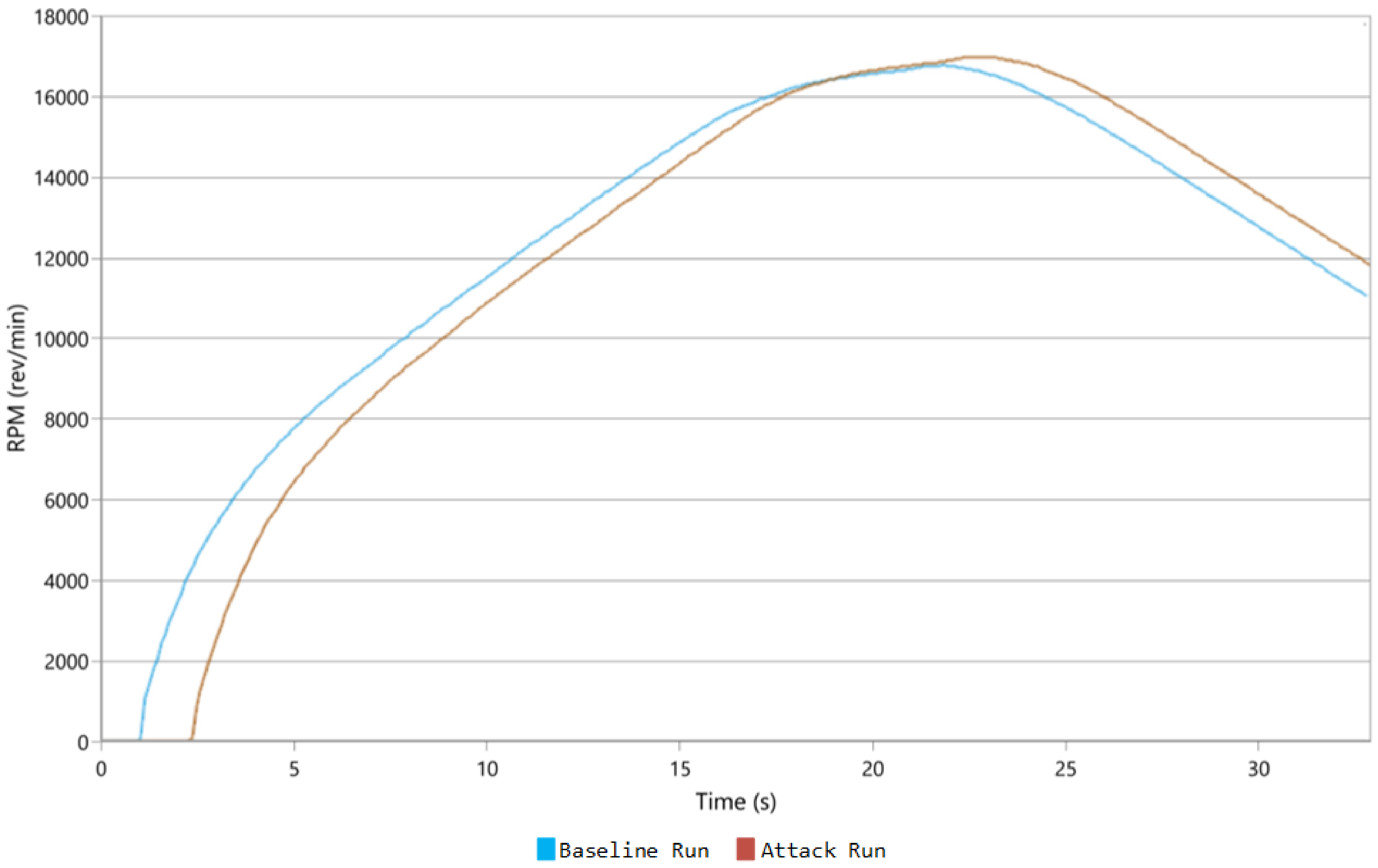
DRIVE Attacks: Pin Control and Configuration Attacks

- Attack 3: Record and playback PWM registers

Results:

Control and Disrupt

RPM vs. Time



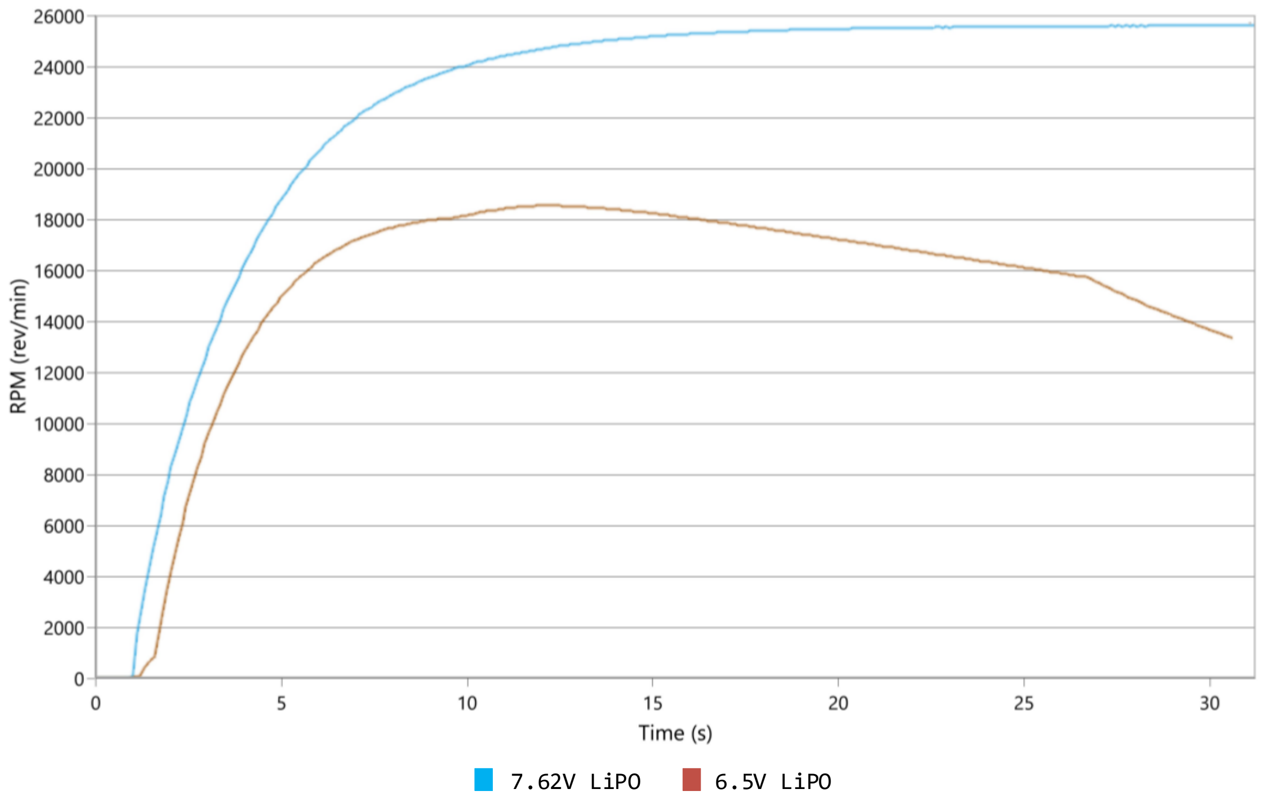
POWER Attack: Motor Performance due to Low Voltage

- Test run with low voltage LiPO battery

Results:

Disrupt

RPM vs. Time



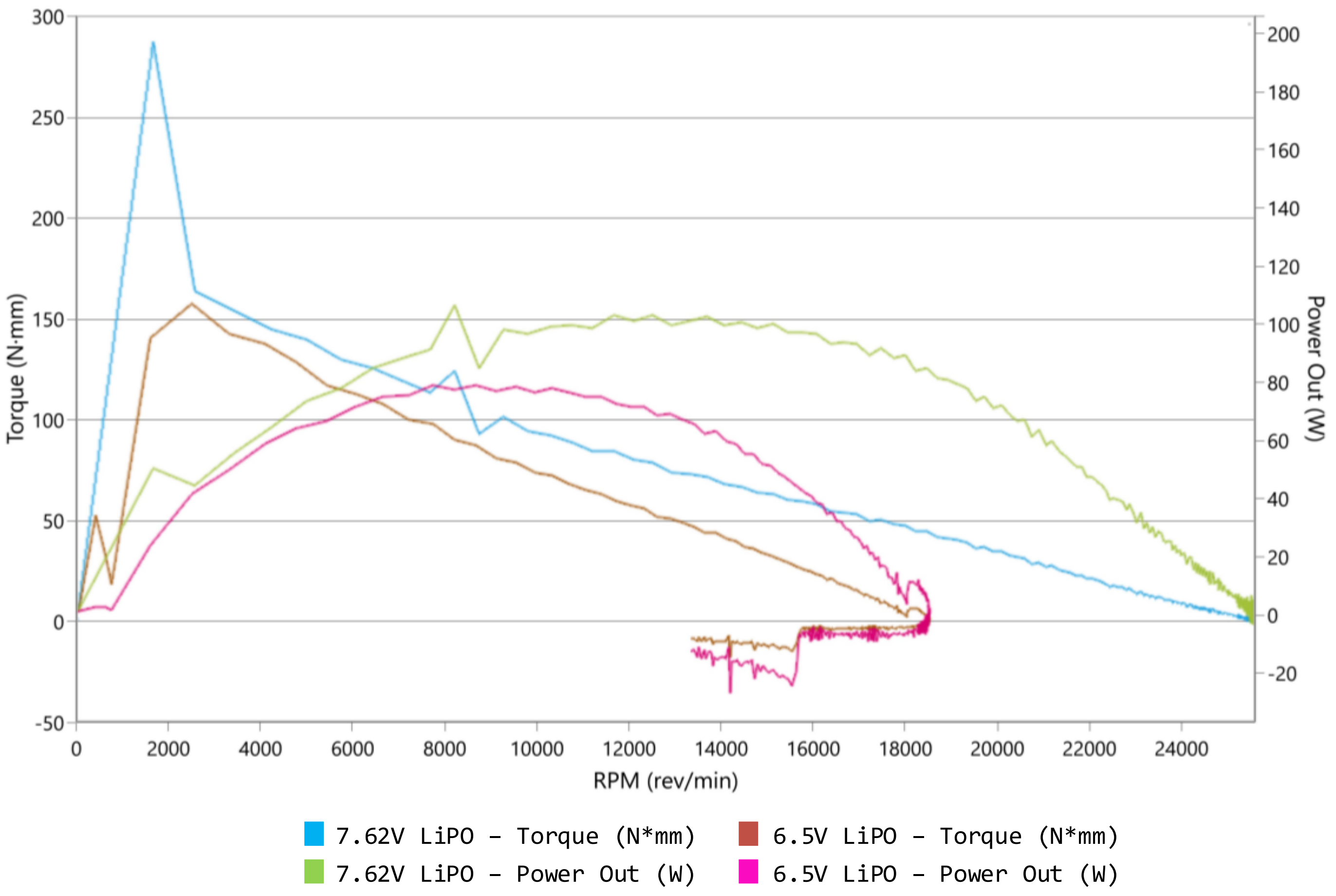
NOTE: LiPO batteries should never be used in low voltage (may overheat or worse)

POWER Attack:
Motor Performance due to Low Voltage

Results:

Disrupt

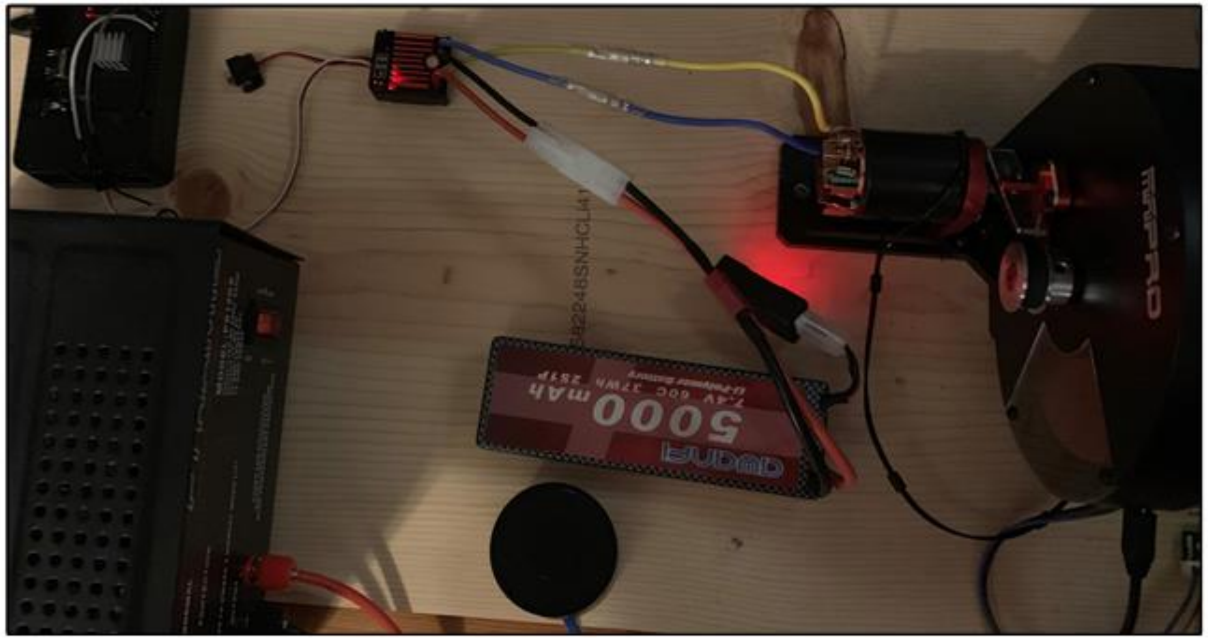
Torque and Power Output vs. Speed

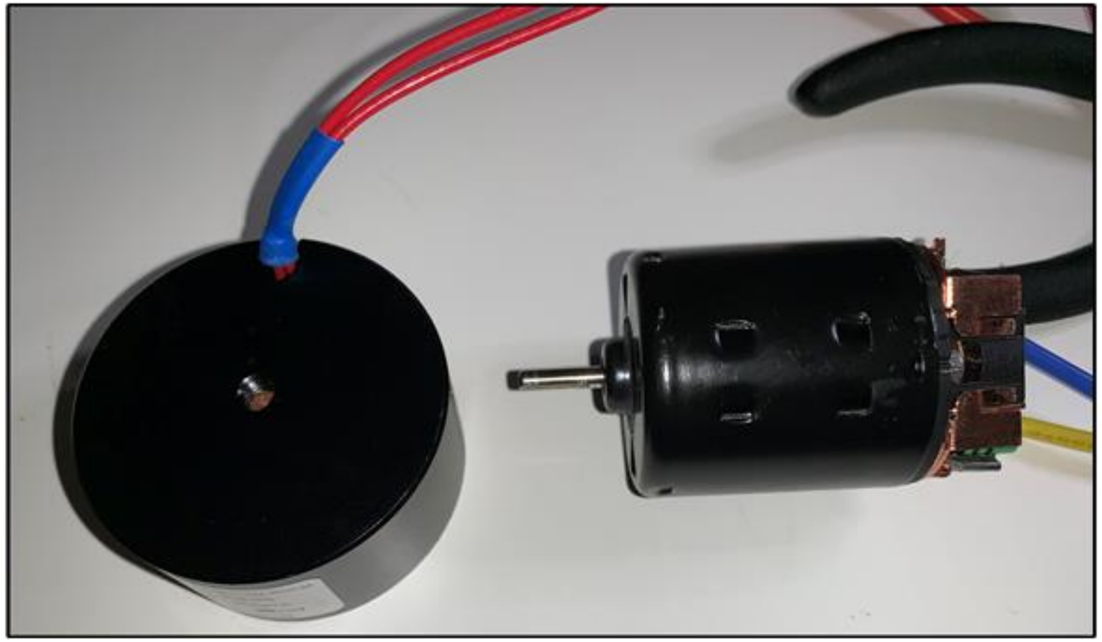


NOTE: LiPO batteries should never be used in low voltage (may overheat or worse)

MOTOR Attack 1: Motor Performance in Presence of External Electromagnet

- Introduced electromagnet (500N suction) to target during run to observe behavior



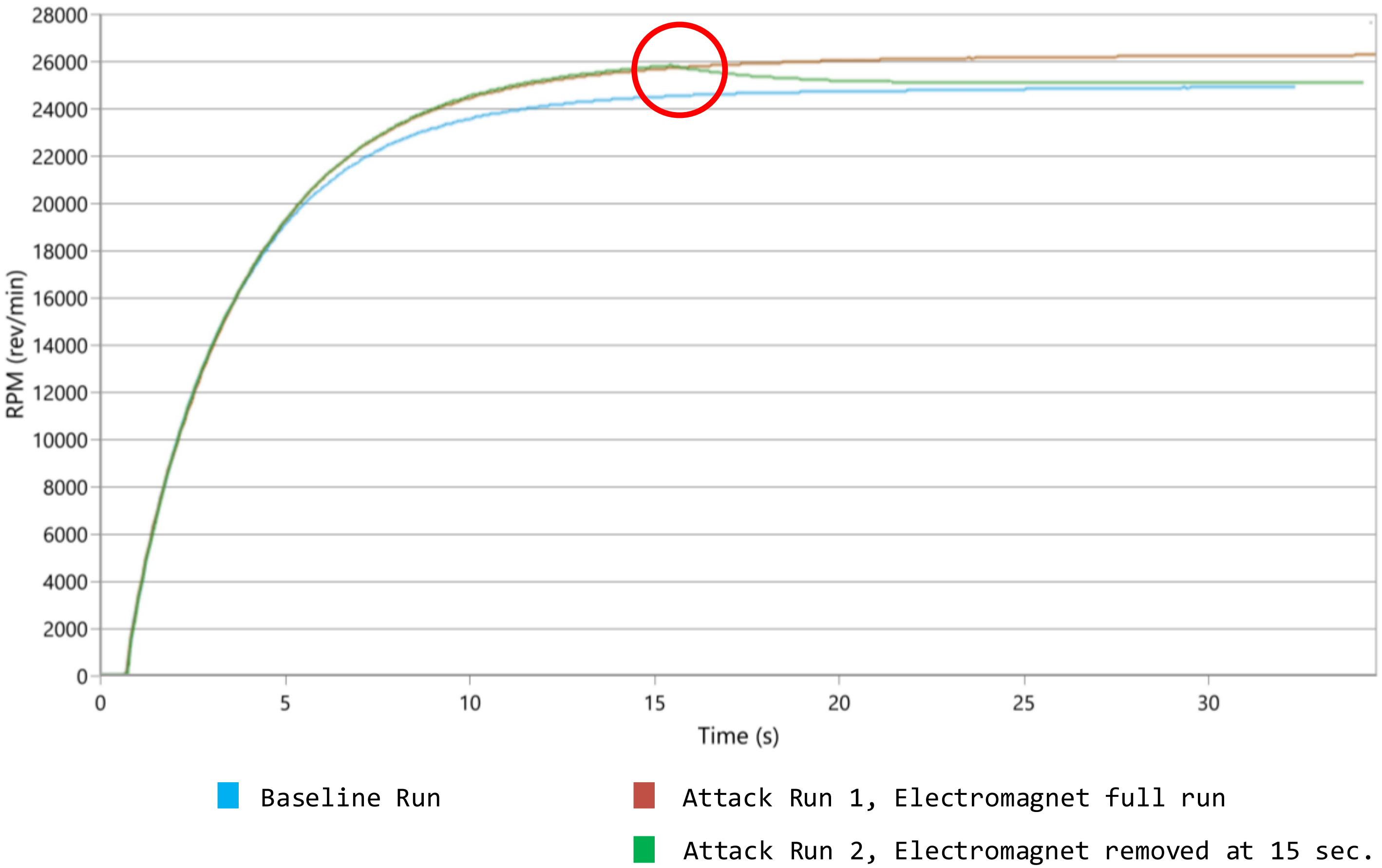


MOTOR Attack 1:
Motor Performance in Presence of External Electromagnet

Results:

Disrupt

RPM vs. Time



MOTOR Attack 1:
Motor Performance in Presence of External Electromagnet

Results:

Disrupt

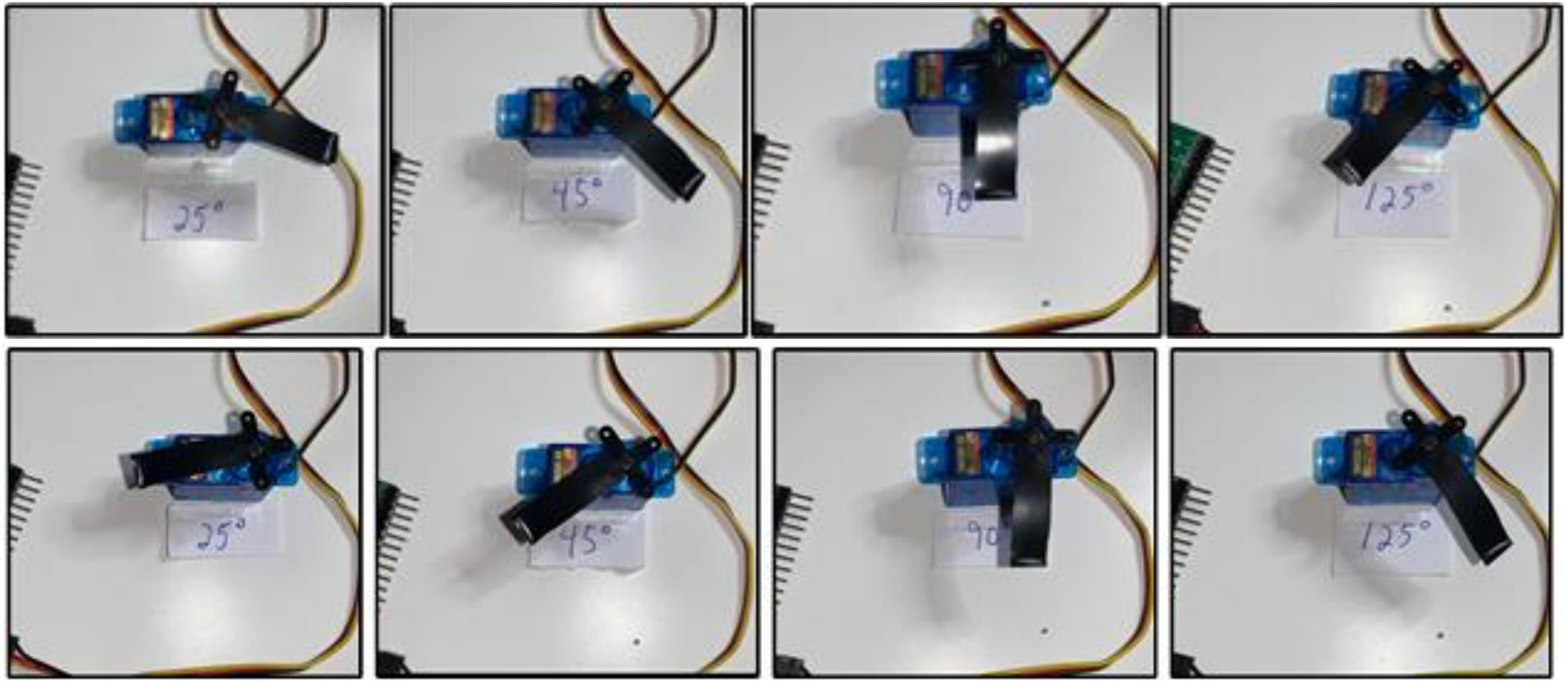
Torque and Power Output vs. Speed

MOTOR Attack 2: Reprogramming Digital Servo Motor

- Digital servo manufacturers provide programming tools
- Identify motor type and procure programmer – no auth!
- Target and programmer:

MOTOR Attack 2: Reprogramming Digital Servo Motor

- Expected behavior (top, CW) vs. reprogrammed (bot, CCW):



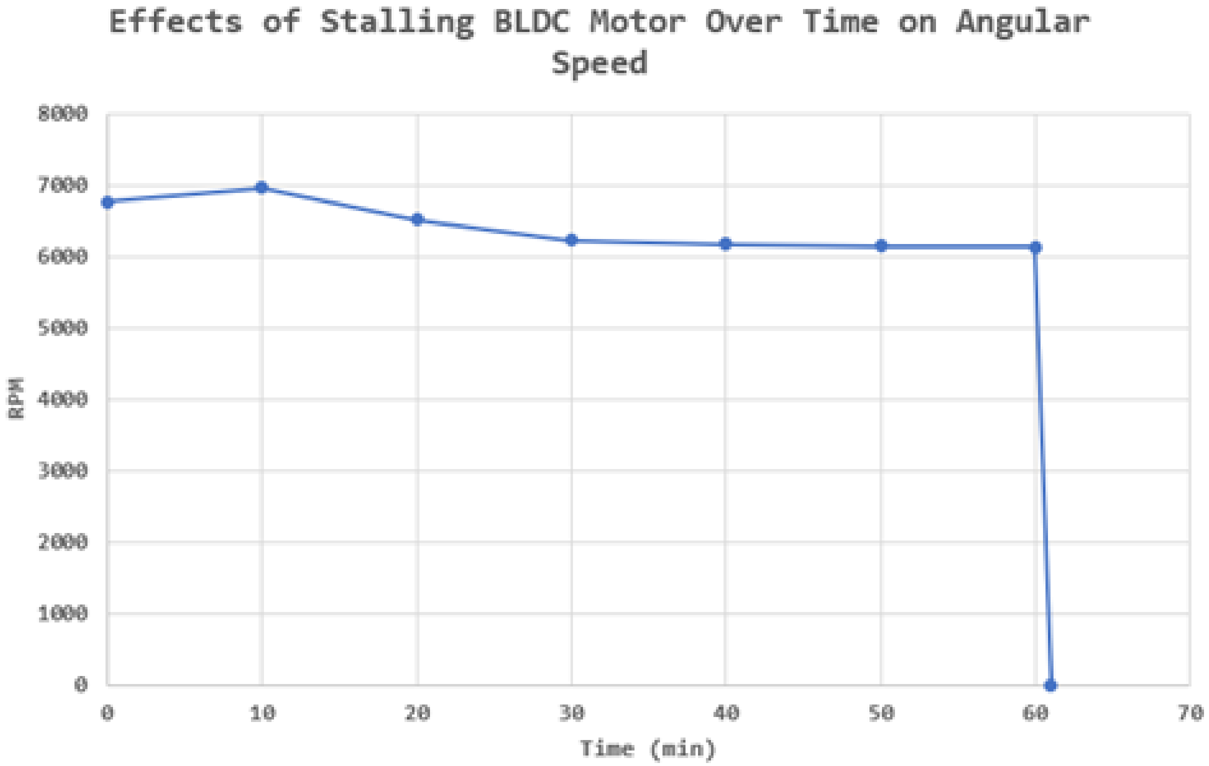
LOAD Attack: Overheating and Stalling a Motor

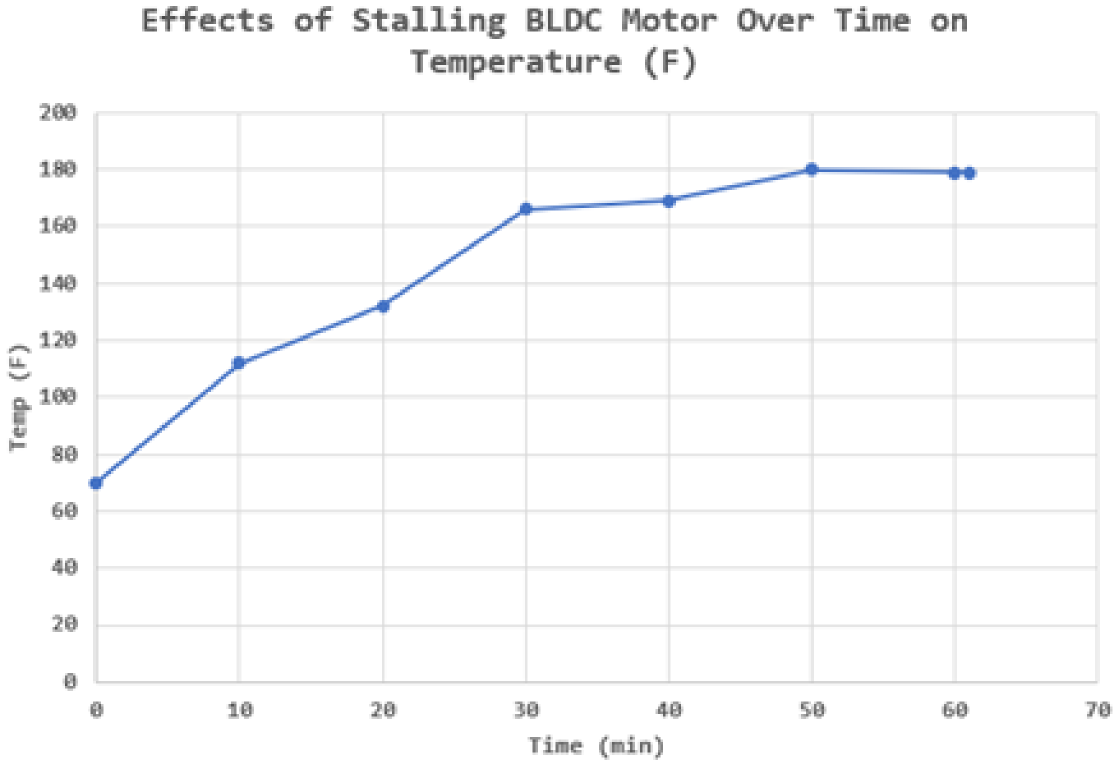
- Target desk fan:

LOAD Attack:
Overheating and Stalling a Motor

- Overheated to ~180° F and motor died at 61-min mark

Results: *Disrupt*

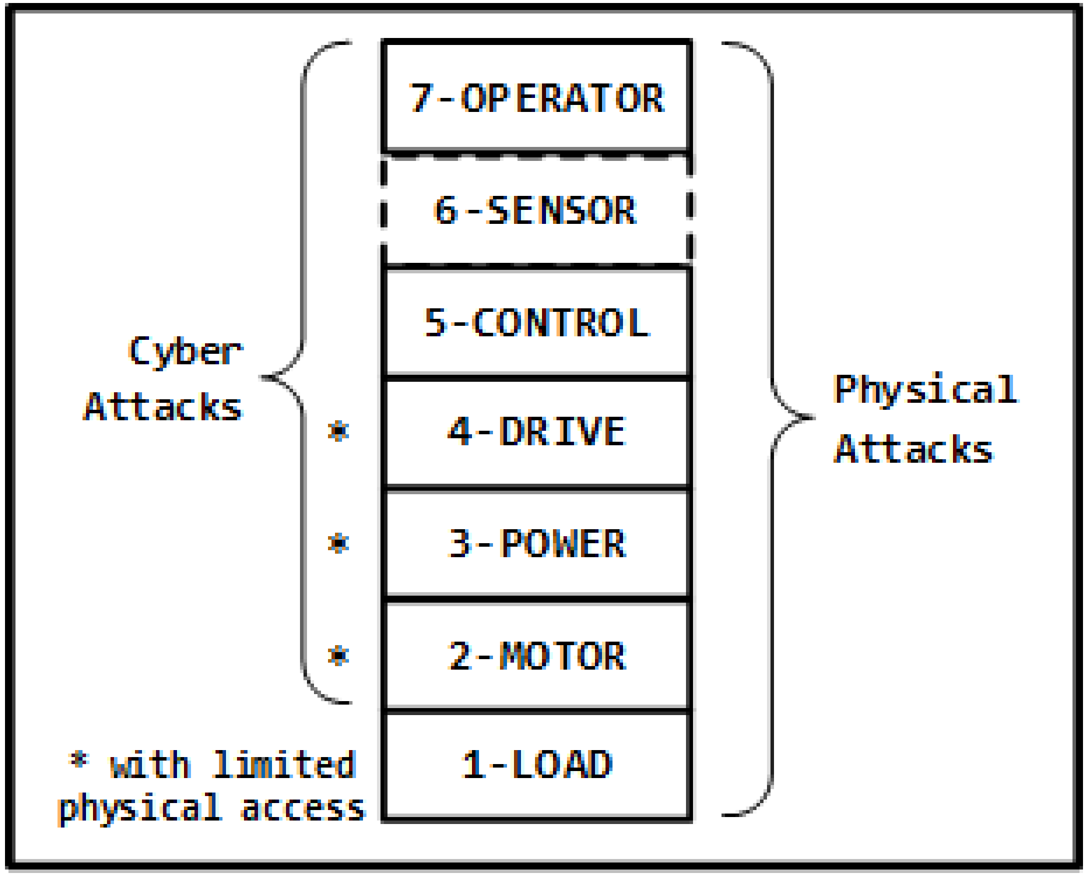




LOAD Attack:
Overheating and Stalling a Motor

- Brushless motor comparison between dead and good fan
- No visual difference

Motor Threat Model Redux



Start Over:
Hypothetical Problem Scenario

- **Your next risk assessment target:**

  A Proprietary Drone System

- Thousands deployed worldwide for package delivery
  - 30 different drone models were dev’ed
  - Hundreds of operators…
  - With physical and remote access…
  - And… background checks aren’t required.
  - Over the Internet.

- **WHAT IS THE ATTACK SURFACE?**

  (and we need your response **NOW**!)

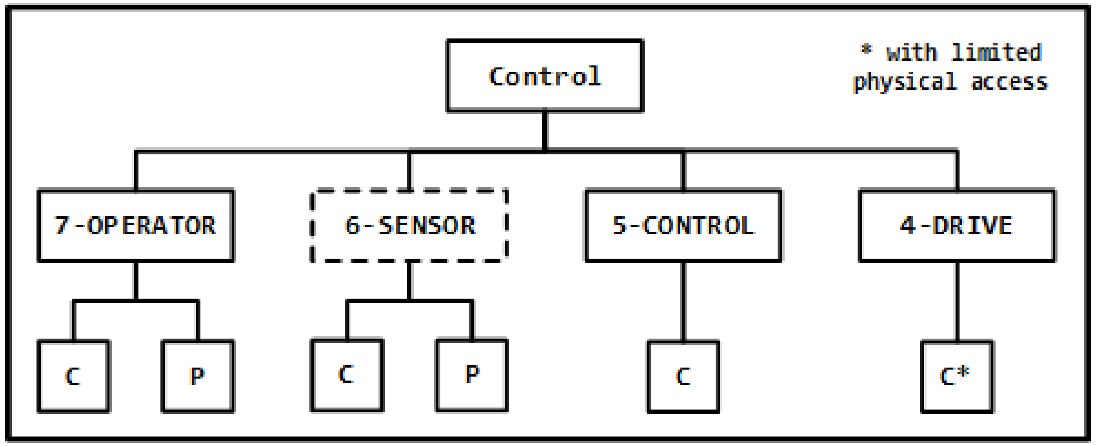
Attacker Model for Drone System

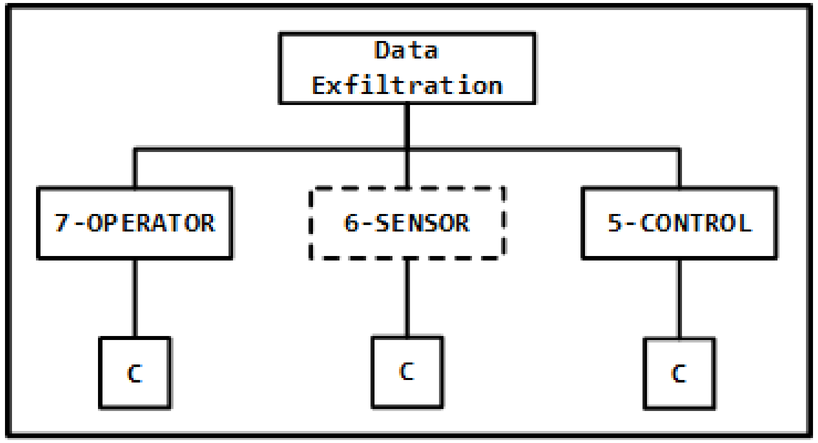
- **Nation State** – C & P; Offensive campaigns directed at accomplishing some mission; Many resources
- **Cybercriminal** – C; Motivated by data collection
- **Terrorist** – C; Motivated by spreading fear
- **Insider** – C or P; Disgruntled employee or social engineering victim

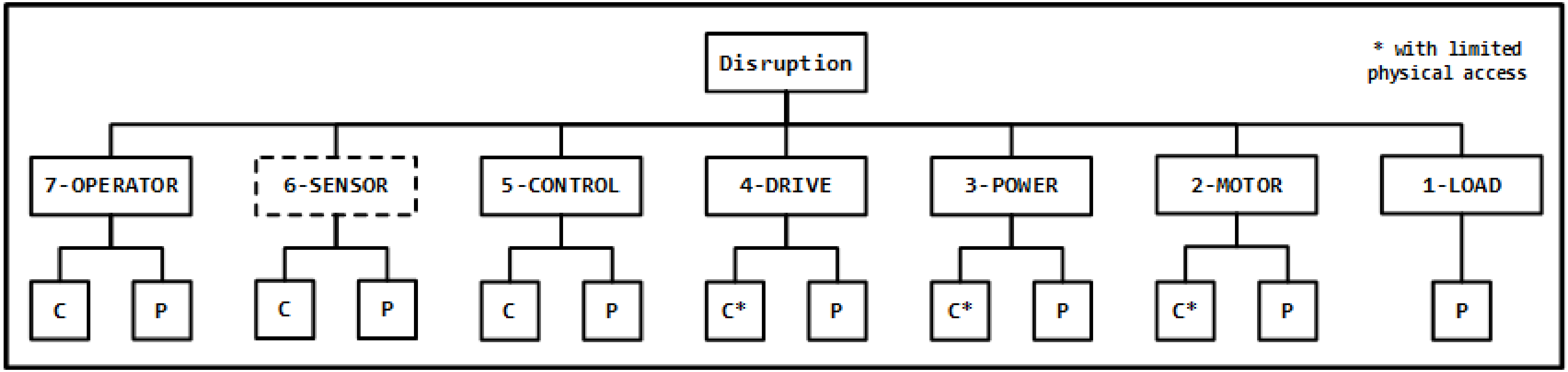
Refined Attack Objectives for Targeting Drone Movement

- **Control –**
  - Steal property
  - Alter predictable movements
- **Disrupt –**
  - Physical damage
  - Physical harm
  - Prevent movement
- **Data Exfiltration –**
  - Privacy Invasion

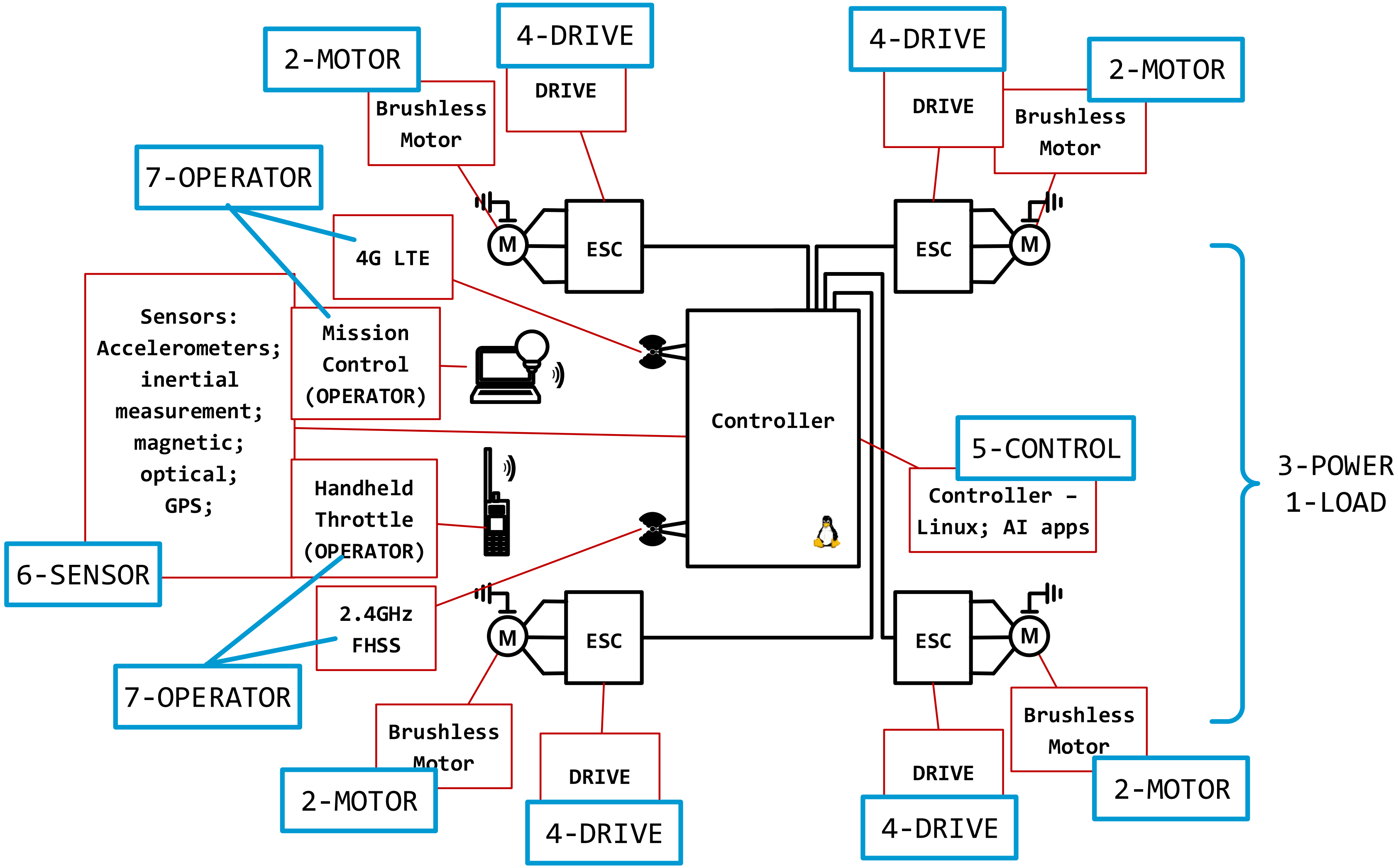
Movement Focused Attack Trees



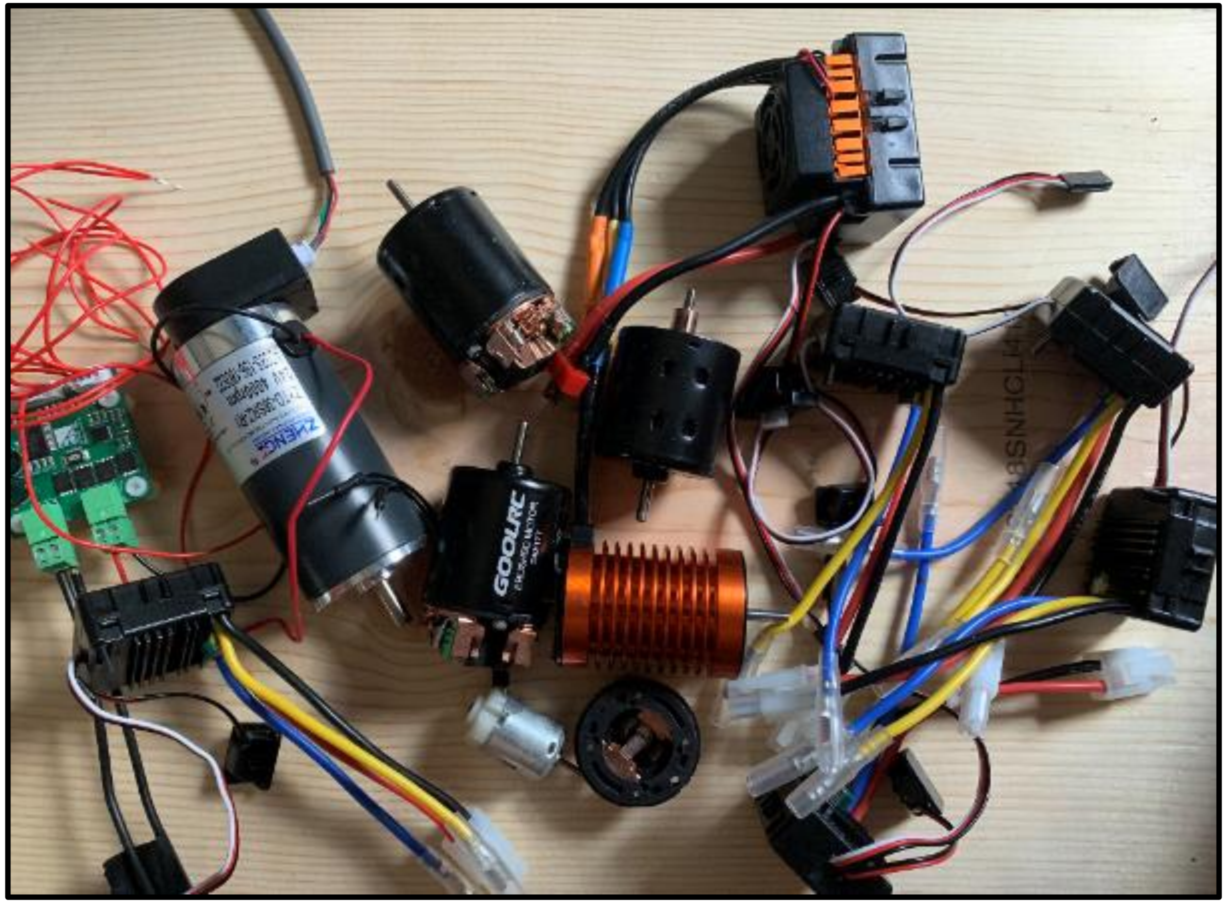




MTM Application for Finding Movement Threats



Experimental Boneyard



Thanks!

Backup Slides

The OPERATOR Layer

- *Unprivileged* motion control (most of the time)
- **2 levels of access:**
  1. Operator interface
  2. OPERATOR-CONTROL channel
- **Type**: cyber and physical
- **Objectives**: control, disrupt, data exfiltration

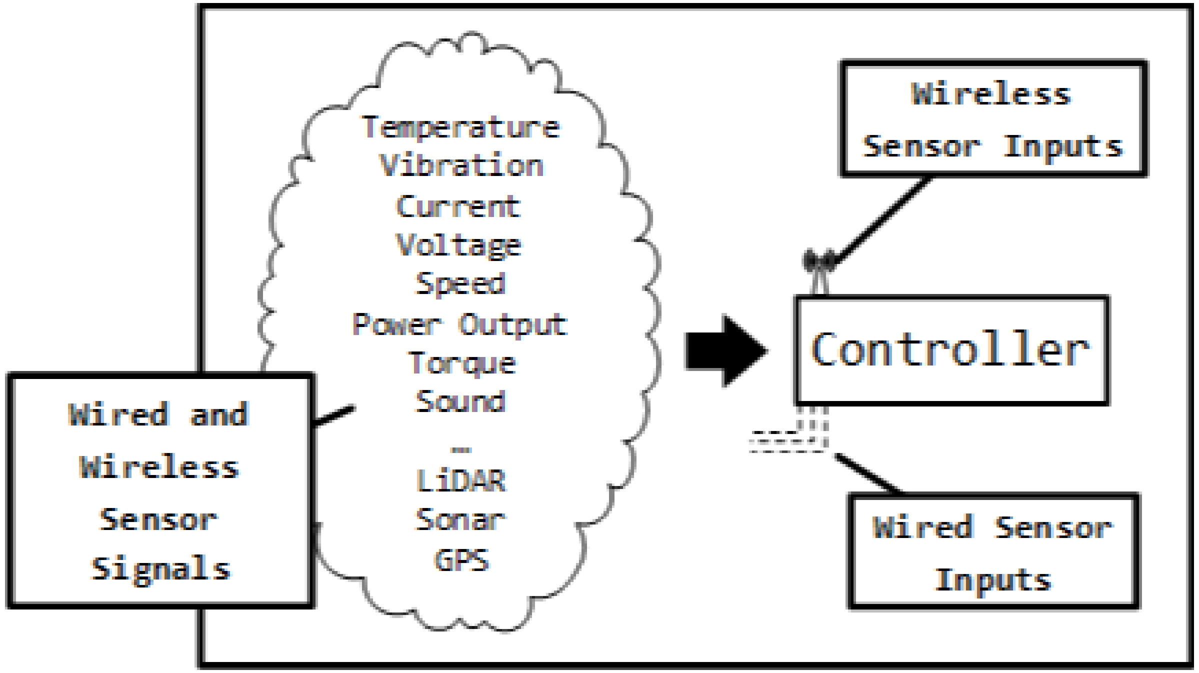
The SENSOR Layer

- Provides input data about physical environment

- **2 levels of access**:
  1. Sensors
  2. Out-of-Band Safety Systems (TRITON)

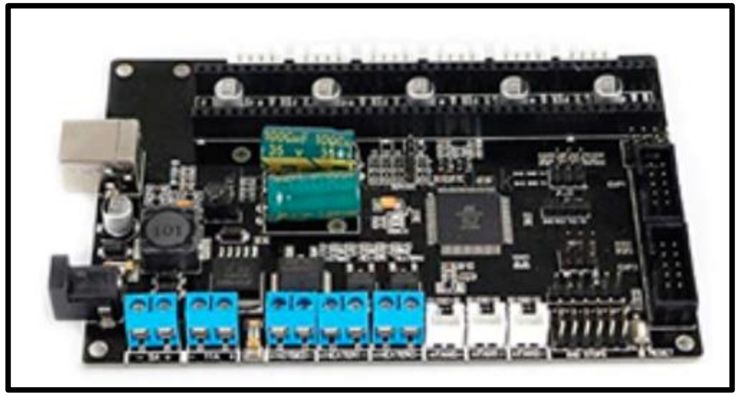
- **Type**: cyber and physical

- **Objectives**: control, disrupt, data exfiltration



The CONTROL Layer

- Privileged motion control (root!)
- **2 levels of access**:
  1. Controller
  2. CONTROL-DRIVE Channel
- **Type**: cyber and physical
- **Objectives**: control, disrupt, data exfiltration



The DRIVE Layer

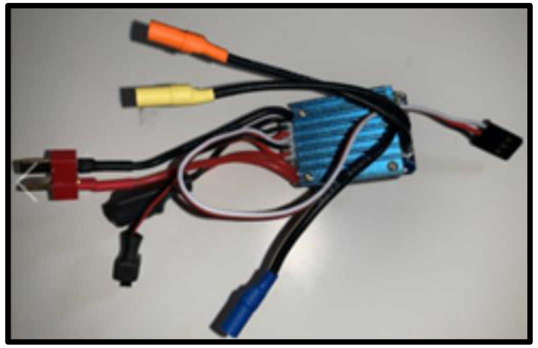
- Modify motor properties during operation

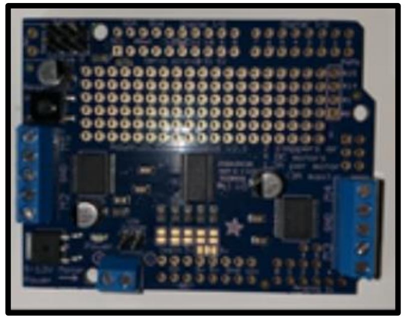
- **2 levels of access**:
  1. Controller
  2. CONTROL-DRIVE Channel

- **Type**: cyber* and physical

- **Objectives**: control and disrupt

* With limited physical access





The POWER LAYER

- Prevent or degrade motor performance

- **1 level of access:**
  - Targeting power input

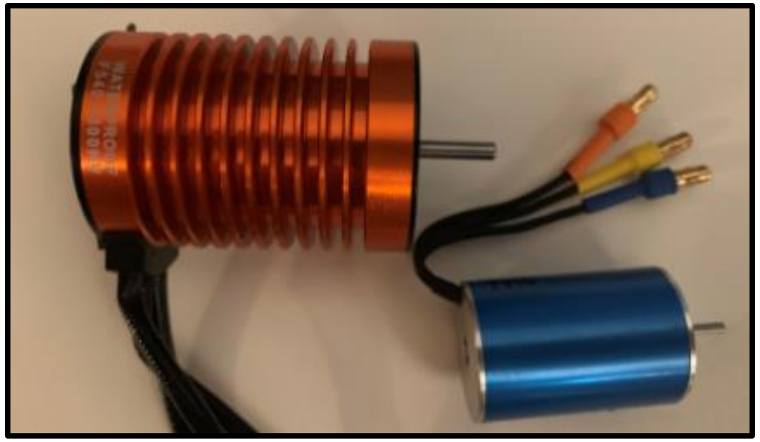
- **Type:** cyber* and physical

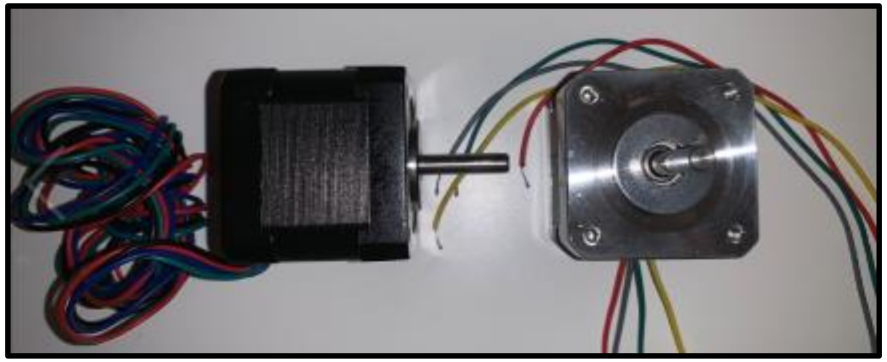
- **Objective:** disrupt

* With limited physical access

The MOTOR Layer

- Disruption of movement at the source of mechanical power
- **1 level of access**:
  - Targeting the motor
- **Type**: cyber* and physical
- **Objective**: disrupt





* With limited physical access

The LOAD Layer

- Movement prevention by overloading the system
- **1 level of access**:
  - Targeting the output system
- **Type**: physical
- **Objective**: disrupt