Is Your ECU Really Yours?

Abbas Ali, Hafiz Malik
University of Michigan-Dearborn

Code · Data · Models
Zenodo — scan to access

4th USENIX Symposium on Vehicle Security and Privacy (VehicleSec '26)
August 2026 · Baltimore, MD, USA

INFORMATION SYSTEMS, SECURITY AND FORENSICS

VehicleSec '26

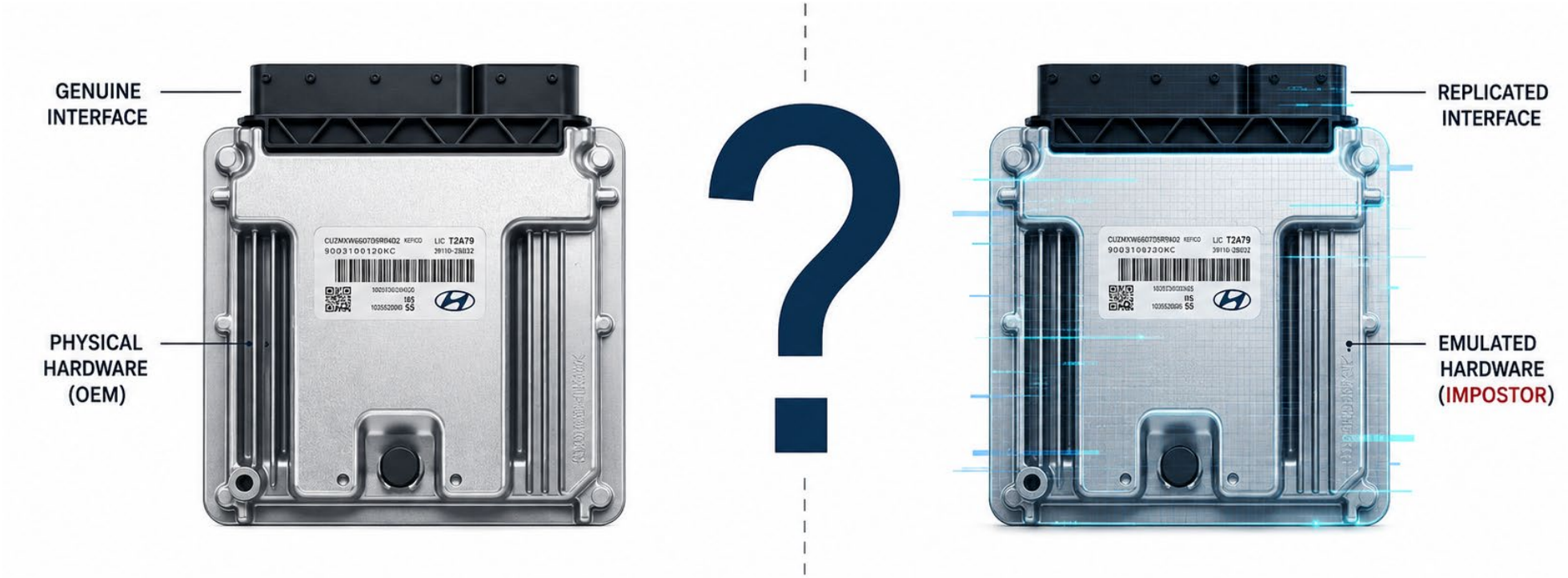
USENIX
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

DEARBORN

Talk Outline

- **Motivation & Problem**
- **Related Work & the Gap**
- **Our Approach:** Physical-Layer Fingerprinting
- **Methodology & Pipeline**
- **Experimental Results**
- **Conclusion & Future Work**
- **Q&A**

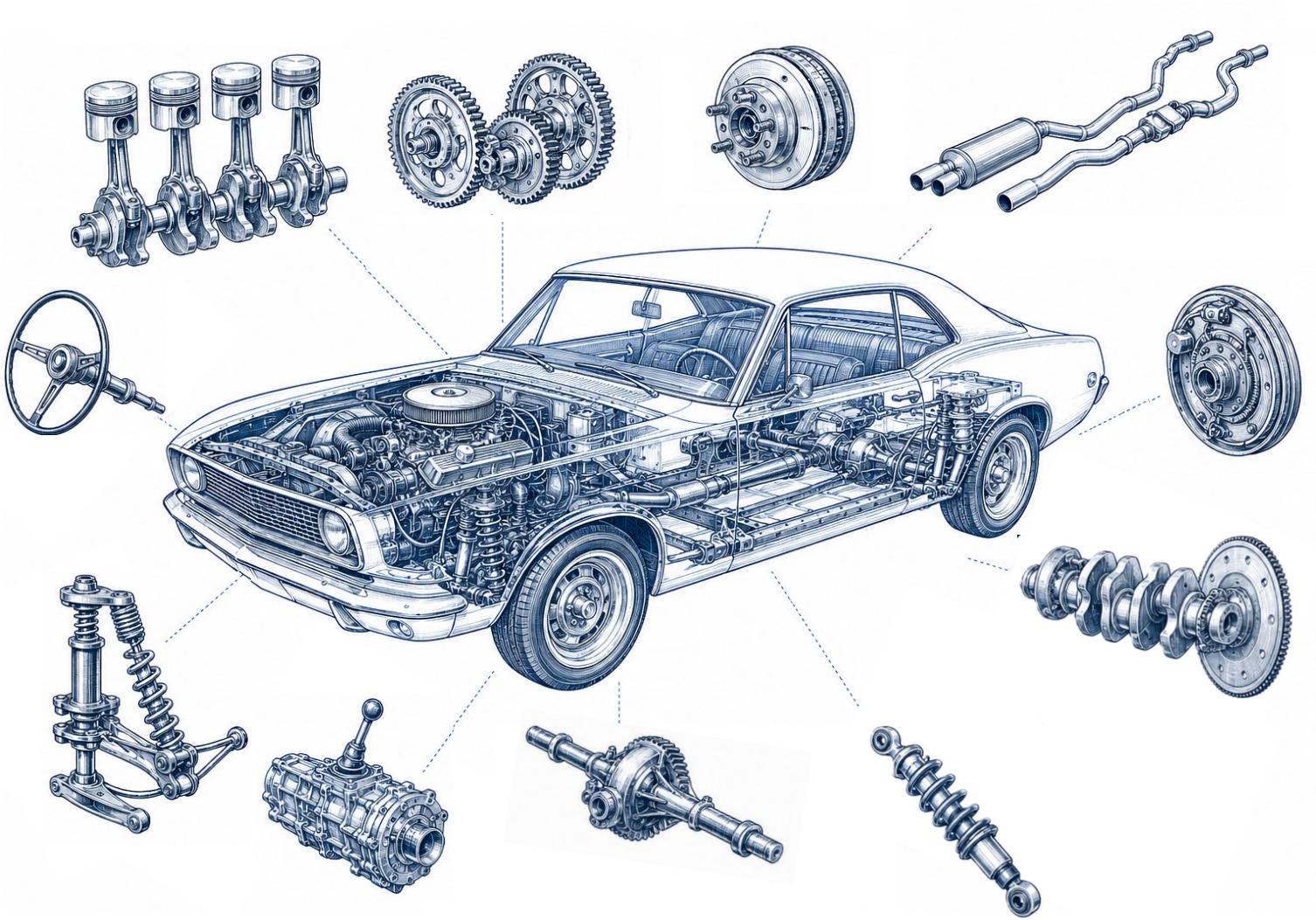
Motivation



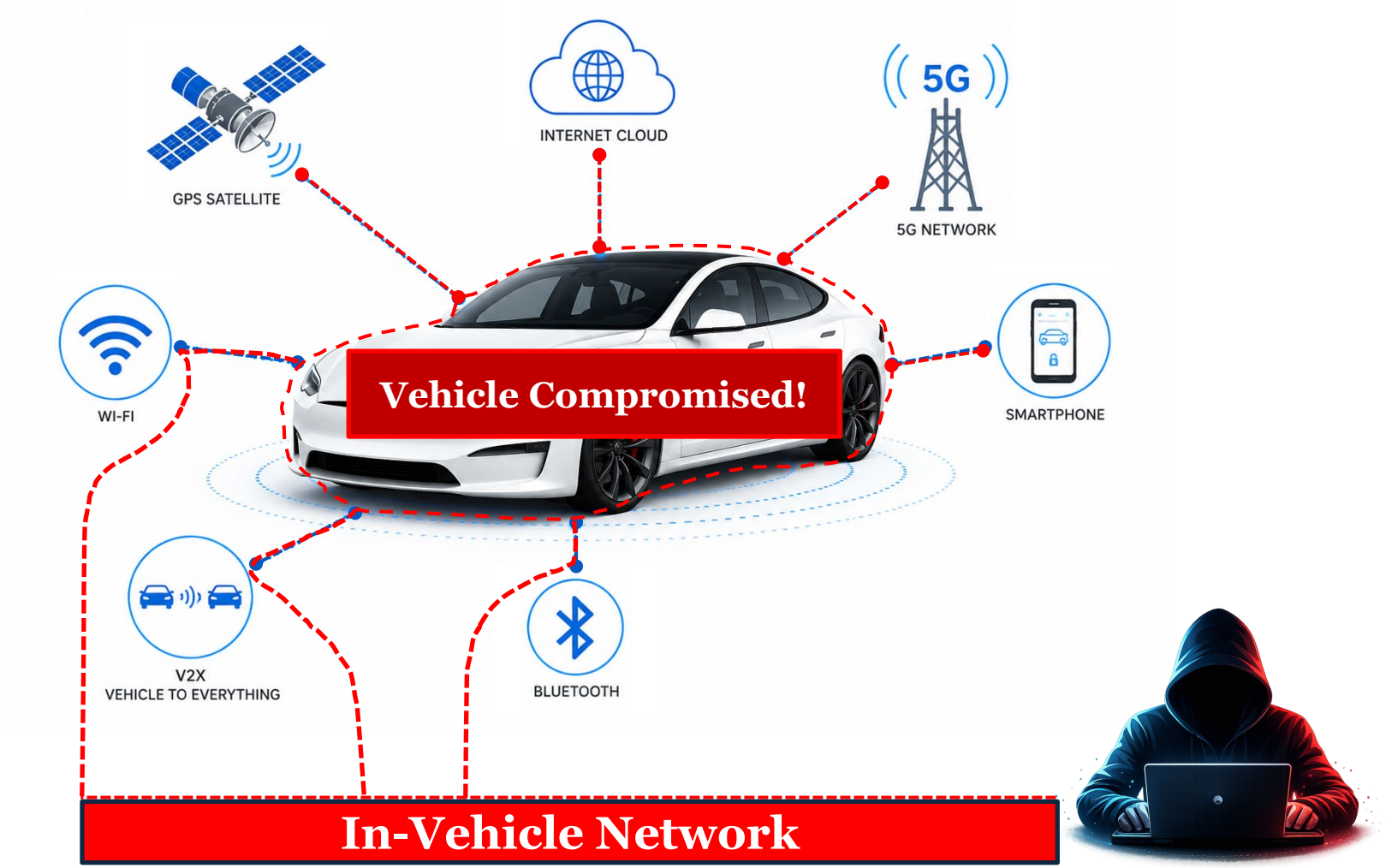
Same model. Same firmware. Same credentials.
To every security system — they are identical.
But one of them is an impostor.

Can we tell them apart? That is exactly what this work is about.

Vehicles Became Computers on Wheels



More Connectivity = A Larger Attack Surface



Remote Attack Surfaces — External Entry Points

A Real Attack Vector: Remote Jeep Takeover (2015).



Source: C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, Las Vegas, NV, 2015.

No Prior Work Can Detect a Same-Model Clone

	Work	Method	NO FW Mod?	Clone Pairs?	Real-Time?
[1]	Cho & Shin (USENIX Sec '16)	Clock drift from CAN timing	✓	✗	✗
[2]	Viden (CCS '17)	Steady-state CAN voltage	✓	✗	✓
[3]	SIMPLE (ACSAC '19)	Single-frame physical layer	✓	✗	✓
[4]	MCU-Token (NDSS '24)	SRAM + clock features	✗	Partial	✗
	* This work **(VehicleSec '26)**	Switching Transcient	✓	✓	✓

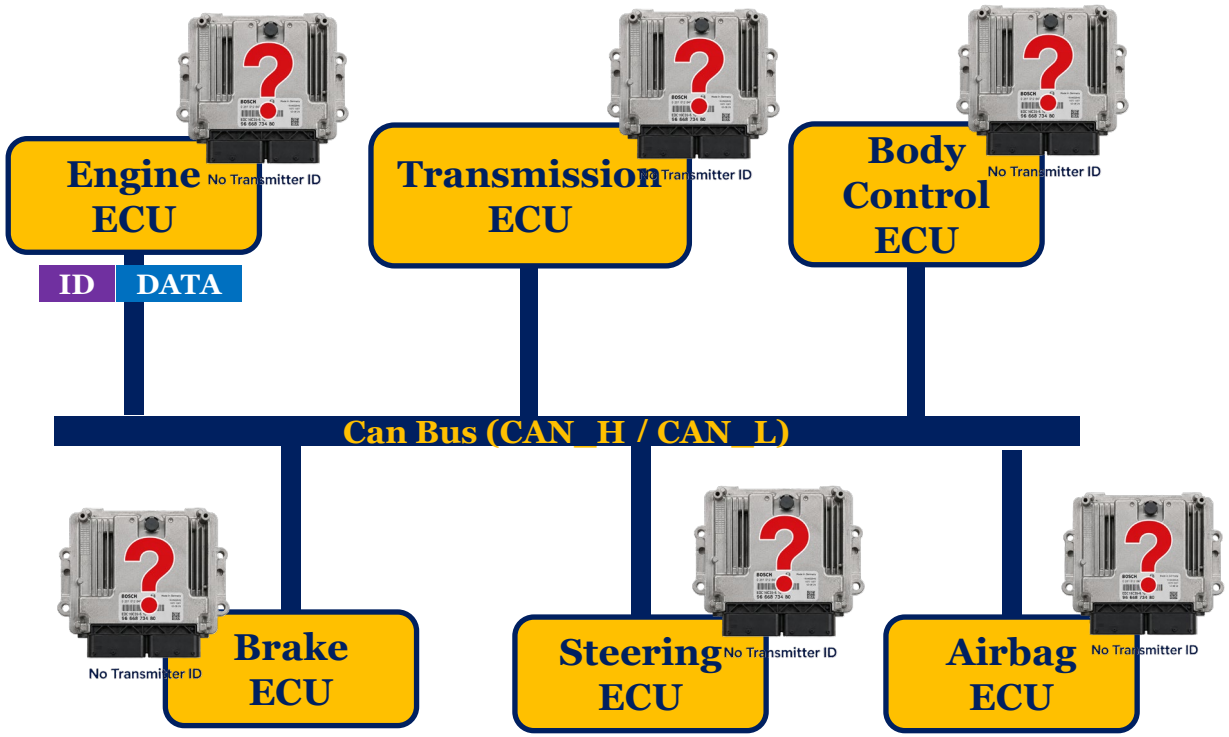
*A. Ali and H. Malik, **"Short: Is Your ECU Really Yours?"** in Proc. 4th USENIX Symposium on Vehicle Security and Privacy (VehicleSec '26), Baltimore, MD, Aug. 2026.

The Problem: CAN Has No Sender Identity

All ECU broadcasting any message on the CAN bus.

There is no transmitter identity: you cannot verify who actually sent a frame.

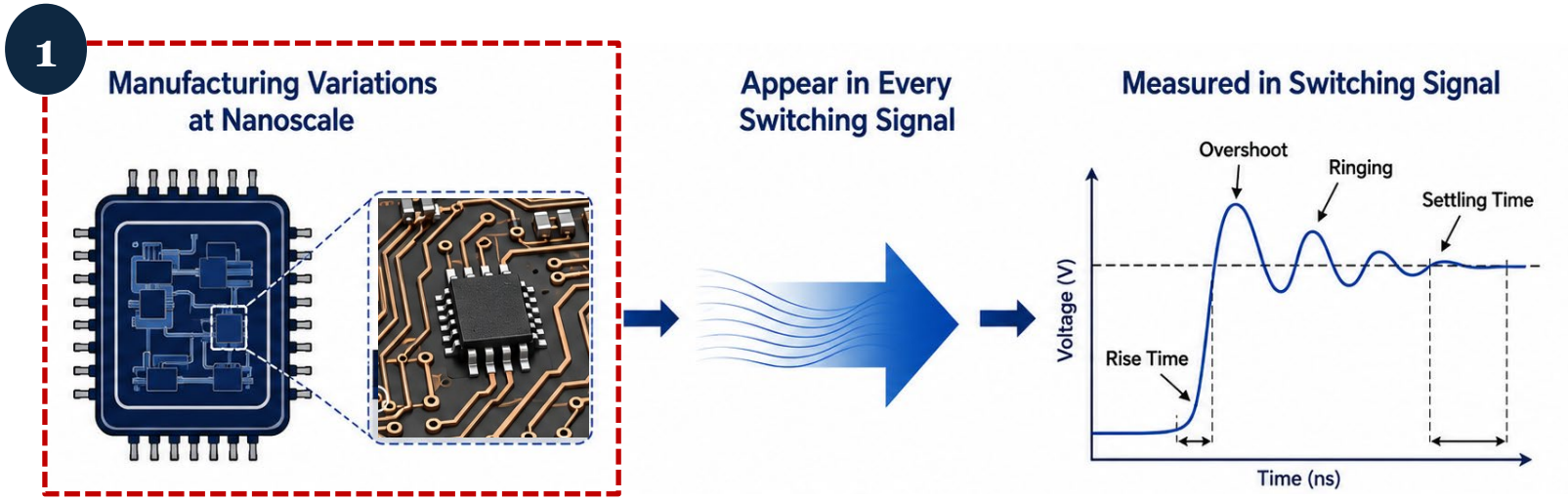
So, you cannot tell a genuine ECU from a swapped or counterfeit clone of the same model.



Why it matters:
counterfeit or aftermarket ECUs can impersonate a genuine one - **a safety and security risk.**

Our Idea: Manufacturing Variations Are an Unclonable Fingerprint

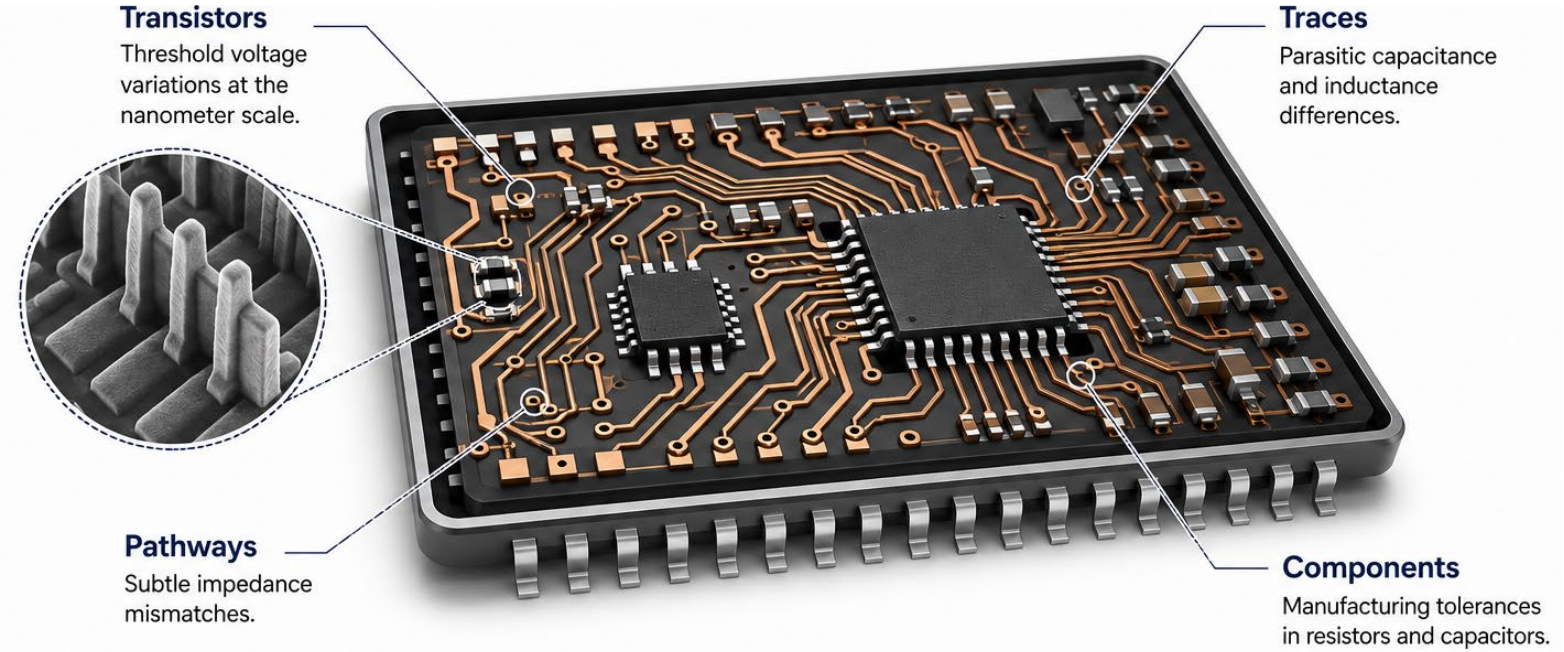
Objective of our work: Fingerprinting the Physics of ECUs



1 Manufacturing Variations (transistor thresholds, parasitic capacitance, PCB trace impedance, and clock jitter) create a **unique physical fingerprint** (invisible to software, unclonable in hardware)

Every Device Is Physically Unique at the Nanometer Scale

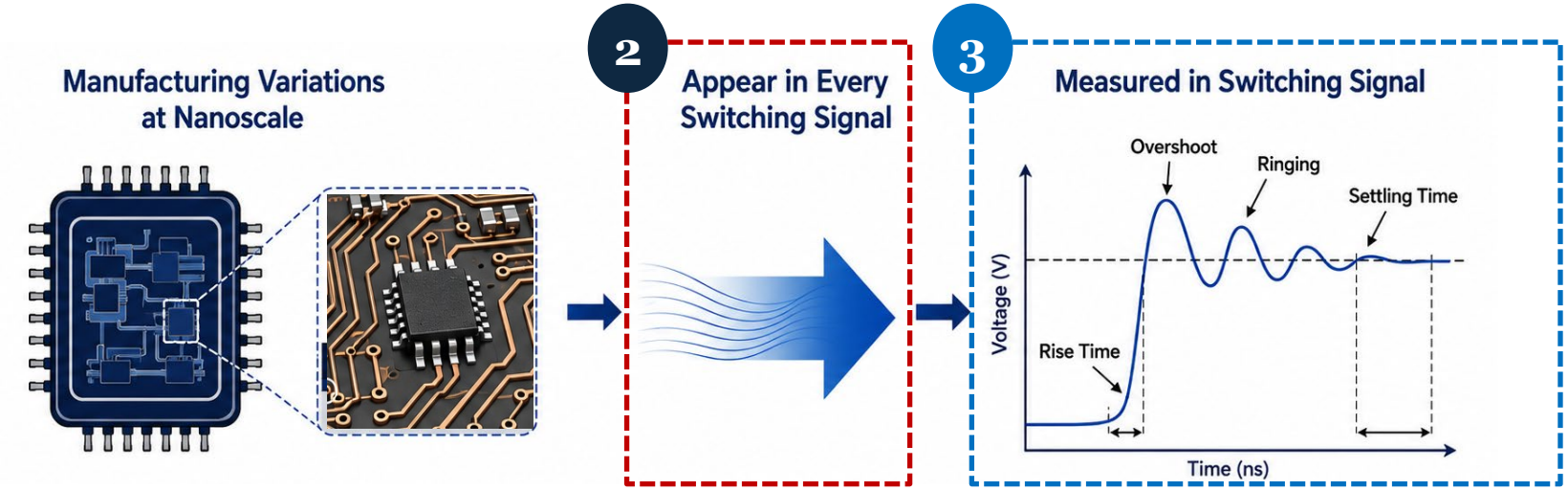
Every ECU, no matter how carefully manufactured, is physically unique at the nanometer scale



Even when two devices roll off the exact same assembly line, the chaotic reality of microscopic manufacturing introduces **unique physical imperfections.** These variations are invisible in the code, but they **fundamentally alter how the hardware conducts electricity.**

Physical Variations Shape the Switching Transient

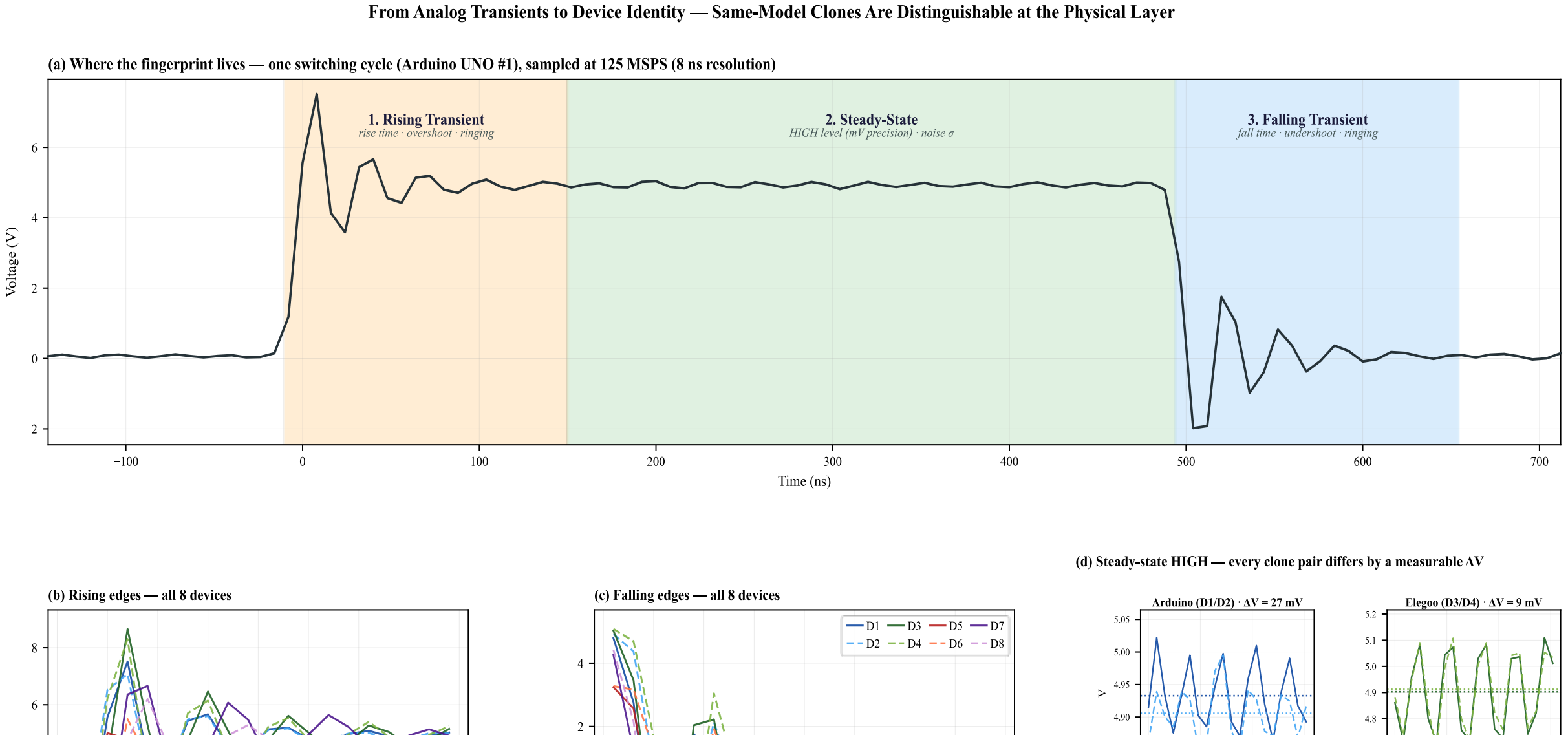
Objective of our work: Fingerprinting the Physics of ECUs

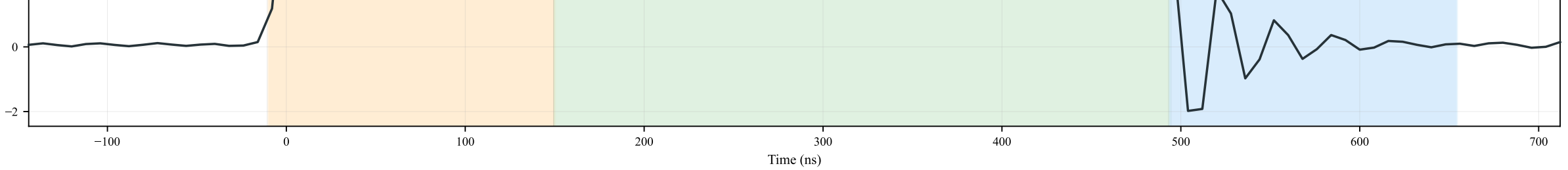


2 These manufacturing variations influence the timing, amplitude, and damping of the **switching transitions**

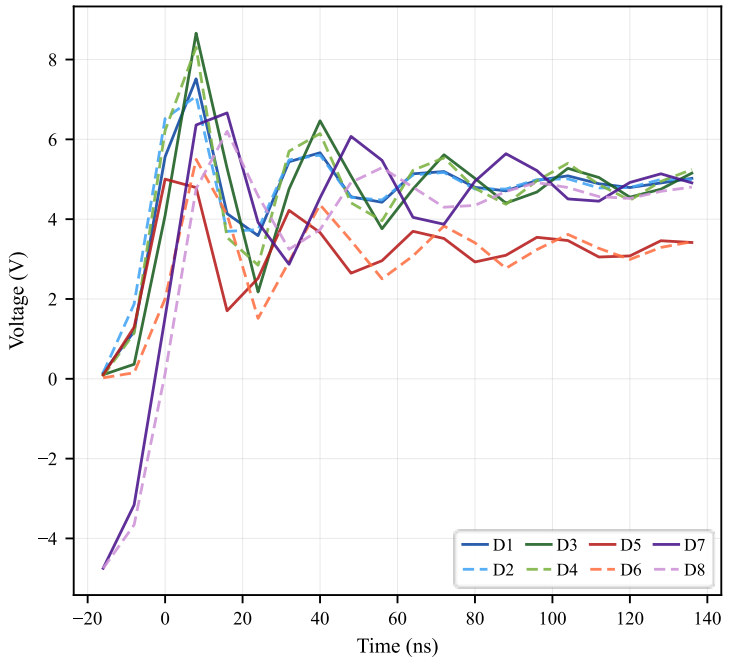
3 Signal Characteristics such as **rise time, fall time, overshoot, ringing and settling time** are unique to each device

Where the Fingerprint Lives

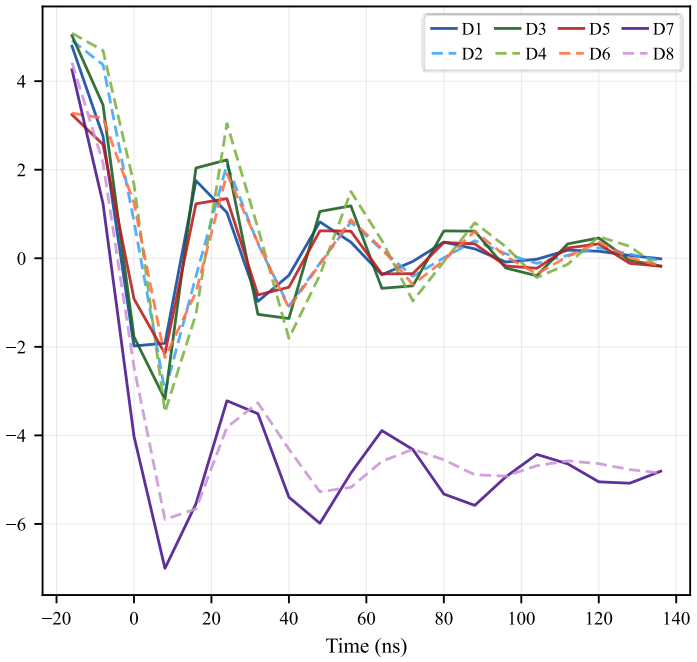




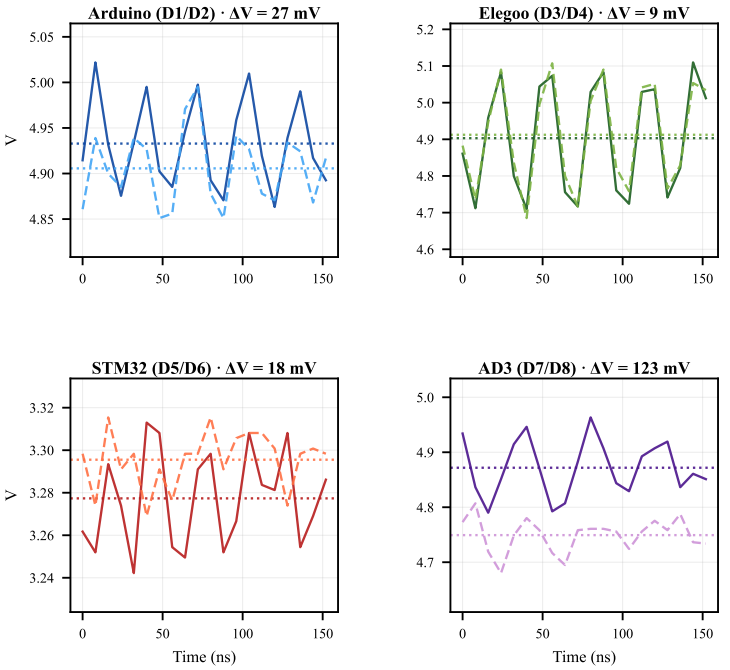
(b) Rising edges — all 8 devices



(c) Falling edges — all 8 devices



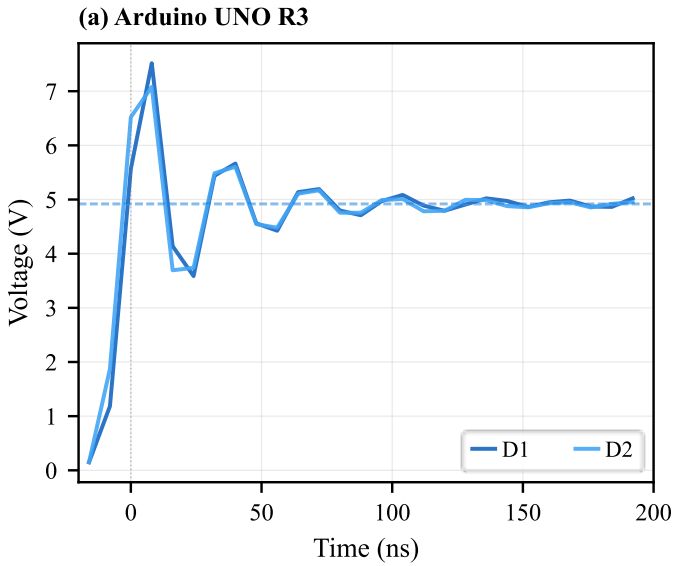
(d) Steady-state HIGH — every clone pair differs by a measurable ΔV

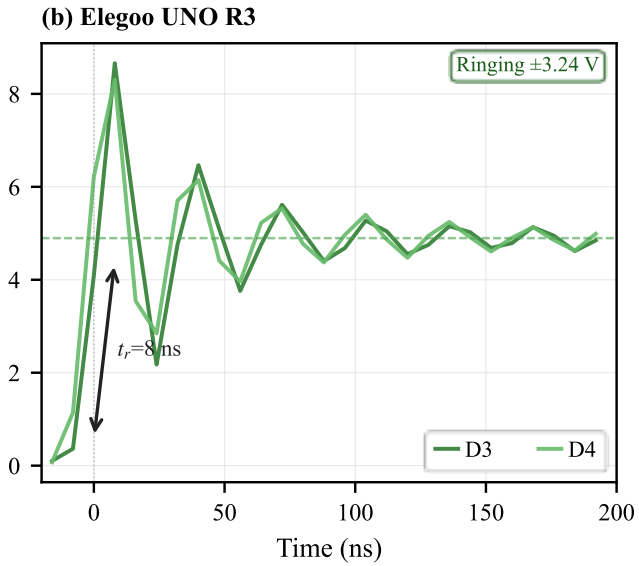


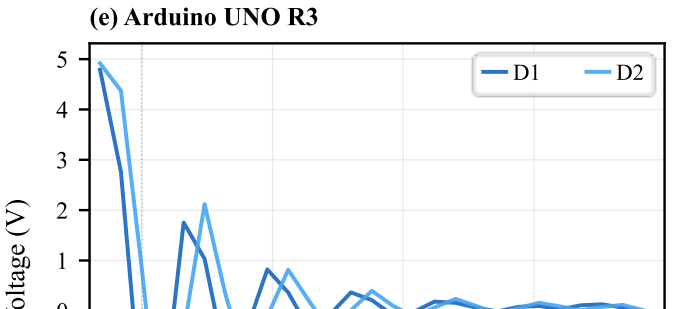
Even Same-Model Clones Differ — Measurably

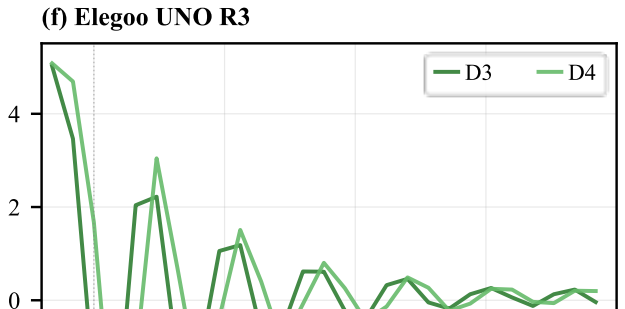
Rising Edge of Devices
D1, D2
and
D3, D4

Transient Signal Characteristics of Same-M
Arduino (D1/D2) · Elegoo (D3/D4) · STM32 (D5/D

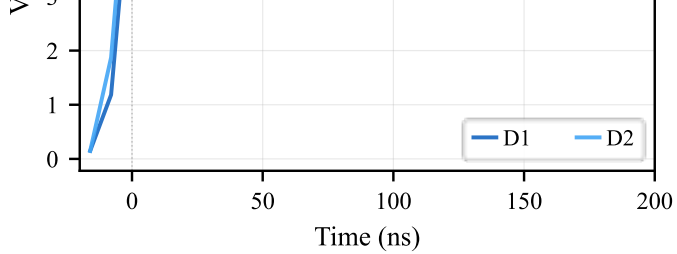


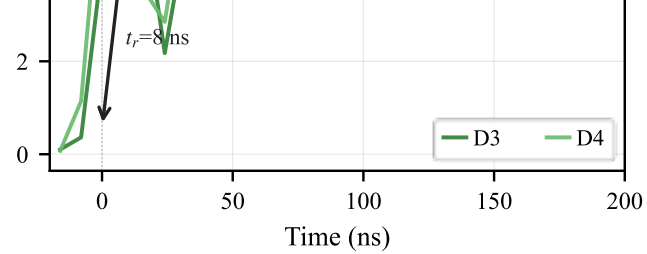




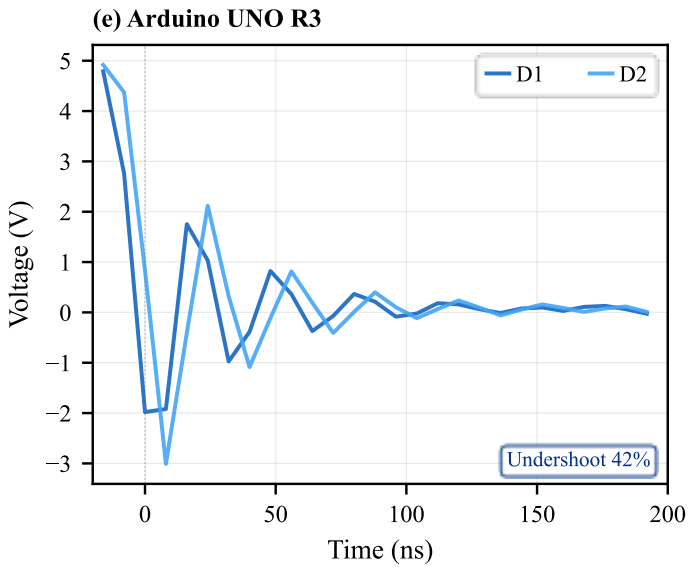


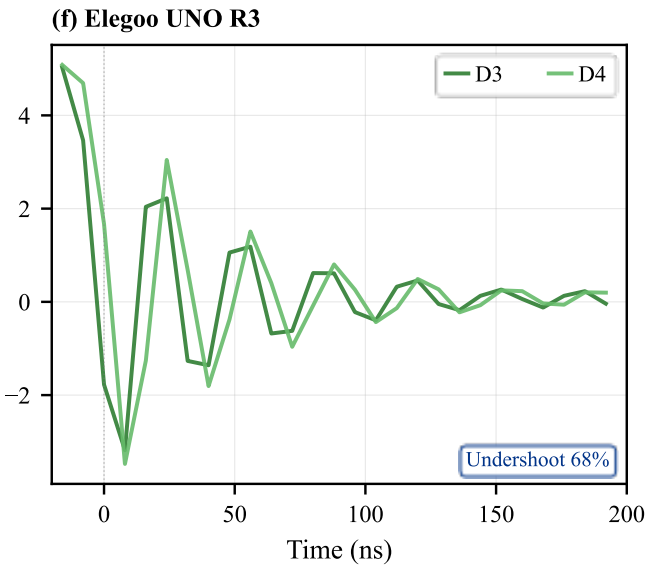
Even Same-Model (



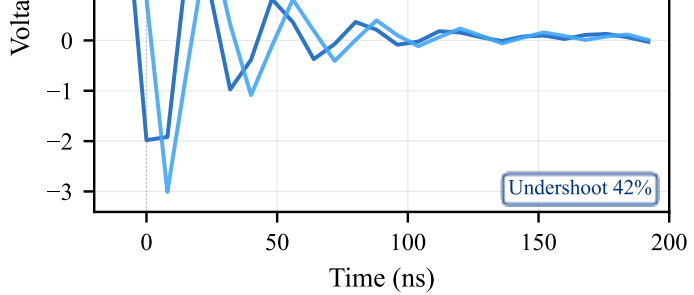


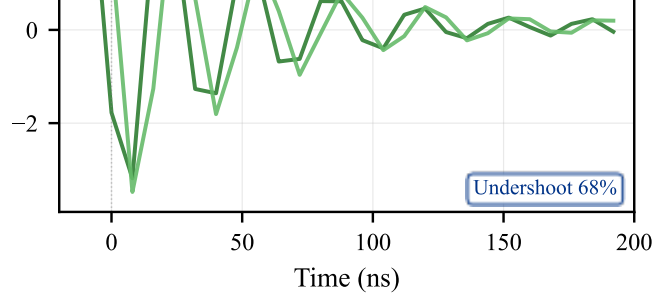
Falling Edge of Devices
D1, D2
and
D3, D4





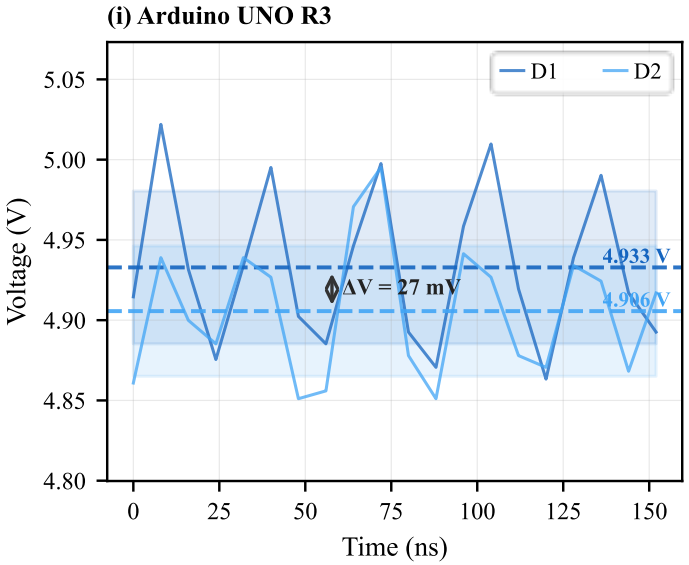
Even Same-Model Cl

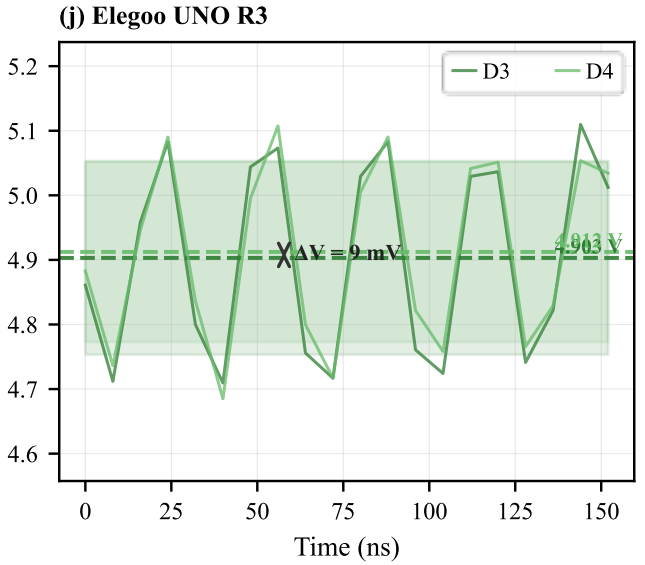




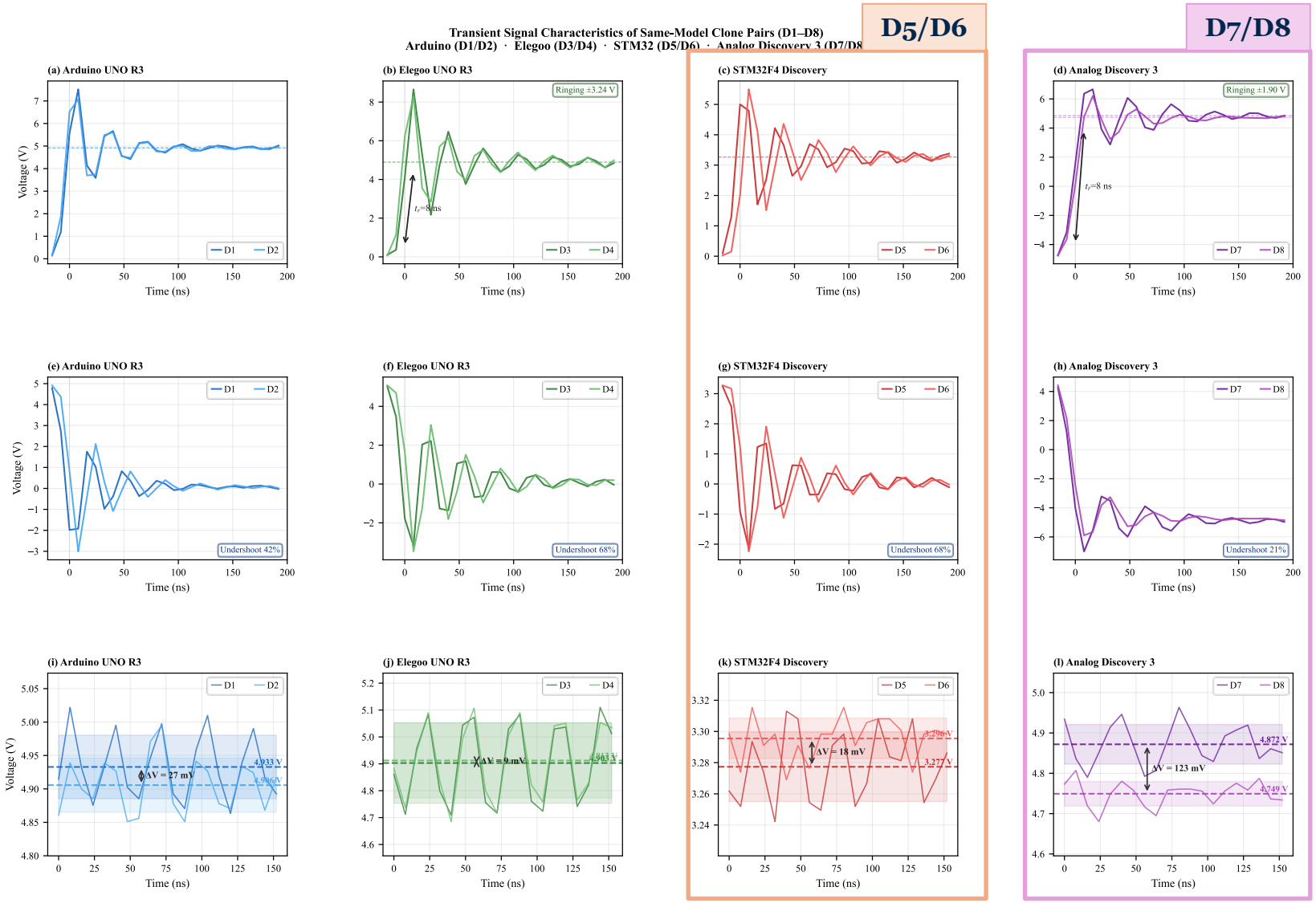
Steady State response of Devices

D1, D2 and D3, D4

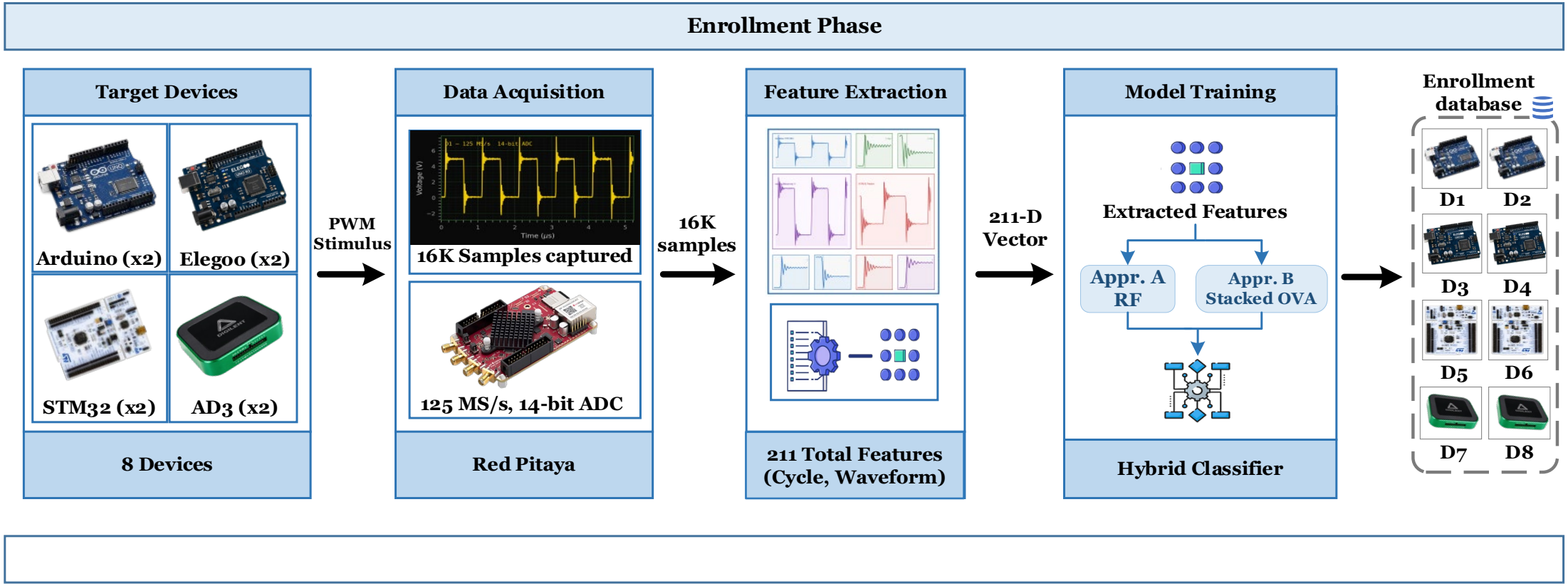




Even Same-Model Clones Differ — Measurably



System Overview / Pipeline

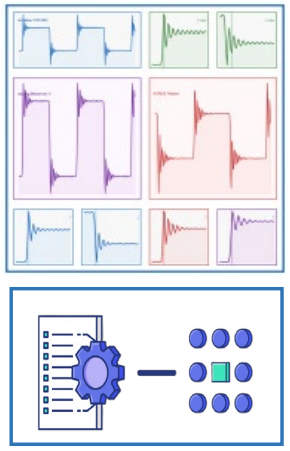


Starting Simple: 14 Raw Signal Features

Enrollment Phase

16K samples

Feature Extraction



14 Features Selected

14 raw signal features

Voltage levels

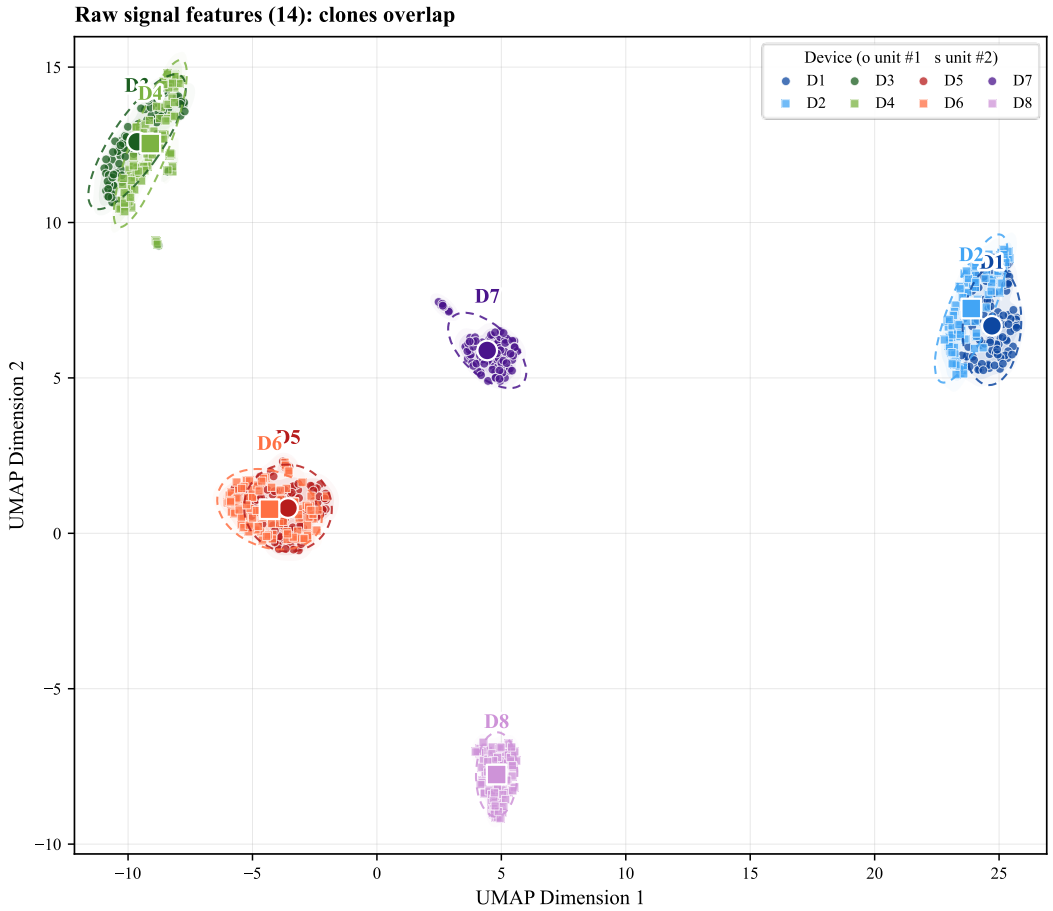
- HIGH mean
- LOW mean
- Swing (HIGH − LOW)
- HIGH noise
- LOW noise

Transients

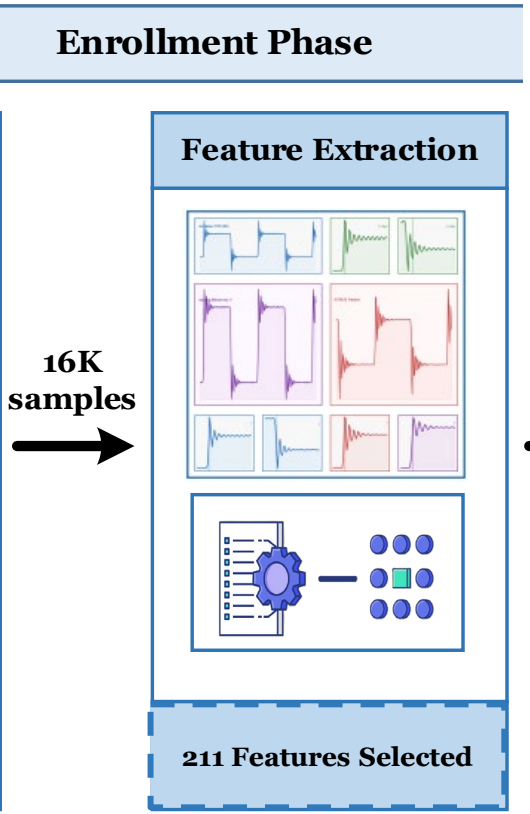
- Rising overshoot
- Falling undershoot
- Rising slew rate
- Falling slew rate

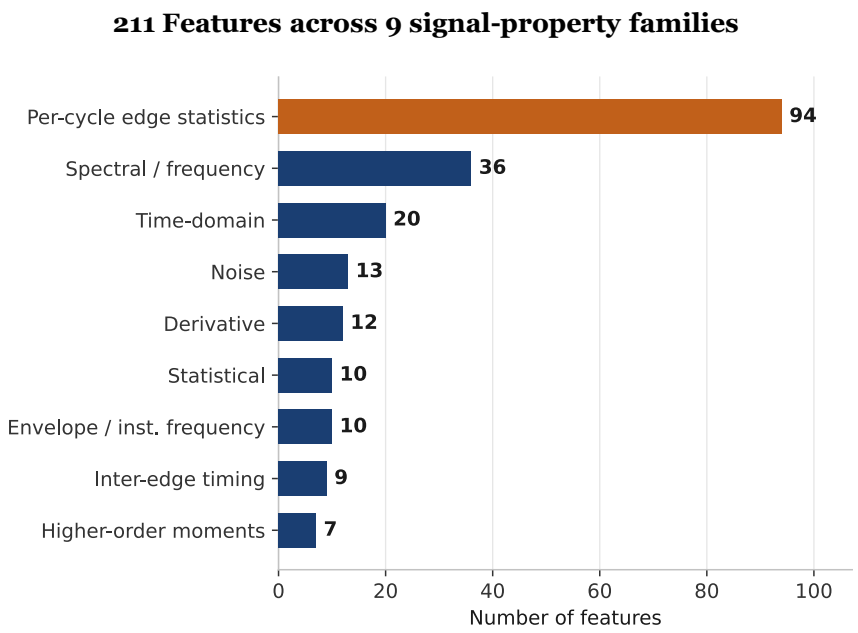
Ringing

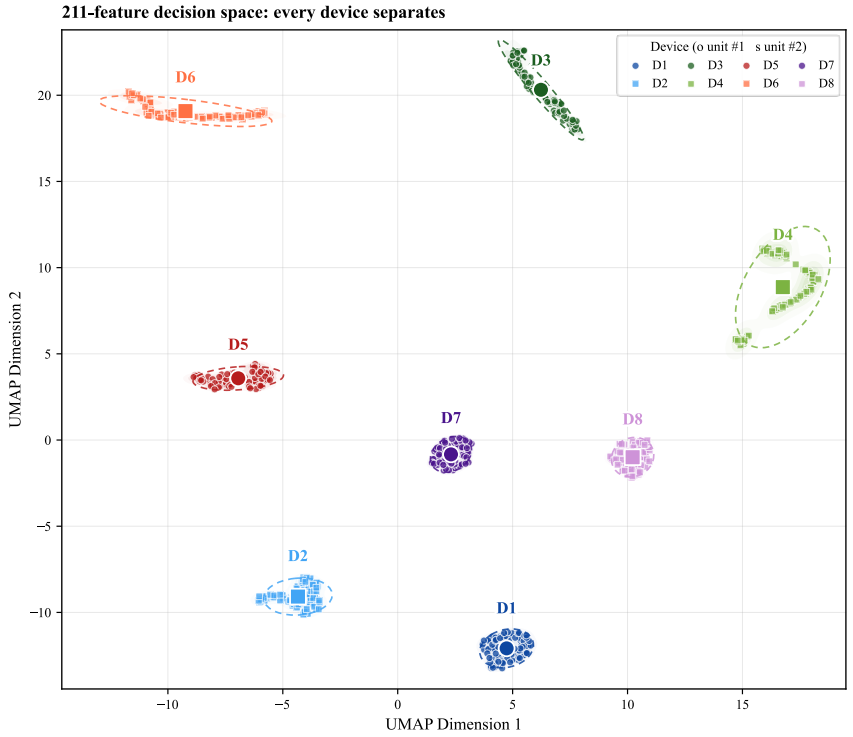
- Rising amplitude
- Rising frequency
- Falling amplitude
- Falling frequency
- Decay (damping)



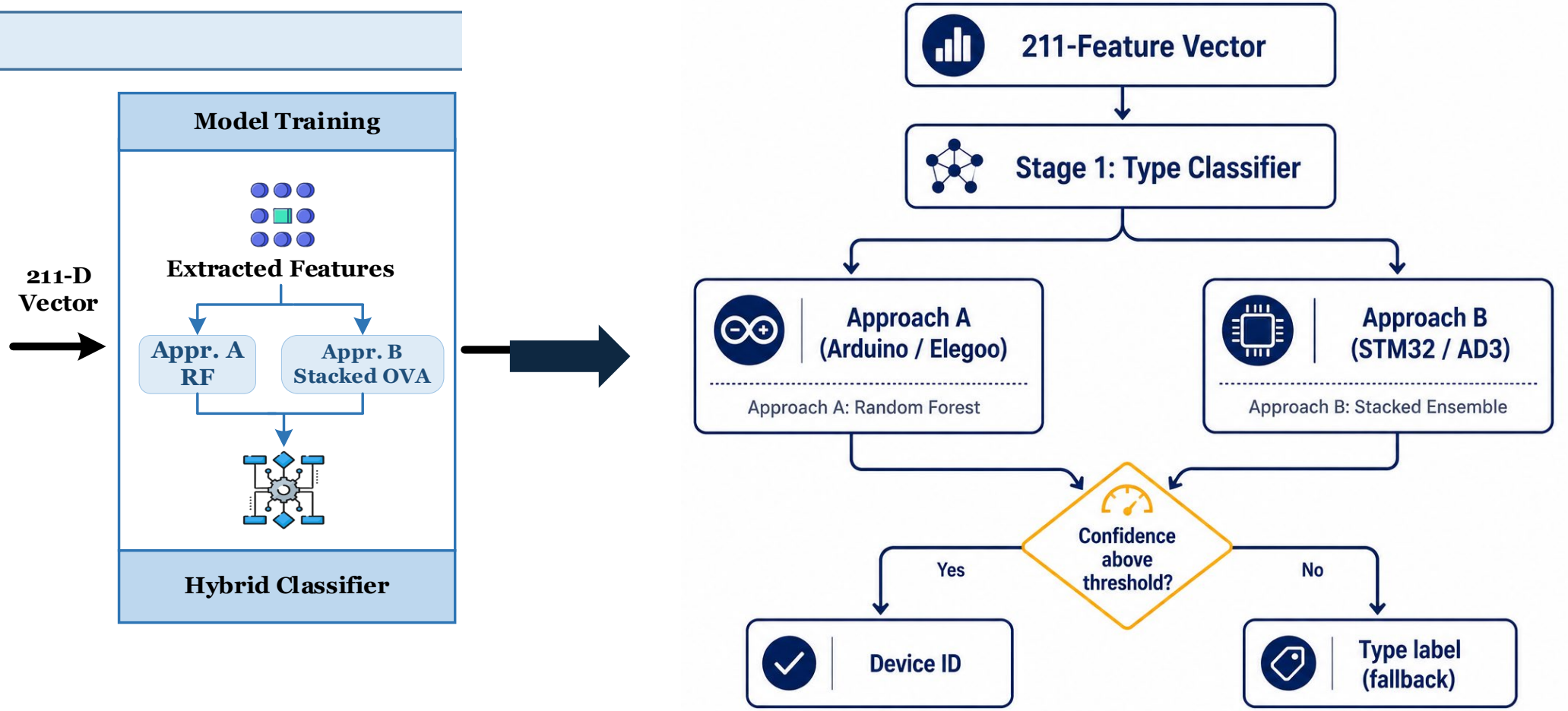
Going Deeper: 211 Features



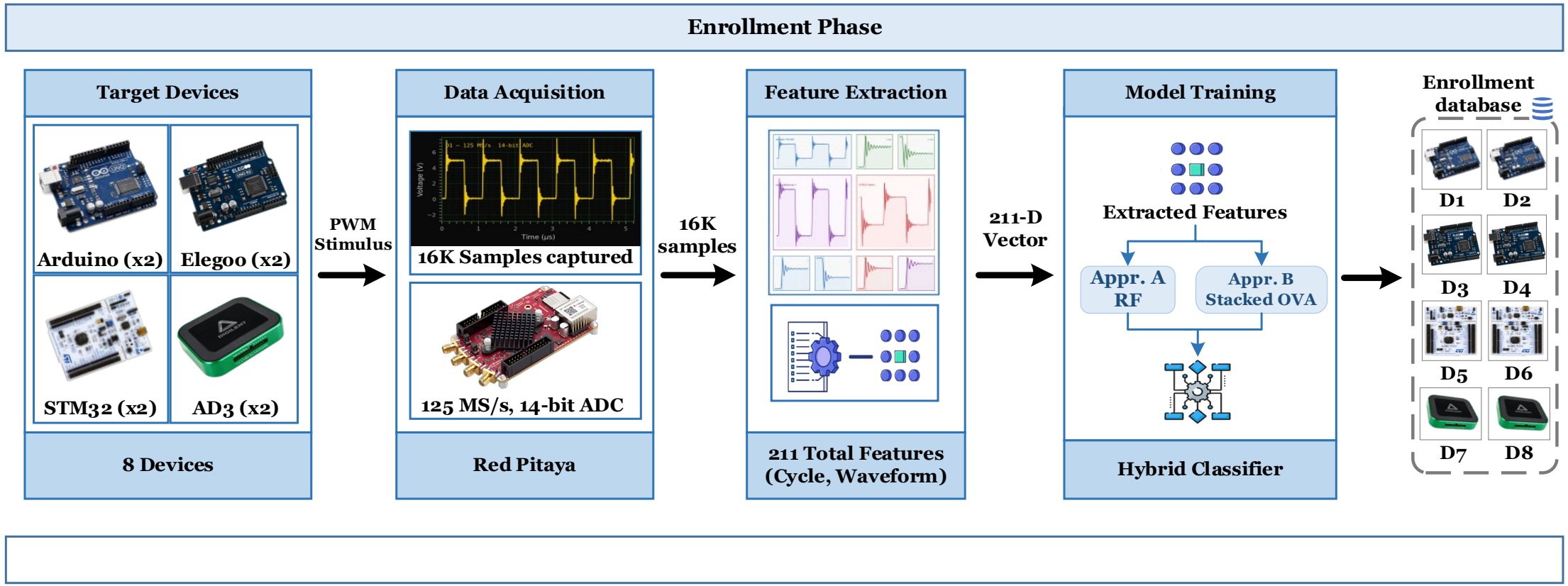




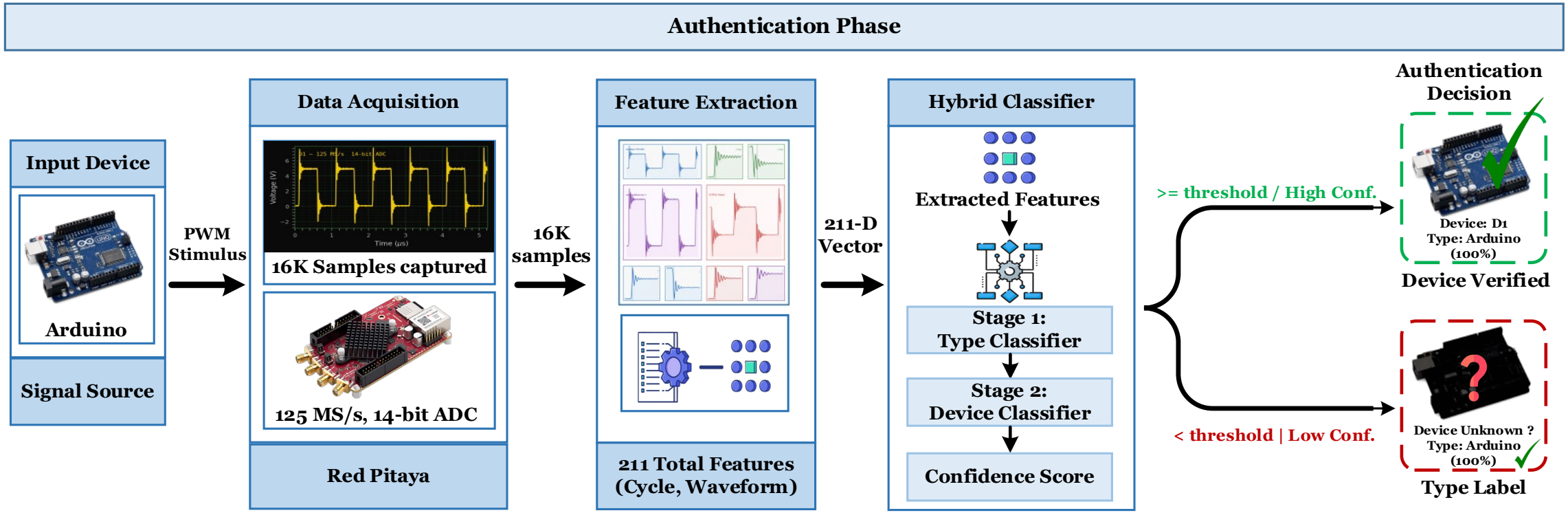
How the Hybrid Classifier Decides



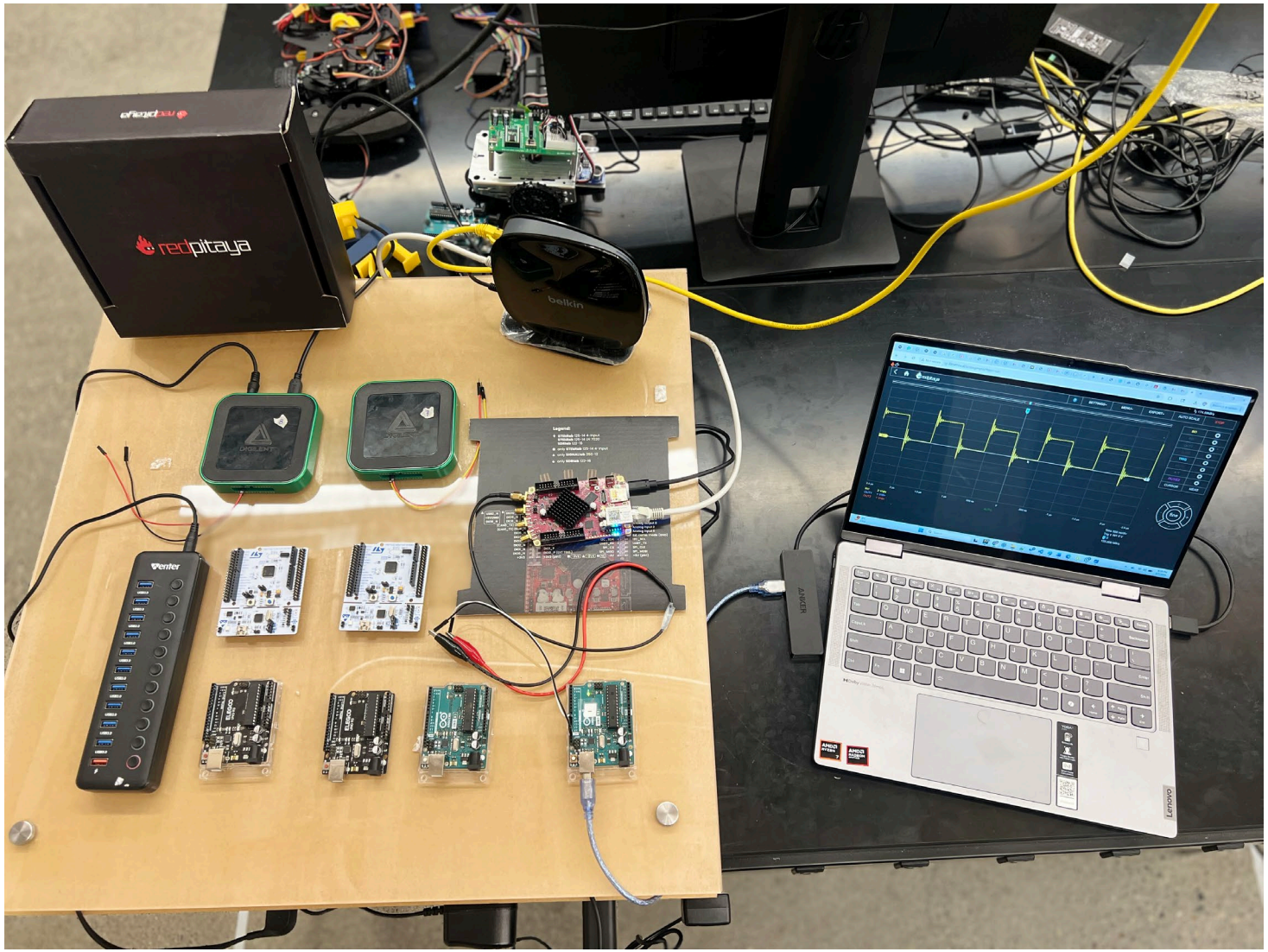
System Overview / Pipeline

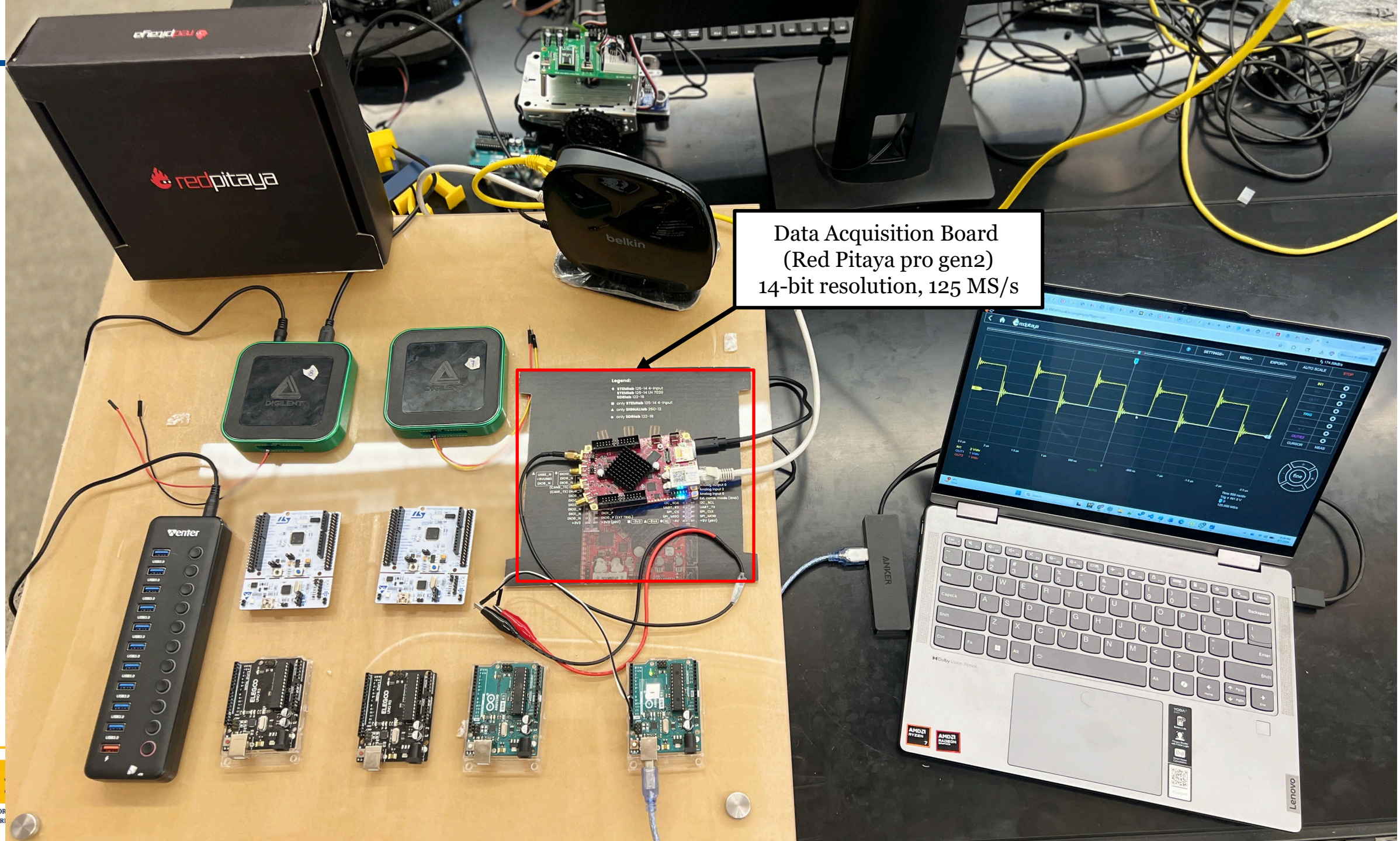


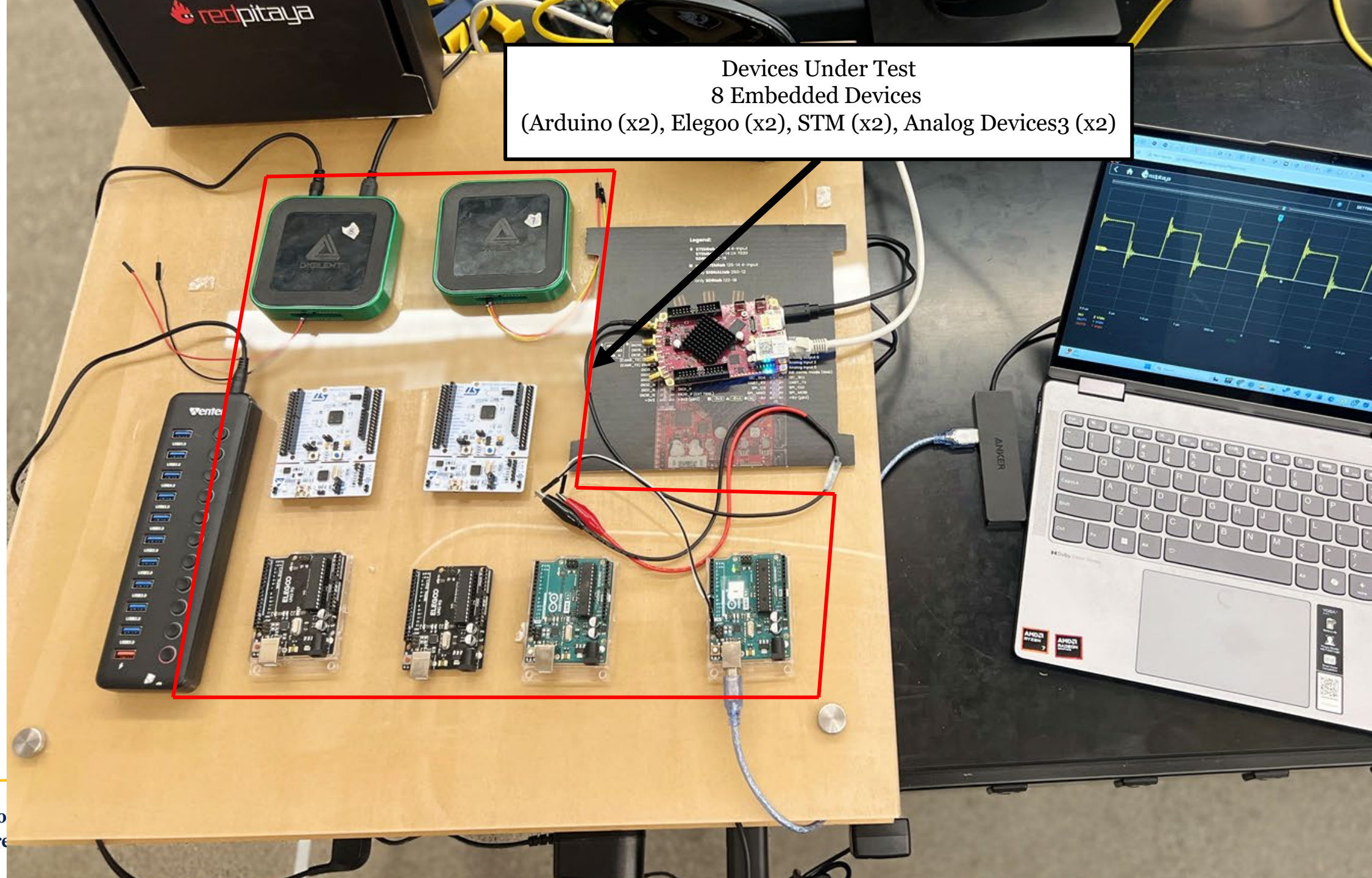
System Overview / Pipeline



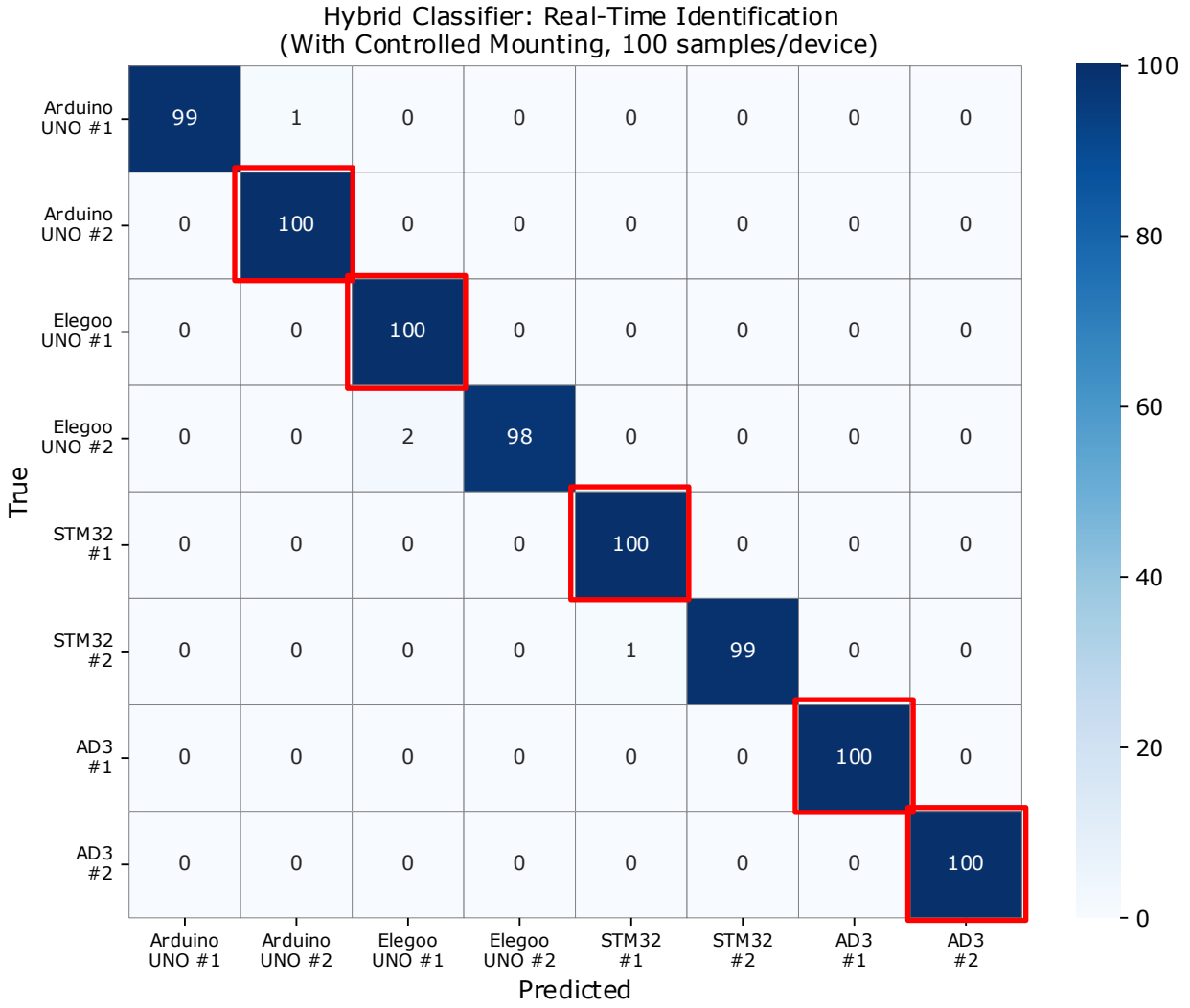
Experimental Setup




redpitaya
belkin
Venter
Lenovo
Data Acquisition Board
(Red Pitaya pro gen2)
14-bit resolution, 125 MS/s


redpitaya
Devices Under Test
8 Embedded Devices
(Arduino (x2), Elegoo (x2), STM (x2), Analog Devices3 (x2)

Results: Even Identical Clones Are Separable



8 identical devices

4 same-model clone pairs

Hybrid ML on analog features

99.5%

real-time identification

5 of 8 devices at 100%

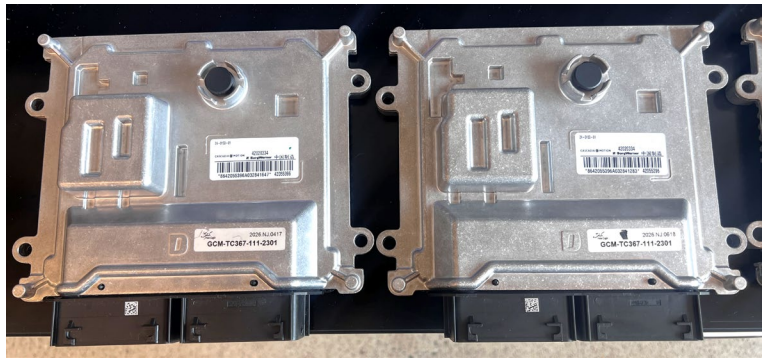
Takeaways

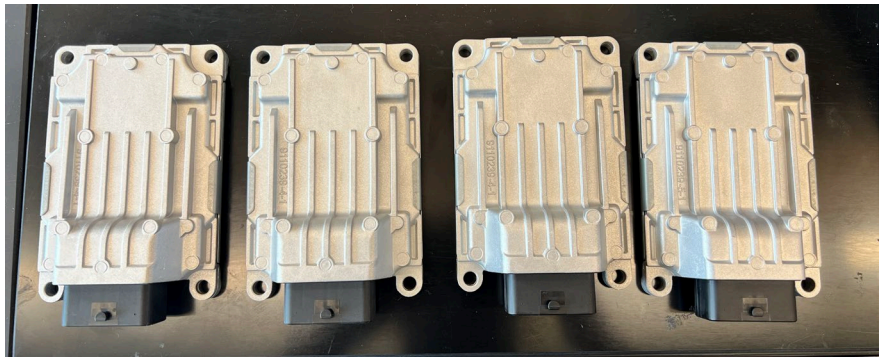
- **CAN has no sender authentication — the physical layer can fill the gap.**
  - Analog switching transients are created by manufacturing variations no attacker can copy.
- **Sub-microsecond transients captured at 125 MSPS distinguish even same-model clones.**
  - Rise/fall shape, overshoot, ringing, and steady-state level differ measurably between identical boards.
- **Lightweight features + hybrid ML enable real-time identification.**
  - 8 devices, 4 clone pairs — high-accuracy identification suitable for edge deployment.

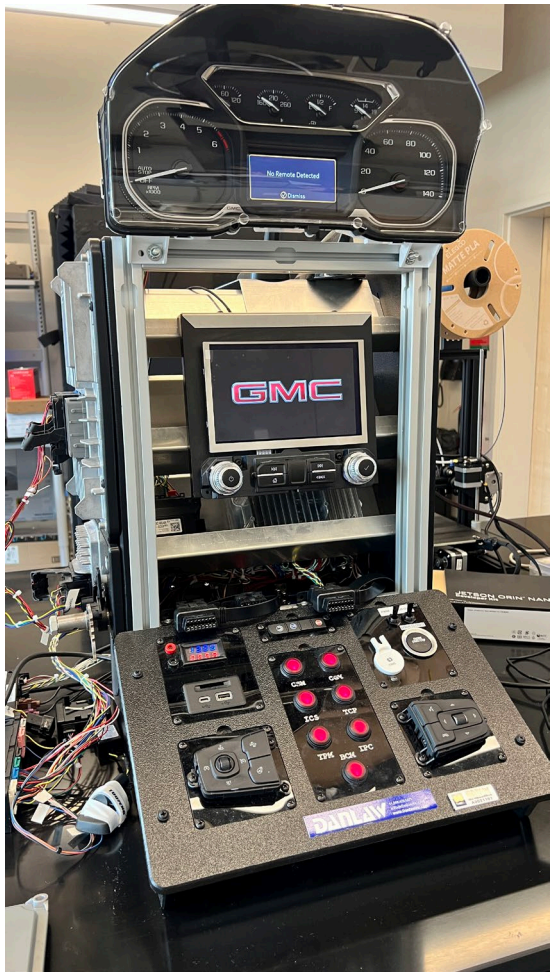
Future Work: From Benchtop to Production ECUs

- **Fingerprinting 14 production automotive ECUs**
  9 identical ECUs from one vendor and 4 from different vendor**.**
  - Same model, same firmware — the hardest possible clone-detection scenario.

- **Robustness: temperature, and aging.**
  - Multi-day sessions to validate fingerprint stability over time.







References

[1] K. Cho and K. G. Shin, "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection," in Proc. 25th USENIX Security Symposium, Austin, TX, 2016.

[2] W. Choi et al., "Viden: Attacker Identification on In-Vehicle Networks," in Proc. ACM Conference on Computer and Communications Security (CCS), Dallas, TX, 2017.

[3] M. Foruhandeh et al., "SIMPLE: Single-Frame based Physical Layer Identification for Intrusion Detection and Prevention on In-Vehicle Networks," in Proc. Annual Computer Security Applications Conference (ACSAC), 2019.

[4] J. Zhang et al., "From Hardware Fingerprint to Access Token: Enhancing the Authentication on IoT Devices," in Proc. Network and Distributed System Security Symposium (NDSS), 2024.

Questions/Answers

Thank you for your attention!

?

Code · Data · Models
Zenodo — scan to access

Acknowledgement

This research was carried out in the **Information Systems, Security and Forensics (ISSF) Laboratory** at the University of Michigan-Dearborn. This material is based upon work supported by the U.S. **National Science Foundation (NSF)** under Awards **#2414729, #2214830, and #2035770**.