Safety≠Security

Ramiro Pareja & Nils Wierma

riscure

Agenda

Introduction

FI on ASIL-D chips

Breaking JTAG

Recommendations

Who are we?

Who are we?


SANGRIA
DON
SIMON
POLAROID
Ramiro Pareja
Senior Security Analyst

Who are we?

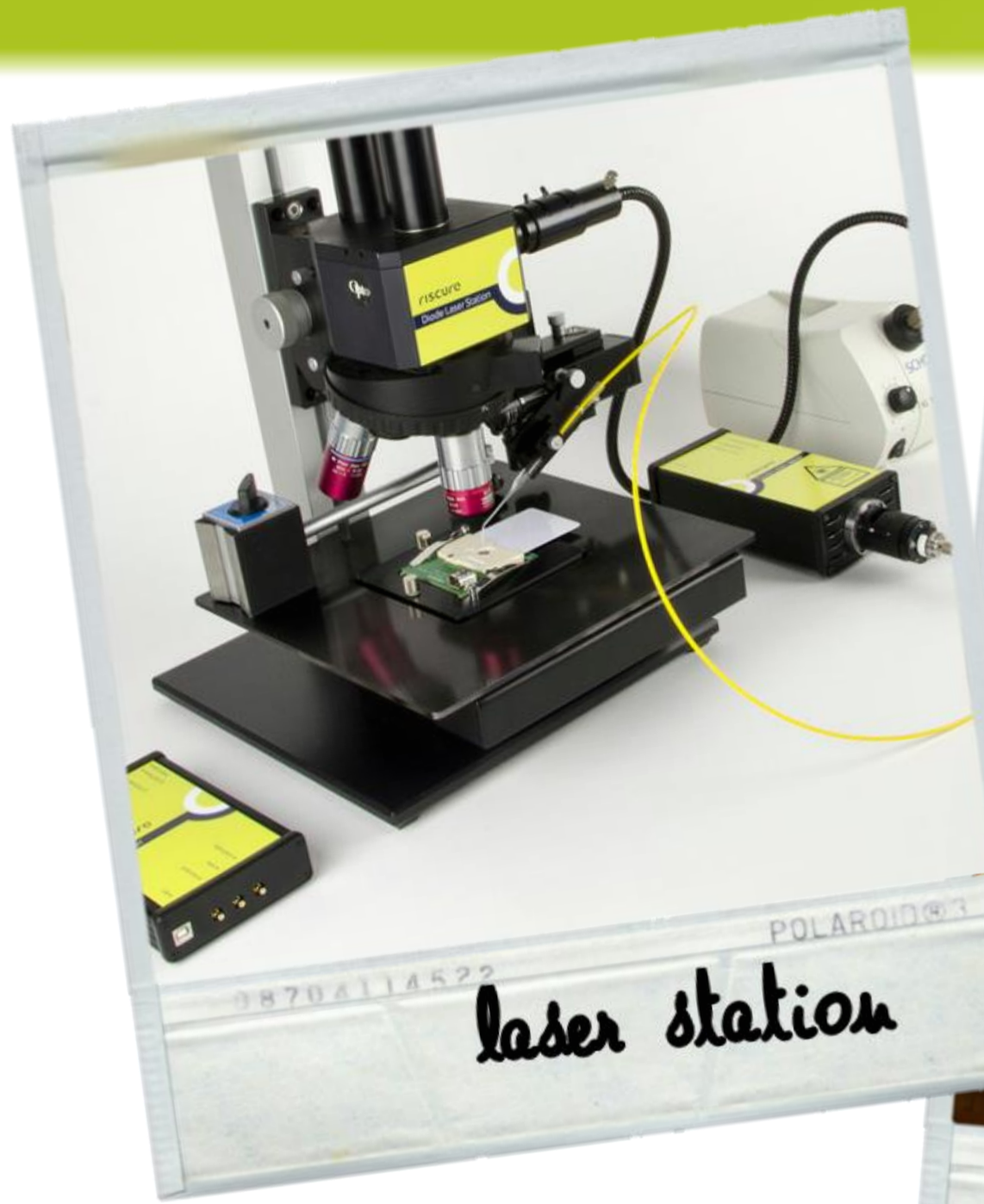

SANGRIA
DON
SIMON
POLAROID
Ramiro Pareja
Senior Security Analyst


POLAROID
Nils Wierma
Security Analyst

What do we do?

What do we do?

What do we do?



laser station

Riscure office

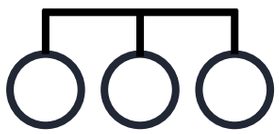
What do we do?


riscure
Diode Laser Station
laser
Evaluation time!
Riscure office

What do we do?

What do we do?

What everybody does



Car Cloud Services

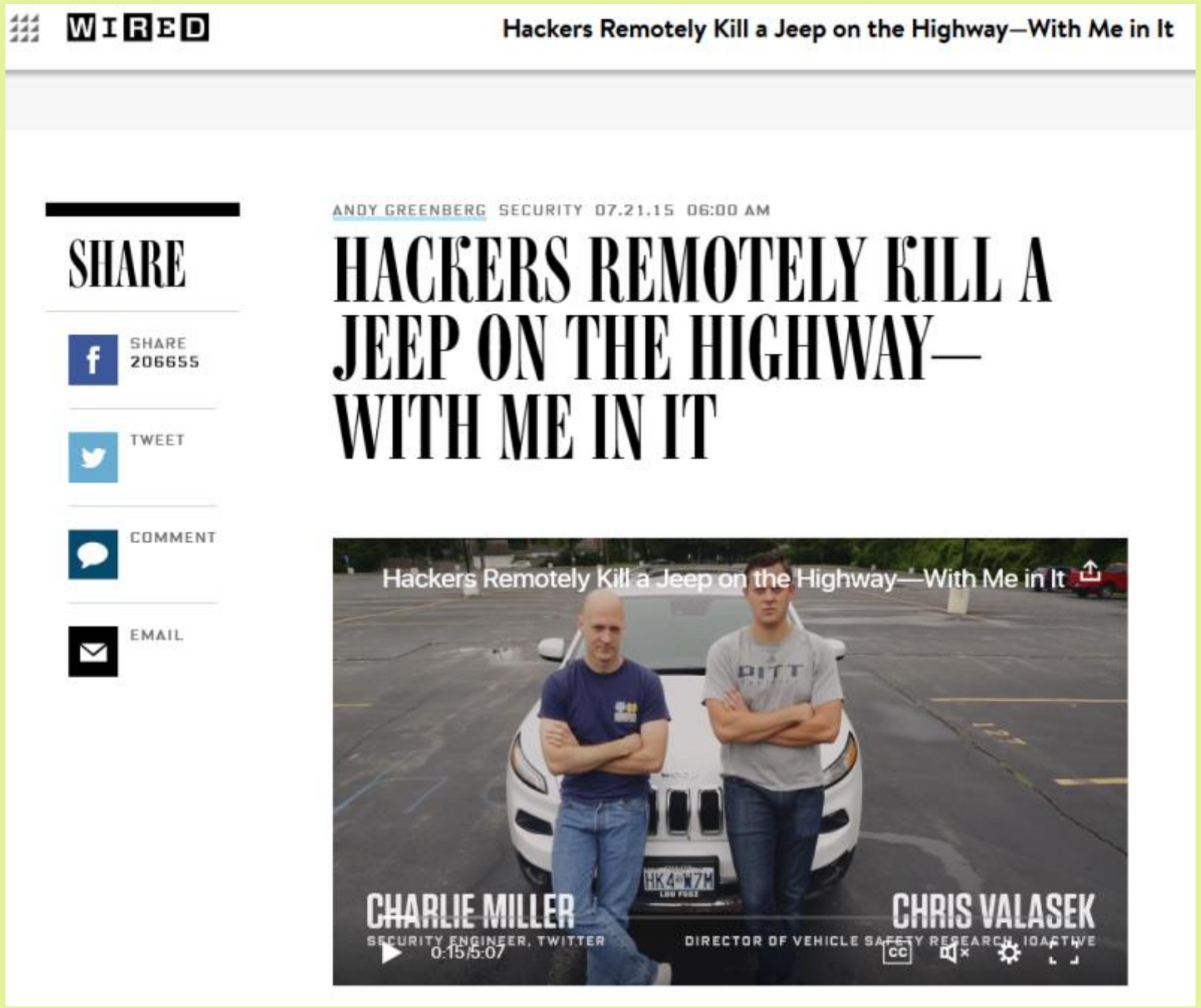
Global Network access

Car Gateway

Car Network

ECU

What everybody does



What everybody does

Team of hackers take remote control of Tesla Model S from 12 miles away

Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc

Now that cars such as Tesla's are increasingly high-tech and connected to the internet, cybersecurity has become as big an issue as traditional safety features. Photograph: Jim Dyson/Getty Images

What everybody does

Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs

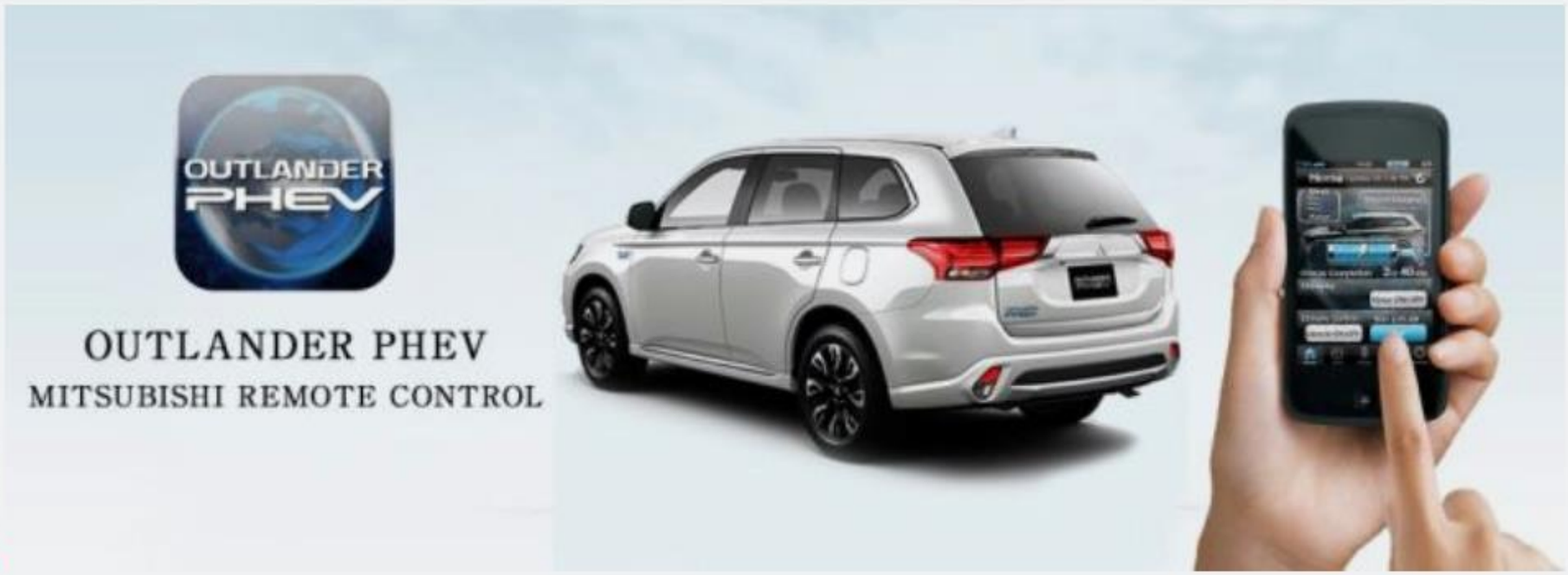
What everybody does

MAYBE THE CLOUD IS SAFER —

Hackers break the connected Mitsubishi Outlander hybrid wide open

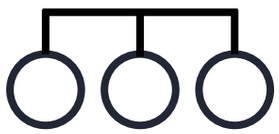
Mitsubishi went for local Wi-Fi instead of LTE, but it's not secure.

JONATHAN M. GITLIN - 6/6/2016, 9:11 PM



Remote functions via Wi-Fi, but easily hacked.

What everybody does



Car Cloud Services

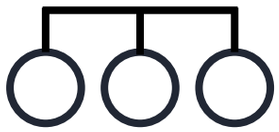
Global Network access

Car Gateway

Car Network

ECU

What differentiate us



Car Cloud Services

Global Network access

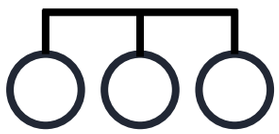
Car Gateway

Car Network

ECU

MCU/TEE

What differentiate us



Car Cloud Services

Global Network access

Car Gateway

Car Network

ECU

MCU/TEE

SCA

FI

Security standards for Automotive CPUs

Secur[illegible] s[illegible]da[illegible]
f[illegible] Automotive CPUs

Functional safety standard

ISO 26262

Functional safety standard

ISO 26262

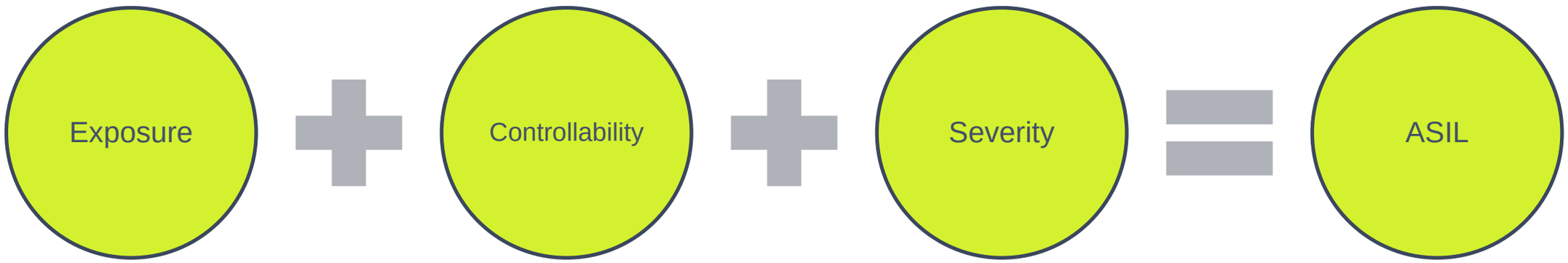
Automotive

Safety

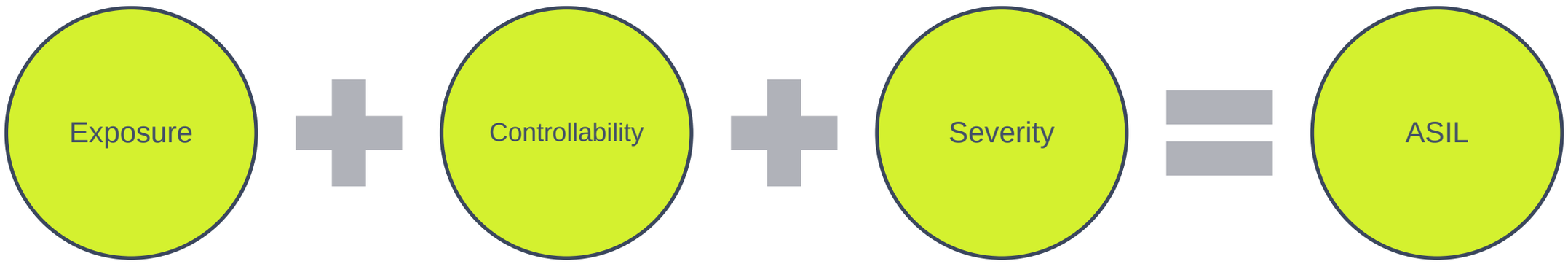
Integrity

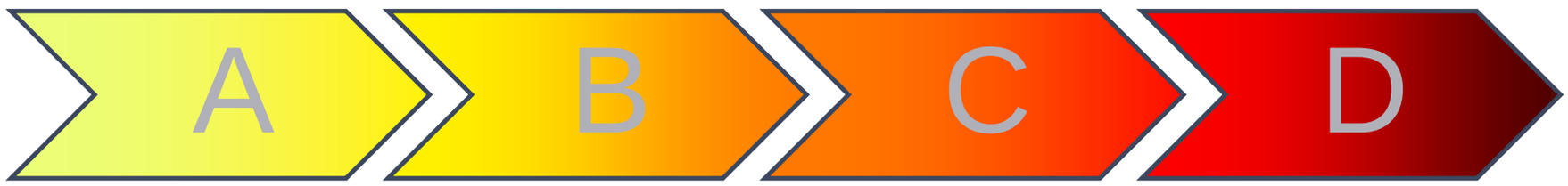
Level

ASIL

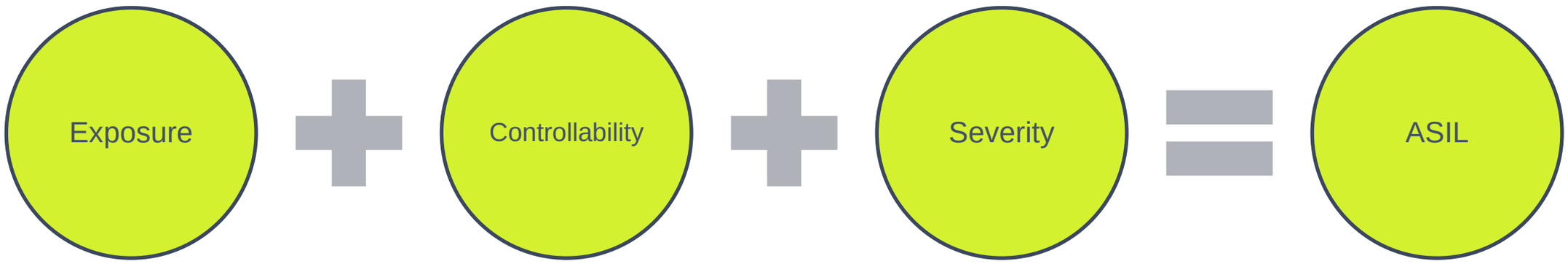


ASIL

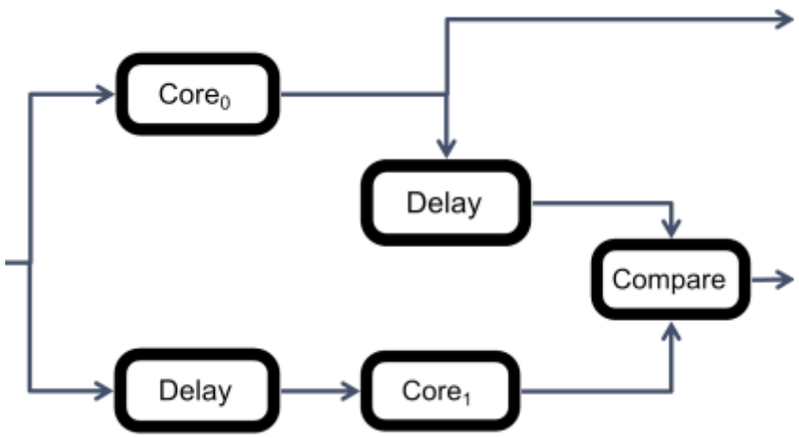




ASIL



Common ASIL-D safety mechanisms



CPU Lockstep

01101010	0
10101101	1
10011010	0
10101010	0
01110101	1
01101101	0
11010101	1

Memory redundancy

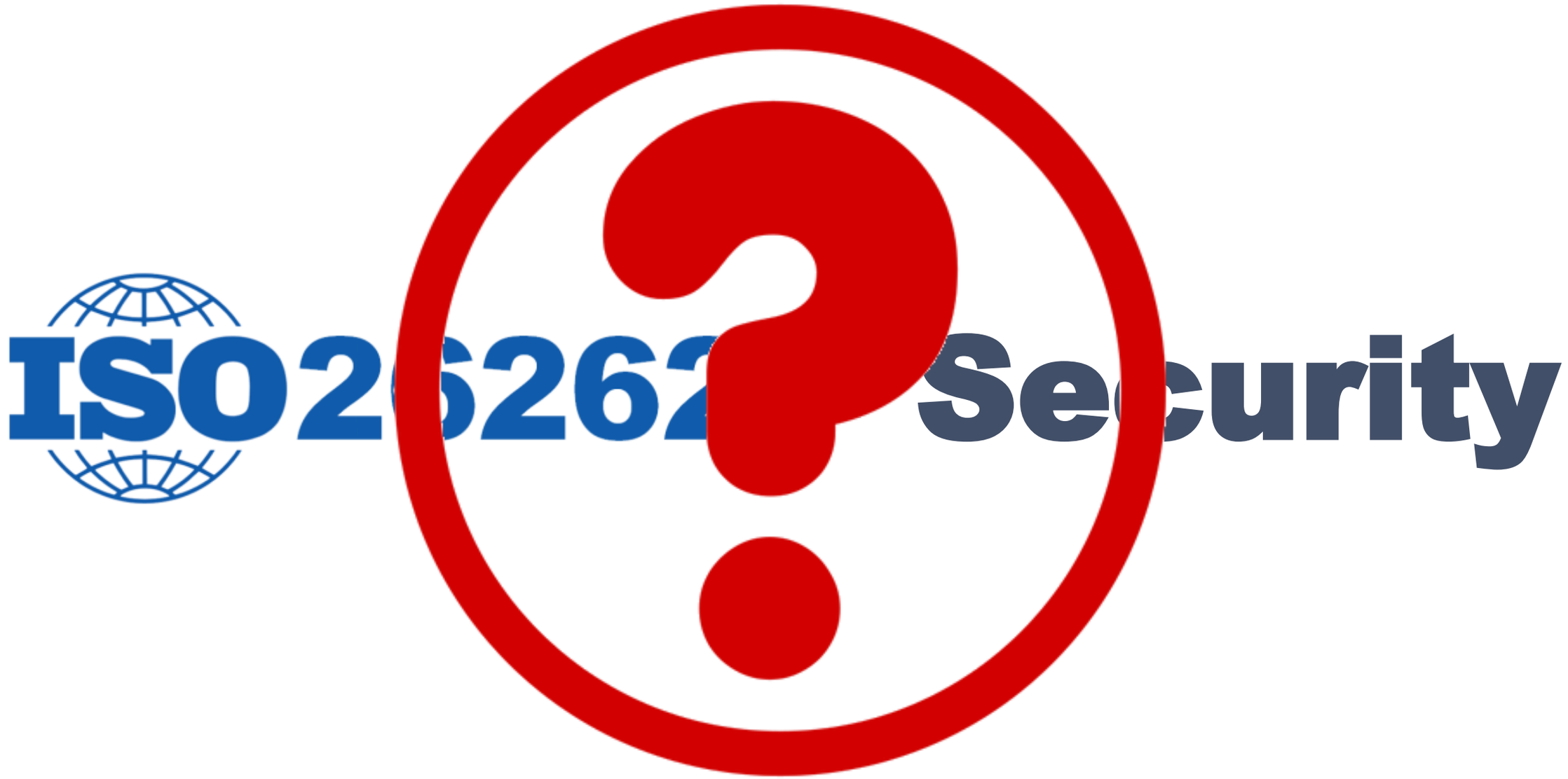
ASIL vs FI

ISO 26262 = Safety

ASIL vs FI

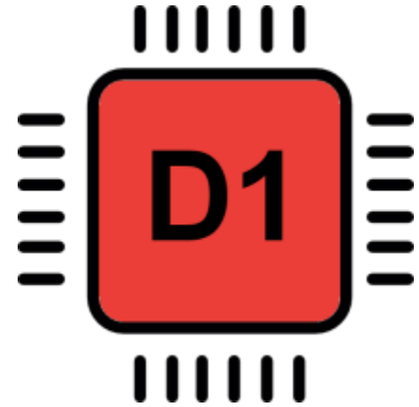
ISO 26262 = Security

ASIL vs FI

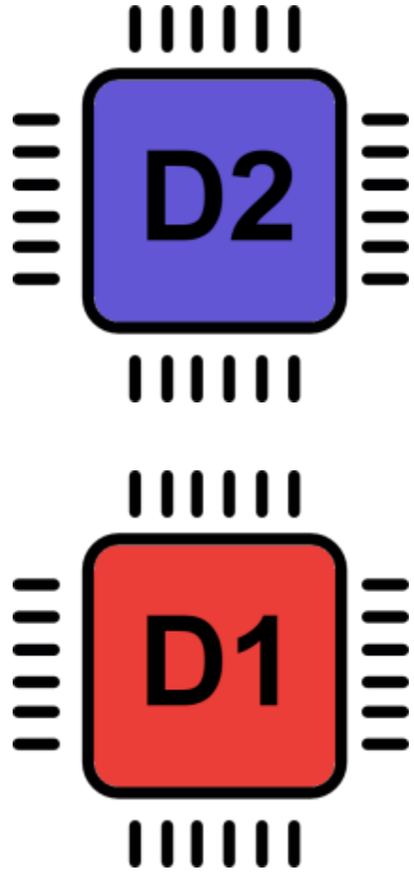


Targets

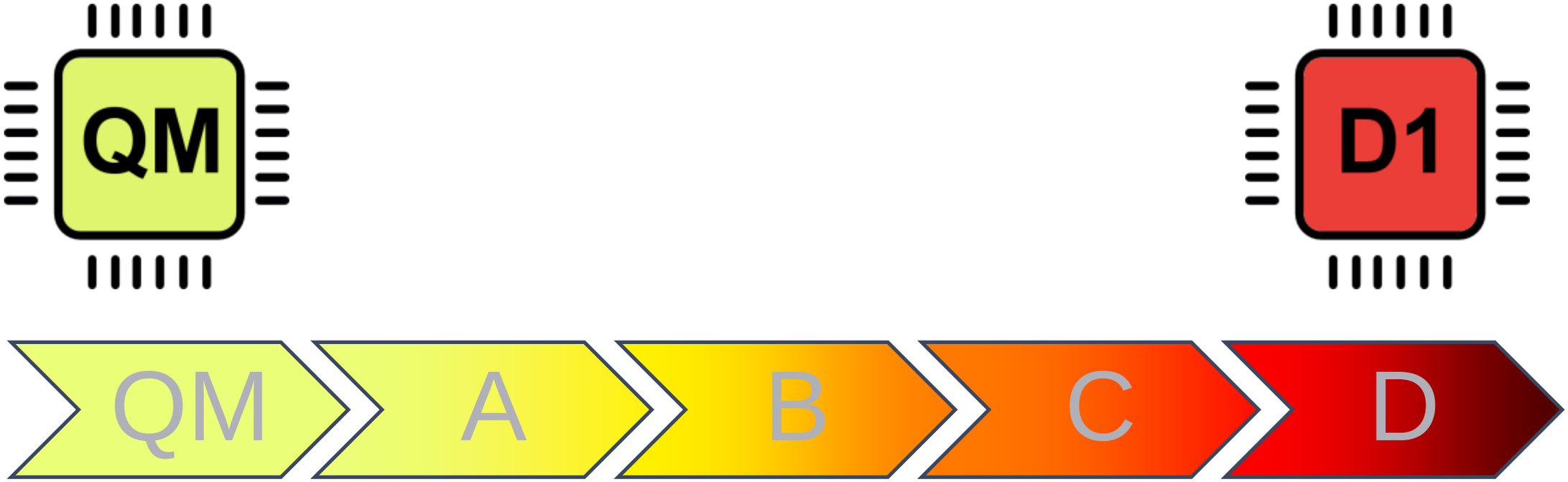
Targets



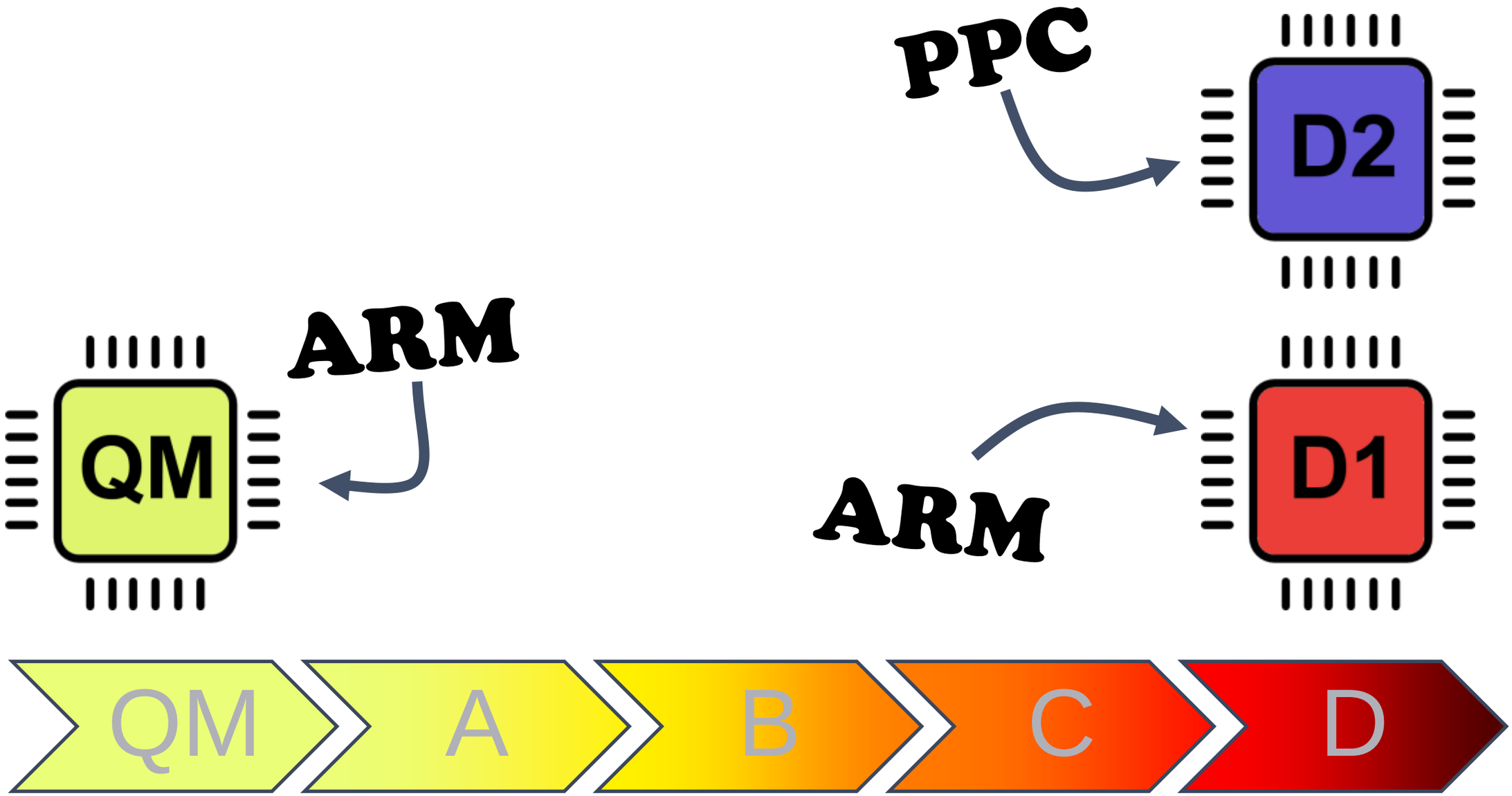
Targets



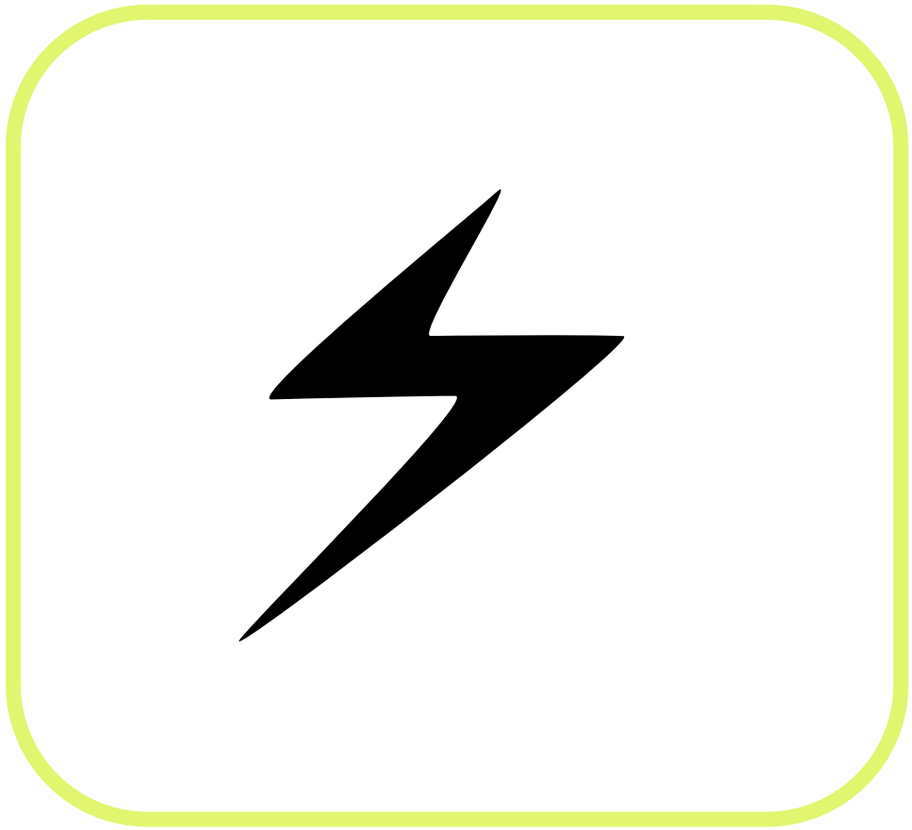
Targets



Targets

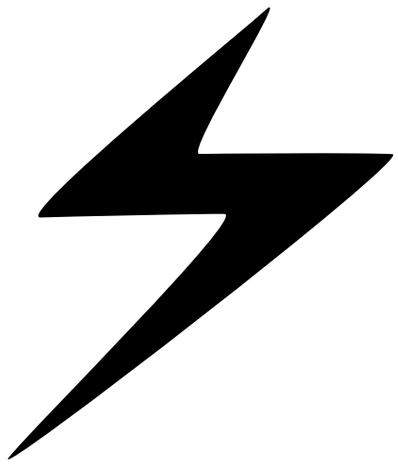


FI methods

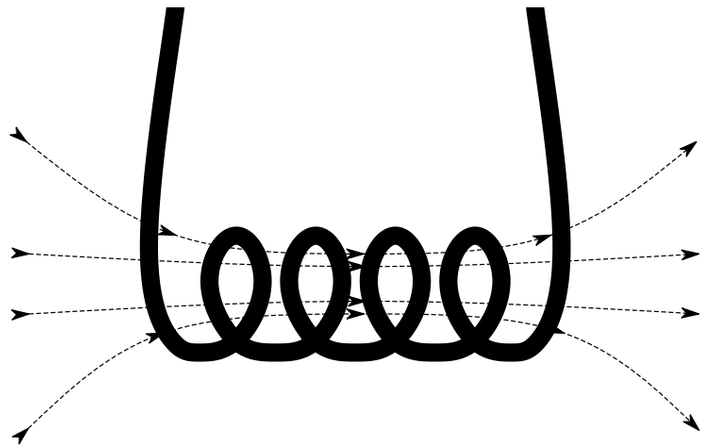


Voltage glitching

FI methods

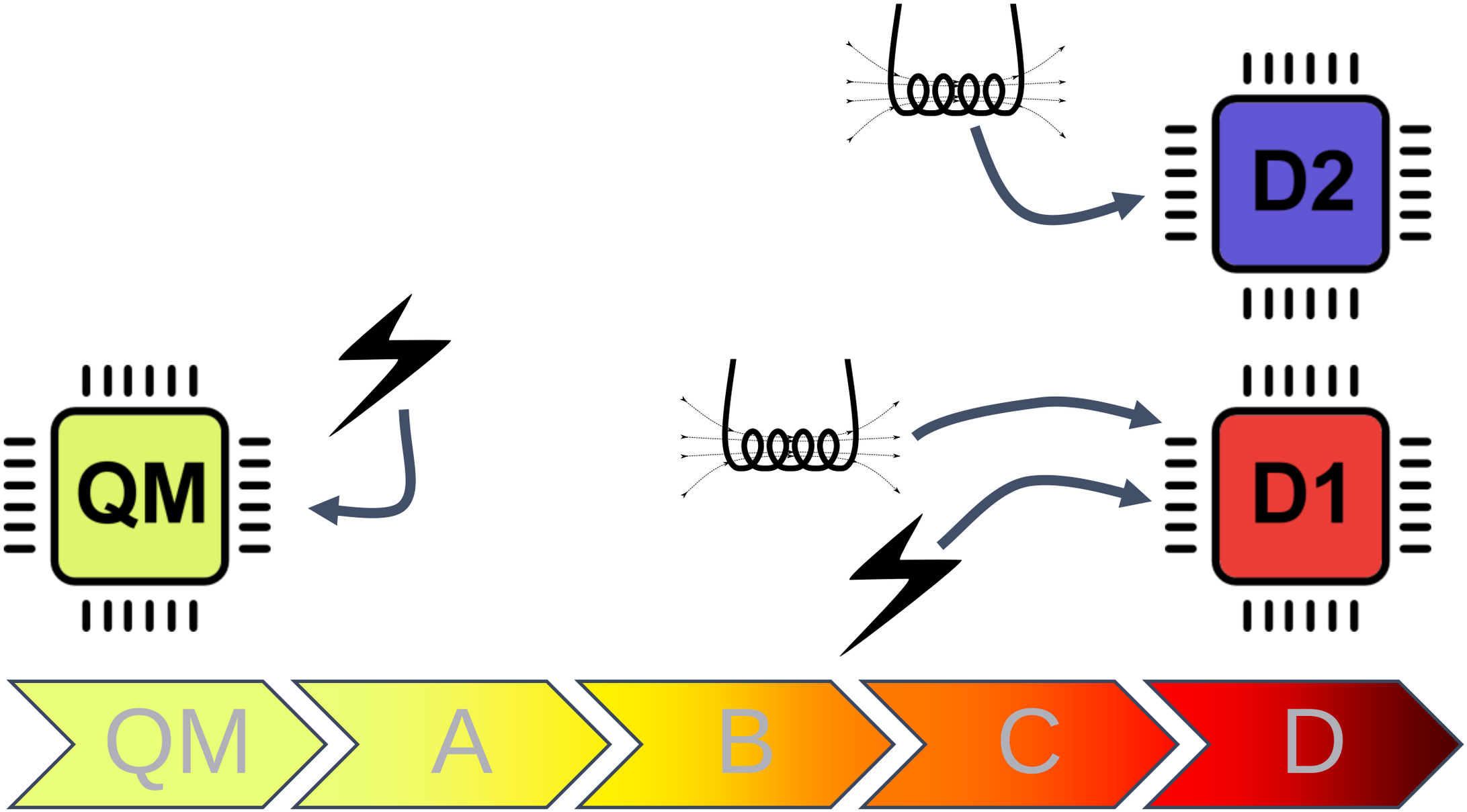


Voltage glitching



EM glitching

FI methods



Characterization experiment

```
counter = 0
…
counter++
counter++
counter++
counter++
…
counter++
print counter
```

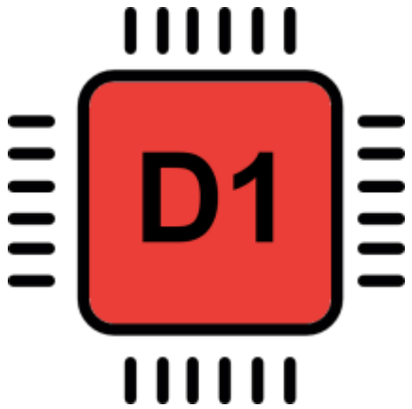
Characterization experiment

```
flag = 1
…
if (flag == 0):                  // flag == 1, so false
   authenticated()               // this is skipped
else
   not_authenticated()           // this is executed
```

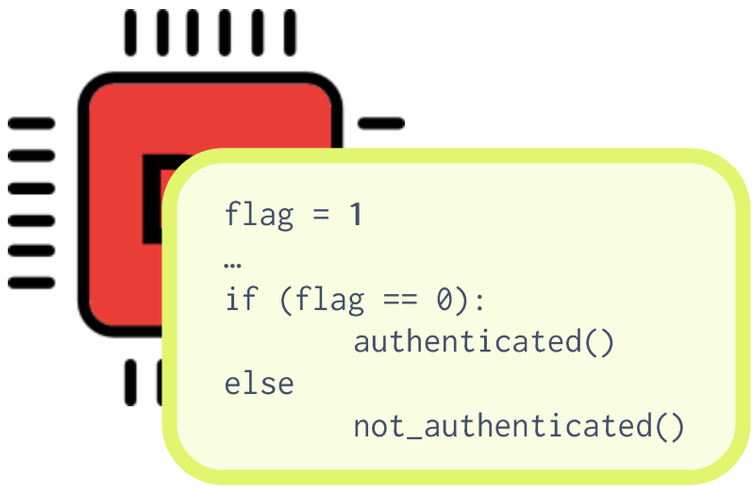
Characterization experiment

```
flag = 1
…
if (flag == 0):                    // skipped with FI
    authenticated()
else
    not_authenticated()
```

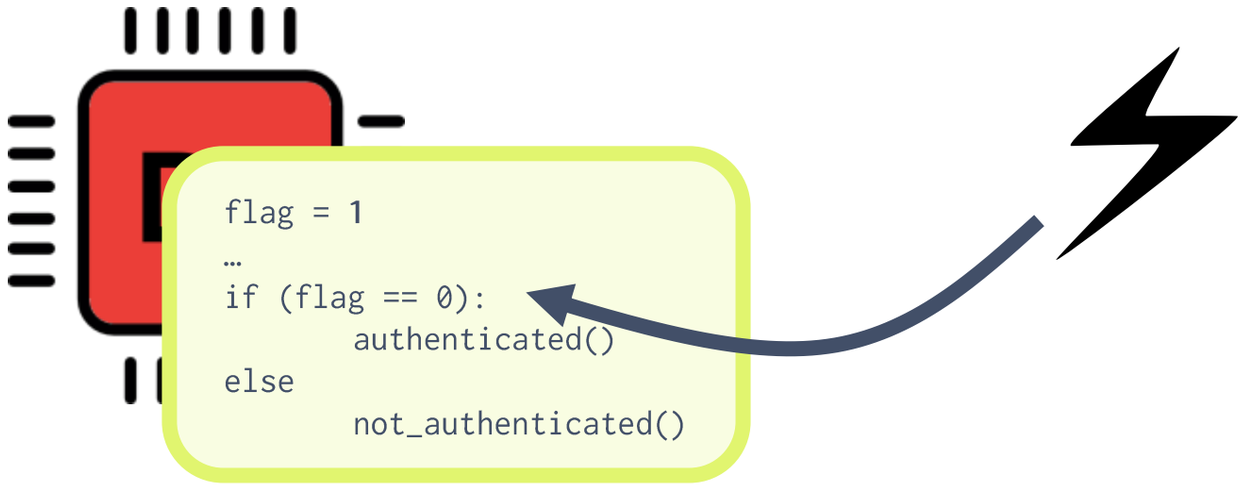
FI parameter tuning campaign



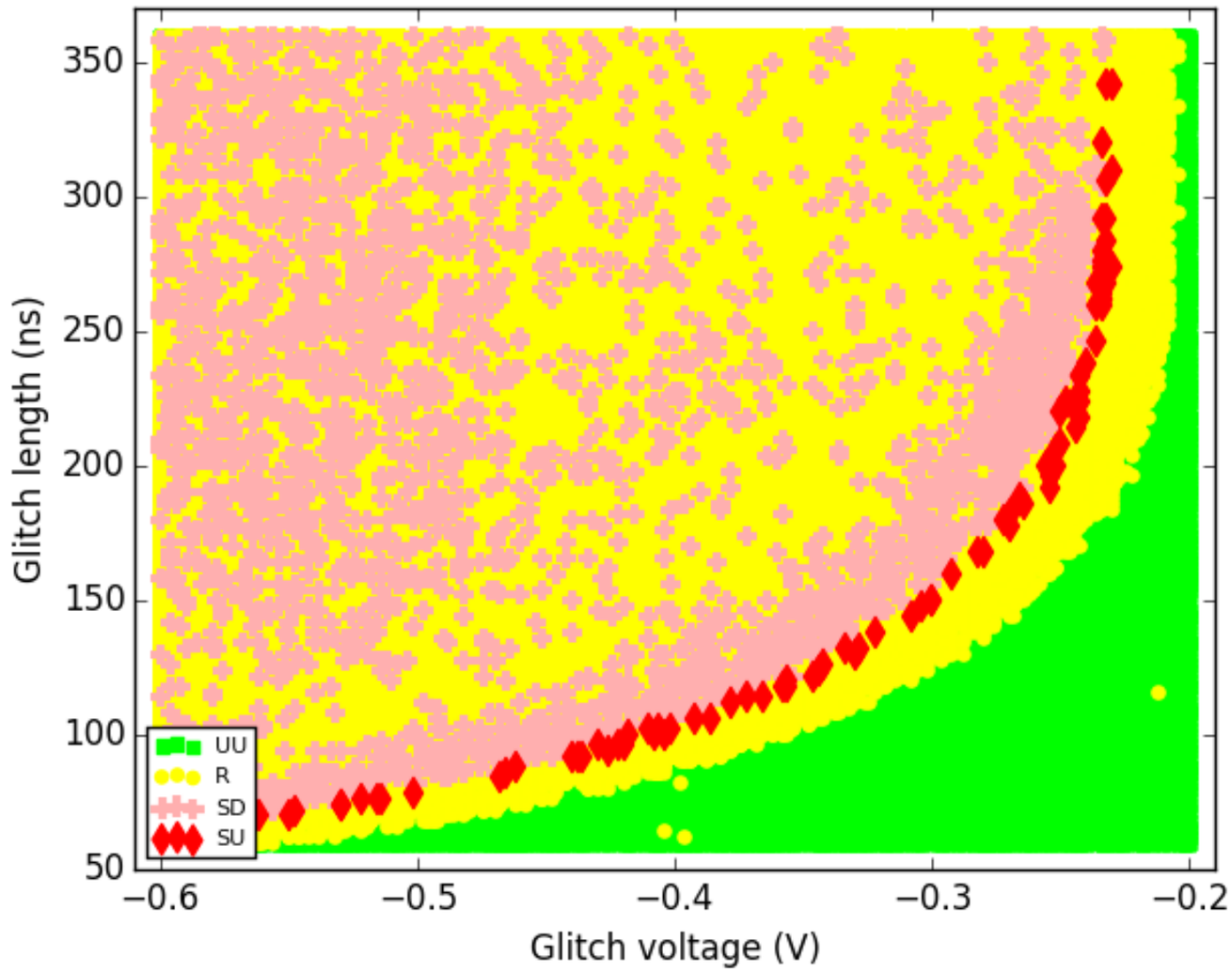
FI parameter tuning campaign



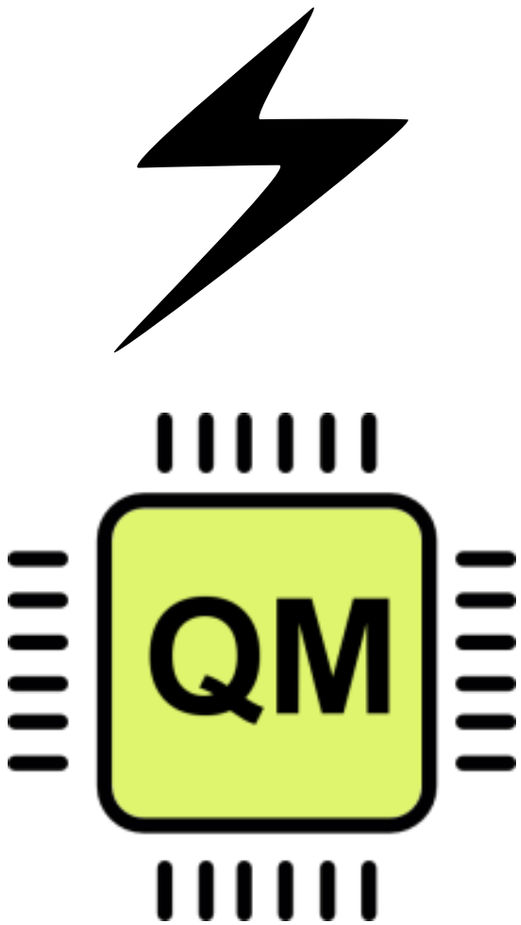
FI parameter tuning campaign



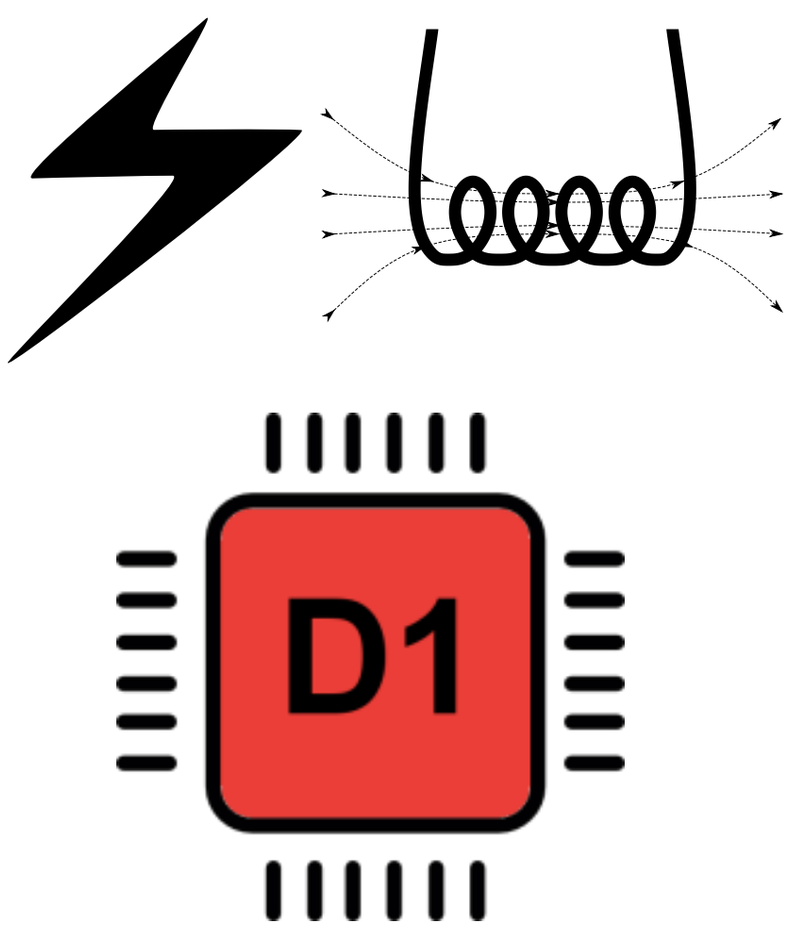
FI parameter tuning campaign



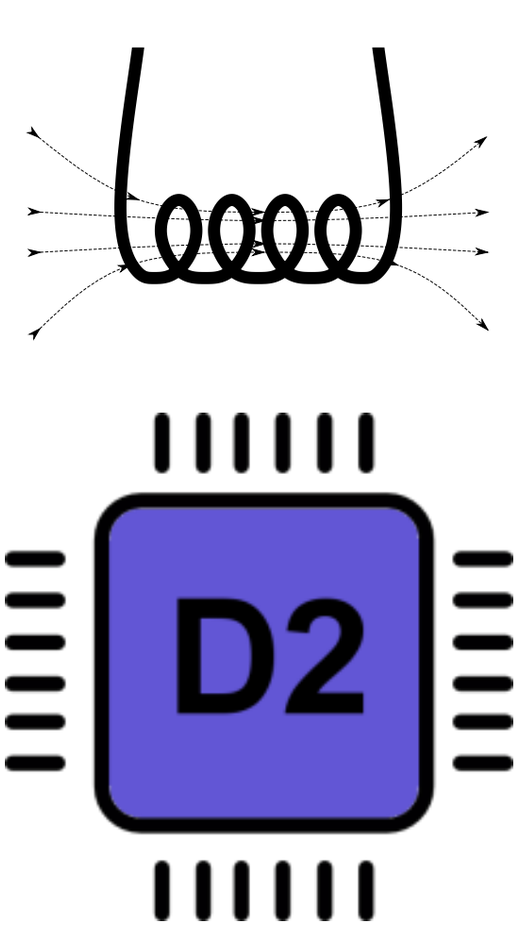
Characterization results
Success rate (average)



100%

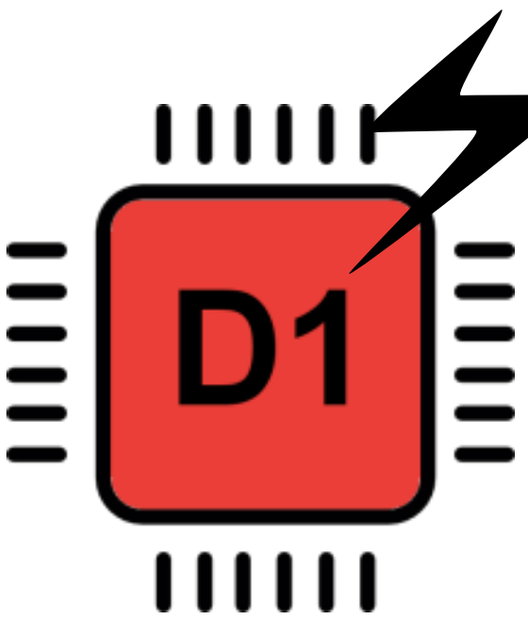


16%



37%

Characterization results
Countermeasure effectiveness (average)



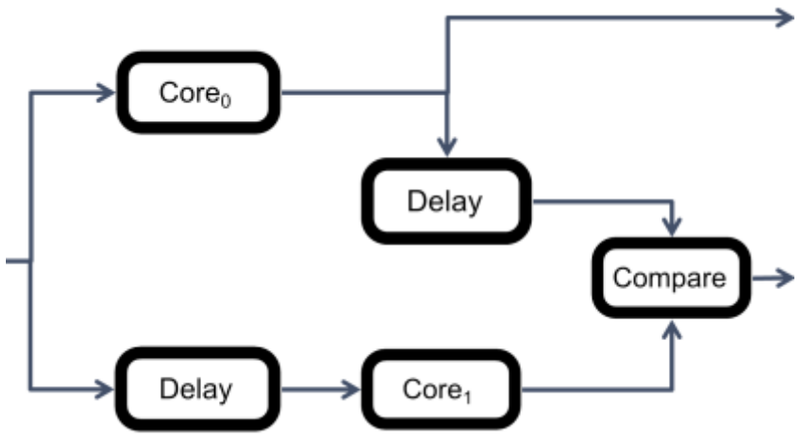
25%

01101010	0
10101101	1
10011010	0
10101010	0
01110101	1
01101101	0
11010101	1

FLASH ECC **68%**

OTP ECC **20%**

RAM parity **14%**



90%

Characterization results
Conclusion

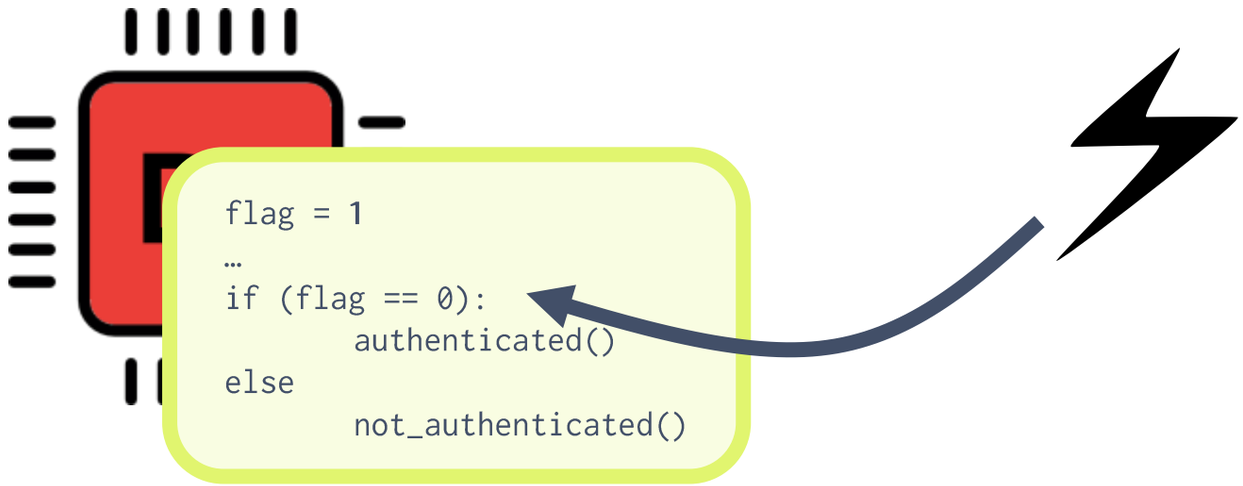
Characterization results
Conclusion

CONFIRMED

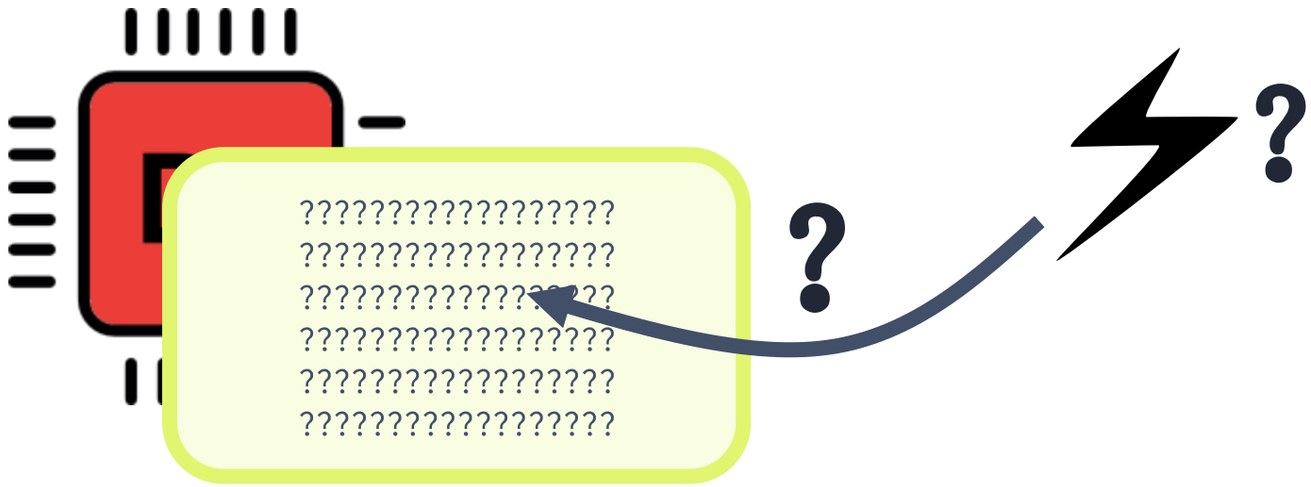
ISO26262 ≠ Security

Breaking JTAG

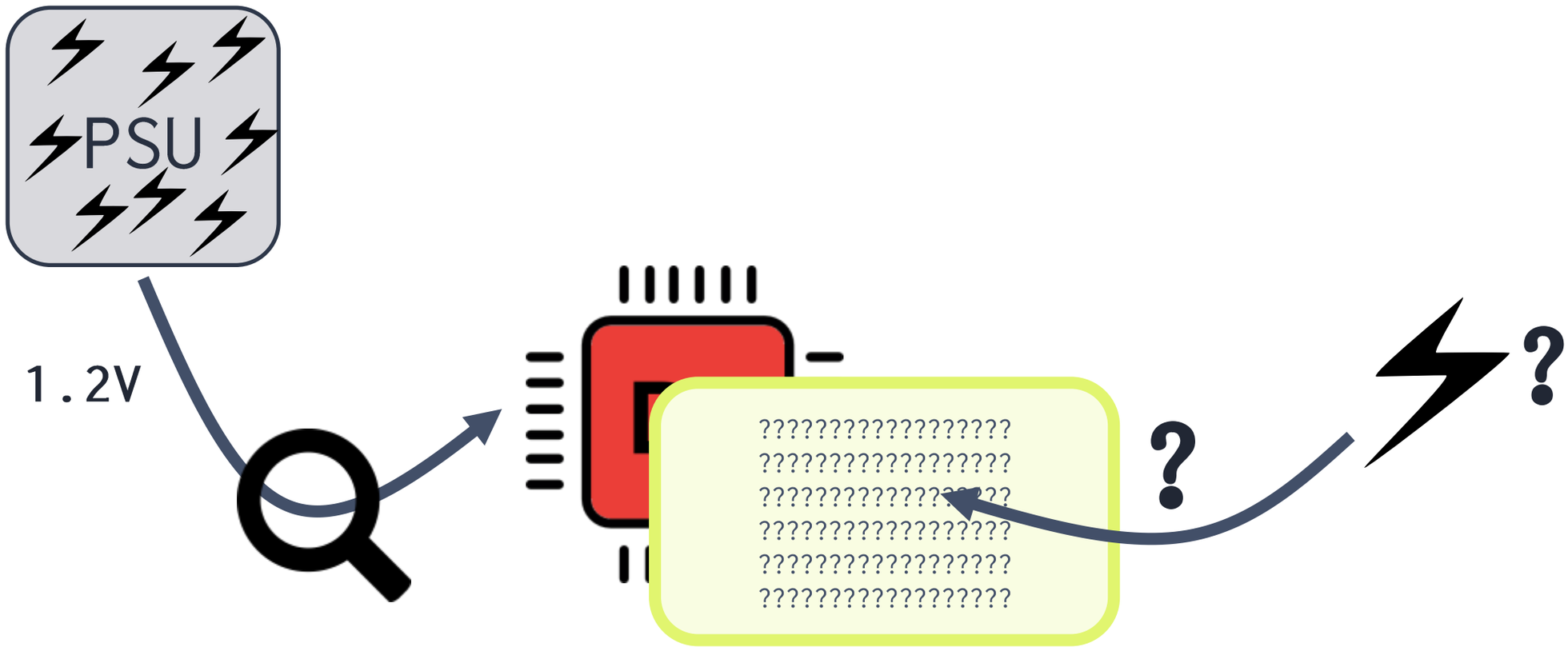
Unlocking JTAG
Setup



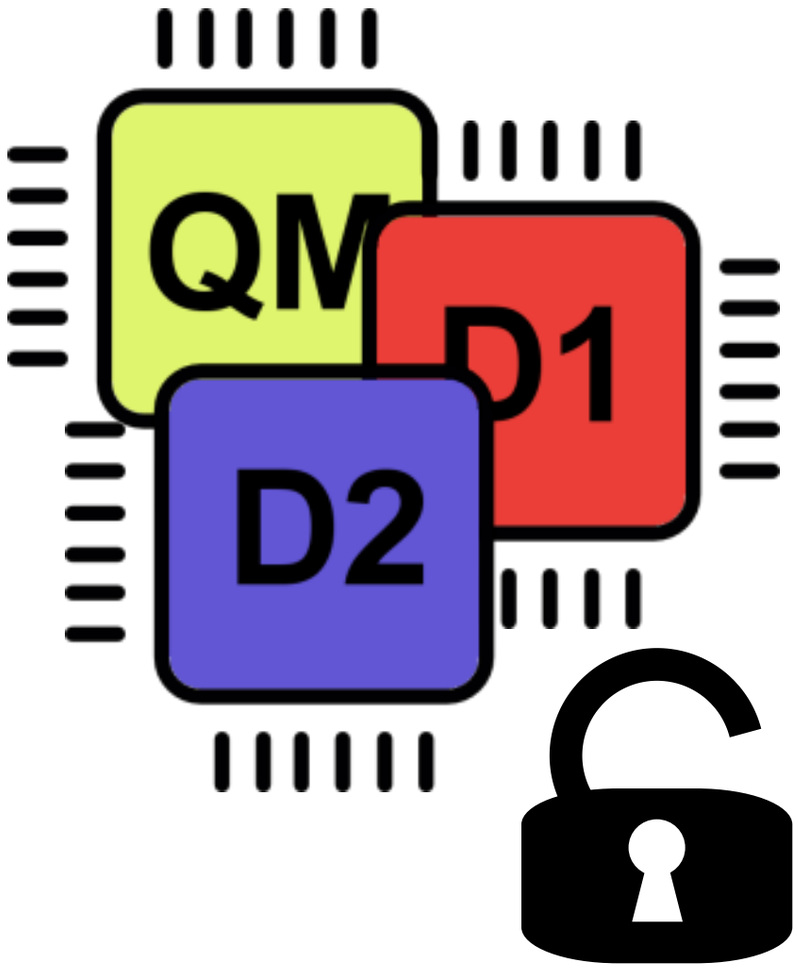
Unlocking JTAG
Setup



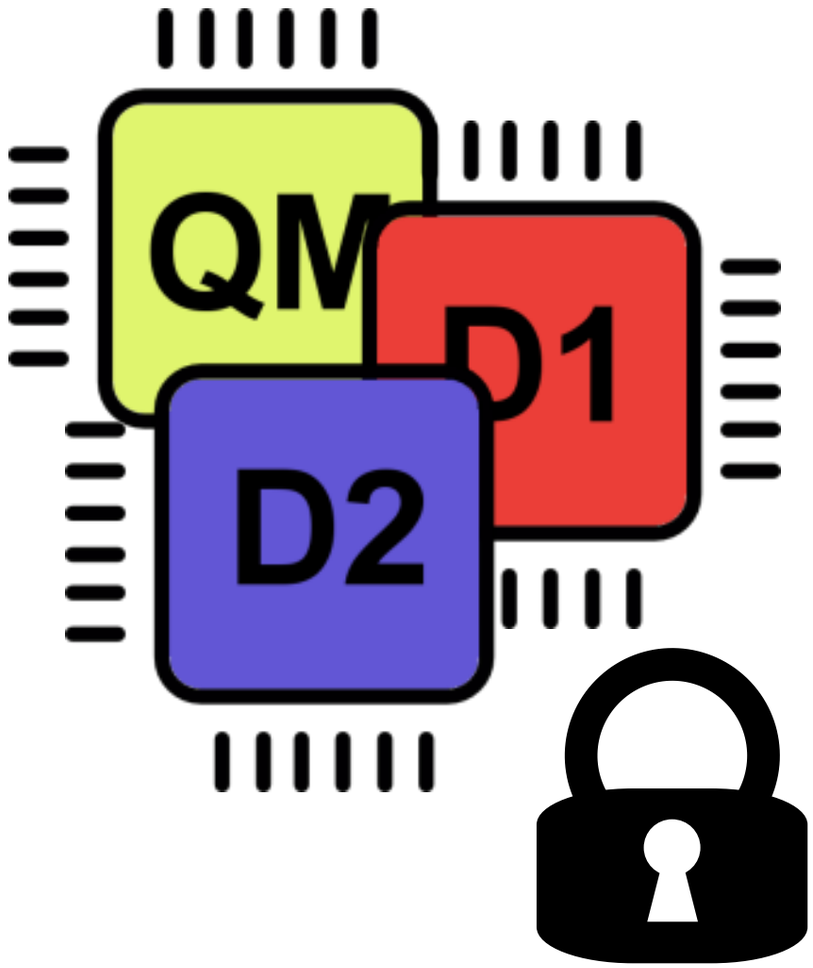
Unlocking JTAG
Setup



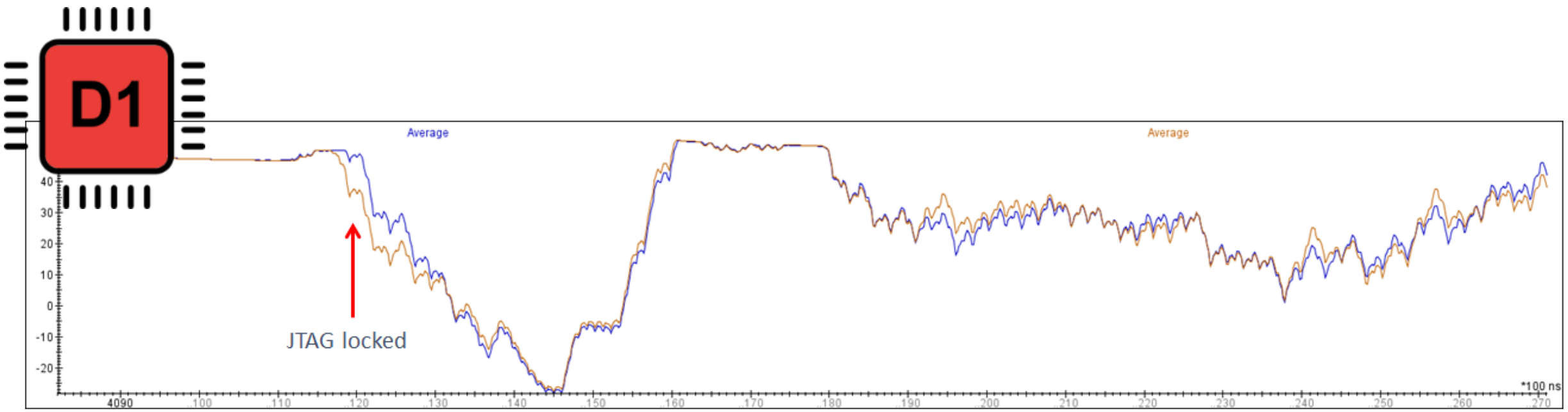
Unlocking JTAG
Differential power analysis



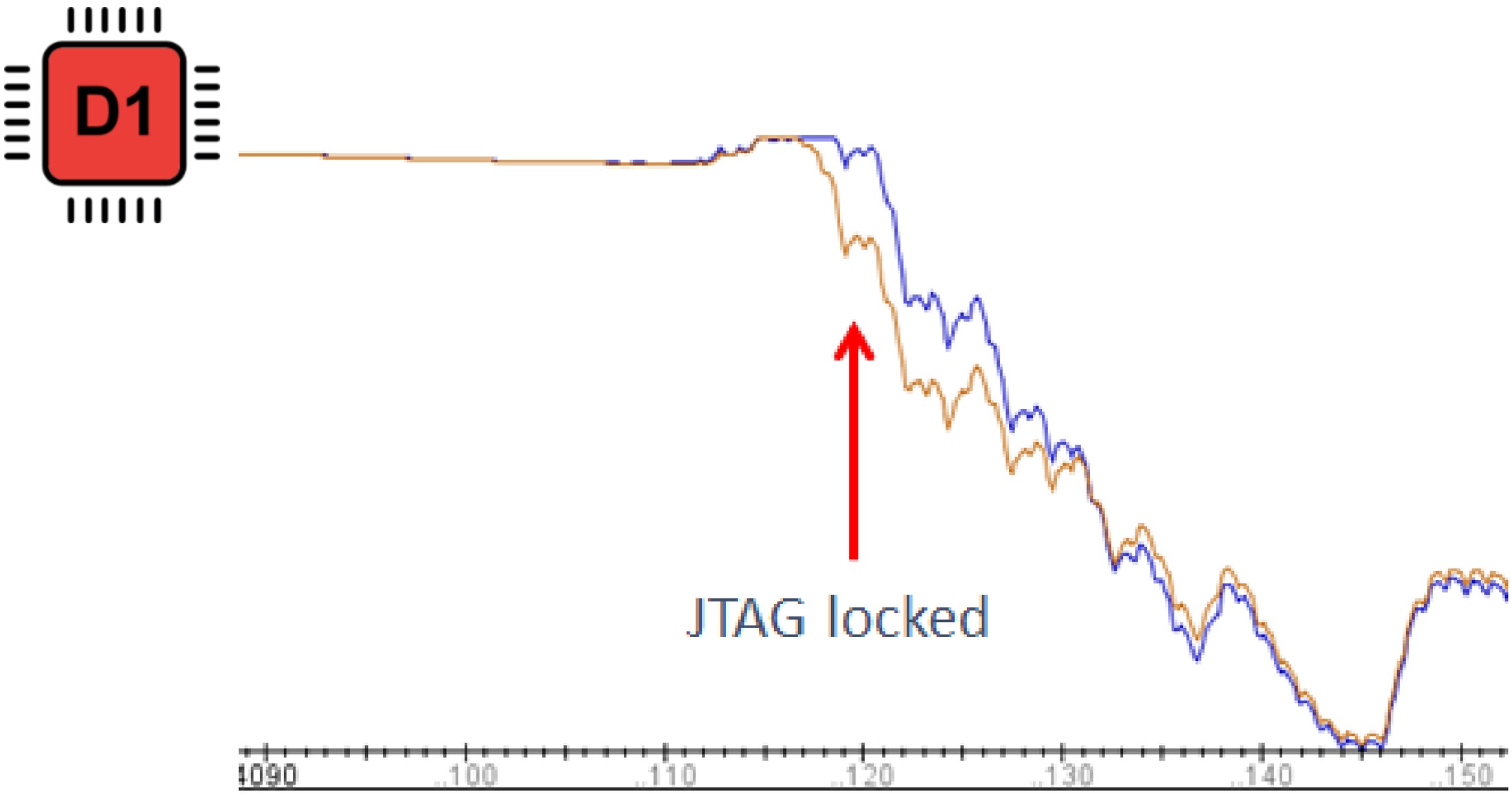
VS.



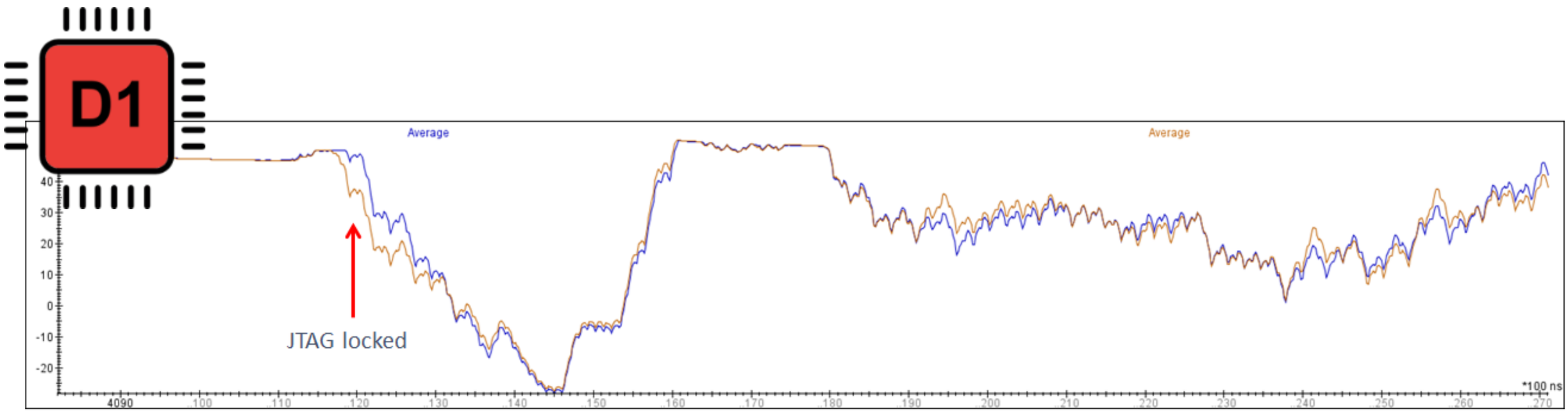
Unlocking JTAG
Differential power analysis

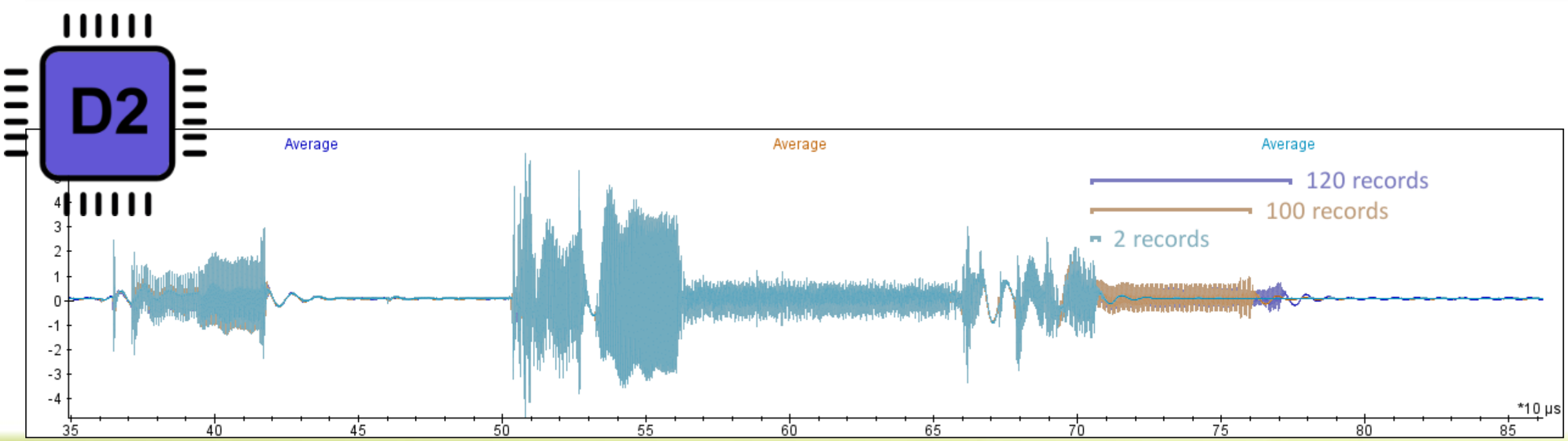


Unlocking JTAG
Differential power analysis

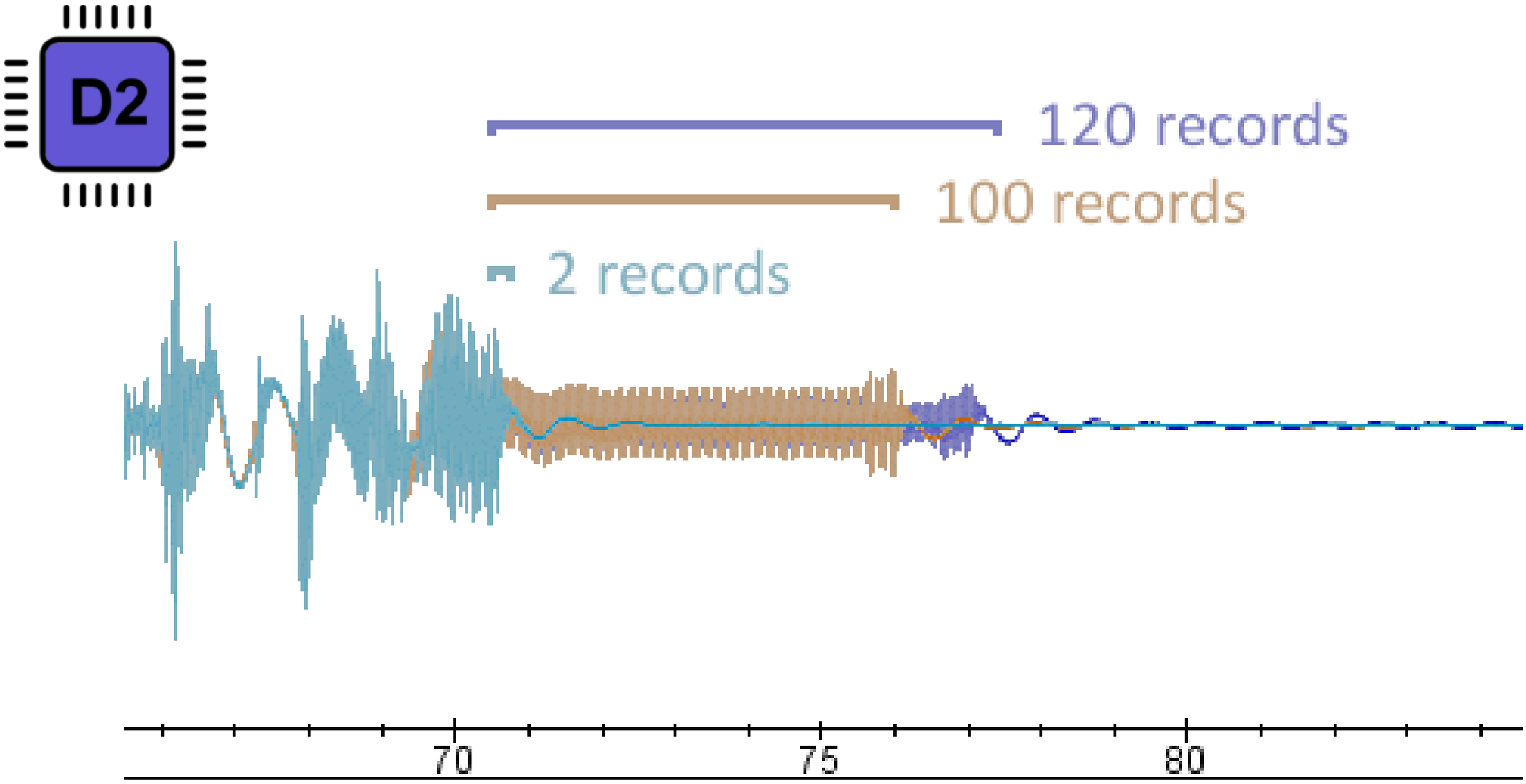


Unlocking JTAG
Differential power analysis

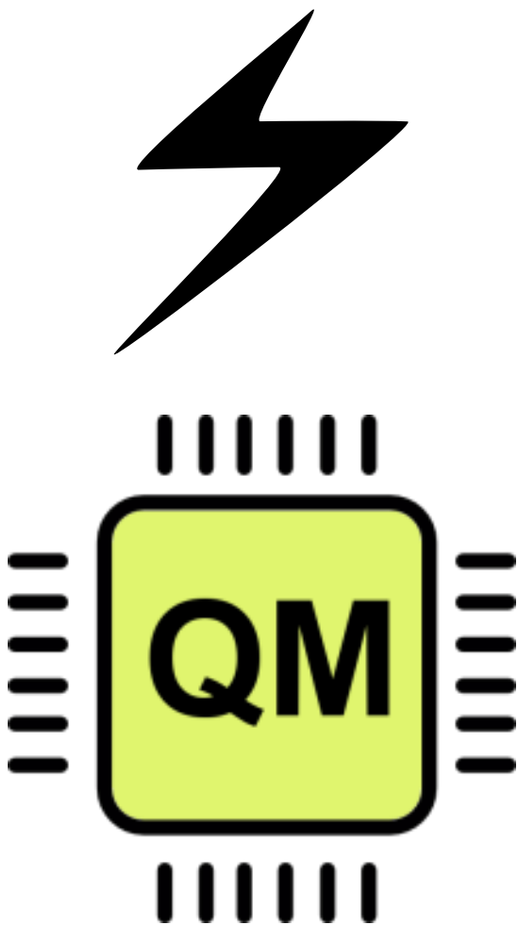


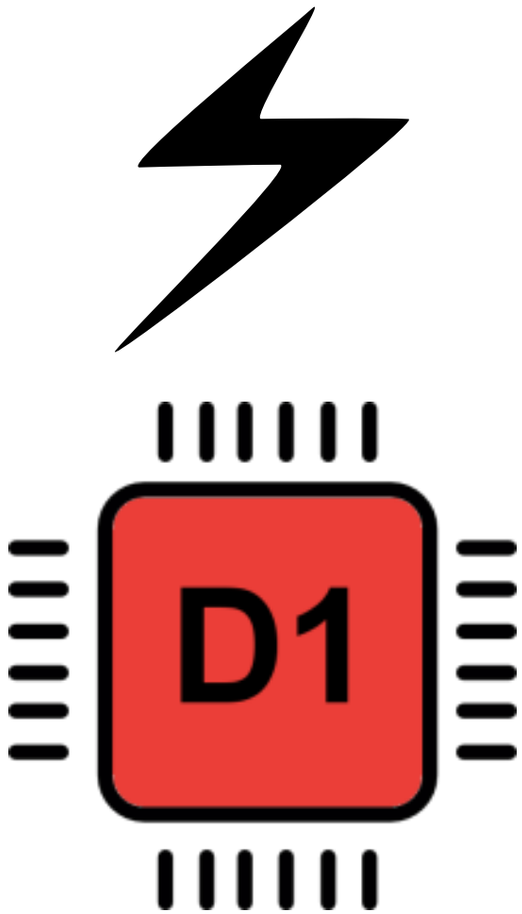


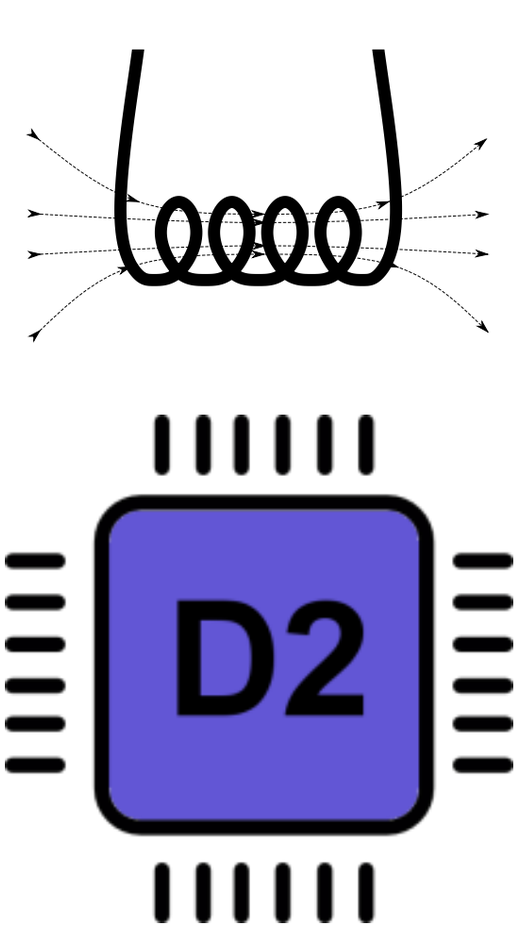
Unlocking JTAG
Differential power analysis



Unlocking JTAG
Success rate



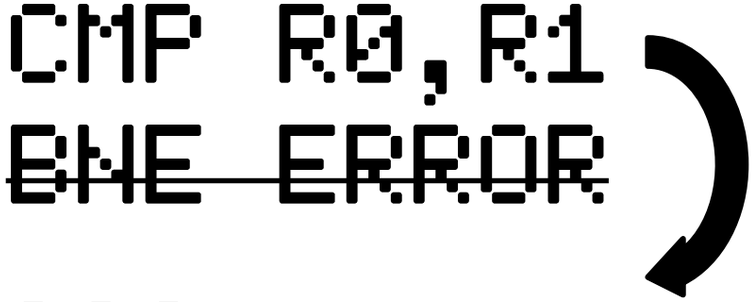




🔓	80%	1.3%	0.34%
🚨	N/A	3.2%	<0.01%

Consequences

Consequences



Change
execution flow

Unlock
JTAG

Consequences

IP stealing

Attack escalation

Firmware modification

Consequences

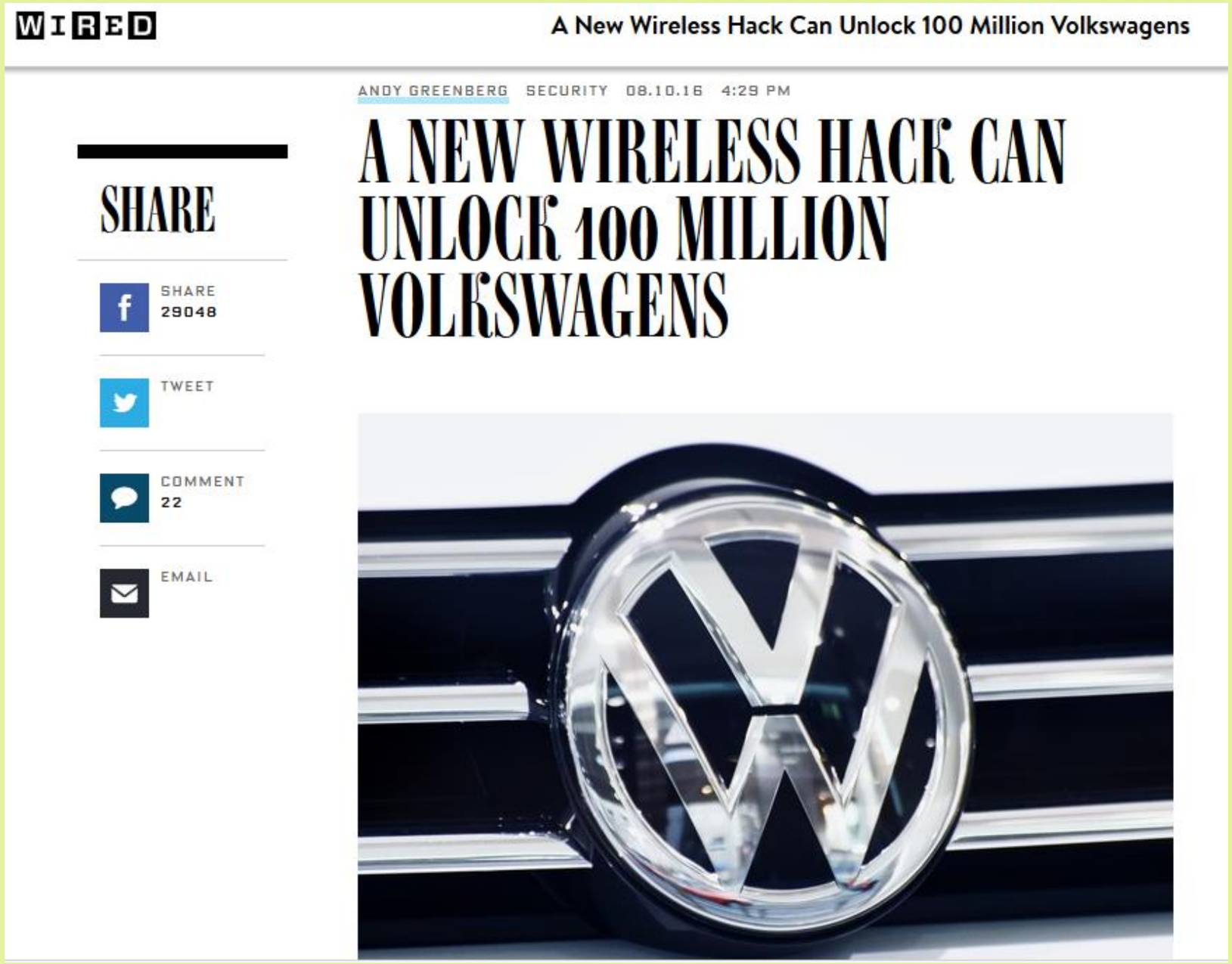
IP stealing

Attack escalation

- Firmware reversing
- Remote exploit finding
- Keys extraction
  - UDS
  - OTA
  - RKE
  - IMMO

Firmware modification

IP stealing + reversing



WIRED

A New Wireless Hack Can Unlock 100 Million Volkswagens

ANDY GREENBERG SECURITY 08.10.16 4:29 PM

A NEW WIRELESS HACK CAN UNLOCK 100 MILLION VOLKSWAGENS

SHARE

SHARE 29048

TWEET

COMMENT 22

EMAIL

Consequences

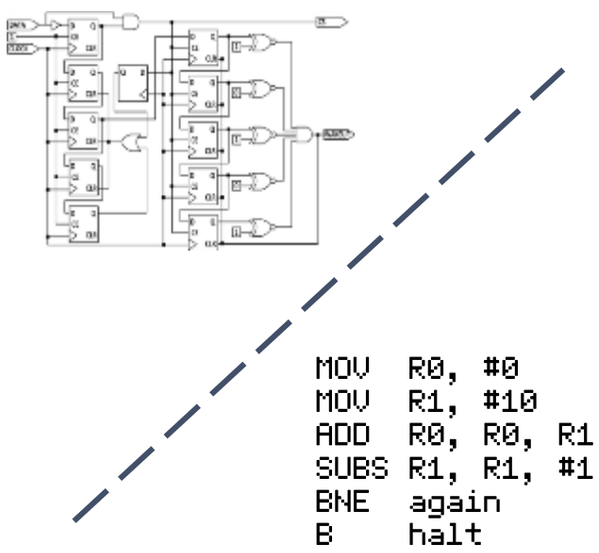
IP stealing

Attack escalation

Firmware modification

- Tuning
- Sabotage

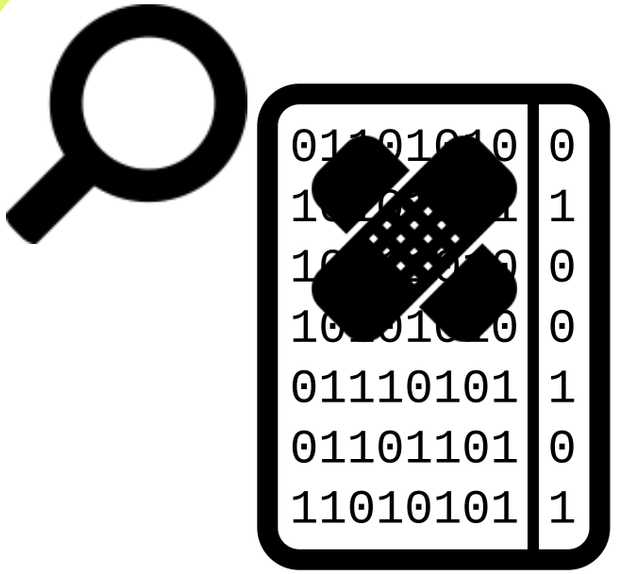
Recommendations



```
MOV  R0, #0
MOV  R1, #10
ADD  R0, R0, R1
SUBS R1, R1, #1
BNE  again
B    halt
```

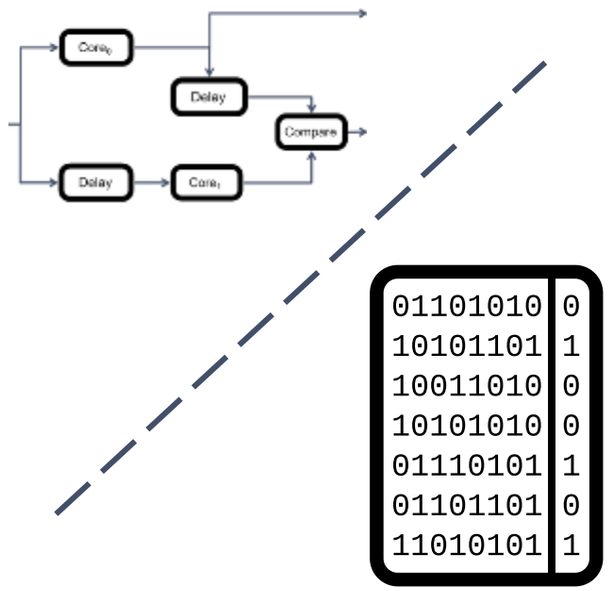
Add HW/SW countermeasures

Don’t reinvent the wheel

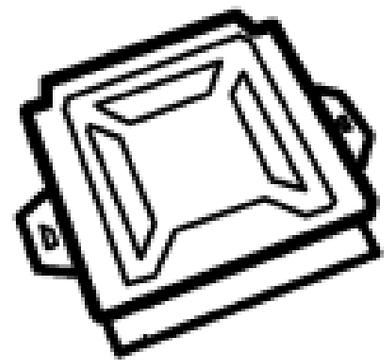


Don’t trust in recovered errors

Future work



Individual characterization of safety mechanism



ECUs in the market

UDS bypassing

Future Standards for Automotive CPU

SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (ACSIL)
SAE J3101	Requirements for Hardware-Protected Security for Ground Vehicle Applications

Questions?

Contact: Ramiro Pareja & Nils Wiersma
pareja@riscure.com / wiersma@riscure.com

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America
550 Kearny St.
Suite 330
San Francisco, CA 94108
+1 (650) 646 9979

inforequest@riscure.com