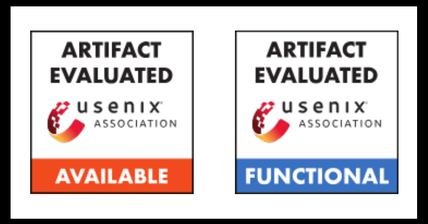


Remote Code Execution by Laser Excitation of P–N Junctions

Joe Loughry and Kasper Rasmussen

WOOT’24, Philadelphia, 12–13 August


SERVICE
ENGINE
SOON

Mnemonic	Opcode	Instruction
NOP	0000	no operation
LDA	0001	load accumulator (addr)
INC	0010	increment accumulator
DEC	0011	decrement accumulator
STA	0100	store accumulator (addr)
BZ	0101	branch if A ≠ 0 (addr)
JMP	0110	unconditional branch (addr)
SR	0111	shift right accumulator
LDI	1001	load immediate

Table 1: M5 instruction set. It consists of 9 instructions including NOP. This is intentionally simple but Turing complete.

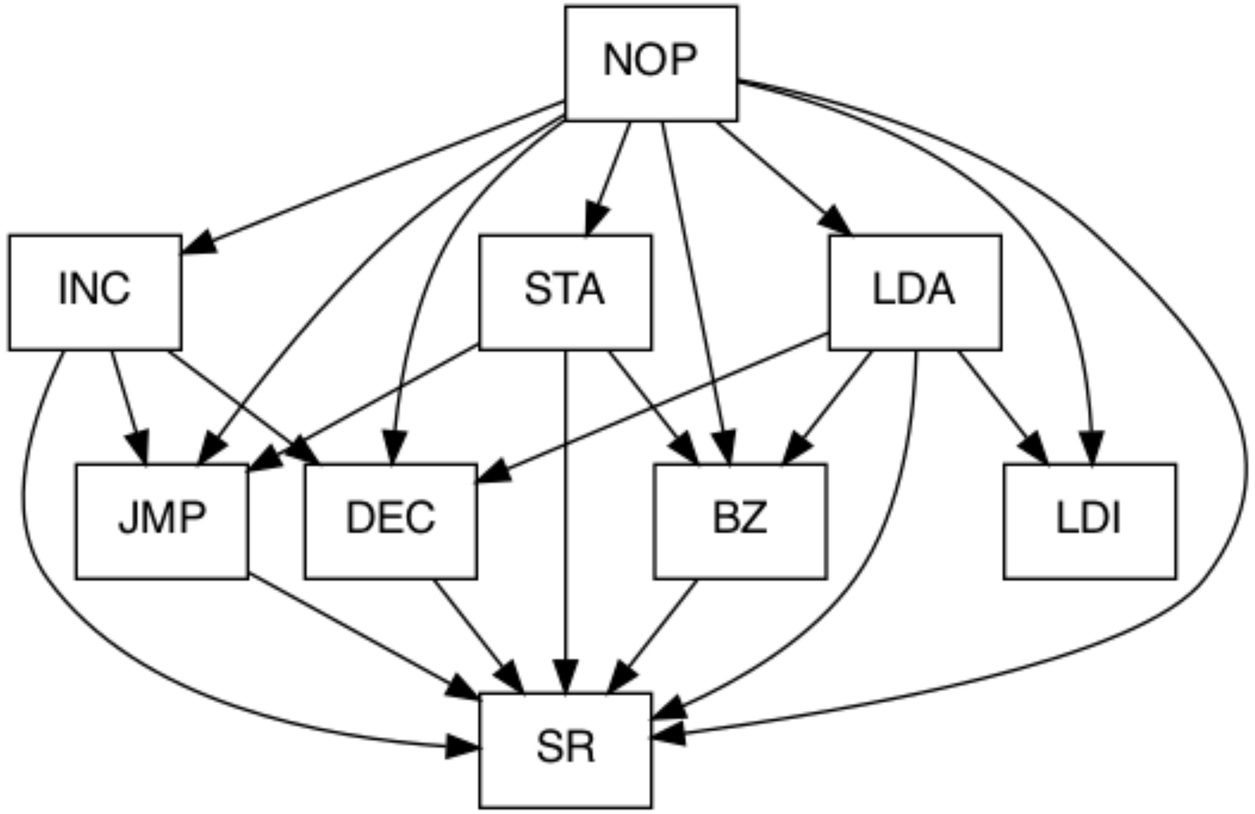
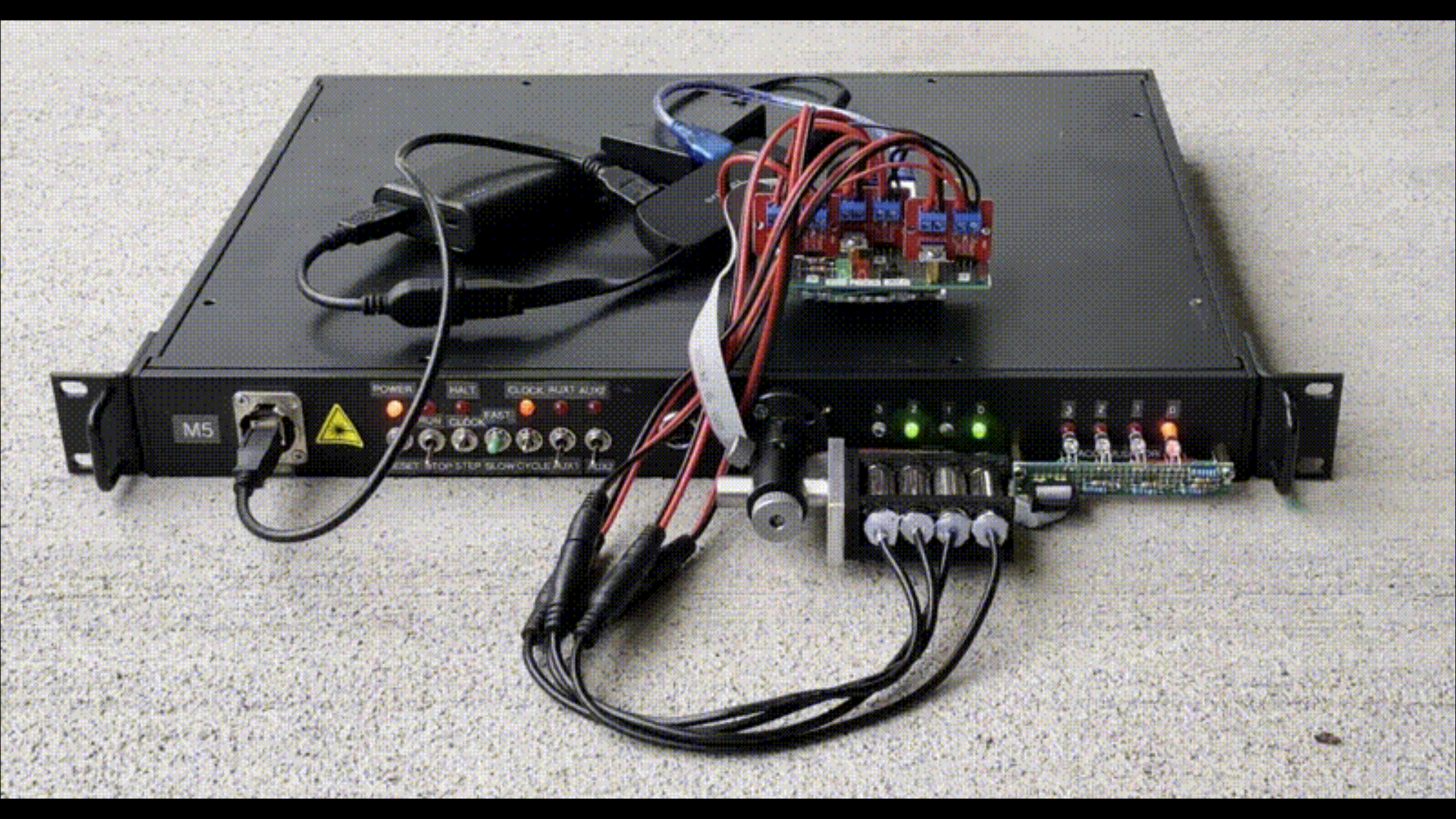
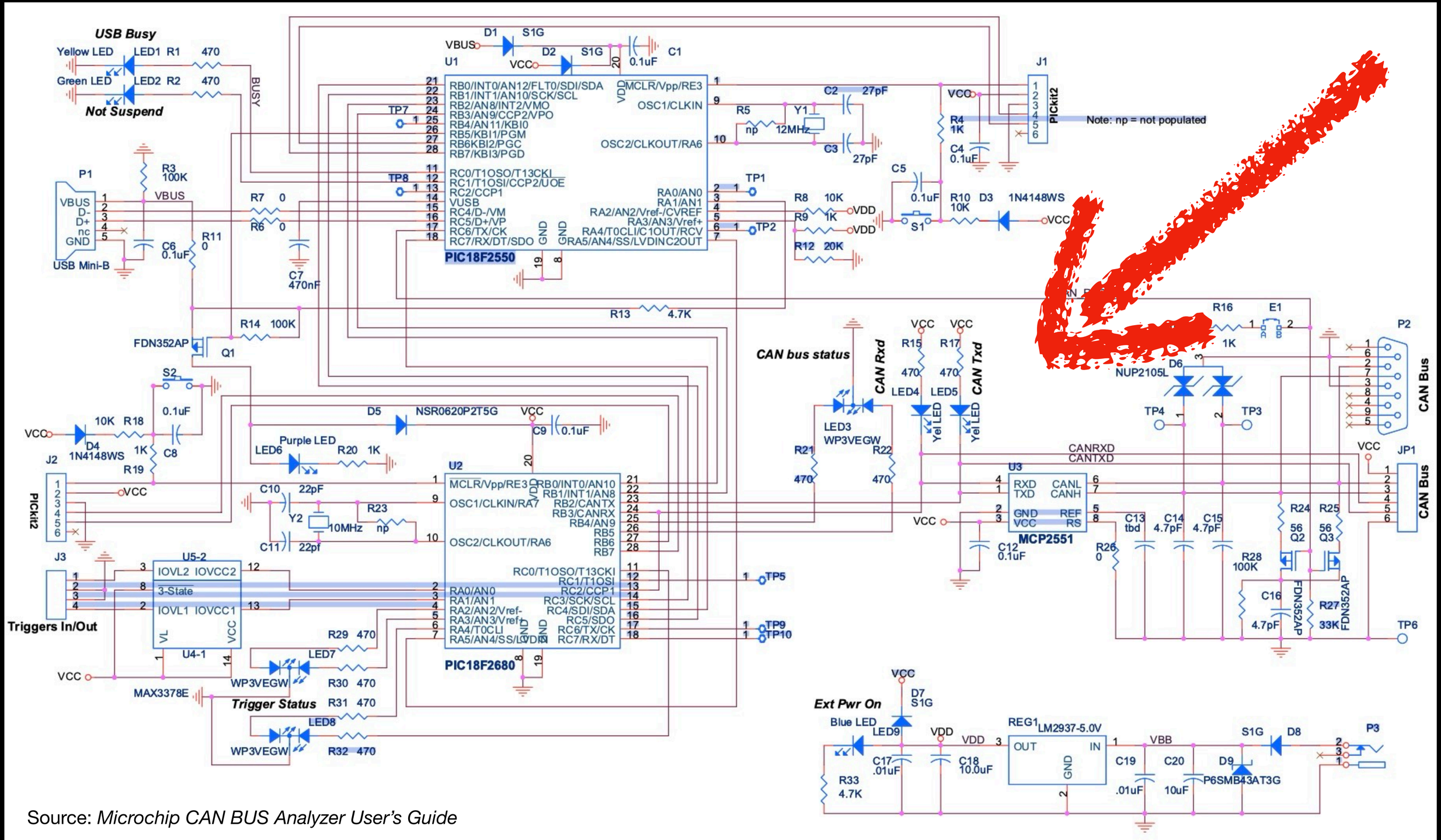
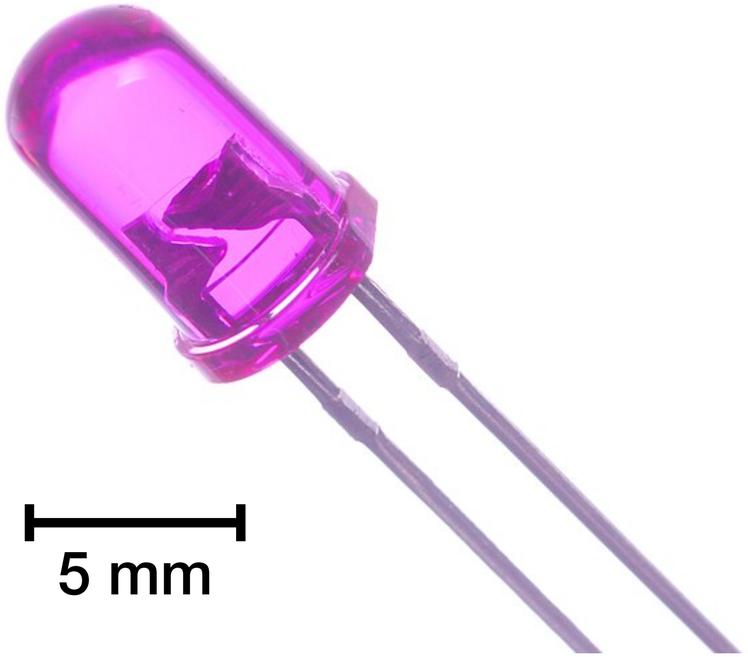


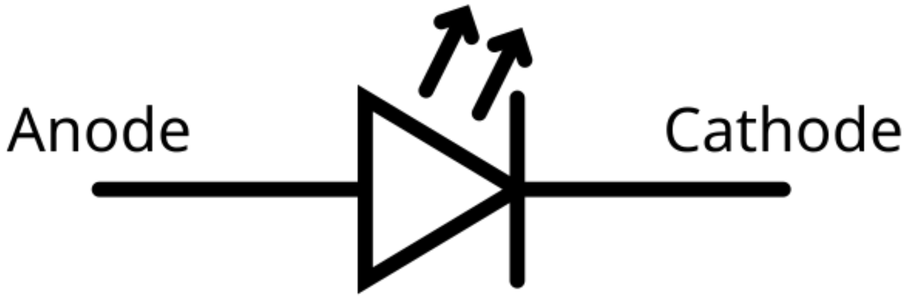
Figure 17: Allowable transitions in the instructions set of the computer defined in Table 1 if the attacker can only set bits, but not reset them.


M5
POWER
HALT
CLOCK
AUX1
AUX2
RUN
FAST
RESET
STOP
STEP
SLOW
CYCLE



Source: *Microchip CAN BUS Analyzer User's Guide*





Source: Wikimedia Commons

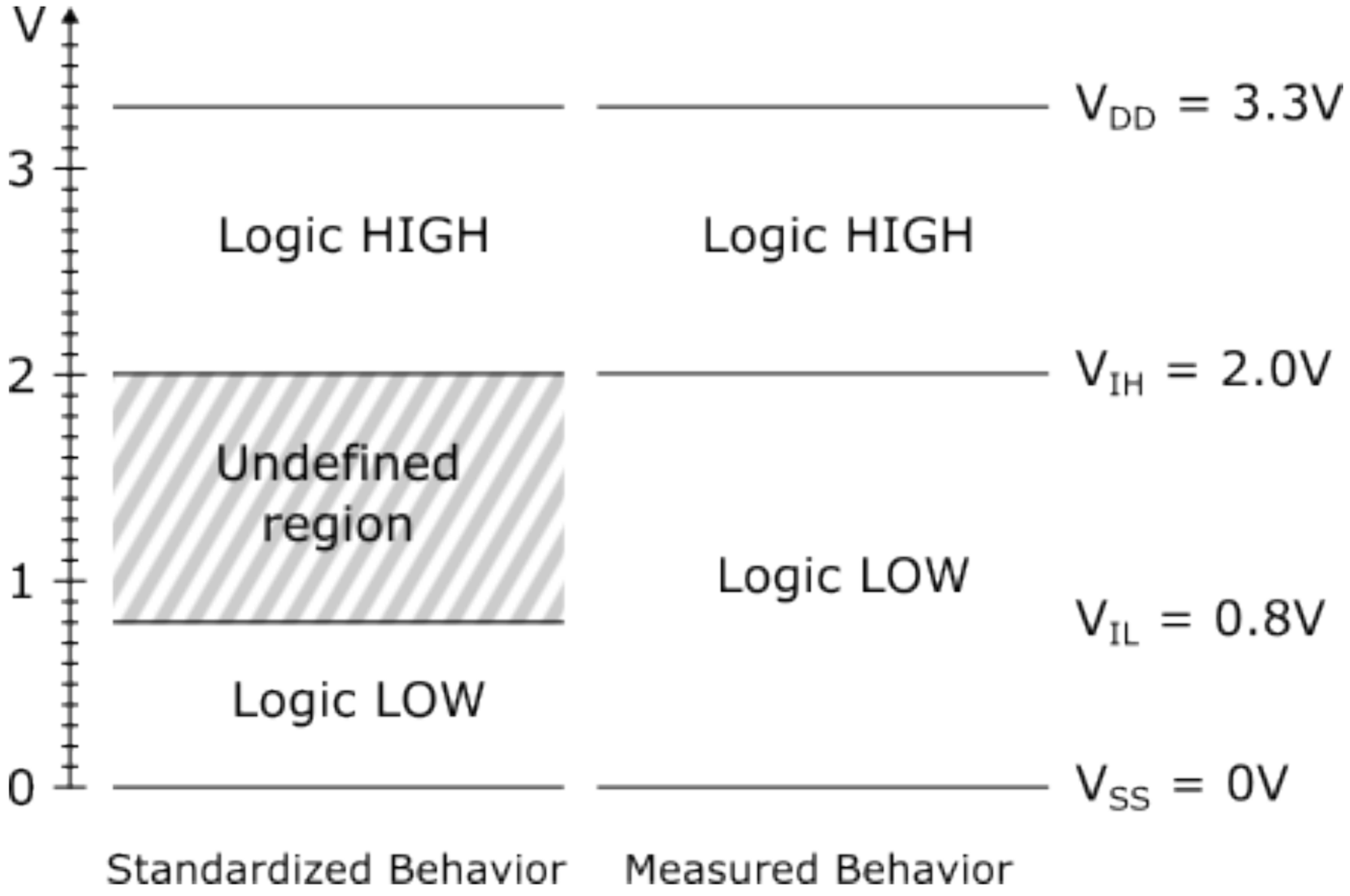
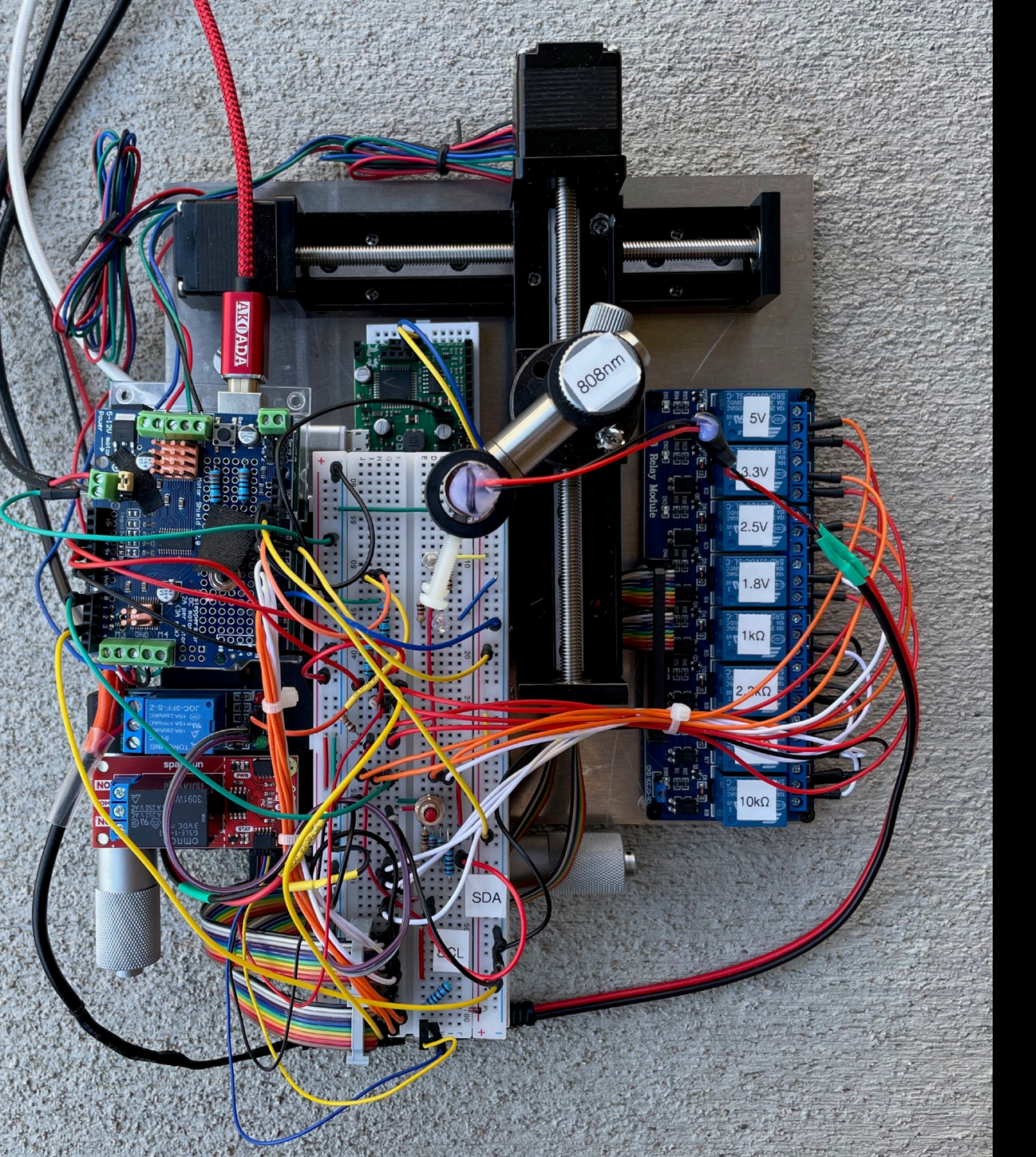
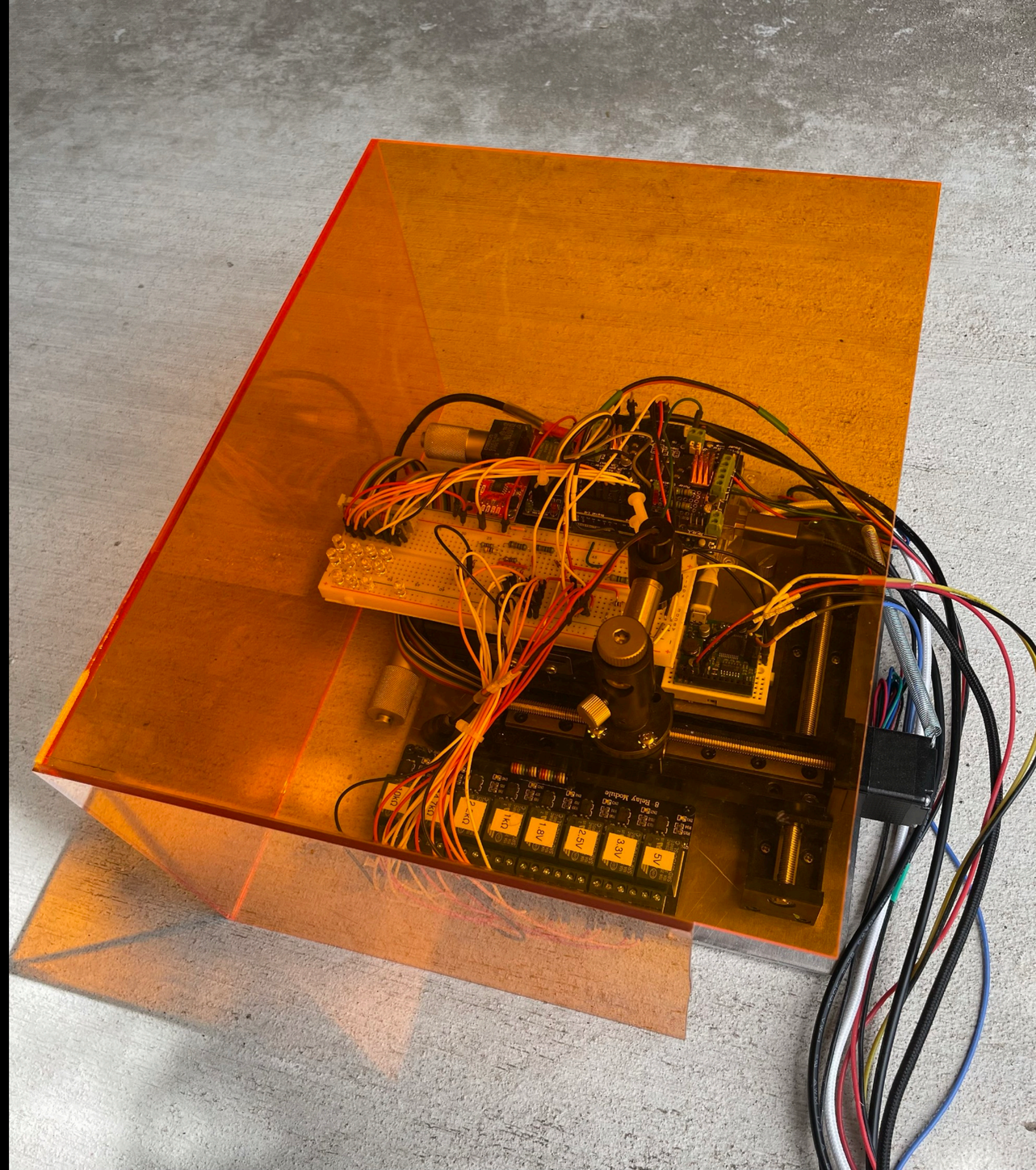
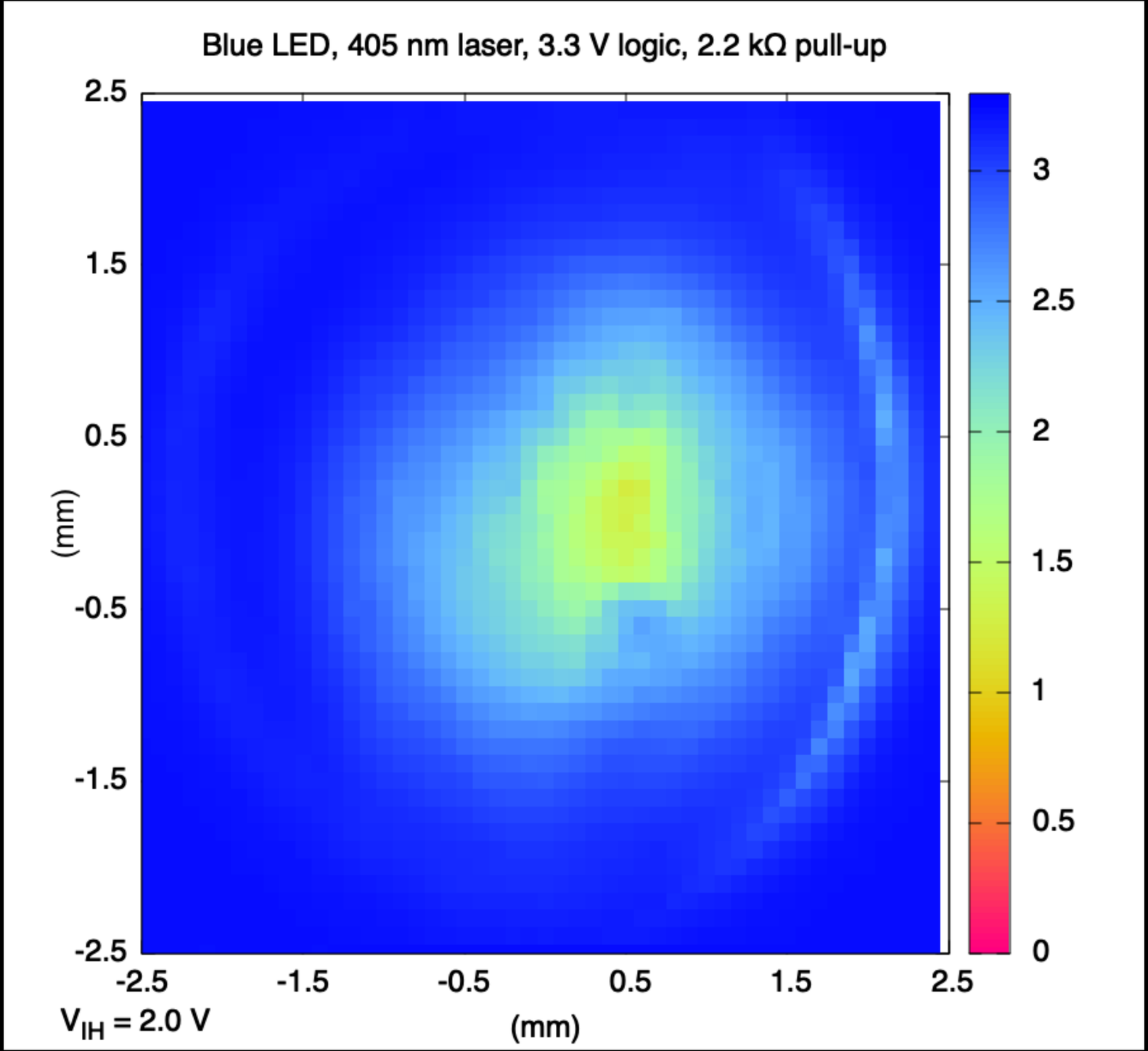
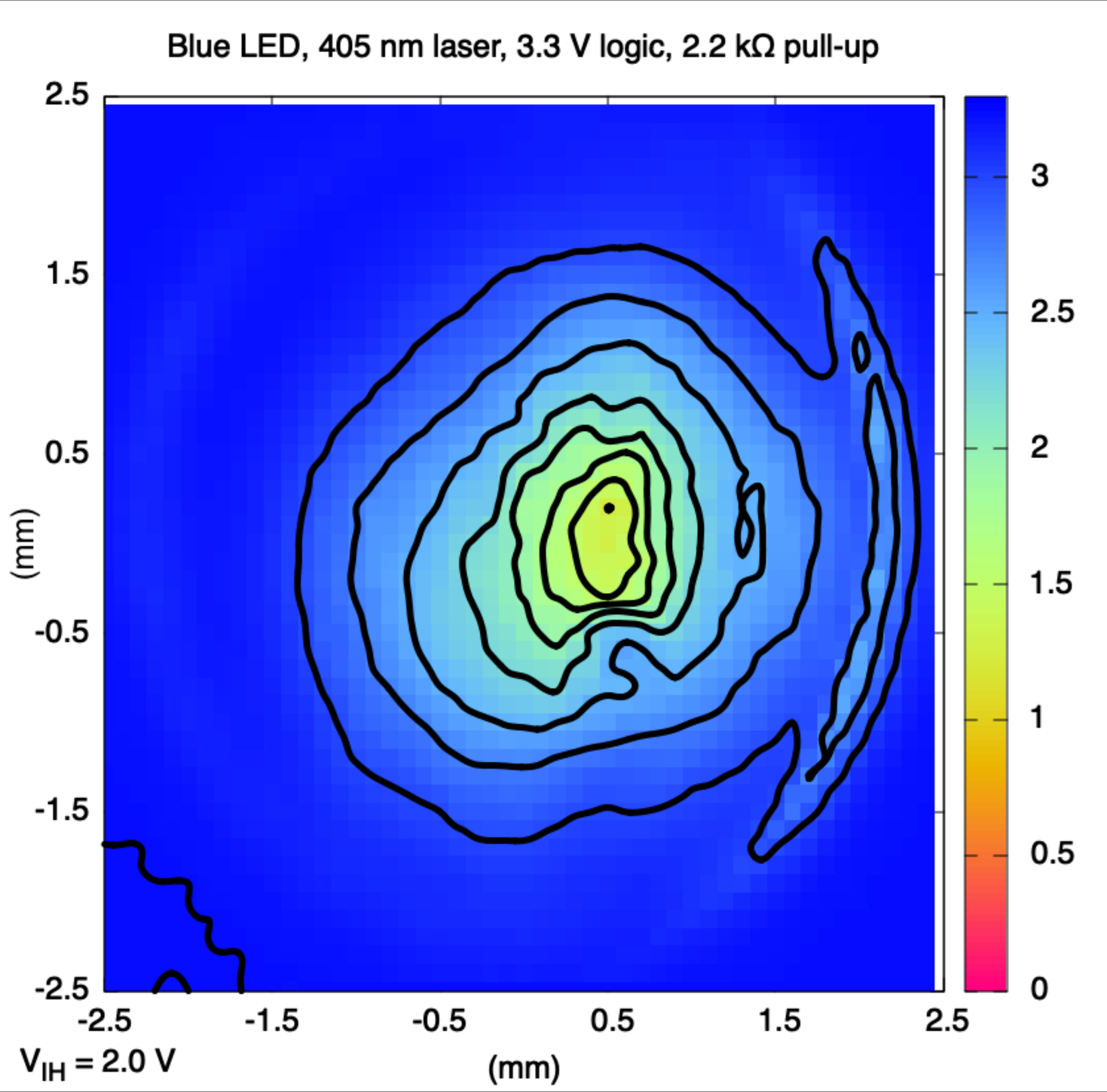


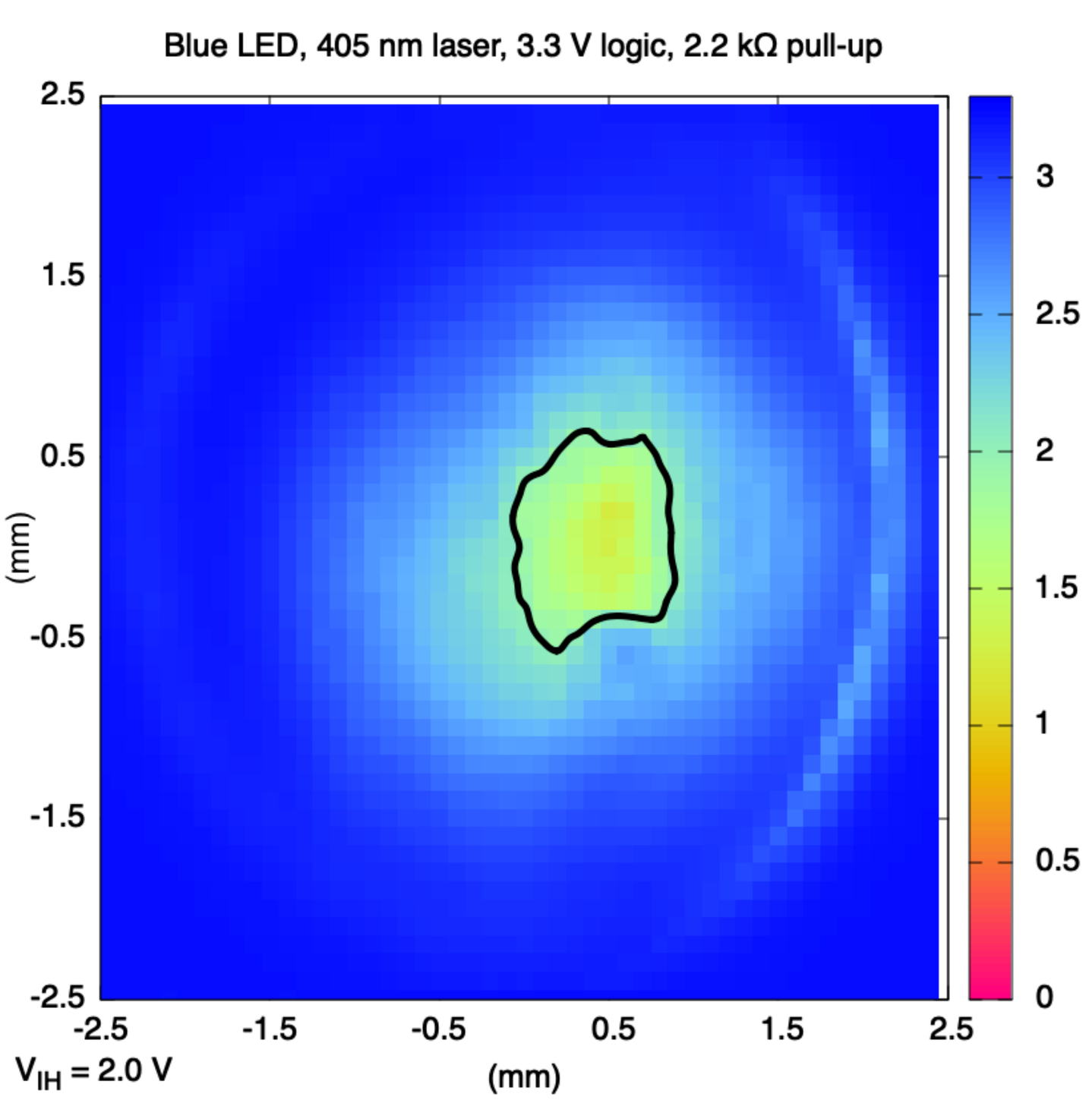
Figure 4. CMOS logic levels for 3.3 V circuits. Signals above 2 V are logic high, and below 0.8 V are logic low. In all our experiments we found that devices will default to a logic low condition in the undefined region, so although it ought never to be used, a signal below 2 V is sufficient for an attack.


AKOADA
808nm
8 Relay Module
5V
3.3V
2.5V
1.8V
1kΩ
10kΩ
SDA
SCL

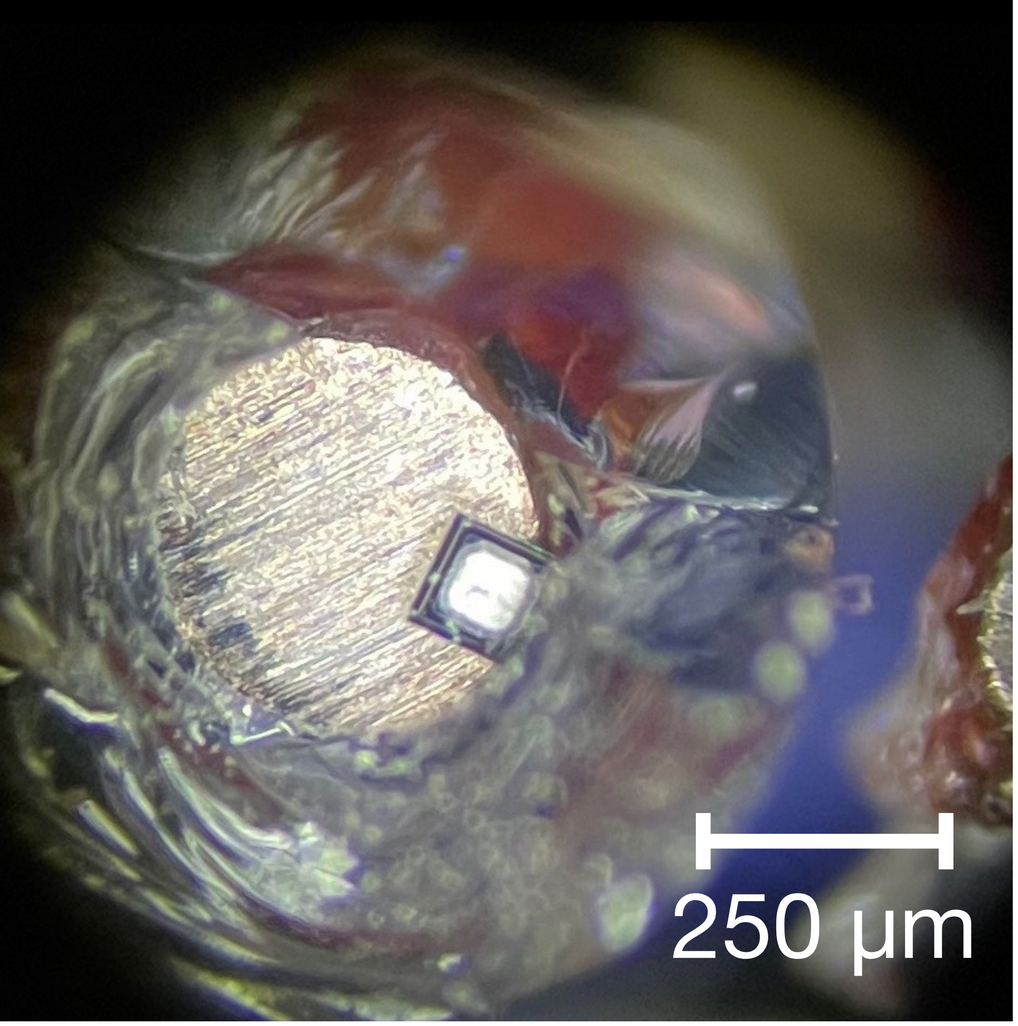

10kΩ
1kΩ
1.8V
2.5V
3.3V
5V

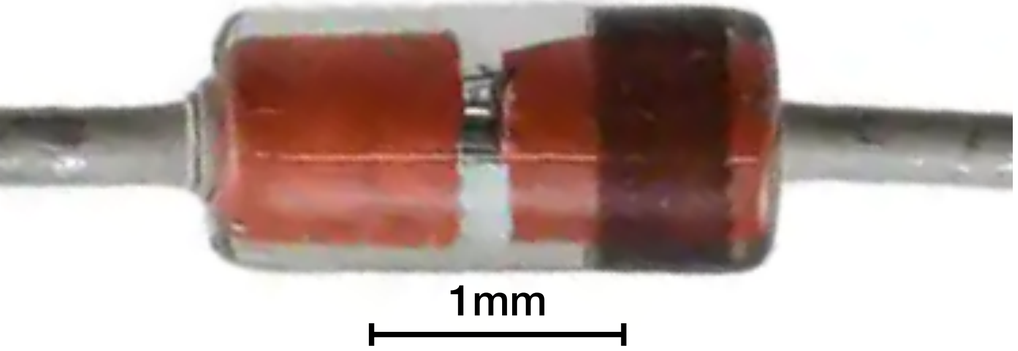

Blue LED, 405 nm laser, 3.3 V logic, 2.2 kΩ pull-up
2.5
1.5
0.5
-0.5
-1.5
-2.5
(mm)
-2.5
-1.5
-0.5
0.5
1.5
2.5
(mm)
3
2.5
2
1.5
1
0.5
0
V_{IH} = 2.0 V


Blue LED, 405 nm laser, 3.3 V logic, 2.2 kΩ pull-up
2.5
1.5
0.5
-0.5
-1.5
-2.5
(mm)
-2.5
-1.5
-0.5
0.5
1.5
2.5
(mm)
3
2.5
2
1.5
1
0.5
0
V_{IH} = 2.0 V

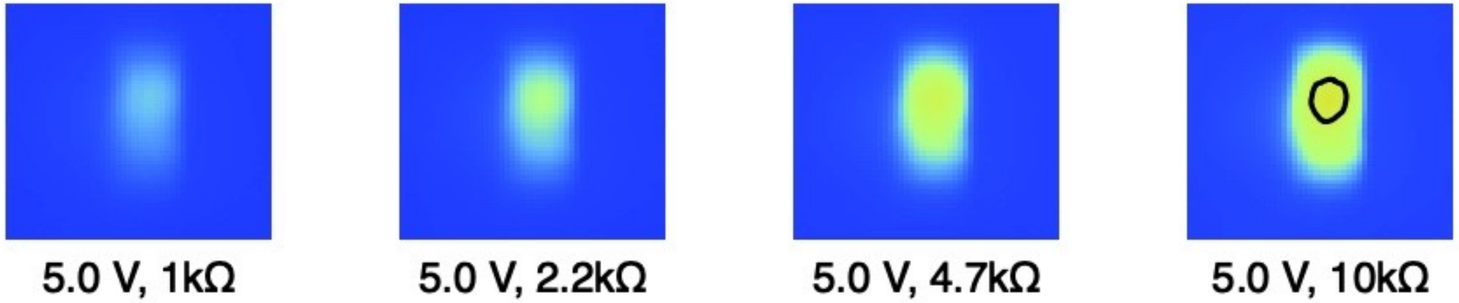

Blue LED, 405 nm laser, 3.3 V logic, 2.2 kΩ pull-up
2.5
1.5
0.5
-0.5
-1.5
-2.5
(mm)
-2.5
-1.5
-0.5
0.5
1.5
2.5
(mm)
3
2.5
2
1.5
1
0.5
0
V_{IH} = 2.0 V

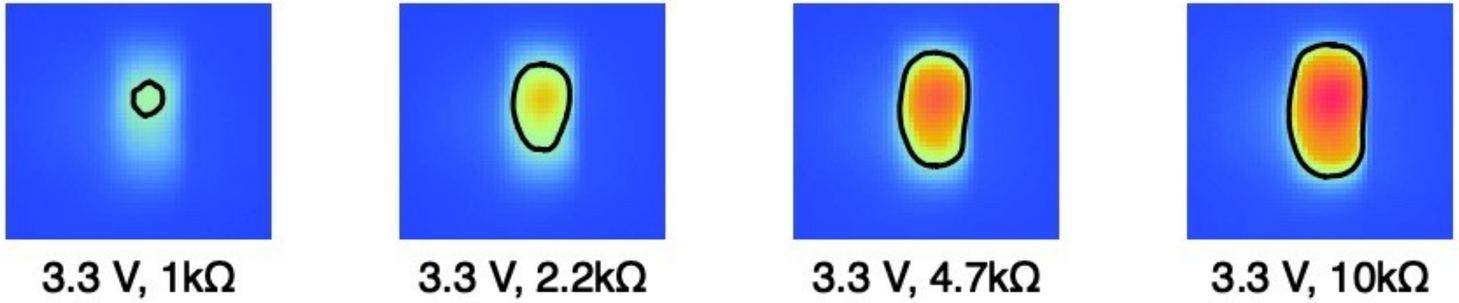
You can’t hit a target that isn’t there.

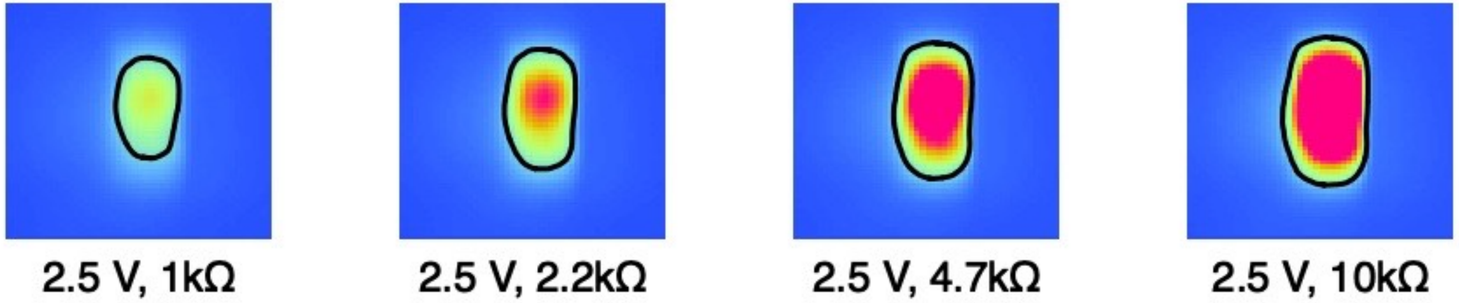


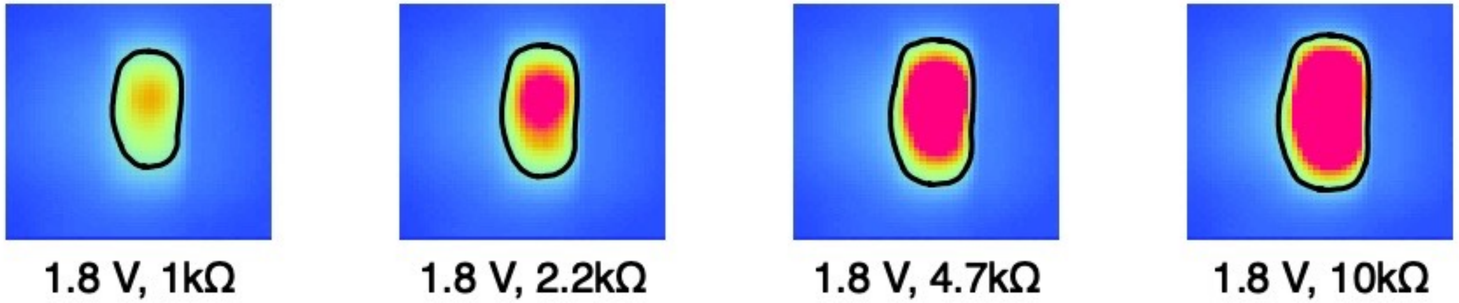


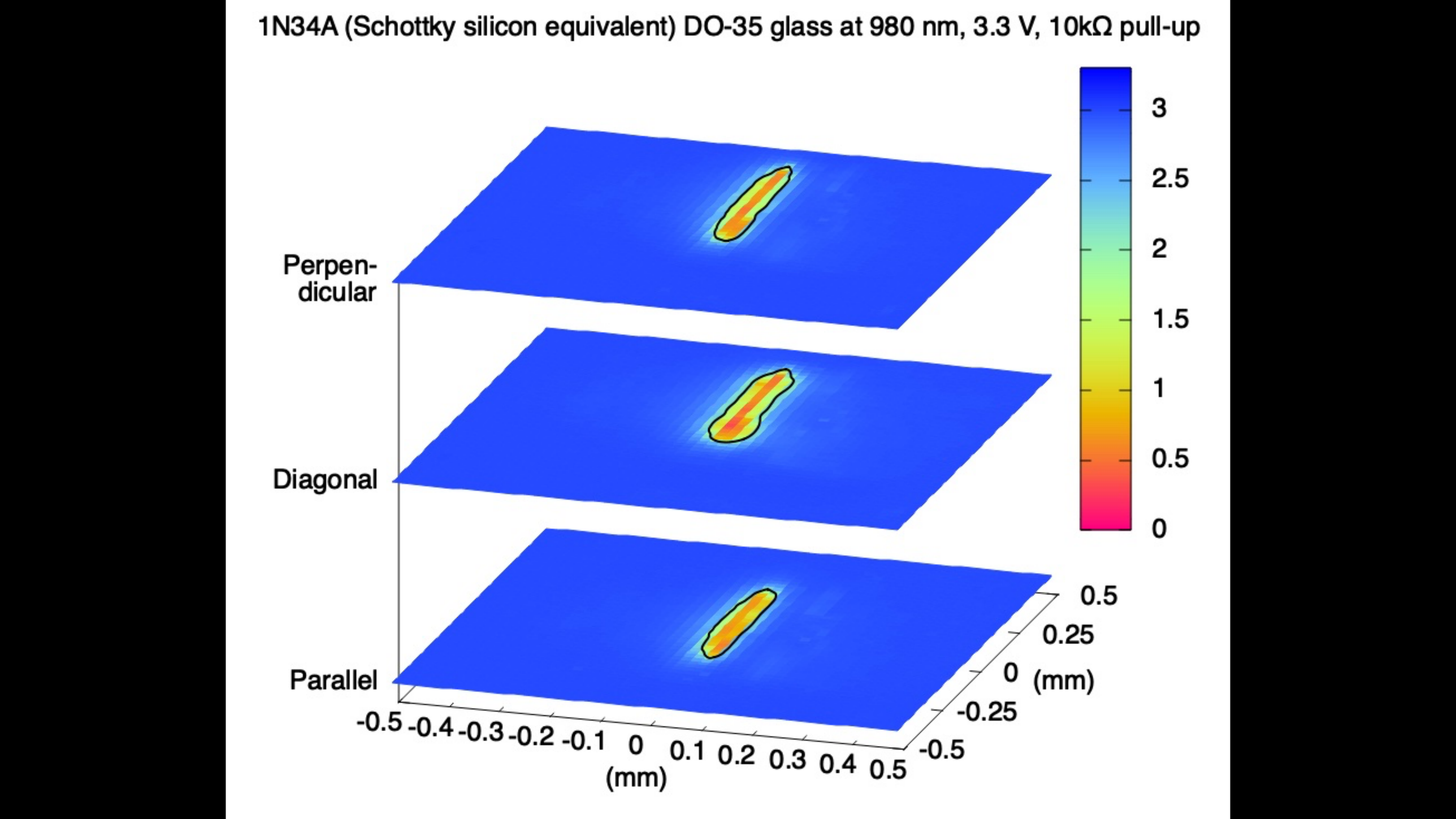
1N34A (Schottky silicon equivalent) DO-35 glass at 808 nm, axis: diagonal










1N34A (Schottky silicon equivalent) DO-35 glass at 980 nm, 3.3 V, 10kΩ pull-up
Perpen-
dicular
Diagonal
Parallel
3
2.5
2
1.5
1
0.5
0
-0.5 -0.4 -0.3 -0.2 -0.1 0 0.1 0.2 0.3 0.4 0.5
(mm)
0.5
0.25
0
-0.25
-0.5
(mm)

Q&A