Hardware Hacking Party Tricks

Techniques for Exploring, Manipulating, and Exploiting Embedded Systems 🥳

Hardware Hacking Process

Information Gathering

Product Teardown

Buses & Interfaces

Memory & Firmware

Fault Injection & Side Channels

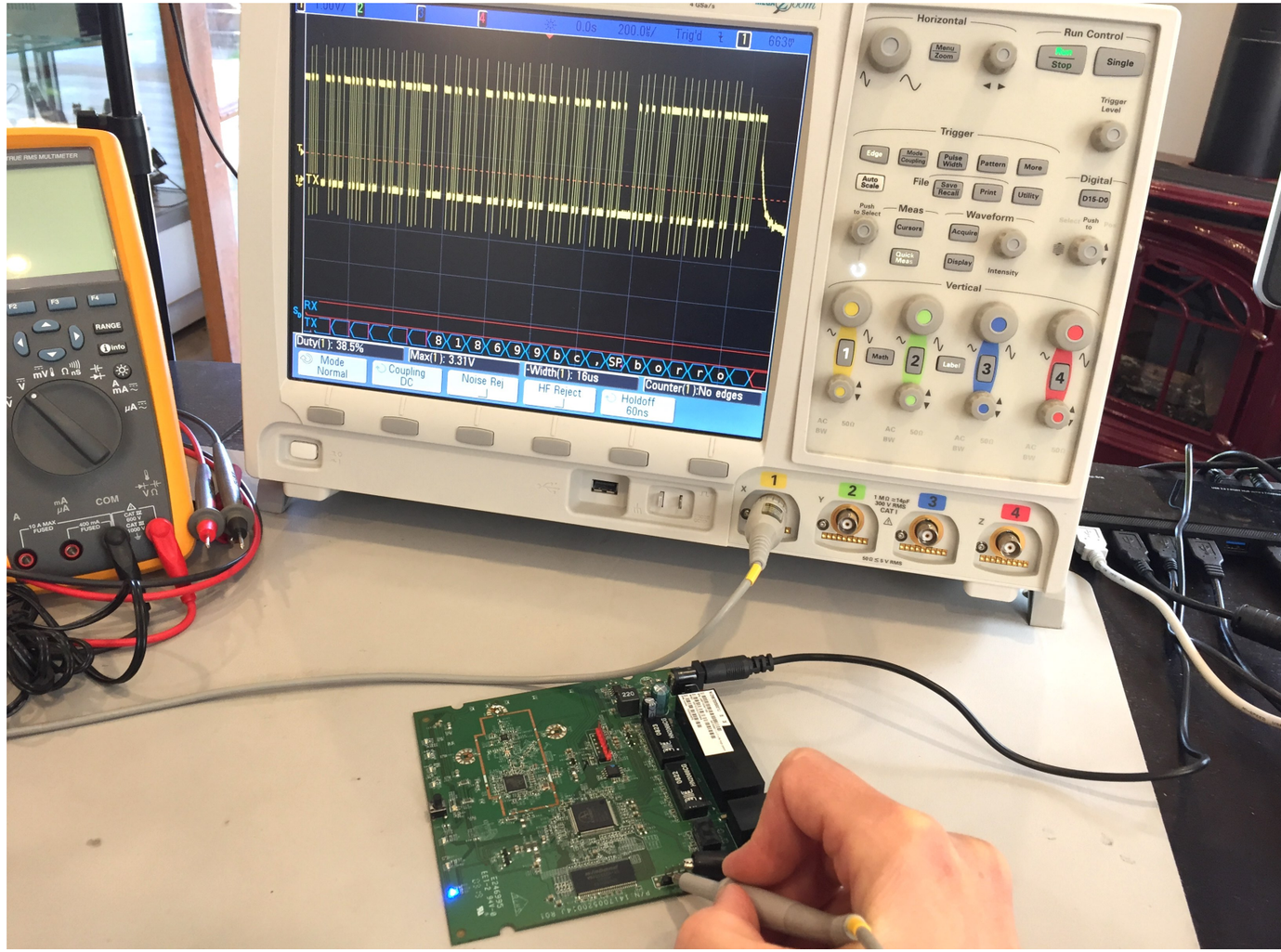
Party Plan

Visualizing Signals
UART
Memory
JTAG
Glitching
EMFI

Visualizing Signals

Identify activity within a system

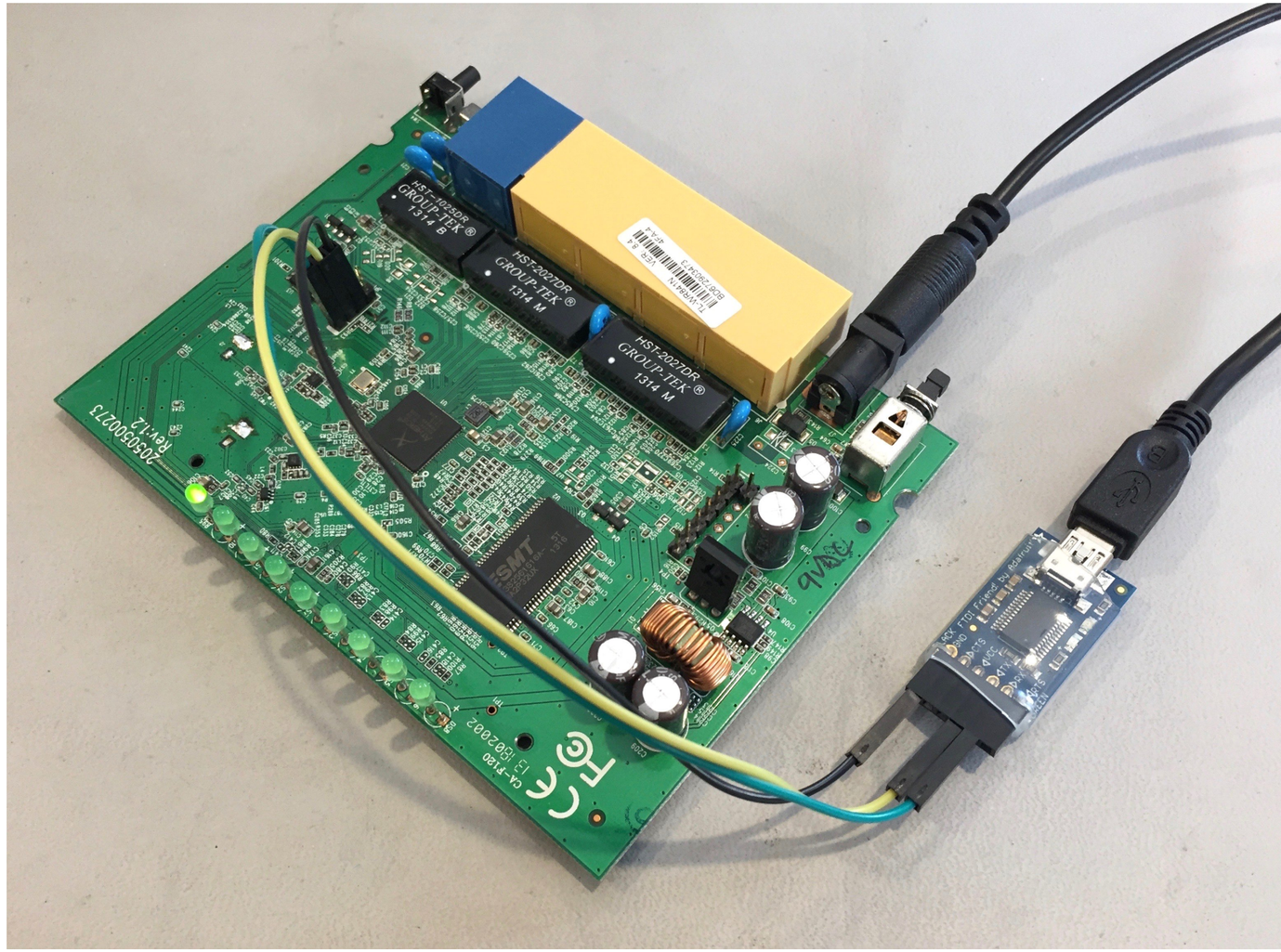
Oscilloscope + Linksys WRT120N



UART

Serial communication to/from target

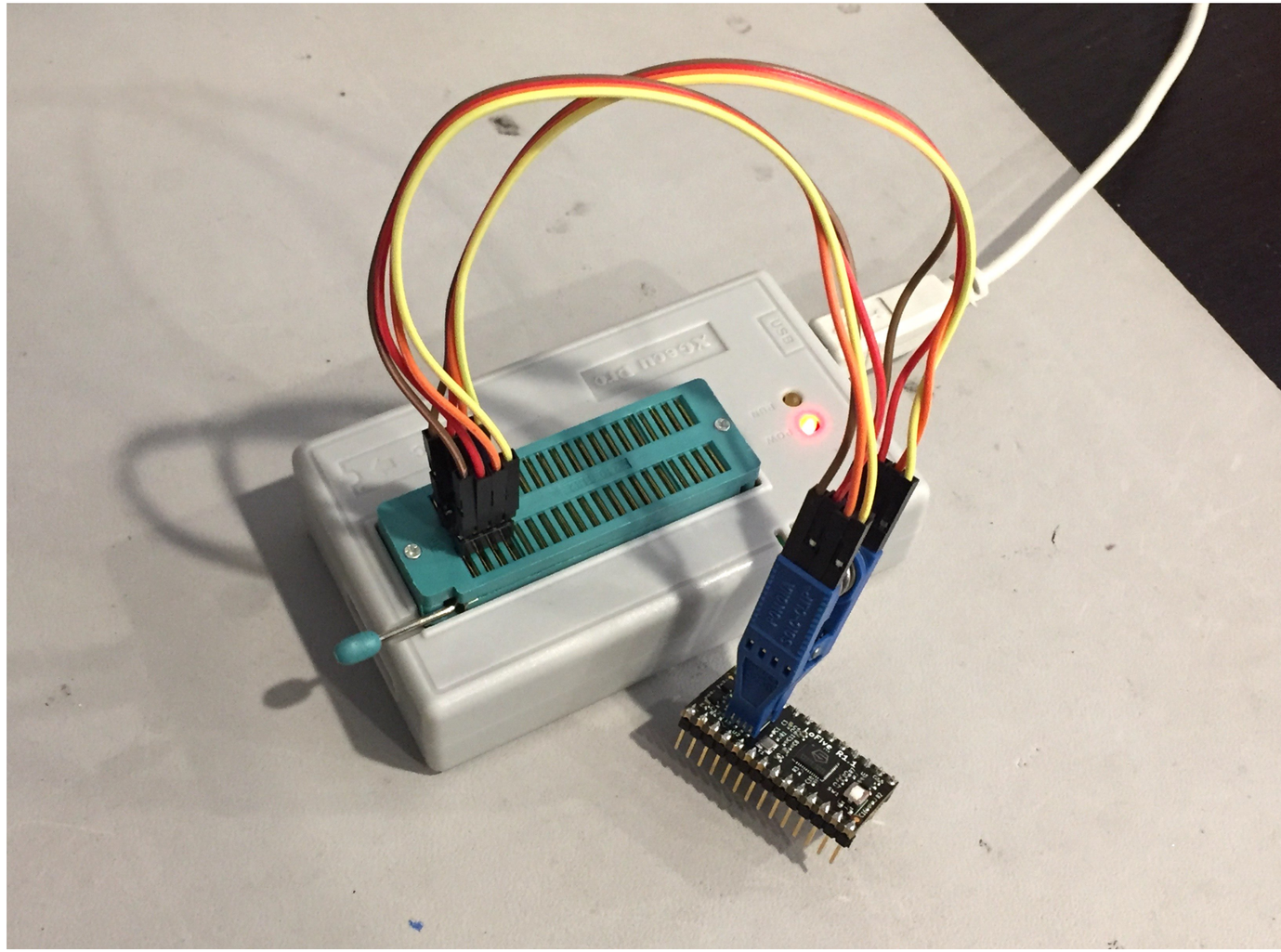
FTDI Friend + TP-Link TL-WR841N



Memory

Extract data contents

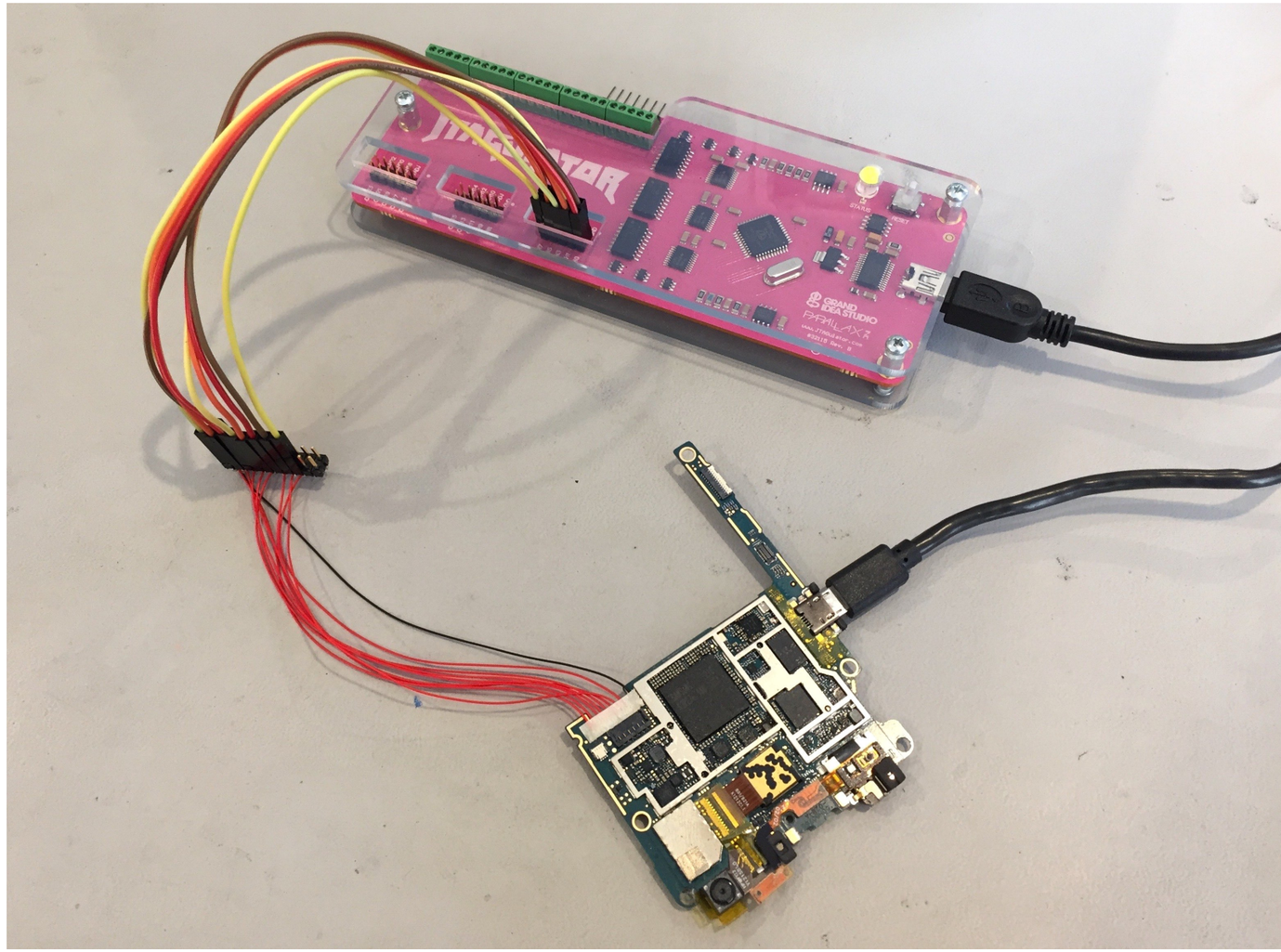
XGecu TL866II Plus + IS25LP128



JTAG

Industry-standard test/debug interface
(aka "the root shell of hardware")

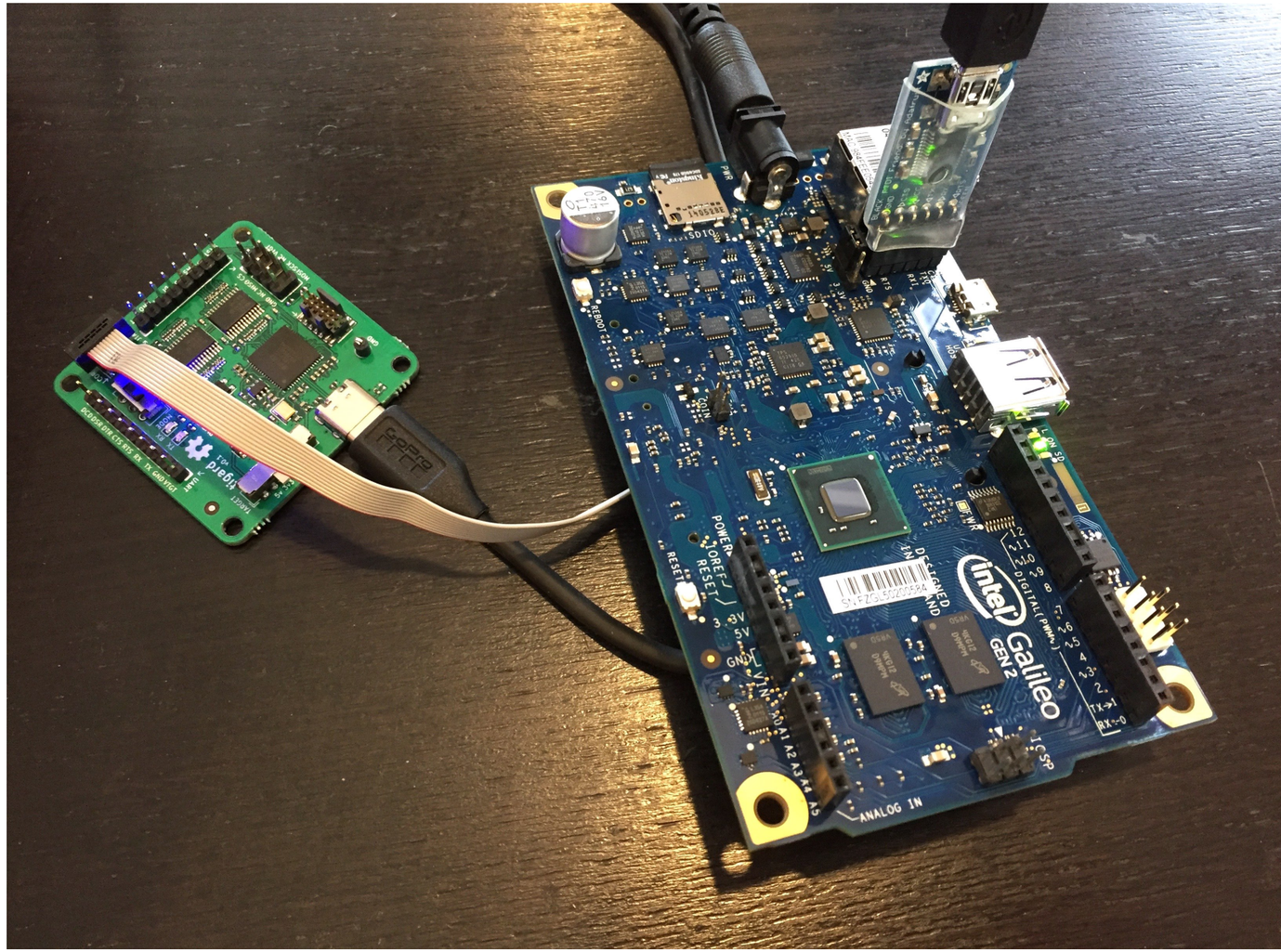
JTAGulator + HTC One X



JTAG

Industry-standard test/debug interface
(aka "the root shell of hardware")

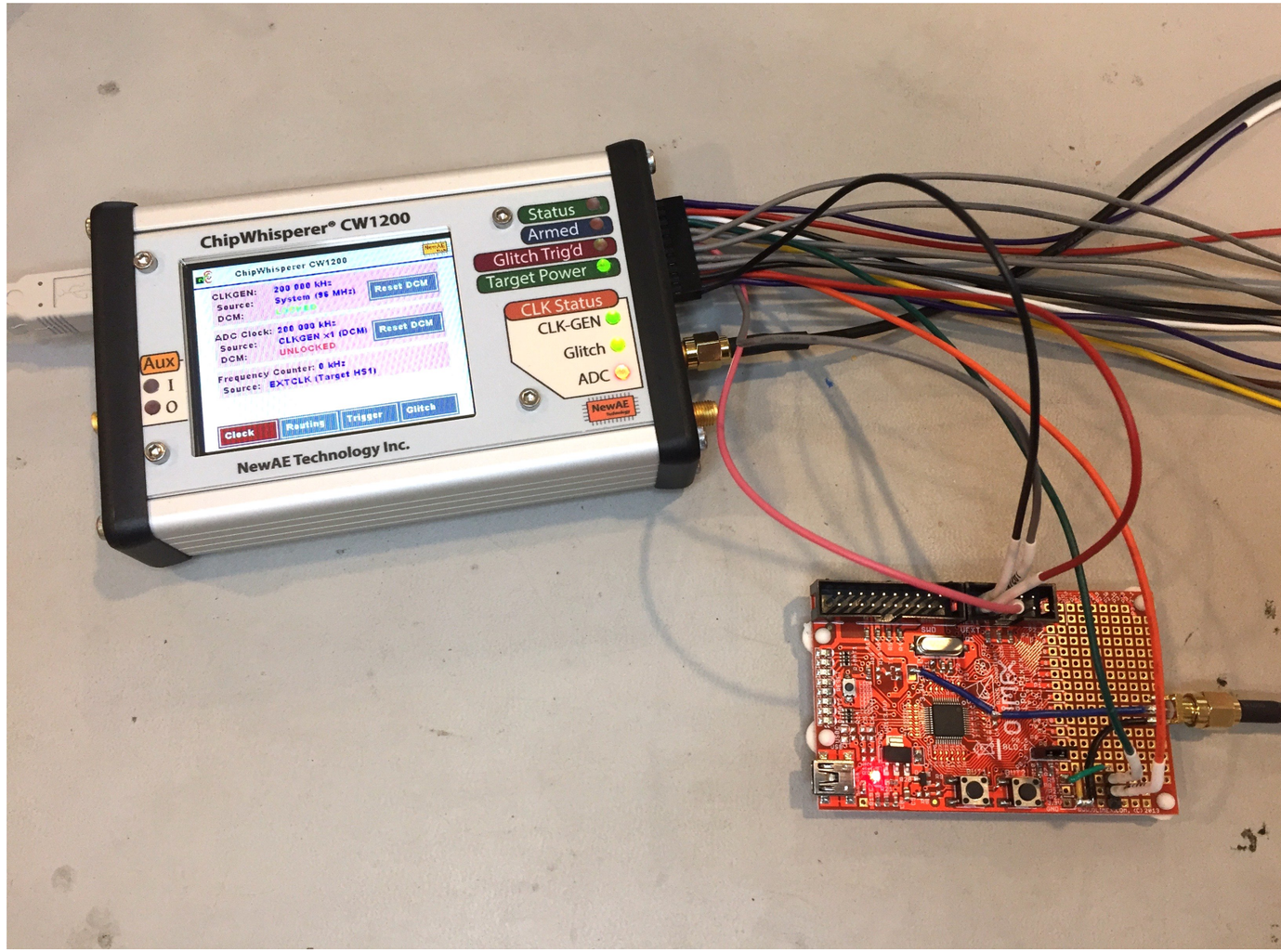
Tigard + Intel Galileo Gen. 2



Glitching

Operate system outside of specification to achieve misbehavior

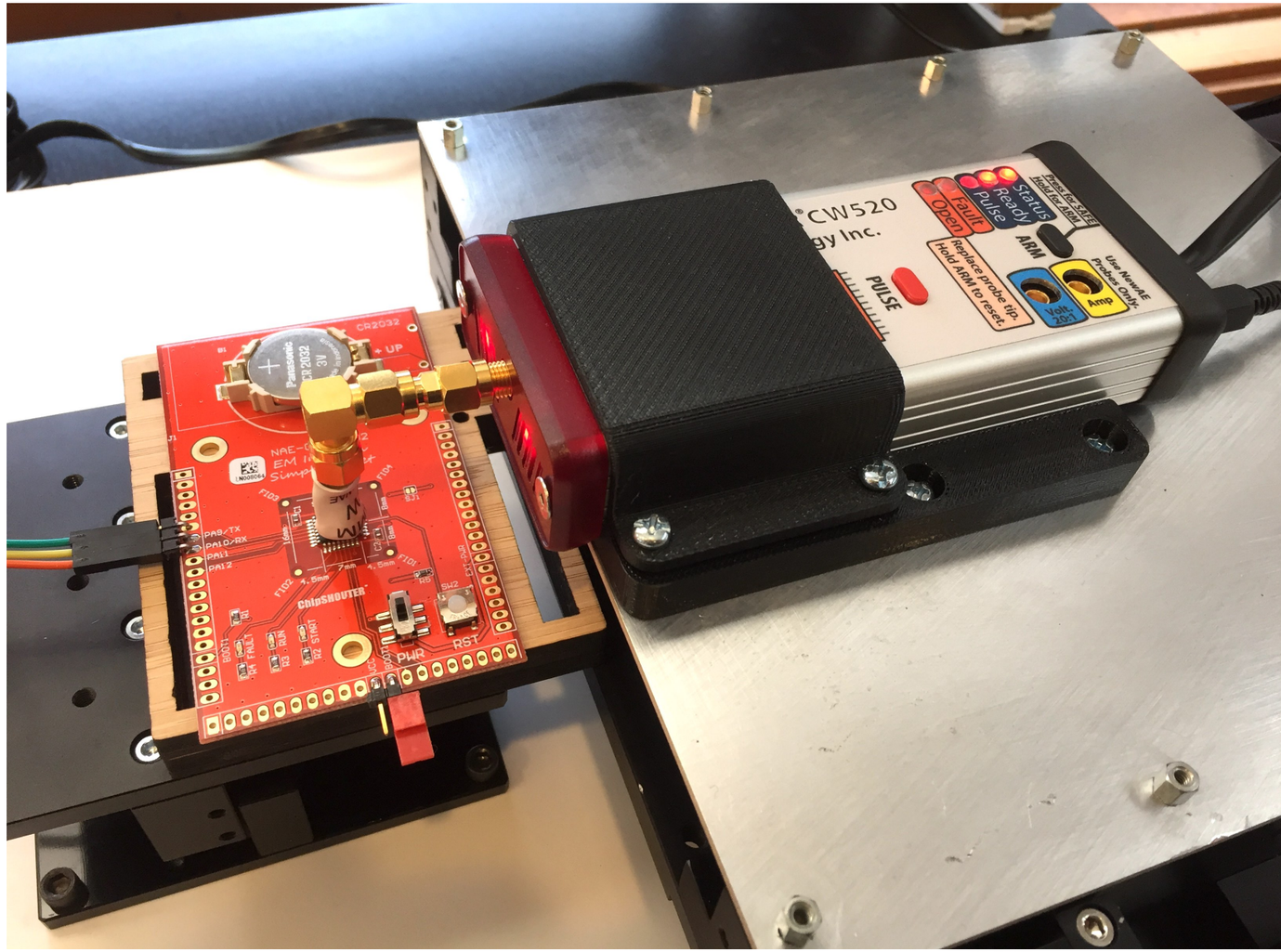
ChipWhisperer + NXP LPC1114



EMFI

Electromagnetic fields induce voltages within silicon

ChipSHOUTER + STM32F303



Thanks for watching!

grandideastudio.com

@joegrand