DISARMAMENT HACKING 2.0

TOWARD A TRUSTED, OPEN-HARDWARE COMPUTING PLATFORM FOR NUCLEAR WARHEAD VERIFICATION

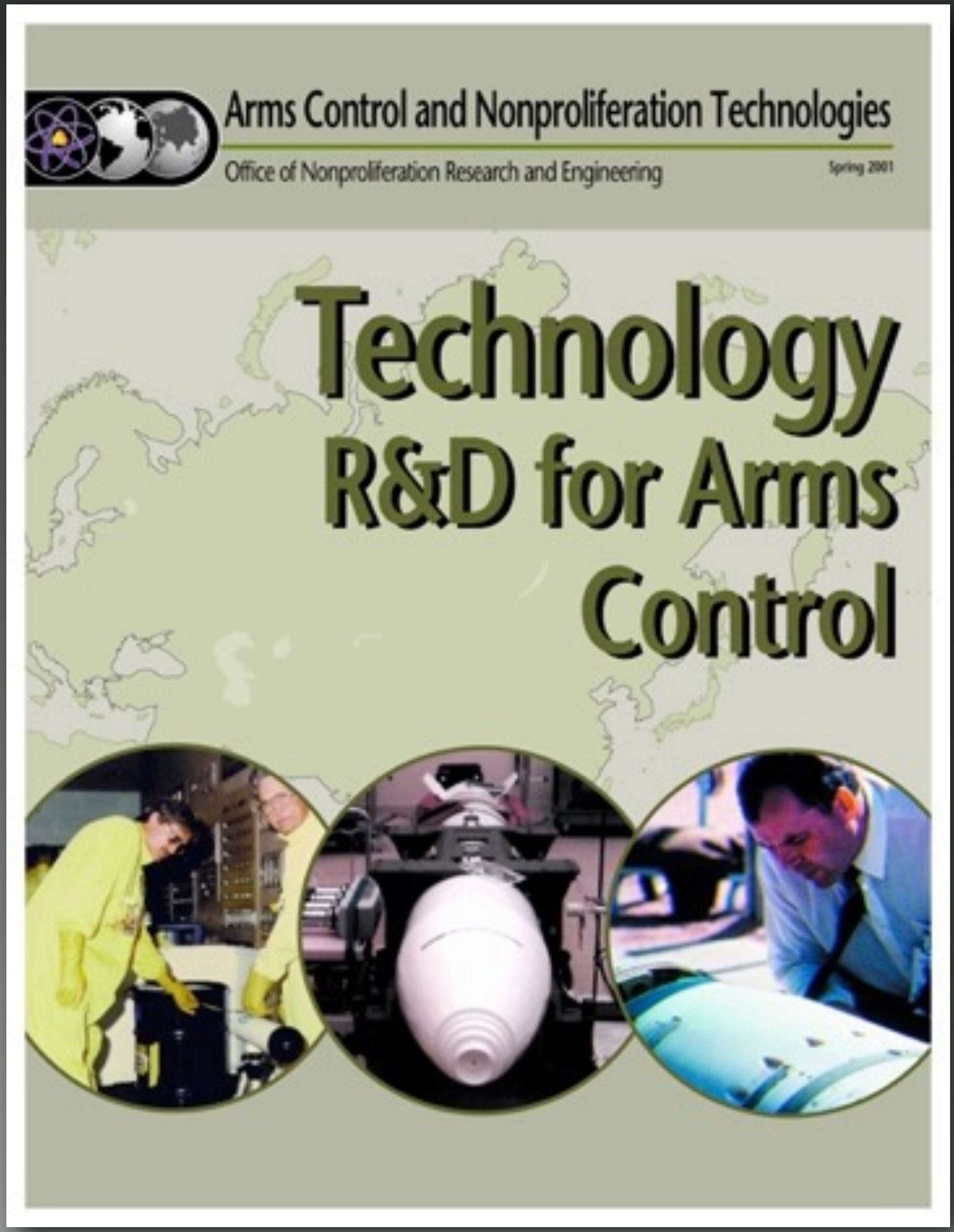
Moritz Kütt, Malte Göttsche, and Alexander Glaser
Princeton University

57th Annual INMM Meeting, Atlanta, Georgia, July 2016

Revision 2a

NUCLEAR WARHEAD VERIFICATION

KEY CONCEPTS OF (PROPOSED) SYSTEMS



edited by D. Spears, 2001

ATTRIBUTE APPROACH

Confirming selected characteristics
of an object in classified form
(for example, the presence/mass of plutonium)

TEMPLATE APPROACH

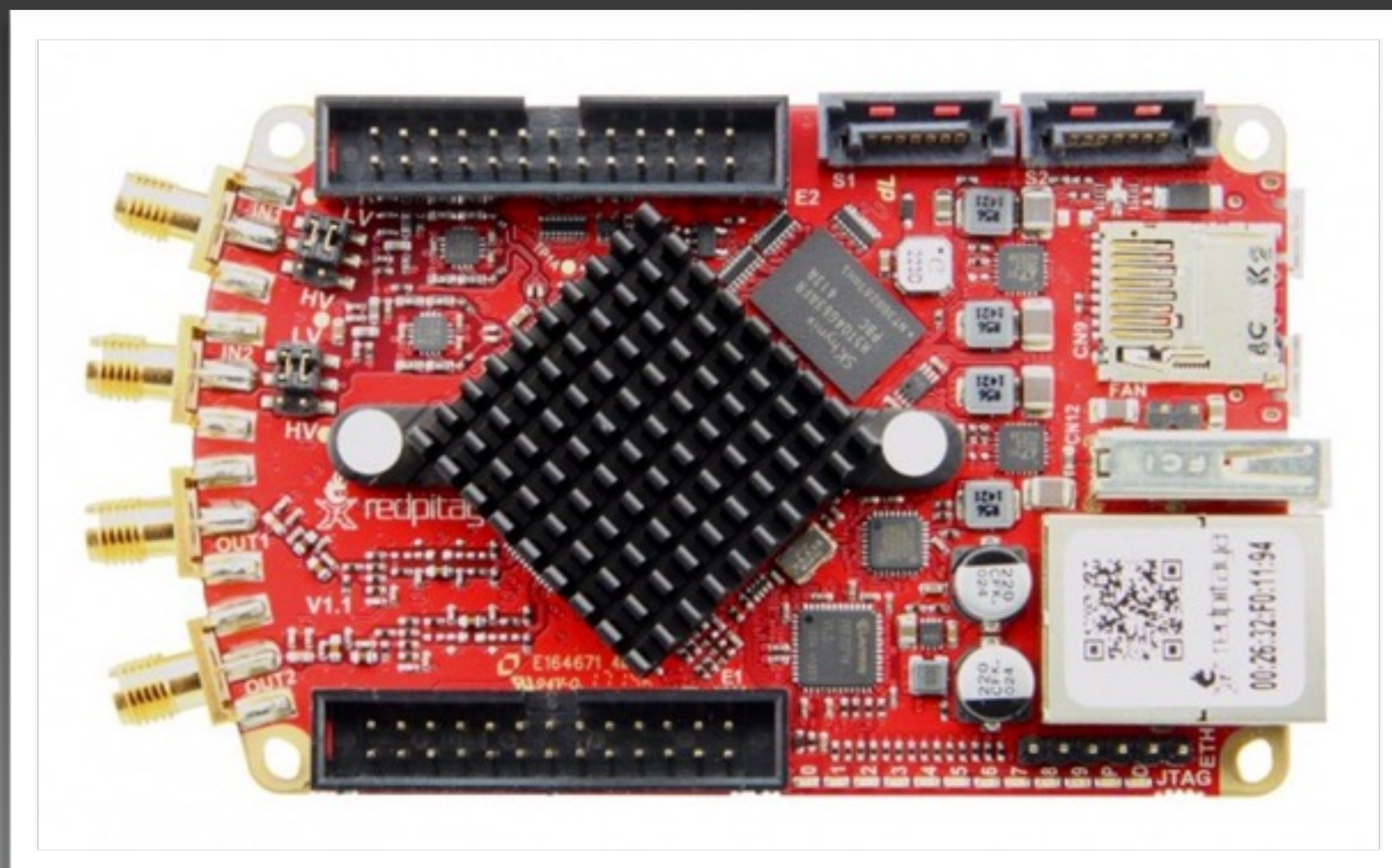
Comparing the radiation signature
from the inspected item with a reference item
("golden warhead") of the same type

INFORMATION BARRIERS

Technologies and procedures that
prevent the release of sensitive nuclear information
(generally needed for both approaches)

BUILDING AN INFORMATION BARRIER

USING A SINGLE-BOARD COMPUTING PLATFORM WITH OPEN-SOURCE SOFTWARE (AND AT MINIMAL COST)



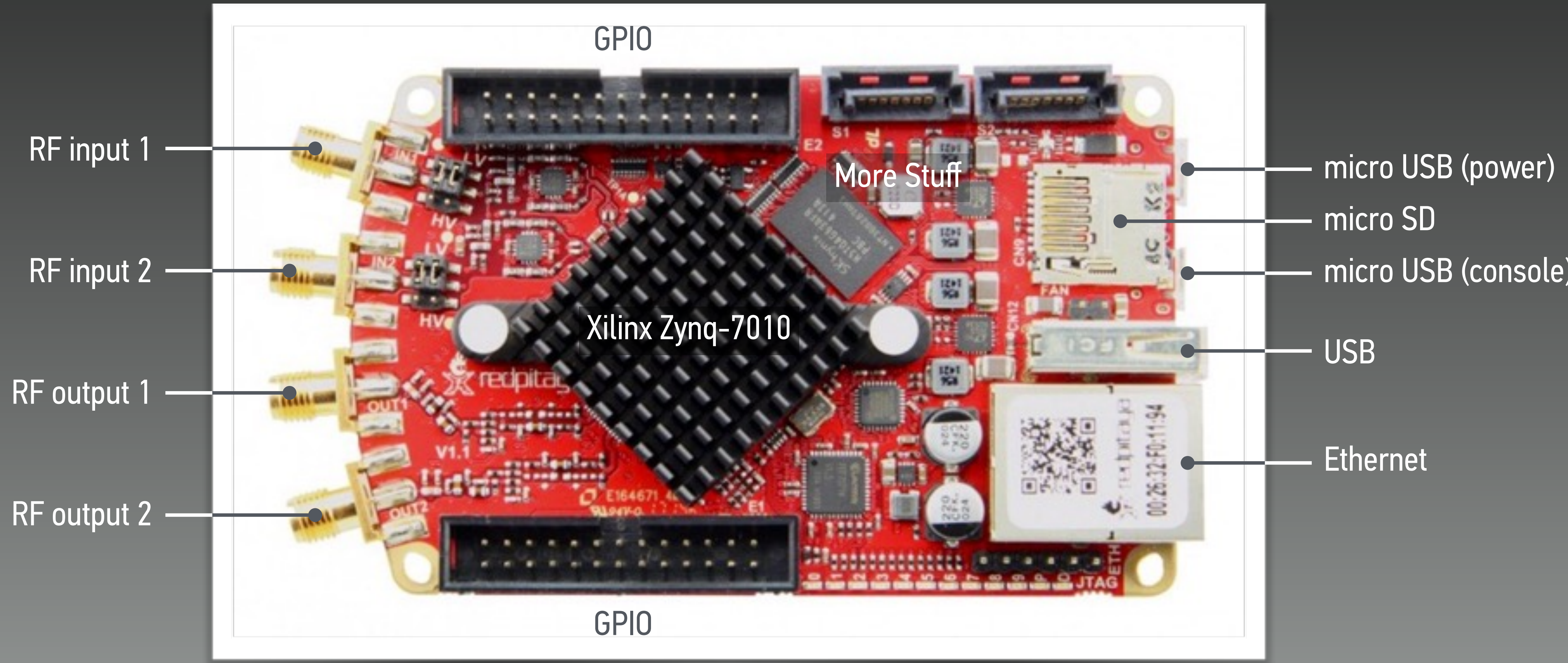
www.redpitaya.com

(RedPitaya launched as a Kickstarter campaign in 2013 raising more than $250,000 in 4 weeks)

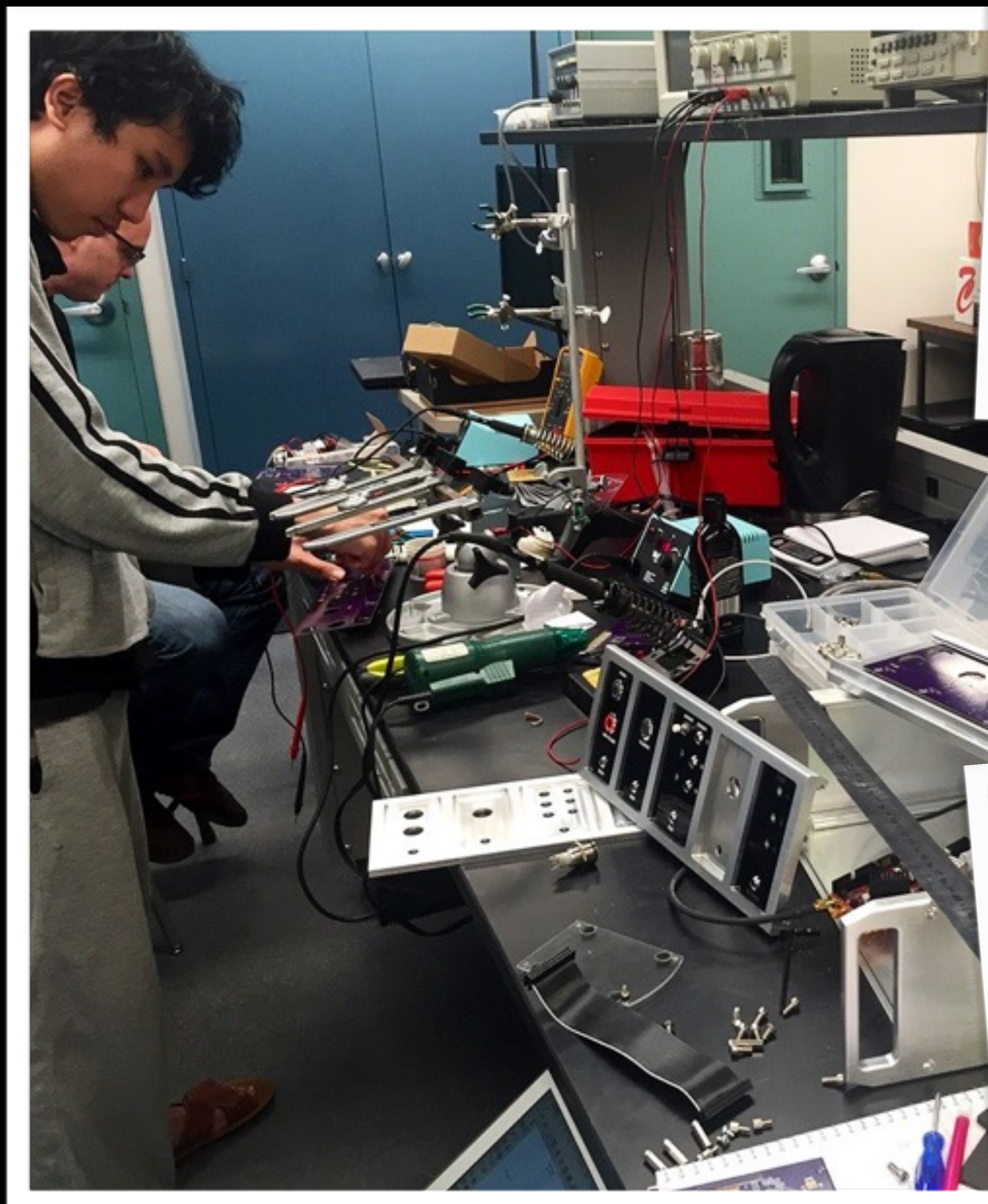
RED PITAYA

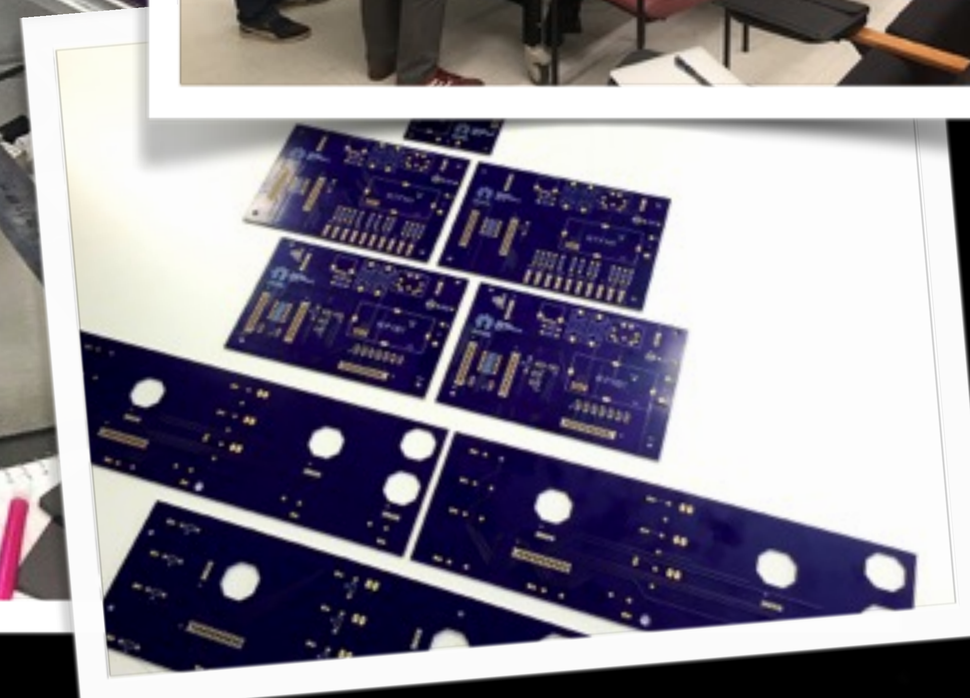
XILINX ZYNQ-7010 SYSTEM-ON-CHIP

(ARM CORTEX-A9 + ARTIX-7 FPGA)

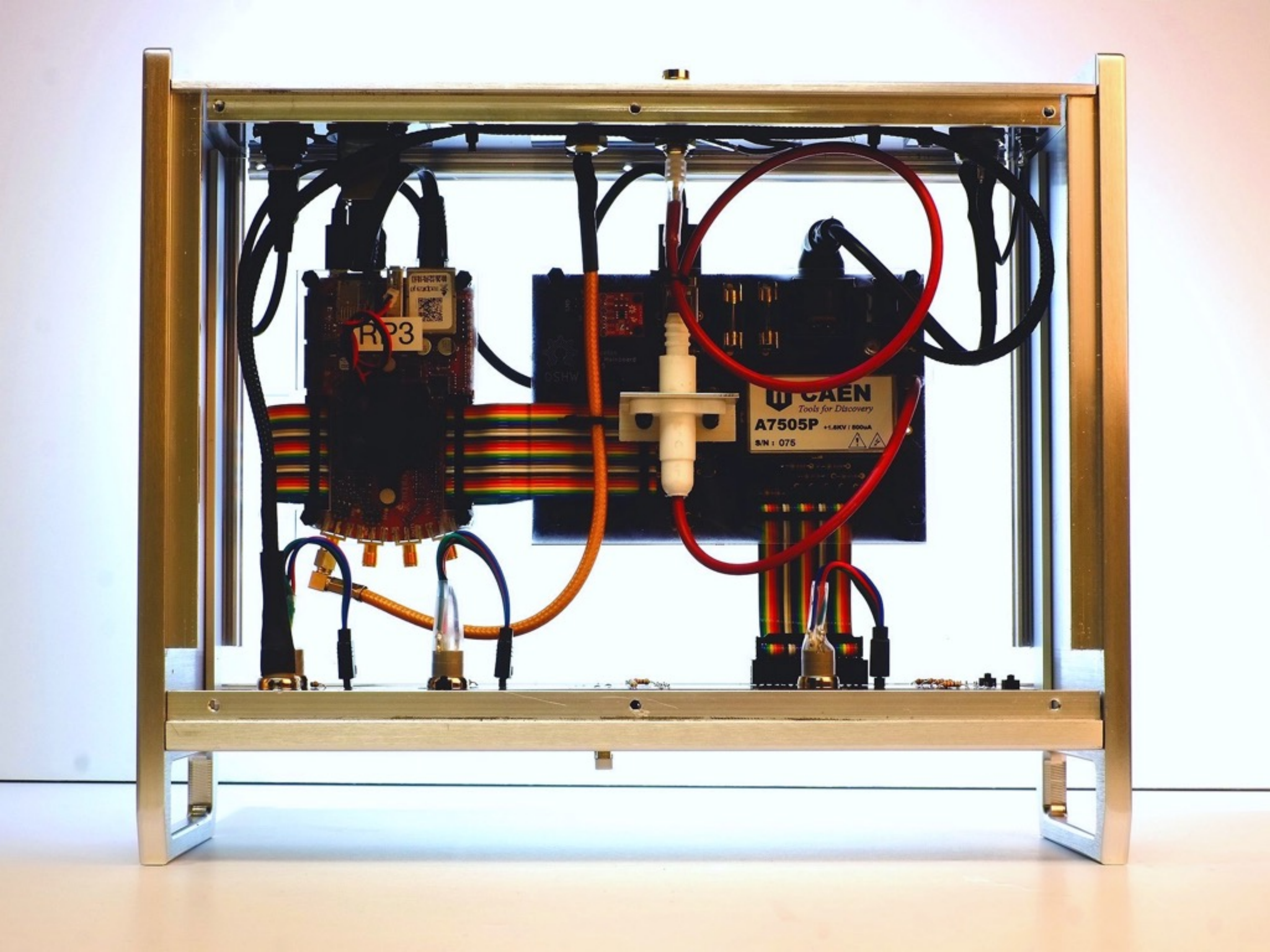


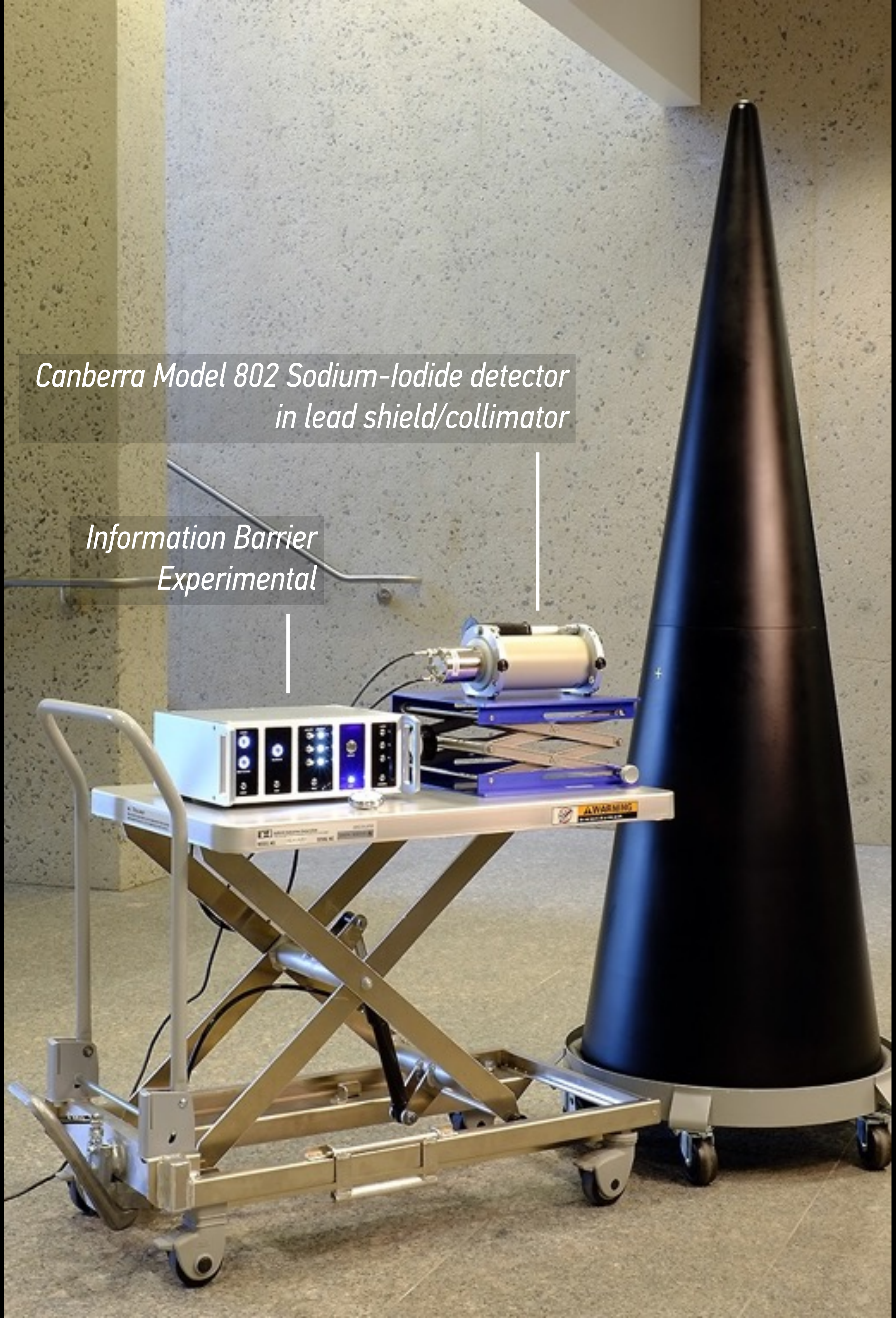
www.redpitaya.com



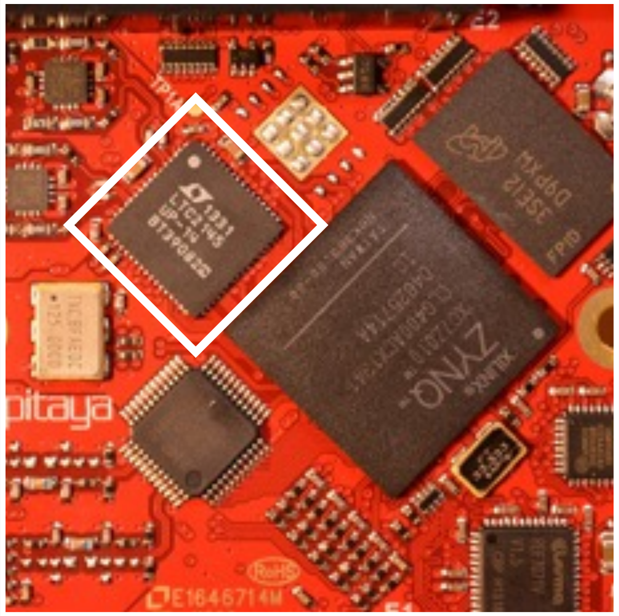
Moments from MAE 354/574, Spring 2016


RP3
CAEN
Tools for Discovery
A7505P
S/N : 075
OSHW


Canberra Model 802 Sodium-Iodide detector
in lead shield/collimator
Information Barrier
Experimental

DIGITAL DATA ACQUISITION APPROACH

DATA ACQUISITION



ANALOG-TO-DIGITAL CONVERTER (LTC2145-14)

14-bit resolution (2^{14} = 16384 states)

125 MHz sampling rate, i.e., voltage levels recorded every 8 nanoseconds

Generates about 220 MB/s of data

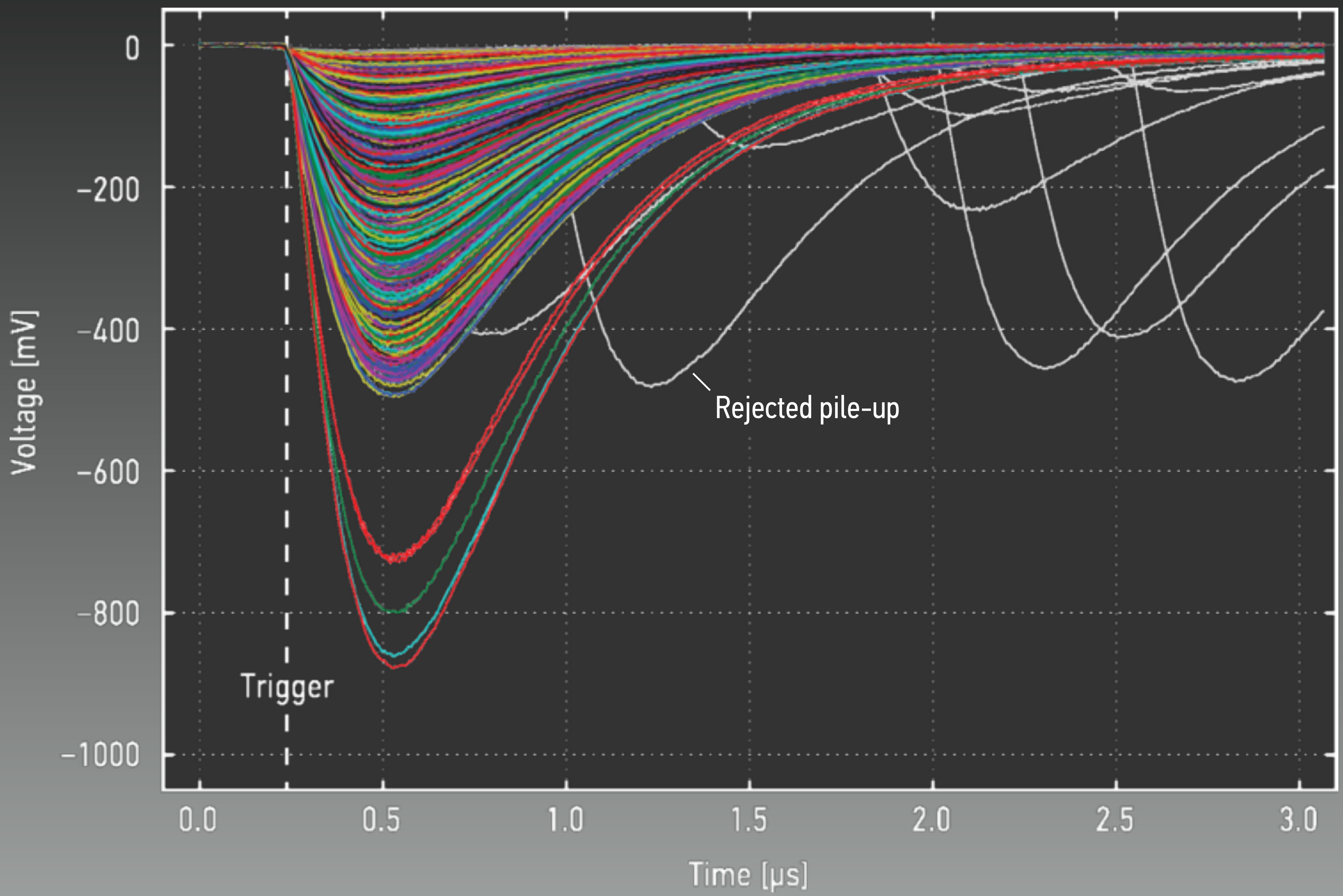
(in fact, closer to 500 MB/s as values are stored as 32-bit integers)

FIELD-PROGRAMMABLE GATE ARRAY (FPGA) AND MICROPROCESSOR

1. Circular buffer in FPGA is continuously filled with data from ADC
2. When an incoming pulse is detected, data acquisition continues for a few microseconds before data acquisition is stopped (to prevent overwrite)
3. Post-trigger data is written to memory and trigger is re-armed

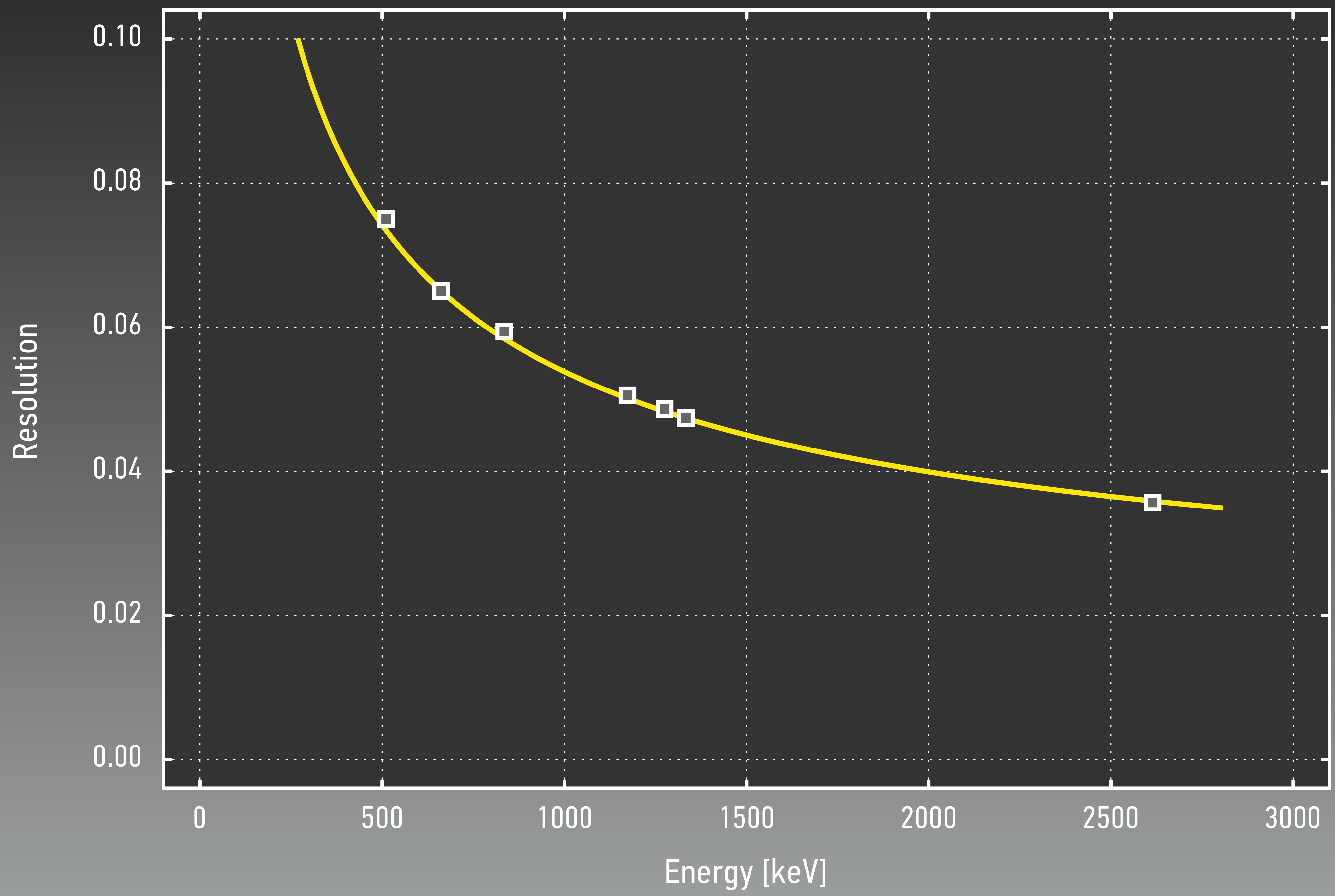
INFORMATION BARRIER EXPERIMENTAL

VOLTAGE PULSES ACQUIRED BY THE RED PITAYA



DETECTOR RESOLUTION

ΔE/E ≈ 6% AT 662 keV



MODE OF OPERATION


1
POWER
HIGH VOLTAGE
READY
CALIBRATE
BUSY
ACQUIRE
PRESENT
T1
T2
T3
BUSY
INSPECT
BUSY
MATCH
T1
T2
T3
NO MATCH
Power-up and High Voltage

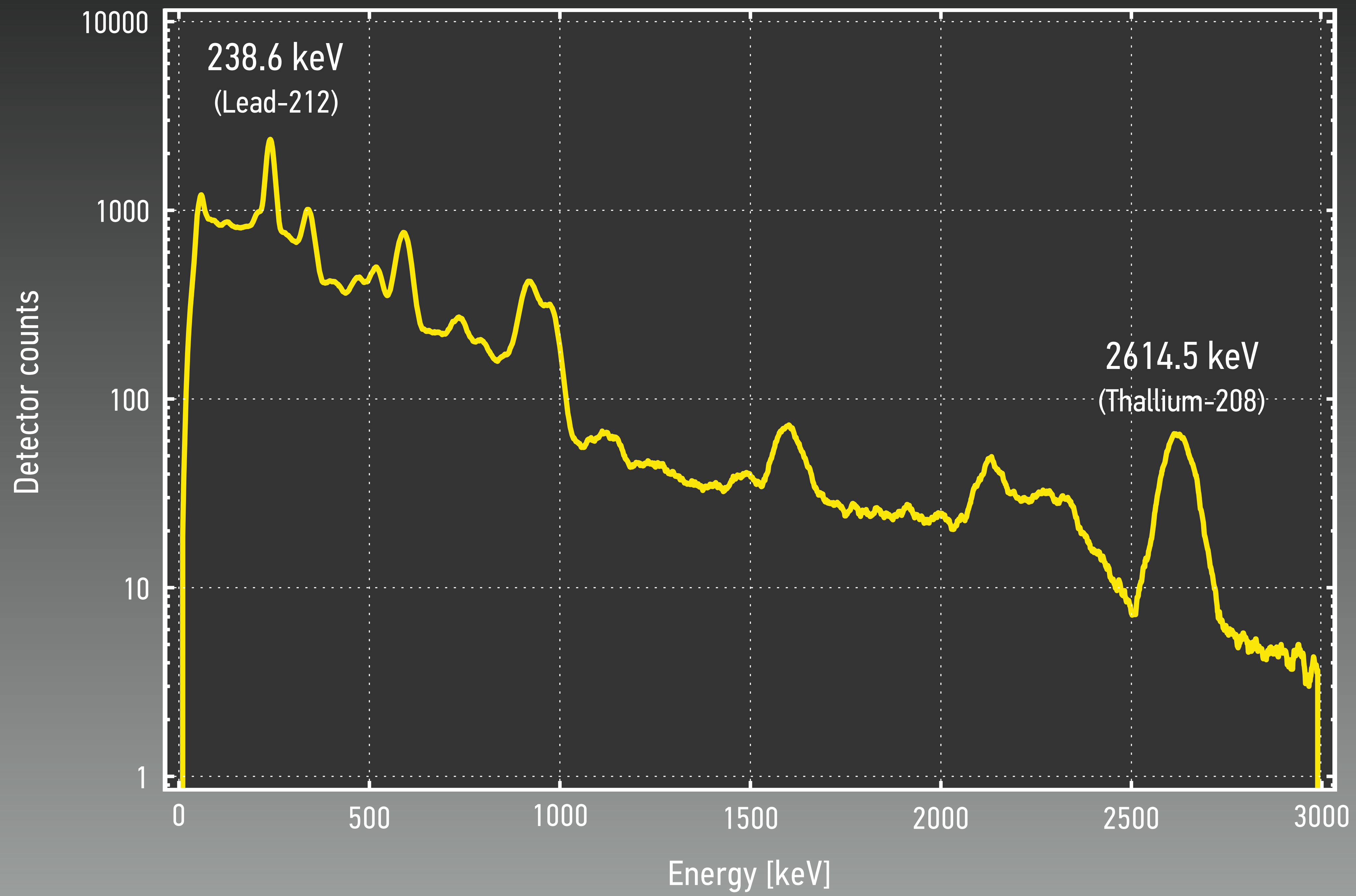
<u>Calibration</u>

Thoriated welding rods wrapped around the sodium-iodide crystal provide a robust signature for calibration; spectrum includes, in particular, 2.6 MeV line from thallium-208 decay

First used in Sandia's Trusted Radiation Identification System (TRIS)

SELF-CALIBRATION SPECTRUM

THORIATED WELDING RODS ONLY; 600 SECONDS



Template Acquisition

IBX can acquire and store up to three templates

Upon startup, the device checks for previously recorded templates and indicates their presence;
this feature is convenient during development and testing, but may be impractical in a true inspection setting


4
POWER
HIGH VOLTAGE
READY
CALIBRATE
BUSY
ACQUIRE
PRESENT
T1
T2
T3
BUSY
INSPECT
BUSY
MATCH
T1
T2
T3
NO MATCH
Inspection

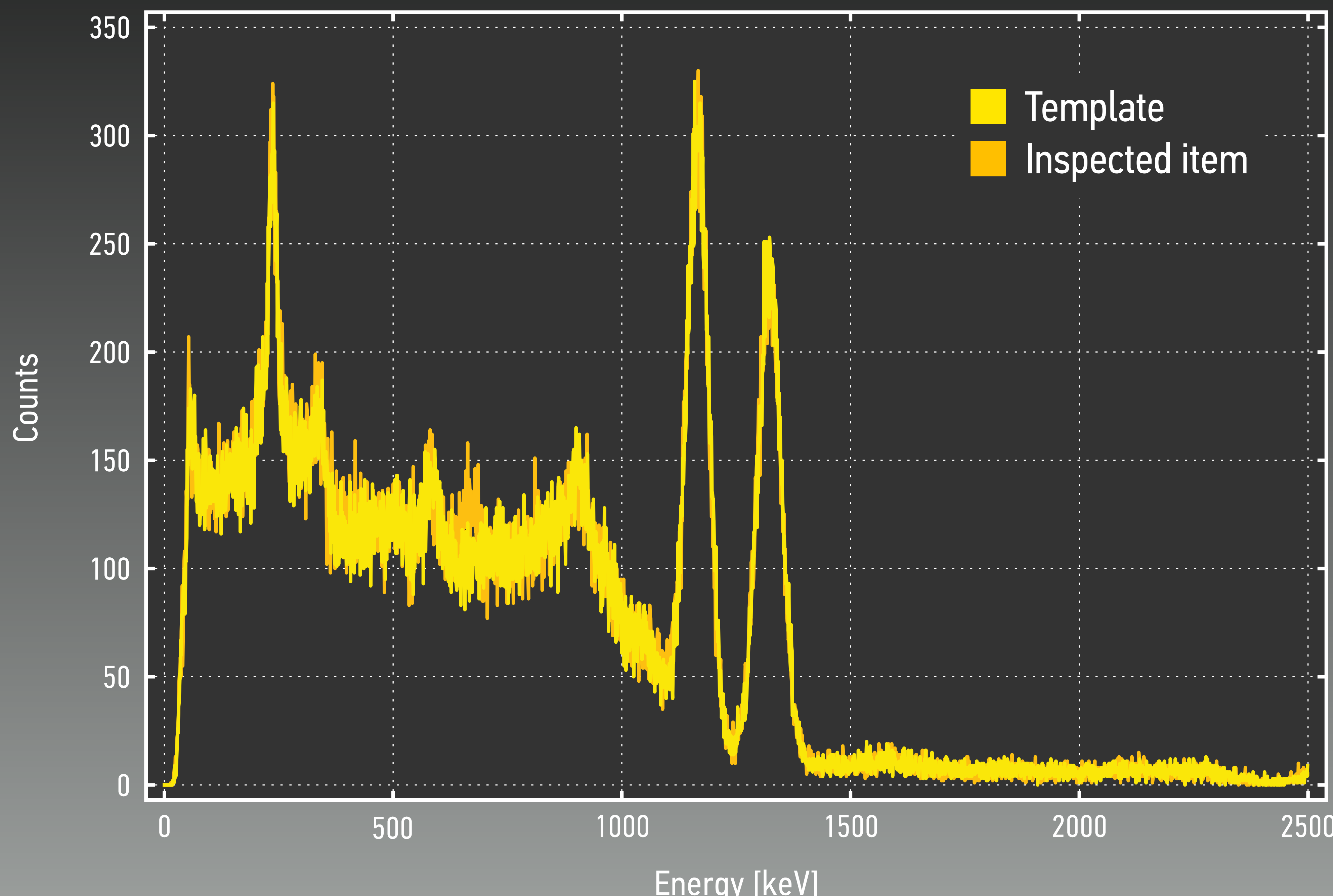
Match / Mismatch

LEDs indicate which template shows closest similarity with the inspected item

If the inspected item is substantially different from all templates, a “no match” situation is signaled

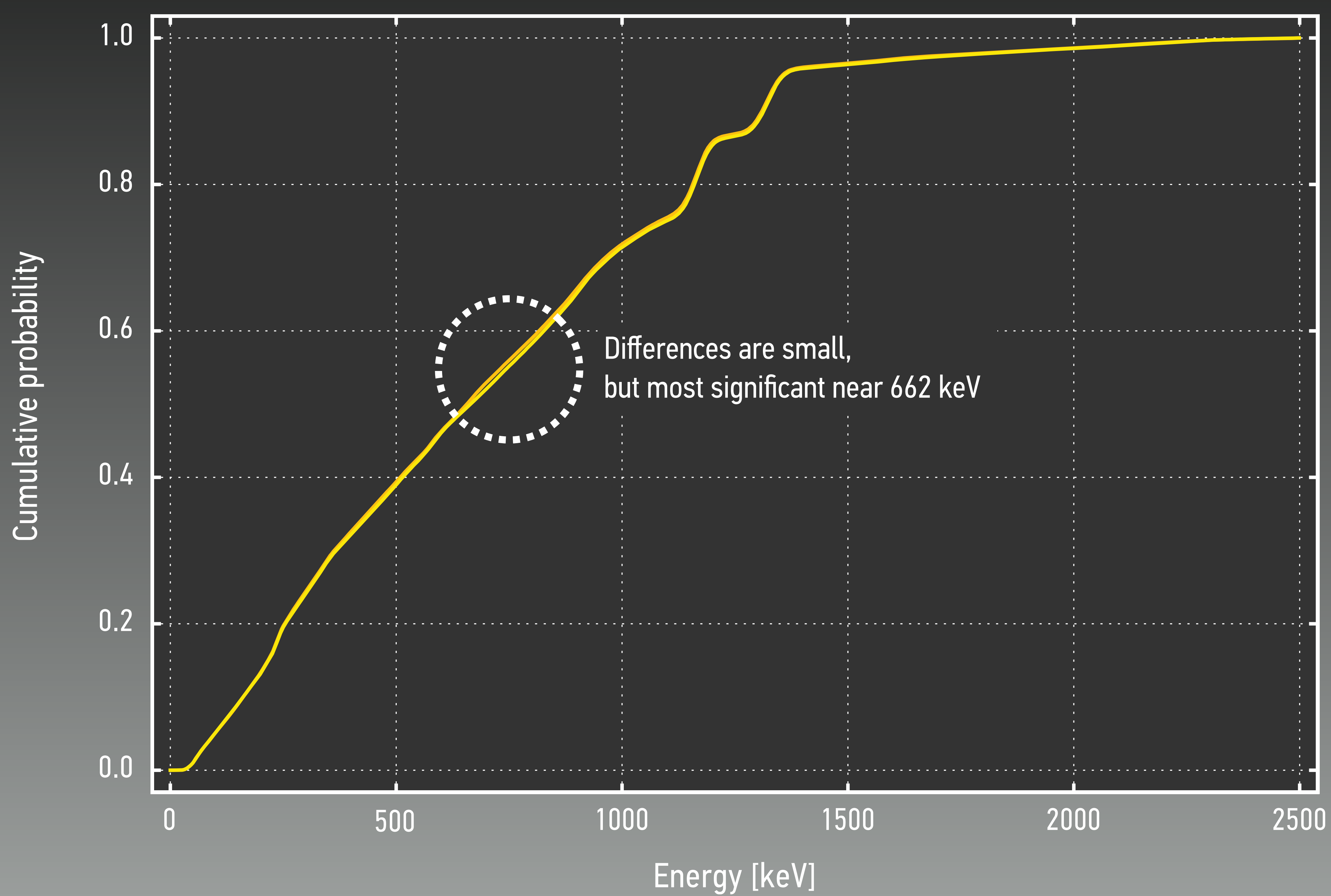
COMPARING RADIATION SPECTRA

(IBX WITH SODIUM-IODIDE DETECTOR, 60 SECONDS, ~175,000 counts)



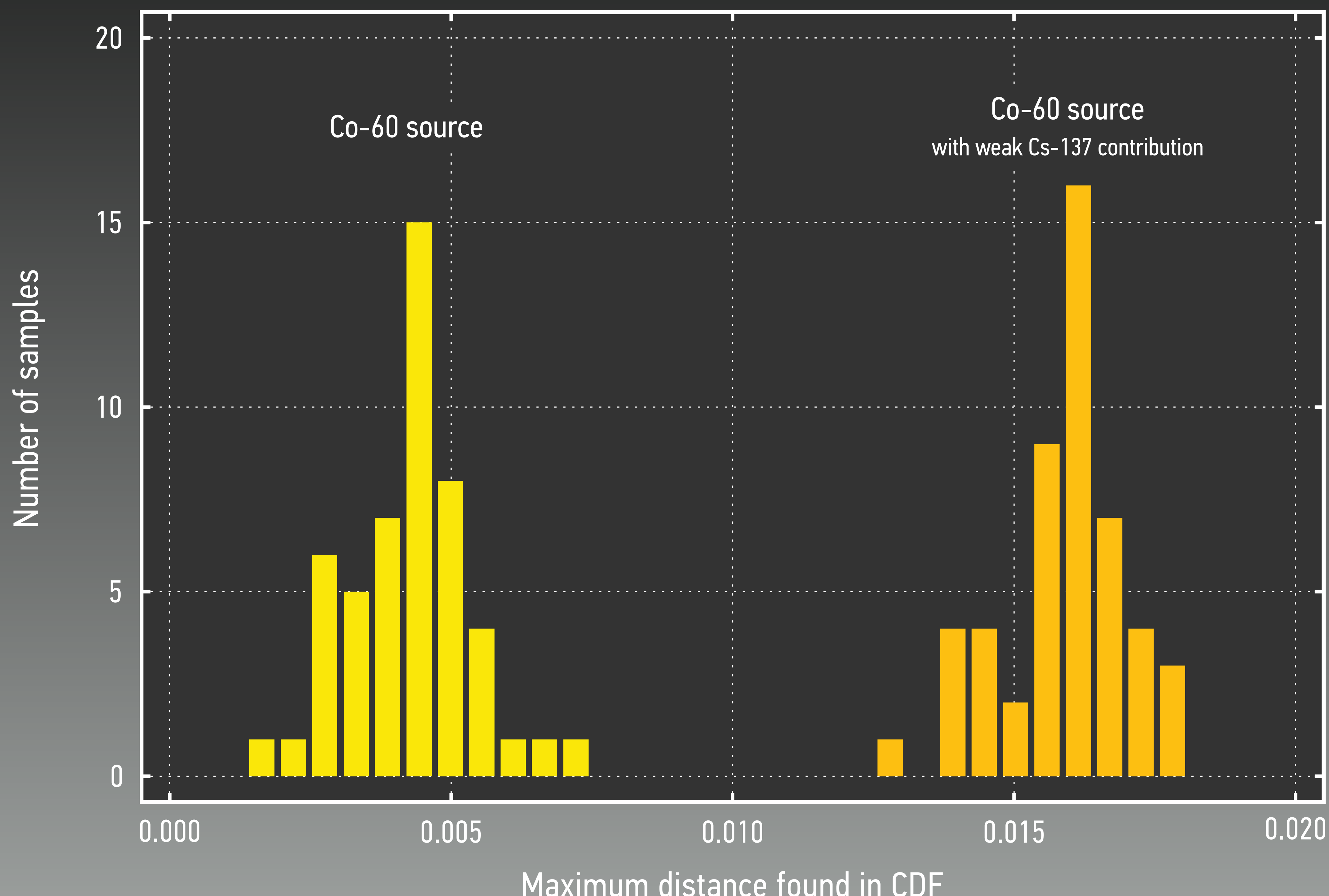
COMPARING RADIATION SPECTRA

(IBX WITH SODIUM-IODIDE DETECTOR, 60 SECONDS, ~175,000 counts)



COMPARING RADIATION SPECTRA

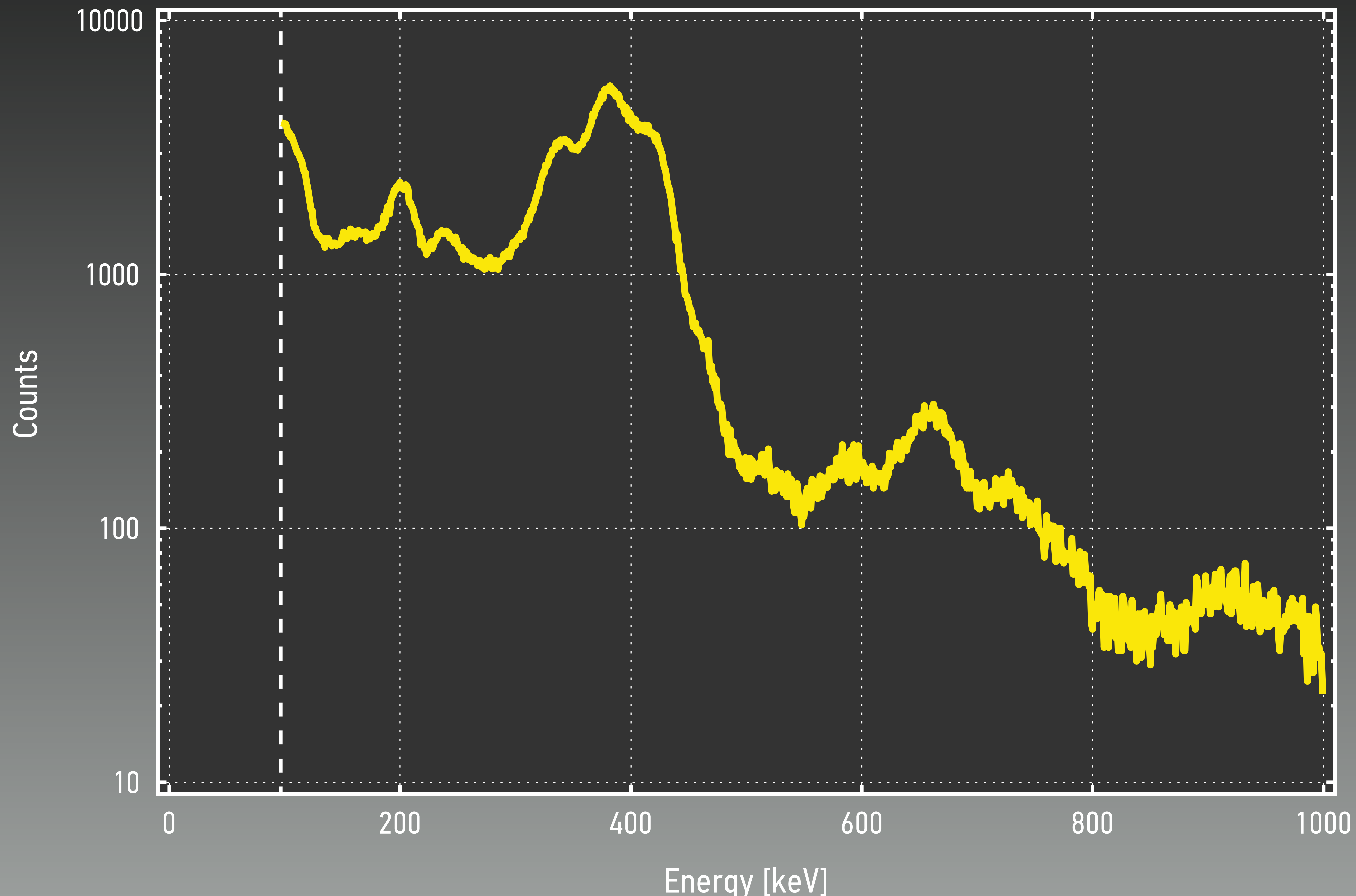
(IBX WITH SODIUM-IODIDE DETECTOR, 60 SECONDS, ~175,000 counts)



WHAT'S NEXT?

EVALUATING REAL DATA

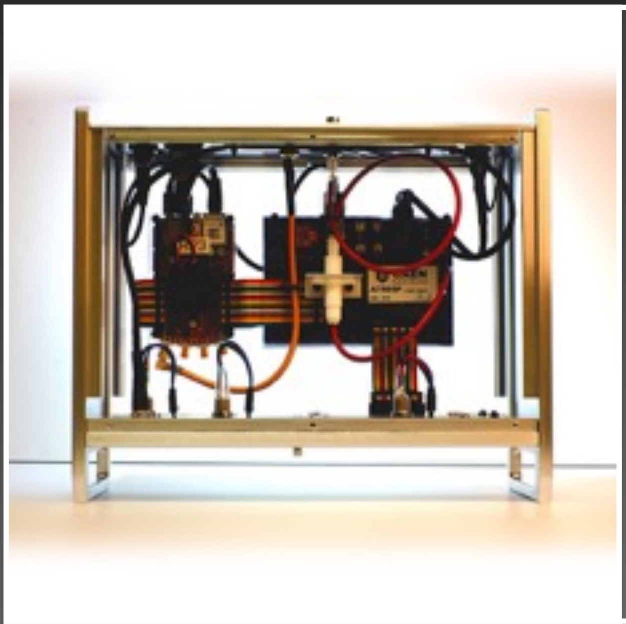
4.5 kg OF WEAPON-GRADE PLUTONIUM, 15-MINUTE MEASUREMENT TIME
DEVICE ASSEMBLY FACILITY, NEVADA, JULY 2016



CAN WE MAKE IT LEAK INFORMATION?

VERIFICATION CHALLENGES ATTACKING THE IBX ON BOTH THE SOFTWARE AND THE HARDWARE LEVEL

SUMMARY AND WAY FORWARD



TOWARD OPEN-HARDWARE COMPUTING FOR NUCLEAR ARMS CONTROL

- Simple and transparent design
- Low cost (~ $700)
- BUT: Needs transition to fully open hardware

IBX (OR A SIMILAR DEVICE) AS A PROTOYPING PLATFORM

- Exploring and benchmarking advanced algorithms
- Implementing all functionalities/computations on FPGA (avoiding CPU)
- Enabling verification challenges for broader hacker community

ACKNOWLEDGEMENTS

Mary Helen deGolian
Bennett McIntosh
Tamara Patton
Himawan Winarto
Al Gaillard
Sébastien Philippe
Mark Walker
Matjaz Vencelj
Peter Ferjančič

and

Consortium for Verification Technology
U.S. Department of Energy

PRINCETON UNIVERSITY | NUCLEAR FUTURES | LAB