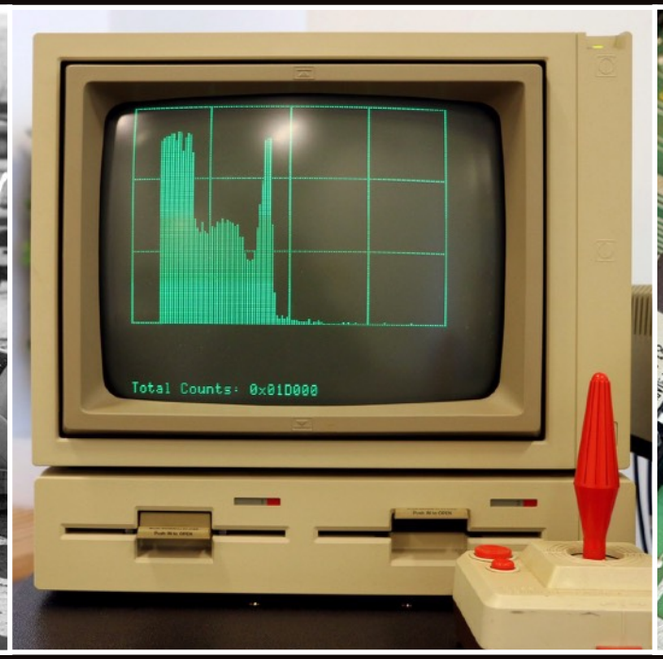
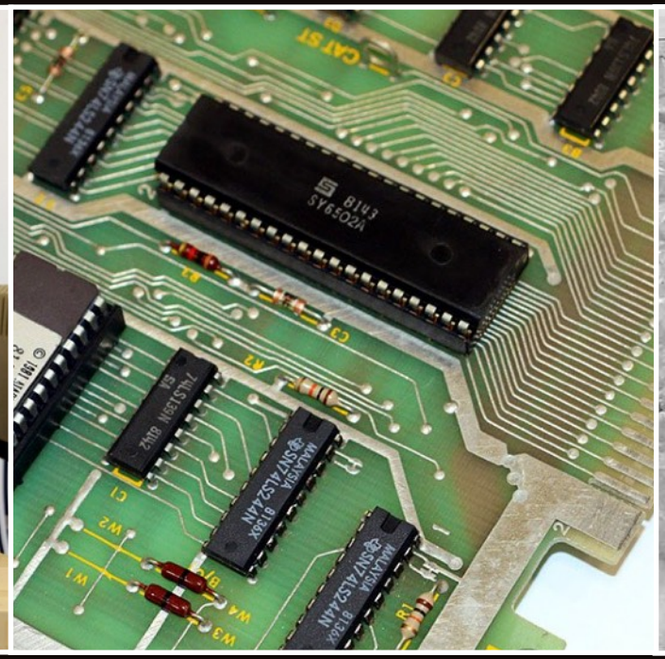




VINTAGE VERIFICATION

FOR TRUSTED RADIATION MEASUREMENTS AND A WORLD FREE OF NUCLEAR WEAPONS

Moritz Kütt and Alex Glaser

34c3, Leipzig, December 2017

Revision 4

BACKGROUND

NUCLEAR WEAPONS: WHERE WE ARE IN 2017/2018

USA
6,800

U.S. Nuclear Weapon

Russia
7,000

United Kingdom
215

France
300

Israel
80

Pakistan
135

India
125

China
270

North Korea
15

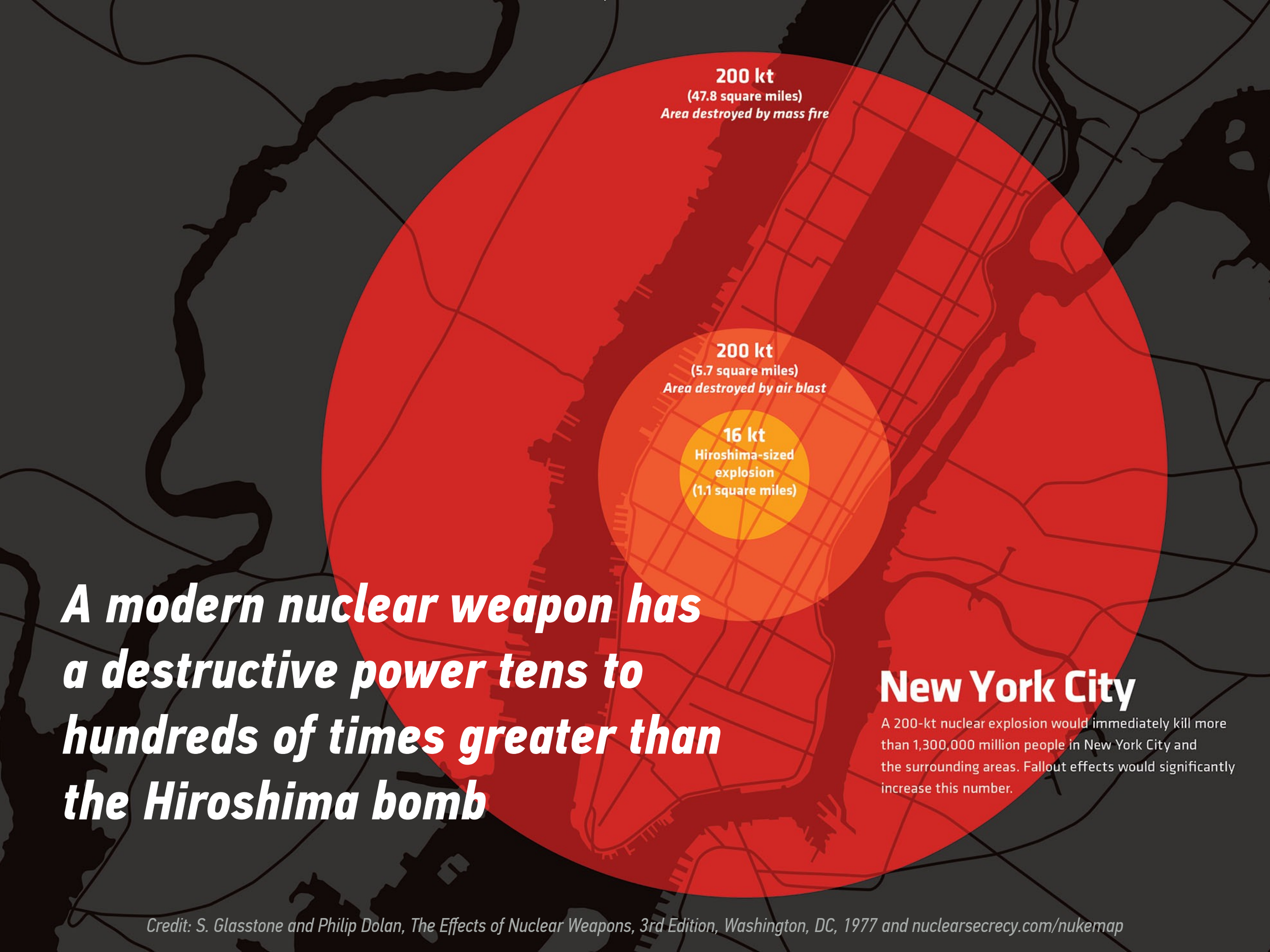
North Korean Nuclear Weapon

There remain about 15,000 nuclear weapons in the world today

Hans Kristensen and Robert Norris, Nuclear Notebook, Federation of American Scientists and thebulletin.org/nuclear-notebook-multimedia

“THE PEANUT”

September 2, 2017, Source: KCNA/EPA
North Korea tested a nuclear weapon with an estimated yield of 250 kt(TNT) on September 3, 2017

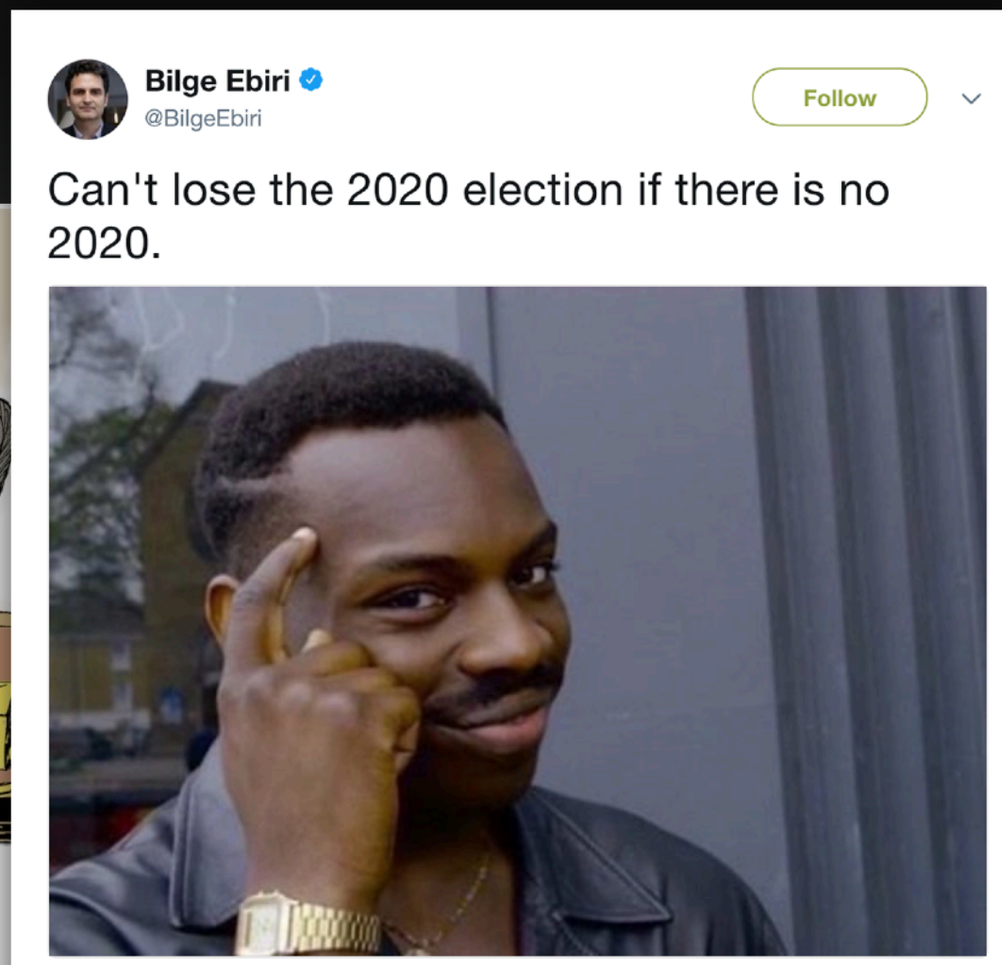


A modern nuclear weapon has a destructive power tens to hundreds of times greater than the Hiroshima bomb

New York City

A 200-kt nuclear explosion would immediately kill more than 1,300,000 million people in New York City and the surrounding areas. Fallout effects would significantly increase this number.

Credit: S. Glasstone and Philip Dolan, The Effects of Nuclear Weapons, 3rd Edition, Washington, DC, 1977 and nuclearsecrecy.com/nukemap



NBC NEWS

EXCLUSIVE INVESTIGATIONS OCT 11 2017, 7:23 AM ET

Trump Wanted Tenfold Increase in Nuclear Arsenal, Surprising Military

by COURTNEY KUBE, KRISTEN WELKER, CAROL E. LEE and SAVANNAH GUTHRIE

www.chappatte.com/en/images/trump-president and twitter.com/bilgeebiri/status/895006813078401027
www.nbcnews.com/news/all/trump-wanted-dramatic-increase-nuclear-arsenal-meeting-military-leaders-n809701

THE BAN TREATY

NEGOTIATED BY 122 COUNTRIES, UNITED NATIONS, MARCH–JULY 2017

Source: Tamara Patton

Treaty on the Prohibition of Nuclear Weapons
www.icanw.org/wp-content/uploads/2017/07/TPNW-English1.pdf

THE BAN TREATY

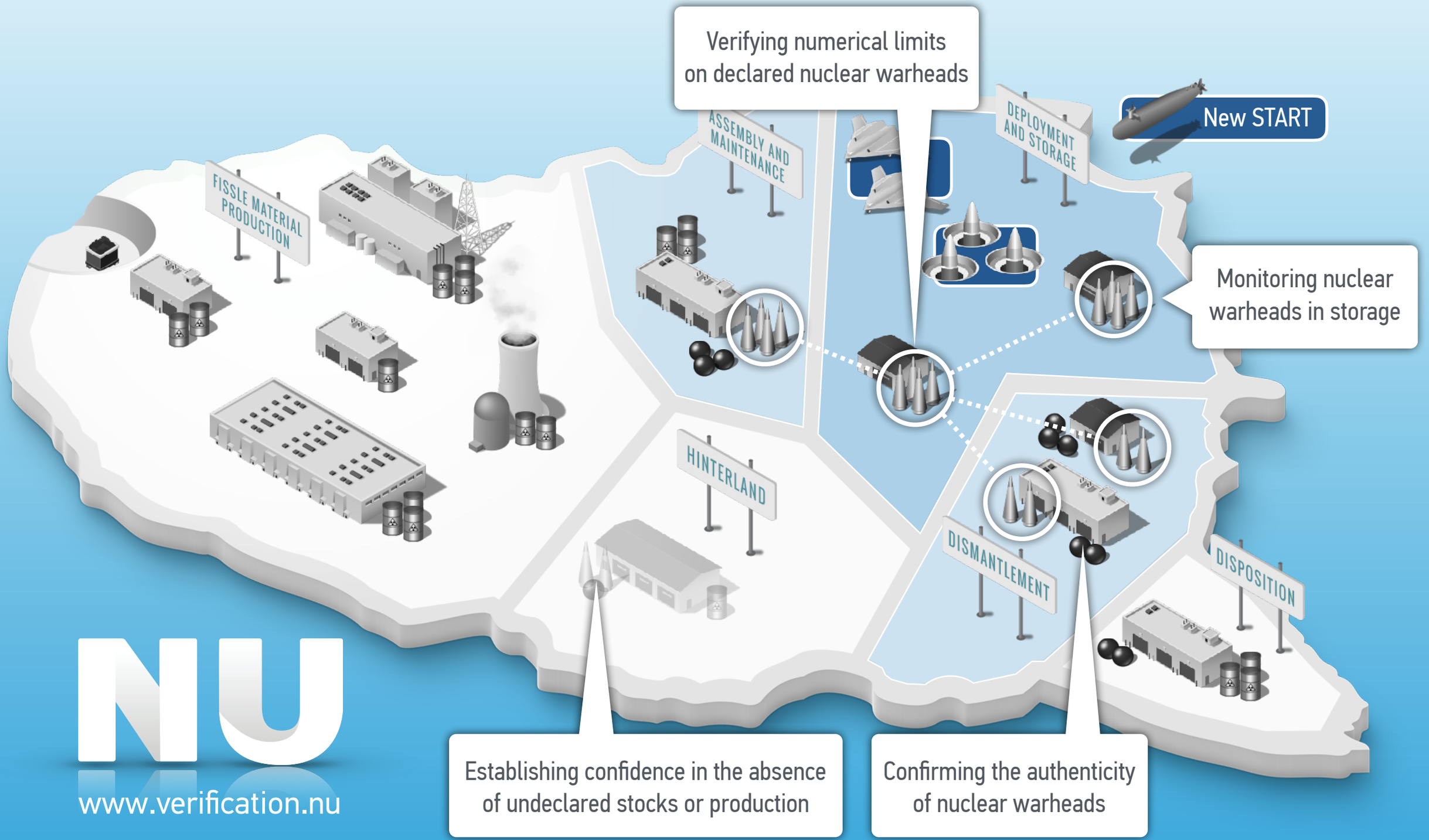
AND THE 2017 NOBEL PEACE PRICE FOR ICAN

Tim Wright and Ray Acheson with Ban Treaty

Setsuko Thurlow and Beatrice Fihn with Berit Reiss-Andersen

WHAT IS TO BE VERIFIED?

VERIFICATION CHALLENGES OF DEEP REDUCTIONS AND A NUCLEAR WEAPON FREE WORLD



NU

www.verification.nu

Revision 3

VERIFICATION CHALLENGES OF DEEP REDUCTIONS AND A NUCLEAR WEAPON FREE WORLD

NU

www.verification.nu

Revision 3

CONFIRMING THE AUTHENTICITY OF WARHEADS

THERMONUCLEAR WARHEAD

ON AVERAGE, A MODERN NUCLEAR WARHEAD MAY CONTAIN 3–4 KG OF PLUTONIUM AND UP TO 25 KG OF HIGHLY ENRICHED URANIUM

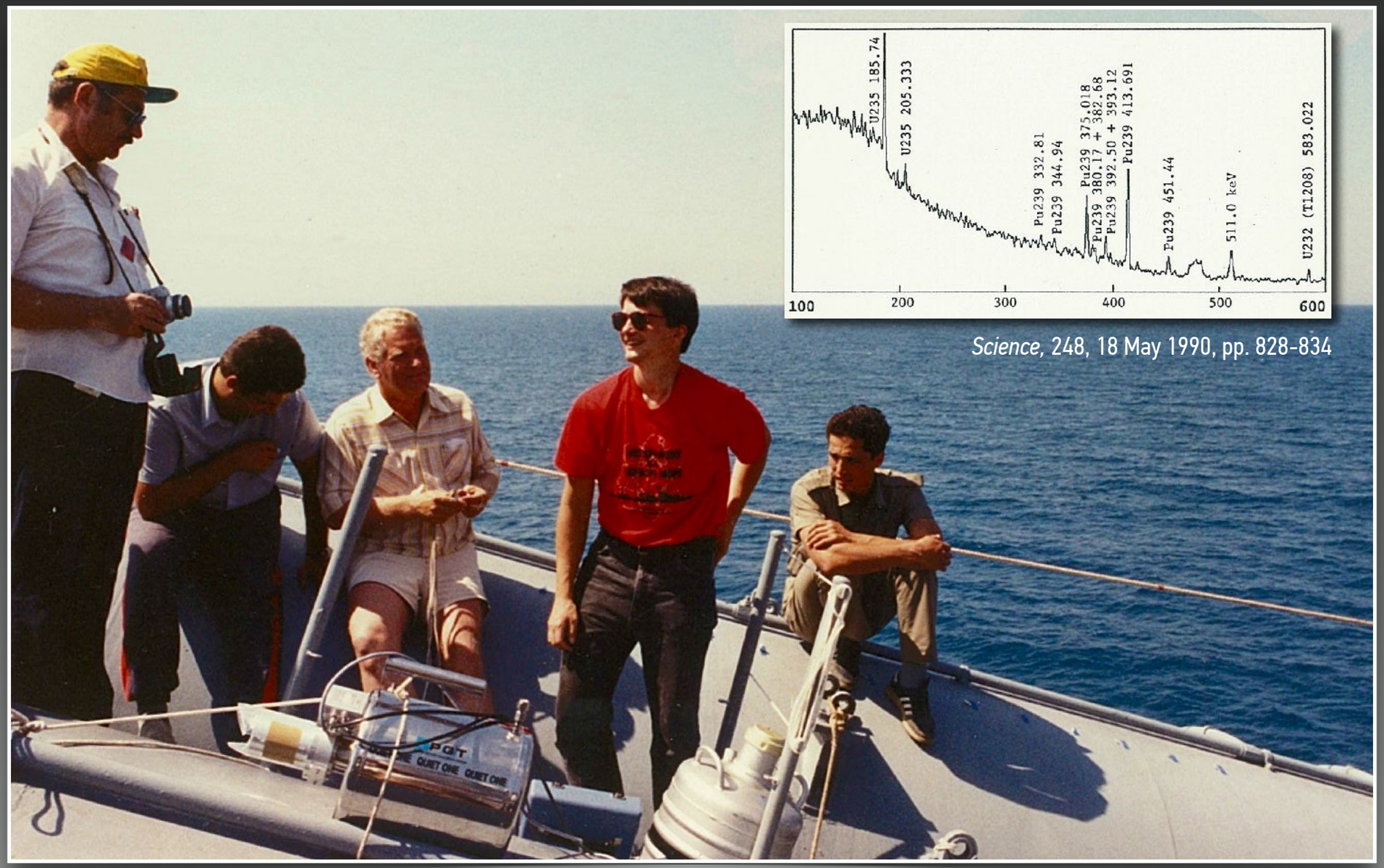
Primary
Typically contains plutonium
(and/or highly enriched uranium)

Secondary
Typically contains highly enriched uranium
(and lithium-deuteride as fusion fuel)

Source: fas.org; U.S. Department of Defense

NUCLEAR WEAPONS HAVE UNIQUE RADIATION SIGNATURES

BUT THEY ARE SENSITIVE AND CANNOT BE REVEALED TO INSPECTORS



U.S. Scientists on a Soviet Cruiser in the Black Sea, 1989

NUCLEAR WARHEAD VERIFICATION

KEY CONCEPTS OF (PROPOSED) INSPECTION SYSTEMS

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

(Examples to follow)

FUNDAMENTAL UNRESOLVED CHALLENGE

How can information barriers simultaneously be authenticated and certified,
i.e., trusted by inspector team and host team at the same time?

"All I see is a green LED
with a battery connected to it."

Russian nuclear weapons expert during technology demonstration
at a U.S. national laboratory in the early 2000s

WHY ARE WARHEAD INSPECTIONS SO HARD?

(AS SEEN FROM INSPECTOR'S PERSPECTIVE)

VERY LITTLE (IF ANY) INFORMATION ABOUT THE INSPECTED ITEM CAN BE REVEALED

Some information may be shared in advance, but no additional information during inspection

ADVERSARY/COMPETITOR HAS (DE FACTO) INFINITE RESOURCES

ADVERSARY/COMPETITOR MAY BE EXTREMELY MOTIVATED (TO DECEIVE INSPECTOR)

Stakes are very high (especially when the number of weapons drops below ~1,000)

HOST HAS LAST OWNERSHIP OF INSPECTION SYSTEM BEFORE THE MEASUREMENT

(and inspector never again has access to system after the measurement is complete)

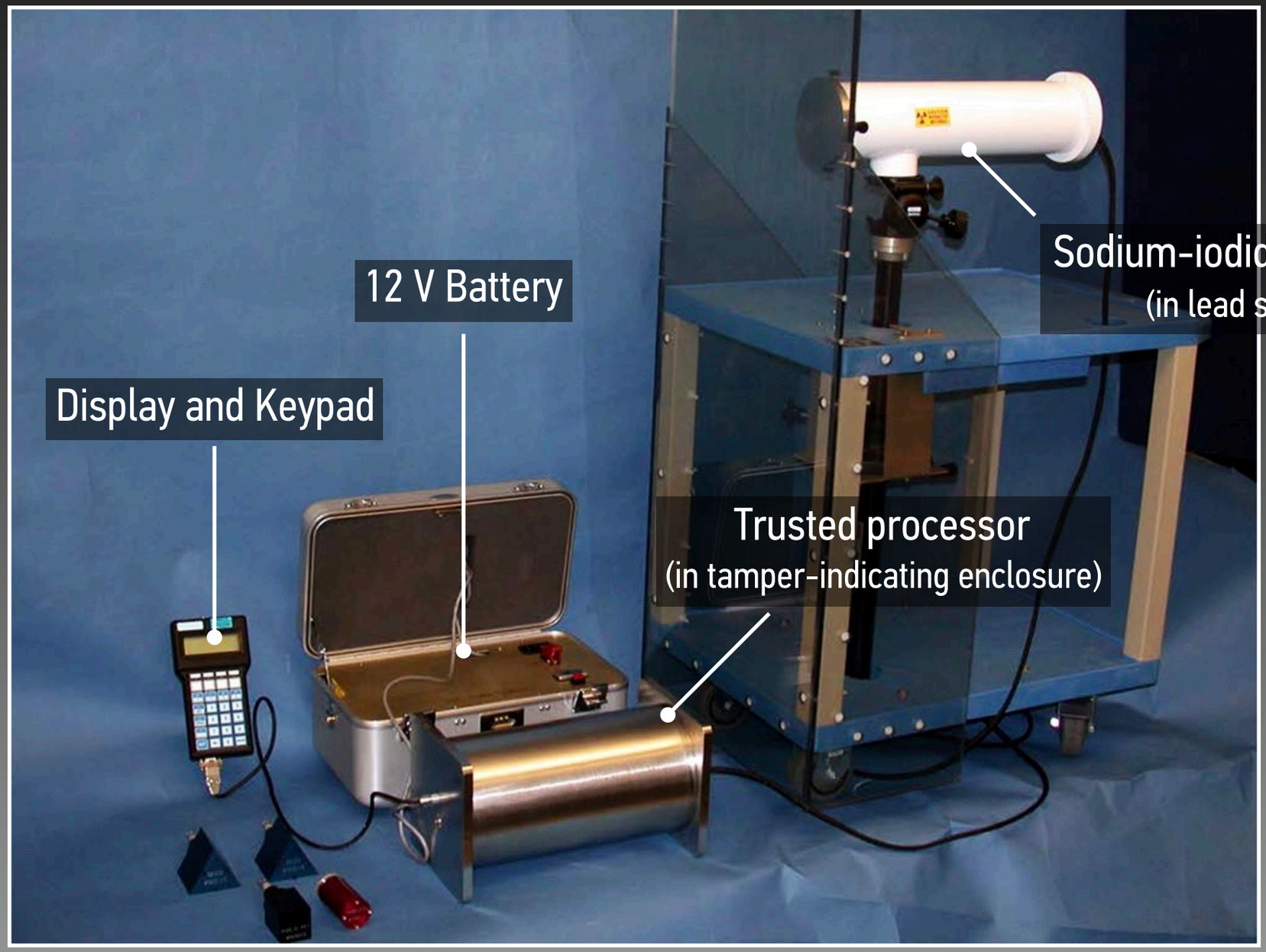
EXAMPLE 1

TRUSTED RADIATION IDENTIFICATION SYSTEM (TRIS)

Sandia National Laboratories, 1999–2001

TRUSTED RADIATION IDENTIFICATION SYSTEM

(SANDIA NATIONAL LABORATORIES)



K. D. Seager, R. L. Lucero, T. W. Laub, K. W. Inch, D. J. Mitchell, Trusted Radiation Identification System (TRIS) Users Manual SAND2017-0578TR, Sandia National Laboratories, Albuquerque, New Mexico, December 2002 (July 2011 Revision)

WHAT WE LIKE ABOUT TRIS

SIMPLE DETECTOR SYSTEM

Passive low-resolution measurement (of gamma emissions from inspected item) with standard sodium-iodide detector

STRONG TAMPER INDICATING ENCLOSURE

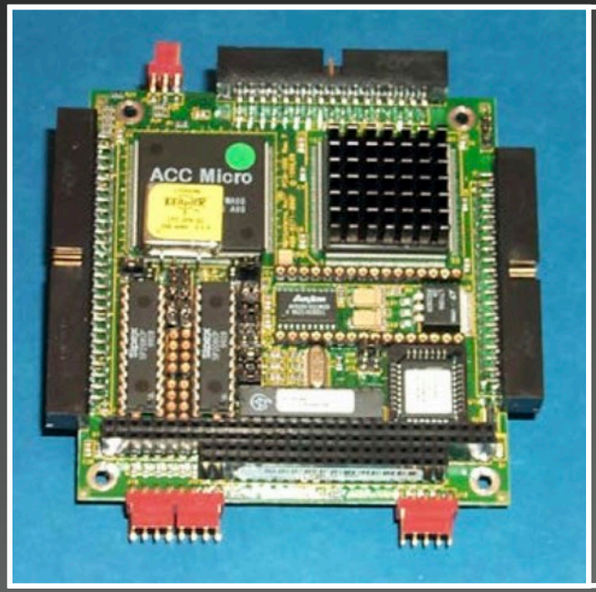
Spiral tamper board and eddy-current scanner to confirm integrity of enclosure;
Red-side (classified) and black-side processors communicate optically (through pinholes)

FAST TEMPLATE APPROACH WITH SIMPLE (AND ROBUST) PASS/FAIL ALGORITHM

Measurement only takes 30–60 seconds; uses 16 numbers and standard statistical test to determine inspection result

Source: U.S. Department of Energy (top and middle), Authors (bottom)

WHAT WE DON'T LIKE AS MUCH



COMPLEX (AND MOSTLY) CLOSED HARDWARE PLATFORM

Includes a PC/104 board made by *WinSystems* (winsystems.com) based on an AMD 586 CPU (~ 4 million transistors) and a Xilinx FPGA to acquire and digitize detector data

ESTABLISHING INSPECTOR CONFIDENCE REMAINS A CHALLENGE

On inspector confidence versus information security:

The protection of classified information is the more important requirement, which dictates that the inspection equipment must be provided by the host country. (TRIS User's Manual)

Source: TRIS User's Manual, 2002/2011 (top) and Joint US-UK Report, 2010, U.S. Department of Energy

EXAMPLE 2

UK-NORWAY INFORMATION BARRIER

UK-Norway Initiative, 2007–2017

www.ukni.info

UK-NORWAY INFORMATION BARRIER

Phase III Design of Information Barrier

Source: ukni.info

WHAT WE LIKE ABOUT THE UKNI-IB

CLEAR OPERATIONAL PROCEDURES

Straightforward interface allows host and inspector to continuously follow sequence of operations and measurement results

COMPREHENSIVE DOCUMENTATION

Project partners have often presented progress in public venues;
Schematics and Bill of Materials for hardware and ADA software available at www.ukni.info

JOINT DESIGN EFFORT INVOLVING NON-WEAPON STATE

First collaboration between weapon owner and non-weapon state
sheds light on possible design challenges for verification among all countries

Source: ukni.info (top and bottom) and pxhere.com/en/photo/536212 (middle)

WHAT WE DON'T LIKE AS MUCH

COMPLEX DETECTOR SYSTEM WITH ATTRIBUTE APPROACH

High-purity Germanium (HPGe) detector requires cryogenic cooling, difficult to operate in the field, inevitable collection of detailed spectra

Complex algorithm, confirms presence and isotopics of plutonium

CLOSED-CHIP ARCHITECTURE MICROCONTROLLER

UKNI design uses two modern 8 bit microcontrollers:
ATmega 2560 for data analysis, *ATtiny13A* for timing of analog circuit;
certification and authentication of these controllers could be challenging;
built-in flash memory possible data leak

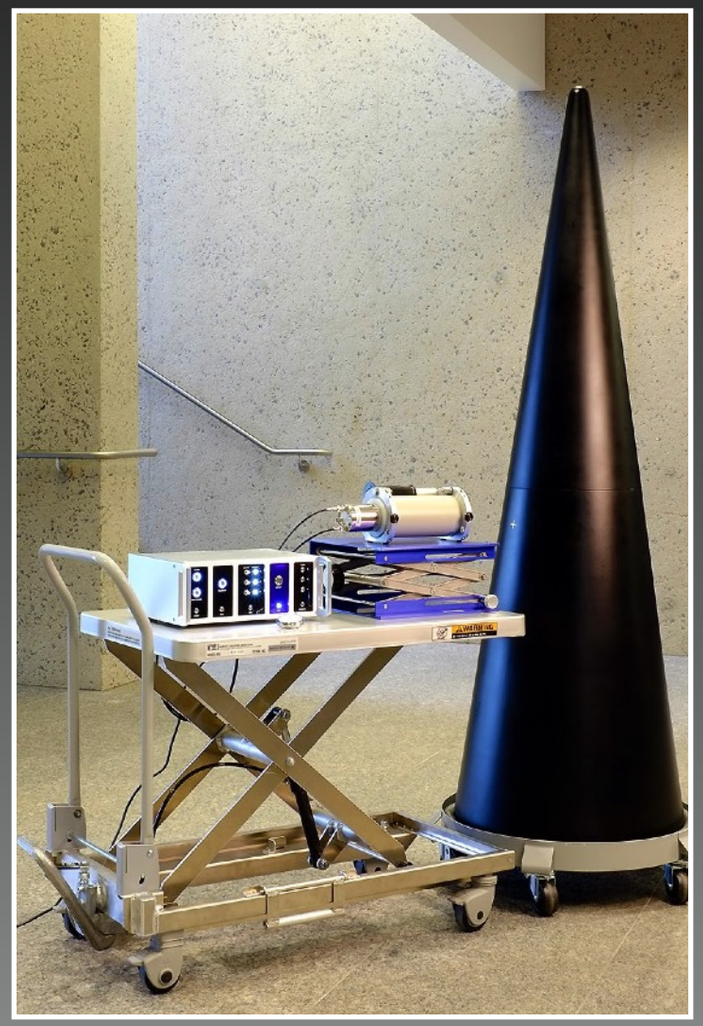
Source: ukni.info and instructables.com

EXAMPLE 3

INFORMATION BARRIER EXPERIMENTAL

Princeton University, 2016

INFORMATION BARRIER EXPERIMENTAL

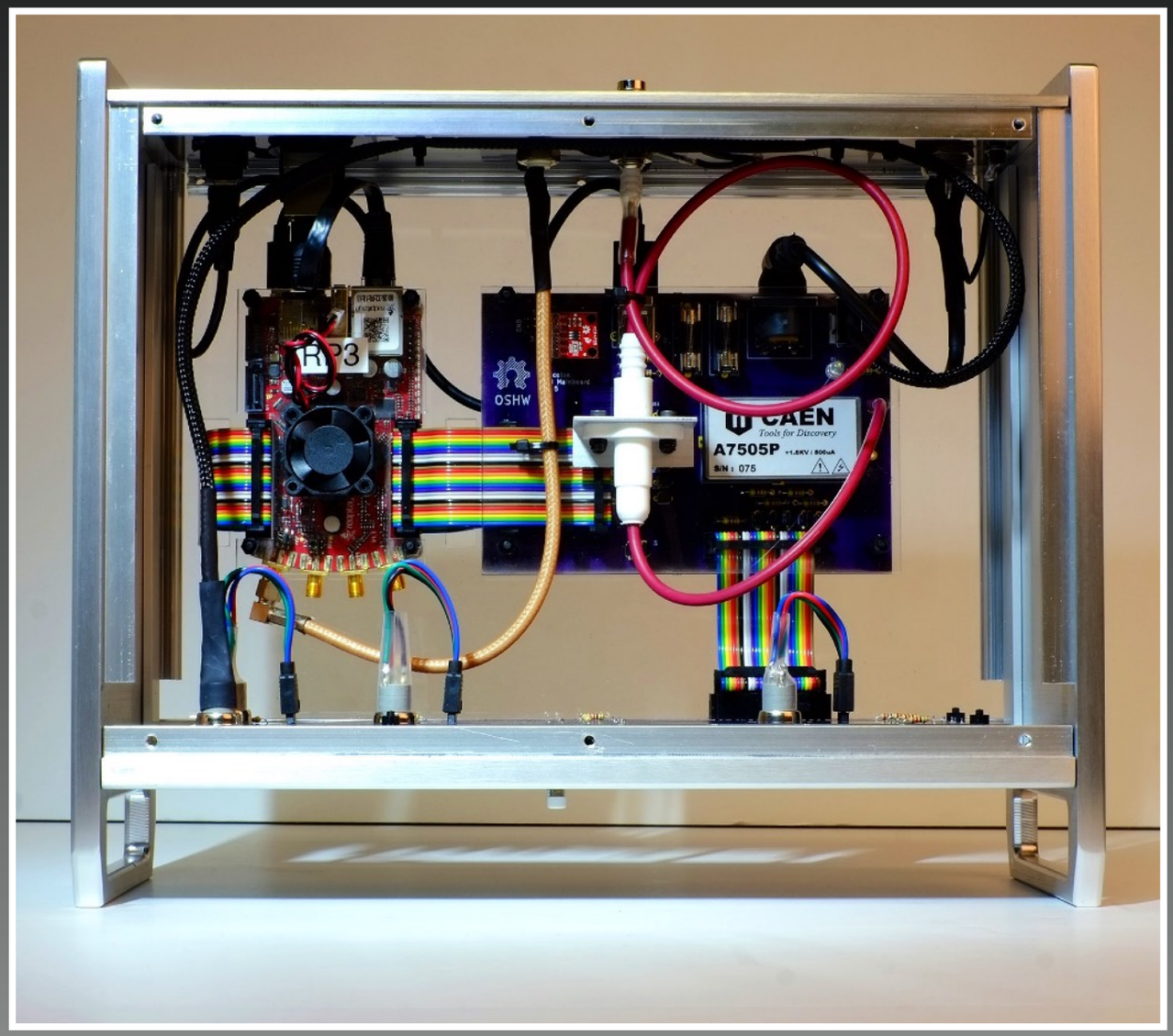


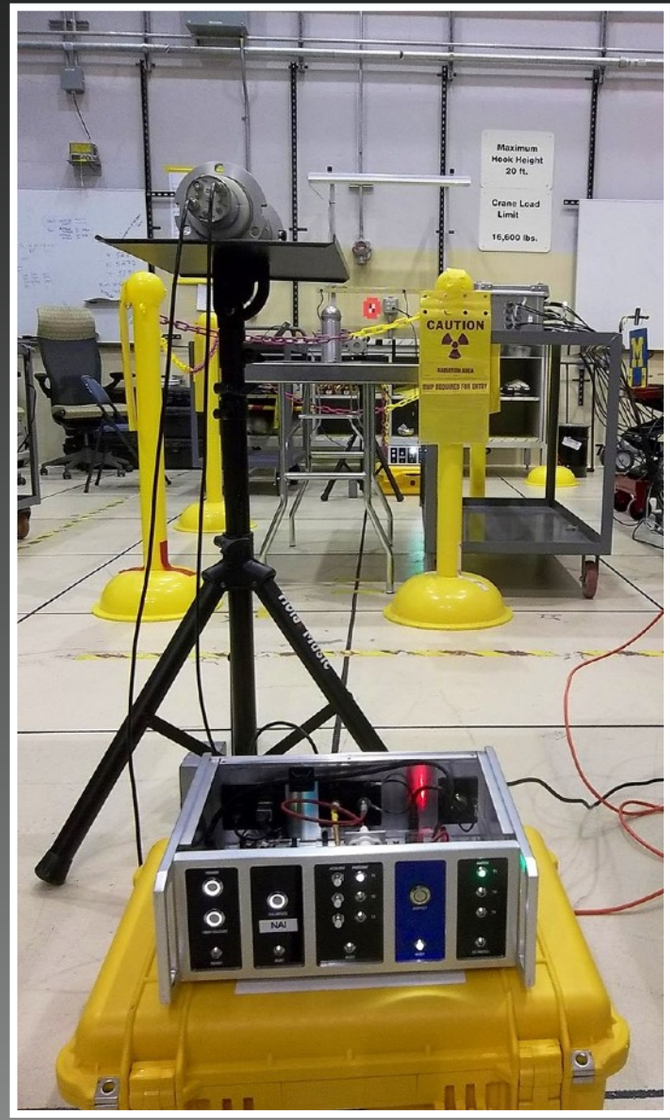
Source: Authors

M. Kütt, M. Göttsche, and A. Glaser, "Information Barrier Experimental," *Measurement,* 114, 2018

M. Göttsche, J. Schirm, and A. Glaser, "Low-resolution Gamma-ray Spectrometry for an Information Barrier Based on a Multi-criteria Template-matching Approach," *Nuclear Instruments and Methods A,* 840, 2016, pp. 139–144

INFORMATION BARRIER EXPERIMENTAL





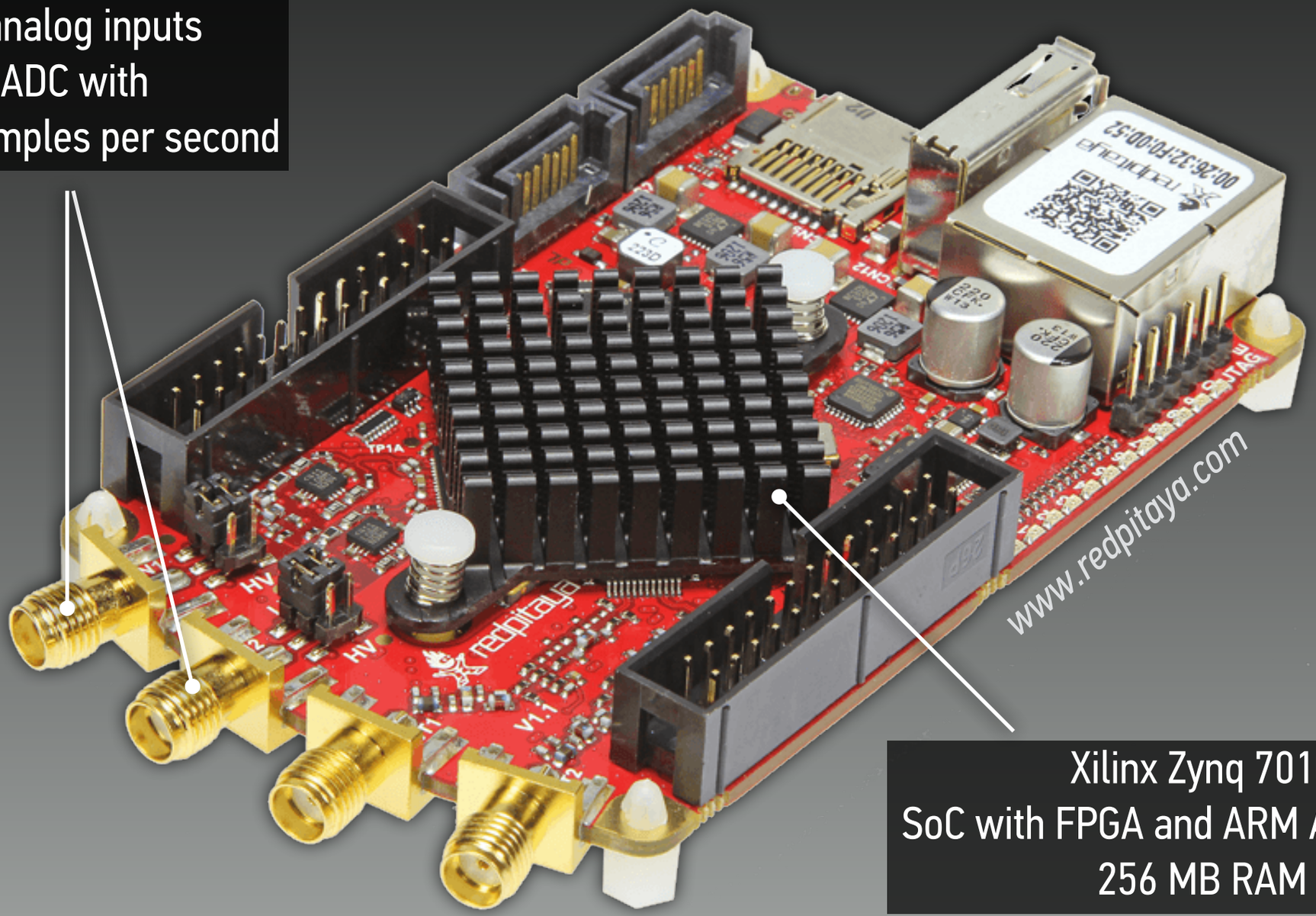
M. Kütt, M. Göttsche, and A. Glaser, “Information Barrier Experimental,” *Measurement,* 114, 2018

M. Göttsche, J. Schirm, and A. Glaser, “Low-resolution Gamma-ray Spectrometry for an Information Barrier Based on a Multi-criteria Template-matching Approach,” *Nuclear Instruments and Methods A,* 840, 2016, pp. 139–144

INFORMATION BARRIER EXPERIMENTAL

(BASED ON THE RED PITAYA)

Two fast analog inputs
14-bit ADC with
125 million samples per second



Xilinx Zynq 7010
SoC with FPGA and ARM A9 (2 cores)
256 MB RAM

VINTAGE VERIFICATION

THE BEST OF ALL WORLDS?

"TRUST THROUGH SIMPLICITY AND OBSOLESCENCE?"

SIMPLE DETECTOR SYSTEM

Sodium-iodide scintillation detector for inherently low-resolution gamma spectroscopy; Widely available, cheap, and simple to use in the field

VINTAGE COMPUTING PLATFORM

Simple, quasi open-source architecture; backdoors and hidden switches unlikely in hardware designed in the distant past, at a time, when use for sensitive measurements was never envisioned

BRING-YOUR-OWN-INFORMATION-BARRIER (BYOIB) OPTION

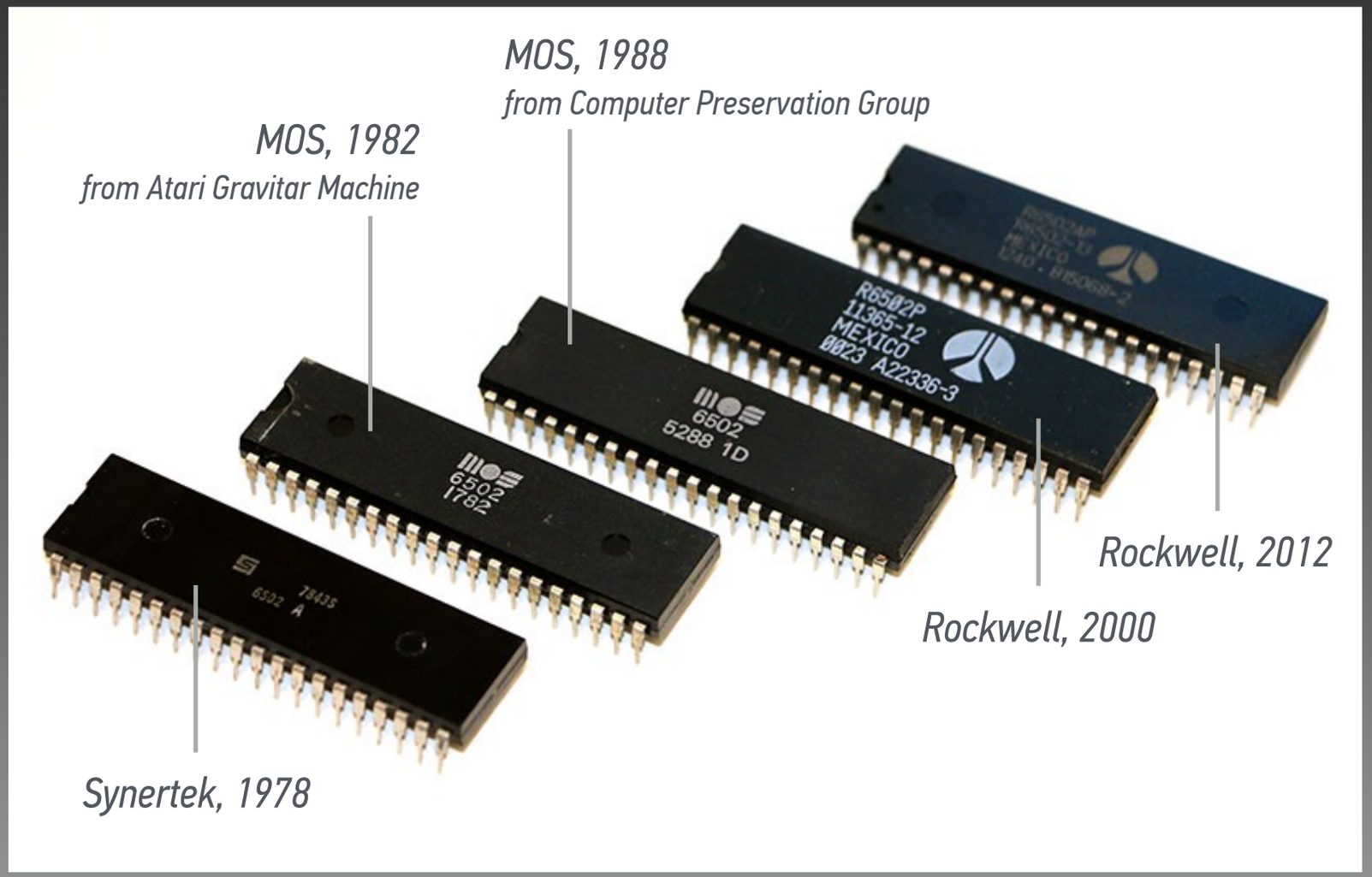
Limited capabilities make it difficult and perhaps impossible to surreptitiously implement extra functionalities to leak secret information; this should simplify verification, as hardware could be inspector-supplied or jointly acquired

Source: Authors (top and middle) and ayaypicante.com (bottom)

WHY CHOOSING THE 6502?

(STILL) FEWER TRANSISTORS THAN THERE ARE NUCLEAR WEAPONS TODAY

(3510 TRANSISTORS, 1 MEGAHERTZ, 56 INSTRUCTIONS)



Five of the 10 billion units made

In-house 6502 functionality testing

Source: Apple Computer, Inc.

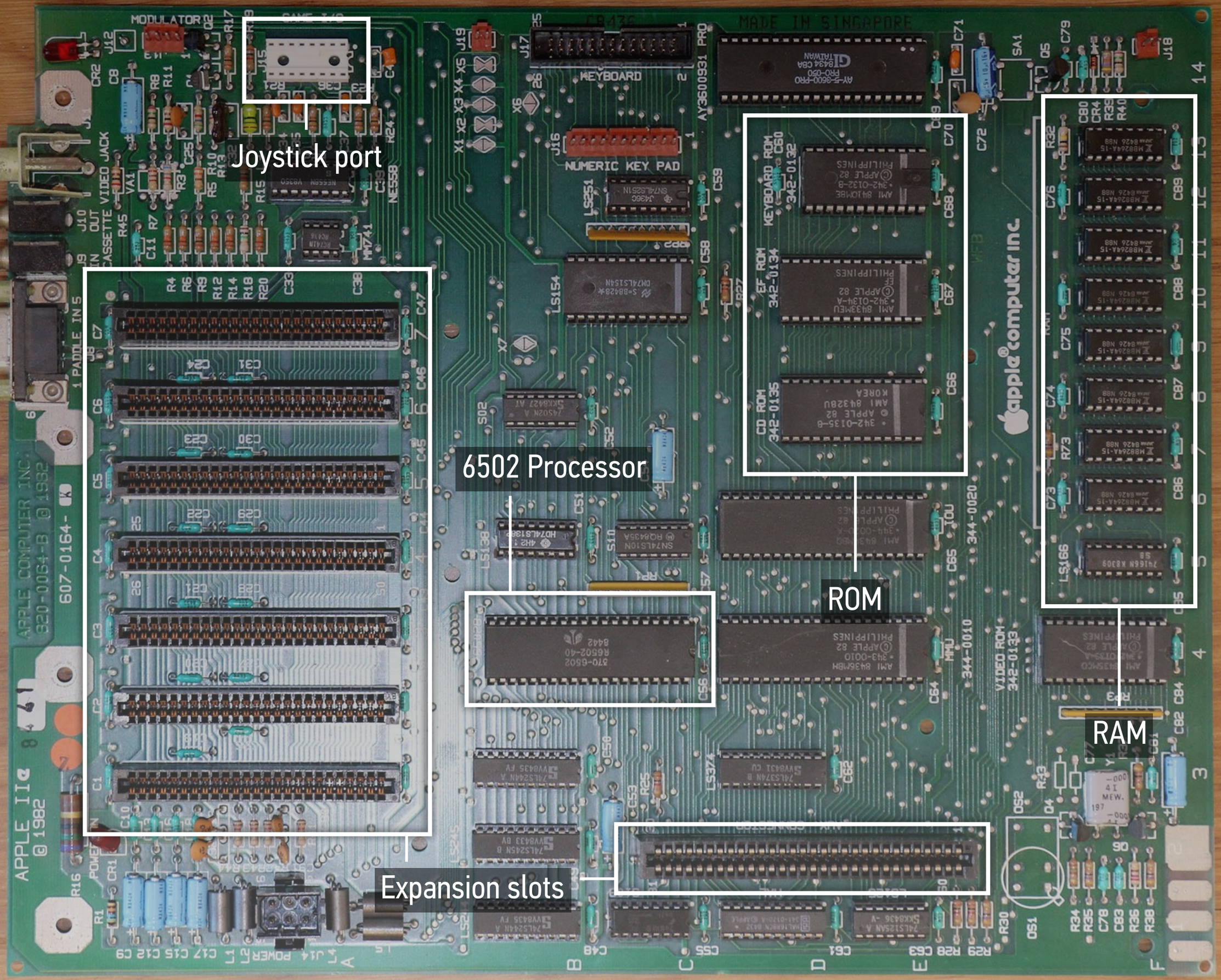
WHY USE THE APPLE][AS A PROTOTYPING PLATFORM?

Source: Authors

Most hackers and hobbyists liked to customize, modify, and jack various things into their computers. To Jobs, this was a threat to a seamless end-to-end user experience.

Wozniak, a hacker at heart, disagreed. He wanted to include eight slots on the Apple II for users to insert whatever smaller circuit boards and peripherals they might want. Jobs insisted there be only two, for a printer and a modem.

Walter Isaacson, Steve Jobs

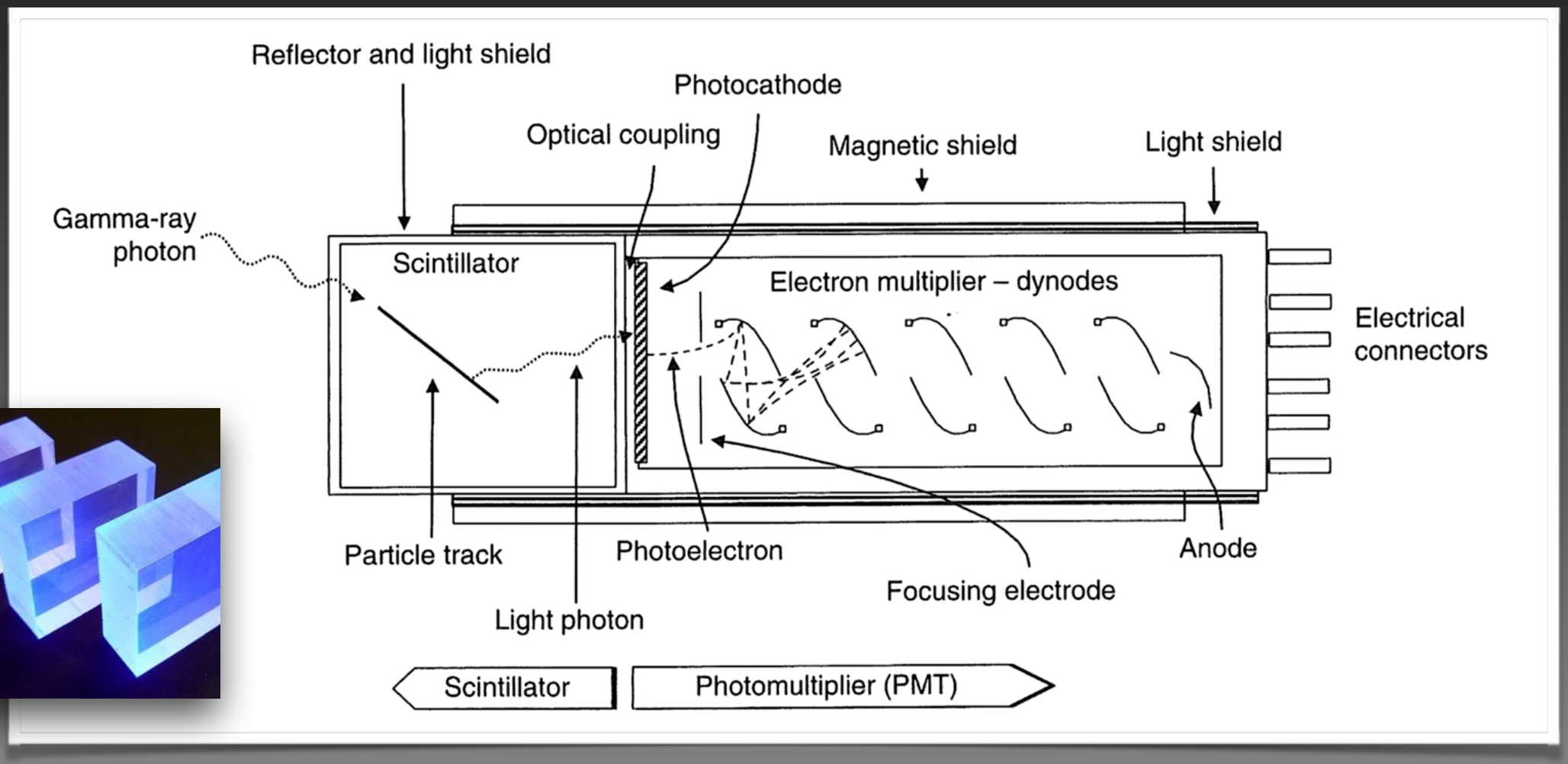

Joystick port
6502 Processor
ROM
RAM
Expansion slots

DEMO TIME

(BOOT FROM DISK, TURN ON HIGH VOLTAGE, ACQUIRE TEMPLATE)

youtu.be/QfXNuIrrJQw

SCINTILLATION DETECTOR



Source: G. Gilmore, Practical Gamma-ray Spectroscopy, Wiley, 2011

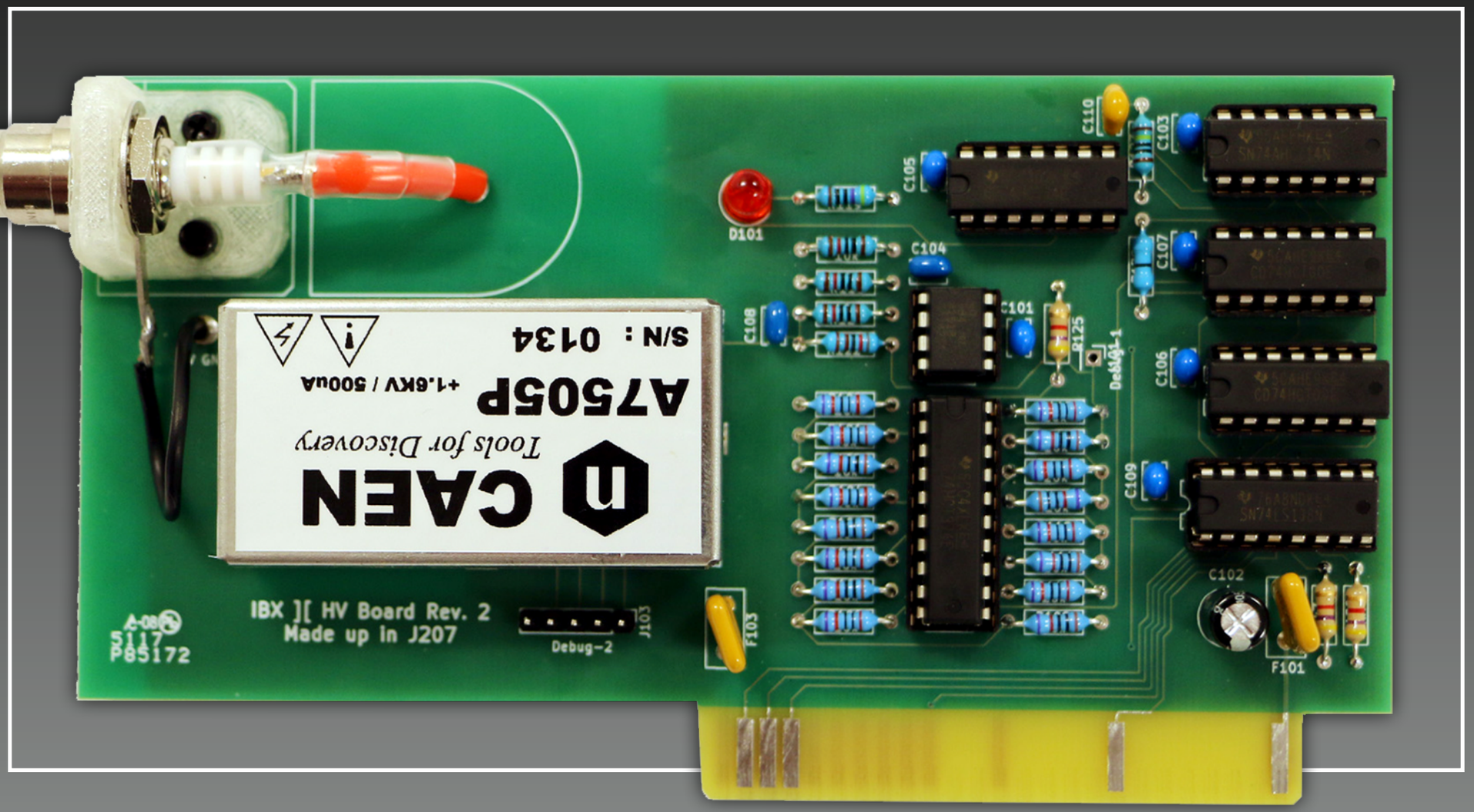
About 38,000 photons per MeV of energy deposited in NaI

For each electron from cathode, photomultiplier produces on the order 10 million electrons

INFORMATION BARRIER EXPERIMENTAL II

HIGH VOLTAGE BOARD

IBX II HIGH VOLTAGE BOARD

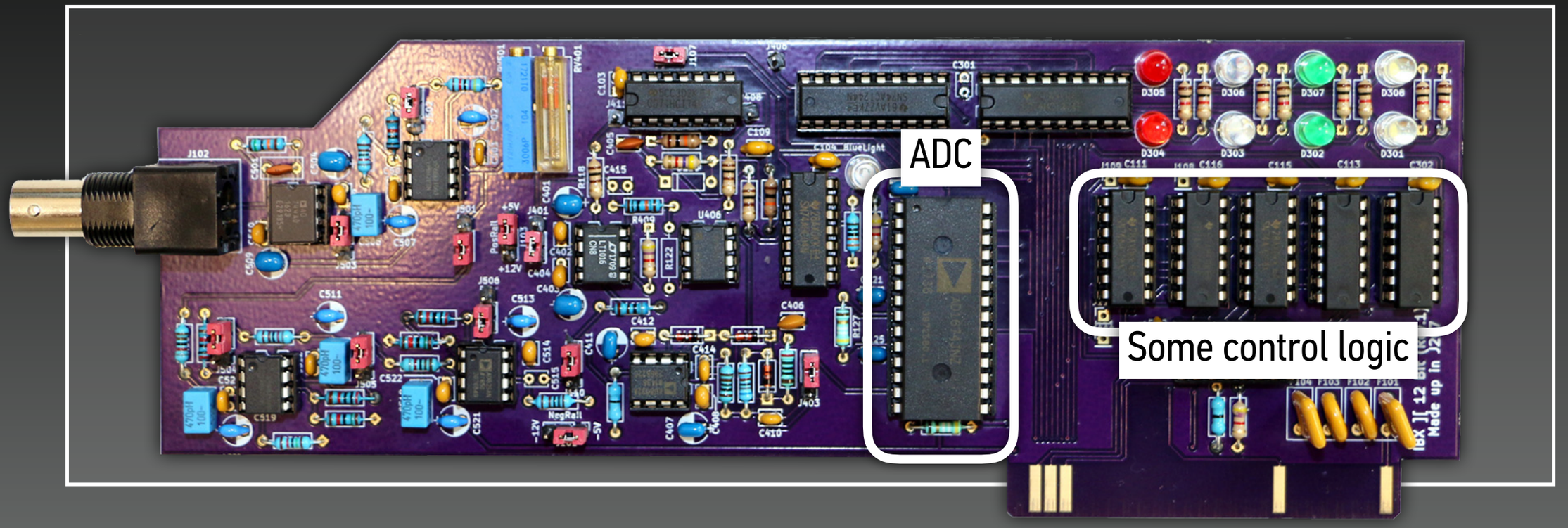


We use a simple R2R Digital-to-Analog Conversion to adjust high voltage (photomultiplier tube needs ramping to protect equipment)

INFORMATION BARRIER EXPERIMENTAL II

DATA ACQUISITION BOARD

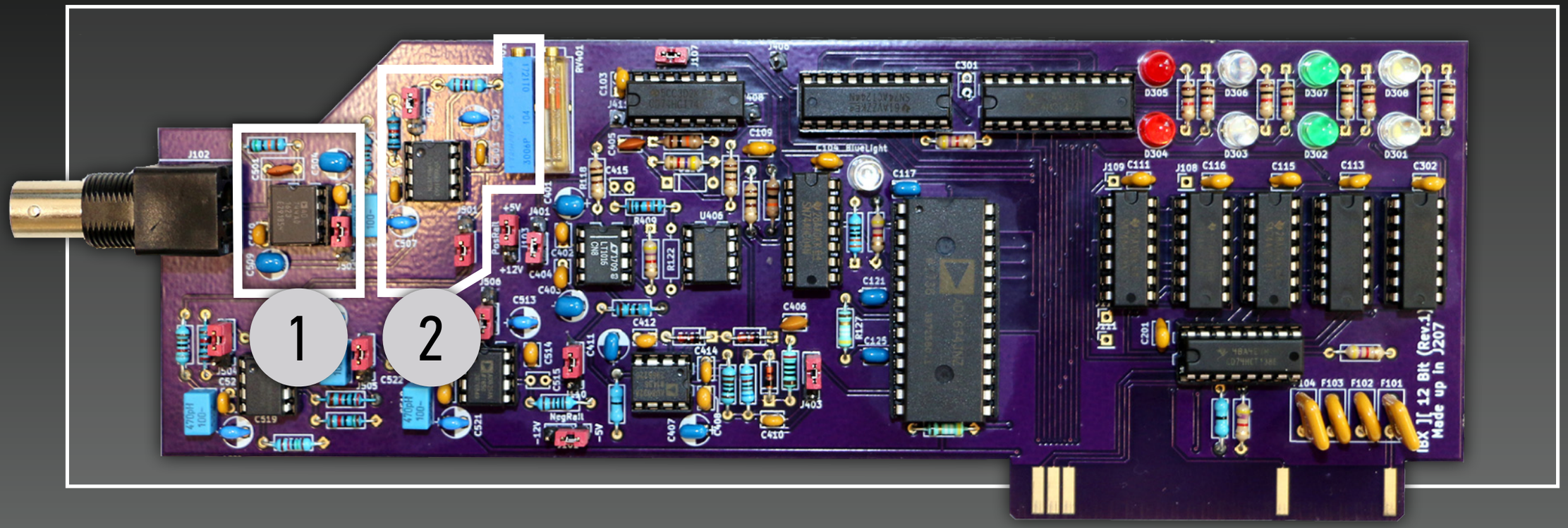
IBX II DATA ACQUISITION BOARD



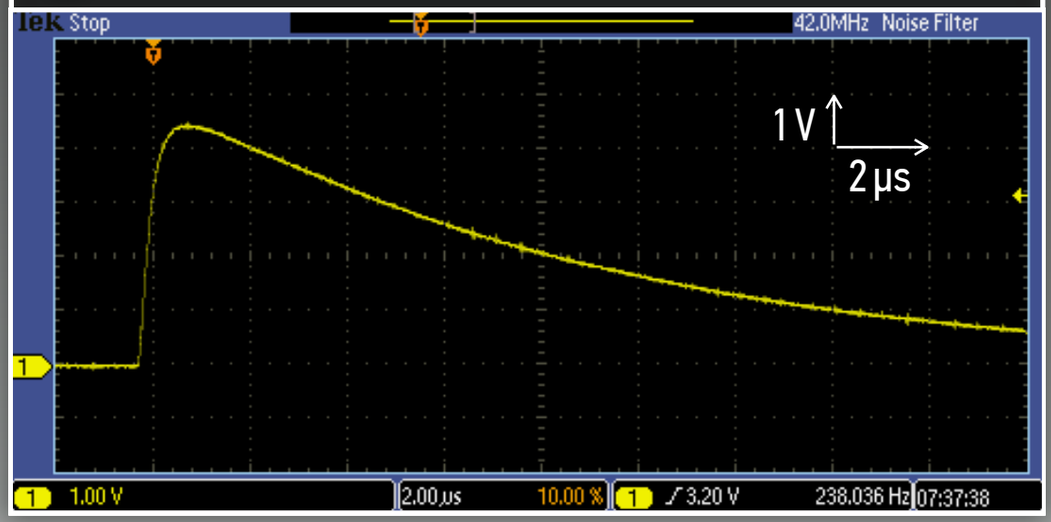
As ADC, we use an AD1674 (12-bit flash ADC with 8-bit bus-interface and internal voltage reference)
The ADC samples an incoming pulse in 10–15 µs

Decode logic (and ADC timing) uses only Quad-NAND (7400) and Hex-NOT (7404) chips,
in addition to one 3-to-8 decoder (74138)

IBX II DATA ACQUISITION BOARD

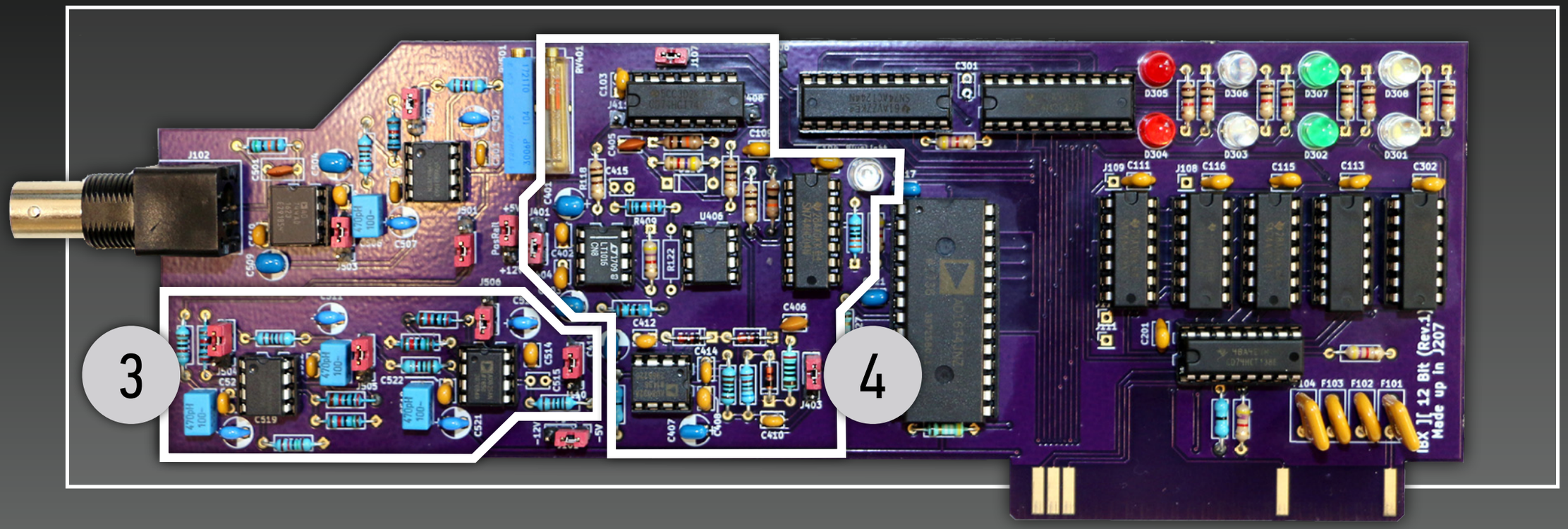


1 Pre-amplifier: Charge-sensitive OpAmp

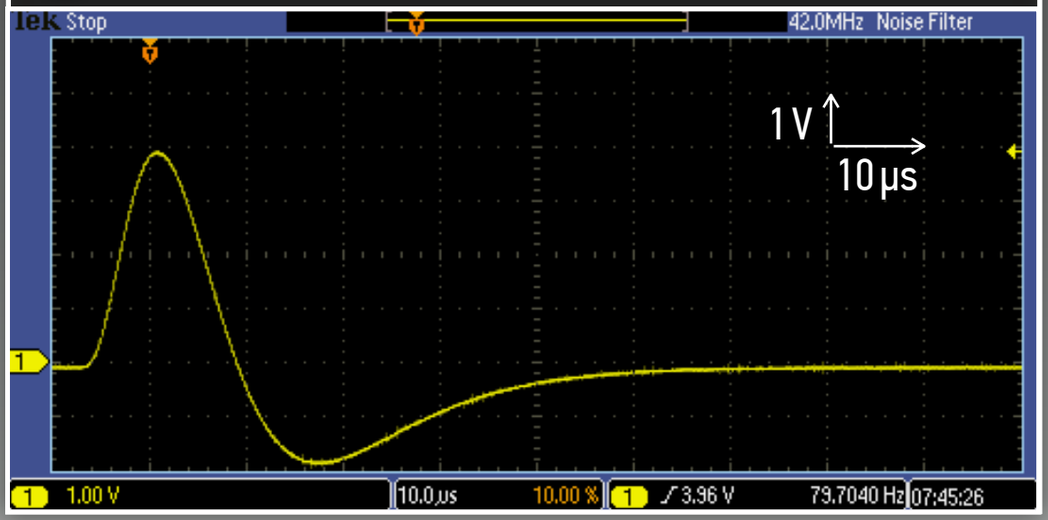


2 Differentiating OpAmp ... and adjustable gain

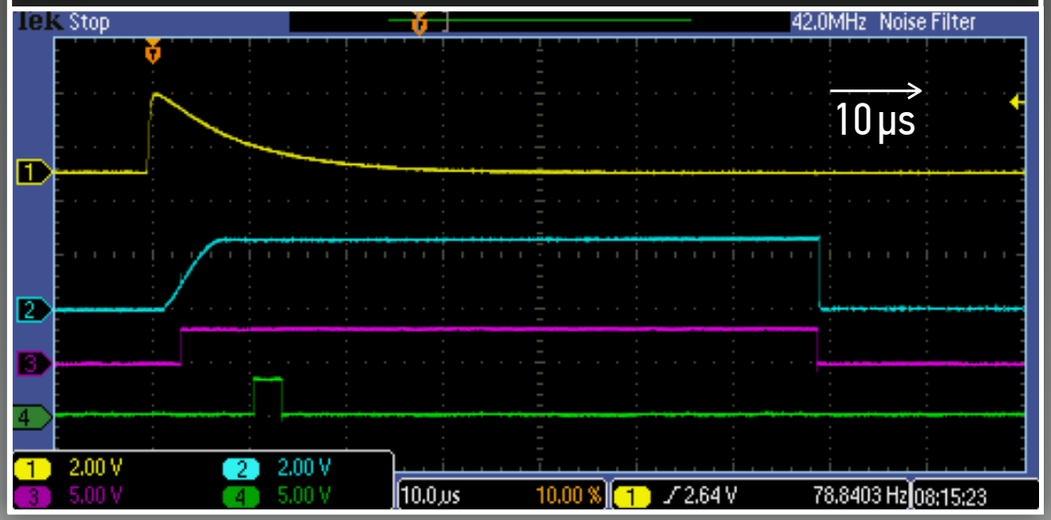
IBX II DATA ACQUISITION BOARD



3 Pulse-shaping: Series of low-pass filters



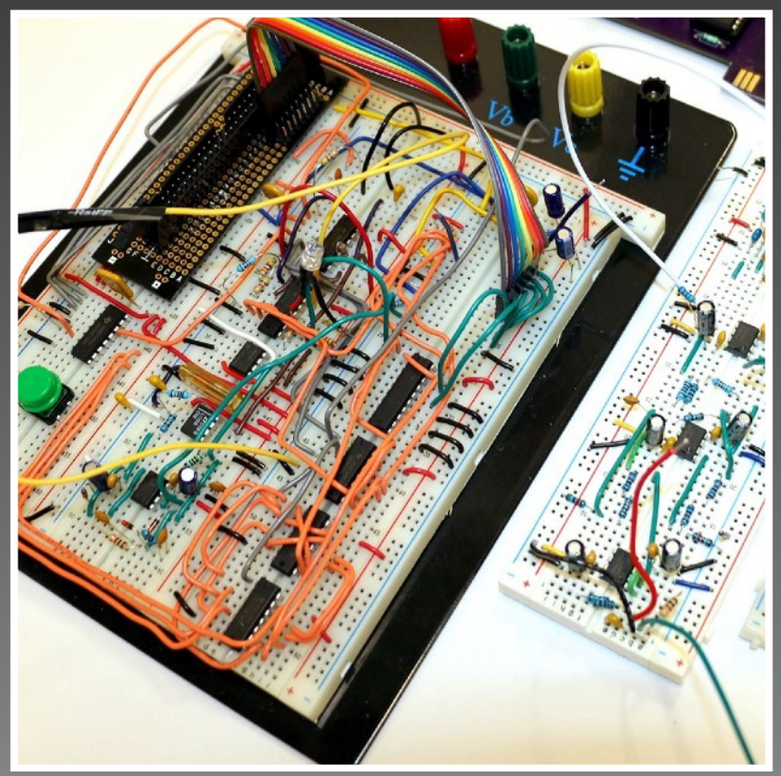
4 Peak detect & hold ... and ADC timing



DEVELOPMENT FOR VINTAGE COMPUTING PLATFORMS

LESSONS LEARNED

Read actual (!) books



Design, try, repeat

Choose a real-world problem

github.com/nuclearfutureslab/ibxII-software

DEMO TIME

(INSPECT ... WITH ANOTHER CHECK SOURCE?)

youtu.be/QfXNuIrrJQw

COMPARING TWO RADIATION SPECTRA

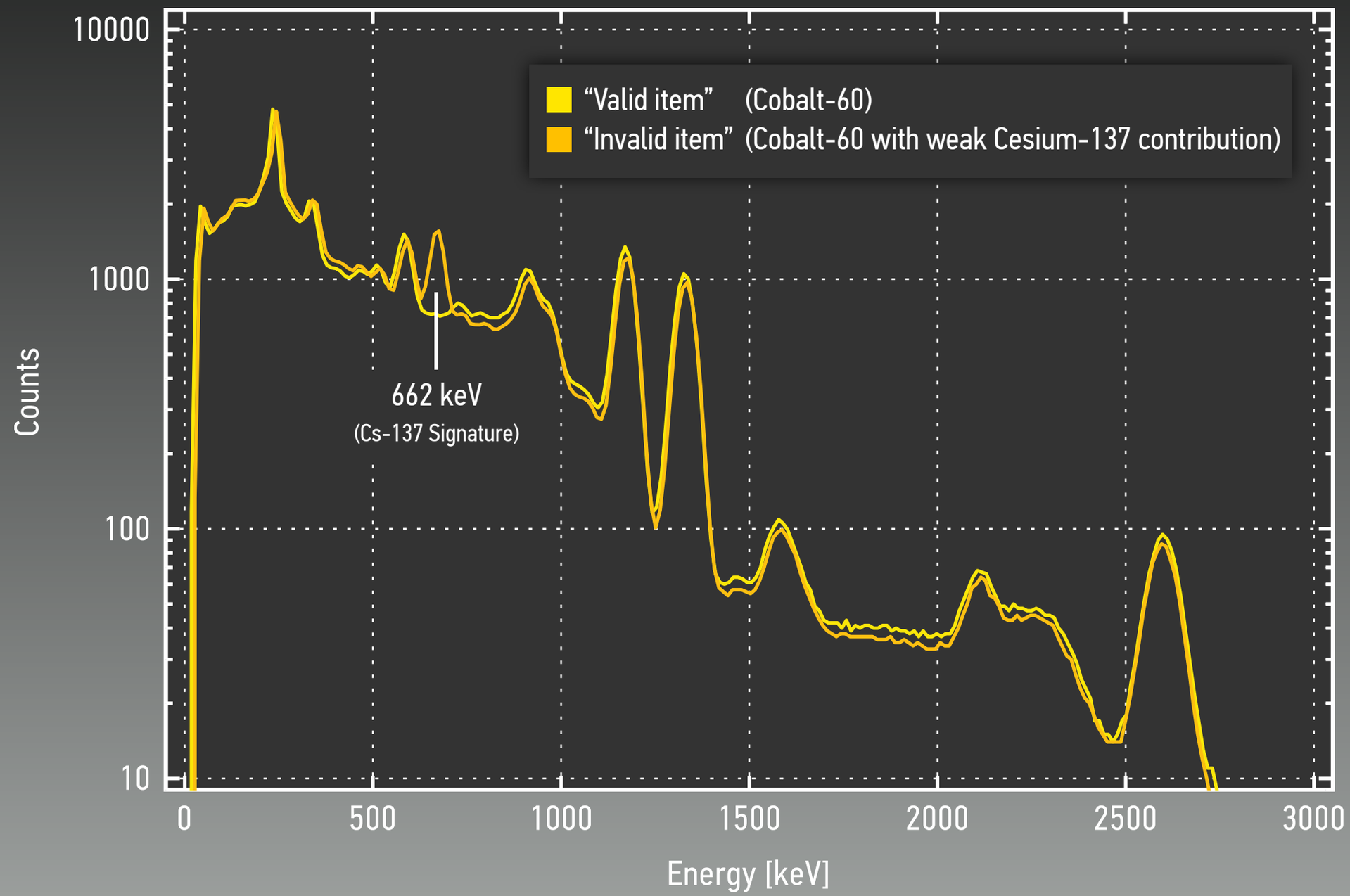
WITH 6502-STYLE COMPUTATIONAL EFFORT

(INSPIRED BY TRIS)

(SKIP TO END)

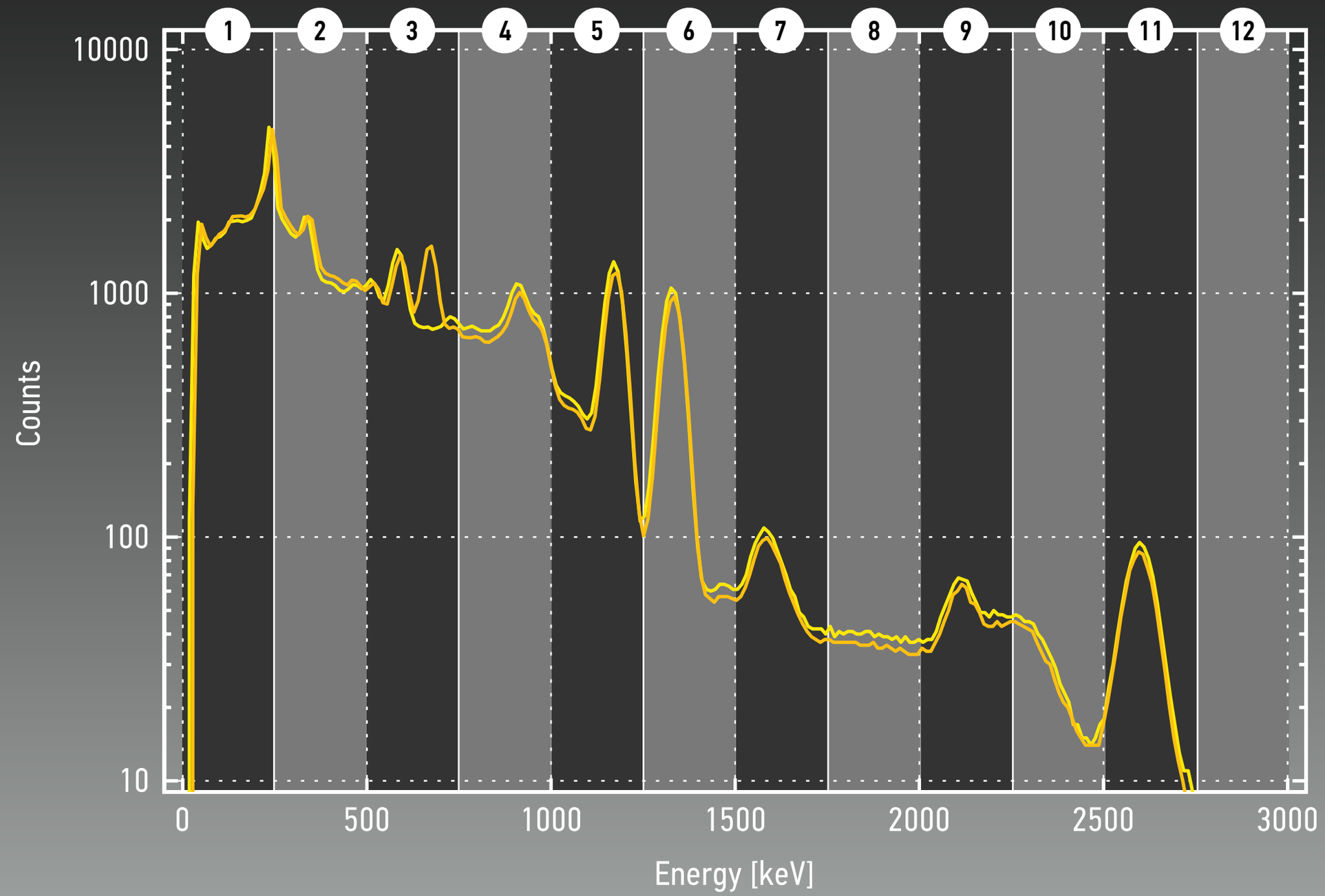
COMPARING TWO RADIATION SPECTRA

(AND DISTINGUISHING A “VALID” ITEM FROM AN “INVALID” ONE)



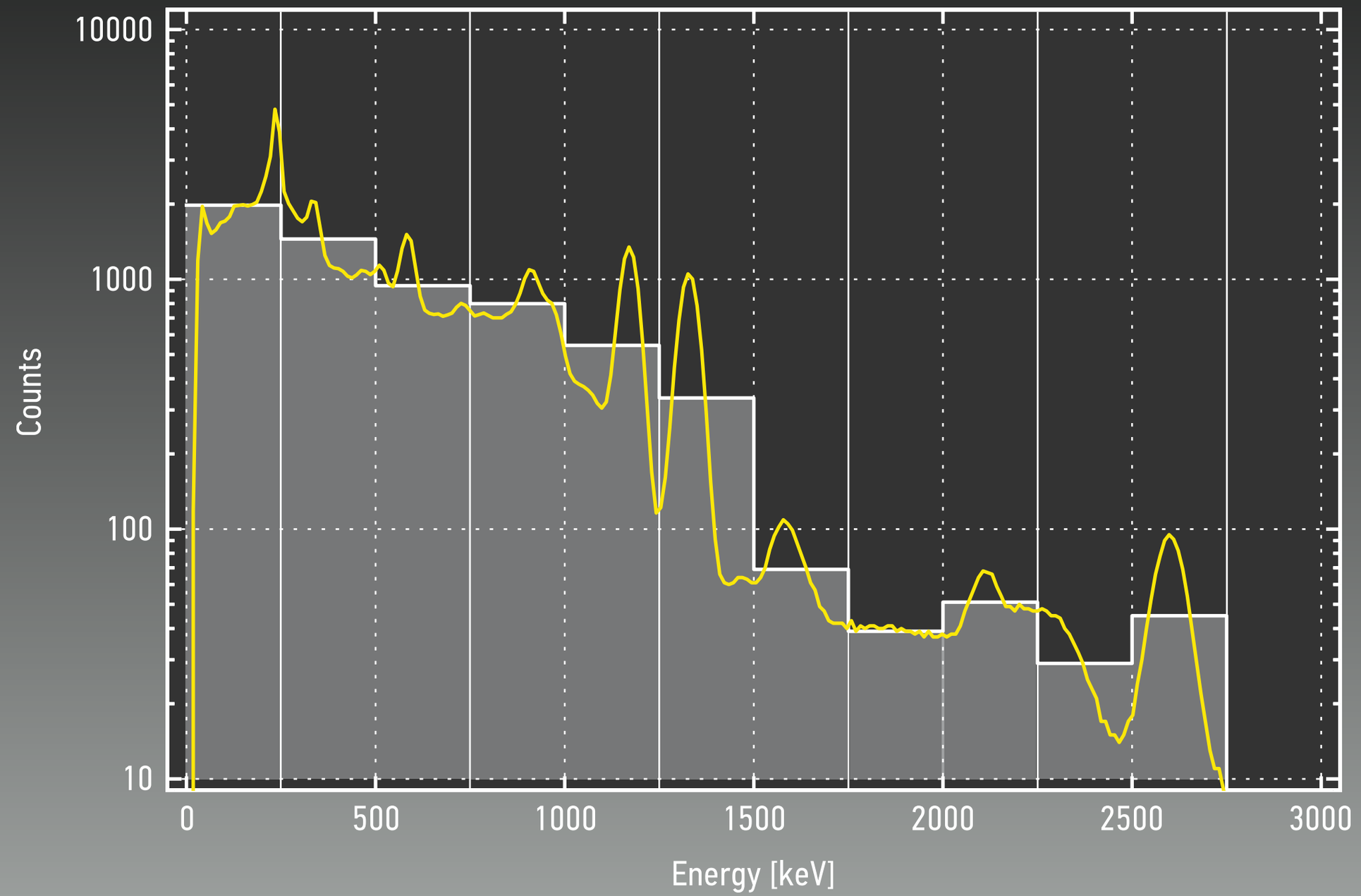
COMPARING TWO RADIATION SPECTRA

(SIMPLIFYING THE PROBLEM BY INTRODUCING A SMALL NUMBER OF BINS)



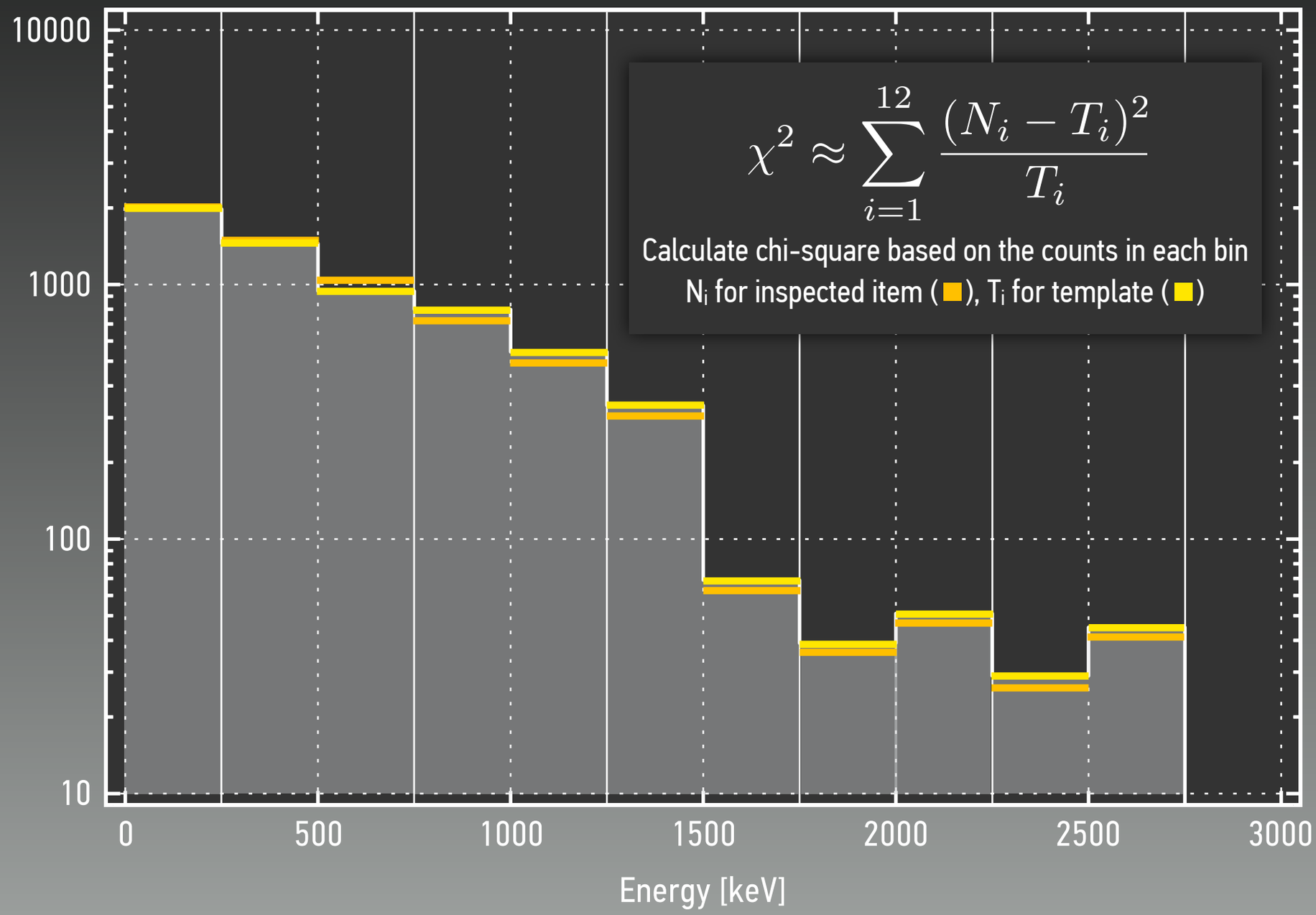
COMPARING TWO RADIATION SPECTRA

BASED ON EXTREMELY SIMPLE (12-NUMBER) FINGERPRINT



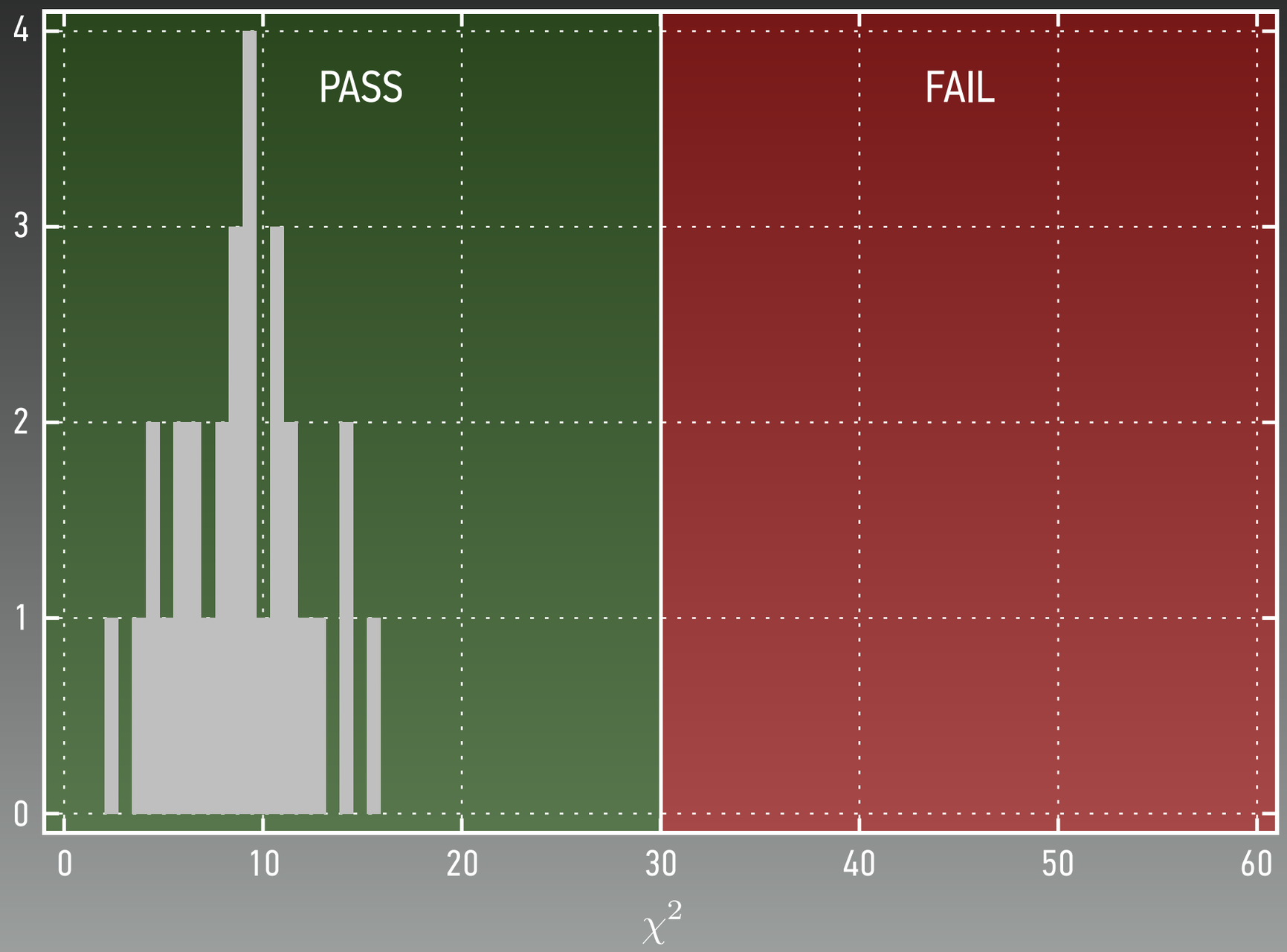
COMPARING TWO RADIATION SPECTRA

USING A STANDARD STATISTICAL HYPOTHESIS TEST



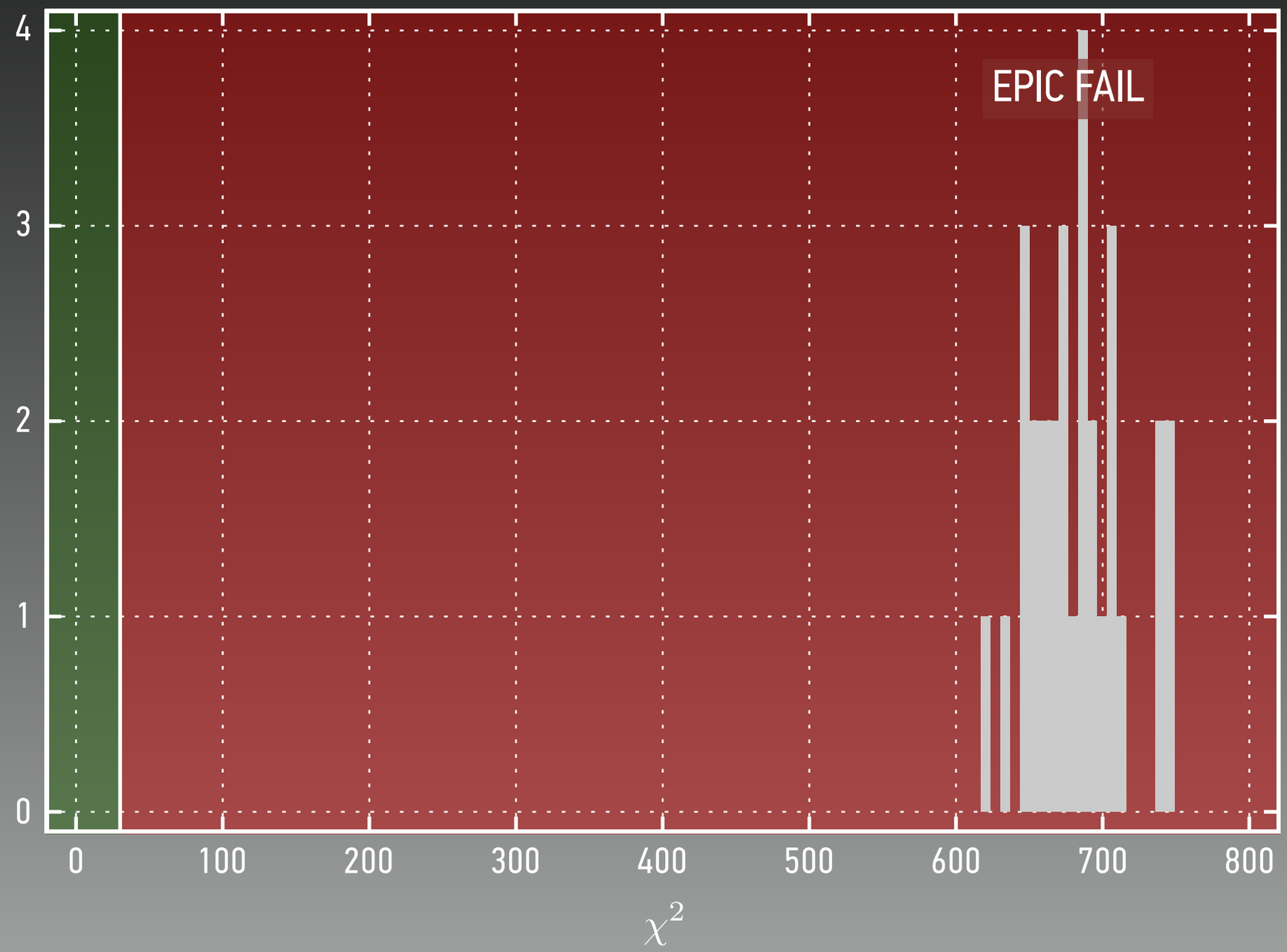
SCORING SIMILARITY

RESULTS FROM THIRTY INSPECTIONS OF A “VALID” ITEM



SCORING SIMILARITY

RESULTS FROM THIRTY INSPECTIONS OF AN “INVALID” ITEM



WHERE DO WE GO FROM HERE?

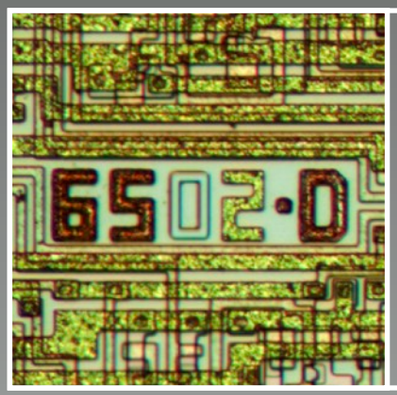
CAN WE TURN THIS INTO A VIABLE DEVICE FOR TRUSTED MEASUREMENTS?

REVISING IBX II SOFTWARE AND HARDWARE (EXPANSION CARDS)

Clean up Assembler code; add some extra functionalities to subtract background and correct for detector drift; replace high-voltage module with basic circuitry

PACKAGING THE EQUIPMENT

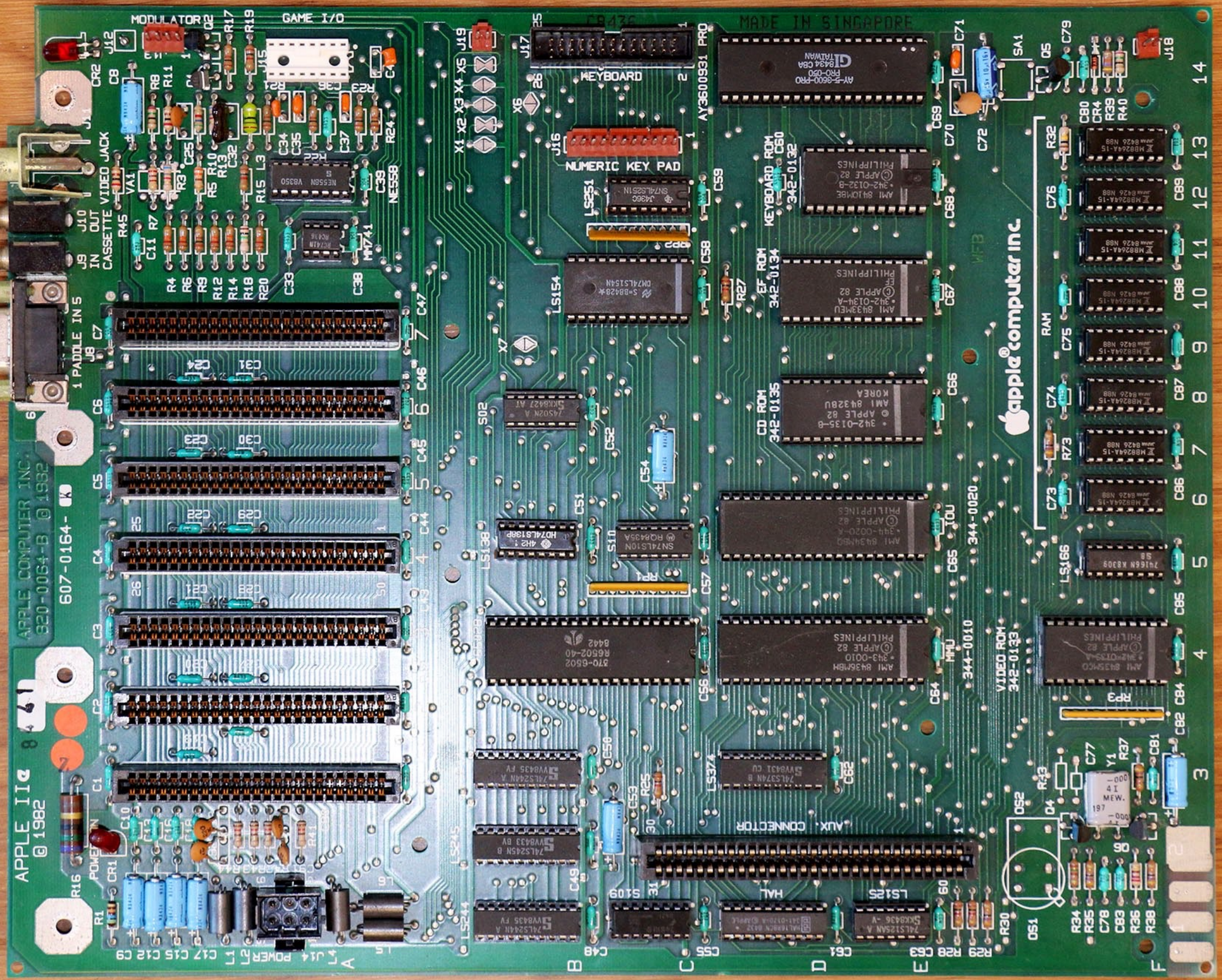
Examine viability of attacks on hardware and software; consider RF enclosure for device; Need for tamper-indicating features … or bring-your-own information barrier?



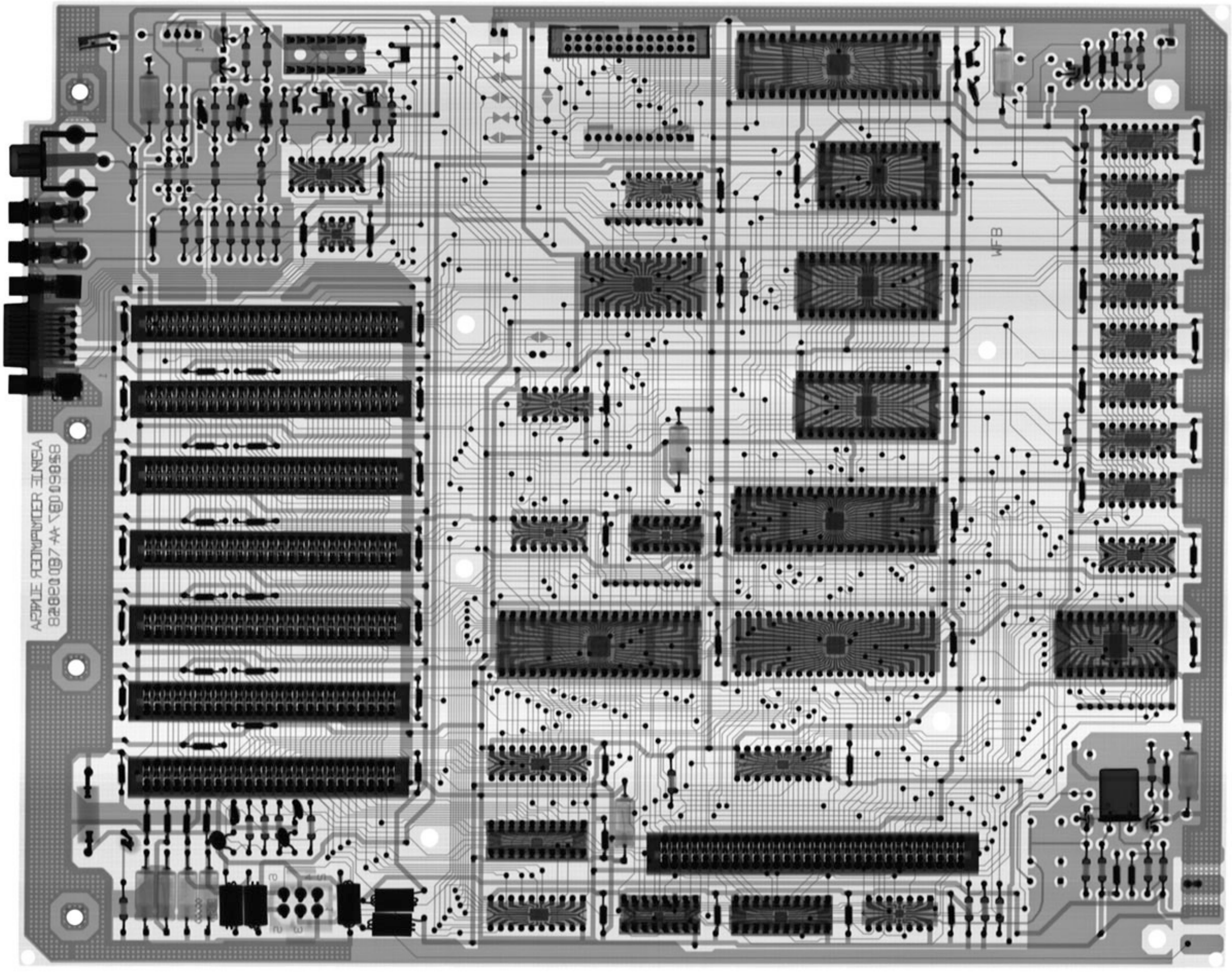
PROVING THAT THE HARDWARE (… and the 6502, in particular …) IS GENUINE

Explore ways to prove authenticity of hardware to address usual concerns about hidden switches, side channels, etc.; ideally, based on “physical” evidence

Source: www.ramayes.com (middle), visual6502.org (bottom)

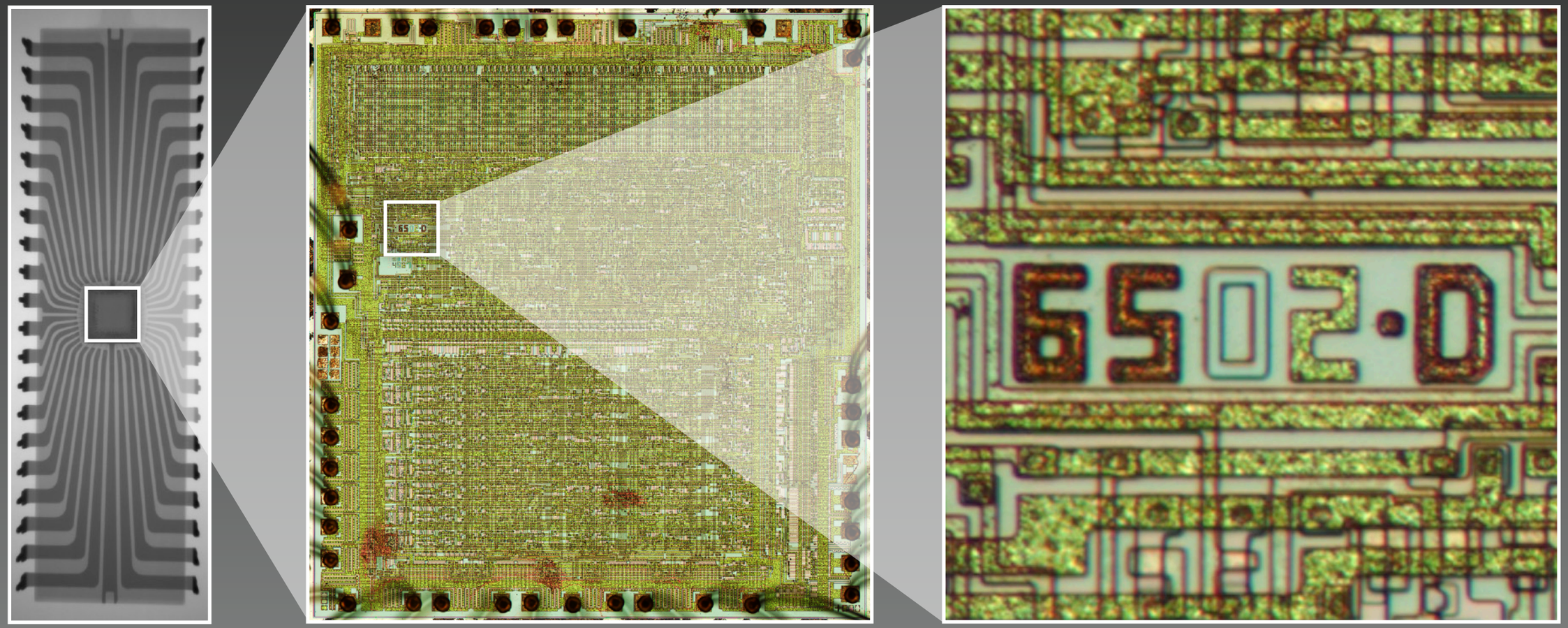


Source: Authors



Source: www.apple2scans.net

“IMAGING THE DIE”



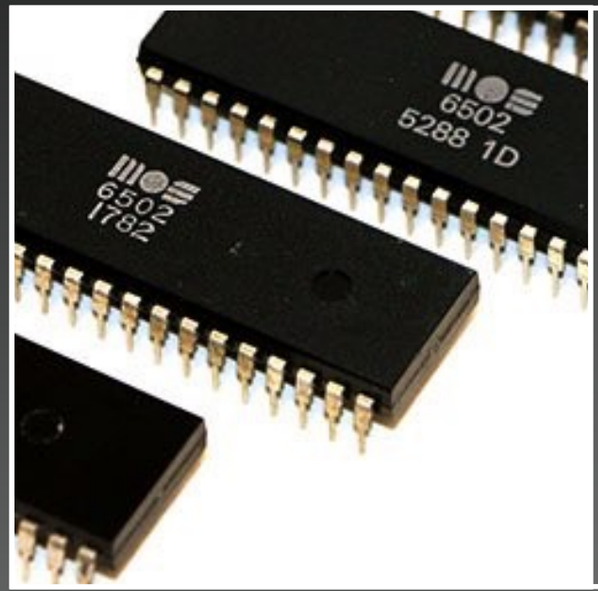
X-ray by Jeung Hun Park

Optical microscopy images by visual6502.org

Can one get similar results with (non-destructive) high-resolution x-ray microscopy?

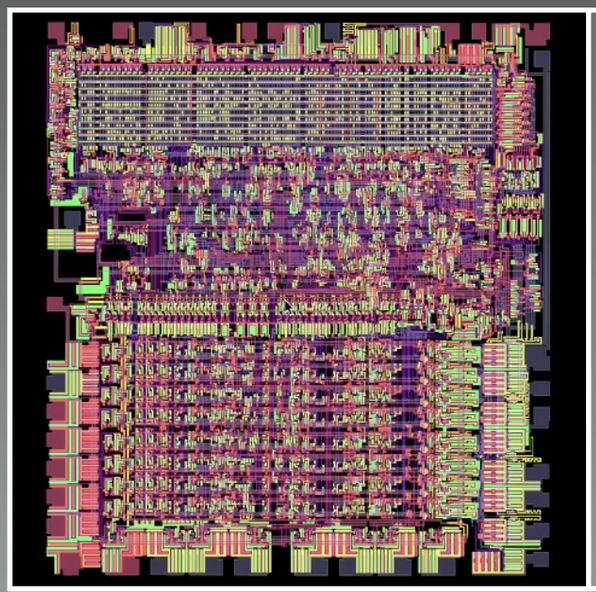
8 µm technology (8000 nm versus 14 nm), about 600-times larger than modern manufacturing processes
3500 transistors in 6502 versus up to a billion transistors in modern chips

HOW DO WE KNOW THAT A PARTICULAR 6502 IS GENUINE?



SEVERAL POSSIBLE OPTIONS … NEED ONLY ONE TO WORK

- Non-destructive imaging of die (high-resolution x-ray microscopy)?
- Age-dating of chip or package using forensic techniques?
- Proof of provenance?
- Logic testing of circuit to confirm original 6502 architecture?



LEVERAGING THE DEEP UNDERSTANDING OF THE 6502 ?

Visual6502.org: Transistor-level simulation of the 6502

Monster6502.com: Transistor-scale replica of the 6502

Can these and other resources be used to develop a test ?

www.visual6502.org/JSSim/index.html

Source: Authors (top) and Visual6502.org (bottom)

Nuclear Weapons

We built them.
We can take them apart.

@NuclearAnthro

vintageverification.org

github.com/nuclearfutureslab