



Verifying Nuclear Disarmament

An Overview of the Global Zero Nuclear Warhead Verification Project

Alexander Glaser

Department of Mechanical and Aerospace Engineering
and Woodrow Wilson School of Public and International Affairs
Princeton University

Symposium on Arms Control Verification Techniques
Mianyang, Sichuan, China
May 27, 2014

© Paul Shambroom

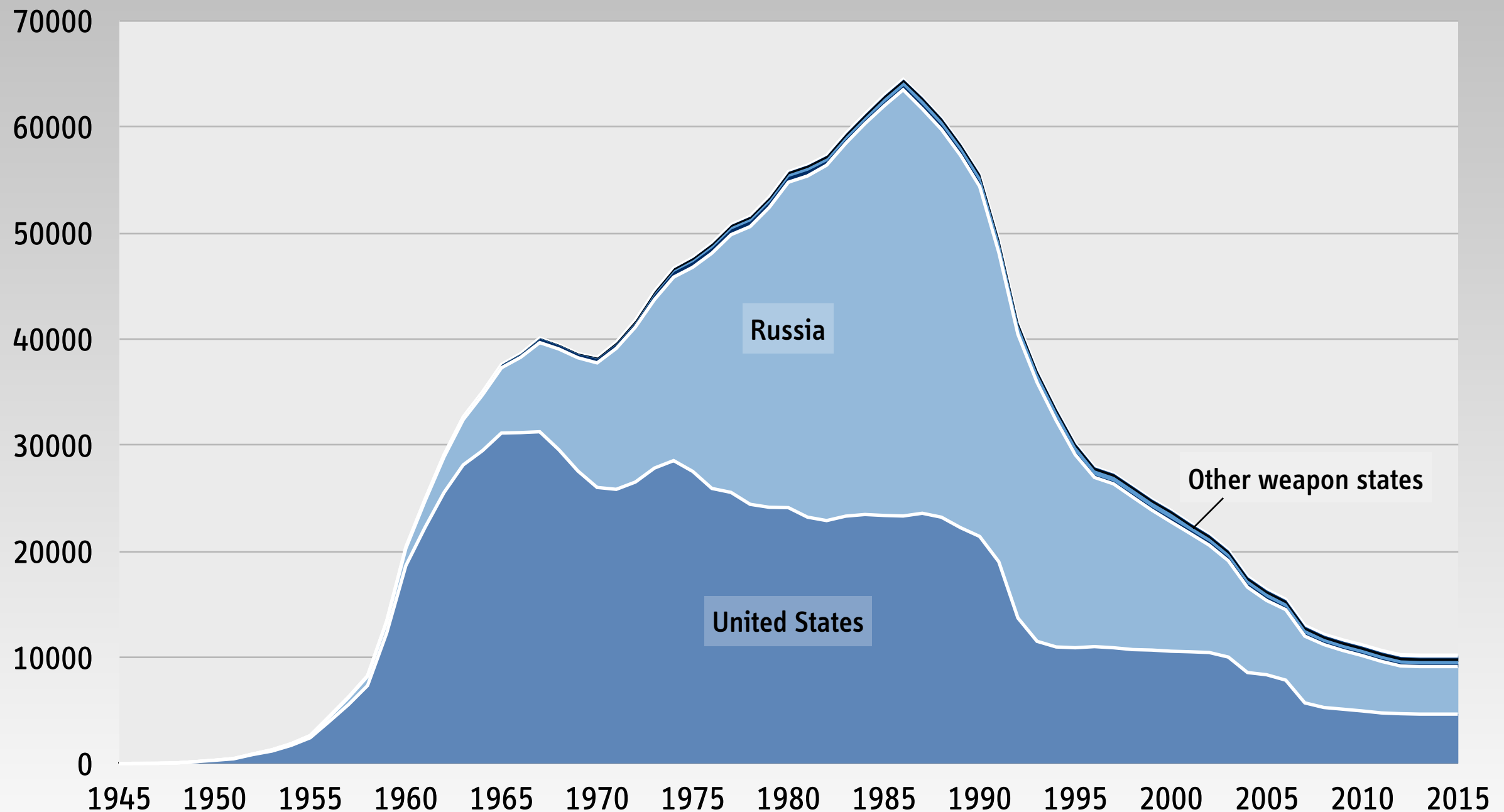
Revision 2

Background

*Nuclear Weapons After the Cold War
and the Challenge of Verifying Nuclear Disarmament*

Global Nuclear Weapons Stockpile

from 1945 to 2013, does not include several thousand warheads in dismantlement queue



H. M. Kristensen and R. S. Norris, "Nuclear Weapons Inventories, 1945–2013," *Bulletin of the Atomic Scientists*, 69, 2013, pp. 75–81

Going “Beyond New START”

“While the New START treaty is an important step forward, it is just one step on a longer journey. As I said last year in Prague, this treaty will set the stage for further cuts. And going forward, we hope to pursue discussions with Russia on reducing both our strategic and tactical weapons, including non-deployed weapons.”

U.S. President Obama, upon signing the New START Treaty, April 2010

Thousands of Nuclear Weapons Are No Longer Deployed and Currently In Storage



W87/Mk-21 Reentry Vehicles in storage, Warren Air Force Base, Cheyenne, Wyoming
Photo courtesy of Paul Shambroom, www.paulshambroom.com

The Challenges of Nuclear Disarmament Verification

Main Cheating Scenarios and Associated Verification Challenges

1

Party offers hoax or tampered devices instead of authentic treaty accountable items (TAI) so that real warheads, warhead components, or fissile material can be “diverted” to a secret stockpile of nuclear weapons

⇒ Verifying the authenticity of nuclear warheads (prior to dismantlement)

2

Party provides incomplete baseline declarations so that some treaty accountable items (e.g. warheads) are never part of the verification regime

⇒ Verifying the completeness of declarations

3

Party has undeclared fissile material production capacities, which are used to supply material for new weapons, e.g. to replace dismantled TAI

⇒ Verifying the non-production of new fissile material for weapons


(Same challenge for NPT and FMCT)

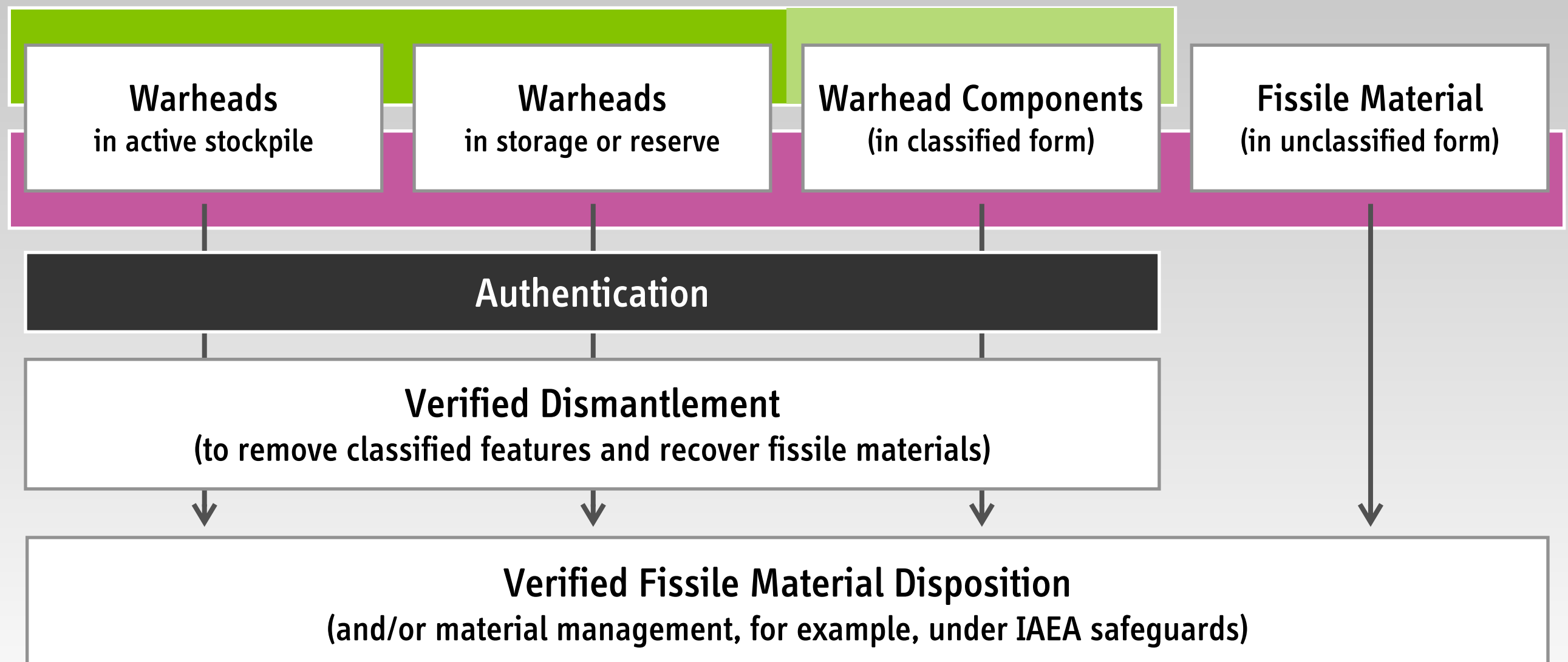
Verified Warhead Dismantlement

and the Challenge of Warhead Authentication

Where Does Warhead Authentication Fit In?

 **Nuclear Warhead Baseline Declarations**
(may or may not include information on warhead components)

 **Fissile Material Baseline Declarations**
(may include material in warheads implicitly or explicitly)

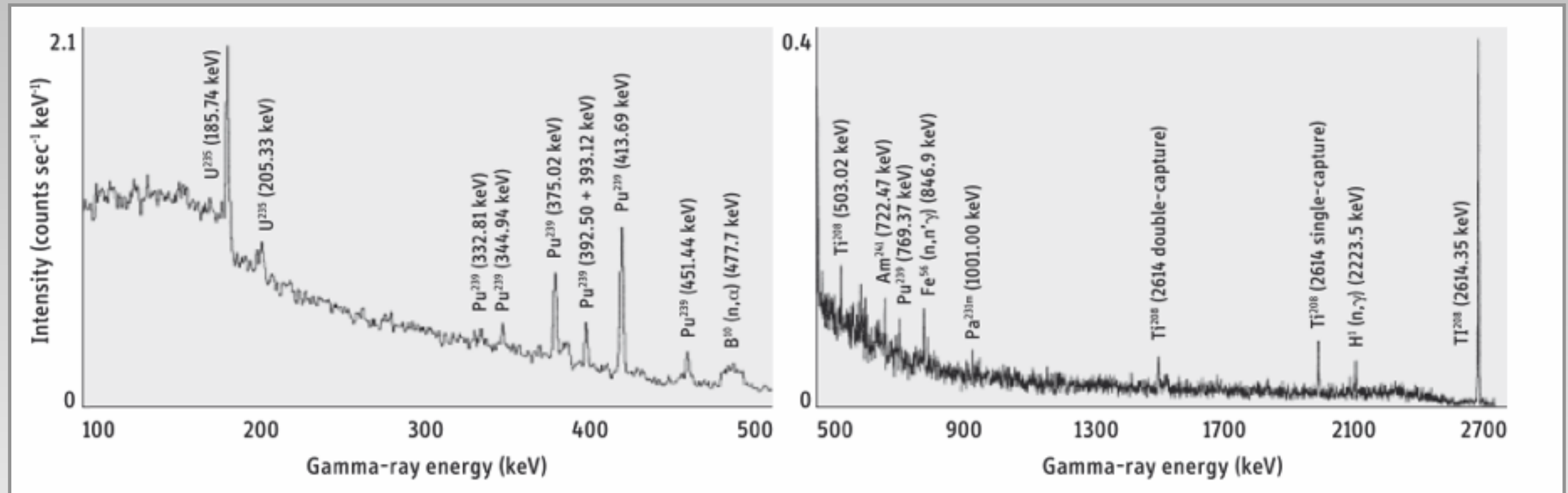


Verified Warhead Dismantlement

(Brief Background and Terminology)

Nuclear Warheads Have Unique Signatures

(but most of them are sensitive and cannot be revealed)

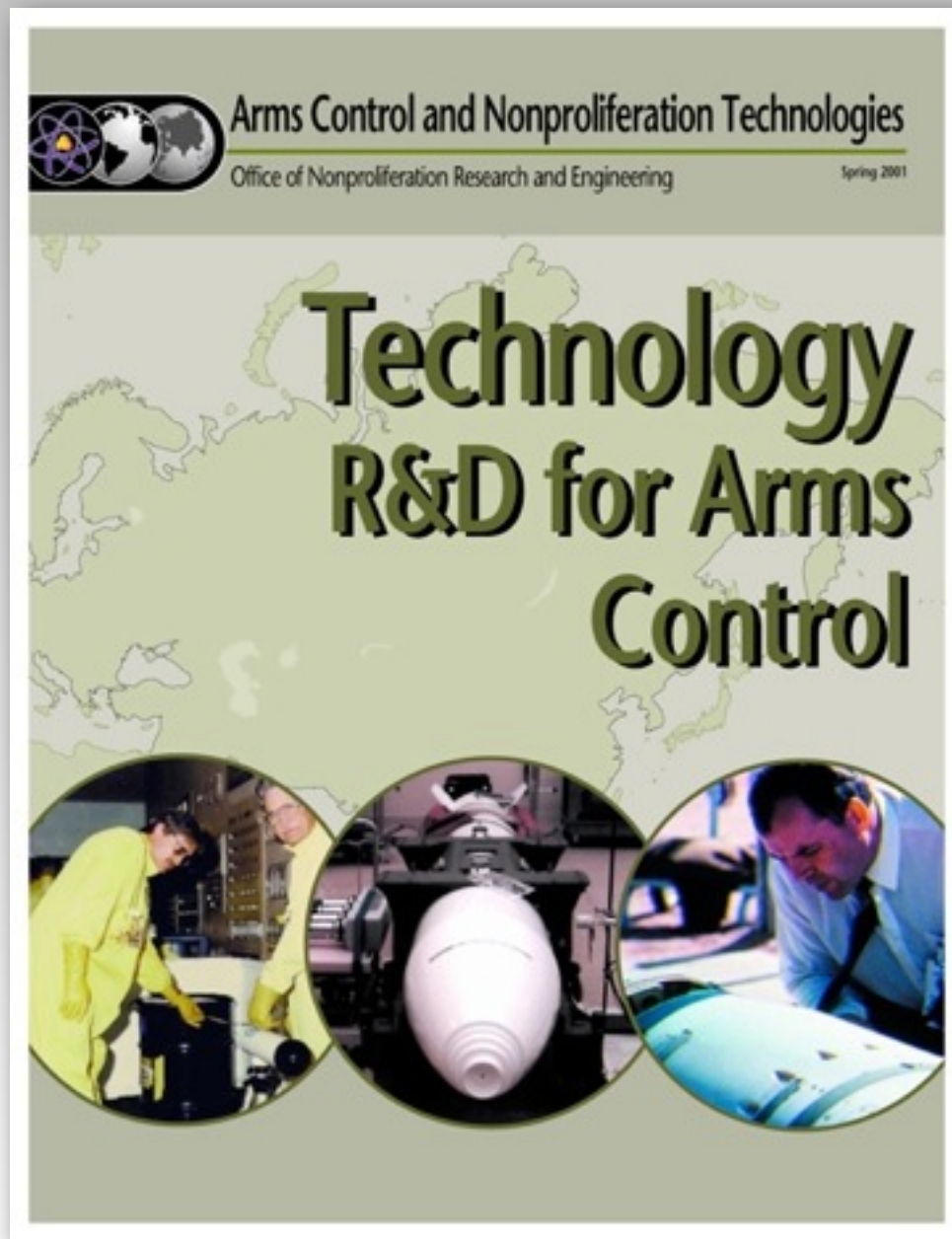


Gamma radiation spectrum from a Soviet warhead measured in 1989

Steve Fetter, Thomas B. Cochran, Lee Grodzins, Harvey L. Lynch and Martin S. Zucker

“Measurements of Gamma Rays from a Soviet Cruise Missile,” *Science*, Vol. 248, 18 May 1990, pp. 828–834

Inspection Systems for Nuclear Warhead Verification Have Been Under Development Since the 1990s



edited by David 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 Barrier

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

Requirements for an Inspection System

Information Security (Certification)

Assuring the host that the system does not divulge information that would be considered proliferation-sensitive or be otherwise classified

Information Integrity (Authentication)

Assuring the inspecting party that the instrument works as designed and that the data collected and displayed during the inspection are genuine measurements

Completeness and Soundness of Approach

If a valid item is presented, then the item is accepted with high probability
If an invalid item is presented, then the item is rejected with high probability
(in spite of elaborate deception efforts that the host might undertake)

Warhead Dismantlement Verification

Some Precedents Exist and Future Work Can Build on Them



Inspection System developed as part of the 1996–2002 Trilateral Initiative during a demonstration at Sarov
Source: Tom Shea



Visual contact with a mockup nuclear weapon during a UK-Norway Initiative Dismantlement Exercise
Source: UK Norway Initiative, David Keir

Why Is It So Hard?

“The Information Barrier Dilemma”

Joint Development + Minimum Complexity



UK-Norway Initiative, 2nd Prototype Information Barrier

David Chambers et al., "UK-Norway Initiative: Research into Information Barriers to Allow Warhead Attribute Verification Without Release of Sensitive or Proliferative Information," INMM 51st Annual Meeting, Baltimore, MD, USA, July 11-15, 2010

Can You Trust This Chip?



Hardware Trojans

Malicious changes or additions to an integrated circuit that add or remove functionalities or reduce the reliability of the system

G, Becker, Intentional and Unintentional Side-Channels in Embedded Systems
PhD dissertation University of Massachusetts Amherst, February 2014

Insertion is possible in every stage of the product cycle

For example, during design, manufacturing, assembly, and shipping (supply-chain)

Hardware Verification Challenges

From High-Level Functions to Transistor-Level Design

Does the hardware meet the design specifications?
Does it perform as intended?

Below Transistor Level ... Terra Incognita

So far no solutions

Becker et al., “Stealthy Dopant-Level Hardware Trojans,” 2013

Reproducibility is Difficult

Trojan can be triggered by aging mechanisms or environmental conditions
Extremely hard for inspector to reproduce

One (Big) Issue Remains

Post-Measurement Inspection of Equipment Are Typically Not Allowed

“After all these years, no one has yet demonstrated either an attribute or template type system using a classified test object in such a way that specialists from the inspecting country can then [i.e., after the measurement] thoroughly examine and proof the measurement equipment.”

James Fuller, October 2012

Is There a Way Out?

(We are pursuing two separate strategies)

Non-Electronic Detectors

Super-heated emulsions (bubble detectors) and neutron activation analysis



Detectors with different neutron-energy thresholds are available
(no cutoff, 500 keV, 1 MeV, 10 MeV)

Special features: pre-loadable (neutron counts), insensitive to gammas

Princeton Global Zero Verification Project

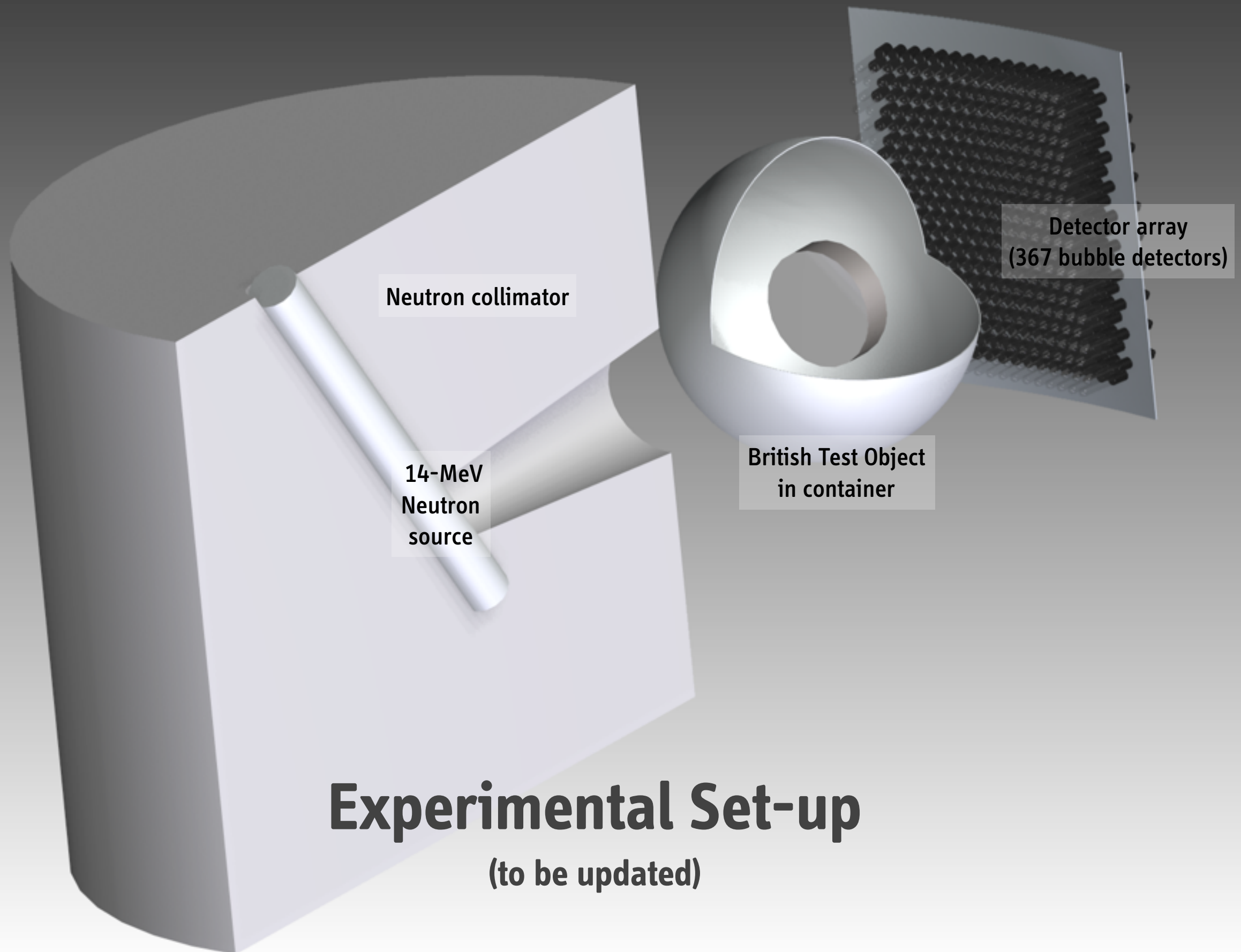
Princeton Global Zero Verification Project



GENERAL APPROACH

- Use 14.1-MeV neutron source (10^8 n/s) available at PPPL
- Use unclassified test objects that do not contain fissile materials (tungsten, lead, depleted uranium, ...)
- Template approach, non-electronic detectors
- Validate conceptual approach with simulated data

Project currently funded by Global Zero (www.globalzero.org) and U.S. Department of State
and previously supported by PPPL Proposal Development Funds



Experimental Set-up

(to be updated)

How Do We Prevent Sensitive Information from Being Detected?

(Physical Implementation of a Zero-knowledge Protocol)

“Number of Marbles in a Cup”

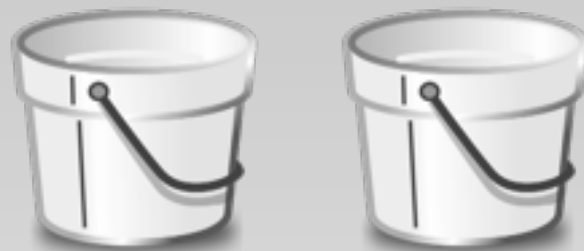


Alice has two small cups each containing the same number of marbles. She wants to prove to Bob that both cups contain the same number of marbles without revealing to him what this number is.

“Number of Marbles in a Cup”

1

*Alice claims that
two cups contain the same
number of marbles*

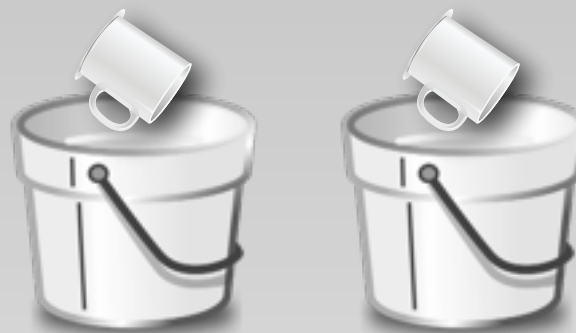


*She then also offers
two buckets of marbles*

*She claims these buckets also contain
an identical number of marbles*

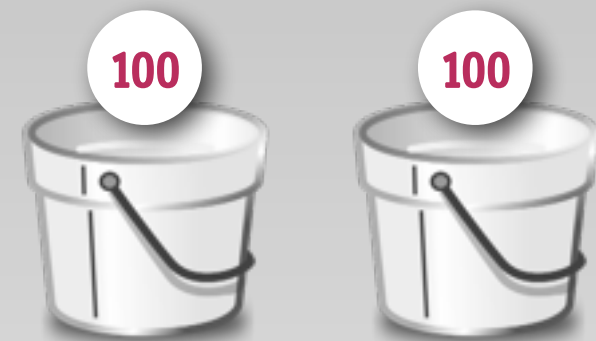
2

*Bob chooses randomly
into which bucket
which cup is poured
(L,L) and (R,R) or (L,R) and (R,L)*



3

*Bob now counts the
marbles in each bucket
and should find the same
number in both*



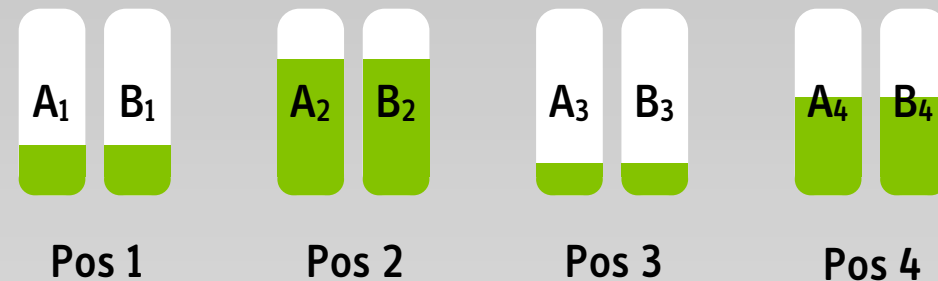
*50% confidence after 1st game
75% confidence after 2nd game
95% confidence after 5th game*

Proposed “Hardware Implementation” of a Zero-Knowledge Protocol for Warhead Verification

“The neutron count obtained by any measurement on the template or on a valid item is distributed according to the Poisson distribution with mean and variance to a previously agreed upon value $N(\max)$ ”

Since the host knows the “secret” (i.e., the design of the warhead), she can individually preload pairs of detectors for every orientation/direction so that they will be “topped up” to N_{\max} during the measurement

Before measurement

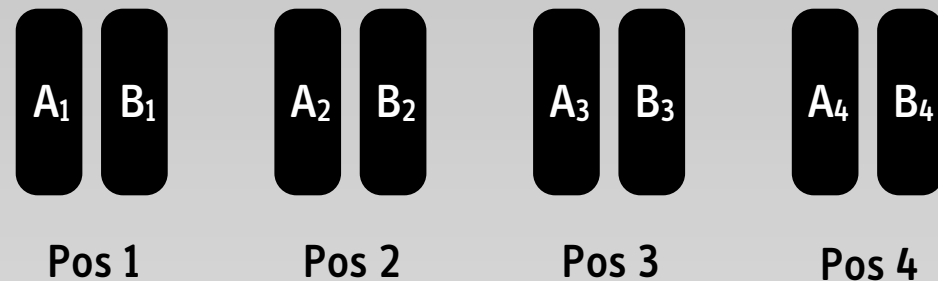


Proposed “Hardware Implementation” of a Zero-Knowledge Protocol for Warhead Verification

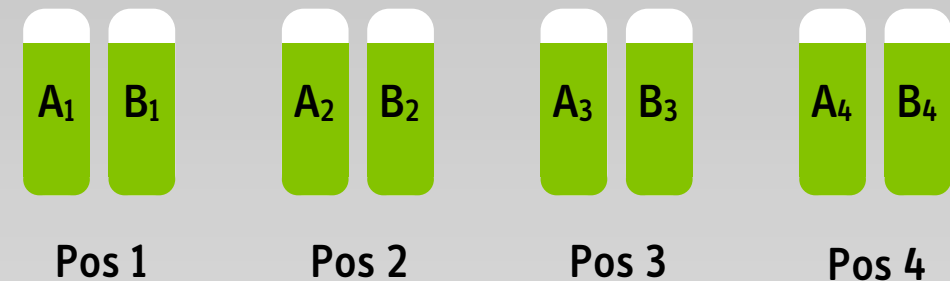
“The neutron count obtained by any measurement on the template or on a valid item is distributed according to the Poisson distribution with mean and variance to a previously agreed upon value $N(\max)$ ”

Since the host knows the “secret” (i.e., the design of the warhead), she can individually preload pairs of detectors for every orientation/direction so that they will be “topped up” to N_{\max} during the measurement

Before measurement



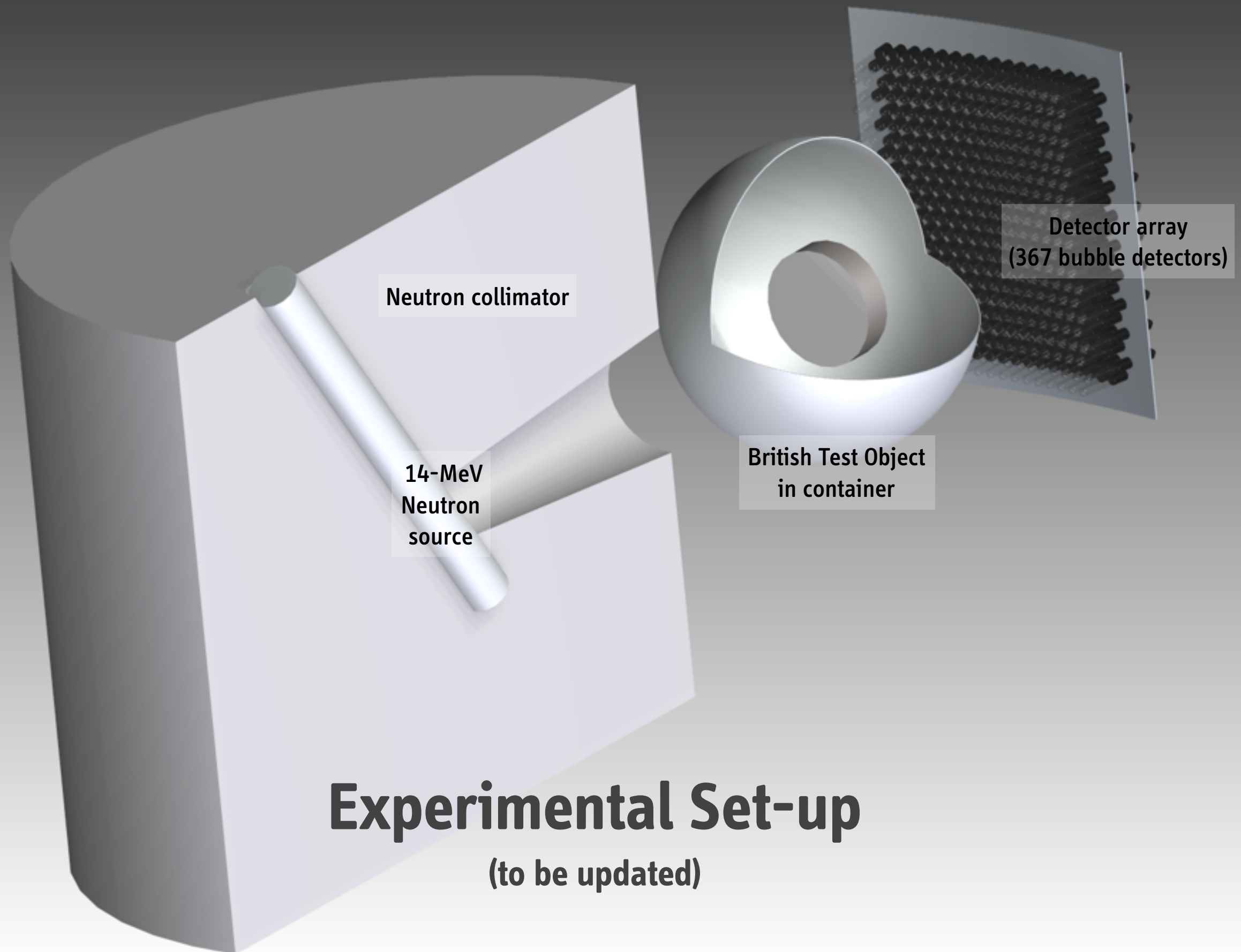
After measurement



Preload is unknown to inspector, i.e., bubble detectors are “wrapped in black tape”

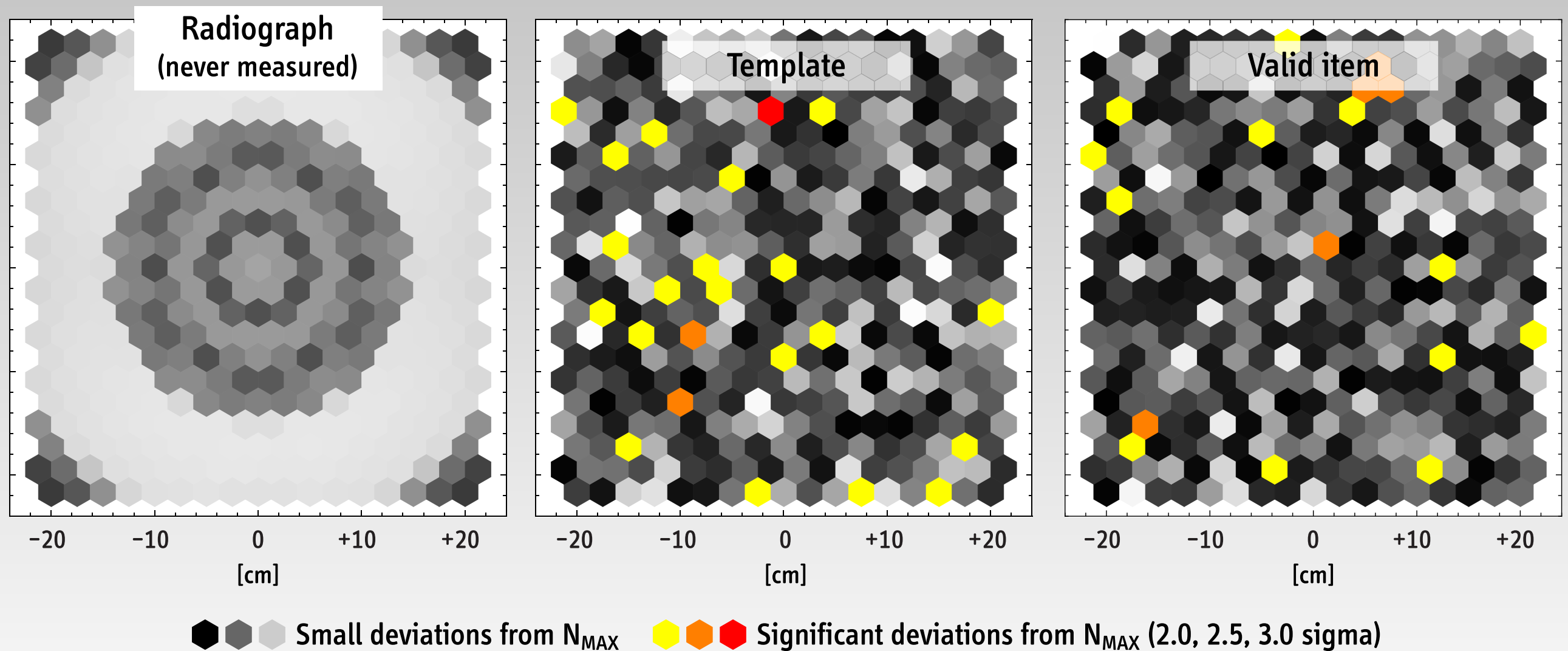
For every position, inspector chooses, which detector (A_i, B_i) to use on golden warhead or on test item
(so that it becomes impossible for the host to conceal a spoof by unequally initializing the detectors)

*Results of Monte Carlo
Neutron Transport Simulations*



Inspecting a Valid Item

(Top View of BT0)

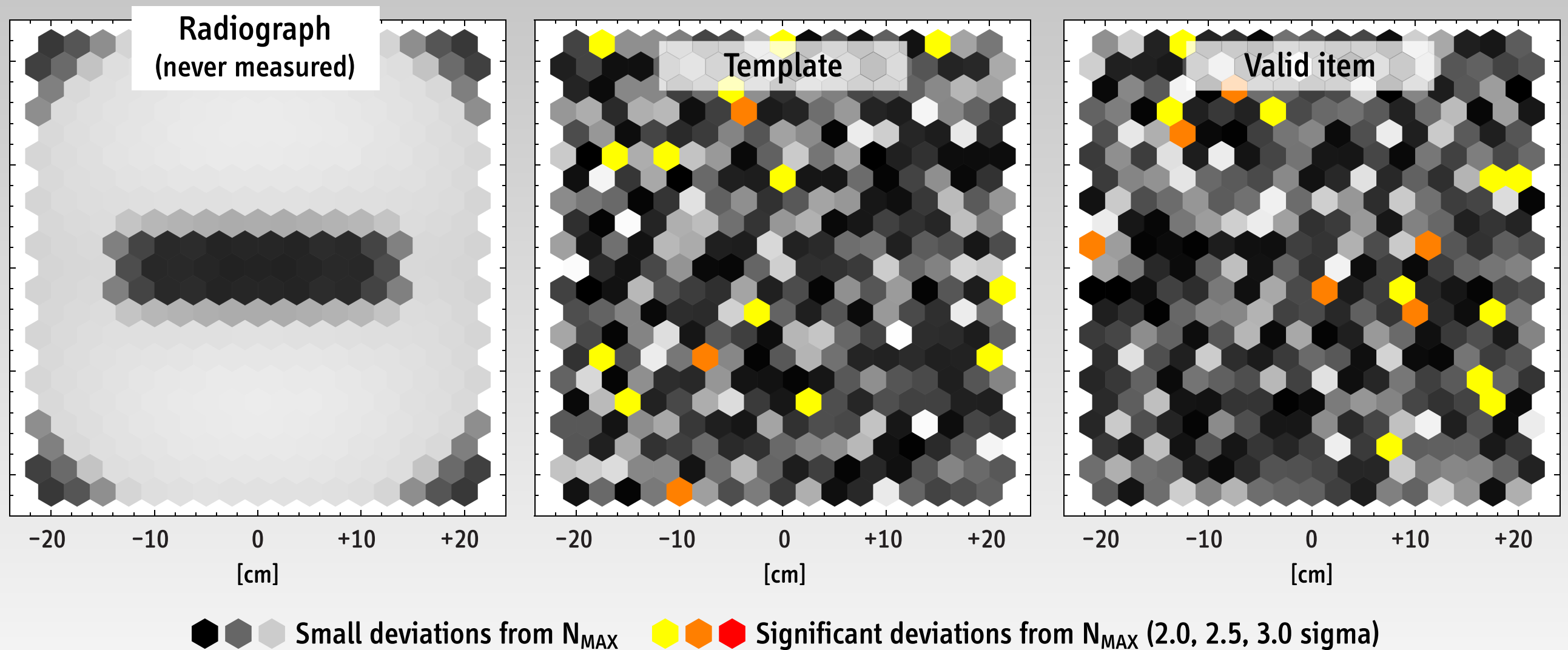


Simulated data from MCNP5 calculations, neutron energies > 10 MeV, $N(\max) = 5,000$

Glaser, Barak, and Goldston, *Nature*, forthcoming (June 2014)

Inspecting a Valid Item

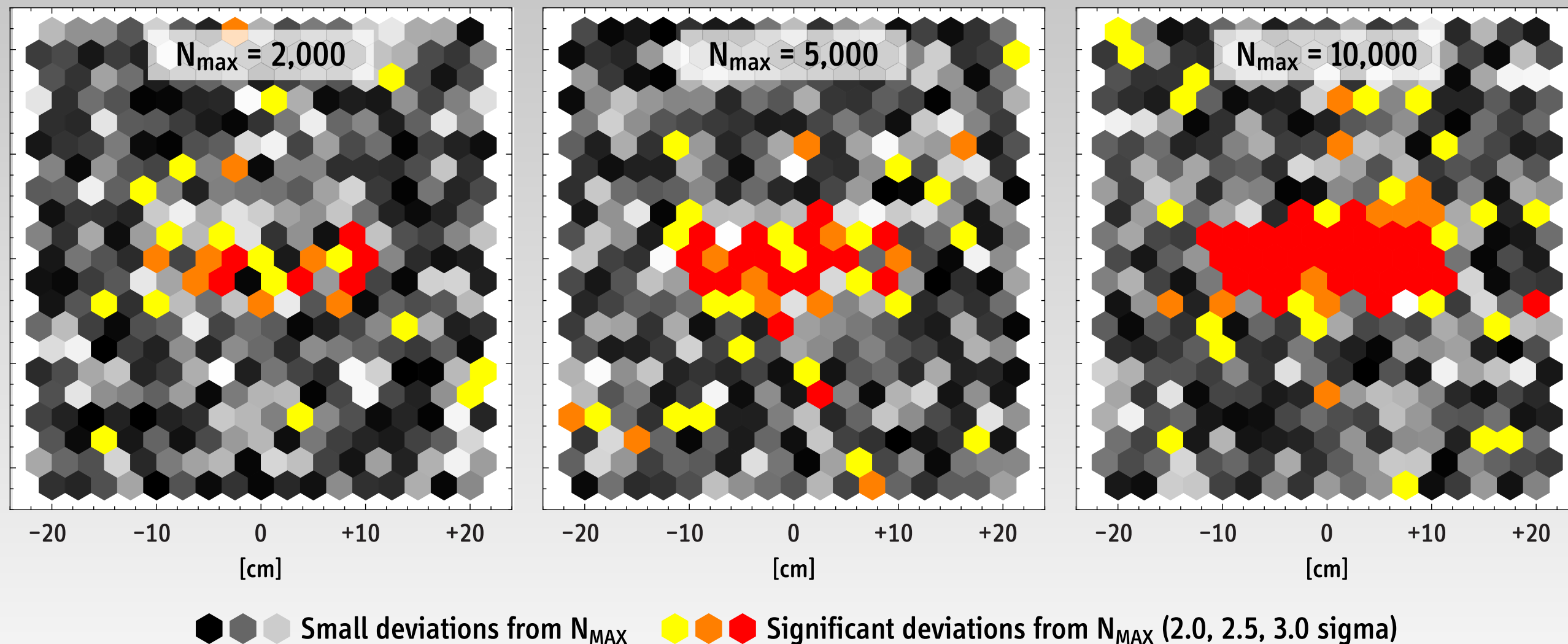
(Side View of BT0)



Simulated data from MCNP5 calculations, neutron energies > 10 MeV, $N(max) = 5,000$
Glaser, Barak, and Goldston, *Nature*, forthcoming (June 2014)

Full Tungsten Substitution

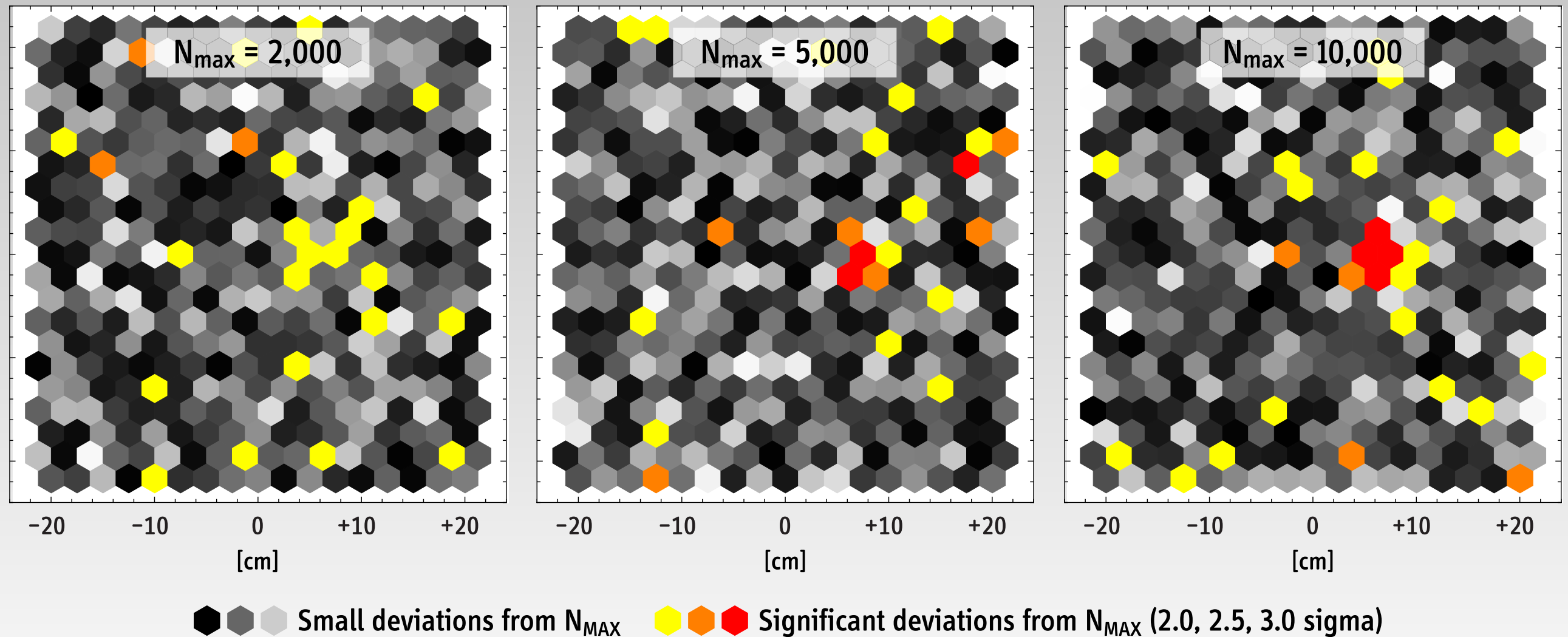
(Side View of BT0)



Tungsten is replaced by lead in both rings of the BT0; Simulated data from MCNP5 calculations, neutron energies > 10 MeV
Glaser, Barak, and Goldston, *Nature*, forthcoming (June 2014)

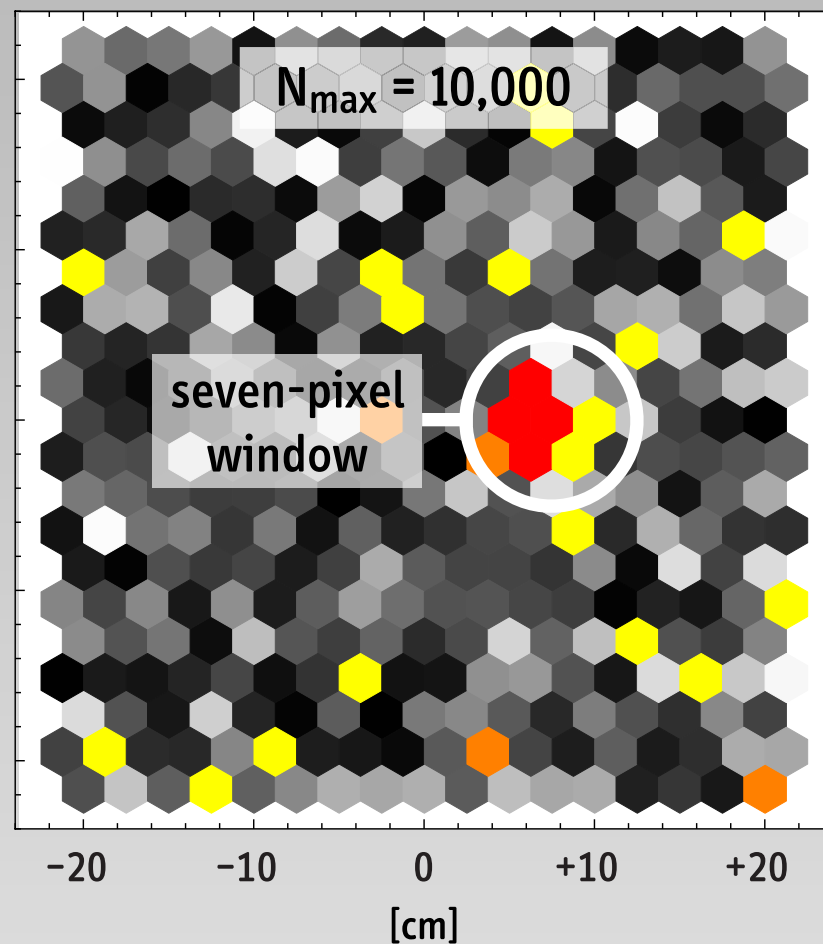
Local Tungsten Removal

(Side View of BT0)



543 grams of tungsten removed from outer ring of BT0; Simulated data from MCNP5 calculations, neutron energies > 10 MeV
Glaser, Barak, and Goldston, *Nature*, forthcoming (June 2014)

Decision Rule for Passed/Failed Test



BASIC STRATEGY

- Define 7-pixel windows, scan the board, and note the most “suspect” position (e.g., window is maximum standard deviations, X , away from mean)
- One can compute a threshold T such that k samples from a true normal distribution will exceed T only with probability $p = 0.05$
- Object fails test if $X > T$

For example, 295 samples from a standard normal distribution: 5% chance that one of the sampled values is $T = 3.76$ standard deviations away from mean

Probabilities for an Item to be Flagged as “Invalid”

N(max)	500	1,000	2,000	5,000	10,000	32,000
Valid item	$\leq 5\%$ (by design, in all cases)					
Full removal	$> 99.9\%$ (in call cases)					
Full substitution	77.7%	99.5%	$> 99.9\%$	$> 99.9\%$	$> 99.9\%$	$> 99.9\%$
Local removal	<i>undetectable</i>	15.7%	41.7%	94.6%	$> 99.9\%$	$> 99.9\%$
Local substitution	<i>undetectable</i>	<i>undetectable</i>	6.0%	11.7%	30.2%	95.5%

Way Forward and Next Steps

Way Forward and Next Steps

Achieving both information security and integrity is hard

Hardware (and software) verification is challenging

As a result non-electronic (pre-loadable) detectors are attractive

Zero-knowledge protocol reveals no information if host does not cheat

Experimental proof-of-concept is underway

