Disarmament Hacking 2.0:
Toward a Trusted, Open-Hardware Computing Platform for Nuclear Warhead Verification

Moritz Kütt, Malte Göttsche, Alex Gläser

Program on Science and Global Security
Princeton University, Princeton, NJ

ABSTRACT. Trusted inspection systems are critical for the verification of future arms-control treaties involving measurements on nuclear warheads or classified nuclear warhead components. Over the years, several research efforts have produced a number of prototype systems exploring a range of different technologies and conceptual approaches to accomplish this task. In general, these systems rely on unique hardware and software. In order to authenticate inspection systems, however, it would be beneficial to use a common, intensively tested hardware and software toolkit—possibly even use the same platform for different measurement types and verification tasks. Here, we propose and examine an inspection system based on a particularly versatile single-board computer, the *Red Pitaya* platform. As a case study, we build and test a prototype information barrier based on the template-matching approach using passive gamma spectroscopy. The *Red Pitaya* has very fast analog-to-digital conversion (ADC) capabilities combined with Field-Programmable Gate Array (FPGA) signal processing, which allows us to reduce the number of components between scintillator and spectrum output. Our results demonstrate that choosing common computing platforms may be possible and should help define the required specifications of such a platform for broad adoption.

Background

Making trusted measurements on nuclear warheads without revealing design information remains one of the major challenges for nuclear verification. Over the years, a number of prototype information barriers have been developed in the United States, as part of the UK-Norway Initiative, and for the Trilateral Initiative between Russia, the United States, and the IAEA. These devices display the results of a sensitive measurement in a simple pass/fail manner, and they have relied on a variety of measurement techniques and technology choices. So far, no common design approach has emerged among developers, impeding faster progress in this important area of research. In particular, as experts have previously argued, "we should work towards creating a more authenticatable, certifiable, and inspectable computer for arms control and nonproliferation regimes."[1]

In an effort to help overcome this shortcoming, we propose and assess the performance of a prototype *Information Barrier Experimental* (IBX) based on a particularly versatile single-board computer, the *Red Pitaya* platform. Our design approach minimizes the number of components required for the detector system. The short-term goal of this project is not to provide an inspection system that would be directly suitable for deployment in the field, i.e., for measurements on classified items in the presence of an inspecting party; instead, the main objective is to provide a basis for a low-cost prototyping platform that could be used by others for a variety of verification applications and therefore enable a cross-comparison of approaches and results.

Design Concept

The IBX uses low-resolution gamma spectrometry for possible nuclear verification applications. The device is based on the template-matching approach, in which the radiation signature from an inspected item is compared against a template from a trusted reference item. This section lays out the main hardware and software choices made for the original IBX prototype.

Hardware. The *Red Pitaya* is a small single-board computer with advanced signal processing capabilities;[2] it has been previously used for gamma spectrometry.[3] The *Red Pitaya* is based on the *Xilinx Zynq-7010* system-on-chip, which combines a dual-core ARM processor (Cortex-A9 at 866 MHz) with a Field Programmable Gate Array (Artix-7 FPGA). The system has 512 MB of memory and uses microSD cards for data storage. In addition to the main processor, the *Red Pitaya* also has a very fast analog-to-digital converter (ADC), which enables a sampling rate of 125 megasamples per second (Msps) with 14-bit resolution. Two voltage ranges can be selected for the ADC, either ± 1 V or ± 20 V, and the digital output of the ADC is written to the FPGA. In addition to the fast analog channels, the *Red Pitaya* also has sixteen digital general purpose input-output (GPIO) pins, eight additional (slow) analog input-output pins, and a variety of other interfaces (I^2C, SPI, USB). Although the original *Kickstarter* campaign to launch the project announced that the devices would be "open instruments for everyone," the hardware design is currently not entirely public. Not being open hardware, the *Red Pitaya* is considered an interim solution for the IBX.[4]

A second circuit board located next to the *Red Pitaya* (Figure 1) provides all other required functionalities. This two-layer board was developed specifically for the IBX, and the schematics and PCB designs are available in the IBX code repository.[5] Most importantly, the board provides high voltage for the photomultiplier and enables communication between the *Red Pitaya* and the front panel of the device. The high-voltage circuit is based on a compact high-voltage module from CAEN (7505P),[6] which can produce stable voltages up to 1600 V. It would be straightforward to replace the module
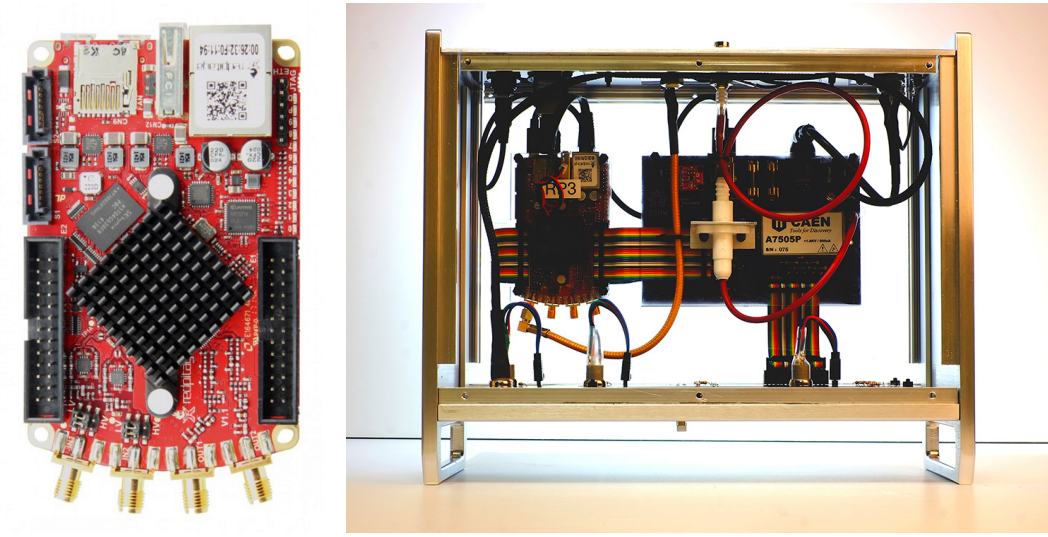
Figure 1: *Red Pitaya* (left) and top view of IBX (right).

in a future design, but the unit is a safe and reliable component for use in the experimental version of the IBX. The HV module is controlled using GPIO pins combined with a small digital-to-analog converter (MCP 4725), which regulates the voltage level supplied by the module. The voltage is continuously monitored using one of the analog input pins on the *Red Pitaya*, but adjustments are generally not necessary.

Software. The *Red Pitaya* runs a modified version of Debian Linux. Several FPGA modules are provided by the manufacturer to perform a number of basic tasks, and only these open-source modules are used for the IBX. In addition, we developed a small C++ program to handle the operation of the FPGA and to quickly transfer the data collected by the FPGA to the microSD card. Most of the additional data processing and analysis is based on *Python* scripts. This includes the information barrier logic, button and LED control, regulation of the high voltage, and calibration of the device. Also implemented in *Python* are the methods and algorithms used to compare radiation spectra from reference items (templates) to an inspected item. At this stage of development, the details of the chosen implementation are not particularly important; rather, the current implementation primarily serves to demonstrate the basic functionality of the prototype device. In fact, as further discussed below, the IBX can be used to develop, test, and validate a variety of algorithms and techniques. These could then also be implemented in other programming languages, such as C, C++, or specialized languages optimized for the development of high integrity software such as SPARK-Ada;[7] it would also be possible to reduce the complexity of the software stack by moving most (or all) of the functionality into the FPGA, which could simplify hardware and software authentication.[8]

3

Digital Data Acquisition Approach

Advanced digital-processing capabilities have recently enabled fully digital data acquisition techniques for many types of radiation measurements. Compared to traditional analog techniques, "the digital approach guarantees superior timing capabilities, while maintaining an adequate if not superior spectroscopic response."[9] In this approach, a fast digitizer converts an analog radiation-induced pulse directly into a digital number without requiring a pre-amplifier, amplifier, or pulse-shaping electronics. For the standard IBX configuration, we use a *Canberra* Model 802 NaI detector and photomultiplier,[10] connected to a Model 2007 Tube Base, which also provides power for the photomultiplier tube. For the acquisition of gamma spectra, the fast analog input of the *Red Pitaya* is directly connected to the anode of the photomultiplier tube. The internal resistance of the *Red Pitaya* port is 1 MΩ. An additional resistor of 2.5 kΩ is used to connect ground to signal for faster discharge of the charge collected at the anode. The size of this resistor has been optimized to balance pulse height and pulse length. With the present detector system, we obtain the minimum value of about -1000 mV for 3-MeV gammas and a pulse length of about 3μs. Figure 2 shows several hundred detection events acquired with this setup.
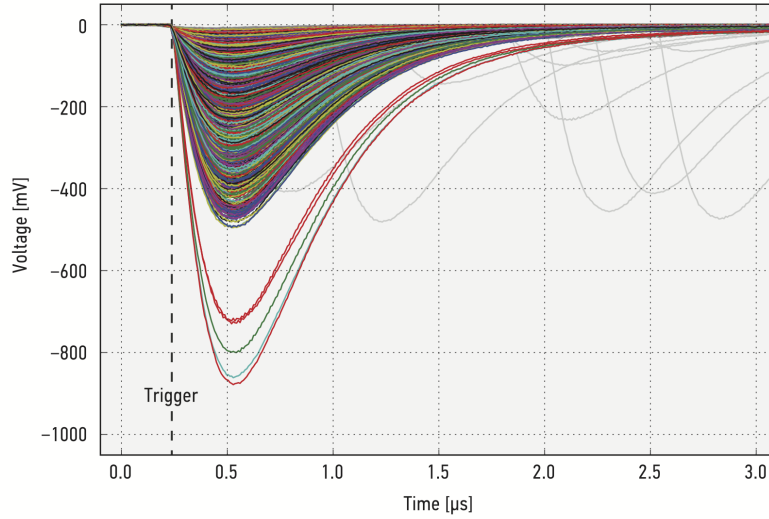

Figure 2: Voltage pulses measured by the *Red Pitaya* based on the charge collected from the anode of the photomultiplier tube after detection events in the scintillation detector. In order to determine the photon energy associated with a particular event, traces are integrated over a period of 3.0 μs to obtain a signal that is proportional to the collected charge. Pulses identified by the pile-up rejection algorithm are shown in gray.

4

Typical data acquisition rates observed in radiation measurements requires the use of the FPGA on the *Red Pitaya*. Data acquisition with 125 Msps and 14 bits per sample creates about 220 MB of raw data per second. Instead of storing the entire data stream, the IBX uses the oscilloscope module on the FPGA to selectively process data only when a pulse has been detected. The oscilloscope module continuously writes data to a ring buffer with a size of $2^{14} = 16{,}384$ samples. The module has a trigger function to check if incoming data exceeds a predefined value. Once this condition is met, the module triggers, while data acquisition continues for a specified number of additional samples to obtain about 3 μs of additional data for a total of 384 samples. The acquisition process is then stopped, and the position of the trigger event in the ring-buffer is returned so that the data can be read by the software running in the Linux environment. While the C++ code is reading the data, writing to the ring buffer is suspended to prevent interference with this process.[11] Once the readout is complete, the C++ software rearms the trigger, and the process starts over, i.e., the detector starts waiting for the next incoming pulse.

The probability of observing an additional event (following the initiating event) in a time interval Δt when the instruments detects an average of λ events per second is given by:

$$p = 1 - \exp(-\lambda \, \Delta t)$$

The probability for such a pile-up condition in a time period of 3 μs is 1% for a count rate of 3,350 cps and reaches 10% for about 35,100 cps. In both cases, a robust pile-up rejection method is desirable or needed. In the current implementation, pile-up rejection is ensured by comparing the negative pulse integral with the pulse minimum, which is reached about 0.30 μs after the pulse is triggered (Figure 2); if this ratio falls outside an expected bracket, the pulse is rejected, i.e., it is then safe to assume that more than one pulse is present. The highest count rates that are currently achievable with the IBX are on the order of 2900–3000 cps. This limit is primarily due to the time needed to write data to the microSD card, and significant improvements may be possible through software and process optimization.

For a basic performance assessment of the detector system, we have tested the IBX with a variety of calibration sources with gamma energies ranging from 200 keV to 2600 keV. In particular, Figure 3 shows the experimentally determined resolution of the system when operated with the Model 802 sodium-iodide detector. At 662 keV, the resolution is 6.0%. Overall, the resolution meets or exceeds values obtained with commercially available products or in similar experiments by other groups.[12] Further measurements and sample spectra are discussed further below.
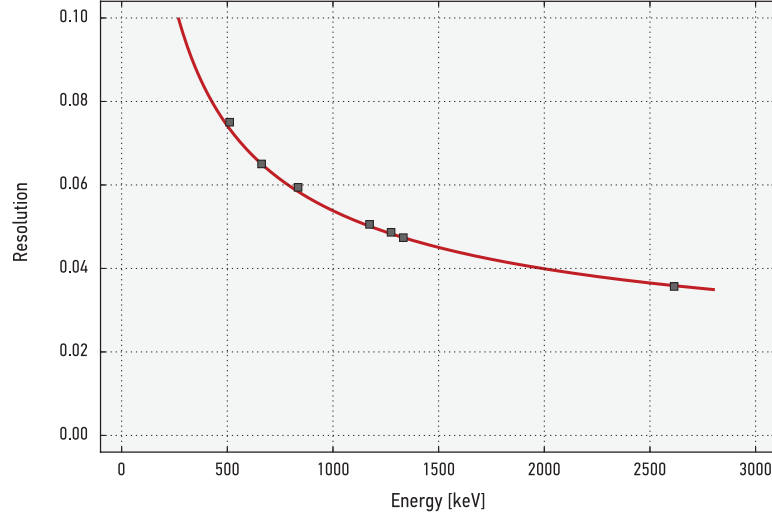
Figure 3: IBX Resolution when operated with a *Canberra* Model 802 sodium-iodide detector. As expected, resolution increases with $1/\sqrt{E}$. At 662 keV, the resolution is 6.0%, which is comparable to (or slightly better than) typical values achievable with this detector type.

IBX Mode of Operation

The front panel of the IBX (Figure 4) is divided into five segments, and a standard inspection proceeds from left to right. The POWER button on the leftmost panel powers up the IBX and automatically starts the control script. The READY LED indicates when the boot process is complete; during operation, this LED indicates whenever the device is ready for user interaction. Depending on the current status, the HIGH VOLTAGE button ramps up or down the high-voltage supply for the detector. The buttons on the other panels are inactive unless the high voltage is present and stable.

The second segment contains the CALIBRATE button. When pressed, a calibration measurement is initiated using the signal from a number of thoriated welding rods that are permanently placed around the detector head.[13] A simple algorithm identifies the centroids of two gamma peaks at 238.6 keV and 2614.5 keV from lead-212 and thallium-208, both decay products of thorium-208. This information is used to calibrate the IBX. A BUSY LED indicates that a calibration is underway; similar LEDs are also located on the next two panels (acquire and inspect) so that the user is aware at any time, which task is currently active.

6

Figure 4: Typical experimental setup with mockup warhead (left) and Information Barrier Experimental (IBX) during initialization sequence (right).

The center segment contains three `ACQUIRE` buttons that can be used to acquire up to three different templates, for example corresponding to three different warhead types. Recorded templates are indicated by the corresponding LED and remain active until they are deleted by a second button press. When the IBX starts up, the device checks for previously recorded templates and indicates their presence. This feature is convenient during development, but may be impractical in a true inspection setting. In the present implementation of the IBX software, the template consists of a gamma spectrum with 2500 1-keV bins, which can be used to perform a series of tests for comparison with another spectrum. For each measurement, the IBX also saves a complete list of individual pulse integrals to enable further analysis of the data and debugging of the device.

If at least one template is active, the `INSPECT` button in the fourth segment can be pressed to inspect an "unknown item" and automatically compare its signature to all active templates. The LEDs on the rightmost panel indicate, which template corresponds to the inspected item. Should an item pass the test for more than one template, the template with the highest similarity is considered the final match, and only the corresponding LED illuminates. The `NO MATCH` LED indicates if the inspected item does not correspond to any of the active templates.

IBX Proof of Concept

To determine the performance of the IBX in an inspection setting, we performed a series of measurements using standard calibration sources as reference and inspected items. These measurements and experimental data can be used to determine and optimize requirements for the inspection, such as the duration of a typical measurement, and

to develop and test basic algorithms for comparison of two radiation spectra, ideally without making any assumptions about their features.[14] Figure 5 shows two one-minute measurements for different configurations of two calibration sources: a simple cobalt-60 source serves as the reference item to record the template. The same source is then used to simulate inspections on a valid item. To simulate an invalid item, a weak cesium-137 source is placed nearby, adding about 7% to the total count rate.
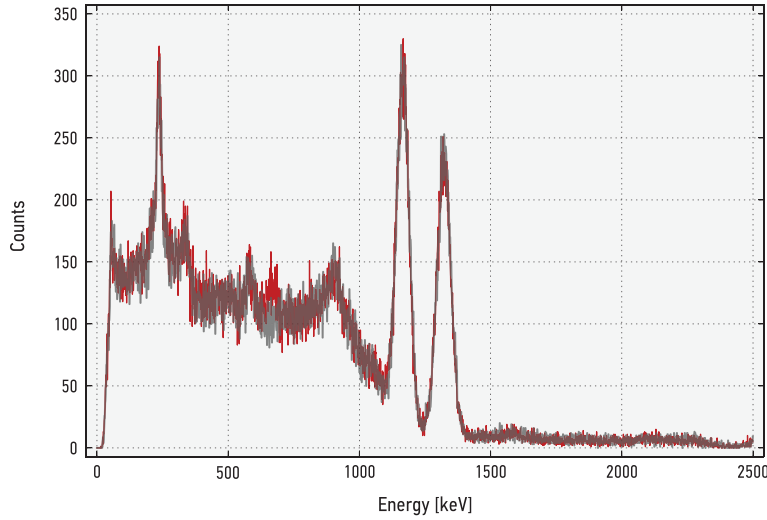

Figure 5: Two IBX spectra acquired in two separate one-minute measurements for a valid item (Co-60 calibration source) and for an invalid item (Co-60 source with weak Cs-137 contribution). As expected, dissimilarities are most significant near 662 keV. Both measurements were carried out with an unshielded detector.

As discussed elsewhere,[15] in the current implementation of the IBX software, gamma spectra are compared using a modified version of the Kolmogorov-Smirnov test, which calculates the maximum distance between the cumulative distribution functions of the two spectra and determines whether it is smaller or larger than a defined threshold D_T. In order to determine the reproducibility of results and the capability of detecting spectral differences, we carried out a series of measurements. Figure 6 summarizes the main results of one such campaign. Even for rather short one-minute measurements, each with about 175,000 counts, the Kolmogorov-Smirnov distances for valid and invalid items are significantly different. While the average value for valid items is $D_V \approx 0.004 \pm 0.003$, the respective value for the invalid item is $D_I = 0.016 \pm 0.003$. Under these conditions, the IBX reliably identifies valid items for a threshold value of $D_T = 0.010$.
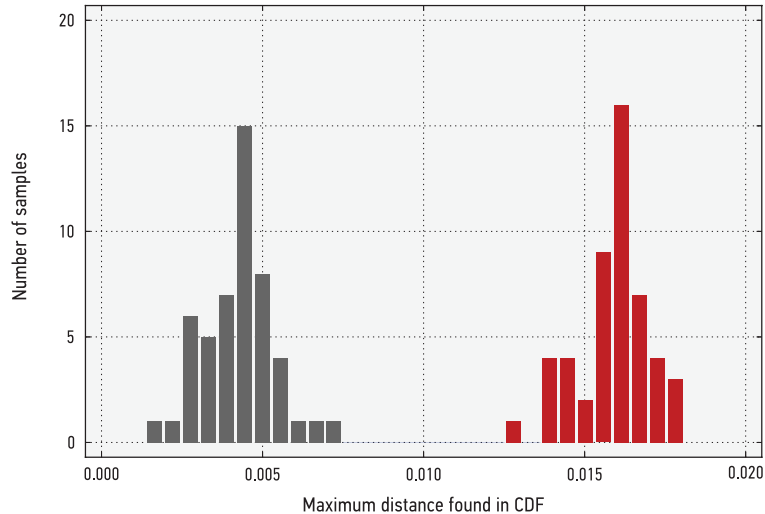
Figure 6: IBX Inspection. 50 one-minute measurements for a valid item (Co-60 calibration source) versus 50 one-minute measurements on an invalid item (Co-60 source with weak Cs-137 contribution). The analysis of each one-minute inspection is based on about 175,000 counts. Under these experimental conditions, the IBX reliably identifies valid items for a threshold value of $D_T = 0.010$.

Outlook

With this project, we have tried to demonstrate that existing or specially designed computing platforms with compact form factors may offer a path toward a common platform for a variety of applications in nuclear verification. The prototype information barrier is low cost, and its design is simple and transparent. At the same time, measurement results are very encouraging as we achieve excellent detector resolution and the capability to detect small differences in radiation spectra, demonstrating the basic viability of the approach.

Several future developments for the IBX are possible with the ultimate objective being a transition to a fully open platform. At present the software is open-source,[5] but the *Red Pitaya* and the high-voltage module are not. On the software level, other, more advanced algorithms could be explored. The current method is based on an empirical version of the Kolmogorov Smirnov test, which requires only [five] lines of code. Many other testing algorithms are imaginable, and a fundamentally different approach could examine machine-learning techniques for this template-matching system. In general, there will be tradeoff between software complexity and sensitivity to subtle differences in radiation spectra. On the hardware level, different types of detectors could be tested,

in particular, to determine the performance of the IBX with higher-resolution detectors, such as lanthanum-bromide scintillation detectors. For data acquisition, processing, and analysis, the IBX currently uses the *Red Pitaya*. This computer features a *Xilinx* system-on-chip, which combines an ARM processor with an FPGA. In principle, it may be possible to perform all functionalities and computations on the FPGA and to avoid the use of a complex CPU altogether. This could help the transition to a platform that is fully open and easier to authenticate.

We envision the IBX (or a similar system) to serve as a prototyping platform that can be used by a diverse group of experts from different fields to examine hardware and software vulnerabilities and to explore strategies to address them.[16] In particular, we hope devices such as the IBX can support future verification challenges similar to the *Underhanded-C Contest,* which in 2015 focused on the software of a hypothetical information barrier.[17] The costs of the device add up to only $700, with the most expensive parts being the *Red Pitaya* ($260) and the high-voltage module ($140–220). In principle, a kit could be made available to facilitate broader adoption and reach a diverse audience to work on the remaining verification challenges for nuclear arms control and disarmament.

Endnotes

[1]G. White, "Trends in Hardware Authentication," *56th Annual Meeting of the Institute for Nuclear Materials Management,* Indian Wells, CA, 2015.

[2]*Red Pitaya Wiki Documentation,* wiki.redpitaya.com.

[3]Matjaz Vencelj and Peter Ferjančič, February 2014, blog.redpitaya.com/?p=9.

[4]M. Kütt, A. Glaser, and M. Englert, "Open Source meets Nuclear Arms Control," *55th Annual Meeting of the Institute for Nuclear Materials Management,* Atlanta, GA, 2014.

[5]github.com/nuclearfutureslab/ibx or ibx.verification.technology.

[6]*A7505 User Manual,* UM3552, Revision 3, May 2016, www.caen.it. Similar products are available from iseg-hv.com/en/products/dc-dc.

[7]C. Marsh, *Information Barrier Software: Ada Design Document,* 2016, ukni.info/mdocs-posts/information-barrier-software-ada-design-document.

[8]For one potential approach, see S. Philippe, M. Kütt, M. McKeown, and A. Glaser, "The Application of Virtual Proofs of Reality to Nuclear Safeguards and Arms Control Verification," *57th Annual INMM Meeting,* July 24–28, 2016, Atlanta, Georgia.

[9]A. Di Fulvio, T. H. Shin, M. C. Hamel, and S. A. Pozzi, "Digital pulse processing for NaI(Tl) detectors," *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment,* 806, 11 January 2016, pp. 169–174.

[10]Canberra, *Model 802 Scintillation Detectors Datasheet,* CSP0232, 2009.

[11]The C++ readout also includes a number of data points preceding the trigger event to determine the level of the baseline offset.

[12]Di Fulvio et al., 2016, *op. cit.*

[13]The same technique is used in Sandia's Trusted Radiation Identification System (TRIS).

[14]M. Göttsche and A. Glaser, "Low-resolution Gamma-ray Spectrometry for an Information Barrier Based on the Template-Matching Approach," *57th Annual Meeting of the Institute for Nuclear Materials Management,* Atlanta, Georgia, 2016.

[15]Göttsche and Glaser, 2016, *op. cit.*

[16]M. Kütt, S. Philippe, and A. Glaser, "Leveraging the Wisdom of the Crowd: Hardware and Software Challenges for Nuclear Disarmament Verification," *56th Annual Meeting of the Institute for Nuclear Materials Management,* Indian Wells, CA, 2015.

[17]*Faking Fissile Material,* www.underhanded-c.org.