ISSN 1977-5296

ESARDA

European Safeguards Research and Development Association

Bulletin

N° 51

December 2014

ISSN 1977-5296

Number 51
December 2014

Editor
Hamid Tagziria

European Commission, Joint Research Centre,
ITU - Nuclear Security Unit
T.P. 800, I-21027 Ispra (VA), Italy
Tel. +39 0332-786324
esarda-bulletin@jrc.ec.europa.eu
hamid.tagziria@jrc.ec.europa.eu

ESARDA is an association formed to advance and harmonize research and development for safeguards. The Parties to the association are:
Areva, France; ATI, Austria; CEA, France; CNCAN, Romania; EDF, France; ENEA, Italy; European Commission; FZJ, Germany; HAEA, Hungary; MTA EK, Hungary; IRSN, France; MINETUR, Spain; NNL, United Kingdom; NRI, Czech Republic; NRPA, Norway; SCK/CEN, Belgium; Sellafield Ltd, United Kingdom; SFOE, Switzerland; SSM, Sweden; Springfields Fuels Limited, United Kingdom; STUK, Finland; University of Hamburg, Germany; University of Liege, Belgium; University of Uppsala, Sweden; UKAEA, United Kingdom; URENCO, Germany; VATESI, Lithuania; WKK, Germany; PAA, Poland; ORNL, USA.

Editorial Committee
K. Axell (SSM, Sweden)
P. Peerani (EC, JRC, ITU, Italy)
E. Raddle (ATI, Austria)
A. Rezniczek (Uba-GmbH, Germany)
B. Richter (FZJ, Germany)
P. Schwalbach (EC, DG ENER)
F. Sevini (EC, JRC, ITU, Italy)
H. Tagziria (EC, JRC, ITU, Italy) (Chairman)
J. Tushingham (NNL, United Kingdom)

Scientific and technical papers submitted for publication in the peer reviewed section are reviewed by independent authors including members of the Editorial Committee.

Manuscripts are to be sent to the Editor (esarda-bulletin@jrc.ec.europa.eu) following the 'instructions for authors' available on https://esarda.jrc.ec.europa.eu/ where the bulletins can also be viewed and downloaded.

Photos or diagrams should be of high quality.

Accepted manuscripts are published free of charge.

N.B. Articles and other material in the ESARDA Bulletin do not necessarily present the views or policies of neither ESARDA nor the European Commission.

ESARDA Bulletin is published jointly by ESARDA and the Joint Research Centre of the European Commission and distributed free of charge to over 1100 registered members, libraries and institutions Worldwide.

The publication is authorized by ESARDA.

© Copyright is reserved, but part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopy, recording, or otherwise, provided that the source is properly acknowledged.

Cover designed by Jose-Joaquim Blasco (JRC Ispra in Italy),

Printed by
IMPRIMERIE CENTRALE, Luxembourg

ESARDA
European Safeguards Research and Development Association
Bulletin

Table of Content Issue n° 51

Editorial

Peer Reviewed Articles

Other Articles

News and Synopses

Editorial

Hamid Tagziria

For the verification and monitoring of nuclear materials the IAEA and EURATOM inspectorates heavily rely on neutron assay techniques in general and on coincidence or multiplicity counting in particular, which predominantly use ^{3}He gas for neutron detection. For a number of decades ^{3}He has been readily available, its counters reliable, safe, easy to use, gamma-ray insensitive, and above all provide a high intrinsic detection efficiency. The well-publicized worldwide shortage of ^{3}He has resulted in important R&D efforts into alternative neutron detection technologies. Numerous initiatives have been launched worldwide and very promising new developments are being prototyped, tested, demonstrated or simply underway.

Year 2014 has been rich in events (measurement campaigns and workshops etc.) regarding novel technologies and safeguards applications in general and in particular for development of ^{3}He alternatives not only for security applications but more recently for nuclear safeguards too.

From the 27 to 28 March, ESARDA NA/NT workshop was held at Oxford University, UK with about 50 experts participating in the event on topics such anti-neutrino detection systems, new neutron detectors, safeguards R&D programmes, non-proliferation, treaty verification, arms control and advances in simulations, nuclear data and novel measurement methods. The abstracts and presentations are available either in CIRCABC web page of ESARDA NA/NT (https://circabc.europa.eu), or directly from the Secretary. Full reports on this event and other activities carried by other Esarda working groups are available on https://esarda.jrc.ec.europa.eu and were appropriate within this bulletin.

From the 13 to 17 October 2014 and under the DOE/NNSA-Euratom/JRC Action Sheet 47, an intensive campaign of measurements and inter-comparison of systems followed by a public workshop was hosted by the Nuclear Security Unit of JRC-ITU in Ispra (Italy) on ^{3}He alternative materials and technologies for safeguards applications.

The first two days of the week were restricted to technology developers only (with Japan as observers) and were dedicated to measurements, testing and inter-comparison in PERLA and ITRAP laboratories in Ispra of a number of systems sub-divided into 3 categories:

1. NCC Collar type: ^{3}He NCC (Euratom), Liq.scint. Collar (IAEA), Born-based collar (ORNL/GERS)
2. HLNCC type: ^{3}He HLNCC (JRC), LiZnS blades (Symetrica/JRC/Euratom), Straw-based HLNCC (PTI)
3. Neutron slab: ^{3}He slab (Euratom), Boron slab (LANL), Plast.scint. with PSD (UMICH)

Reference nuclear material and other radioactive sources available on the Ispra site were used and the systems were also benchmarked against standard and commonly used ^{3}He-based counters (e.g. HLNCC and the NCC).

The well attended workshop which followed the measurement campaign, from Wednesday to Friday, provided a further in-depth review of international efforts and progress on the matter. About 50 experts from U.S. national laboratories, European laboratories, the IAEA and Japan have been invited to attend. Furthermore and most importantly the presentations also included results of the measurements carried out during the week in addition to modelling results and data obtained since the last workshop in LANL in June 2013. On Thursday afternoon all workshop attendees were invited to a tour on the Ispra site of the laboratories PERLA, ITRAP, PUNITA and EUSECTRA laboratories (which together with valuable reference nuclear materials will be housed in the near future within one new purposely built building). The ^{3}He alternative technologies and the prototype systems were also demonstrated and shown by their developers.

Discussions regarding safeguards-relevant parameters for ^{3}He alternatives, work on specific materials and technologies, detector evaluation, comparison methodologies, and best practices were, as during the Los Alamos workshop in June 2013, most interesting and valuable to all.

This eventful week in Ispra was followed tightly from 20 to 24 October by the IAEA symposium on International Safeguards in Vienna where a few of the technologies demonstrated and used in Ispra will be presented and the new data shown and discussed; http://eventegg.com/iaea-symposium-2014.

Another important forthcoming event to retain is the 37th ESARDA symposium on Safeguards and Nuclear

Non-Proliferation which will be held in Manchester, UK from 19-21 May, 2015. The symposium is an opportunity for research organisations, safeguards authorities and nuclear plant operators to exchange information on new aspects of international safeguards and non-proliferation, as well as recent developments in nuclear safeguards and non-proliferation related research activities and their implications for the safeguards community. Other topics such as nuclear security applications and arms control verification technologies will also be covered. The best papers will be selected for peer-reviewing in view of publication in the ESARDA bulletin. Papers need be uploaded (via easychair) at least two weeks before the symposium to be considered for selection. See https://esarda.jrc.ec.europa.eu and the leaflet within this bulletin for further information.

Hamid Tagziria

Editor and Editorial Committee Chairman
Nuclear Security Unit of the JRC-ITU in Ispra (Italy)

https://esarda.jrc.ec.europa.eu
Esardabulletin@jrc.ec.europa.eu
hamid.tagziria@jrc.ec.europa.eu

Recent modelling studies for analysing the partial-defect detection capability of the Digital Cherenkov Viewing Device

Sophie Grape[1], Staffan Jacobsson Svärd[1]

[1] Department of Physics and Astronomy, Uppsala University, Box 516, SE-75120 Uppsala, Sweden

Abstract:

Strong sources of radioactivity, such as spent nuclear fuel stored in water pools, give rise to Cherenkov light. This light originates from particles, in this case electrons released from gamma-ray interactions, which travel faster than the speed of light in the water. In nuclear safeguards, detection of the Cherenkov light intensity is used as a means for verifying gross and partial defect of irradiated fuel assemblies in wet storage.

For spent nuclear fuel, the magnitude of the Cherenkov light emission depends on the initial fuel enrichment (IE), the power history (in particular the total fuel burnup (BU)) and the cooling time (CT). This paper presents recent results on the expected Cherenkov light emission intensity obtained from modelling a full 8x8 BWR fuel assembly with varying values of IE, BU and CT. These results are part of a larger effort to also investigate the Cherenkov light emission for fuels with varying irradiation history and other fuel geometries in order to increase the capability to predict the light intensity and thus lower the detection limits for the Digital Cherenkov Viewing Device (DCVD).

The results show that there is a strong dependence of the Cherenkov light intensity on BU and CT, in accordance with previous studies. However, the dependences demonstrated previously are not fully repeated; the current study indicates a less steep decrease of the intensity with increasing CT. Accordingly, it is suggested to perform dedicated experimental studies on fuel with different BU and CT to resolve the differences and to enhance future predictive capability. In addition to this, the dependence of the Cherenkov light intensity on the IE has been investigated. Furthermore, the modelling of the Cherenkov light emission has been extended to CTs shorter than one year. The results indicate that high-accuracy predictions for short-cooled fuel may require more detailed information on the irradiation history.

Keywords: DCVD, Cherenkov light emission, partial defects, initial enrichment, burnup, cooling time, Geant4

1. Introduction

The nuclear safeguards system relies on the verification of operator declared information as well as on the confirmation of absence of undeclared activities. As part of the former category, inspections are continuously carried out at nuclear facilities, where different instruments are used to draw conclusions about the inventory of spent nuclear fuel. The Digital Cherenkov Viewing Device (DCVD) is one of the instruments that are available to inspectors at such occasions. Its principle is based on the detection of Cherenkov light; a type of light that is created in e.g. water around strong radioactive sources due to the release of highly energetic electrons, which move faster than the speed of light in water. These electrons are themselves products of the photoelectric effect and Compton scattering, caused by the interaction of gamma rays from decaying fission products with electrons in the water. Specifically for electrons moving in water (with a refractive index of 1.34), one can calculate that the electrons need at least a kinetic energy of 257 keV in order to produce Cherenkov light. Higher electron energies lead to increased Cherenkov emissions, according to the Tamm-Frank equation [1].

For gross verification purposes, where inspectors draw conclusions on whether or not an item in a storage pool is a nuclear fuel assembly or a non-fuel item, the specific intensity of the Cherenkov light is not as important as its mere presence and distribution. However, for partial defect verification, where the goal is to determine if a fraction of the fuel rods in an assembly are removed or replaced, it is important to relate the detected Cherenkov light intensity to the intensity that is expected from that particular fuel assembly.

As a means to support partial-defect analysis, simulations of the expected Cherenkov light intensity as a function of burnup and cooling time are available [2] and have so-far been used for evaluations. These expected intensities are given in relative terms, and a calibration light source is needed for the absolute scale. However, some reasons have been put forward for repeating this type of simulations: (1) reported disagreements between simulated and experimental data, especially for cooling times below 5 years where large variations between the detected intensities from fuel assemblies with almost identical declared information but varying fuel irradiation history have been seen, (2) previous data do not include simulations for enrichments higher than around 2% nor do they take into account the irradiation history, (3) previous data do not include simulations with uncertainty estimates, and (4) current simulation tools and computer power would enable more detailed simulations than previously possible.

By repeating and extending the previously performed simulations, the goal of this work is to obtain a measure of the modelling accuracy and to investigate to what extent initial enrichment and fuel irradiation history influence the Cherenkov light emission. In the longer term, we envisage improved capability to predict the Cherenkov light intensity from intact fuel assemblies, which will benefit the partial defect detection process and possibly lower the detection level of the DCVD to partial defects. The purpose of this paper is to report on new simulation results, obtained using state-of-the-art simulation codes for the same type of fuel as in the previous simulations, in order to allow for comparisons. An additional objective is to present results on the dependence of the Cherenkov light intensity on initial enrichment and irradiation history, which has previously not been reported.

2. Simulation software

A dedicated simulation tool for modelling the response in the Digital Cherenkov Viewing Device (DCVD) has been developed [3]. It comprises three main steps: 1) the generation of gamma-ray source terms in the fuel, 2) the modelling of the gamma-ray interaction (including the release of electrons in the water), particle transport and consecutive Cherenkov light emission, and 3) the transport of Cherenkov light from the fuel to the DCVD, including its detection in the device. In this work, only the Cherenkov light emission has been under study, and accordingly the last step has been omitted.

In the first step, the fuel's initial enrichment (IE), irradiation history and cooling time (CT) are taken into account, which is important since these parameters strongly affect the gamma-ray emission from the fuel, and thus can be expected to influence the emission of Cherenkov light around the fuel. As an output, a gamma-ray spectrum is produced. In the earlier simulations [2], the source term generation was handled by the burnup calculation code ORIGEN 2, while now ORIGEN-ARP [4] in the Scale6.1-package [5] is used. The new code includes more fuel types, a larger number of energy groups, and more importantly updated cross sections for neutron reactions based on continuous-energy and multi-group neutron data and coupled neutron-gamma data based on ENDF/B-VI.8 and ENDF/B-VII.0. Furthermore, the data libraries include decay data, neutron-induced fission product yields, delayed gamma-ray emission data, and neutron emission data based on ENDF/B-VII and JEFF-3.0/A. Photon yield data libraries are based on the recent evaluations from Evaluated Nuclear Structure Data File (ENSDF).

The second step is modelled using the Geant4 (version 9.0 patch 02) simulation tool [6], as compared to Geant3.15, which was used for the simulations in [2]. Geant4 is a modern and updated version of the former and is written in object-oriented C++. It is adapted to large-scale, accurate and comprehensive simulations of particle detectors used in nuclear physics experiments, radiation physics, space science and nuclear medicine. Geant4 includes, among other things, new, refined and updated physics models, several different interaction models adapted to a variety of energy regimes and interaction types and offers a much better computing performance as compared to previous versions [6].

3. Modelling specifications

For all gamma-ray source term generation simulations included in this paper, gamma-rays with energies in the region of 0.257-3 MeV were extracted from ORIGEN-ARP, and here a total of 42 non-equal energy groups (intervals) were selected to provide sufficient energy resolution of the resulting gamma-ray spectrum. An example of a resulting gamma-ray spectrum is shown in figure 1. In the old simulations, only six broad energy groups were included.

ORIGEN-ARP offers modelling of several types of fuel. To be consistent with previous simulations, the 8x8 BWR fuel geometry was selected in this work. This geometry was also used in the second step, the simulations of the gamma-ray interaction, which were performed using the Monte Carlo software tool Geant4.

In the Geant4 simulations performed here, 10^5 gamma photons were isotropically generated per fuel rod according to the source distribution obtained in the former step, exemplified in figure 1. According to the Monte Carlo technique, each photon was traced individually whereby its interactions with the materials of the model geometry were governed by statistical properties. In this context, one may note that the Cherenkov photons are emitted in all directions and in this work no angular discrimination was performed among them, in accordance with the previous simulations [2], although the DCVD preferentially records photons emitted vertically. The validity of this description should be studied in greater detail but is outside the scope of this work. The details of the Cherenkov photon generation and its recording in Geant4 are not the focus for this paper and the reader is referred to ref [3] for more details.

The three main fuel parameters, which are under study here are the fuel's initial enrichment, its total burnup and its cooling time. A higher burnup corresponds to a larger power outtake from the fuel and hence more fission products that may initiate Cherenkov emission. Conversely, a longer cooling time allows for a larger fraction of these fission products to decay and their successively lower abundance implies a lower Cherenkov light emission with

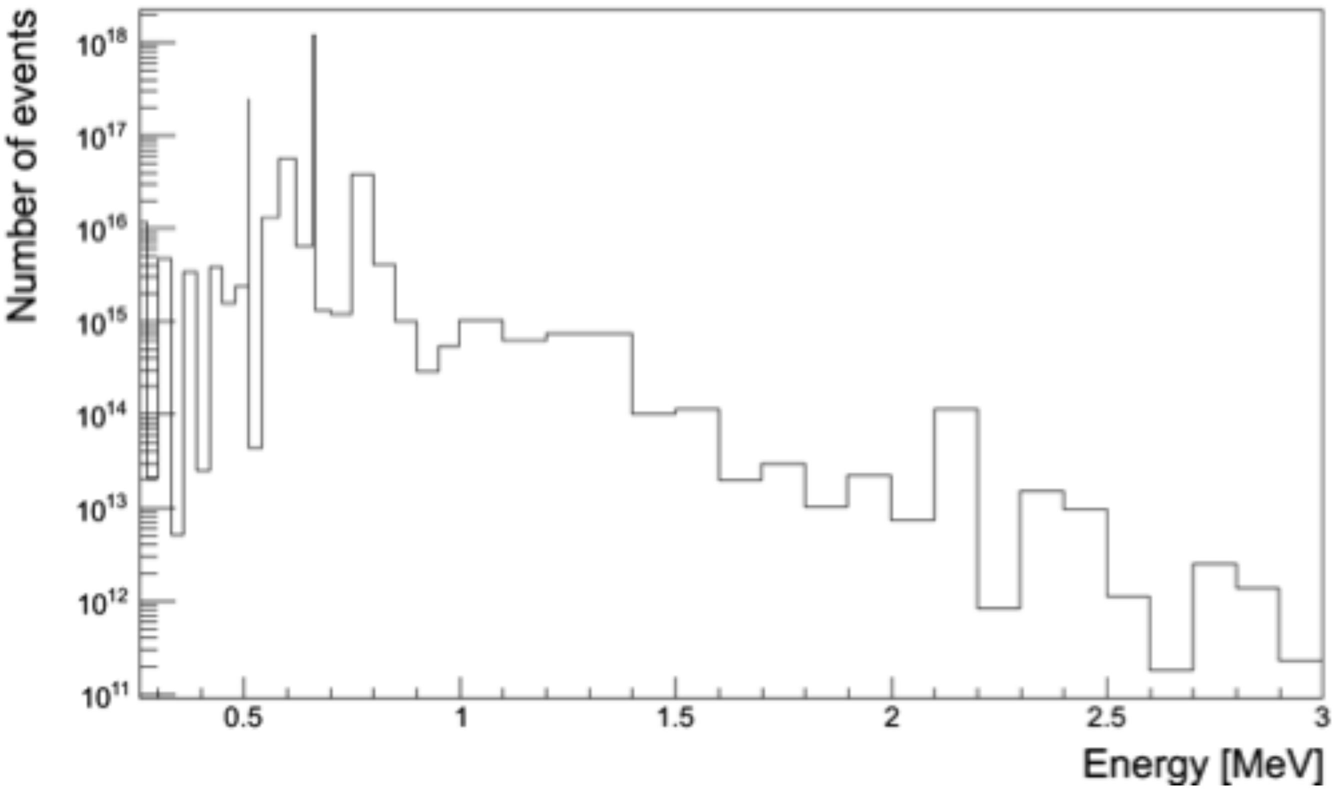


Figure 1: A typical ORIGEN-ARP spectrum obtained in this work, showing the simulated gamma-ray spectrum from an 8x8 fuel assembly with an initial enrichment of 2%, a BU of 40 GWd/tU and a CT of 2 years.

time. The impact of the initial enrichment is not as clear as that of burnup and cooling time, but the differences in fission yields of U-235 and U-238, and for high burnups also Pu-239, do affect the fission product contents and hence it may also affect the emitted Cherenkov light intensity.

In order to relate the new modelling results to the older ones [2], an initial enrichment of 2% was selected for the dominant part of the simulations. As modern fuel may comprise uranium enriched to 5%, enrichments up to that level were also simulated in a study of the dependence of the Cherenkov light emission on this parameter.

The dominant part of the investigations was performed of the complete 8x8 BWR fuel assembly with the purpose to extend the previously obtained Cherenkov intensity values to both shorter and longer cooling times, as well as to extend them to other initial enrichments. In this study, burnups of 10, 20, 30, 40 and 50 GWd/tU and cooling times of 0.25, 0.5, 1, 2, 3, 5, 7, 10, 15, 20, 30, 40 and 50 years were chosen. In addition to this, it is desired to investigate the uncertainties of the data points and in the future, also study how the Cherenkov emission depends on fuel geometry and irradiation cycle.

Finally, one may note that the power level and irradiation history will also affect the Cherenkov light intensity, since it will affect the gamma-ray emission. For this reason, a limited study of how changes in the power level and irradiation history affects the light intensity is also included. Just like the other fuel parameters, the irradiation histories were initially also selected to be as similar as possible to the previous simulations. Accordingly, the power level during every cycle in each simulation was 8 MW/tU for 10 GWd/tU, 16 MW/tU for 20 GWd/tU and 24 MW/tU for 30-50 GWd/tU. The irradiation cycles were chosen to be 330 days followed by 35 days of outage, for all cycles except for the last one. Given the desired burnup for each simulation and the selected power level, the last cycle was adapted so that it became 260 days for BU=10-30 GWd/tU, 347 days for 40 GWd/tU and 104 days for 50 GWd/tU.

4. Results

4.1 Dependence on burnup, cooling time and fuel cycle history

In figure 2, the simulated Cherenkov-light emission for a complete 8x8 BWR fuel assembly with an initial enrichment of 2% is shown, together with simulated data from earlier simulations. The data sets are normalized to their respective mean values, taking into accounts only data points that are common for both cases i.e only including cooling times of 1-40 years.

No comparison between absolute emission values between the new and previous simulations has been performed for the simple reason that previous data do not provide absolute numbers. However, irrespective of absolute numbers, it is seen that the simulated Cherenkov-light emission falls off

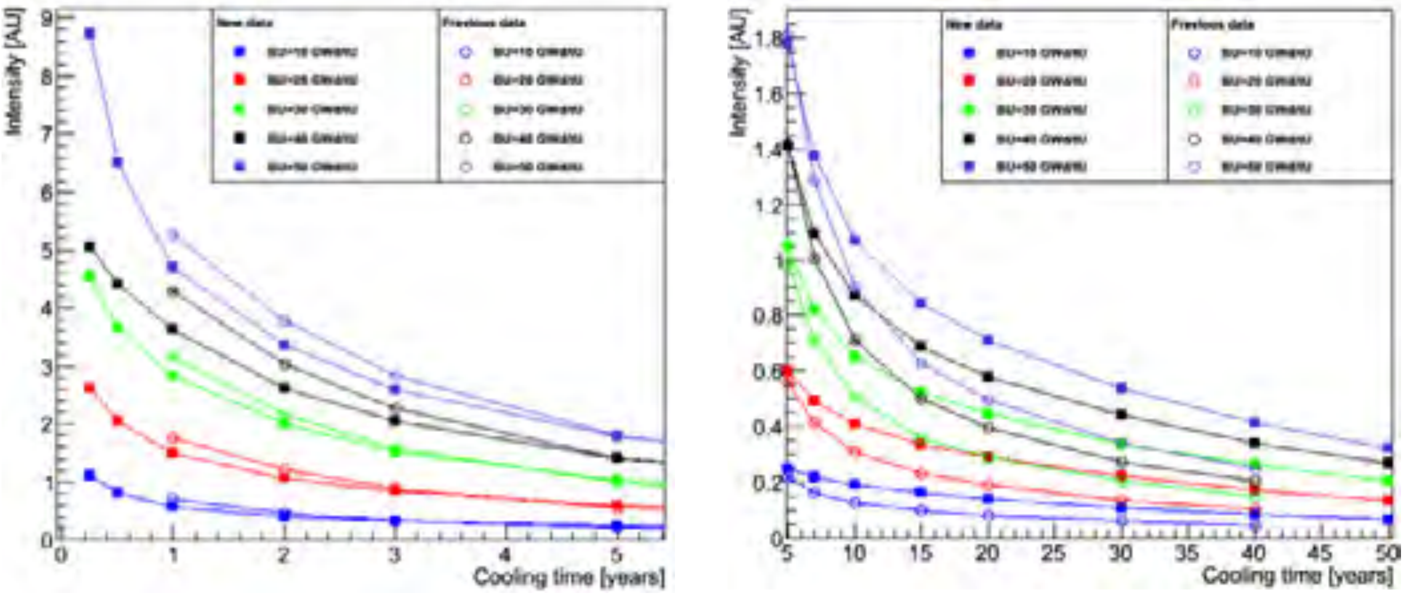


Figure 2: Simulated relative Cherenkov light emission from a 8x8 BWR fuel assembly with an initial enrichment of 2%. The squared markers indicate the new results, the circles mark original results from [2].

slightly slower with cooling time according to the current study as compared to the previous data. As compared to previous simulations, the new simulations have also been extended to shorter cooling times, which show a much higher rate of Cherenkov-light emission. The intensity after 3 months cooling time, as compared to one year, is almost 70% higher for a high-burnup of 50 GWd/tU fuel and almost 60% for 10 GWd/tU fuel. However, the corresponding Cherenkov intensity for BU=40 GWd/tU shows a significantly smaller difference. One identified possible reason for this may be the irradiation history, because the last irradiation period simulated for this specific burnup is longer than in the other simulations. This should however be investigated in further detail before conclusions can be drawn.

Although it is not visible in figure 2, the new data points do include statistical uncertainties as estimated by Geant4 based on the stochastic nature of Cherenkov light emission. These uncertainties are in the order of 0.07%, for all simulations presented here. Repeating the same simulation four times for the data point with BU=30 GWd/tU and CT=20 years gives a maximum variation of around 0.2% and a standard deviation of 0.1%, confirming this level of precision. However, other sources of uncertainties and approximations are expected to cause significantly larger imprecision, such as the irradiation history for which the impact of needs to be individually modelled for each (authentic) fuel assembly.

In order to get an indication of how much the irradiation history may affect the Cherenkov emission, two additional simulations were performed. Now, the power production was chosen such that the last irradiation period amounted to 260 days for both the burnup levels BU=40 GWd/tU and BU=50 GWd/tU. The results at a CT of 3 months are shown in table 1 and reveal that the irradiation history does in fact matter. Adjusting the number of days in the last cycle gives a change in Cherenkov emission of 2-3%.

Due to the lack of short cooled 8x8 fuel in the world, depending on that this fuel type is not manufactured any more, it is not possible to collect new data with cooling times below 10-15 years. And although scattered data exist from earlier measurements, it is not enough to evaluate the simulation models used. Instead, a dedicated experimental study is suggested, according to section 5.

BU [GWd/tU]	Power level [MW/tU]	Number of irradiation cycles	Days in the last irradiation cycle	Relative Cherenkov emission intensity
40	24.0	5	347	5.06
40	21.0	6	260	5.17 (+2.2%)
50	24.0	7	104	8.73
50	22.3	7	260	8.49 (-2.7%)

Table 1: Relative Cherenkov emission intensities at a CT of 3 months in the “default” simulation cases for BU=40 GWd/tU and BU=50 GWd/tU as well as for a selected case when the last irradiation cycle has 260 days, in accordance with the simulations of lower burnups.

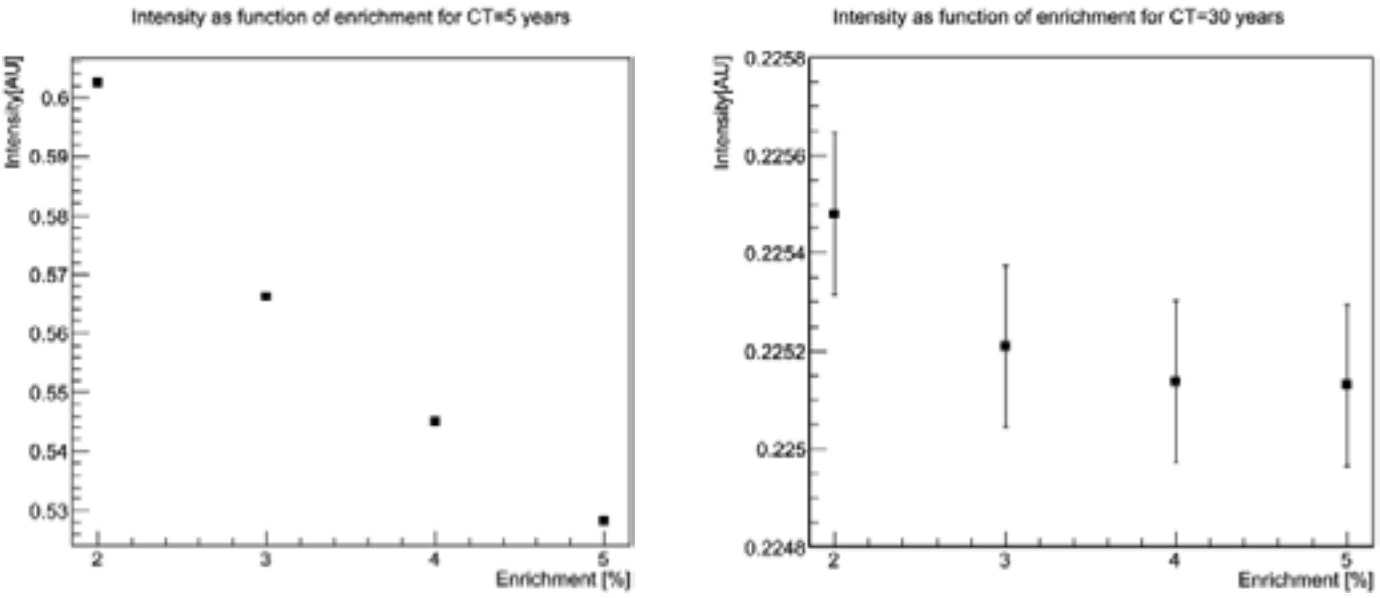


Figure 3: The Cherenkov light intensity for initial enrichments of 2-5% for a fuel with BU of 20 GWd/tU and a cooling time of 5 years (left) and 30 years (right). The apparent difference in error bars is due to the use of different scales on the vertical axes in the figures. Note that both axes have been cut.

4.2 Dependence on initial enrichment

The dependence of the emission of Cherenkov light on the initial enrichment was investigated at a BU of 20 GWd/tU and for cooling times of 5 and 30 years. Simulations were performed for initial enrichments of 3%, 4% and 5%, in addition to the 2% already covered in the previous section. It may be noted that the neutron flux is implicitly set in Origen-ARP depending on the selected fuel type, fuel burnup and power level, which means that for the same burnup but different initial enrichments, the neutron flux will be, and accordingly the total amount of gamma-rays produced will differ.

The results are shown in figure 3. The lowest intensity is obtained with the highest initial enrichment of 5%. The effect of the enrichment on the Cherenkov emission is strongly dependent on time. The Cherenkov emission for an enrichment of 5%, a BU of 20 GWd/tU and a CT of 5 years is for instance 13% lower than the emission for 2% enrichment, whereas for a CT of 30 years, the corresponding difference is only 0.16%.

One explanation to the decrease in Cherenkov emission intensity with increasing initial enrichment may be found in the gamma ray spectrum created in Origen-ARP. More detailed results from the simulations of a CT of 5 years are presented in table 2, showing that the total number of events in the input spectrum to Geant4 decreases with increasing enrichment. Reasons for this dependence can most likely be found in the adaptation of the neutron flux in Origen-Arp (in order to reach the specified burnup and power level for different fissile contents), which in turn affects the interaction in the fuel and hence the gamma-ray spectrum.

Initial enrichment [%]	Total number of events in Origen-Arp spectrum [10^{18}]	Cherenkov intensity [AU]
2	2.30	0.60
3	2.22	0.57
4	2.17	0.55
5	2.13	0.53

Table 2: Simulated data for assemblies with a BU of 20 GWd/tU, a CT of 5 years and initial enrichments of 2%, 3%, 4% and 5%, respectively.

A deeper study of the connection between the gamma-ray source spectrum, the electron energy distribution and the resulting number of Cherenkov photons is needed in order to conclude the detailed features that give rise to these results. It should however be noted that initial enrichment does play a role for the emission of Cherenkov light from the fuel.

5. Conclusions and outlook

The detection of Cherenkov light is one of the means used for the verification of spent nuclear fuel in accordance with nuclear safeguards agreements in force. In order to draw conclusions on partial defects, where a fraction of the fuel material has been removed and/or replaced, using the Cherenkov light, one must have a predictive capability accurate enough to enable experimental verification within decent limits. The higher the precision of predictions as well as measurements, the smaller diversions may be detected. At present, a sensitivity to detect 50% partial defects is established, but improved procedures may lead to a lowering of this limit.

Earlier simulations of the Cherenkov emission have been performed [2], but without being experimentally confirmed. It is however possible to repeat the simulations using other software in order to get an estimate of their accuracy. In this case, the repeated simulations result in differences in the relative Cherenkov light emission of -18% for BU=10 GWd/tU and 1 year cooling time, and +80% for the same burnup but at 40 years cooling time. The results point out a need for experimental data, for the purpose of systematically studying the response of the DCVD to irradiated nuclear fuel with varying fuel parameters and irradiation histories.

From the results, it can be seen that cooling times shorter than one year result in a very strong Cherenkov light emission. It can also be seen that the dependence of the emission on fuel burnup and cooling time from the older simulations is not fully repeated. The fall-off of Cherenkov light emission in the new simulations is slightly less steep with increasing cooling times.

In addition, it has been shown that there is a dependence on Cherenkov light emission on the initial enrichment, in particular at short cooling times, explained by the fact that the enrichment affects the gamma-ray spectrum. The details of the reasons for this dependence may be focus for future studies.

A number of items may be subject for future work:

- In order to obtain experimental verification for the results, the next step is to simulate other fuel geometries, such as common PWR geometries, which are available for verification also for cooling times shorter than 10 years.
- Because experimental data have exhibited large variations in detected Cherenkov light intensity for spent nuclear fuels with almost identical burnup but with different irradiation histories, investigations of this effect have a high priority.
- An experimental campaign should be performed in line with the above suggestions.
- The apparent reduction in Cherenkov light intensity for increasing initial enrichment should be studied.
- Furthermore, in this work, the total emission of Cherenkov light has been studied. Since safeguards verification using the DCVD is performed using instrumentation placed above the fuel, only Cherenkov light emitted in the vertical direction is collected. Further studies have to be made to investigate whether the vertical component of the light may be represented by the total emitted light in order to apply these data to the analysis of fuel inspection data.

Validated Cherenkov light emission intensities will be valuable in the continuous process of developing the capabilities of the DCVD as a partial defect tester. By improving the predictive capabilities using accurate modelling, the capabilities to detect smaller fractions of diverted fuel material may also be expected to improve. This work discusses a first and very important step on the way, where further verification of other fuel types and irradiation histories is crucial.

6. Acknowledgements

The Geant4 computations were performed using resources from Uppsala Multidisciplinary Centre for Advanced Computational Science (UPPMAX) under project p2007011.

The Swedish and Canadian IAEA support programmes are acknowledged for information sharing and fruitful discussions. The Swedish Radiation Safety Authority, SSM, is in addition acknowledged for financial support.

7. References

[1] *Cerenkov emission induced by external beam radiation stimulates molecular fluorescence*,Johan Axelsson, Scott C. Davis, David J. Gladstone, Brian W. Pogue, Med. Phys. **38**, 4127 (2011). Egentligen: I. E. Tamm and I. M. Frank, "*Coherent radiation from a fast electron in a medium*," Dokl. Akad. Nauk SSSR 14, 107–112 (1937)

[2] Rolandson S. *Determination of Cerenkov Light Intensities from irradiated BWR Fuel*, IAEA task ID JNTA0704, SKI Report #: SE 1-94, March, (1994)

[3] Grape S., Jacobsson Svärd S., Lindberg B., *Verifying nuclear fuel assemblies in wet storages on a partial defect level: A software simulation tool for evaluating the capabilities of the Digital Cherenkov Viewing Device*, Nuclear Inst. and Meth. A, Volume 698, 11 January (2013), Pages 66-71, ISSN 0168-9002, 10.1016/j.nima.2012.09.048.

[4] Bowman S. M et al., *ORIGEN-ARP, a fast and easy-to-use source term generation tool*, Paper submitted to ICRS – 9, Ninth International Conference on Radiation Shielding, August 6, (1999)

[5] https://rsicc.ornl.gov/codes/ccc/ccc7/ccc-785.html

[6] Agostinelli S., et al (the Geant4 Collaboration), Geant4—a simulation toolkit, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, Volume 506, Issue 3, 1 July (2003), Pages 250-303

Impact of Nuclear Data Uncertainties on Calculated Spent Fuel Nuclide Inventories and Advanced NDA Instrument Response

Jianwei Hu and Ian C. Gauld

Reactor and Nuclear System Division, Oak Ridge National Laboratory,
1 Bethel Valley Road, PO Box 2008, MS-6172, Oak Ridge, TN 37831-6172, United States
E-mail: huj1@ornl.gov, gauldi@ornl.gov

Abstract:

The U.S. Department of Energy's Next Generation Safeguards Initiative Spent Fuel (NGSI-SF) project is nearing the final phase of developing several advanced nondestructive assay (NDA) instruments designed to measure spent nuclear fuel assemblies for the purpose of improving nuclear safeguards. Current efforts are focusing on calibrating several of these instruments with spent fuel assemblies at two international spent fuel facilities. Modelling and simulation is expected to play an important role in predicting nuclide compositions, neutron and gamma source terms, and instrument responses in order to inform the instrument calibration procedures. As part of NGSI-SF project, this work was carried out to assess the impacts of uncertainties in the nuclear data used in the calculations of spent fuel content, radiation emissions and instrument responses.

Nuclear data is an essential part of nuclear fuel burnup and decay codes and nuclear transport codes. Such codes are routinely used for analysis of spent fuel and NDA safeguards instruments. Hence, the uncertainties existing in the nuclear data used in these codes affect the accuracies of such analysis. In addition, nuclear data uncertainties represent the limiting (smallest) uncertainties that can be expected from nuclear code predictions, and therefore define the highest attainable accuracy of the NDA instrument. This work studies the impacts of nuclear data uncertainties on calculated spent fuel nuclide inventories and the associated NDA instrument response. Recently developed methods within the SCALE code system are applied in this study. The Californium Interrogation with Prompt Neutron instrument was selected to illustrate the impact of these uncertainties on NDA instrument response.

Keywords: nuclear data; uncertainty; spent fuel safeguards; CIPN; NDA.

1. Introduction

The U.S. Department of Energy Next Generation Safeguards Initiative Spent Fuel (NGSI-SF) Project is nearing the final phase of developing several advanced nondestructive assay (NDA) instruments designed to measure spent nuclear fuel assemblies for the purpose of improving nuclear safeguards [1, 2]. As the project completes the initial R&D and instrument development phase, current efforts are focusing on instrument deployment and experimental measurements at the Swedish Central Interim Storage Facility for Spent Nuclear Fuel (Clab), operated by the Swedish Nuclear Fuel and Waste Management Company SKB, and at the Post Irradiation Experimental Facility at the Korea Atomic Energy Research Institute in the Republic of Korea (ROK).

The advanced NDA instrument performance must be evaluated using spent fuel assemblies that have well known characteristics and compositions in order to understand the instrument response, and the instruments must be accurately calibrated to enable measurement of the absolute plutonium mass and other spent fuel attributes of interest to safeguards with high reliability. Advanced modelling and simulation codes, such as MCNPX [3] and SCALE [4], have been used extensively for instrument design, development, and calibration. Quantifying the uncertainties in these calculations is an important task required for instrument calibration because these uncertainties will affect the NDA instrument performance prediction and limit the accuracy that can be attained. Many of the advanced instruments rely on complex analysis of the measured signals, and interpretation of these data is informed in large measure by modelling and simulation codes. The uncertainties in calculated spent fuel content arise from various sources, such as irradiation history, burnup, irradiation conditions (e.g., exposure to burnable poisons), etc. These uncertainties are discussed in detail in a separate report [5]. The uncertainties in the underlying nuclear data used by the computer codes also affect the calculated nuclide concentrations in spent fuel and thus the predicted instrument responses for the spent fuel measurement; however, such impacts have not been previously studied under the NGSI program. Nuclear data uncertainties represent the limiting (smallest) uncertainties that can be expected from the code predictions, and therefore define the highest attainable accuracy of the instrument.

In this work, the impacts of nuclear data uncertainties on calculations of spent nuclear fuel content and associated NDA instrument responses are studied. Recently developed methods [6] within the SCALE code system are applied in this study. The Californium Interrogation with Prompt Neutron (CIPN) instrument [7] was selected to illustrate the impact of these uncertainties on instrument response. The study addresses only the uncertainties in the calculated nuclide concentrations of the spent fuel assembly; it does not include the impacts of nuclear data uncertainties on radiation transport calculations of the MCNPX detector model.

2. Uncertainties in nuclear data

Burnup codes are routinely used to calculate nuclide concentrations in spent fuel. These calculations require simulation of neutron transport to determine the neutron flux in the fuel during irradiation, and nuclear depletion and decay analysis. There are three main types of nuclear data involved in burnup calculations: 1) neutron cross sections (e.g., fission and absorption cross sections); 2) fission product yields (e.g., fission product generation due to the fission of an actinide); and 3) decay data (e.g., decay modes, half-lives, branching ratios). Uncertainties exist in all nuclear data; for example, uncertainties exist in the cross-section values, measured half-lives, and branching ratios. In addition, many of the data are correlated, and accurate representations of these data correlations (covariance files) are necessary for rigorous uncertainty analysis.

The majority of the research effort in uncertainty analysis has been directed at expanding the covariance data for nuclear cross sections. The most recent release of the Evaluated Nuclear Data Files, ENDF/B-VII.1 [8], provides extensive data on cross-section uncertainties (covariance data evaluations) for 190 isotopes that are particularly important in nuclear technology applications. The previous release, ENDF/B-VII.0 [9], contained neutron cross-section covariances for only 26 materials, of which 14 were considered a complete representation of the reaction energy range and major reaction channels. The expansion of neutron cross-section covariance data represents one of the major advances in the latest nuclear data library. The neutron cross-section covariance data used in this work were developed prior to the release of ENDF/B-VII.1, and are distributed with the SCALE code system. Selected covariance evaluations were taken from the pre-release of ENDF.B-VII.1, while most of the data were taken from

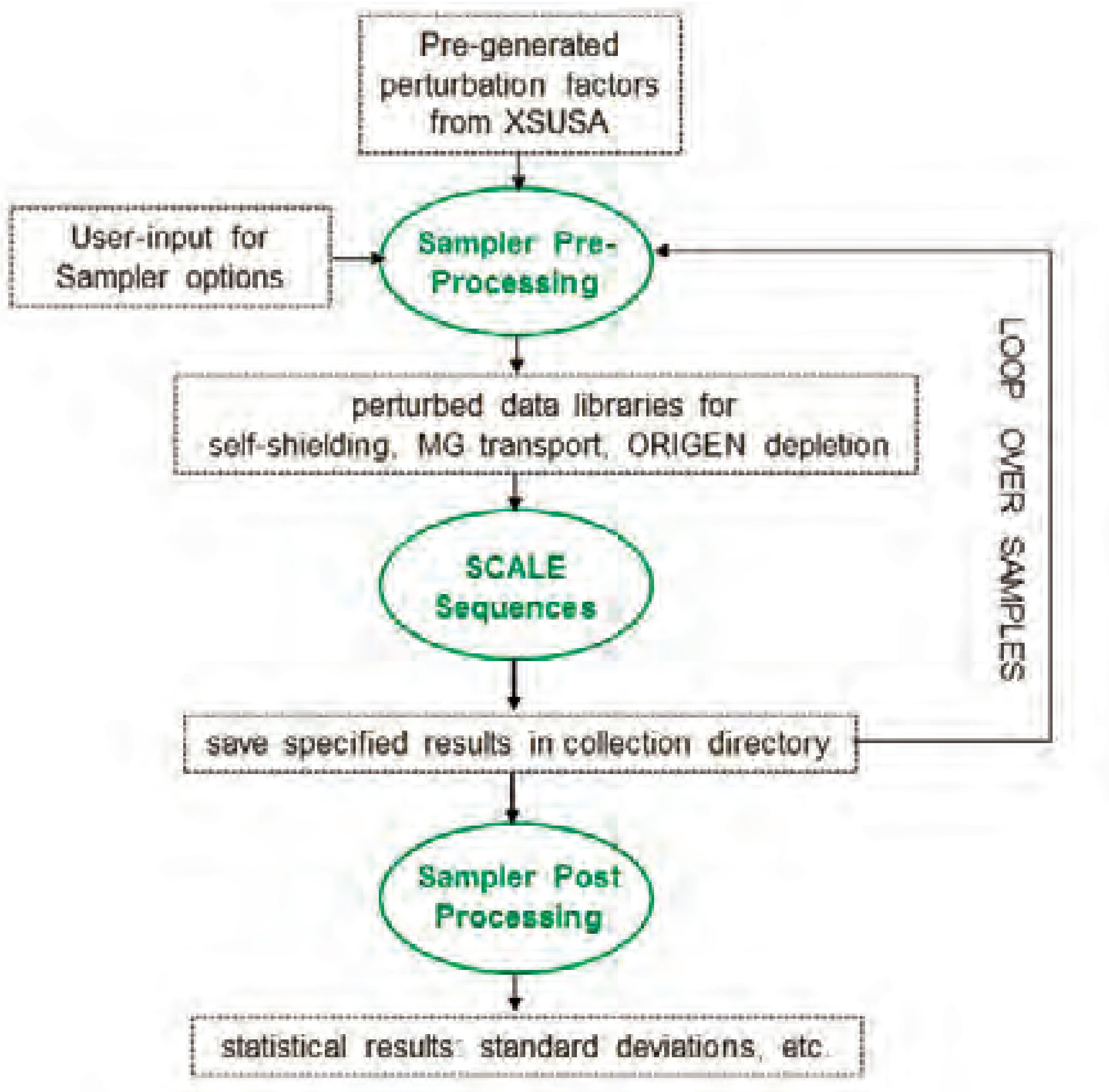


Figure 1: Sampler flowchart [6].

ENDF/B-VII.0, ENDF/B-VI, JENDL, and additional low-fidelity data for more than 300 nuclides developed by U.S. national laboratories under a DOE project for nuclear criticality safety [10]. Cross-section covariances for a total of 401 materials were available.

ENDF/B-VII and other international evaluated nuclear data files currently do not include covariance information for fission product yields, which are highly correlated. The evaluations contain uncertainties for the direct and cumulative fission yields, but not the correlations necessary to apply the data for fission product uncertainty analysis. To support uncertainty analysis for fission products, correlation matrices for direct fission yields have recently been developed by Oak Ridge National Laboratory (ORNL) [6] using the nuclear data and uncertainties in the ENDF/B-VII.0 evaluations, developed by England and Rider [11], and these covariance files have been implemented for use in SCALE.

Decay data are generally correlated to a lesser degree, and the uncertainties for decay data are available through ENDF/B-VII. The covariance files are utilized by SCALE for the uncertainty analyses.

3. Uncertainty analysis methods

A newly developed uncertainty analysis tool within SCALE, named Sampler [6], was applied to the burnup calculations used to support NGSI spent fuel analysis in this work. Sampler generates perturbed nuclear data libraries that have been adjusted by Monte Carlo (stochastic) sampling of the data in a manner that is consistent with the uncertainties and correlations in the data. This stochastic sampling of the correlated nuclear data uncertainties is performed using the XSUSA code [12] developed by Gesellschaft für Anlagen-und Reaktorsicherheit (GRS) in Germany. Sampler can be applied to any SCALE sequence (e.g., reactor lattice physics, burnup and decay, shielding and criticality calculations). Sampler repeatedly calls the SCALE sequence to perform the calculation, each time using a different set of perturbed nuclear data libraries, and then post-processes the results to obtain the distribution and statistical parameters on the calculated quantities. Figure 1 shows the flowchart of Sampler.

The TRITON module within SCALE (version 6.1.2) is widely used to perform burnup calculations, and is used within the

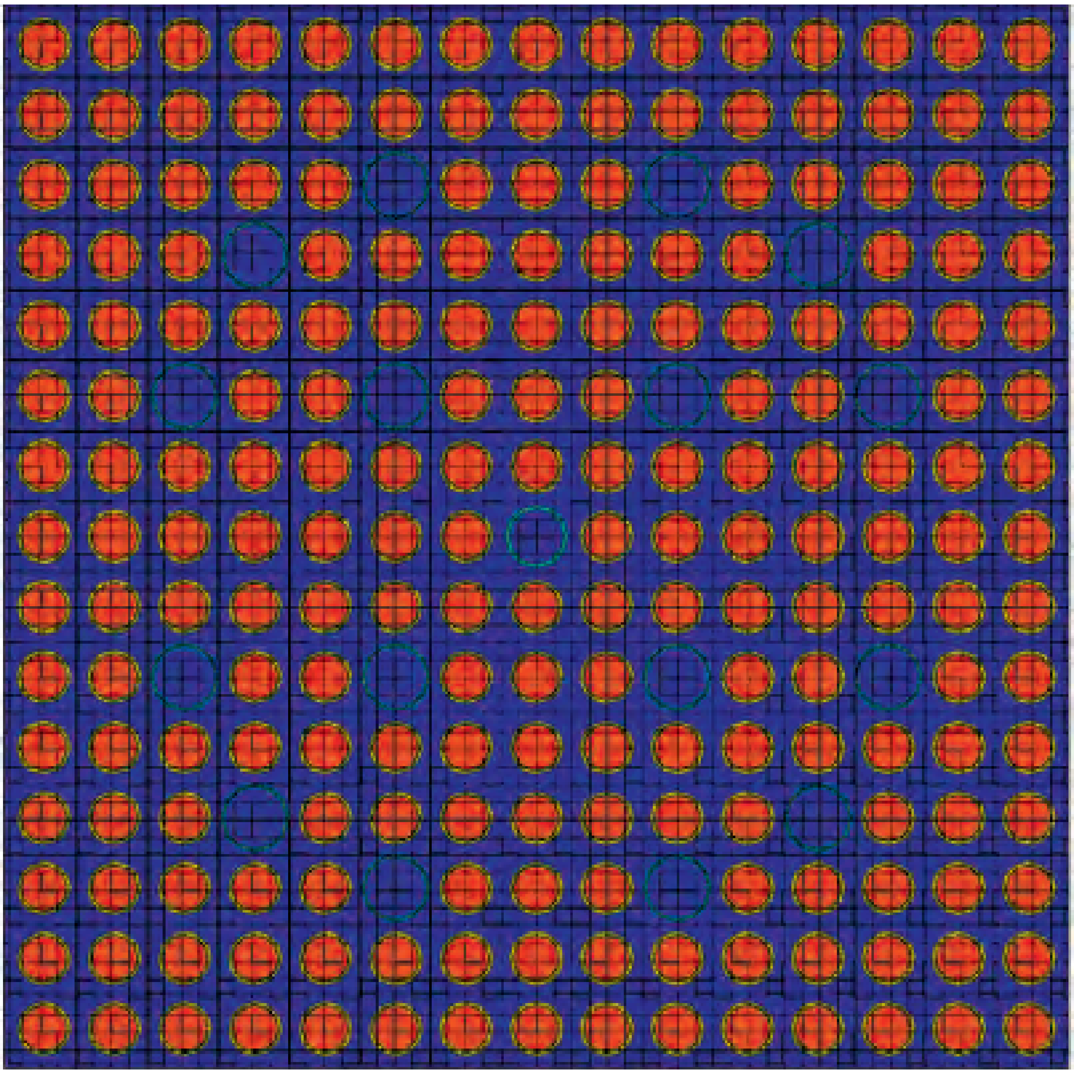


Figure 2: The simplified 15×15 PWR spent fuel assembly as modeled in TRITON.

NGSI-SF project to generate the reference spent fuel inventories for the spent fuel assemblies being measured at the Clab facility in Sweden and the assemblies measured in ROK. For each set of the perturbed data libraries, an individual SCALE/TRITON calculation was executed and the responses (e.g., nuclide concentrations in this case) due to the different data libraries were obtained. The variance in the NDA detector responses attributed to the nuclear data uncertainties can thus be assessed. Sampler will post-process the response distributions to compute statistical parameters (e.g., standard deviation of the concentration of a particular nuclide). Sampler can also perform perturbations to modelling parameters of a system to assess the impacts of uncertainties from other sources in input information including material densities, temperatures, dimensions, etc.

SCALE/TRITON couples the two-dimensional deterministic neutron transport code NEWT, which was used in this work, or the three-dimensional Monte Carlo KENO code for the neutron transport calculation, with the ORIGEN code for nuclide depletion and decay calculations. Therefore, uncertainties in the neutron cross sections (used in both the neutron transport and depletion calculation), fission product yields, and nuclear decay data are all included in the total uncertainty analysis.

4. Impact of nuclear data uncertainties on nuclide concentrations

A simplified assembly model of a typical 15×15 PWR design with 16 guide tubes and 1 central instrument tube was developed for this work, shown in Figure 2. The fuel has an initial ^{235}U enrichment of 4.5 wt% and was irradiated to 45 GWd/tU and cooled for 5 years. All the fuel rods were modelled during the burnup analysis using a single fuel material mixture (uniform composition). In reality, the fuel content will vary from rod to rod, but for the purposes of this study, uniform fuel compositions were determined to be sufficient to quantify the impacts from nuclear data uncertainties alone.

A total of 120 separate burnup calculations were performed, with each calculation using a different set of perturbed cross section, fission yield, and decay libraries. By examining the distribution of nuclide concentrations from these calculations, the standard deviation for each nuclide due to the uncertainties in the nuclear data used in the calculations was obtained. Figure 3 shows average relative uncertainty in calculated ^{239}Pu content, in these 120 cases, caused by nuclear data uncertainties. The uncertainty of ^{239}Pu increases with burnup and reaches 1.3% at 45 GWd/tU due to the accumulation of nuclear data uncertainties at higher burnups. Figure 4 shows the distribution of ^{239}Pu content after the 5-year cooling time for all 120 samples, indicating that approximately 88% of the predicted ^{239}Pu content is within the range of 27 to 28 mol per tonne U (tU) (equivalent to 0.6% of heavy metal mass). The mean value and relative standard deviation of the distribution is 27.42 mol/tU ± 1.3%. This value presents the expected uncertainty in the calculated result due to the nuclear data alone. Uncertainties for any other nuclides or any other calculated quantity can be obtained in a similar manner. The distribution of the results will approach a normal distribution as the number of samples increases.

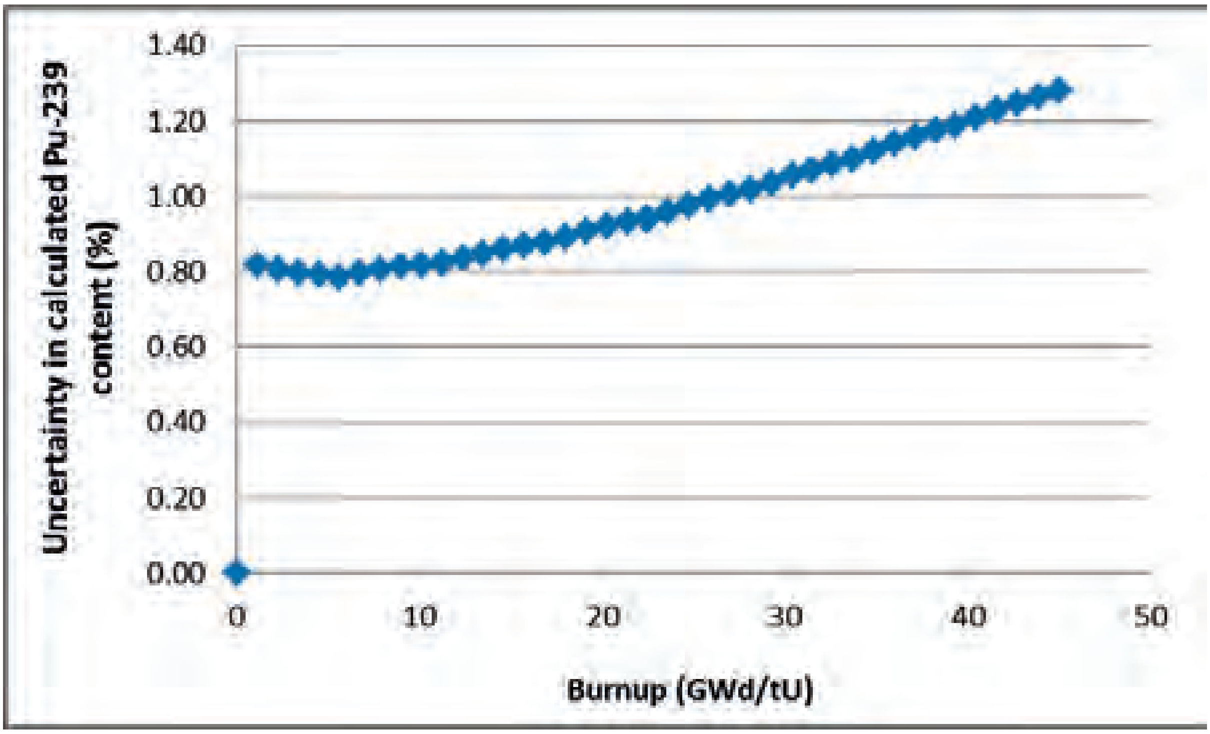


Figure 3: Uncertainty in calculated ^{239}Pu content as a function of burnup.

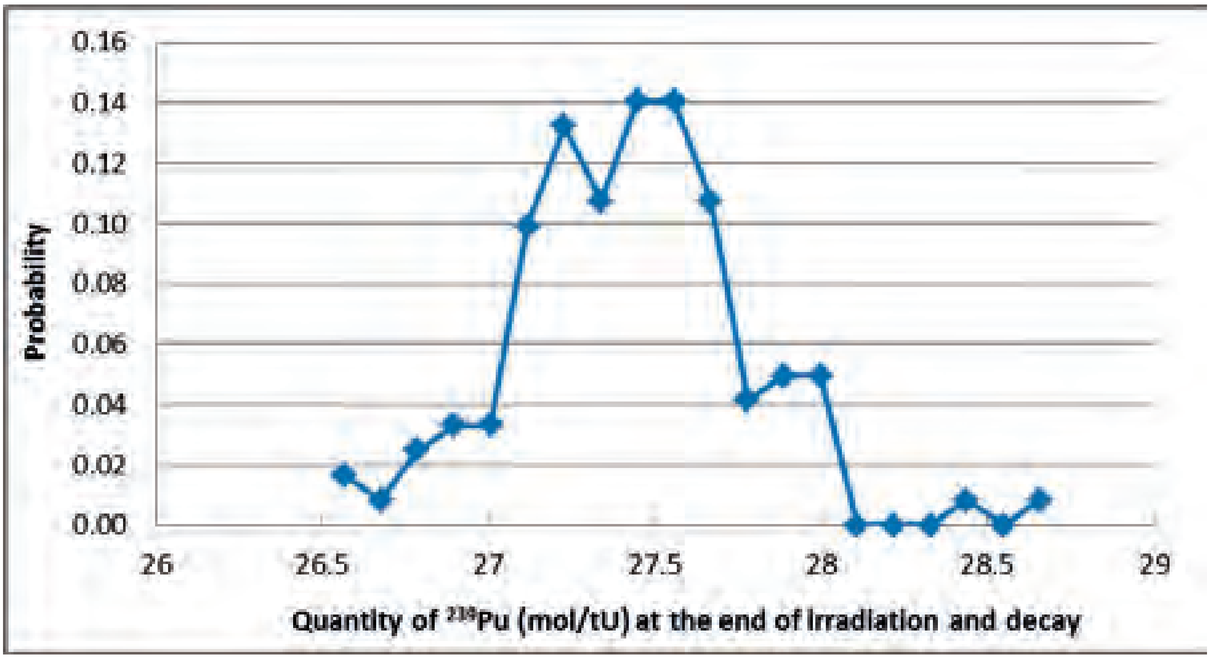


Figure 4: Distribution of calculated ^{239}Pu mass results for 120 samples.

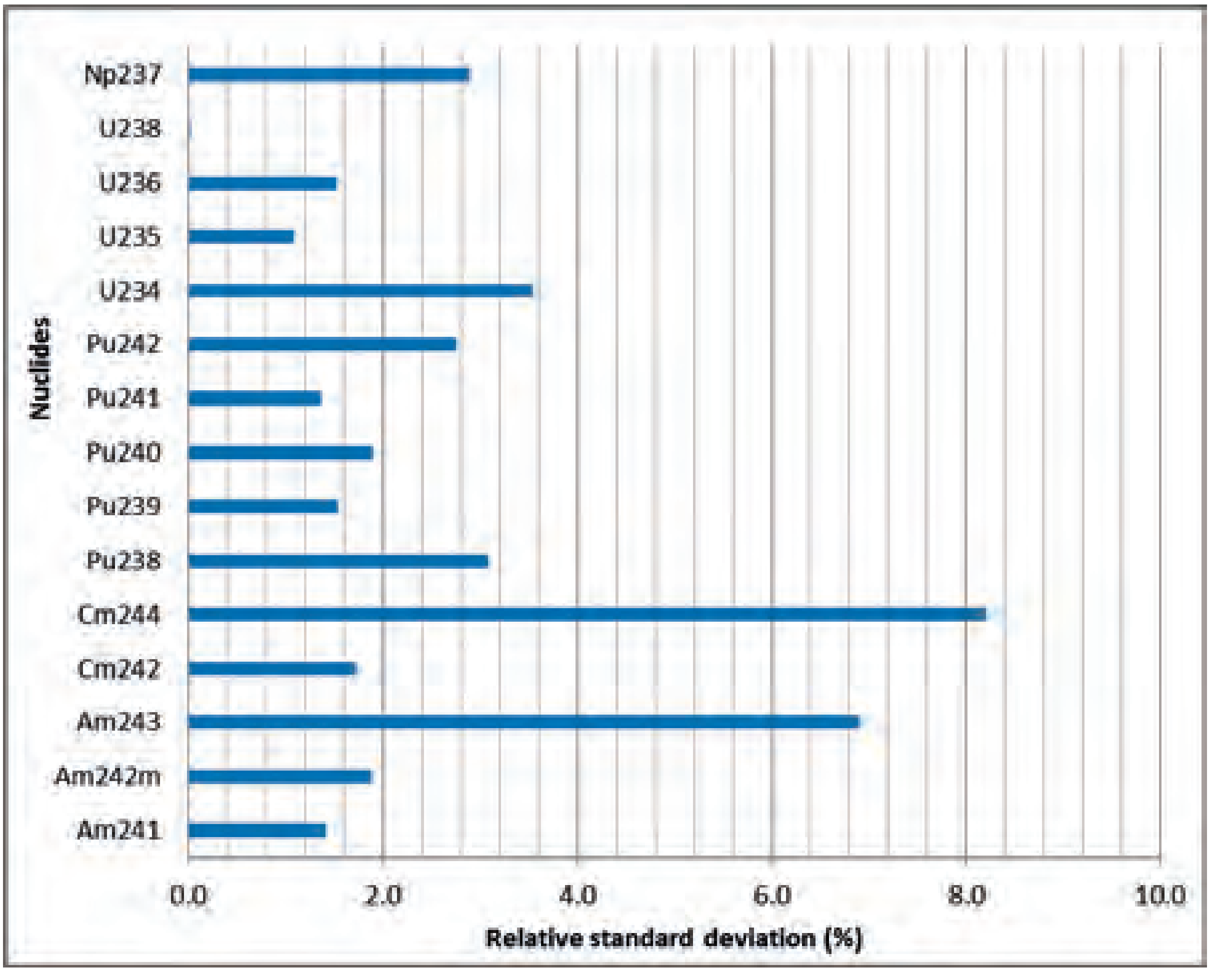


Figure 5: Relative standard deviation of major actinides due to nuclear data uncertainties.

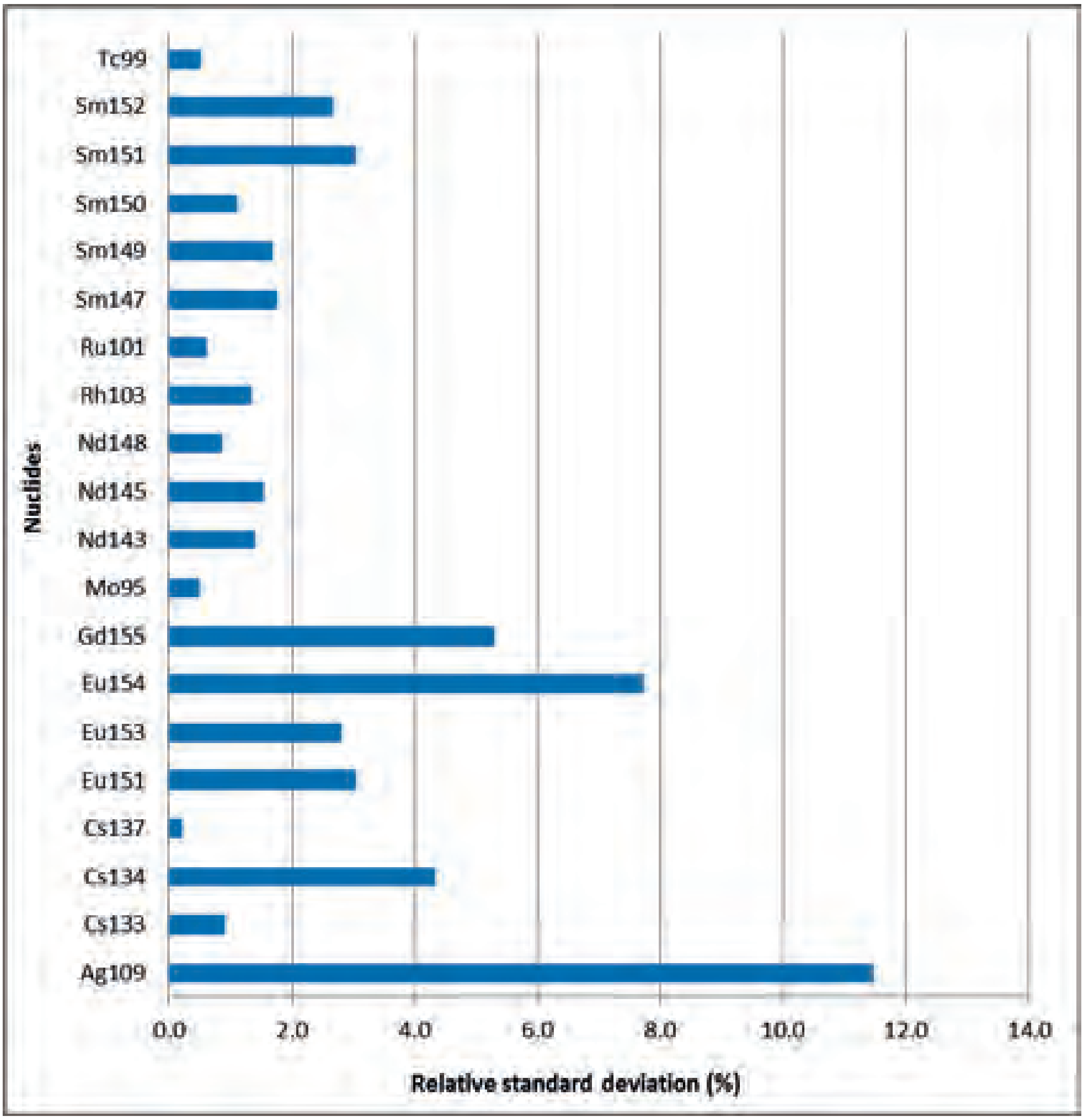


Figure 6: Relative standard deviation of important fission products due to nuclear data uncertainties.

Figure 5 shows the relative standard deviation of the major actinides. The relative standard deviations caused by the uncertainties in nuclear data are generally within 2% for most actinides, and they vary from one nuclide to another because their production paths are different. The standard deviations for ^{239}Pu, ^{240}Pu, and ^{241}Pu, the three major plutonium isotopes, are 1.5%, 1.9%, and 1.4%, respectively. Because ^{244}Cm is a dominant passive neutron source in spent fuel, the relatively large uncertainty (8.2%) in ^{244}Cm inventory calculation will limit the accuracy of the predicted NDA instrument response for those whose signals are dependent on passive neutrons emitted from the fuel. The isotopes ^{235}U, ^{239}Pu, and ^{241}Pu are the primary fissile nuclides in spent fuel, and ^{240}Pu and ^{241}Am are the primary neutron absorbers. These nuclides have a significant impact on the neutron multiplication factor in spent fuel and thus on NDA neutron signals.

Figure 6 shows the relative standard deviation for a few important fission products. As shown, the relative standard deviations are within 5% for most fission products, except for ^{155}Gd, ^{154}Eu, and ^{109}Ag. The relative standard deviations for ^{134}Cs, ^{137}Cs, and ^{154}Eu, the three important gamma-emitting nuclides, are 0.2%, 4.3% and 7.7%, respectively. Uncertainties in fission products will also affect NDA neutron signals because some of the fission products have large neutron absorption cross sections, including ^{133}Cs, ^{143}Nd, ^{149}Sm, ^{154}Eu, and ^{155}Gd, some of which have relatively large uncertainties such as ^{155}Gd (5.3%).

5. Impacts on NDA instrument responses

While the impact of nuclear data uncertainties on the spent nuclear fuel nuclide contents is important, ultimately for nuclear safeguards purposes it is the net effect of the nuclide uncertainties on the instrument response that is required. CIPN is one of the advanced NDA instruments developed under the NGSI-SF project that is being used in field tests [2]. CIPN was selected to evaluate the impact of uncertainties for this study because its neutron detection capability extends across the entire fuel assembly (interior and periphery rods).

CIPN is a relatively low-cost and lightweight instrument that resembles a Fork detector [13], except that CIPN has an active interrogation source (^{252}Cf). CIPN shows promising capability for determining fissile content and detecting diversion of fuel rods in spent nuclear fuel assemblies [7]. Figure 7 shows the cross-sectional views of the CIPN instrument at two axial levels: Z = -3 cm and Z = 3 cm (the center of the assembly is set at Z = 0). As shown, there are four fission chambers in the instrument to detect neutrons and two ion chambers to detect photons. CIPN can operate in both passive and active modes. In the passive mode, the californium source is not present, and the neutrons and photons emitted from the spent fuel assembly itself are measured. In the active mode, the californium source is placed in proximity to the assembly. The neutrons emitted from the californium source will induce fissions in the fuel, and these fission neutrons will add to the neutron signal in addition to the passive neutrons. The difference in neutron counts between the active and passive mode, or the net neutron count, is related to the neutron multiplication factor of the assembly and thus the fissile content [7]. (For photon counts, the active mode is similar to the passive mode because addition of the active neutron source does not appreciably impact the photon counts.) The net neutron counts are mainly driven by the external neutron source (californium) and the multiplication factor, which is primarily determined by the combined effect of several fissile nuclides and neutron-absorber nuclides. In addition to the passive gamma signal, both the passive and active neutron signals have been studied in this work.

Given the high computational demand of MCNPX (version 2.6.0) simulation, only 20 detector simulation calculations were performed for this study. These 20 sets of assembly nuclide concentrations based on the perturbed nuclear data libraries, a subset of the 120 samples used to analyse the variance in the spent fuel compositions, were applied in the MCNPX model used to simulate uncertainties in the CIPN count rates. These assembly nuclide concentrations can also be applied to test any other NDA instruments using different MCNPX models. Figure 8 shows the relative percent difference between the passive gamma count rates for each of the 20 perturbed cases from that of the reference case (in which the nuclear data were not perturbed). For the relatively long cooling time (5 years) used, ^{137}Cs and ^{154}Eu are the main gamma sources. As shown, the uncertainties in nuclear data introduce an average uncertainty in the CIPN passive gamma count rates of 1.5% (relative standard deviation). Figure 9 shows the uncertainty in the passive neutron count rate, dominated by ^{244}Cm. The average uncertainty in the CIPN passive neutron count rates is 8.2%, which is similar to that of ^{244}Cm, as shown in Figure 5. The nuclear data uncertainties have a larger impact on passive neutron count rates than gamma count rates, because ^{244}Cm is more sensitive to nuclear data uncertainties than ^{137}Cs.

The net neutron count rate can be obtained by subtracting the passive count rate from the active count rate. Figure 10 shows the percent difference of the net neutron count rate of the samples from that of the reference case. As shown, the nuclear data affect the CIPN net neutron count rates with a standard deviation of about 1%. The CIPN net neutron count rate is mainly driven by the multiplication of the assembly, which is defined by the geometry and the

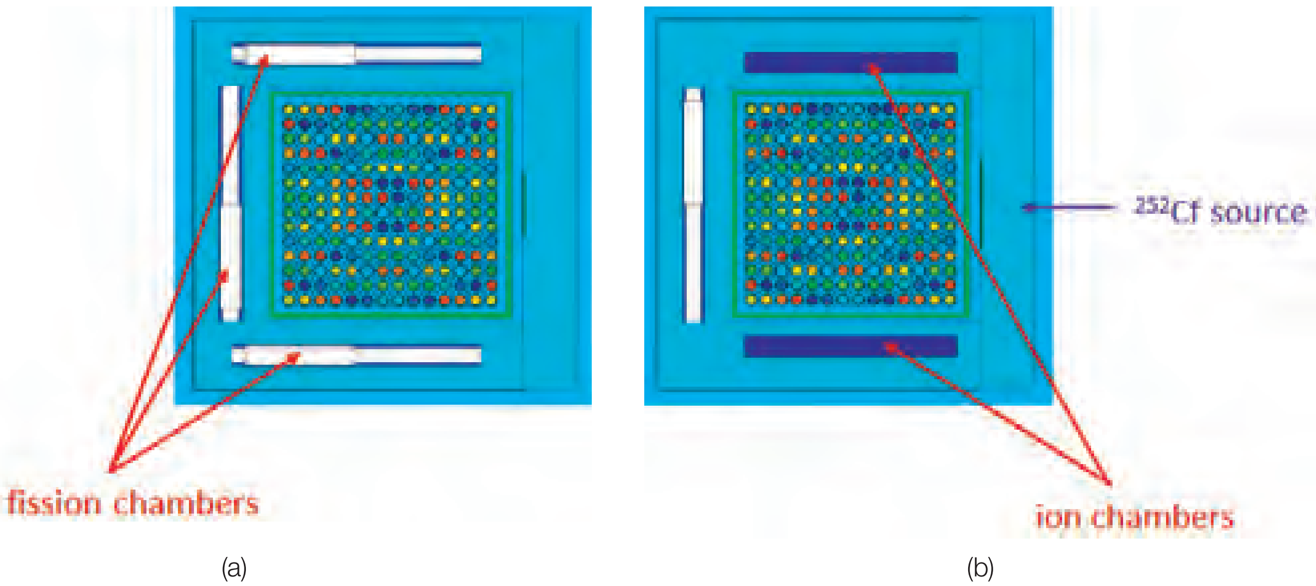


Figure 7: Cross-sectional views of the CIPN instrument at two axial levels: (a) Z = -3 cm; (b) Z = 3 cm.

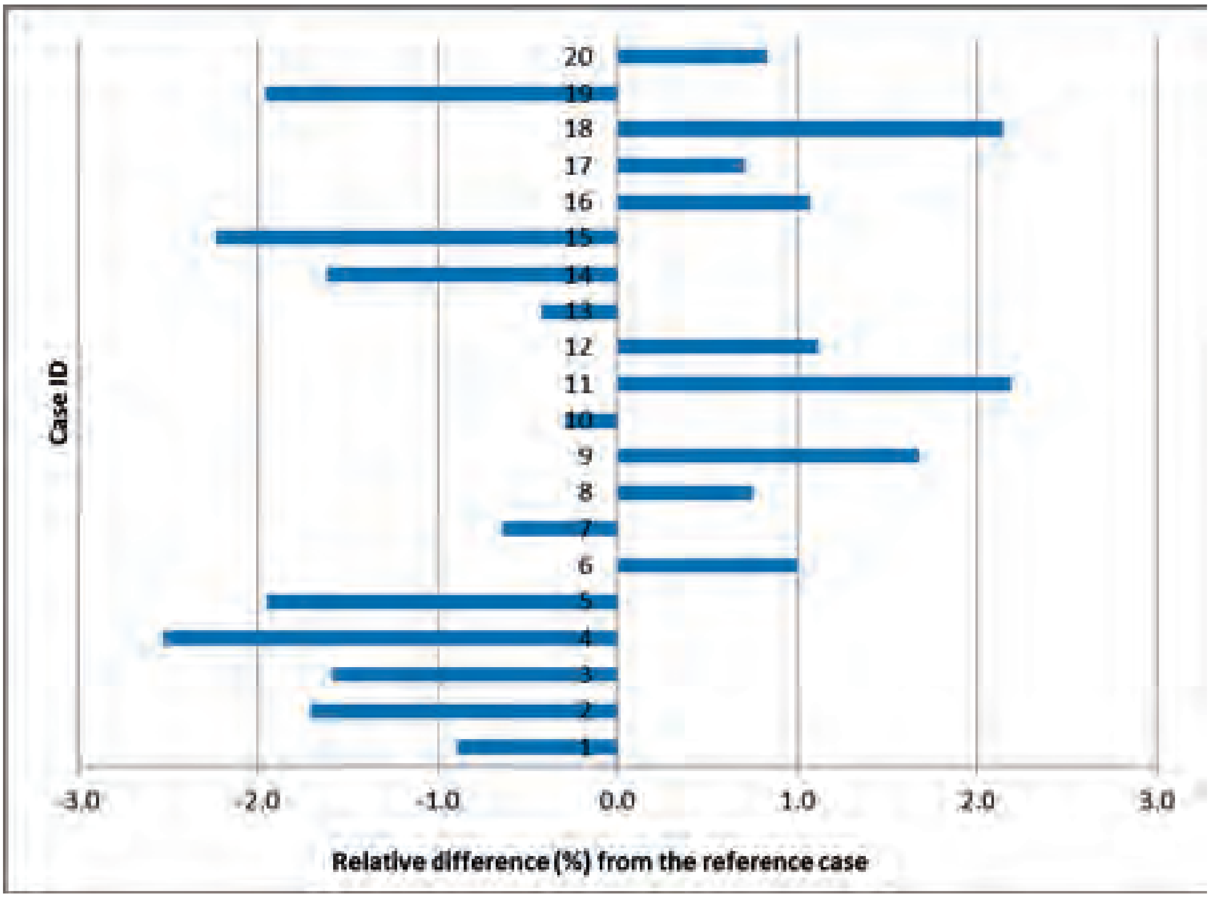


Figure 8: Relative difference of the CIPN passive gamma count rate of the samples from that of the reference case.

concentrations of the major actinides and fission products in the fuel. The relatively low impact on net neutron count rate is consistent with the small standard deviations found in the major fissile nuclides (e.g., ^{235}U and ^{239}Pu) and major actinide neutron absorber (e.g., ^{240}Pu), as shown in Figure 5.

6. Summary and conclusions

This work has examined the impact of nuclear data uncertainties on nuclide concentrations in spent fuel and the resulting NDA response of the CIPN instrument. Uncertainties in the nuclide concentrations were estimated based on burnup calculations using 120 sets of perturbed nuclear data libraries generated with stochastic sampling of covariance data. The resulting nuclide concentrations in each case were compared to that of the reference case, in which the nuclear data were not perturbed. To study the impact on the CIPN instrument response, a subset of 20 perturbed sets of assembly nuclide concentrations was imported into the MCNPX model to simulate the uncertainties in the CIPN count rates.

Analysis of the uncertainties is important to the NGSI project because modelling and simulation of the spent fuel assembly concentrations have been extensively used to predict instrument performance, and spent fuel calculations will be required for instrument calibration. The uncertainties in the nuclear data used by the codes represent the minimum uncertainties that can be realistically expected due to limitations in the accuracy of the basic nuclear data used in the simulations. An alternate and more direct approach to the determination of bias and uncertainties associated with the modelling and simulation would be by experimental benchmarking. However, in the case of the new advanced NGSI instruments, there is a lack of destructive analysis measurements of the spent fuel assembly compositions for the measured assemblies, and thus no such benchmarks exist. The quantification of uncertainties associated with the nuclear data used by the codes represents one option for NDA system uncertainty analysis.

The impact of nuclear data uncertainties on the concentrations of major plutonium isotopes in spent fuel is estimated to be approximately 1%, and the impact on most other actinides is less than 3%. For ^{244}Cm, the most important source of passive neutrons in spent fuel, the uncertainties are greater (~8%). Uncertainties in calculated concentrations for most fission products are within 5%. The uncertainties for ^{134}Cs, ^{137}Cs, and ^{154}Eu, the three important gamma-emitting nuclides, are 0.2%, 4.3% and 7.7%, respectively. Uncertainties in fission products will also affect NDA neutron signals because some of the fission products have large neutron absorption cross sections, including ^{133}Cs, ^{143}Nd, ^{149}Sm, ^{154}Eu, and ^{155}Gd, some of which have relatively large uncertainties such as ^{155}Gd (5.3%).

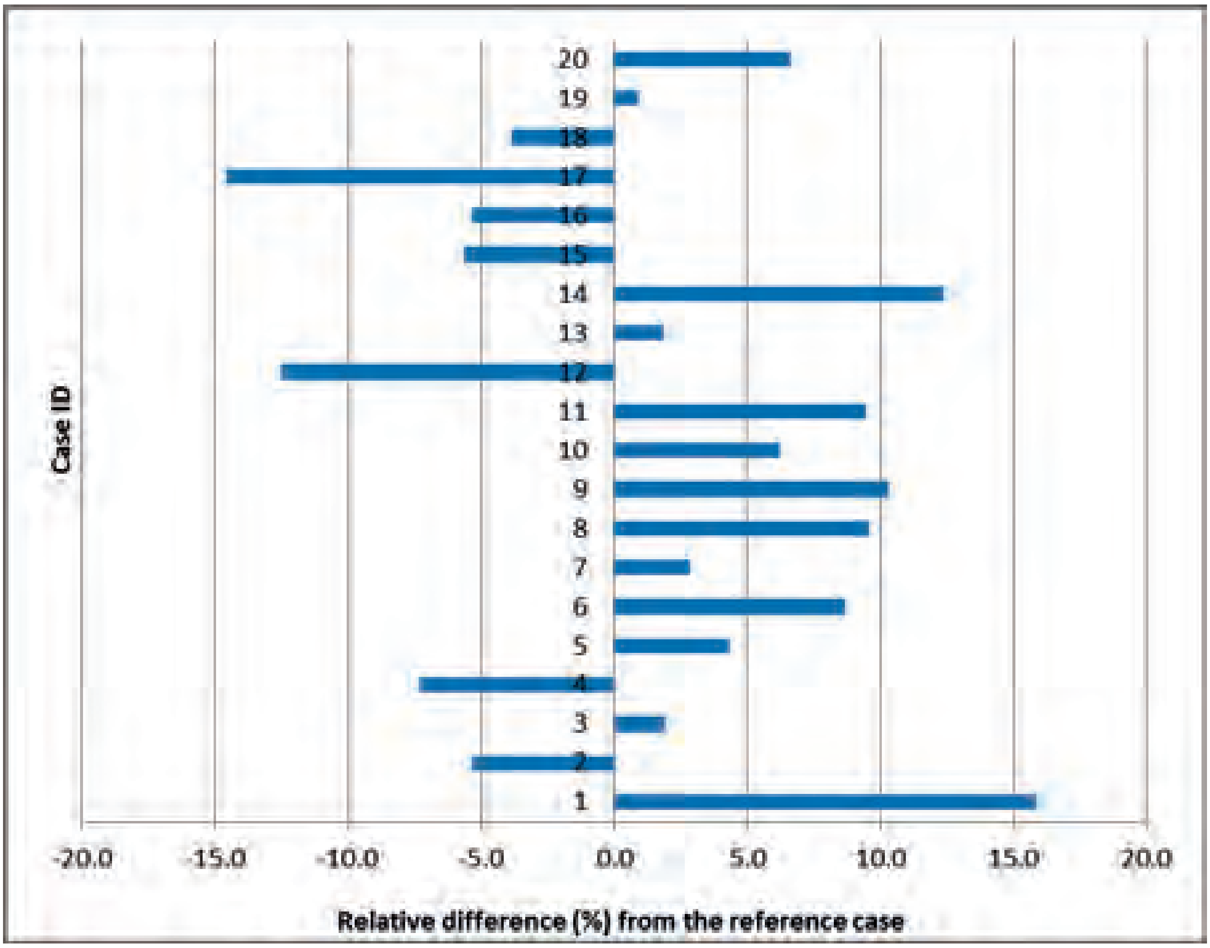


Figure 9: Relative difference of the CIPN passive neutron count rate of the samples from that of the reference case.

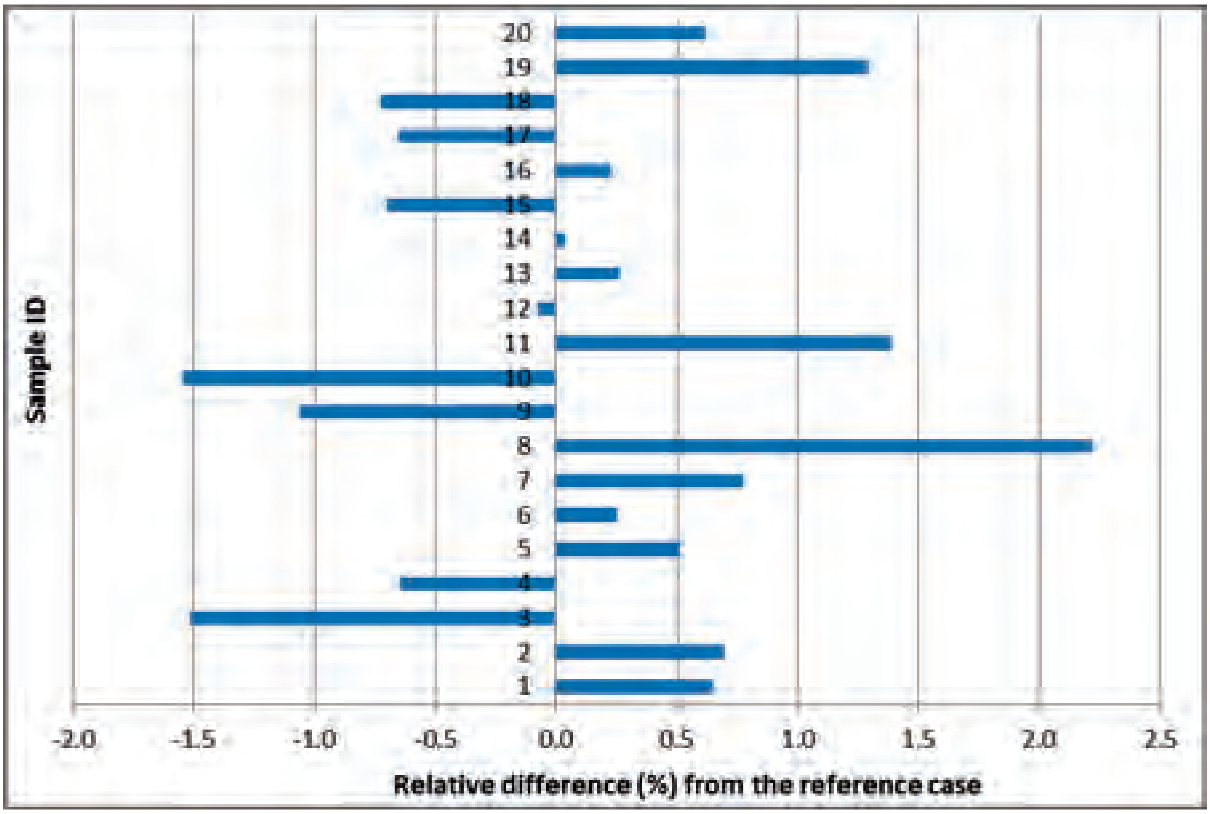


Figure 10: Relative difference (%) of the CIPN net neutron count rate of the samples from that of the reference case.

The impact on the CIPN passive neutron count rates were the largest (~8%), followed by passive gamma (~1.5%), and net neutron (~1%). The sensitivity of other NDA instruments to nuclear data will vary due to the different responses of the instruments. The assembly nuclide concentrations generated based on the perturbed nuclear data can be used to study the sensitivity of other NDA instruments. This work provides quantitative assessments of the nuclear data uncertainties on nuclide concentrations in spent fuel and also on NDA instrument responses. These values provide a realistic assessment of the impact of nuclear data uncertainties on instrument performance, and represent the expected minimum level of uncertainty in many cases since these uncertainties exclude other sources of uncertainty associated with the NDA measurements.

Finally, in addition to the assessment of total uncertainties in the modelling and simulation due to nuclear data, the methods described in this work may also be applied to evaluate the impact of different types of nuclear data and specific nuclides on the application. Such an approach may be useful to identify specific areas where improved nuclear data would result in lower uncertainties in the advanced NDA instrument performance.

7. Acknowledgments

This work is supported by the Next Generation Safeguards Initiative, Office of Nonproliferation and International Security, National Nuclear Security Administration. The authors thank Kang Seog Kim of ORNL for the guidance of using Sampler. The authors would like to acknowledge all those who have reviewed these guidelines and contributed to their completion.

This manuscript has been authored by the Oak Ridge National Laboratory, managed by UT-Battelle LLC under Contract No. DE-AC05-00OR22725 with the US Department of Energy. The US Government retains and the publisher, by accepting the article for publication, acknowledges that the US Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US Government purposes.

8. References

[1] M. A. Humphrey, S. J. Tobin and K. D. Veal, “The Next Generation Safeguards Initiative’s Spent Fuel Nondestructive Assay Project,” *Journal of Nuclear Materials Management,* vol. 40, no. 3, p. 6, 2012.

[2] S. J. Tobin, H. Menlove, M. Swinhoe, H. Trellue and M. Humphrey, “Prototype Development and Field Trails under the Next Generation Safeguards Initiative Spent Fuel Non-Destructive Assay Project,” in *Proc. of ESARDA 35th Annual Meeting,* Bruges, Belgium, 2013.

[3] J. F. Pelowitz (editor), *MCNPX User’s Manual, Version 2.6.0*, Los Alamos National Laboratory report, LACP-07-1473, 2008.

[4] S. M. Bowman, “SCALE 6: Comprehensive Nuclear Safety Analysis Code System,” *Nucl. Technol*. **174**(2), 126-148, May 2011.

[5] J. Hu, I. C. Gauld, J. Banfield, and S. Skutnik, *Developing Spent Fuel Assembly Standards for Advanced NDA Instrument Calibration – NGSI Spent Fuel Project*, Oak Ridge National Laboratory report, ORNL/TM-2013/576, February 2014.

[6] M. L. Williams, F. Havluj, D. Wiarda, M. Pigni, and I. C. Gauld, “SCALE Uncertainty Quantification Methodology for Criticality Safety Analysis of Used Nuclear Fuel,” Proceedings of the American Nuclear Society, *NCSD 2013 – Criticality Safety in the Modern Era: Raising the Bar,* Wilmington, NC, September 2013.

[7] J. Hu, S. Tobin, H. Menlove, D. Henzlova, J. Gerhart, M. Swinhoe and S. Croft, “Developing the Californium Interrogation Prompt Neutron Technique to Measure Fissile Content and to Detect Diversion in Spent Nuclear Fuel Assemblies,” *Journal of Nuclear Materials Management,*vol. 40, no. 3, pp. 49-57, Spring 2012.

[8] M. B. Chadwick et al., “ENDF/B-VII.1 Nuclear Data for Science and Technology: Cross sections, Covariances, Fission Product Yields and Decay Data,” *Nuclear Data Sheets* **112** (12), 2887, December 2011.

[9] M. B. Chadwick et al., “ENDF/B-VII.0: Next Generation Evaluated Nuclear Data Library for Nuclear Science and Technology,” *Nuclear Data Sheets* **107** (12), 2931, December 2006.

[10] R. C. Little, T. Kawano, G. D. Hale et al., “Low-Fidelity Project,” *Nuclear Data Sheets* **109** (12), 2928, 2008.

[11] T. R. England and B. F. Rider, *ENDF-349 Evaluation and Compilation of Fission Product Yields*, Technical Report LA-UR-94-3106, Los Alamos National Laboratory, 1994.

[12] B. Krzykacz, E. Hofer, and M. Kloos, “A Software System for Probabilistic Uncertainty and Sensitivity Analysis of Results from Computer Modelsk,” Proc. International Conference on Probabilistic Safety Assessment and Management (PSAM-II), San Diego, CA, 1994.

[13] D. Reilly, N. Ensslin, H. Smith Jr., Sarah Kreiner, “*Passive Nondestructive Assay of Nuclear Materials*”, LA-UR-90-732, *p.551-554* (1991).

Managing threats from emerging technologies: can safeguards show the way?[1]

Teri N. Leffer

Independent Researcher
Owings Mills, MD, USA
E-mail: westerfeldt@msn.com

Abstract:

The system of international nuclear safeguards implemented by the International Atomic Energy Agency (IAEA) is primarily a means of verification of states' commitments under various legal instruments, principally the Nuclear Non-Proliferation Treaty (NPT), to utilize controlled nuclear fission for peaceful purposes only. However, the safeguards system can also be seen as a mechanism through which states acted to reduce the threat posed by a new technology that had a transformative impact on existing national security paradigms when it emerged in the twentieth century. In the twenty-first century, new technologies with equally profound national security implications are emerging. These include biotechnology and synthetic biology, nanotechnology, information technology, cognitive science, robotics and artificial intelligence. Throughout its history, the safeguards system has evolved to accommodate new technologies, new undertakings and new threats. Because multiple emerging technologies now constitute potential national security threats, it is appropriate to consider whether and how the lessons and successes of the safeguards system, including its capacity to evolve in response to changing requirements, could be leveraged to mitigate the threat posed by these new technologies. This paper addresses the possibility of re-imagining safeguards in a way that makes them applicable to a broader range of technology-based threats without compromising their effectiveness for their original purpose.

Keywords: emerging technologies; national security; molecular manufacturing; robotics; synthetic biology

1. Introduction

The system of international nuclear safeguards implemented by the International Atomic Energy Agency (IAEA) is primarily a system of verification. Safeguards verify that a dual-use technology (controlled nuclear fission) is not being used for other-than-peaceful purposes in accordance with the terms of certain international legal instruments, most importantly the Nuclear Nonproliferation Treaty (NPT). However, safeguards can also be viewed more broadly as a mechanism for mitigating the threat associated with the existence and spread of a new technology that had a transformative impact on national security when it emerged in the mid-20th century.

In the early 21st century, a variety of new technologies are emerging that are poised to drastically disrupt existing national security paradigms in the same way that controlled nuclear fission did in the 20th century. These technologies are, for the most part, still in the early stages of development and are possessed by a relatively small number of states, but their perfection, dissemination and use are inevitable. How can the international community best mitigate the national security risks posed by these technologies while allowing states to reap the benefits of their peaceful application?

Throughout its history, the IAEA safeguards system has evolved to accommodate new technologies, new undertakings and new threats. Because multiple emerging technologies now constitute potential national security threats, it is appropriate to consider whether and how the lessons and successes of the safeguards system, including its capacity to evolve in response to changing requirements, could be leveraged to mitigate these new threats. This paper addresses the possibility of re-imagining safeguards in a way that makes them applicable to a broader range of technology-based threats without compromising their effectiveness for their original purpose.

Safeguards: Unique or Replicable? The nuclear nonproliferation regime[2] restricts the behavior of participating states with respect to their use of the technology of controlled nuclear fission. States consent to such restriction in exchange for access to nuclear technology and the benefits of its peaceful application. Safeguards are the mechanism by which states' compliance with their commitment to use nuclear technology only for peaceful purposes is verified. The success of any multilateral control regime for a dual-use technology can be assessed by multiple

[1] The concepts, analyses, opinions and policy options presented in this paper are those of the author and do not in any way represent policy of the United States government or any U.S. government department or agency.

[2] For purposes of this analysis, the nuclear nonproliferation regime is considered to consist of the Nuclear Nonproliferation Treaty (NPT), mandatory safeguards agreements entered into by non-nuclear weapons states parties to the NPT, voluntary safeguards agreements entered into by nuclear weapons states, associated export control regimes (e.g., the Zangger Committee and the Nuclear Suppliers Group) and associated resolutions of the United Nations Security Council (e.g., UNSCR 1640).

factors, including: the degree of state participation in the regime; the regime's duration; the existence and effectiveness of a verification system for the regime; the frequency with which the regime has been successfully circumvented; the extent to which the controlled technology has proliferated despite regime restrictions; and the frequency with which the controlled technology has been used for other-than-peaceful purposes since the regime's entry into force. By these measures the IAEA safeguards system, more than fifty years after its inception, still constitutes one of the most successful example to date of a multilateral system for the management of national security risk from a dual-use technology. Safeguards are applied in virtually all states that use nuclear material and have been accepted to such an extent that they can now legitimately be considered to constitute an international norm.

The success enjoyed by the IAEA and by the international safeguards system is attributable for the most part to the political environment that pertained during the decades after controlled nuclear fission emerged as a mature technology. This environment generated the political will that was necessary for the creation of the nuclear nonproliferation regime, including safeguards, and for its effective implementation up to the present day. But is political will alone sufficient to support an effective verification regime for a dual-use technology? The existence of well-subscribed international agreements for the control of other dual-use technologies that lack a corresponding verification mechanism (the Biological and Toxin Weapons Convention being the foremost example) suggests that there are separate thresholds for each component: in other words, the political will that is sufficient to generate a broadly-subscribed multilateral agreement for control of a given technology may not be enough to establish an effective verification mechanism for that agreement. This is due, in part, to the technology's inherent characteristics, which play a major role in either facilitating or thwarting the creation of an effective verification system for any such agreement. They can be a headwind against which the verification system must continually push, or a tailwind that helps propel it to success. If this is the case, then the IAEA safeguards system owes at least some of its success to aspects of the technology of controlled nuclear fission itself, aspects which may or may not pertain to other technologies for which international control regimes have been or will be established. If so, then it would be useful to identify those characteristics of controlled nuclear fission which made it amenable to an effective verification system and to determine whether any of the emerging technologies of the early 21st century exhibit those same characteristics. To the extent that they do, these technologies may be good candidates for a treaty-based international control regime incorporating a safeguards-like system of verification.

Evaluating the potential of emerging technologies to support a system of verification and controls similar to IAEA safeguards requires a brief digression into the origin, development and impact of new technologies. We may then return to the discussion of whether and how the principles and techniques of safeguards may be applied to these technologies.

2. Characterizing technologies for inherent safeguardability

Technologies can be characterized in any number of ways: according to their stage of development, their degree of dissemination and adoption, their economic and societal impact, and so forth. For purposes of assessing the amenability of technologies to a verification system, it is useful to characterize them according to three attributes:

Applicability. Does a technology have only a few realized or potential applications, or a very large number of applications? Technologies that are more generally applicable spread rapidly throughout the economy and society and are therefore harder to control, all other factors being equal. The applicability of technology can be described along a continuum from those which have only a few uses, such as hydraulic fracturing technology used by the oil and gas industry, to those which have near-universal applicability, such as writing and agriculture (see Figure 1).

Technologies which have the broadest applicability are called *general-purpose technologies* or GPTs. A GPT is a new method of producing and inventing that is significant enough to have a deep and protracted impact on the economy and on society as a whole. A GPT is pervasive, improves over time (thereby lowering its cost to users) and makes it easier to invent or produce new products or processes.[3] Experts differ in their assessment of which technologies constitute GPTs, but it has been suggested that over the course of human history there have been only twenty-four technologies that can be classified as true GPTs, among them the domestication of plants and animals, the wheel, writing and the internet.[4]

Cost. How expensive is it to develop, acquire and use a particular technology? The cost of a given technology plays a part in that technology's attractiveness versus alternatives and helps to determine the speed and extent of its spread. Technologies which are inexpensive to use, even if the initial development and acquisition costs are high, are more attractive and should, on balance, be harder to safeguard than technologies that are costly to acquire and that remain costly to use relative to their alternatives.

[3] See Philippe Aghion and Steven N. Durlauf, eds., *Handbook of Economic Growth, Volume 1B.* Elsevier, 2005.

[4] The technology of controlled nuclear fission does not meet the generally accepted criteria for a GPT, which are: 1) it presents as a single, recognizable generic technology; 2) it has much scope for improvement initially but comes to be widely used across the economy; 3) it has many different uses; and 4) it creates many spillover effects. See Lipsey, Richard; Kenneth I. Carlaw and Clifford T. Bekhar, *Economic Transformations: General Purpose Technologies and Long Term Economic Growth.* Oxford University Press, 2005, pp. 131–218.

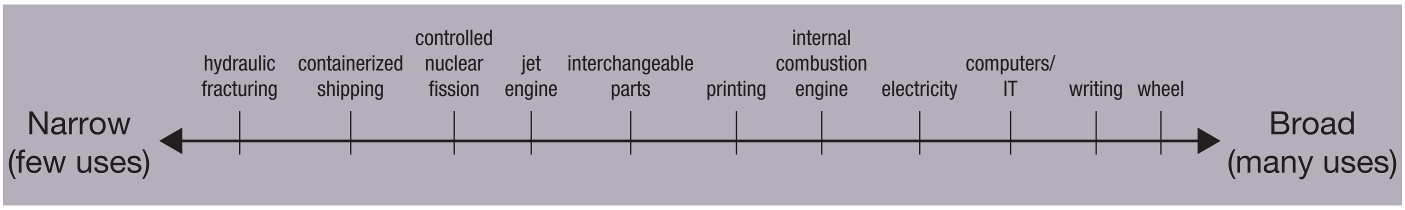


Figure 1: Spectrum of technology applicability

The very high initial cost of controlled nuclear fission (i.e., the cost to acquire nuclear material) contributes substantially to its safeguardability. The fact that acquiring nuclear material is the most costly and difficult element of the technology is one of the reasons why nuclear material serves as the leverage point for the majority of safeguards techniques, which are designed to account for material and detect its diversion.

Complexity. Are applications of the technology usable by non-specialists, or is some sort of training required in order to use them? If the latter, how difficult is it to master? Technologies that are accessible to anyone should be harder to control than those which are highly complex and require a specialized skill set in order to use. The use of controlled nuclear fission, regardless of whether it is being applied for power generation, propulsion, weapons, source production, or any other application, requires specialized training and is therefore inherently more safeguardable than a technology which is usable by anyone without the need for any sort of prior training.

With these three criteria, it is possible to construct a representation of the "technology space" for safeguards which can help to categorize technologies and identify those which are the most or least amenable to a safeguards-like system of verification and control (see Figure 2). All other factors being equal, the easiest technologies to safeguard should be those technologies that have only a few applications and are therefore not widely dispersed throughout society and the economy, have a high cost barrier to their acquisition and use, and have a high complexity barrier to their use. Controlled nuclear fission satisfies all of these conditions and is therefore a technology with a high inherent safeguardability. The most difficult technologies to safeguard, again assuming all other factors are equal, should be those technologies that have many actual or potential applications, are inexpensive to acquire and use, and which require no specialized training for their use. General-purpose technologies typically satisfy all three of these criteria, making them inherently difficult to safeguard.

Emerging Technologies. Emerging technologies constitute significant technological advances that render accessible far-reaching innovations in their respective fields. Emerging technologies can be categorized according to their degree of development. Many organizations use the concept of *technology readiness level* (TRL) to characterize emerging technologies. This paper characterizes technologies according to the U.S. Department of Energy TRL system, which recognizes nine levels of technological maturity (see Figure 3). For purposes of this study, which attempts to place emerging technologies into a political and

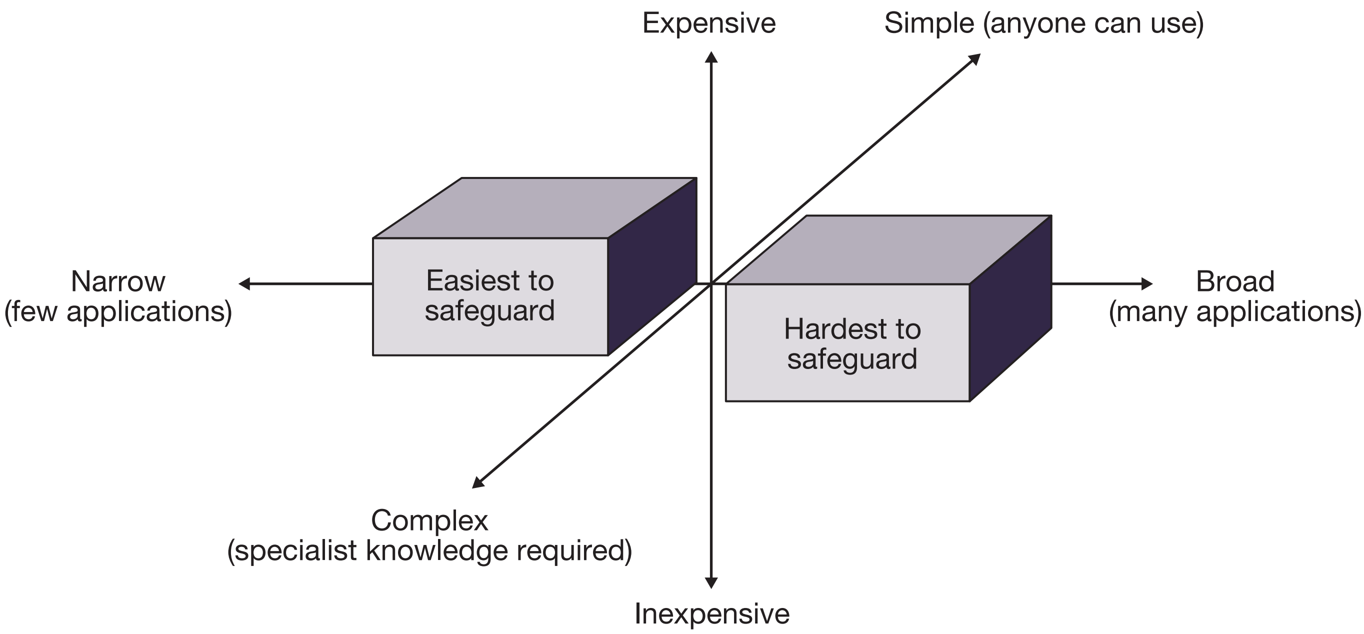


Figure 2: Inherent safeguardability of technologies

national security context rather than a purely scientific one, a technology is considered to be emerging — that is, becoming feasible to the point where governments must begin paying attention to potential consequences of its applications — when it reaches TRL 7 (a prototype of the technology is at or near the level of the planned operational system). A technology is considered to have fully emerged when it reaches TRL 9 (actual application of the technology in its final form).

3. The technology of controlled nuclear fission

Nuclear fission and the related potential for the chain reaction were discovered in 1938, leading to concern that the Nazi government in Germany would become aware of this new physical principle and its potential to be exploited for weapons purposes. Prompted by warnings from prominent physicists, the United States began work in 1939 on what would, in 1942, become the Manhattan Project, with the goal of realizing the weapons potential of controlled nuclear fission before Germany could do so. As part of the Manhattan Project, the first controlled nuclear chain reaction was achieved at the University of Chicago in December 1942. At this point, the technology of controlled nuclear fission[5] was at approximately TRL 3 (initiation of active research and development). With the Trinity test in July of 1945, it had reached TRL 8 (technology qualified through test and demonstration). One month later, the atomic bombings of Japan marked the final emergence of controlled nuclear fission as a mature technology and demonstrated on the largest stage imaginable the catastrophic nature of the threat posed by its weaponization.

Three months after the bombings of Japan, the states that had collaborated under the Manhattan Project (the United States, the United Kingdom[6] and Canada) issued the Three State Declaration on Atomic Energy, which required effective safeguards and inspections as a precondition for access to peaceful applications of controlled nuclear fission. At this point, all three governments were considering placing atomic weapons under international control. In 1946 the United States established a Committee on Atomic Energy

Technology Readiness Level	Description
TRL 1	**Scientific research moves to applied research and development (R&D):** Lowest level of technology readiness. Examples include paper studies of a technology's basic properties.
TRL 2	**Invention begins:** Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
TRL 3	**Active R&D is initiated:** This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
TRL 4	**Basic technological components are integrated:** Technological components are integrated to establish that the pieces will work together.
TRL 5	**Fidelity of breadboard technology improves significantly:** The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include high fidelity laboratory integration of components.
TRL 6	**Model/prototype is tested in a relevant environment:** Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment
TRL 7	**Prototype near or at planned operational system:** Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment.
TRL 8	**Technology is proven to work:** Actual technology completed and qualified through test and demonstration.
TRL 9	**Actual application of technology in its final form:** Technology proven through successful operations.

Figure 3: Technology Readiness Levels in the U.S. Department of Energy

5 For purposes of this study, the development of the technology of controlled nuclear fission refers to its first application (weaponization) rather than to power generation, propulsion or other subsequent applications.

6 The United Kingdom was initially reluctant to collaborate with the United States on atomic research since its own atomic project, code named Tube Alloys, was more advanced than the U.S. program and the British were loath to share their technological lead. Only after it became clear that the U.S. research effort was poised to surpass that of the U.K. was an offer to collaborate forthcoming. The U.S., having taken the lead in atomic research, subsequently restricted the flow of information to the British in order to prevent the U.K. from being able to build its own atomic weapons after the war. This episode is instructive as to how states are likely to approach the prospect of sharing control over any newly emerging technology.

that was charged with identifying a workable international arrangement that would promote the peaceful uses of controlled nuclear fission while preventing its weaponization. The committee's final report, which became known as the Acheson-Lilienthal Report, acknowledged the inevitable spread of the new technology and recommended creating a system of international control to govern its use.

Later that year, the newly-created United Nations Atomic Energy Commission began to discuss how an international control system for nuclear technology might be set up. The plan put forward by the United States (known as the Baruch Plan after Bernard Baruch, the U.S. representative to the Commission), called for centralized international control over nuclear technology and nuclear material production. But the Soviet Union, which by then was working on its own bomb, was unwilling to accept the establishment of an international control authority for atomic weapons and technology before the United States had relinquished its own atomic weapons. Thus, the notion of centralized international control over nuclear technology arrived stillborn into an as-yet unproliferated world in which a single state held a monopoly on the new technology that other states were determined to break. This took place in 1949 with the first Soviet nuclear test. The United Kingdom followed with its own test in 1952, and in 1953 the first commercial application of nuclear energy was realized as construction began on the Calder Hall nuclear power reactor in the United Kingdom. Collectively, these developments gave fresh impetus to the search for a workable means of international management of nuclear technology, and the result was President Eisenhower's "Atoms for Peace" proposal issued later that year. That proposal initiated the negotiation of the IAEA statute, which led to the establishment of the IAEA and its initial system of safeguards in 1957.

Characteristics of controlled nuclear fission. In retrospect, several aspects of the technology of controlled nuclear fission and the context in which it developed to maturity stand out as being significant for the eventual establishment and continuing success of the multilateral system of controls for that technology as constituted by the IAEA and the system of international safeguards.

Inherent characteristics. The technology of controlled nuclear fission has a number of inherent characteristics that make it amenable to a system of safeguards designed to restrict its use to peaceful purposes. It has a narrow range of potential applications; it has an obvious weapons application; its use requires specialist knowledge and training; it is dependent on a critical material that is difficult and expensive to acquire and hard to acquire clandestinely; and it exhibits a number of natural leverage points for controls.

Applicability. The most widely-applicable technologies are the general purpose technologies, which have so many applications that they come to permeate the economy and society as a whole. In many ways, nuclear technology is the opposite of a general-purpose technology, which makes it ideally suited to safeguards. Since its emergence in 1945, controlled nuclear fission has had only a handful of applications: the generation of electric power, the creation of isotopes for medical purposes, naval propulsion, and the fabrication of extremely powerful explosive devices.[7] There have been attempts to find other applications for controlled nuclear fission — for example, the U.S. and Soviet atomic demolition munitions programs and the U.S. Air Force's Nuclear Energy for the Propulsion of Aircraft (NEPA) program — but in each case nuclear technology proved to be less suitable than the available alternatives. The relatively narrow range of applications for nuclear technology is a key factor in its amenability to multilateral controls on its use.

When considering applicability, there is one application which outweighs all others: the potential for the new technology to be used as a weapon. The *raison d'être* for international management of controlled nuclear fission is to prevent states from using the technology to acquire weapons. An emerging technology that lacks an obvious weapons application is unlikely to find itself the subject of a drive to establish international control over its use. Another critical element is the actual or imminent realization of commercial uses for the new technology. The fact that the Calder Hall atomic power plant was already under construction by 1953 was a significant factor leading to the adoption of the IAEA statute in 1957. Thus, questions we should ask with respect to an emerging technology's applicability include:

- Is the new technology a general-purpose technology?
- How broad is the range of potential applications for the new technology?
- Do the actual or potential applications of the new technology include weapons that are novel or that are of significantly greater military utility than existing weapons?
- Are there existing or imminent commercial applications for the new technology at the time of its emergence?

Complexity. The complexity of a new technology's applications[8] plays an important part in determining the speed with which the technology spreads throughout society as well as the new technology's attractiveness relative to alternatives. Complexity manifests itself practically as a skill barrier that must be overcome in order to use the various applications of a technology. For example, the skill barrier to using the applied technology of language (learning to read and write) is surmountable by most people in early childhood.

[7] Although there are other uses for nuclear technology apart from these principal ones (for example, nuclear technology is used in blood irradiators, has been used as part of insect eradication programs, etc.), these uses are too few and too specialized to constitute a serious obstacle to the establishment of an international system for control over nuclear technology.

[8] It is the complexity of a new technology's applications, and not that of the technology itself, which constitutes the barrier to its use and spread. It isn't necessary to know how to construct an internal combustion engine in order to operate a motor vehicle, nor does one need a thorough understanding of hydraulics to be able to flush a toilet.

Likewise, the skill barrier to using the applied technology of the internal combustion engine (learning to drive) is also readily surmountable by most people. In contrast, the skill barrier to using the applied technology of heavier-than-air aircraft (learning to fly an airplane) is surmountable by fewer people, while the skill barrier to using controlled nuclear fission in any application (power generation, propulsion, weapons) is surmountable by still fewer people. For any emerging technology, then, a key factor affecting its safeguardability is the complexity of its application:

- Are applications of the new technology accessible to anyone who wishes to use them with little or no training, or is specialized training required? If so, how high a barrier does that specialized training constitute?

Cost. The context in which controlled nuclear fission was developed into a mature technology was the Manhattan Project. The research effort that would become the Manhattan Project began modestly in 1939 but grew into a massive state-sponsored effort that employed more than 130,000 people and cost nearly $2 billion (equivalent to about $26 billion today).[9] The effort required the construction of two enormous physical plants (the uranium enrichment facility at Oak Ridge and the plutonium production facility at Hanford) and a secret city in New Mexico to turn the products of the Oak Ridge and Hanford facilities into weapons. Over 90% of the cost of the Manhattan Project was for construction of factories and the production of fissionable materials, with less than 10% for the development and production of the weapons themselves.[10] The return on this unprecedented effort was the evolution of controlled nuclear fission from TRL 3 to TRL 9 in a span of only three years. The expense and logistical difficulty of producing fissionable materials clearly constitutes a formidable barrier to acquiring nuclear technology. For newly-emerging technologies, key questions related to cost are:

- Is the technology or its critical component expensive to acquire relative to its alternatives?
- Do the costs of the technology diminish significantly once the initial infrastructure or material investment has been made?

Leverage points for controls. The technology of controlled nuclear fission depends on a critical material that is difficult and expensive to obtain and whose creation requires the construction of a substantial physical infrastructure that is hard to conceal. In addition, the key material possesses a physical property (the emission of radiation) that manifests in a consistent manner, is well understood, and which can be detected remotely and measured. Each of these factors constitutes a separate leverage point that can be (and is) exploited by a system of safeguards designed to ensure that the technology is used only in acceptable ways. For emerging technologies, we may therefore ask:

- Is the technology dependent on a critical material such that the inability to create or obtain this material makes it impossible to utilize the technology?
- Does it require the construction of a large, hard-to-conceal physical infrastructure?
- Does it exhibit any physical property that can be leveraged for a system of controls (i.e., measured, detected remotely, etc.)?
- Does it incorporate any material(s) that can be reliably sampled and analyzed for evidence of prohibited activities?

Political context. Regardless of how much a technology's inherent characteristics help or hinder its safeguardability, the political environment into which the new technology emerges will determine whether, how, and how quickly an international system of controls on its use will be established. Key factors include the degree to which control of the technology is concentrated during its emergence and the existence or absence of a "demonstration effect" event involving that technology.

Concentration of control. Controlled nuclear fission was developed into a mature technology by the government of a single state, as opposed to simultaneous independent efforts undertaken by multiple states or by private entities. The work was undertaken in absolute secrecy, without the potential for either collaboration as in an academic environment or technology theft as in private industry,[11] in a wartime effort of unprecedented scope and expense as opposed to a resource-constrained academic or industry environment. At the time of its emergence, the mature technology was entirely under the control of the government of a single state. Once it had emerged, it was clear that the United States would not keep its monopoly on nuclear technology forever, that commercial applications of the new technology were imminent, and that the establishment of a system of international controls on its use was therefore in the United States' interest. Thus, important questions to ask with respect to an emerging technology include:

- Is the technology being developed exclusively by government(s) as opposed to an academic or private industry environment?
- Is the technology being developed by a single entity or by multiple entities engaged in simultaneous independent efforts?

[9] Nichols, Kenneth D. *The Road to Trinity: A Personal Account of How America's Nuclear Policies Were Made.* New York: William Morrow and Company, 1987, pp. 34-35

[10] "Atomic Bomb Seen as Cheap at Price," (http://news.google.com/newspapers?id=yuVkAAAAIBAJ&sjid=KoENAAAAIBAJ&pg=5621%2C2841878) Edmonton Journal, August 7, 1945, retrieved March 31, 2013

[11] Although Soviet spies did infiltrate the Manhattan Project, the impact of their activities on the speed with which nuclear technology spread was minimal since the principal constraint on the Soviet atomic program was a shortage of uranium ore. See Holloway, David, *Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939-1956.* New Haven, CT, Yale University Press, 1994, pp. 222-223.

- How many entities (both states and non-state actors) possess the technology at the time of its emergence?
- How many entities appear likely to possess it within the first few years after its emergence?

Demonstration effect. The political impetus for the development of an international system of controls on the use of nuclear technology benefited enormously from the demonstration effect constituted by the atomic bombings in Japan. After August 6, 1945, the existence, technical viability and destructive impact of nuclear weapons were no longer matters of conjecture or open to debate. Thus, an important factor in determining whether emerging technologies could be subject to multilateral control is whether or not the national security implications of the new technology have been publicly demonstrated:

- Has a weapon that is clearly based on the new technology been used overtly?
- Has the technology been used by terrorists?
- Has a widely-publicized accident involving the technology taken place?

The characteristics exhibited by the technology of controlled nuclear fission from the time that its development began in earnest (the startup of what would become the Manhattan Project in 1939) to the creation of a regime of controls on its use by governments (the entry into force of the IAEA statute in 1957) are summarized in Figure 4 below.

4. Emerging technologies with national security implications

Nearly every technology has national security implications ranging from the profound to the negligible, and as the twenty-first century unfolds and the rate of technology development accelerates, it is certain that the international community will be confronted with a variety of new, technologically-driven security challenges. But it is also certain that some of these new capabilities will have more immediate and more profound national security impacts than others: for example, the perfection of a technology to grow artificial meat *in vitro* would have fewer and less direct potential national security implications than would the perfection of either swarm robotics or laser propulsion. The challenge for policymakers is to identify which technologies

Emerging Technology Attributes			**Controlled Nuclear Fission (1939-1957)**
Inherent characteristics	Applicability	General purpose technology (GPT)?	No
		Broad range of potential applications?	No (weapons, power generation, propulsion)
		Existing or imminent weapons applications?	Yes (atomic bomb)
		Existing or imminent commercial application?	Yes (power generation)
	Complexity	Specialized knowledge/training required to use?	Yes
	Cost	Critical material expensive to create/obtain?	Yes (fissile material)
		Cost of technology diminishes significantly once initial investment has been made?	Yes (most expensive aspect of nuclear technology is obtaining fissile material)
	Leverage points for controls	Exhibits property that can be detected remotely?	Yes (radiation)
		Dependent on single critical component or materials?	Yes (fissile material)
		Components or materials that can be sampled and analyzed for evidence of prohibited activity?	Yes (HEU, Pu, others)
		Requires construction of large, hard to conceal physical plant?	Yes
Political context	Concentration of control	Technology developed exclusively by government(s)?	Yes
		Technology developed by a single entity or by multiple entities engaged in simultaneous, independent efforts?	Single entity (United States government)
		Number of entities possessing technology at time of emergence	One (United States government)
		Number of entities that appear likely to possess technology within first few years after its emergence	Several (Soviet Union, UK, Canada)
	Demonstration Effect	Overt weaponization?	Yes (atomic bombings of Japan)
		Terrorist use?	No
		Accident?	No

Figure 4: Emerging technology characteristics of controlled nuclear fission, 1939-1957

have the greatest potential to disrupt existing national security paradigms and then to devise and implement appropriate mitigation measures in a timely fashion.

Over the last decade, the inherent potential of new technologies to cause national security disruptions has received a great deal of attention. Multiple studies, reports and conferences have examined the national security implications of emerging technologies[12]. Taken collectively, this body of thought reveals a growing consensus as to which of the technologies that are now emerging are likely to have the most immediate and profound impact on existing national security paradigms. The technologies that are cited most frequently include nanotechnology, biotechnology, robotics, information technology, cognitive science and artificial intelligence. A consideration of all of these technologies is beyond the scope of this paper. Instead, this analysis will concentrate on four technologies that collectively represent the range of early 21st century innovation: molecular manufacturing, synthetic biology, robotics and information technology. These are the technologies which will be examined for their potential to benefit from the lessons and techniques of IAEA safeguards. The selected technologies are described briefly below, along with an assessment of their current readiness levels, their degree of dissemination, their potential national security impacts and any existing proposals for their control.

Molecular Manufacturing. Molecular manufacturing, sometimes referred to as molecular nanotechnology, is the most advanced form of nanotechnology, an emerging technology that involves the discovery and exploitation of novel behaviors and properties of materials with dimensions between 1 and 100 nanometers[13] (referred to as nanomaterials). Like the steam engine, electricity and computers, nanotechnology is a general purpose technology with the potential to drastically alter society through its impact on existing economic and social structures. When fully developed, nanotechnology holds the potential for vastly improved manufacturing processes which could make the mass production of physical objects as inexpensive as copying a computer file. The most advanced nanotechnology, so-called fourth generation nanotechnology or molecular manufacturing, will enable the chemical synthesis of complex structures by mechanically positioning reactive molecules, allowing for the assembly of nanoscale machines. Among the items that such "nanofactories" could produce would be more nanofactories, thereby multiplying exponentially the productive capacity of the technology. Once mature, the technology of molecular manufacturing will have a societal impact as profound as that of the industrial revolution but compressed into a timescale of a few years rather than six decades. Molecular manufacturing is presently in the very earliest stages of development (TRL 1), and its emergence as a mature technology is generally assessed to be several decades away.

The national security implications of molecular manufacturing include:

- cheap, easily produced nanoscale weapons and surveillance devices[14]
- small, portable nanofactories that can be easily smuggled
- desktop manufacturing of weapons and surveillance devices[15]
- use of nanomanufacturing by terrorists, both individuals and groups
- malicious release of free-range self-replicators[16]

Nanotechnology is still in its infancy and is not yet broadly disseminated. Although many states have launched nanotechnology research initiatives,[17] no government has yet offered a proposal for international controls on molecular manufacturing or on nanotechnology research or applications in general.

Synthetic Biology. Synthetic biology is a subset of biotechnology that incorporates elements of engineering to enable the design and construction of devices that use biological systems as their platform. Synthetic biology differs from genetic engineering in that it does not merely alter the DNA of existing organisms, but instead uses identified gene sequences as building blocks for the construction of

[12] See, for example, Carolyn S. Mattick, Brad R. Allenby and George R. Lucas, Jr. *Implications of Emerging Military/Security Technologies for the Laws of War*, 2012 Chautauqua Council Final Report. Additional examinations of the national security implications of emerging technologies may be found in reports of the Consortium for Emerging Technologies, Military Operations and National Security (CETMONS, http://lincolncenter-dev.asu.edu/CETMONS/) and the Center for Responsible Nanotechnology (http://www.crnano.org).

[13] By comparison, a human hair is roughly 100,000 nanometers wide.

[14] The latter are particularly problematic, since governments will make decisions under the assumption that adversaries are monitoring much of what they are doing, thereby contributing to crisis instability. "Technology and Innovation 2025," Toffler Associates, November 2008,p. 7 (http://www.toffler.com/docs/2025.pdf, accessed February 27, 2013)

[15] Desktop manufacturing is already commercially available, although not via molecular manufacturing but rather by additive manufacturing, in which successive layers of material are laid down in varying shapes according to a digital template. Desktop devices for additive manufacturing (3-D printers) can be purchased for less than USD 1,000 per unit and are capable of turning any.STL file downloaded to its software into a three-dimensional plastic object (including, to great Internet acclaim, a working handgun: http://www.forbes.com/sites/andygreenberg/2013/05/03/this-is-the-worlds-first-entirely-3d-printed-gun-photos/)

[16] When nanotechnology-based manufacturing was first conceived, a concern arose that tiny manufacturing systems might be accidentally introduced into the environment and 'eat' the biosphere, reducing it to copies of themselves (a scenario referred to as ecophagy or "grey goo"). Although it is now clear that replicating assemblers will not be used for manufacturing, grey goo remains a risk. Grey goo has essentially no military or commercial value and only limited terrorist value, but could be used as a tool for blackmail: cleaning up a single grey goo outbreak would be very expensive and might require severe physical disruption of the affected area (the nanotechnology equivalent of a radioactive "dirty bomb"). Another possible source of grey goo release is irresponsible or attention-seeking hobbyists (the nanotechnology equivalent of computer worms and viruses). Center for Responsible Nanotechnology, http://www.crnano.org/dangers.htm, accessed March 17, 2013.

[17] The United States established its National Nanotechnology Initiative (http://www.nano.gov) in 2000. Between 2001 and 2004, more than 60 countries established their own national-level nanotechnology programs (Sargent, John F. "Nanotechnology: A Policy Primer," Congressional Research Service, April 13, 2012, p. 4). However, only a few countries are acknowledged as leaders in nanotech research and development, among them the United States, Japan, Germany, South Korea and Taiwan (Hwang, David, "Ranking the Nations on Nanotechnology," *Solid State Technology*, August 27, 2010, http://www.electroiq.com/articles/stm/2010/08/ranking-the-nations.html, accessed April 30, 2013).

entirely new organisms that exhibit some desired useful combination of traits not found in nature. The process is similar to computer programming in that it involves the assembly of blocks of genetic code into sets of instructions for cellular machines. Potential applications of synthetic biology range from human health (new vaccines, pharmaceuticals and diagnostic tools) to energy (carbon-neutral alternative fuels) and the environment (organisms engineered to consume pollutants).

The accelerating development of synthetic biology is made possible by the ever-increasing speed and diminishing cost of key enabling technologies, such as DNA sequencing, gene fabrication and computer modeling of how synthetic genes will behave. Synthetic biology has progressed to the extent that it is now cheaper to synthesize a gene that it is to clone it.[18] In addition, the large and growing collection of genome databases provides a readily-accessible source of templates for the creation of new viruses at minimal cost.

Potential national security implications of synthetic biology include:

- synthesis of treatment-resistant bacteria and viruses to serve as bioweapons
- synthetic organisms designed to generate weapons-usable materials or components (e.g., explosives, propellants, etc.)
- use of synthetic organisms by terrorists
- accidental release into the environment of synthetic organisms that may prove harmful or difficult to eradicate ("bioerror" as opposed to bioterror)

Synthetic biology is a newly-mature but still evolving technology, having reached TRL 9 in 2010 with the creation of the first entirely artificial living organism.[19] Several U.S. government agencies are funding research in synthetic biology and the European Union is funding the development of a European strategy for synthetic biology, but the majority of the considerable funding being directed at this area comes from the commercial private sector. Although leadership in the research and development of biotechnology and synthetic biology is confined to a few states (with the U.S. spending by far the most money per year on R&D[20]), many states are actively pursuing synthetic biology research, including Canada, India, Israel, Japan, Korea, Slovenia and Turkey.[21] Although it is very new, the technology of synthetic biology is nevertheless widely disseminated due to the commercial nature of much synthetic biology research. The standard, interoperable pieces of DNA that are used for creating synthetic cellular machines and organisms, known as "biobricks," are already widely commercially available, accessible to anyone with an Internet connection and a credit card, and the relevant skills for creating them are known to any reasonably competent biology graduate student.[22]

Applications of synthetic biology that are expressly conceived as weapons are already prohibited under the Biological and Toxin Weapons Convention (BTWC), but the status of other weapons-related applications is murkier.[23] During the most recent BTWC Review Conference in 2012, delegates acknowledged that the speed of advances in biotechnology made review of new developments necessary on an annual basis as opposed to every five years as is now the case. As of yet, no government has offered proposals for new controls pertaining specifically to synthetic biology.

Robotics. Much attention has been paid in recent years to the emergence of unmanned and robotic weapons, in particular unmanned aerial vehicles (UAVs) or drones, as a result of their often controversial use by the United States in Iraq, Afghanistan and elsewhere. In 2001, the United States Congress set a goal for the Army, stating "…that, within 10 years, one-third of U.S. military operational deep strike aircraft would be unmanned, and, within 15 years, one-third of all U.S. military ground combat vehicles would be unmanned."[24] Unmanned and robotic systems are attractive because of their military utility: they allow combat to be conducted over a larger geographical area and reduce human casualties by keeping soldiers out of harm's way. They are capable of integrating and processing much larger quantities of information much more rapidly than a human soldier could do. They are not subject to fatigue or psychological stress. Robotic weapons also act as a force multiplier, since their deployment reduces the number of troops required for a given mission. This aspect

18 In 2007, several companies offered gene sequence synthesis up to 2,000 base pairs long for a price of about $1 per base pair and a turnaround time of less than two weeks (Pollack, Andrew, "How Do You Like Your Genes? Biofabs Take Orders," http://www.nytimes.com./2007/09/12/technology/techspecial/12gene.html?pagewanted=2&_r=1). As of May 2013, the price had dropped to less than $0.29 per base pair with a turnaround time as low as four days (http://www.genscript.com/gene_synthesis.html?src=google&gclid=CLLA7uis-rYCFcIv4A-od-B0ACQ, accessed May 3, 2013).

19 The J. Craig Venter Institute created the organism by synthesizing the entire genome of one bacterium and transplanting it into another, an undertaking that required fifteen years and $40 million. At a news conference, Venter described the new organism as "the first self-replicating species…on the planet whose parent is a computer." "First Synthetic Organism Created," http://discovermagazine.com/2011/jan-feb/02,accessed May 3, 2013.

20 Van Beuzekom, Brigette and Anthony Arundel. *OECD Biotechnology Statistics 2009*, p. 25 (http://www.biotechnologie.de/BIO/Redaktion/PDF/de/laenderfokus/suedkorea-oecd-report,property=pdf,bereich=bio,sprache=de,rwb=true.pdf, accessed May 3, 2013)

21 Caruso, Denise. "Synthetic Biology: An Overview and Recommendations for Anticipating and Addressing Emerging Risks, *Science Progress*, 2008, p. 4 http://www.bio.org/articles/synthetic-biology-overview-and-recommendations-anticipating-and-addressing-emerging-risks, accessed May 3, 2013.

22 Moreno, Jonathan D. "Synthetic Biology Grows Up," Science Progress, http://scienceprogress.org/2010/05/synthetic-biology-grows-up, accessed May 3, 2013.

23 Applications of synthetic biology that are weapons-related but not weapons themselves, such as synthetic organisms that produce explosives, could conceivably be seen as violating Article 1 of the BTWC, which enjoins signatories to neither produce nor possess microbial or other biological agents "that have no justification for prophylactic, protective or other peaceful purposes." Carlson, Rob and Daniel Grushkin, "The Military's Push to Green Our Explosives," Slate, January 19, 2012, http://www.slate.com/articles/technology/future_tense/2012/01/synthetic_biology_environmentally_friendly_weapons_and_the_biological_and_toxin_weapons_convention_.html, accessed May 5, 2013.

24 "U.S. Army Roadmap for Unmanned Systems: 2010-2035," http://www.fas.org/irp/program/collect/uas-army.pdf (September 21, 2012), p. 5, accessed May 1, 2013.

could incentivize continual increases in robotic systems' level of autonomy, since ongoing, labor-intensive human oversight would dilute the force multiplication effect. On the other hand, a robotic system has no need to protect itself and may therefore act more conservatively than a human would in making decisions regarding use of force.[25]

Most of the unmanned and robotic weapon systems that have been deployed to date are simply an extension of the soldier, meaning that a human remains in control at all times. They are capable of moving and targeting autonomously, but a human must still make the decision to fire. These systems include some types of torpedoes, Predator and Reaper UAVs, and Israel's Harpy missile.[26] However, an increasing number of robotic systems are capable of being programmed to act with varying degrees of autonomy. Such systems could, in principle, make their own decisions regarding the application of force, including lethal force. An example of such an autonomous system is iRobot's Packbot. Most models of the Packbot are capable of Tasering enemy combatants without the need for authorization from a human decision-maker, but some models are equipped with lethal weapons.[27] Other examples of potentially lethal autonomous systems include the Samsung SGR-A1 robot, which is used by South Korea to patrol the demilitarized zone at the border with North Korea, as well as the U.S. Navy's Patriot and Phalanx missiles. In practice, these systems are all presently supervised at some level by human operators and their software includes limits on which decisions can be delegated to the computer. But in principle, each of these systems could be capable of making an autonomous decision to use lethal force.

The national security implications of robotics include:

- autonomous weapons capable of making decisions to apply lethal force without a "human-in-the loop"[28]
- proliferation of lethal autonomous systems to terrorist groups
- vulnerability of lethal autonomous systems to cyber attack or hijacking

As of today, there is no technological barrier to the construction and deployment of the types of systems described above, including lethal autonomous variants. More than seventy countries now possess unmanned aerial vehicles (UAVs) and pilotless aircraft, but only five (the United States, the United Kingdom, China, Israel and Italy) operate UAVs that are armed.[29] Other types of robotic weapons systems are currently deployed by the United States, Israel, South Korea, Japan and Singapore. More sophisticated unmanned and robotic systems, such a swarm robotics, are at a much earlier stage of development and are unlikely to cross the TRL 7 threshold for decades.[30]

Proposals for international control of unmanned and robotic weapons systems have so far been confined to non-governmental organizations. In 2009, the International Committee for Robot Arms Control issued a statement calling for a treaty banning autonomous weapons, the equipping of robotic weapons with nuclear arms, and the deployment of armed robots in space, as well as national reporting on the treaty's implementation.[31] In 2012, Human Rights Watch called for all states to "prohibit the development, production, and use of fully-autonomous weapons through an international legally binding instrument."[32] In April 2013, the UN General Assembly voted to adopt the Arms Trade Treaty (ATT), which aims to constrain the flow of conventional weapons to states and organizations that threaten peace and security or engage in gross violations of human rights and humanitarian law. Advocacy groups had been pushing for the inclusion of language in the ATT that would cover emerging weapons technologies, but no specific provisions pertaining to unmanned weapons appear in the final agreement.

Information Technology. Information technology (IT) is a mature but still evolving general-purpose technology which has become ubiquitous over the last three decades and has thereby created an entirely new type of national security risk: an attack against a state that uses the state's own IT infrastructure as the delivery vehicle. Attacks that utilize IT infrastructure (cyber attacks or cyber warfare) differ from kinetic attacks in that attribution is difficult and attribution with absolute certainty is impossible, thus making both deterrence and retaliation problematic. Cyber attacks have the potential to return a great deal of information and/or create broad disruption, particularly in the realm of military C3I (command, control, communication and intelligence) for a small initial investment, all while allowing the perpetrator to remain anonymous. In a cyber conflict, states with the most advanced IT infrastructures are generally more vulnerable while states with little IT infrastructure are much less susceptible to disruption. Examples of how information technology can be used for offensive

25 Mattick, et. al., p. 16-18

26 ibid., p. 17

27 ibid.

28 Robotic weapons are often divided into three categories based on the amount of human involvement in their actions: human-*in*-the loop robots can select targets and deliver force only with a human command; human-*on*- the-loop robots can select targets and deliver force under the oversight of a human operator who can override the robot's actions; human-*out-of*-the-loop robots are capable of selecting targets and delivering force without any human input or interaction. "Losing Humanity: The Case Against Killer Robots," Human Rights Watch, November 2012, p. 2.

29 Roberts, Kristin. "When the Whole World Has Drones," *National Journal*, March 22, 2013 (http://www.nationaljournal.com, accessed May 1, 2013).

30 Swarm robotics is a research area in which large numbers of small, simple robots (a swarm or collective) are designed to work cooperatively and mimic the emergent behavior of "swarm intelligence" as exhibited by some insects. When mature, a technology of swarm robotics would have profound national security implications. However, swarm robotics is presently in the early stages of development, somewhere between TRL 2 and 3.

31 Mission statement of the International Committee on Robot Arms Control (http://icrac.net/statements/), accessed May 1, 2013.

32 "Losing Humanity: The Case Against Killer Robots," Human Rights Watch, November 2012, p. 5

military purposes include the Stuxnet attack on Iran[33] in 2010 and the Israeli Air Force bombing of the nuclear site under construction at Dayr az-Zawr in Syria in 2007.[34]

National security implications of information technology and cyber conflict include:

- attacks designed to disable or destroy a state's domestic critical infrastructure (e.g., electricity grid, power plants, dams) as well as military assets and infrastructure
- disruption of defenses prior to kinetic attack (e.g., an attack to disrupt military communications prior to a conventional attack)
- placement of "logic bombs" in the critical systems of a targeted state which may then be deterred from taking certain actions through their threatened activation

For the United States, much of the difficulty in defending against cyber attack stems from the fact that the bulk of its IT infrastructure is privately owned, thus limiting the ability of government to secure it. The U.S. government is legally constrained in its ability to help companies protect their networks, in part because of privacy issues surrounding the sharing of information between the government and the private sector.[35] While industry has assumed the responsibility to protect their systems from infiltration, in many cases the financial losses stemming from information security lapses are less than the cost of the security required to prevent such losses. There may be a "public good" aspect of cyber security in that the investment to protect electronic assets, though it would benefit everyone, is under-incentivized for individuals and corporations.[36]

The idea of an international agreement governing the use of information technology is receiving attention in multiple fora, including the United Nations, the North Atlantic Treaty Organization (NATO), and the International Telecommunications Union. The Russian Federation has proposed a binding United Nations treaty on information security that would classify "information warfare" as a crime against international peace and security. Many Western countries, including the United States, have opposed the treaty, fearing that such an agreement would endorse the concept of a governmental role in controlling expression online and would be used by authoritarian governments to repress their citizens. The United States contends that the law of armed conflict, which requires the use of proportional force and the minimization of harm against civilians, applies in cyberspace, a position that is accepted by Russia but not by China.[37]

5. Safeguarding emerging technologies

To what extent could a safeguards-like system of controls be established to reduce the national security threat posed by these technologies? Creating a system similar to IAEA safeguards for the mitigation of threats from emerging technologies requires solving two problems, one technical and the other political. The technical problem stems from the need to devise new safeguards tools that are effective for each technology. The political problem arises from the need to create political will among states for the adoption of a regime of controls that would confine the use of these technologies to peaceful applications.

Technical Challenge. To what extent do the emerging technologies of the early 21st century resemble the technology that gave us the IAEA and the international safeguards systems? Figure 5 provides a thumbnail sketch of each of the emerging technologies considered here and the degree to which they exhibit the characteristics that made controlled nuclear fission amenable to safeguards. Controlled nuclear fission possesses all of the desired technology attributes for safeguardability and therefore serves as our benchmark. Nuclear technology's high acquisition cost, narrow range of applications, high skill barrier to utilization, requirement for a large and hard-to-conceal physical plant, dependence on a single critical component, concentration of control within a single state at the time of its emergence and staggering demonstration effect collectively made, and continue to make, safeguards possible. If fissile material were inexpensive and easy to obtain, its acquisition hard to detect and the complexity barriers to using its applications low enough to be surmounted by non-specialists, nuclear proliferation would have proceeded much more rapidly and to many more entities, including non-state and sub-state groups and potentially even to private individuals. The nuclear nonproliferation regime might then more closely resemble the chemical weapons control regime, with verified destruction of existing stockpiles of nuclear weapons as a principle feature.

Unfortunately, the emerging technologies of the early 21st century for the most part bear little resemblance to controlled nuclear fission. Molecular manufacturing will be a general-purpose technology and therefore inherently difficult to subject to multilateral restrictions: its applications will be too numerous and too useful for states to want to limit their utilization of it. However, it is likely that when molecular manufacturing reaches TRL 7 its control will be concentrated within a small number of states that have invested the

33 The Stuxnet virus targeted the control systems of Siemens industrial equipment and disproportionately infected systems that were located in Iran. Stuxnet is widely assumed to have been developed by the United States and Israel as a means of delaying Iran's acquisition of nuclear weapons by disabling the centrifuges at Iran's Natanz uranium enrichment facility.

34 The Israeli government, apparently having purchased access to software "backdoors" in a Syrian radar system, allegedly disabled the system that would have alerted Syria to the incoming Israeli planes. On September 6, 2007, the Israeli force slipped past Syrian air defenses, bombed the target, and exited without further incident (see Mattick *et. al.*, p. 13)

35 "Several Nations Trying to Penetrate U.S. Cyber-Networks, Says ex-FBI Official," *The Washington Post*, April 18, 2012

36 Mattick, *et. al.*, p. 11.

37 "In U.S.-Russia Deal, Nuclear Communication System May Be Used for Cybersecurity," *Washington Post*, April 26, 2012.

Characteristic	Controlled Nuclear Fission	Molecular Manufacturing	Synthetic Biology	Robotics	Information Technology
Narrow range of applications?	**Yes**	No	No	No	No
Dependent on critical material that is difficult and expensive to obtain?	**Yes**	No	No	No	No
Requires large, hard to conceal physical plant?	**Yes**	No	No	No	No
High complexity barrier to using applications?	**Yes**	Yes (initially)	Yes	No	No
Exhibits physical property that can be detected remotely and measured?	**Yes**	No	No	No	No
Control highly concentrated at time of emergence?	**Yes**	Probably	No	No	No
Demonstration effect?	**Yes**	No	No	No	Yes

Figure 5: Characteristics of nuclear technology vs. emerging technologies

most resources into its development. To the extent that this occurs, these states could agree among themselves to subject molecular manufacturing to a system of access controls similar to IAEA safeguards, in which access to technology is made conditional upon acceptance of verified limits on its use. In contrast to molecular manufacturing, the toolkit of synthetic biology is already widely commercially available in many countries and on the Internet, making the task of safeguarding it much more challenging. Robotics is more widely disseminated still, and information technology has spread worldwide. The challenge of devising a safeguards system for these technologies and getting broad international acceptance for them would be enormous.

Adaptation of IAEA Safeguards to Emerging Technologies. Setting aside for the moment the question of whether and how an international agreement could be achieved and a corresponding verification authority established, to what extent could the principles and techniques used by the IAEA in carrying out its nuclear safeguards mission be applied productively to these technologies? Obviously, those safeguards techniques which rely on measurements of radiation will not be applicable beyond nuclear technology. However, many other IAEA safeguards principles and techniques could be transferred more or less directly from nuclear technology to emerging technologies with good effect. Figure 6 provides an overview of the potential applicability of various existing safeguards techniques to the emerging technologies that are considered here. Possible applications of (or adaptations of) established IAEA international safeguards techniques to the emerging technologies that have been considered here are outlined below.

Molecular Manufacturing. Many IAEA safeguards techniques could be adapted for the verification of an international agreement governing use of nanotechnology and molecular manufacturing:

- state self-reporting via declared facilities (this would likely require the development of a regulatory infrastructure within each participating state to register and account for desktop nanofactories owned by private entities and individuals)
- material accountancy to verify bulk quantities of nanomaterials whose production is limited by international agreements
- material sampling to verify adherence to treaty-based restrictions on size or type of nano-material (particle, machine, etc.)
- weight and volume measurements to verify restrictions on quantities of nanomaterials that may be produced in a given facility or during a specified period of time
- on-site monitoring via a permanent inspector presence at facilities in which nanotechnology or molecular manufacturing applications are used
- unattended and remote monitoring via sensors (desktop nanofactories could come pre-equipped with sensors that report to the international verification authority the type and quantity of items manufactured and which prohibit the manufacture of restricted items)
- containment, surveillance and physical protection to prevent unauthorized access to and use of nanomanufacturing devices
- environmental sampling to detect the presence of nanoparticles
- open-source information analysis to detect evidence of prohibited uses of molecular manufacturing

Synthetic biology. As with nanotechnology, an international agreement governing the uses of synthetic biology could make use of adapted versions of many IAEA safeguards techniques:

- state self-reporting via declared facilities (as with molecular manufacturing, a state-level regulatory mechanism would be needed to ensure compliance by private entities with reporting requirements)

- material accountancy to verify bulk quantities of synthetic organisms whose production is limited by international agreements
- material sampling to verify adherence to treaty-based restrictions on types of synthetic organisms
- weight and volume measurements to verify restrictions on quantities of bioengineered substances, materials or organisms that may be produced in a given facility or during a specified period of time
- on-site monitoring via a permanent inspector presence at facilities where bioengineered or synthetic organisms are created and used
- containment, surveillance and physical protection to prevent unauthorized access to biotech facilities
- environmental sampling to detect the presence of bioengineered organisms
- unattended and remote monitoring via sensors designed to detect specific engineered substances and organisms (this may require creation of an international registry of synthetic organisms)
- open-source information analysis to detect evidence of prohibited uses of synthetic biology

Robotics. Fewer safeguards techniques are applicable to a verification regime for unmanned and robotic weapons. Some, however, might have value if properly adapted:

- state self-reporting of activities involving unmanned or robotic weapons systems (a modification of declared facilities)
- item accounting of treaty-limited unmanned and robotic weapons systems
- unattended and remote monitoring of unmanned and robotic weapons to detect prohibited modifications and uses (for example, a "black box" that records the date, time and duration of each use similar to that incorporated into Tasers. Such a device built into an unmanned or robotic weapon system could not only record information about its use but also transmit information about the system's location and status to the international verification authority. Also, GPS tracking of specified unmanned or robotic systems could be used to verify compliance with treaty-based limitations on where such systems can be deployed.)
- open-source information analysis to detect evidence of prohibited activities (e.g., patent applications or software for prohibited classes of weapons)

Information technology. There appear to be no existing safeguards techniques that would be readily transferrable to verifying compliance with an international agreement on the rules of cyber warfare or the appropriate military uses of information technology. There are no materials to be measured or sampled, no items to be accounted for, and nothing to be inspected. We shall therefore need to look elsewhere for IT safeguards techniques, assuming any exist at all.

Emerging technologies themselves may open new possibilities for safeguards and verification techniques that can then be applied to any prospective regime for their control, or even to existing technology control regimes. Nanotechnology in particular offers the prospect of new tools to effectively and profoundly strengthen the nonproliferation regimes for chemical and biological weapons. Sensitive, selective and inexpensive nanotech sensors and materials could detect and bind components of chemical, biological or radiological weapons on the atomic or molecular level, due to the large surface-to-volume ratio of nanoparticles or of nanoporous material.[38] The combination of nanotechnology and robotics would seem to lend itself well to verification applications: one can envision nanoscale autonomous sensors and surveillance devices being applied for this purpose, although as previously noted, the same technology could promote crisis instability when used by governments for covert surveillance.

Political Challenge. Emerging technologies take time to develop, and this time can be used by the international community to prepare for the disruptions that the mature technologies will engender. Ideally, by the time an emerging technology has reached TRL 7, the international community should have: 1) identified and understood the risks; 2) made appropriate policy; 3) designed the necessary institutions; and 4) established these institutions, both domestically and internationally.[39] Unfortunately, this sort of advance planning is very difficult for governments to achieve in practice. Political will is finite, and governments must direct their limited supply toward addressing today's problems which usually means there is little left over to address problems that may not manifest for decades. Creating a risk-mitigation regime for an emerging technology similar to the one that has grown up around controlled nuclear fission would require an underlying international legal instrument with sufficient – and sufficiently important – state subscribers to make it matter; a normative infrastructure that develops from the agreement; an internationally-administered control authority with broad legitimacy; corresponding regulatory infrastructures in the participating states; and, in some cases, a corresponding export control regime. What sorts of conditions or incentives could create the political will that would be needed to lift such a heavy payload?

The desire for transparency surrounding states' uses of an emerging technology could conceivably create the political will necessary to establish an international agreement governing that technology. So could the desire to cement a technological advantage for a particular state or group of states, although this desire would presumably be met by a countervailing desire on the part of technology laggards

[38] Ibrugger, Lothar (rapporteur), "The Security Implications of Nanotechnology," Report of the NATO Parliamentary Assembly (179 STCMT 05 E), 2005 (http://www.nato-pa.int?Default.asp?SHORTCUT=667, retrieved December 21, 2012)

[39] "Administration Options for Molecular Manufacturing," Center for Responsible Nanotechnology, op. cit.

Safeguards Principle	IAEA Safeguards Technique	Molecular Manufac-turing	Synthetic Biology	Robotics	Info Tech.
Material Accountancy	Bulk inventory accounting techniques (material balance areas, batch accounting, key measurement points)	•	•		
	Item accounting techniques (serial numbers)	•	•	•	
State Self-Reporting	Declared facilities	•	•	•	
Non-Destructive Analysis	Radiation detection techniques (γ, neutron)				
Destructive Analysis	Material sampling	•	•		
Physical Property Measurement	Design information verification (ground penetrating radar, 3D laser range finder, ultrasonic thickness gauge)				
	Volume measurement (portable pressure measurement device)	•	•		
	Weight measurement (load cell based weighting system)	•	•		
On-Site Monitoring	Permanent inspector presence	•	•		
Unattended and Remote Monitoring	Weight, volume, temperature, flow monitoring	•	•		
	GPS tracking	•	•	•	
	Video surveillance	•	•		
	Unattended monitoring systems (including sensors for radiation, temperature, pressure, flow, vibration, optical and electromagnetic)	•	•	•	
Containment	Single use seals (metallic, adhesive)	•	•		
	In situ verifiable seals (fiber optic, ultrasonic, electronic, radiofrequency)	•	•		
	Container verification (laser mapping, laser item identification system)	•	•		
Surveillance	Optical surveillance (cameras, CCTV)	•	•		
Environmental Sampling	Bulk analysis (mass spectrometry, scanning electron microscopy)	•	•		
	Particle analysis (swipes, air sampling)	•	•		
Material Flow Measurement	Process holdup measurement				
Physical Protection	Access control	•	•		
	Intrusion detection	•	•		
Open-Source Information Analysis	Patent applications	•	•	•	
	Published scientific and technical literature	•	•	•	
	Publicly available information (news media, NGOs, governments)	•	•	•	
	Commercial satellite imagery	•	•	•	

Figure 6: Applicability of Existing IAEA Safeguards Techniques to Emerging Technologies

to impose no constraints on the acquisition or uses of the technology, at least until they have caught up. However, as with controlled nuclear fission, the most powerful generator of political impetus for a control regime on a given technology would probably be a compelling demonstration effect in the form of a highly-publicized weaponization of or accident involving a new technology, although this is not the sort of thing that governments can count on (nor can they seek to bring it about). Given these limitations, the prospects for achieving an international control regime for each of the emerging technologies considered here are sketched briefly below.

Molecular manufacturing. Although no government has yet offered a proposal for an international agreement restricting nanotechnology research or applications, academic and policy groups have given some thought to how the international community might best manage the national security consequences of a mature technology for molecular manufacturing. The Center for Molecular Nanotechnology (CMN) suggests that careful administration of molecular manufacturing technology will be required in order to mitigate its inherent danger. Like controlled nuclear fission, molecular nanotechnology has features that simultaneously increase the technology's risk while facilitating the sort of restrictions on its use that could become the components of an international administration program. For example, the compactness of molecular nanotechnology could make possible the safeguarding of a human-scale nanomanufacturing product, such as a personal nanofactory, by incorporating dedicated security or monitoring hardware directly into the device. Experts have also suggested that both the Chemical Weapons Convention and the BTWC be supplemented with an appropriate "clarifying interpretation that nanotech-enabled microscopic systems that can enter the body, damage life processes and are partly or fully artificial are included" within the scope of each agreement.[40]

However, CMN concludes that safe use of molecular nanotechnology will ultimately require "the creation of a single, trustworthy international administration to impose tight controls on the technology," but that unless the technology "is made widely available for a broad range of applications, there will be strong incentives for states to pursue their own independent molecular nanotechnology programs."[41] This reading of the impact of molecular nanotechnology and the resulting prescription for mitigating its risk tracks very closely with the evolution of controls on nuclear technology and the creation of the IAEA. The CMN proposal even goes so far as to call for "a closely-guarded crash program to develop a self-contained, secure molecular manufacturing system" which would then be made available only for the manufacture of approved products or classes of products.[42] This proposal would develop molecular manufacturing to maturity in a manner that precisely duplicates the development of controlled nuclear fission, right down to its own Manhattan Project. Thus nanotechnology, despite being a GPT, could be a plausible candidate for a treaty-based international control regime and accompanying system of safeguards administered by an authority analogous to the IAEA, assuming that the technology is developed to maturity in a manner that mirrors the development of controlled nuclear fission. If not, attempting to establish international control over molecular manufacturing after it has already worked its changes on society will likely prove futile.

Synthetic biology. Application of synthetic biology that are expressly conceived as weapons, such as artificial organisms incorporating enhanced virulence factors, are already prohibited by the BTWC, although verification remains problematic. Otherwise, synthetic biology is very tightly coupled with proprietary commercial development and thus difficult for governments to regulate. In March 2012, over one hundred environmental and civil society groups issued a collective statement on "The Principles for the Oversight of Synthetic Biology" which calls for a worldwide moratorium on the release and commercial use of synthetic organisms until more robust regulations and rigorous biosafety measures are established. The group also called for an outright ban on the use of synthetic biology on the human genome or human microbiome.[43] A 2007 study concluded that "with very few exceptions, synthetic genomics would not now be the technology of choice for a bioterrorist or a nation-state hoping to develop a virus for use as a weapon. Within five to ten years, however, it may very well be the case that synthesis will be easier than other means of obtaining a virus."[44] The creation of an international control regime for synthetic biology would likely be hindered by the same factors that contribute to the continuing absence of a verification regime for the BTWC, compounded by the intensely commercial nature of most synthetic biology development.

Robotics. Despite the media, academic and popular attention being given to unmanned and robotic weapons systems and the calls for an international agreement banning certain kinds of lethal autonomous systems, it seems unlikely that an international agreement governing robotic systems will be forthcoming anytime soon. UAVs are already widespread and have far too much utility, military and otherwise, for states to be willing to restrict their use. It may be possible to reach an agreement to ban entirely autonomous systems capable of exercising lethal force without a "human-in-the-loop," since no states have openly deployed such systems yet. But verification of such a ban would be extremely difficult, even if sufficient political will could be mustered for a verification system that is highly intrusive. The difference between a human-controlled or human-mediated robotic weapon system and a fully-autonomous lethal robotic weapon system is simply a matter of software. It would be extremely easy to re-program treaty-compliant weapon systems to function as a prohibited type of system, making the verification task functionally impossible for even the most robust inspectorate. Perhaps the best chance at an agreement banning an entire category of robotic weapons would be a ban on equipping robotic systems with nuclear weapons, since such a system would seem to have little military utility and many potential drawbacks.

40 "The Security Implications of Nanotechnology," op. cit., p. 6

41 "Administration Options for Molecular Manufacturing," Center for Responsible Nanotechnology (http://www.crnano.org/administration.htm), accessed April 13, 2013.

42 ibid.

43 Boyle, Alan (March 14, 2012). "What To Do about Synthetic Life?" http://cosmiclog.msnbc.msn.com/_news/2012/03/13/10672301-what-do-do-about-synthetic-life, retrieved May 3, 2013.

44 Garfinkel, Michele S., Drew Endy, Gerald L. Epstein and Robert M. Friedman. "Chapter 35: Synthetic Biology," *The Hastings Center Bioethics Briefing Book*, p. 164. http://www.thehastingscenter.org/uploadedFiles/Publications/Briefing_Book/synthetic%20biology%20chapter.pdf, accessed May 3, 2013.

Information technology. Of the technologies considered here, information technology is the only one that is presently the subject of an ongoing international negotiation as described previously. As of now, there is only one international agreement in place that governs use of the internet: the Council of Europe's Cybercrime Convention, adopted in 2001. However, the Cybercrime Convention is widely viewed as unsuccessful due to failures of verification and enforcement.[45] States cannot determine quickly or easily when their IT systems are being attacked, and once the attack is discovered, the computer or geographic source of the attack often cannot be ascertained quickly or precisely. If a computer or geographic source is identified, it is hard to know whether the responsibility for the attack lies there or with a different computer somewhere else. Even if a state has certain knowledge about which computer was the ultimate source of the attack, it is hard to know whether the human agent behind it is a private individual or a government. If the latter, it is frequently hard to determine the state affiliation.[46] Any conceivable verification regime for an international agreement on the use of information technology would require such extensive governmental monitoring of the internet as to prove unworkable in many countries. For these reasons, it seems unlikely that an effective regime of international controls over the uses of information technology will emerge in anything that resembles today's international environment.

Role of the IAEA. The IAEA is the obvious model for any future international control authority charged with promoting the peaceful use of an emerging technology while verifying the absence of any prohibited uses under the terms of such agreements as may be forthcoming. To what extent could we — or should we — leverage the IAEA itself for this purpose? The IAEA enjoys a considerable advantage compared to other potential implementing mechanisms for any new control regimes that would govern the use of emerging technologies. These include its established reputation for independence and objectivity, its international character and ability to build consensus worldwide (and its considerable experience in doing so), and its capability to establish – and assist member states in complying with – international norms and standards governing a dual-use technology.[47] In addition, the IAEA is responsible for ensuring that the advantages of the technology under its purview are used to benefit human well-being and sustain socioeconomic development while also seeking to ensure that the risks associated with nuclear technology are minimized.[48] Finally, the IAEA has a role in ensuring the safe and secure application of nuclear technology and in reducing the likelihood of accidents through human or technical failure. These are all desirable characteristics for any future control regime governing access to and use of molecular manufacturing, synthetic biology, information technology, and/or robotics. By far the easiest route to creating a verification authority for any future agreements governing these technologies would be the adaptation of the IAEA itself.

The obvious disadvantage of attempting to use the IAEA as a direct platform for launching international verification and control systems for emerging technologies is that the IAEA's current expertise is confined entirely to nuclear technology. Any new expertise would need to be "bolted on," possibly compromising the Agency's effectiveness in executing its existing nuclear safeguards mandate. This danger is especially acute if governments attempted to leverage the IAEA for an emerging technology verification mission without a corresponding increase in Agency resources. The best approach to capitalizing on the success of the IAEA and the international safeguards system for a new technology safeguards mission would be the establishment of a dedicated verification authority for the relevant international agreement and the subsequent incorporation the IAEA's lessons learned from fifty years of safeguards implementation. This could be accomplished by establishing short-term dedicated working groups comprised of personnel from the IAEA and the new verification authority. These working groups could provide guidance to those governments and international organizations that are working to set up the new verification entity. Once the new verification authority is established, IAEA expertise could be further leveraged through longer-term detail assignments and personnel exchanges.

6. Conclusions

As the 21st century progresses, the national security challenge posed by emerging and converging technologies will become ever more acute. But the continued success of the nuclear nonproliferation regime and of the IAEA safeguards system demonstrates that successful management of the national security risks associated with emerging technologies is not only achievable but is sustainable over the long term, even in the face of serious tests. The ongoing evolution of IAEA safeguards from a system that verifies legitimate and declared uses of nuclear technology into a system for discovering illicit and clandestine ones shows that safeguards are capable of adapting successfully to changing political and technological requirements. In the coming decades, the IAEA and the international safeguards system will remain vital instruments of global security, not only in their role as guarantors of the nuclear nonproliferation regime but also increasingly as the pathfinders to a secure human future that is protected, as much as it ever can be, from the risks that come with our ever-evolving technology.

[45] Goldsmith, Jack "Cybersecurity Treaties: A Skeptical View (February 2011)," in *Future Challenges in National Security and Law*, edited by Peter Berkowitz, http://www.futurechallengesessays.com, pp. 1-2

[46] ibid, pp. 3-4

[47] "*20/20 Vision for the Future: Background Report by the Director General for the Commission of Eminent Persons.*" International Atomic Energy Agency, May 23, 2008 (GOV/2008/22-GC (52)/INF/4 Annex), p. 4.

[48] ibid, p. 12

The 'Room within a Room' Concept for Monitored Warhead Dismantlement

Jennifer Tanner, Jake Benz, Pacific Northwest National Laboratory, USA
Helen White, Sarah McOmish, Keir Allen, Atomic Weapons Establishment, UK
Keith Tolk, Milagro Consulting LLC, USA
George Weeks, Savannah River National Laboratory, USA

© British Crown Owned Copyright 2014
This document is of United Kingdom origin and contains proprietary information which is the property of the Secretary of State for Defence. It is furnished in confidence and may not be copied, used or disclosed in whole or in part without prior written consent of Defence Intellectual Property Rights DGDCDIPR-PL - Ministry of Defence, Abbey Wood, Bristol, BS34 8JH, England.

Abstract:

Over the past 10 years, US and UK experts have engaged in a technical collaboration with the aim of improving scientific and technological abilities in support of potential future nuclear arms control and non-proliferation agreements. In 2011 a monitored dismantlement exercise provided an opportunity to develop and test potential monitoring technologies and approaches. The exercise followed a simulated nuclear object through a dismantlement process and looked to explore, with a level of realism, issues surrounding device and material monitoring, chain of custody, authentication and certification of equipment, data management and managed access. This paper focuses on the development and deployment of the 'room-within-a-room' system, which was designed to maintain chain of custody during disassembly operations. A key challenge for any verification regime operating within a nuclear weapon complex is to provide the monitoring party with the opportunity to gather sufficient evidence, whilst protecting sensitive or proliferative information held by the host. The requirement to address both monitoring and host party concerns led to a dual function design which:

- *Created a controlled boundary around the disassembly process area which could provide evidence of unauthorised diversion activities.*
- *Shielded sensitive disassembly operations from monitoring party observation.*

The deployed room-within-a-room was an integrated system which combined a number of chain of custody technologies (i.e. cameras, tamper indicating panels and enclosures, seals, unique identifiers and radiation portals) and supporting deployment procedures. This paper discusses the bounding aims and constraints identified by the monitoring and host parties with respect to the disassembly phase, the design of the room-within-a-room system, lessons learned during deployment, conclusions and potential areas of future work. Overall it was agreed that the room-within-a-room approach was effective but the individual technologies used to create the system deployed during this exercise required further development.

Keywords: Nuclear Weapon, Dismantlement, Chain of Custody, Containment, Surveillance

1. Introduction

In 2011, US and UK technical experts took part in a monitoring exercise designed to investigate potential facility issues and technologies which might be associated with the verification of nuclear warhead dismantlement [1]. The hypothetical scenario followed a simulated nuclear object through a series of internal transport, storage and disassembly phases. The deployed monitoring regime included device and material monitoring, chain of custody, authentication and certification of equipment and data management. This paper focuses on the chain of custody system, called 'room-within-a-room', which was deployed during the disassembly phase. Chain of custody, in this context, is a connected series of procedures and technologies designed to account for treaty accountable items throughout a dismantlement process, and provide confidence that the integrity and authenticity of an item has been maintained [1,2,3,4,5,6,7,8,9]. In essence, the room-within-a-room system created a controlled boundary around the disassembly operations which was fully understood and accepted by both the host and monitoring parties. The boundary used multiple complementary technologies (i.e. cameras, tamper indicating panels and enclosures, seals, unique identifiers and radiation portals) in one integrated design. This paper discusses how the exercise participants arrived at this chain of custody design given the bounding aims and constraints identified by the monitoring and host parties. The paper also presents lesson learned and conclusions from the exercised deployment of this chain of custody approach.

2. Background: The 2011 Monitored Dismantlement Exercise

The nuclear Non Proliferation Treaty (NPT) sets out, among other elements, the obligation to pursue negotiations on "… disarmament under strict and effective international control". Therefore research into effective approaches to technical verification is an important building block when considering the implementation of possible future nuclear disarmament agreements [2,3]. However the design of effective technologies and methodologies in support of this area is a complex challenge for technology developers [2,3,4,10,12]. Technical verification would be undertaken by a 'monitoring party' within facilities overseen by a 'host party'. However, monitoring party access to facilities and information is likely to be restricted, as the host party has an obligation to protect proliferative and nationally sensitive information [2,10]. This leads to a key challenge: balancing the need to protect classified and sensitive information with the desire to obtain sufficient information to inform the monitoring process [2,10,11,12,13]. The differing perspectives of the parties involved influence and drive the design of the final negotiated monitoring regime and managed access approach [11,12,13]. The challenge is to create a robust monitoring approach which meets the requirements of all relevant parties.

The 2011 monitored dismantlement exercise was based on a hypothetical agreement between two fictitious Nuclear Weapon States (NWS) involving the dismantlement of a nuclear object [1]. The exercise followed a treaty accountable item, which for this scenario was a fictional nuclear warhead represented for exercise purposes by a quantity of fissile material and simulated high explosives [1], through a series of phases including transport, storage and disassembly (Figure 1). The scenario also included a negotiation stage, which provided a realistic background scenario for the participants and an opportunity to understand any host party sensitivities that might impact upon the monitoring regime. Note that in order to create a challenging 'worst case' scenario, it was specified that no sensitive, classified or proliferative information could be shared between the two fictitious Nuclear Weapon States. A representative facility was used to support the exercise (Figure 2) which included a work area for the monitoring party, secured compounds, entry control points, receipt and dispatch, a store, a process facility and change barrier facilities (where participants were required to change into and out of protective clothing). The disassembly process facility, the focus of this paper, consisted of a corridor and the disassembly process area.

3. Key Aims and Constraints Driving the Room-Within-A-Room Design

The negotiation stage of the exercise allowed all participants to discuss the objectives of the monitoring party, and any sensitivities and issues raised by the host party. The disassembly phase was of particular concern for the host party as treaty accountable components would be visible to anyone working in the area and operations needed to be performed with respect to strict safety regulations. The monitoring party emphasised the importance of maintaining chain of custody during disassembly operations. The negotiation process provided key aims and constraints which ultimately drove the design of the room-within-a-room system for the disassembly phase.

Key Aims:

- To ensure that no treaty accountable items, components, or material were diverted from the process during the disassembly phase.
- To maintain the integrity and authenticity of the monitoring equipment, and any associated data outputs, for the entirety of disassembly operations including any periods of time where the facility and equipment would be left unattended.

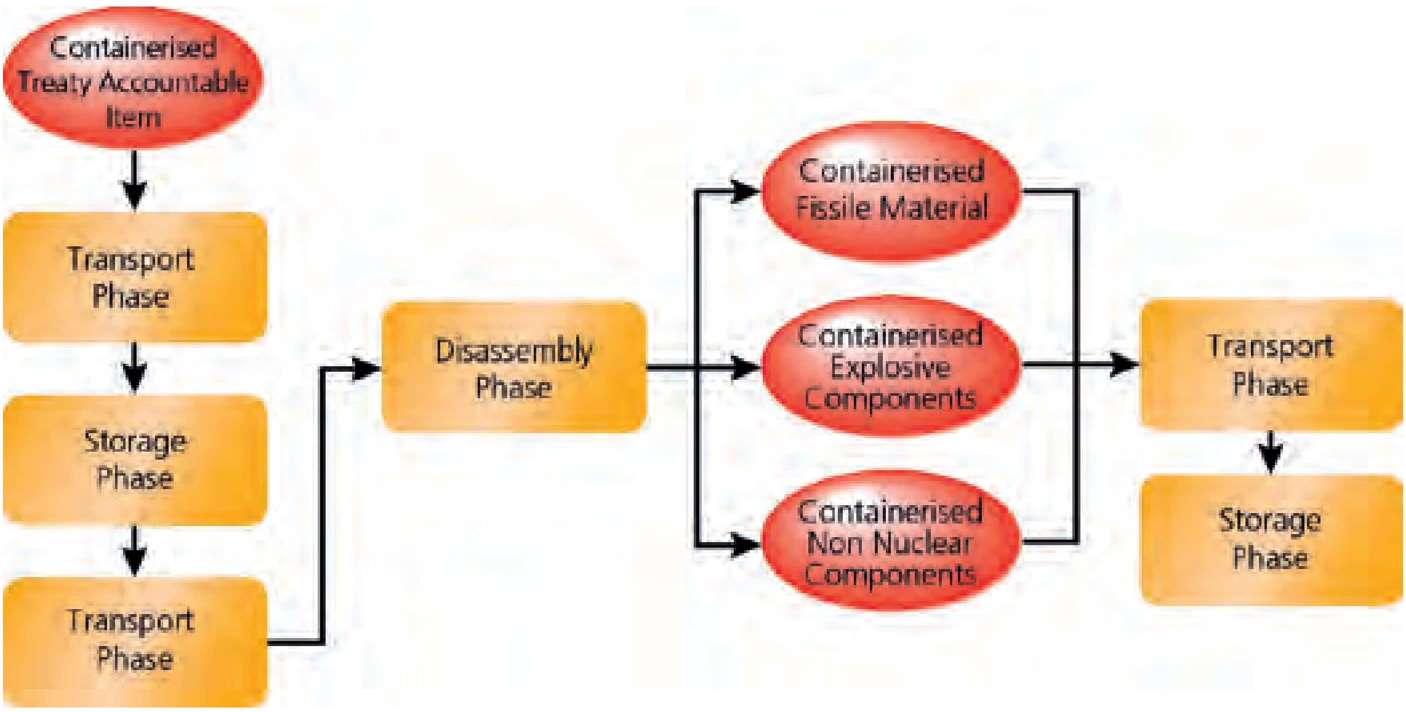


Figure 1: Monitored dismantlement exercise - dismantlement process.

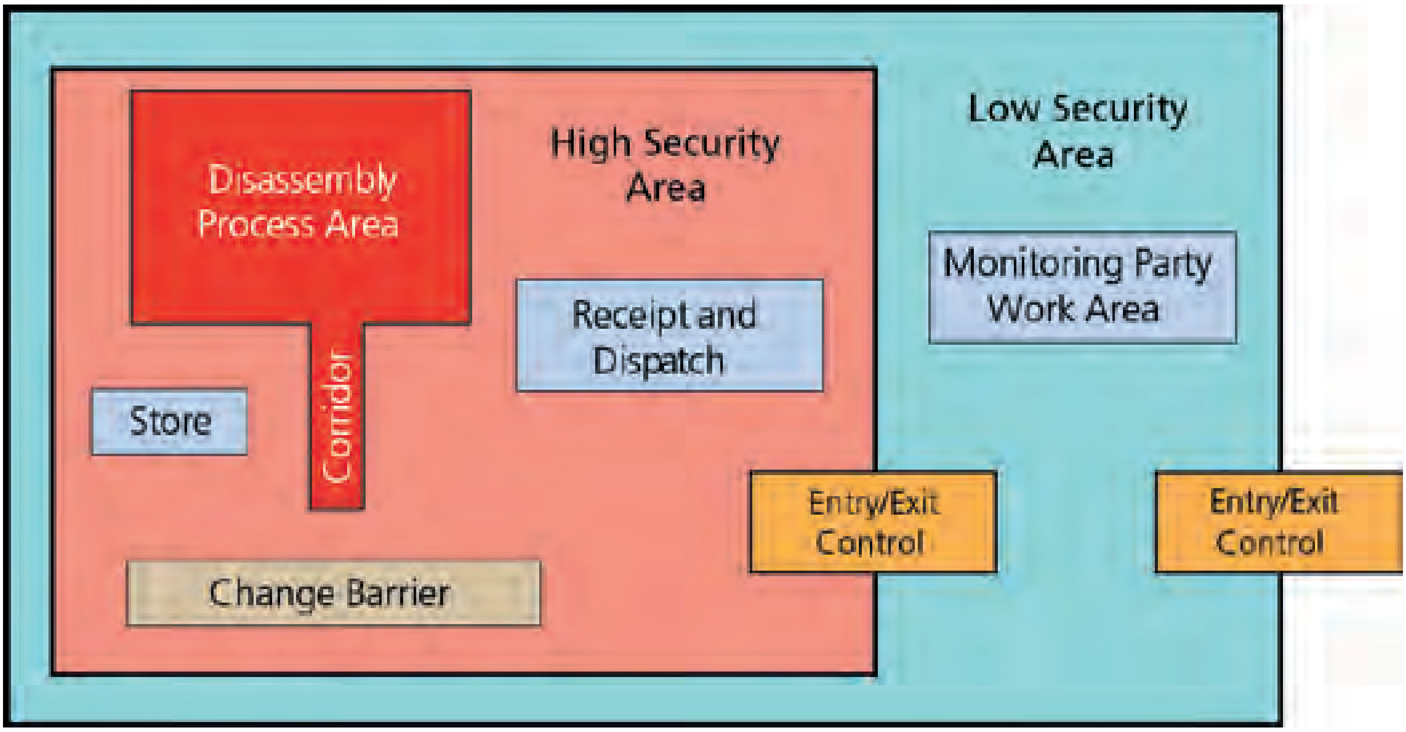


Figure 2: Monitored dismantlement exercise – representative dismantlement facility.

Key Constraints:

- The requirement for the monitoring party to leave the disassembly facility at any point during operations where sensitive treaty accountable components were in view. Monitoring equipment was not allowed to record (visually or otherwise) disassembly operations.
- The deployed monitoring equipment could not hinder disassembly operations.
- Safety regulations had to be adhered to.
- The information relating to the facility, containers and toolboxes was restricted to visible images of non-sensitive external features. Simple background radiation measurements were permitted before and after the disassembly phase. Note that physical security technologies deployed within the facility were considered to be sensitive features.
- The monitoring party could not access surrounding facilities deemed to be outside the scope of the monitoring process.
- Any data gathered by the monitoring equipment had to be reviewed by the host party prior to release to the monitoring party.

In summary, an overarching aim for the disassembly phase of the monitoring regime was to maintain chain of custody whilst shielding sensitive disassembly operations from monitoring party observation. This was particularly challenging, as the monitoring party could not be present in the facility during the disassembly phase, and knowledge of any facility or container specifications was severely restricted.

4. A Room-Within-A-Room for the Disassembly Phase

The chain of custody regime for the disassembly phase had to meet the aims set out by the monitoring party, and operate within the constraints specified by the host party. A joint host/monitor technical working group was formed in order to discuss and develop a jointly agreed solution. Initial discussions focused on three key concepts:

- The identification and control of potential diversion routes.
- Establishing and maintaining boundary control during dismantlement operations.
- Protecting sensitive operations from direct monitoring party observation.

The monitoring party wished to create a controlled boundary around the disassembly process area that would provide evidence of any unauthorised removal of treaty accountable items or components. Potential diversion routes out of the process were associated with the facility, containers, toolboxes and facility personnel. The monitoring party did not have sufficient information about the facility to identify all possible diversion pathways; simple background radiation measurements and visual observations could only partially address this. To account for this issue, the working group proposed the concept of a room-within-a-room. In this approach, the monitoring boundaries were simplified by creating a temporary room which surrounded the entire process area. The room-within-a-room was designed to:

- Maintain boundary control whilst protecting sensitive operations from monitoring party observation.
- Provide a boundary to the process area that the monitoring party could fully understand, inspect and control.
- Detect the unauthorized diversion of treaty accountable items or components out of the process area.

Note that additional radiation measurements and visual observations were required to account for the potential use of shrouded items or empty containers as a diversion route.

The room-within-a-room system designed and implemented during this exercise is summarised in Figure 3. The design considered the walls, ceiling, floor and normal point of entry for the disassembly process area and employed multiple complementary technologies in one integrated design. Chain of custody over the monitoring equipment was maintained via a combination of tamper indicating enclosures (TIE), seals, and careful positioning of the CCTV cameras. The room-within-a-room was supported by deployment procedures and was implemented in a specified chronological order:

1. The process area, along with any pre-staged empty containers and shrouded toolboxes, was inspected visually and with gamma and neutron dose rate meters (this was to identify any 'suspicious' features or unexpected radiation sources).
2. The room-within-a-room was constructed taking care to maintain chain of custody over the monitoring equipment.
3. The room-within-a-room boundary was initialized and the system was tested.
4. The treaty accountable item was brought into the facility and the monitoring party left the facility.
5. Dismantlement operations took place over a number of days. At the beginning and end of each day, the monitoring party was allowed to return to the facility to unseal/seal the door and download data from the CCTV cameras and portal monitors.
6. Once dismantlement operations were complete, and all treaty accountable components were sealed in containers, the monitoring party was allowed back into the process area.
7. The room-within-a-room boundary was fully inspected.
8. All containers were sealed and the 'full' containers were moved out of the process area.

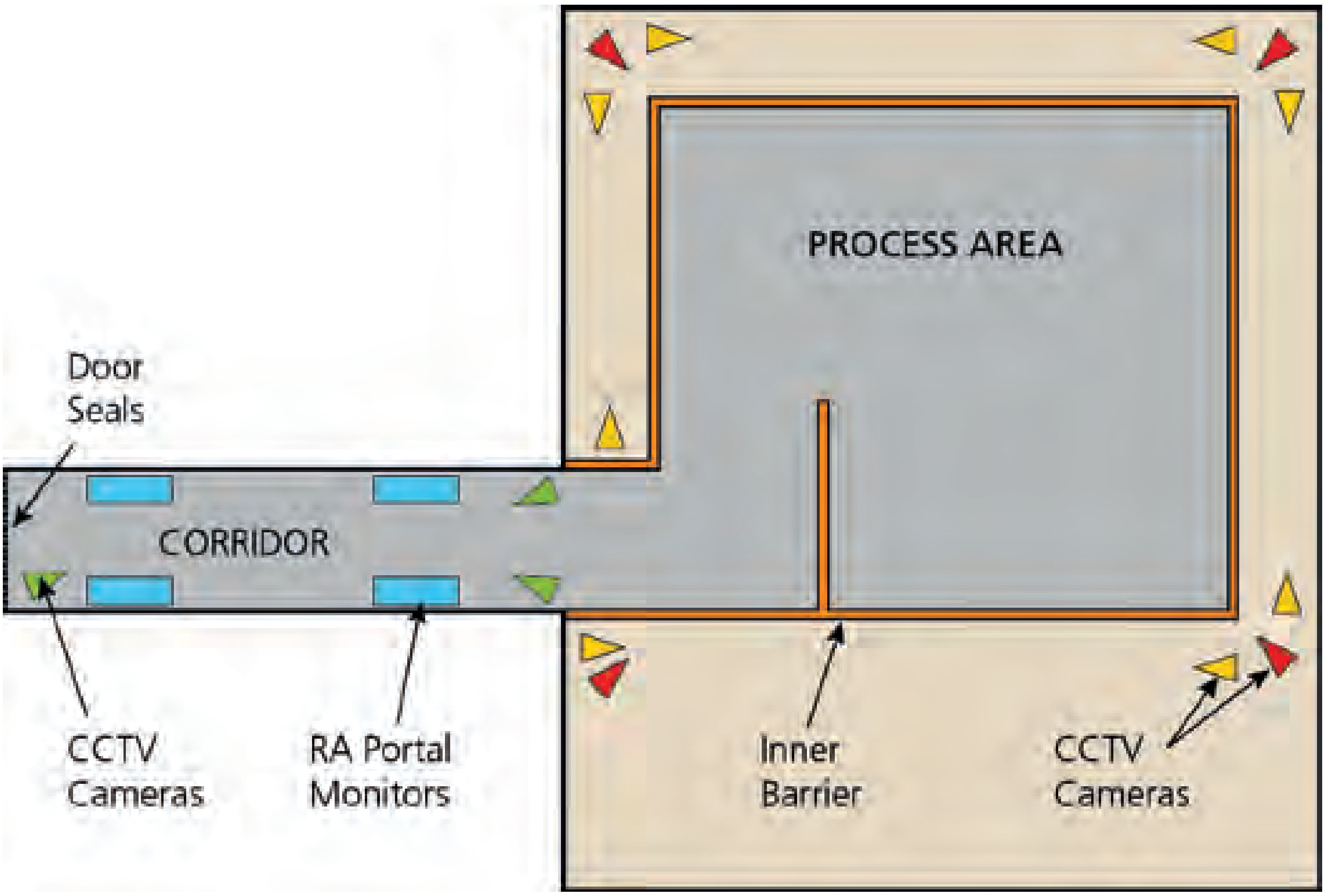


Figure 3: The room-within-a-room deployed during the 2011 monitored dismantlement exercise.

9. The process area, empty containers and shrouded toolboxes were inspected visually and with gamma and neutron dose rate meters.

The following section discusses the detailed design of the room-within-a-room and lessons learned during deployment.

5. Technologies Deployed and Lessons Learned

This section discusses each element of the room-within-a-room as deployed during the 2011 monitored dismantlement exercise (Figure 3): walls, ceiling, floor, normal point of entry, chain of custody of monitoring equipment, supporting visual/radiation inspections and data management. The section presents the technologies deployed, discusses lesson learned during deployment and highlights any potential areas for future work. A final summary captures overarching comments on the system as a whole.

5.1 Process Area: Walls, Ceiling and Floor

Temporary barriers were erected to define the process area. A gap was created between the barriers and the facility walls; cameras (yellow triangles in Figure 3) were positioned at floor level to monitor the gap. This arrangement shielded the disassembly operations from direct view but captured any attempt to gain unauthorised access to the walls of the facility. The barrier panels were secured to each other using uniquely identified adhesive seals (Figure 4). Image change detection techniques were deployed on the barrier panels and where the temporary barriers met the floor; in order to comply with facility fire regulations, the barriers could not extend from floor to ceiling. To accommodate disassembly operations the barriers could not continue across to form a temporary ceiling. Cameras (red triangles in Figure 3) were positioned so that any unauthorised attempt to access the facility ceiling would be captured. The cameras were positioned at ceiling height with a restricted field of view which precluded the imaging of any disassembly operations or physical security features. The field of view of each camera was adjusted to ensure the system provided full wall and ceiling coverage. The existing facility floor was visually inspected for indications of tampering. Before and after images of significant features were photographed for analysis via change detection techniques.

The floor within the process area was a particular area of concern as this was the only surface of the room not covered by the CCTV camera system. There was discussion of putting down a temporary floor with tamper indicating features which could be inspected. For this scenario, any tamper indicating flooring would have to:

- Meet facility safety regulations.
- Be strong enough to accommodate the weight of the equipment and staff.
- Be robust enough to be able to distinguish between tampering and any damage created during legitimate disassembly operations.

Figure 4: The process area was surrounded by barriers connected together with uniquely identified adhesive seals. The barriers were inspected using imaging change detection techniques.

Although several temporary flooring concepts were discussed (for instance, utilizing fibre optics, guided waves or CCTV under-floor imaging) none were sufficiently advanced to be included in this exercise. This remains an area of future work.

Image change detection was used in several ways during the exercise:

- Photographs were taken of the unique identifying features (ink runs or simple random particulate patterns) associated with the seals.
- Wide area reference photographs were taken of the barriers.
- The floor was visually inspected for significant features and potential areas of tamper; reference photographs were taken for later comparison.

Change detection associated with high resolution images of defined areas, as exemplified by the unique identifiers, worked well. Although the unique identifiers deployed during this exercise were relatively simple concepts, a comparison of reference and inspection images clearly identified areas of damage. It was noted, however, that a secondary layer of defence would be desirable which could be used as additional evidence supporting any inquiries into how that damage was produced.

Image change detection of the barriers and flooring was challenging for the following reasons:

- The system had to distinguish between a tampering event and changes due to legitimate activities within the facility.
- It was too time consuming to deploy large numbers of markings to aid in image alignment (feducials) and perform high resolution imaging.

The images taken of the barriers lacked the resolution and feducials necessary to perform the in-depth analysis required to (a) identify areas of change and (b) confidently identify how that change had occurred. Inspecting the floor for significant features was a subjective approach that did not allow for the before and after images necessary to deploy this concept robustly. Future work in this area would be to investigate change detection techniques for large areas.

5.2 Normal Point of Entry

Entry and egress to the facility was via the corridor. The associated chain of custody system was designed to detect the unauthorised movement of radiation sources, tooling and equipment into and out of the facility, whilst allowing for free access by facility staff during disassembly operations. The treaty accountable item, tooling and equipment were moved into the facility under the supervision of the monitoring party. Once the disassembly had begun, and the monitoring party was absent, the facility staff were not allowed to remove these items from the designated process area. CCTV cameras were positioned to encompass the key areas of the corridor whilst precluding sensitive physical security features from view (green triangles figure 3). Radiation portal monitors, measuring gross gamma and neutron, were positioned to capture the movement of sources in and out of the process area. A sealing system on the main door was used when the facility was vacated overnight and over the weekend. The door seals consisted of a passive break bar system secured with uniquely identified loop seals and uniquely identified adhesive seals (Figure 5).

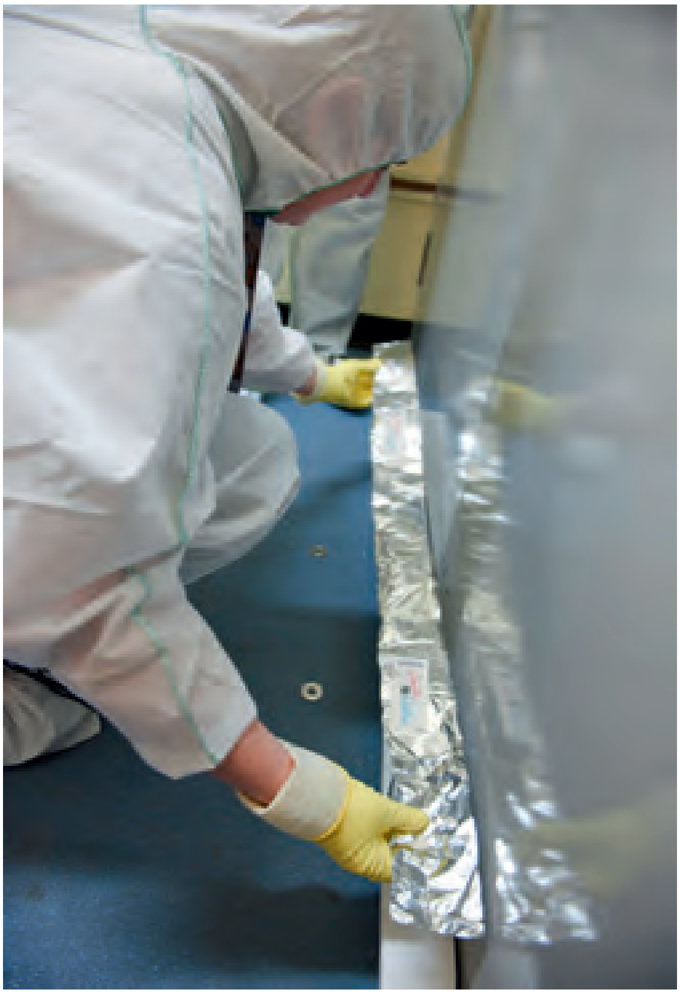


Figure 5: A passive break bar sealing system was designed for the main door into the disassembly facility, consisting of a polystyrene bar and an aluminium foil (which was easily broken but was hard to repair without leaving a visible join) and uniquely identified seals.

The design of the door seal was an example of how safety regulations can be a key factor in the specification of a given technology. In this case, the break bar concept deployed was designed to account for fire regulations which required fast and unencumbered access to the facility in the event of an emergency. The door seals were a passive, unpowered, secondary defensive layer which complemented the main deployment of the CCTV camera system and the portal monitors in the corridor. The use of radiation

Figure 6: Each CCTV cameras was enclosed within a passive Tamper Indicating Enclosure (TIE). The TIE was based on Poly (Methyl MethAcrylate) (PMMA) and had an integrated particulate based unique identifier [6]. The TIE was inspected via a combination of polarimetry, visual inspection and image change detection.

portal monitors was demonstrated during this exercise but continued research is required into how such a system could be designed so that both parties have confidence in the outputs.

Unlike in the process area, the CCTV cameras in the corridor imaged monitoring and host party personnel, and concerns were raised regarding the use of CCTV cameras and the protection of personnel privacy (e.g. imaging the faces of monitoring and host party personnel). This could be of concern to the monitoring party, facility employees and the host party as an employer, and may have to be accounted for either in the design of the system or in the handling of the recorded data.

5.3 Chain of Custody of Monitoring Equipment

Chain of custody over the monitoring equipment was maintained via a combination of tamper indicating enclosures (TIE), seals, and careful positioning of the CCTV cameras. Each CCTV camera was placed into a passive TIE (Figure 6) that had been specifically designed for this purpose [6]. All the other supporting equipment, such as digital cameras associated with the change detection activities, were secured in a passive optical fibre based TIE [5,6] when not in use. In order to provide an additional layer of protection, each camera was positioned so that it was in the direct field of view of at least one other camera. All the monitoring equipment to be left within the facility (including all the cabling, data recording devices and TIEs) was also positioned in the field of view of at least one CCTV camera.

The deployment of TIEs decreased the number of seals that were required and, therefore, decreased the overall workload for the monitoring party. The development of TIEs for robust boundary protection of everything from equipment to rooms remains an active ongoing area of work for this collaboration [5,6].

5.4 Supporting Visual and Radiation Inspections

Visual observations, and measurements using hand held radiation dose meters (gamma and neutron), were undertaken to highlight any ‘suspicious’ features, potential diversion routes and radiation sources. Visual and radiation based observation were used to support the deployment of the room-within-a-room by providing a baseline of the facility before and after disassembly operations. These activities, however, were the primary method by which diversion routes associated with empty containers and shrouded items, such as tool boxes, were identified and secured. Note that the monitoring party were not permitted to look inside the containers, under shrouds, into wall cavities or into air ducts. Detailed maps of the facility, and exact container designs, were also withheld.

Although visual and radiation dose measurements are capable of detecting significant radiation sources and obvious diversion routes, there is potential for highly shielded radiation sources to be missed. Therefore, while the facility boundaries were accounted for by the room-within-a-room system, the shrouded items and empty containers remained a potential route for diversion of material. Confirming the absence of radiation sources in shrouded items and empty containers remains an area for future development.

5.5 Data Management

Data management during deployment was an important element of the overall system design. The chain of custody measures deployed relied almost entirely on image analysis, either through change detection or video capture. Data from the main door sealing system, CCTV cameras and portal monitors was collected at the beginning and end of each operational day. Images from the tamper indicating enclosures, process area seals, unique identifiers, barriers and floor, were collected at the beginning and end of the whole disassembly operation. The data needed to be transferred from the disassembly process facility to the monitoring party work area where image analysis took place.

The monitoring data was downloaded from the room-within-a-room system onto the removable media under joint host/monitor control; two copies were created, one for the monitoring party and one for the host party. The removable media was placed in a TIE inside a protective bag; this system was specifically designed to maintain chain of custody over the removable media while the media underwent decontamination at the change barrier (note that the TIE design was based on the Sample Vial Secure Container (SVSC) [16]). The monitoring party copy remained within the protective bag and TIE whilst the host party reviewed the second copy. An anomaly procedure allowed for any data redaction activities. Once the host party was satisfied, the monitoring party copy was taken over the change barrier to the monitoring party work area and released for analysis.

This exercise demonstrated some of the challenges faced when considering the chain of custody of data within this kind of regime. Both parties underestimated the time and resource required to review such a large volume of data. This resulted in long delays which decreased the time available to the monitoring party for anomaly investigation. This, in turn, impacted on monitoring party confidence in the released data and the chain of custody regime. Significant work is needed to develop and optimise trusted data management systems.

5.6 Overarching Comments and Lessons Learned

The room-within-a-room approach successfully maintained chain of custody during the disassembly process whilst effectively shrouding sensitive operations from monitoring party observation. It was agreed that the overall concept was sound, although the specific technologies used to support it during this exercise required further work.

There was a heavy reliance on the CCTV system which had the dual function of boundary control and a layer of defence against tampering of monitoring equipment. It was noted that the loss of the CCTV system would only be partially compensated for by the deployment of sealing systems and TIEs. It was recognized that additional layers of boundary defence associated with the barriers, ceiling and floor were required. Large scale boundary tamper indicating concepts remain a research area of interest from this perspective. The infrastructure required to run the CCTV system for an extended period of time was not exercised but was discussed as an area that would need to be addressed.

For this exercise, the issue of authentication and certification of equipment was not rigorously played. It is important that both parties have confidence that all of the equipment [14,15]:

1. Has been fabricated as designed and agreed upon.
2. Is incapable of divulging sensitive or proliferative information.
3. Complies with facility regulations.
4. Provides an accurate and trusted record of the verification activity.
5. Can demonstrate that the ultimate output has not been altered.

The task of authentication and certification is not always straightforward, particularly when considering complex systems. It was unanimously agreed that the development of techniques to support authentication activities is a significant area for future research.

6. Conclusion

A recent monitored dismantlement exercise provided an opportunity for US and UK technology experts to develop and test technologies and methodologies which might form part of a verification regime for future nuclear disarmament agreements [1]. The exercise followed a treaty accountable item through a simulated dismantlement process which included transport, storage and disassembly phases [1]. The key to effective verification is the ability to balance the need to protect sensitive and proliferative information with the desire to obtain sufficient information to inform the process [2,10,11,12,13]. This exercise therefore presented a challenge to the participating technical experts in that the requirement for the monitoring party to gather confirmatory evidence of compliance had to be balanced with managed access and safety concerns raised by the host. This was an ambitious exercise both in terms of technical scope and attempted realism and resulted in the development of a number of innovative technologies. This paper focused on a discussion of the ‘room-within-a-room’ approach developed to maintain chain of custody during the disassembly phase.

The disassembly phase was particularly challenging in terms of maintaining chain of custody as the monitoring party was not permitted to access or image sensitive disassembly operations, and knowledge of any facility specifications or layouts was severely restricted. An approach was devised, called room-within-a-room, which maintained a monitored boundary around the operational area whilst shielding the disassembly operations from monitoring party view. The room-within-a-room deployed during this exercise combined a variety of complementary technologies (including large scale barriers, CCTV camera systems, portal monitors, image change detection, passive tamper indicating enclosures and passive seals) with supporting procedures (such as radiation sweeping activities) to create an integrated system. The deployed room-within-a-room system:

- Successfully maintained control of the disassembly facility boundary for the duration of the exercise.
- Protected sensitive operations from monitoring party observation.
- Allowed for the detection of diversion from the disassembly facility.

Overall it was agreed that the room-within-a-room strategy was effective but the individual technologies used to create the system deployed during this exercise required development. Lessons learned from this exercise highlighted the following areas for the future development:

- Passive boundary tamper indicating technologies that have the potential to be scaled to cover room sized areas. These should consider the inspection method which needs to be fast and simple to deploy. Currently, this US-UK technical collaboration is focusing on passive concepts which provide a visual indication of unauthorised tampering; future work could also include active variants.
- Tamper indicating flooring.
- Fast, easily deployed, imaging change detection techniques capable of covering large areas.
- The use of radiation portals within nuclear weapon dismantlement scenarios.
- Inspection techniques determining the absence of unauthorised radiation sources within shrouded items and empty containers.
- Improved Tamper Indicating Enclosures (TIEs) for monitoring equipment. This collaboration currently focuses on passive concepts but also has a long term interest in active alternatives.
- Authentication and certification techniques for monitoring equipment.
- Improved data management techniques for use within nuclear weapon dismantlement scenarios.

It should be noted that the room-within-a-room system would be one element of a larger chain of custody regime. Ultimately, research in chain of custody needs to provide a toolbox of technologies and methodologies with the flexibility to respond effectively to a number of different potential future treaty scenarios.

7. Acknowledgements

The authors would like to thank the U.S. National Nuclear Security Administration Office of Nuclear Verification and the UK Ministry of Defence for their continued support of this technical collaboration. The authors would also like to thank the many contributors to this successful exercise including the DOE national laboratories and UK AWE.

8. References

[1] *Overview of US and UK Cooperation to Address Technical Challenges in Verification of Nuclear Disarmament* (side meeting and presentation), United Nations General Assembly First Committee on Disarmament and International Security, November 2013 (http://webtv.un.org/watch/technical-challenges-in-verifying-nuclear-disarmament/2769294424001/)

[2] Smith, MR (et al), *Future Directions for Arms Control Verification Technologies*, Proceedings of the 51st Annual Meeting of the Institute of Nuclear Materials Management, July 2010

[3] The U.S. Department of Energy, Office of Arms Control and Non-proliferation, *Transparency and Verification Options: An Initial Analysis of Approaches for Monitoring Warhead Dismantlement*, May 19, 1997

[4] Committee on International Security and Arms Control, [US] National Research Council, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials: An Assessment of Methods and Capabilities*, ISBN: 0-309-54889-6, (http://www.nap.edu/catalog/11265.html), 2005; p 45-47

[5] White H (et al.), *Passive Tamper Indicating Enclosures Incorporating Embedded Optical Fibre*, Proceedings of the 52nd Annual Meeting of the Institute of Nuclear Materials Management, July 2011

[6] White H (et al.), *A Passive Tamper Indicating Enclosure for use within a Nuclear Weapons Monitoring Regime*, Proceedings of the 53rd Annual Meeting of the Institute of Nuclear Materials Management, July 2012

[7] Daborn P (et al.), *The use of Modal Testing within Nuclear Weapon Dismantlement Verification*, Proceedings of the 53rd Annual Meeting of the Institute of Nuclear Materials Management, July 2012

[8] Benz, J (et al), *Templating as a Chain of Custody Tool for Arms Control*, Proceedings of the 35th Annual ESARDA Symposium, May 28-30, 2013

[9] MacArthur D (et al), *Confirmation of Nuclear Treaty Limited Items: Pre-dismantlement vs. Post-dismantlement*, Proceedings of the 35th Annual ESARDA Symposium, May 28-30, 2013

[10] Dreicer M (et al), *Applicability of Nonproliferation Tools and Concepts to Future Arms Control*, ESARDA Bulletin, No. 49, June 2013

[11] UKNI, *UK Norway Workshop on Nuclear Disarmament*, presentation pack, 2011

[12] UKNI, *The United Kingdom-Norway Initiative: Research into the Verification of Nuclear Warhead Dismantlement*, NPT Review Conference, 2010

[13] Backe S (et al.), *The United Kingdom-Norway Initiative: Further Research into Managed Access of Inspectors During Warhead Dismantlement Verification*, Proceedings of the 53rd Annual Meeting of the Institute of Nuclear Materials Management, July 2012

[14] Tolk K, *Authentication Issues in Safeguards*, IAEA-CN-184/175

[15] Allen K, *Item Tagging Considerations under a Verified Warhead Dismantlement Regime*, Proceedings of the 33rd ESARDA Symposium On Safeguards and Nuclear Material Management, May 2011

[16] Baumann M, *Sample Vial Secure Container*, Sandia National Laboratories

The ^{252}Cf neutron spectrum in ISO Standard 8529

David Thomas
National Physical Laboratory, NPL, Teddington, Middlesex, TW11 0LW, UK
E-mail: david.thomas@npl.co.uk

Abstract:

The provenance of the ^{252}Cf neutron spectrum tabulated in ISO Standard 8529 Part 1 is discussed in the light of queries raised in an earlier ESARDA article. It is shown that neither the ISO spectrum nor a Maxwellian representation is compatible with the most recent evaluation of this important standard spectrum.

Keywords: ^{252}Cf spectrum; ISO Standard 8529

1. Introduction

A paper by Croft and Miller in the ESARDA Bulletin [1] raised questions about the accuracy of the ^{252}Cf neutron spectrum tabulated in ISO Standard 8529 Part 1 published in 2001 [2]. The standard states, in Annex A at A.1, that the tabulated spectrum was calculated "by numerical integration using the analytical function given in section 4.3.2". This function, a Maxwellian, has the form:

$$B_E = \frac{2}{\sqrt{\pi}T^{3/2}} \times \sqrt{E} \times e^{-E/T} \times B \qquad (1)$$

where:

B_E is the neutron emission rate per unit energy at energy E,

B is the total neutron emission rate of the source (this can be set to 1 if only the spectral shape is of interest), and

T is a spectrum parameter given, according to the standard, by T = 1.42 MeV.

The standard does, however, state in 4.3.2, that the spectrum can be described by eq. (1), "in the energy range from 100 keV to 10 MeV", implying that the spectrum is not well described by a Maxwellian shape outside this range. However, the text at A.1 explicitly states that the tabulated data were derived from the Maxwellian function. The paper of Croft and Miller points out that an integration of the Maxwellian function over the energy groups used in the standard does not reproduce the spectral data as tabulated. Checking this involves solving the integral:

$$B_i = \int_{E_i}^{E_{i+1}} B_E \, \mathrm{d}E \qquad (2)$$

where:

B_i is the group source strength in an energy group (bin) extending from energy E_i to E_{i+1}.

The integration was performed by Croft and Miller using Excel functions. (A check of the results, performed using a simple Fortran program incorporating a NAG library algorithm to perform the integration, confirmed the values and produced identical results.) The question raised is whether there were problems with the numerical integration used to obtain the numbers in the ISO standard, or whether the spectral data were derived in some other way.

2. Review of available data

Discussions with members of the working group who wrote the standard were inconclusive, but they raised the possibility that the data in an earlier standard, ISO 8529 (1989) [3], had been derived from the Maxwellian function, and that changes may have been made to the numbers for the 2001 version of the standard, if not to the text. To investigate this possibility the 1989 data were compared to the values derived from integration of the Maxwellian function and the results are shown in Table 1. It can be seen that although the agreement is not exact, it is sufficiently good to suggest that the1989 data were indeed derived from a numerical integration of a Maxwellian function with perhaps a different method used to perform the integration.

In order to investigate the possibility that the 2001 data are based on a different approach, developments in measurements and evaluations of the ^{252}Cf spectrum in the period leading up to 2001 were investigated. The fact that a Maxwellian is not a good representation of the ^{252}Cf spectrum at all energies had been shown in an evaluation published in 1975 although a derivation of a smooth spectrum over the entire range would be difficult from this paper as information is only given in broad energy bins [4]. A great deal of work was undertaken in this period, involving extensive evaluation of a number of experimental measurements, by W. Mannhart. Important insights can be found in his paper *Status of the Cf-252 fission neutron spectrum evaluation with regard to recent experiments*. This was published in 1989 in the IAEA INDC document NDS-220 [5]. The data plotted there show that the evaluated spectrum is lower than a Maxwellian at both ends of the energy range and in particular by more than 30% at the upper end. The results of Croft and Miller show that the spectral data from the ISO 2001 standard are also lower than those obtained from numerical integration of a Maxwellian at high and low energies thus raising the possibility that the ISO 8529-1 values may have been based on evaluated data rather than the Maxwellian function.

Various versions of Mannhart's evaluation of the ^{252}Cf spectrum are available. Reference 5, does not unfortunately contain any tabulated data. An earlier publication, NDS-98 [6],

Group	Energy (MeV)	ISO 8529 (1989) fluence		Maxwellian		Difference %
		/group	/lethargy	/group	/lethargy	
1	4.14E-07	4.44E-04	4.40E-05	4.43E-04	4.39E-05	-0.31%
2	0.01	4.41E-03	2.74E-03	4.42E-03	2.75E-03	0.32%
3	0.05	8.60E-03	1.24E-02	8.61E-03	1.24E-02	0.20%
4	0.10	2.31E-02	3.33E-02	2.31E-02	3.33E-02	0.04%
5	0.20	1.35E-02	6.04E-02	1.35E-02	6.05E-02	0.09%
6	0.25	1.44E-02	7.90E-02	1.44E-02	7.90E-02	-0.02%
7	0.30	3.08E-02	1.07E-01	3.08E-02	1.07E-01	0.03%
8	0.40	3.26E-02	1.46E-01	3.26E-02	1.46E-01	-0.09%
9	0.50	3.35E-02	1.84E-01	3.36E-02	1.84E-01	0.01%
10	0.60	3.41E-02	2.21E-01	3.40E-02	2.21E-01	-0.20%
11	0.70	3.41E-02	2.55E-01	3.40E-02	2.55E-01	-0.03%
12	0.80	6.72E-02	3.01E-01	6.71E-02	3.01E-01	-0.16%
13	1.0	6.44E-02	3.53E-01	6.44E-02	3.53E-01	0.11%
14	1.2	6.09E-02	3.95E-01	6.09E-02	3.95E-01	-0.06%
15	1.4	2.89E-02	4.19E-01	2.89E-02	4.19E-01	0.04%
16	1.5	2.79E-02	4.32E-01	2.79E-02	4.32E-01	-0.04%
17	1.6	5.25E-02	4.46E-01	5.25E-02	4.46E-01	-0.02%
18	1.8	4.83E-02	4.58E-01	4.82E-02	4.58E-01	-0.03%
19	2.0	4.40E-02	4.62E-01	4.41E-02	4.62E-01	0.04%
20	2.2	2.05E-02	4.61E-01	2.05E-02	4.61E-01	0.09%
21	2.3	1.95E-02	4.59E-01	1.95E-02	4.59E-01	0.03%
22	2.4	3.63E-02	4.53E-01	3.63E-02	4.53E-01	0.03%
23	2.6	3.28E-02	4.42E-01	3.27E-02	4.42E-01	-0.05%
24	2.8	2.95E-02	4.27E-01	2.95E-02	4.27E-01	0.07%
25	3.0	5.02E-02	4.01E-01	5.02E-02	4.01E-01	0.02%
26	3.4	3.09E-02	3.66E-01	3.10E-02	3.66E-01	0.07%
27	3.7	4.12E-02	3.25E-01	4.12E-02	3.25E-01	-0.06%
28	4.2	2.53E-02	2.78E-01	2.53E-02	2.78E-01	0.04%
29	4.6	1.99E-02	2.39E-01	1.99E-02	2.39E-01	0.06%
30	5.0	1.90E-02	1.99E-01	1.90E-02	1.99E-01	0.23%
31	5.5	1.40E-02	1.61E-01	1.40E-02	1.61E-01	-0.13%
32	6.0	1.02E-02	1.28E-01	1.03E-02	1.28E-01	0.14%
33	6.5	7.48E-03	1.01E-01	7.50E-03	1.01E-01	0.17%
34	7.0	5.46E-03	7.92E-02	5.47E-03	7.92E-02	0.01%
35	7.5	3.98E-03	6.16E-02	3.97E-03	6.16E-02	-0.04%
36	8.0	2.89E-03	4.76E-02	2.88E-03	4.76E-02	-0.09%
37	8.5	2.09E-03	3.65E-02	2.09E-03	3.65E-02	0.08%
38	9.0	1.51E-03	2.79E-02	1.51E-03	2.79E-02	0.10%
39	9.5	1.09E-03	2.13E-02	1.09E-03	2.13E-02	-0.23%
40	10.0	1.35E-03	1.42E-02	1.35E-03	1.42E-02	-0.10%
41	11.0	7.00E-04	8.04E-03	7.00E-04	8.04E-03	0.03%
42	12.0	3.61E-04	4.51E-03	3.61E-04	4.51E-03	-0.03%
43	13.0	1.85E-04	2.50E-03	1.86E-04	2.50E-03	0.12%
44	14.0	1.44E-04	1.08E-03	1.44E-04	1.08E-03	-0.36%
45	16.0	3.77E-05	3.20E-04	3.74E-05	3.18E-04	-0.66%
	18.0					

Table 1: Comparison of ISO 8529 (1989) spectral data with integration of a Maxwellian function. Data are presented as both group fluences and fluences per unit lethargy as tabulated in the standard. The energy quoted in a row is for the lower boundary of the group.

in 1987 consists of a paper by Mannhart entitled, *Cf-252 Neutron Spectrum* and the spectral information is presented as 271 point data values between 1 keV and 20 MeV, or as 70 group-averaged values between 15 keV and 20 MeV. Since the ISO 8529-1 spectrum extends down to 0.414 eV it is unlikely that it was obtained entirely from NDS-98. However, to investigate whether some or all of the NDS-98 data might have been used to derive the ISO 8529-1 spectrum the point data were transformed into group data in the ISO group structure and the differences calculated. (The interpolation procedures specified in NDS-98 were used.) The differences were generally relatively small being less than 4% over most of the energy range, although 12% for the highest energy bin. These differences are sufficiently large to indicate that the ISO 8529-1 data did not come from NDS-98.

The evaluation produced by Mannhart was eventually used in the ENDF/B evaluated data files [7]. In the most recent version, ENDF/B-VII, the spectrum is presented in both a 71 group representation and as fluence per unit energy point data. (The grouped data have one more group, from 0 to 15 keV, than NDS-98). The point data are given as 122 numbers extending from 0 to 20 MeV although the lowest energy with a non-zero fluence value is 10^{-5} eV. These point data thus cover the whole range of the spectrum as presented in ISO 8529-1. They have been re-binned into the ISO 8529-1 group structure by first deriving an average fluence per unit energy over the group, using a linear-linear interpolation between the points, and then multiplying by the group energy width to derive the group fluence. As a test of the procedure the point data were re-binned into the 71 group representation and the results reproduced those of ENDF/B-VII exactly. The results in the ISO group structure are compared with ISO 8529-1 and a Maxwellian with T = 1.42 MeV in Figure 1 and Table 2.

In the figure the data have been plotted as histograms and this highlights the large widths of the low energy groups when viewed on a logarithmic scale. On a linear scale they would of course be very narrow. The figure shows that the ISO 8529-1 spectrum is a better estimate of the ENDF/B-VII spectrum than a Maxwellian with T = 1.42 MeV for the vast majority of the bins, but with the notable exception of the second and third bins. The reason for this is not clear, but the fact that these two bins are the widest on a lethargy scale may be significant. The fact that the Maxwellian spectrum and the ISO 8529-1 spectrum diverge from the ENDF/B-VII evaluation in opposite directions is perhaps surprising.

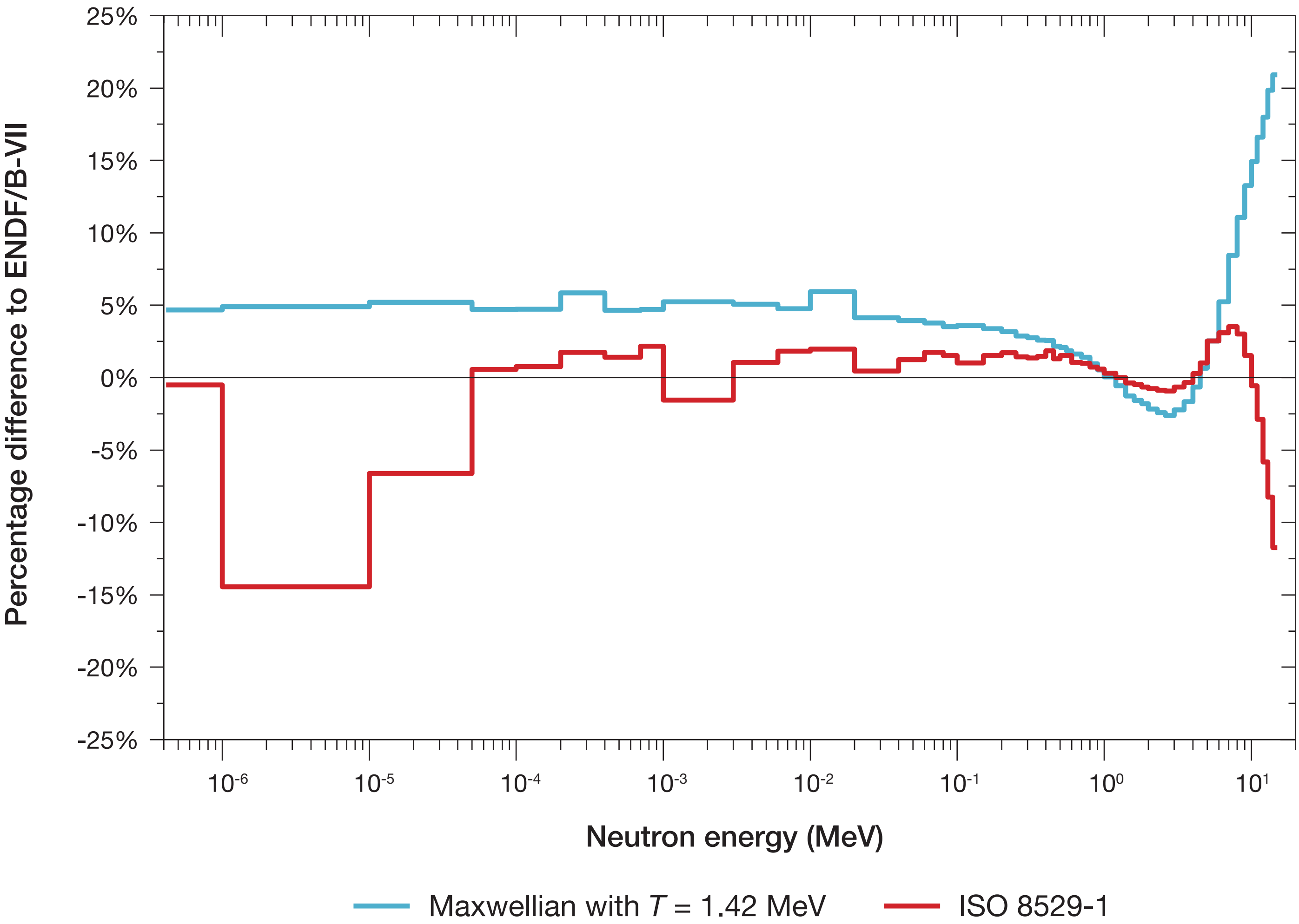


Figure 1: Percentage differences between ENDF/B-VII and a Maxwellian at T=1.42 MeV or ISO 8529-1 (2001) for each group of the ^{252}Cf spectrum tabulated in the ISO standard.

Group	Energy (MeV)	ENDF/B-VII group fluence	Maxwellian T=1.42 MeV		ISO 8529-1	
			Group fluence	Difference to ENDF/B	Group fluence	Difference to ENDF/B
1	4.14E-07	3.12E-10	3.26E-10	4.66%	3.10E-10	-0.50%
2	1.0E-06	1.30E-08	1.36E-08	4.90%	1.11E-08	-14.45%
3	1.0E-05	1.36E-07	1.43E-07	5.22%	1.27E-07	-6.62%
4	5.0E-05	2.75E-07	2.87E-07	4.70%	2.76E-07	0.55%
5	1.0E-04	7.76E-07	8.13E-07	4.74%	7.82E-07	0.77%
6	2.0E-04	2.17E-06	2.30E-06	5.85%	2.21E-06	1.75%
7	4.0E-04	4.47E-06	4.68E-06	4.64%	4.53E-06	1.40%
8	7.0E-04	5.56E-06	5.82E-06	4.71%	5.68E-06	2.18%
9	1.0E-03	5.60E-05	5.89E-05	5.24%	5.51E-05	-1.55%
10	3.0E-03	1.27E-04	1.33E-04	5.06%	1.28E-04	1.03%
11	6.0E-03	2.26E-04	2.37E-04	4.76%	2.30E-04	1.84%
12	0.01	7.59E-04	8.04E-04	5.94%	7.74E-04	1.98%
13	0.02	2.16E-03	2.25E-03	4.15%	2.17E-03	0.44%
14	0.04	2.77E-03	2.87E-03	3.93%	2.80E-03	1.25%
15	0.06	3.23E-03	3.36E-03	3.76%	3.29E-03	1.75%
16	0.08	3.63E-03	3.75E-03	3.53%	3.68E-03	1.52%
17	0.10	1.04E-02	1.08E-02	3.59%	1.05E-02	1.00%
18	0.15	1.19E-02	1.23E-02	3.37%	1.21E-02	1.52%
19	0.20	1.31E-02	1.35E-02	3.17%	1.33E-02	1.72%
20	0.25	1.40E-02	1.44E-02	2.86%	1.42E-02	1.43%
21	0.30	1.47E-02	1.51E-02	2.76%	1.49E-02	1.34%
22	0.35	1.53E-02	1.57E-02	2.58%	1.55E-02	1.46%
23	0.40	1.57E-02	1.61E-02	2.56%	1.60E-02	1.86%
24	0.45	1.61E-02	1.64E-02	2.17%	1.63E-02	1.30%
25	0.50	1.64E-02	1.67E-02	2.08%	1.66E-02	1.53%
26	0.55	1.66E-02	1.69E-02	1.87%	1.68E-02	1.51%
27	0.60	3.35E-02	3.40E-02	1.64%	3.38E-02	1.05%
28	0.70	3.36E-02	3.40E-02	1.41%	3.39E-02	0.99%
29	0.80	3.35E-02	3.38E-02	0.96%	3.37E-02	0.72%
30	0.90	3.31E-02	3.33E-02	0.54%	3.33E-02	0.60%
31	1.0	6.44E-02	6.44E-02	0.05%	6.46E-02	0.31%
32	1.2	6.12E-02	6.09E-02	-0.57%	6.12E-02	0.00%
33	1.4	5.75E-02	5.68E-02	-1.27%	5.73E-02	-0.38%
34	1.6	5.34E-02	5.25E-02	-1.57%	5.31E-02	-0.49%
35	1.8	4.91E-02	4.82E-02	-1.79%	4.88E-02	-0.65%
36	2.0	6.60E-02	6.46E-02	-2.18%	6.55E-02	-0.76%
37	2.3	5.72E-02	5.58E-02	-2.43%	5.67E-02	-0.88%
38	2.6	6.39E-02	6.22E-02	-2.63%	6.33E-02	-0.94%
39	3.0	6.25E-02	6.11E-02	-2.22%	6.21E-02	-0.64%
40	3.5	4.70E-02	4.62E-02	-1.66%	4.68E-02	-0.34%
41	4.0	3.48E-02	3.46E-02	-0.64%	3.49E-02	0.28%
42	4.5	2.55E-02	2.57E-02	0.66%	2.58E-02	1.01%
43	5.0	3.22E-02	3.30E-02	2.54%	3.30E-02	2.54%
44	6.0	1.69E-02	1.78E-02	5.24%	1.74E-02	3.11%
45	7.0	8.70E-03	9.44E-03	8.45%	9.01E-03	3.52%
46	8.0	4.48E-03	4.97E-03	11.06%	4.61E-03	3.00%
47	9.0	2.30E-03	2.60E-03	13.27%	2.33E-03	1.51%
48	10.0	1.18E-03	1.35E-03	14.92%	1.17E-03	-0.55%
49	11.0	6.00E-04	7.00E-04	16.60%	5.83E-04	-2.86%
50	12.0	3.06E-04	3.61E-04	17.99%	2.88E-04	-5.84%
51	13.0	1.55E-04	1.86E-04	19.86%	1.42E-04	-8.25%
52	14.0	7.86E-05	9.51E-05	20.91%	6.94E-05	-11.74%
	15.0					

Table 2: Comparison of ENDF/B-VII ^{252}Cf spectral data with integration of a Maxwellian function and with ISO 8529-1 when all data are grouped into the ISO 8529-1 energy group structure. The energy quoted in a row is for the lower boundary of the group.

The spectral data derived by Mannhart is assumed to be that for un-encapsulated ^{252}Cf. When the ^{252}Cf is encapsulated the spectrum changes slightly, due primarily to scattering. This effect would be most noticeable at low energies so is unlikely to explain the differences between the Mannhart spectrum and the ISO 8529-1 representation at high energies, and at low energies the effect of encapsulation is an increase in the number of neutrons whereas the ISO 8529-1 spectrum is lower than the ENDF/B spectrum in this region. Finally, ^{252}Cf source capsules are physically very small and are not expected to alter the spectrum significantly.

3. Conclusions

As pointed out by Croft and Miller the ISO 8529-1 ^{252}Cf spectrum does not appear to have been derived from a numerical integration of a Maxwellian function. Although the ISO spectrum is, on the whole, a better match to ENDF/B-VII, than a Maxwellian, the correspondence is certainly not exact. The differences between ENDF/B-VII and either the ISO standard or a Maxwellian are small when viewed on absolute terms although large in some areas when viewed as relative values. These large relative differences occur at either end of the spectrum where the fluence as a fraction of the total is small, the fluence in the lowest bin being a factor of more than 10^8 lower than that at the peak, and the uncertainties in the evaluated data are large, up to 30% or more at the highest and lowest energies.

Figure 2 shows a plot of the ^{252}Cf spectrum as fluence per unit lethargy in the ISO energy group structure for: the ISO 8529-1 data, a Maxwellian with T=1.42 MeV, and the binned point data from ENDF/B-VII. In the main plot with logarithmic energy and fluence axes the differences are barely visible, even at the ends of the energy range, because of the very wide dynamic range of fluences. The inset plot, which has linear energy and fluence axes, shows the region around the peak where the relative differences are small, however, in absolute terms they are the largest differences.

The deviations between the data sets are probably negligible in most situations, and the ISO 8529-1 spectrum is adequate for the majority of applications. The text in the standard is, nevertheless, misleading, and any revision should correct it to explain where the spectral data have been derived from. A future revision of the standard will also require a decision to be made on the best data to use.

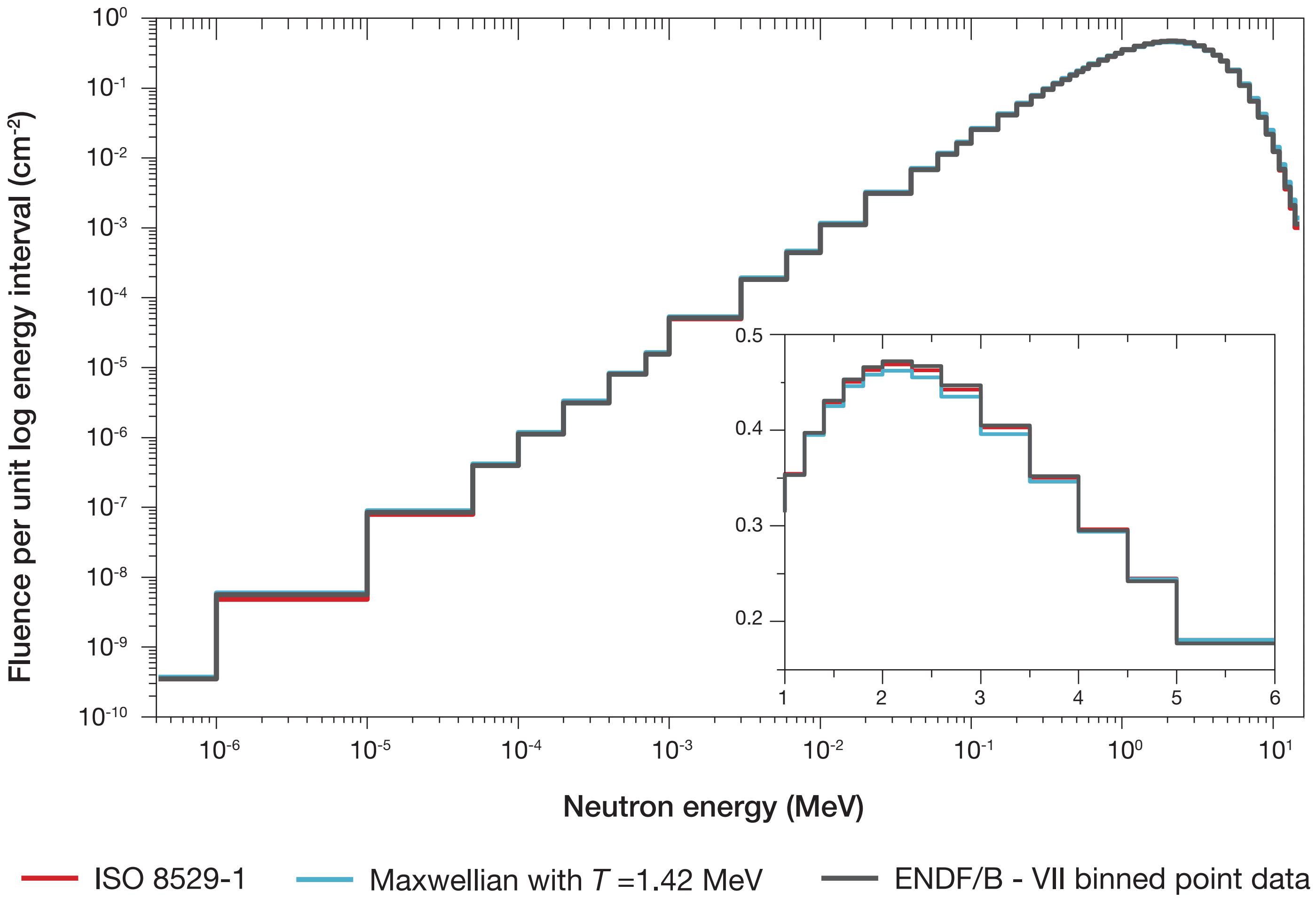


Figure 2: The ^{252}Cf spectrum in the ISO 8529-1 group structure for: tabulated data from ISO 8529-1, a Maxwellian representation with T=1.42 MeV, and binned ENDF/B-VII point data.

4. Acknowledgements

This work was supported by the National Measurement Office, an Executive Agency of the UK government's Department for Business, Innovation and Skills. The author is grateful to Jean-Louis Chartier for insights into the deliberations of the ISO Working Group responsible for the 8529 series of standards on Neutron Reference Fields.

5. References

[1] Croft, S. and Miller, K.A., *Group Representation of the Prompt Fission Neutron Spectrum of* ^{252}*Cf*, ESARDA Bulletin No. 46, December 2011.

[2] International Organization for Standardization, *Reference neutron radiations – Part 1: Characteristics and methods of production,* International Standard, 8529-1, (ISO, Geneva, Switzerland) 2001.

[3] International Organization for Standardization, *Neutron reference radiations for calibrating neutron-measuring devices used for radiation protection purposes and for determining their response as a function of neutron energy*, International Standard, 8529, (ISO, Geneva, Switzerland) 1989.

[4] Grundl, J.A. and Eisenhauer, C.N., *Fission spectrum neutrons for cross section validation and neutron flux transfer, NBS Special Publication 425, Vol. 1 of the proceedings of Nuclear Cross Sections and Technology*, Eds Schrack R.A. and Bowman C.D. (US Government Printing, Washington) 1975.

[5] International Atomic Energy Agency, IAEA, International Nuclear Data Committee, INDC(NDC)-220, *Physics of Neutron Emission in Fission Proceeding of a Consultants Meeting on Physics of Neutron Emission in Fission*, Organized by The International Atomic Energy Agency and held in Mito City, Japan, 24-27 May 1988, Lemmel, H.D.(ed.) June 1989.

[6] International Atomic Energy Agency, IAEA, Nuclear Data services, IAEA-NDS-98, Lemmel, H.D.(ed.) December 1987.

[7] Chadwick, M.B. et al., *ENDF/B-VII.1 Nuclear Data for Science and Technology: Cross Sections, Covariances, Fission Product Yields and Decay Data*, Nuclear Data Sheets 112, 2887–2996, 2011.

Attaining and Maintaining a Continuity of Knowledge to Draw Safeguards Conclusions with Confidence

Robert S. Bean

Purdue University[1]
400 Central Drive, West Lafayette, IN 47907
bean@purdue.edu

Dianna S. Blair

Sandia National Laboratories[2]
PO Box 5800 MS 1371, Albuquerque, NM 87185-1371
dsblair@sandia.gov

Chris A. Pickett

Oak Ridge National Laboratory[3]
PO Box 2008 MS6166, Oak Ridge, TN 37831-6166
pickettca@ornl.gov

Abstract:

As the 21st century progresses, new nuclear facilities and the expansion of nuclear activities into new countries will require the International Atomic Energy Agency (IAEA) to place a higher reliance on attaining and maintaining a Continuity of Knowledge (CoK) of its safeguards information than is currently practiced. Additionally, a conceptual view of where and how CoK can be applied will need to evolve to support improved efficiency and efficacy of drawing a safeguards conclusion for each Member State. The ability to draw a safeguards conclusion for a Member State will be predicated on the confidence that CoK has been attained and subsequently maintained with respect to the data and information streams used by the IAEA. This confidence can be described as a function of factors such as elapsed time since the measurement, surveillance of attributes, authentication of information, historic knowledge of potential system failures, and the number and type of data collections. A set of general scenarios are described for determining what is required to attain CoK and whether CoK has been maintained. A high-level analysis of example scenarios is presented to identify failures or gaps that could cause a loss of CoK. Potential areas for technological research and development are discussed for the next generation of CoK tools.

Keywords: Safeguards; Continuity of Knowledge

1 Purdue University School of Nuclear Engineering. Author was employed at the Idaho National Laboratory at the time this work was performed. The Idaho National Laboratory is operated by the Battelle Energy Alliance under DOE Idaho Operations Office Contract DE-AC07-05ID14517

2 Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

3 This manuscript has been authored by UT-Battelle LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

1. Introduction

Beginning with the entry into force of the "Treaty on the Non-proliferation of Nuclear Weapons" in 1970, signatory Member States agreed to declare to the International Atomic Energy Agency (IAEA) the location, quantity, and use of fissile materials under their control. [1] The IAEA in turn is charged with verifying the declaration with the goal of drawing a safeguards conclusion regarding whether the fissile material in the Member State has remained in peaceful use. [2] The IAEA develops a safeguards approach with each country, typically under the auspices of INFCIRC/153, to gather, both via declaration by the State and measurement and inspection activities by the IAEA, the information needed to draw a safeguards conclusion. [3] Under the Additional Protocol, the IAEA has additional authority to access and inspect all aspects of a State's nuclear activities in order to verify that there are no undeclared fissile materials or activities related to diversion of nuclear material from peaceful purposes. Therefore, the IAEA is tasked with verifying the *correctness* (i.e. declared materials and activities) and the *completeness* (i.e. lack of undeclared materials and activities) of each Member State's declarations.

Historically, nuclear material accountancy (NMA), or rather direct measurement of the nuclear material (via either destructive or nondestructive assay), has formed the basis for safeguards conclusions. For example, a Member State's declarations of material production can be verified by an inspector measuring the product material with IAEA equipment. In addition to NMA, containment and surveillance (C/S), often in the form of container seals and video camera systems, provides a complementary means to verify Member State declarations. For example, declarations involving fuel movements can be checked against video footage to determine if the IAEA system recorded the same number of fuel elements being loaded, or intact seals can verify that other fuel has not been transferred without being declared. Together, NMA and C/S are used to attain knowledge about the nuclear material activities, and then further used to maintain that knowledge, preferably in a continuous fashion.

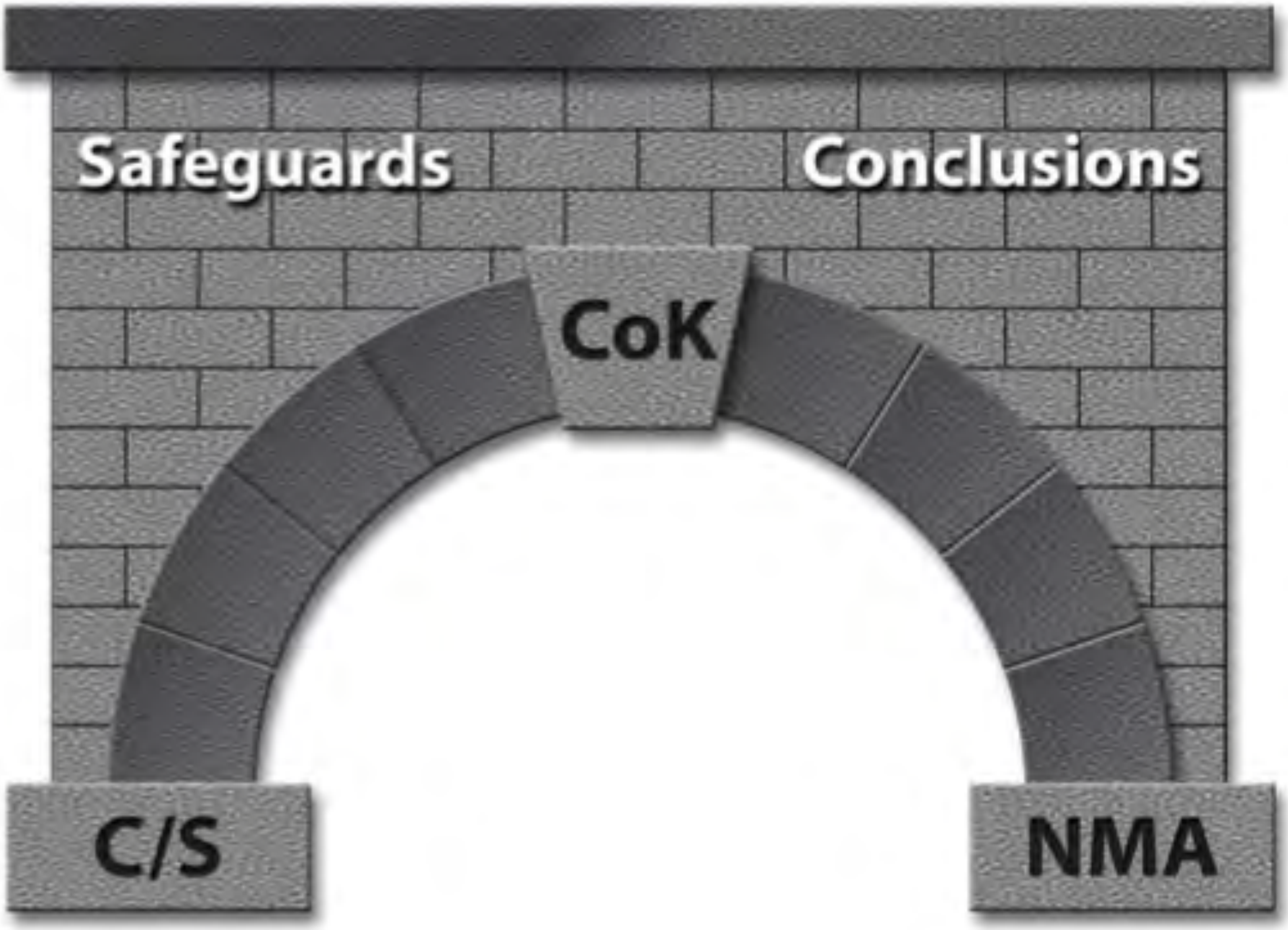


Figure 1: Built on a foundation of nuclear material accountancy (NMA) and containment and surveillance measures (C/S), Continuity of Knowledge (CoK) provides the confidence to support a safeguards conclusion. [4]

Continuity of Knowledge (CoK) for safeguards is the outcome of "a system of data or information regarding an item or activity that is uninterrupted and authentic and provides the IAEA with adequate insight to draw definitive conclusions that nuclear material is not being diverted from peaceful purposes." [4, 5] In other words, attaining and maintaining CoK is the goal of safeguards measures. If this outcome is achieved, a safeguards conclusion can be supported with confidence.

Note that while the examples of NMA and C/S were used to describe attaining and maintaining CoK, the principle is fully extensible to other types of data that are used to inform the safeguards conclusion. Complimentary access visits under the Additional Protocol, surveys of literature and publications, and shipping and receiving records, are other examples of means to provide information and therefore contribute to attaining and maintaining CoK. As the IAEA further refines the state level concept and moves to safeguard not only newly constructed but new *types* of nuclear facilities (such as long-term geologic repositories), the safeguards approach will require a reliance on information that goes beyond traditional NMA.

The ability of the IAEA to draw a safeguards conclusion about a Member State's activities will be predicated on IAEA confidence that it has been able to attain and subsequently maintain CoK.

2. Sampling Theory

Maintaining CoK requires that periodic "checks" be performed to renew confidence that the knowledge is still current and correct. While continuous and/or real-time monitoring are often espoused as the ideal, the reality is that continuous or near-continuous checks generate a tremendous quantity of data that may not necessarily improve the confidence that CoK has been maintained. There is an optimum rate that produces the maximum information, or rather confidence that the collected information is correct, without overwhelming both the data collection system and the safeguards inspector who must evaluate the results.

The case of simple production of digital sound files provides an example of sampling theory. [6] A natural signal, from a voice or from a musical instrument is inherently analog. To process these signals in computers, we must convert them to a digital form. While an analog signal is

**Long-term fuel storage:
A case where CoK will be primary over NMA**

When spent nuclear fuel is packaged for long term disposition in a geological repository, the nuclear material quantities should be established via NMA. Whether measured by existing techniques, or future advanced techniques [9], NMA establishes the inspector's knowledge of the nuclear material quantity. During short term storage and transportation to the geologic repository, additional measures such as C/S to maintain CoK can eliminate the need for to re-measurement of the fuel. During the operational and post-closure periods C/S measures could provide CoK for the site and the material under safeguards.

As the geologic repository is filled, it becomes increasingly difficult to perform NMA. Measures such as C/S are used to maintain CoK of the nuclear material. Eventually, the repository will be backfilled, and further NMA will be impossible. Even C/S measures such as container seals will have reduced effectiveness due to the inability to physically verify those that have been buried. Maintaining CoK through measures such as C/S on the repository entrance and seismic monitoring for undeclared digging will become the primary means to maintain Cok and thus support a safeguards conclusion about the nuclear material.

continuous in both time and amplitude, a digital signal is discrete for both. A process called "digitizing," or "sampling" is used to convert a signal from continuous time to discrete time. The value of the original signal is measured, or sampled, at certain time intervals. The necessary rate of taking samples to ensure appropriate preservation of the original analog information is defined by the Sampling Theorem. The Sampling Theorem simply states that if the original signal contains high frequency components, it must be sampled at a rate higher than the highest frequency component in the original signal to avoid losing information. [7] To preserve the full information of the signal, it is necessary to sample at a rate of twice the maximum frequency of the signal, known as the Nyquist rate. The Nyquist rate gives a reliable benchmark for accurately preserving analog information.

If we sample a signal at a frequency lower than the Nyquist rate it will exhibit a phenomenon called "aliasing" when the signal is converted back into a continuous time signal. Aliasing results from unwanted or missing frequency components in the reconstructed signal and can distort the resulting information. Examples of aliasing can be seen on automobiles where the wheels of a moving vehicle appear to be turning backwards as the vehicle propels forward. This is due to your eye sampling the image at a slower rate (around 10 or 12 times per second) than the vehicle's distinctive rim or hubcap features are moving. The eye, therefore, is losing information because it is sampling too slowly. Conversely, movies appear to display continuous motion because they are filmed at a rate of 30 frames per second—at least twice the rate your eye refreshes—although your eye still will perceive the film of a wheel rotating backward due to the limitations of the eye.

In safeguards, we must ask ourselves, "How much information is needed to maintain CoK?" The sampling rate for checking and re-checking an information stream must be equivalent to or greater than the Nyquist rate for the information signal being sampled. This will be determined by factors such as the type of technology collecting the information, the attractiveness of the nuclear material, the potential diversion or misuse of that material, and the time scale of the diversion or misuse actions. For example, in a situation where low enriched uranium fresh reactor fuel is in storage before being loaded into a reactor, the combination of C/S, possible diversion scenarios (such as diversion to a clandestine enrichment facility and subsequent enrichment to highly enriched uranium), and the safeguards inspection schedule would allow a diversion analysis to be performed on the time required for operator diversion of one significant quantity of U-235 (75 kg of U-235 in the form of enriched uranium enriched to <20%). If we assume that in this case the result of the analysis is that the diversion would take twelve months, then maintaining CoK by "sampling" the facility every six months or less provides assurance that the diversion would be detected without creating an overwhelming demand for either physical inspections or information collection.

Additionally, the concept of nested sampling, familiar to computer programmers, must be considered. For each potential concern, each component will need to be sampled at a minimum rate equal to the Nyquist rate. For example, while it may be necessary for an inspector to visually verify an electronic seal only on a monthly basis, the seal electronics may need to self-test for tamper indications every millisecond and verify communications connections with the data collection system every few seconds. Each part of the system must be sampled, or monitored, such that there is confidence that no information has been lost.

3. Maintaining Continuity of Knowledge

Once knowledge has been attained, maintaining CoK is required to have confidence that the knowledge is still correct and, therefore, useable. Continuity of Knowledge must be maintained in such a way that the information is sampled at the appropriate rate to identify issues in a timely fashion. Continuity of Knowledge must be attained and subsequently maintained with sufficient confidence that the knowledge can be used to support a safeguards conclusion. This confidence can be described as a function of factors such as the level of initial knowledge, elapsed time since the measurement, surveillance of attributes, authentication of information, historic knowledge of potential system failures, and the number and type of data collections. Additional information, such as indications of attempted tampering, adversary sophistication, and advances in technology will also impact this confidence. This concept is described by the following function:

$$C_{CoK\ method} = f(\textit{initial knowledge, time, sampling rate, failure rate, adversary actions, ...}) \quad \text{(Eq. 1)}$$

where $C_{CoK/method}$ is the confidence that CoK has been maintained by the particular system or method in question. The value of $C_{CoK/method}$ would be expressed as a percentage between 0 and 100%, where 0% indicates no confidence at all and 100% represents complete confidence that the method in question has maintained CoK. For simplicity, if you assume that the various factors are independent of each other, the confidence that CoK has been maintained by that method can be expressed in the form:

$$C_{CoK\ method} = f(\textit{initial knowledge}) \times f(\textit{time}) \times f(\textit{sampling rate}) \times f(\textit{failure rate}) \times f(\textit{adversary actions}) \times f(...) \quad \text{(Eq. 2)}$$

where this equation represents $C_{CoK\ method}$ as a function of the indicated factor. These functions can also be described in terms of the confidence that they provide to the overall $C_{CoK\ method}$.

$$C_{CoK\ method} = C_{time} \times C_{CoK\ sampling\ rate} \times C_{CoK\ failure\ rate} \times \ldots \quad \text{(Eq. 3)}$$

Similarly, the confidence that each component provides would range from 0 to100%. Mathematically, equation 2 is multiplicative, because the failure of any component ($C_{CoK/component} = 0$) would drive $C_{CoK/method}$ for the entire method to zero. In practice, the principle of defense in depth leads to the use of multiple, potentially redundant, methods to maintain CoK. In this case the overall confidence that CoK was maintained will be additive as in:

$$C_{CoK\ overall} = \frac{\sum_{i=1}^{n} \omega_i C_{CoK\ method\ i}}{\sum_{i=1}^{n} \omega_i} \quad \text{(Eq. 4)}$$

where is the weighting factor, or "quality or effectiveness" of each method, indicating how much that method contributes to the overall confidence that CoK has been maintained. Note that equation 4 is a significant simplification as there may be interdependencies (such as common modes of failure) and no matter how many methods are used total confidence cannot exceed 100%.

In practice, confidence that CoK has been maintained will be highest at the time of a verification action. For an item of nuclear material, this would ideally be quantitative assay. As time passes, confidence that the knowledge in the records correctly reflects the safeguarded item declines. Questions about actions since the last verification - Has the item been moved? Has the seal been broken? Has the unattended monitor failed? Has the operator done something that impacts the item? – can reduce, per equations 2 and 3, the confidence that CoK has been maintained. When the next monitoring action is taken, the confidence is restored to a high level. Failure of a component ($C_{CoK/component} = 0$) will cause a step change to lower confidence that CoK has been maintained. At some reduced level of confidence, it can no longer be sufficiently assured that CoK has been maintained to depend on that knowledge to draw a conclusion. In this case, a full re-verification is necessary to re-establish CoK.[4]

Previous work has demonstrated this principle, see Figure 3. [8] For both a passive and an active tamper indicating device (TID), the probability of sensing a tamper event was calculated with respect to time. The rising and falling of the probability of detecting a tamper event for the passive TID correspond to when the device is monitored (i.e. visually inspected) and subsequently left in place. The much smaller fluctuations of the active device are due to the faster sampling rate, allowing the confidence in the TID to be maintained at a high level. In both cases, the probability of sensing a tamper event (in other words, the confidence that the device has maintained CoK of the sealed item) is a function of time, selected technology, and potential adversary actions as described in equation 3.

The systems chosen to attain and maintain CoK must, therefore, take into account the principles of:

- accuracy and precision of initial knowledge;
- appropriate sampling rate for each component, or sub component;
- appropriate reporting rate for active items (not necessarily the same as the sampling rate);
- effects over time of confidence in CoK for each component, such as:
  - technology failure rates,
  - effectiveness of technology selections, and
  - adversary capability advances; and

[4] It should be noted that this is a departure from the current IAEA practice regarding the use of multiple containment and surveillance (C/S) methods to maintain CoK. According to the IAEA Safeguards Glossary [10], where a "dual C/S" system is used (i.e. more than one method to give an overall confidence that CoK has been maintained) "…an acceptable C/S result is obtained when both C/S devices function as specified, their data confirm the validity of the operator's declarations and there is no evidence of tampering." The inverse of this is that when either system fails, the confidence that CoK has been maintained is lost (e.g. *CCoK overall = 0*). The more robust concept described in this paper would have a reduced overall confidence in the event of component or method failure, but would avoid an "all or nothing" approach, resulting in a different impact on the requirement for reverification activities.

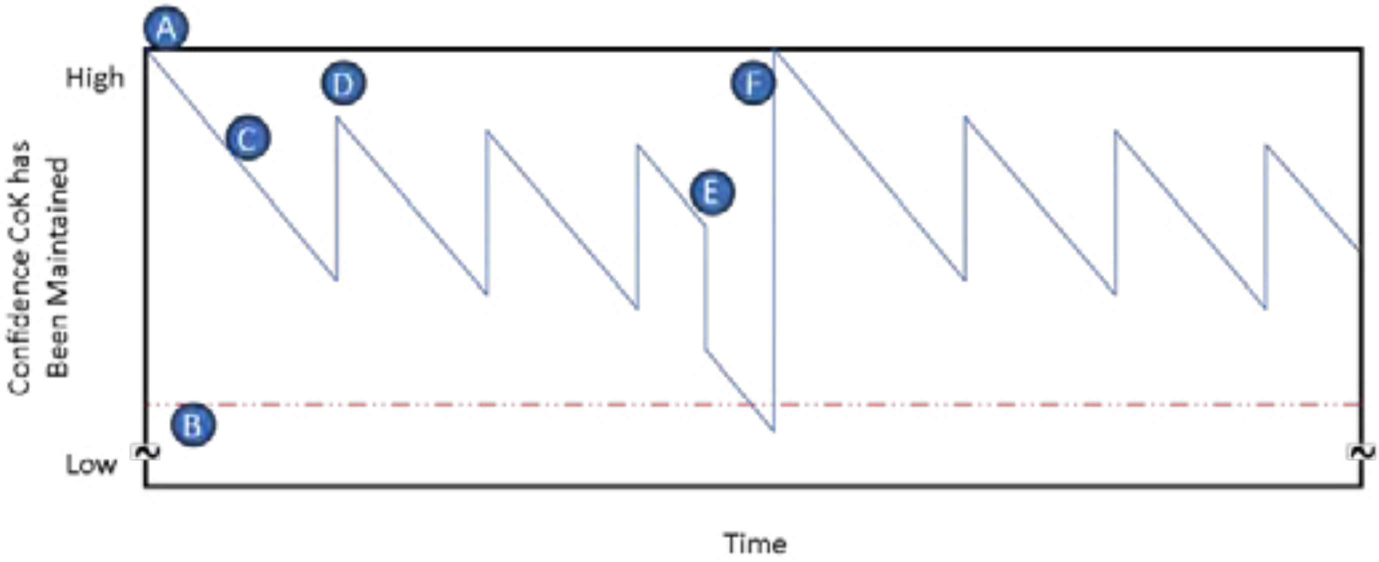


Figure 2: Confidence that CoK has been maintained changes over time. A) When knowledge is first attained (through NMA for a safeguarded item), confidence is highest. B) There is some level of confidence below which it can no longer be assured that CoK has been maintained. C) Confidence that CoK has been maintained falls as time passes. D) Sampling the system (such as through a physical inventory, review of unattended monitoring data, etc.) increases the confidence. E) Events such as equipment failure can cause a step change reduction in confidence. F) If the confidence that CoK has been maintained is lost, a re-verification is required.

- a systems approach for avoiding common failure modes and loss of sufficient confidence in maintaining CoK that re-verification is required.

When a monitoring system is selected properly, there will be sufficient confidence that knowledge regarding the status of the nuclear material was attained, and that CoK was maintained for drawing an overall safeguards conclusion—with confidence.

4. Safeguards CoK Scenarios

Safeguards activities can be grouped, at a high level, into three categories: stable, dynamic, and transportation. Stable facilities are those where nuclear material is typically stored and safeguarded in place after arrival, or moved on a slow, predictable schedule (i.e. scheduled shipments). Dynamic facilities are those where safeguarded nuclear material movement is a constant or near-constant activity, most notably bulk processing facilities. Not only is the material moving, but it may be changing its physical or chemical characteristics as well. Transportation is the category where the nuclear material is not at a safeguarded facility, but is in transit between facilities, and possibly between Member States as well. It would also be appropriate to discuss “sub-facilities” or material balance areas as stable or dynamic; for example, the vault at a processing plant may have nuclear material in storage with a long dwell (storage) time, especially as compared to the processing areas of the same plant.

Descriptions are given for a fuel storage facility as a typical example of a stable facility, a bulk processing facility as a dynamic facility, and a general transportation scenario.

4.1 CoK of Stored Nuclear Material

A stable scenario is fairly straightforward with respect to what is required to attain and then maintain CoK of the nuclear material. When nuclear material is shipped or transferred to the facility, initial knowledge must be established. Ideally, this is done by NMA on site. An inspector then must be able to verify that the material is then stored in the declared location. Various tools, such as unique identification numbers or other unique identifiers (UID), on the nuclear material containers or items, seals to ensure that those containers remain closed, cameras to verify equipment and container movement, gamma or neutron detectors (depending on the nature of the nuclear material) to maintain confidence that the movement was of the declared material, and others, will provide confidence that CoK was maintained through the placement of the item into storage. Once in storage, CoK must be maintained for that nuclear material, possibly for a period of decades or more. Periodic verification of UIDs, tamper indication status of seals, radiation signals, and camera footage can be used to verify that the nuclear material is still in place.

4.2 CoK During Bulk Processing

The crucial distinction, in terms of maintaining CoK, between a stable facility and a dynamic one is that in a dynamic facility there is a potential for a loss of CoK *simply due to the bulk processing* itself. To explain this, consider measurement uncertainty and a simple case of moving nuclear material from one container and splitting it among three others via process equipment. The high confidence that all of the reported material is in the first container is replaced by the confidence that all of the material is now in the three secondary containers.

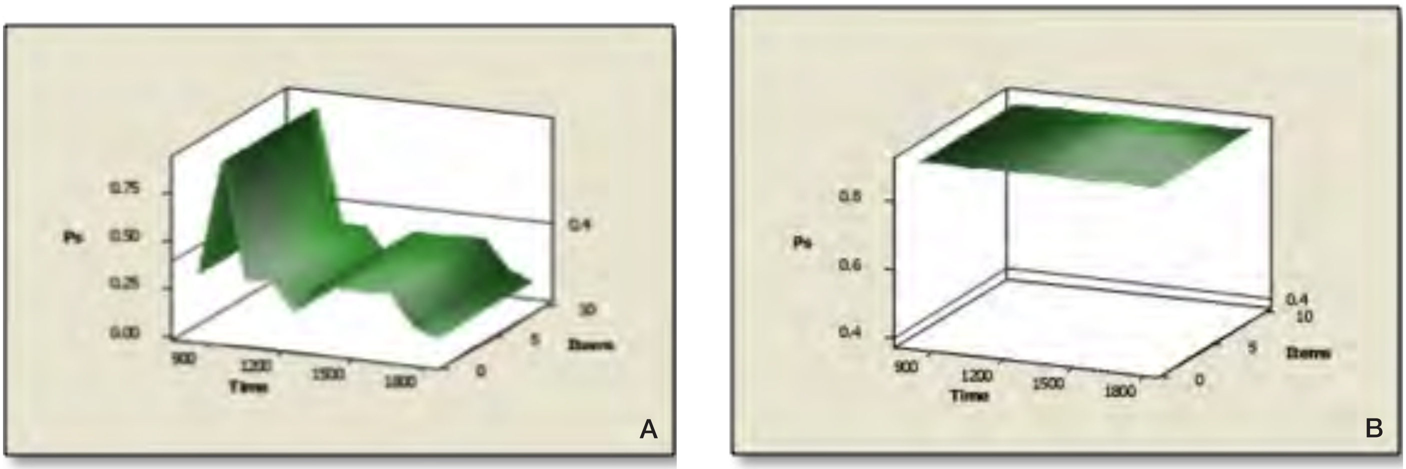


Figure 3: A) Surface Plot of Probability of Sensing Tamper by Passive TID. B) Surface Plot of Probability of Sensing Tamper by Active TID. [8]

Except that it is not all there – some of it is still in the first container as a heel, some of it is in the process equipment as holdup, or some may be in filters. Even if it were possible to easily measure each of these amounts, the total measurement uncertainty will have increased. It is even more important, therefore, to assure that once CoK has been attained, it is maintained throughout the dynamic processes, and it must be maintained at the level of the entire facility, not just for individual items of nuclear material.

As with the stable facility, the nuclear material is, ideally, measured on-site to establish knowledge of the nuclear material quantity. The material will arrive as items or in containers, and thus UIDs and seals can be used to maintain CoK as the material is brought into the facility and prepared for processing (there may be storage areas to be considered, similar to larger stable facilities). Again, cameras, radiation detectors, etc. can be used to verify the movements until the material enters the process. Once in the process, the physical and chemical nature of the material will be changed. It may be chopped, dissolved, chemically converted, mixed, ground, or any other number of steps until the final product is complete. Sufficient monitoring of the processes is vital to provide confidence that the process is operating as declared; in other words, CoK of the process itself must be attained and maintained. This will require process specific monitoring technologies. For example, a CoK of chemical processing plant for spent fuel would use tank level indicators, liquid flow rate monitors, and pH meters, whereas CoK for an enrichment plant would use load cells and enrichment meters. In either case, with maintained CoK, the desired outcome is sufficient confidence that knowledge of the plant operation can be used to draw a safeguards conclusion.

4.3 CoK During Transportation

Maintaining CoK during transportation currently relies upon an active seal attached to a container prior to shipment and verified upon receipt. [9] The goal of the seal is to record any opening of the transport container (e.g., trailer, shipping container, etc.) that occurs during transportation. This approach requires an inspector to be present at either the point of shipment *and* receipt or, minimally, at the point of receipt when the seal is removed. The inspector must verify that the seal was properly applied (e.g., through the hasp) and that the collected information accurately indicates that the item was properly received. This verification also may include a confirmation of physical attribute(s) (i.e. weight and/or NDA).

Many shippers prefer (for a variety of reasons) not to provide real-time active monitoring or surveillance during transport; this type of surveillance has been considered too sensitive or intrusive for shippers to consider. However, emerging needs to improve detection of potential diversion during transport (e.g., of spent fuel) warrant greater monitoring during transport. Technologies and approaches that can provide high assurance that fuel cycle materials leaving one location arrive (intact) to the designated location will need to be developed as the number of global fuel cycle activities that require transportation continue to expand.

4.4 Confidence that CoK Has Been Maintained

When all of the components used for CoK function correctly, an inspector will have sufficient confidence that CoK has been attained and subsequently maintained to use for drawing a safeguards conclusion. When CoK is properly implemented with a systems approach, even the loss of a limited number of components will not reduce the overall confidence enough to lose assurance that the nuclear material is as declared. There will be many commonalities over the three scenarios in the selection of technology and activities to maintain high confidence that CoK has been maintained.

The potential loss of CoK leads to a “Schrödinger’s cat” thought experiment for safeguards. As in the famous example used to explain quantum probabilities, a safeguards inspector has good knowledge of the state of the nuclear material at the time it is verified (i.e. measured and observed). After that, however, the choice of TID, cameras, inspection frequency, unattended monitoring, process monitoring for bulk facilities, etc. gives (or does not give) confidence that the inspector's knowledge represents the true state of that nuclear material. The purpose for maintaining CoK is to produce an outcome where the confidence is high enough to base safeguards conclusions on that knowledge.

What is needed is a rigorous analysis of the impact of each type of technology and inspection activity on the confidence that CoK has been maintained. Simple cases, such as depicted in Figure 3, need to be extended to incorporate disparate technologies and activities. The analyses must include an understanding of the causes and impacts of events including (but in no way limited to):

- Potential loss of CoK. For example, due to power failure, communications loss, adversary nuisance tampering, or adversary malicious attack.
- Changes in vulnerabilities due to technology selections. For example, designs that create penetrations in a tamper indicating enclosure.
- Operational considerations. For example, the trade-off between hardwire and wireless communications.
- Combining independent data. For example, if a seal appears to be broken, but the camera in the same area shows no undeclared activities, what is the impact on overall confidence in CoK?

5. Conclusions

As the number of safeguarded fuel cycle operations expand, and new types of facilities are built and operated, the importance of attaining and subsequently maintaining CoK will continue to increase. Depending on the facility type and use, dependence on CoK could potentially become the primary method by which safeguards inspectors draw a conclusion. To maintain CoK, the safeguards equipment and practices used will need to monitor, or sample, the status of the nuclear material and the CoK components at a rate sufficient to ensure that potential tamper and diversion pathways will be detected. The sampling rate will also need to be appropriately nested to account for varying monitoring needs such as electronic self-monitoring vs. visual inspection. Selection of technology and actions to maintain CoK at safeguarded facilities needs to take into account the declared activities, the nature of the facility, and potential diversion pathways. Selected components to maintain CoK must be considered together as there may be interdependencies of failure modes and each technology has its own potential vulnerabilities. A rigorous analysis of the confidence that CoK has been maintained is needed to assist safeguards inspectors in understanding when they have sufficient confidence that CoK has been maintained to draw safeguards conclusions.

6. References

[1] International Atomic Energy Agency. *Treaty on the Non-Proliferation of Nuclear Weapons*. INFCIRC/140 April 22, 1970.

[2] International Atomic Energy Agency. *Safeguards Statement for 2011*. Available at: http://www.iaea.org/OurWork/SV/Safeguards/documents/es2011.pdf

[3] International Atomic Energy Agency. *The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-proliferation of Nuclear Weapons*. INFCIRC/153 (Corrected), June 1972.

[4] Blair, D., Baldwin, G., Bean, R., Pickett, C., Tolk, K. *A New Look at Continuity of Knowledge: Safeguarding the 21st Century Nuclear Fuel Cycle*. ICFO-SI 9 – The 9th International Conference on Facility Operations- Safeguards Interface, Savannah, Georgia, USA, September 23-28, 2012, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2012).

[5] Baldwin, G., Pickett, C., Bean, R., Blair, D., Lawson, R, Rowe, N., Tolk, K. *The Importance of Establishing and Maintaining Continuity of Knowledge During 21st Century Nuclear Fuel Cycle Activities*. Journal of Nuclear Materials Management, Volume 40, Issue 4, July 2012, Page 86.

[6] Zawistowski, T., Shah, P. *An Introduction to Sampling Theory*. Web Applet available at http://www2.egr.uh.edu/~glover/applets/Sampling/Sampling.html

[7] Texas Instruments. AN-236 *An Introduction to the Sampling Theorem*. Texas Instruments Application Report, Texas Instruments, SNAA079C–May 2004–Revised May 2004

[8] Dawson, P., Hester, P. *Real-Time Effectiveness Approach to Protecting Nuclear Materials*. Proceedings of the INMM 47th Annual Meeting, Tucson, AZ, July 8-12, 2007. SAND 2006-3653

[9] Pregent, W., Kelly, S. *Tracking and Monitoring Nuclear Materials During Transit*. Sandia National Laboratories SAND99-1577C.

Unattended Safeguards Instrumentation at Centrifuge Enrichment Plants

L. Eric Smith, Alain R. Lebrun, Rocco Labella

International Atomic Energy Agency Wagramerstrasse 5, Vienna, Austria
E-mail: e.smith@iaea.org, a.lebrun@iaea.org, r.labella@iaea.org

Abstract:

As global uranium enrichment capacity under international safeguards expands, the International Atomic Energy Agency (IAEA) is challenged to develop effective safeguards approaches at gaseous centrifuge enrichment plants, particularly high-capacity plants, while working within budgetary constraints. New safeguards approaches should meet the high-level verification objectives for such facilities (i.e., timely detection of: diversion of declared material, excess production beyond declared amounts, and production of enrichment levels higher than declared), but should also strive for efficiency advantages in implementation, for both the IAEA and operators. Under the Agency's State- level approach to safeguards implementation, the Agency needs a flexible toolbox of technologies, allowing tailoring of safeguards measures for each individual enrichment facility. In this paper, the potential roles and development status for three different types of unattended measurement instrumentation are discussed. On-Line Enrichment Monitors (OLEM) could provide continuous enrichment measurement for 100% of the declared gas flowing through unit header pipes. Unattended Cylinder Verification Stations (UCVS) could provide unattended verification of the declared uranium mass and enrichment of 100% of the cylinders moving through the plant, but also apply and verify an 'NDA Fingerprint' to preserve verification knowledge on the contents of each cylinder throughout its life in the facility. Sharing of the operator's load cell signals from feed and withdrawal stations could count all cylinders introduced to the process and provide periodic monitoring of the uranium mass balance for in-process material. The integration of load cell, OLEM and UCVS data streams offers the possibility for 100% verification of declared cylinder flow, and enables the periodic verification of the declared ^{235}U mass balance in the plant. These new capabilities would enhance the IAEA's effectiveness in meeting the high-level verification objectives at enrichment facilities. In addition, such unattended instrumentation could reduce or eliminate the need for routine interim inspections, and significantly reduce the need for drawing samples from gas and cylinders during inspections—thereby achieving operational efficiencies.

Keywords: enrichment plants; unattended instruments; non-destructive assay

1. Introduction

The IAEA's model safeguards approach for gas centrifuge enrichment plants [1] describes the challenges associated with safeguarding large centrifuge enrichment plants, and defines the high-level verification objectives for enrichment plant safeguards approaches, i.e., the timely detection and deterrence of:

a) diversion of natural, depleted or low-enriched UF_6 from the declared flow in the plant;

b) misuse of the facility to produce undeclared product (at the normal product enrichment levels) from undeclared feed (i.e., excess production);

c) misuse of the facility to produce UF_6 at enrichments higher than the declared maximum, in particular highly enriched uranium.

At present, the IAEA's safeguards approaches at enrichment plants are based on a combination of routine and random inspections, during which time a number of verification activities are performed, including: environmental sampling (ES) for subsequent laboratory analysis; collection of UF_6 samples from in-process material and selected cylinders for subsequent destructive analysis (DA) in a laboratory; weighing and nondestructive assay (NDA) of a subset of the plant's cylinder flow and inventory. The weight measurements of cylinders are performed using either operator-owned scales or the IAEA's portable hanging load cells, while the NDA measurements utilize handheld gamma-ray spectrometers combined with ultrasonic wall-thickness gauges.

Detection of prominent diversion scenarios could be improved at enrichment plants if the IAEA could monitor 100% of material flows and periodically calculate independent uranium and ^{235}U mass balances for the facility. However, human and financial resources preclude continuous inspector presence at the facility to measure all of the material flow using today's attended methods. Further, the portable measurement methods currently used by inspectors have relatively low accuracy for both the total uranium mass and ^{235}U enrichment in a cylinder, which would lead to very large uncertainties on a ^{235}U balance based on such instruments. The poor accuracy of today's cylinder verification instruments necessitates additional safeguards measures, including the destructive analysis of UF_6 samples drawn from some of the cylinder population. These are among the reasons that the IAEA is exploring how unattended instruments capable of continuously and more accurately verifying material flows (both in-process gas and cylinders) on a quasi-continuous basis could help improve the deterrence and timely detection of protracted diversion scenarios. This paper discusses three candidate unattended measurement systems currently being considered by the IAEA: On-Line Enrichment Monitors (OLEM), Unattended Cylinder Verification Stations (UCVS), and sharing of the operator's load cell signals (Figure 1).

These unattended instruments are potential tools in a flexible toolbox of safeguards measures that is aimed at addressing the verification challenges posed by advanced centrifuge technologies and the growth in separative work unit capacity at modern centrifuge enrichment plants [2][3][4]. Permanently installed, unattended instruments could perform the routine and repetitive measurements previously performed by inspectors, thereby allowing the inspectors to use their time on tasks and investigation that depend more heavily on human intuition and decision making. When combined with other safeguards measures, unattended instruments at centrifuge enrichment plants have the potential to significantly improve the Agency's effectiveness to detect and deter the primary diversion scenarios of concern, while simultaneously improving the efficiency of facility-level safeguards approaches. Further, the unattended measurement systems have the potential to be beneficial to facility operators as well, for example for process control, for meeting regional or State regulatory requirements, or to ease and expedite the process for releasing cylinders from the facility. Identifying and developing improvements in safeguards efficiency, while maintaining or improving effectiveness, are important considerations as the IAEA fully implements the State-level concept and evolves the role of safeguards technologies [5].

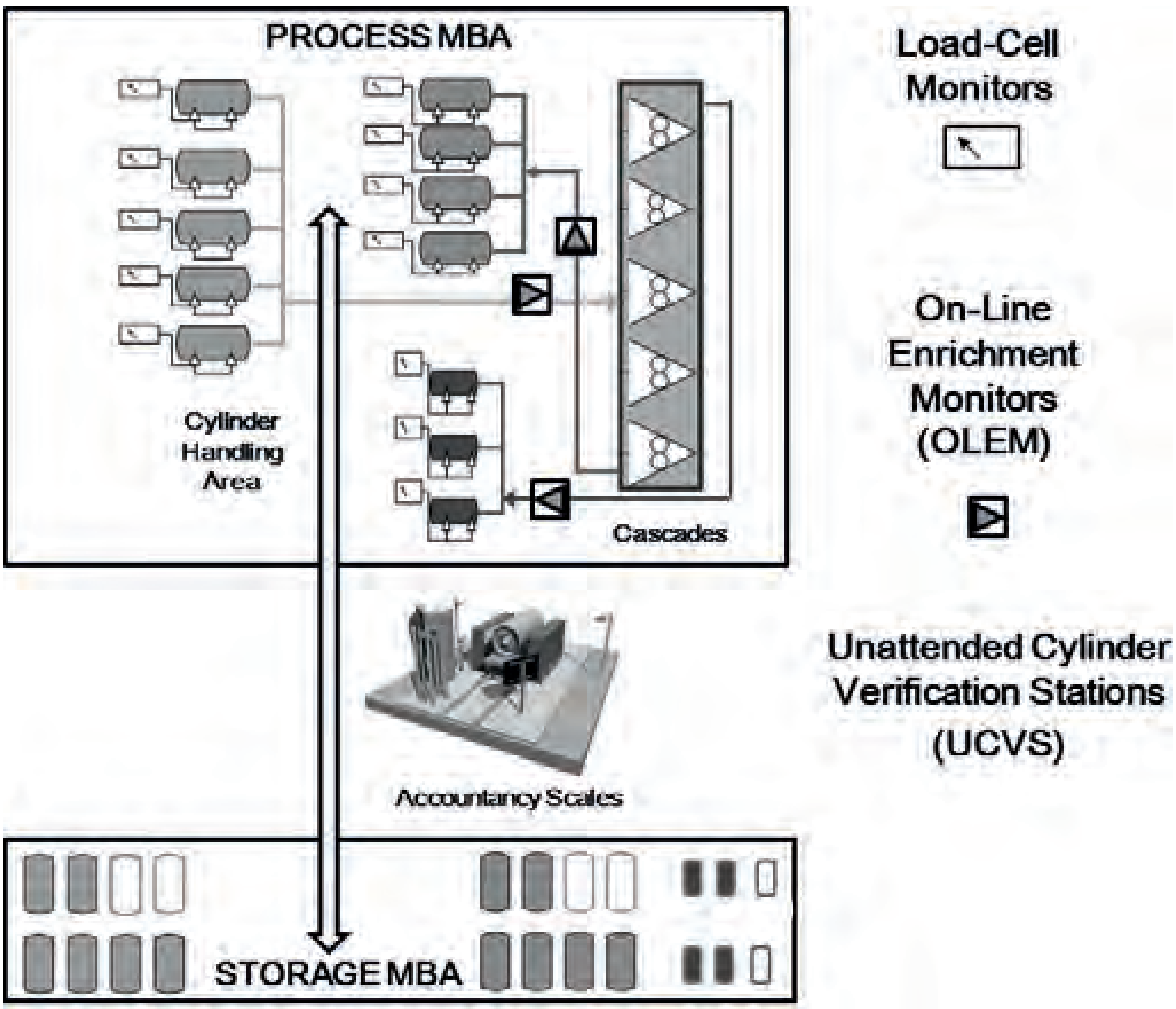


Figure 1: Schematic overview of load-cell monitors, OLEM and UCVS in an enrichment facility divided into a process material balance area (MBA) and a storage MBA.

To support the discussions that follow, a reference centrifuge enrichment plant is defined. This plant represents the modern, large-capacity centrifuge facilities that are a primary motivation for the IAEA's study of a new generation of safeguards measures and approaches. The reference facility is 4,000 tonne SWU/year, with 8 process units consisting of 10 cascades each, and utilizing UF_6 withdrawal by desublimation directly into product and tails cylinders. Two material balance areas (MBAs) are defined in the plant: a process MBA and a storage MBA. A schematic overview of this reference facility is given in Figure 1, and a summary of the roles of each unattended instrument is given here.

The OLEM could provide continuous measurement of 100% of the declared gas flowing through unit header pipes, a key capability for the detection of the higher-than declared production and diversion- from-declared scenarios. In the reference large-capacity enrichment plant described above, 16-24 OLEM units would be required, depending on whether the feed is monitored. The OLEM units would be owned and operated by the IAEA, but include data-security provisions to allow sharing with the operator (e.g. for process control and criticality control purposes) or other stakeholders (e.g. regional or national authorities). Sharing of the operator's load-cell signals from feed and withdrawal stations has the potential to count cylinders introduced to the process and to provide periodic balance of the uranium mass for the in-process material at the plant. Load-cell monitoring supports the detection and deterrence of excess production scenarios in a way that other unattended instrumentation cannot. More than 100 feed or withdrawal stations would need to be monitored in the reference facility. UCVS units could provide unattended verification of the declared uranium mass and enrichment in 100% of the cylinders moving through the plant, but also apply and verify an 'NDA Fingerprint' to preserve verification knowledge on the contents of each cylinder throughout its life in the facility, without the need for an inspector's presence to apply and verify traditional seals. The UCVS NDA features also have the potential to provide independent cross-verification of the signals from operator weighing systems. The UCVS would be built around the operator's accountancy scales, so that two or three UCVS units might be utilized in each plant. Apart from the accountancy scales, UCVS would be owned and operated by the IAEA, but include data-security provisions so that data streams could be shared with the operator (e.g. for cylinder tracking and process control).

A soon-to-be-published journal article from the IAEA provides detailed discussion of the potential roles, development status and remaining development questions for these three candidate unattended measurement systems [6]. An example case study in that paper demonstrates quantitatively how unattended instruments could simultaneously improve effectiveness and efficiency over today's measures, through the integration of load cell, OLEM and UCVS data streams that can support 100% verification of declared cylinder flow and enable the periodic verification of the declared ^{235}U mass balance in the plant. The case study illustrates how the continuous presence and relatively high accuracy of the OLEM and UCVS ^{235}U assay could support the detection of protracted diversion scenarios in a way that has never before been viable for the IAEA, due to accuracy and operational limitations associated with portable instruments for cylinder assay.

This paper draws from [6] to provide an overview of the IAEA's evolving vision for a new generation of unattended safeguards instruments at enrichment plants, and how those instruments might support a flexible toolbox of verification measures that the IAEA could draw upon under its State-level approach to safeguards implementation.

2. Unattended Instrumentation in Context of the IAEA's State-Level Concept

Under the IAEA's State-level concept for defining safeguards approaches, the specific measures implemented at each facility will depend on a set of factors that include: State-specific characteristics (e.g. additional protocol in force); effectiveness in detecting and deterring the key diversion scenarios for that facility; plant design (e.g. size, re-configurability); operator acceptance (e.g. proprietary concerns); and efficiency (e.g. cost, complexity of safeguards measures) [2]. In order to optimize the efficacy and efficiency of safeguards measures at each different enrichment facility under safeguards, the IAEA needs a flexible toolbox of technologies (e.g. unattended and attended) and inspection options (e.g. announced and unannounced).

The IAEA's guiding philosophy is to rely on unattended instruments to perform routine, repetitive measurements, thereby unencumbering inspectors to do the investigative activities that rely on human intuition, tacit knowledge and decision making, such as design information verification or verifying the absence of indicators for undeclared activities. This implementation philosophy should lead to important operational advantages for all stakeholders, for example a significant reduction or elimination of routine interim inspections, reduction of material sampling activities during inspections, and the expediting of product-cylinder release for the operators.

Figure 2 provides a graphical representation of how the IAEA's inspection and technology tools (left side of fulcrum) might be balanced against the data needed to draw safeguards conclusions at the facility level (right side of fulcrum). For the tools on the left side of the fulcrum, the level of data independence increases from right to left. The potential volume of data derived from each measure during a given material balance period is depicted by the height of the box for each tool. For example, the volume of data derived from operator-owned and maintained load cells

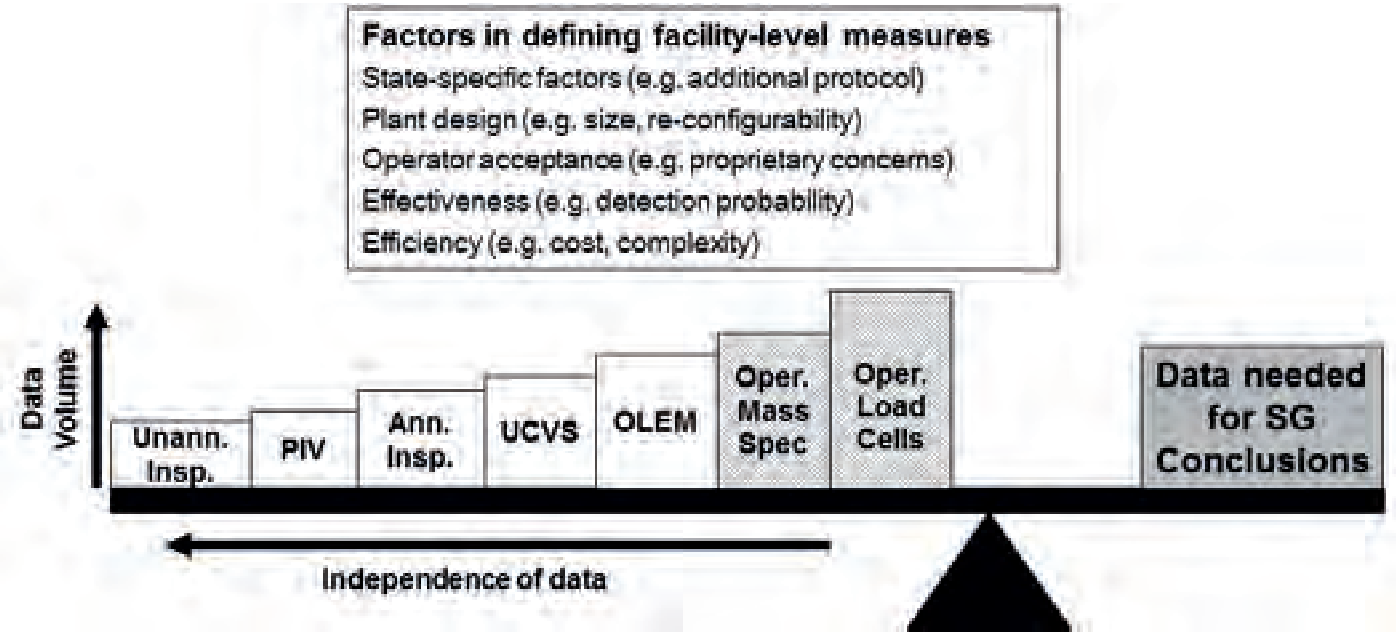


Figure 2: Depiction of how the IAEA might balance a toolbox of safeguards measures (left side of fulcrum) including announced and unannounced inspection activities, a physical inventory verification (PIV) and unattended instrumentation, against the data needed to draw facility-level safeguards conclusions (right side of fulcrum). Only selected measures on the left side of would be implemented at a given facility, depending on the data needed to draw safeguards conclusions under the State-level concept.

and mass spectrometers (boxes with grey hash) may be quite large, but this less-independent data would exert less force on the fulcrum arm than the same volume of more-independent data coming from IAEA-owned-and-operated instruments such as OLEM and UCVS. It is important to note that unattended instrumentation technology would always be accompanied and complemented by inspections (e.g. announced inspections, unannounced inspections and periodic physical inventories) that include investigative and data security activities.

As an example of how the State-level concept might be applied to enrichment plant safeguards, consider 'Facility Y' located in a State with a comprehensive safeguards agreement and additional protocol in force, where integrated safeguards (e.g. including results from complementary access and open-source information analysis) has supported the broader conclusion that there are no undeclared nuclear material or activities in the State. Under these conditions, the importance of the excess production diversion scenario would be reduced, since the IAEA would have already concluded that there are no undeclared enrichment plants to further enrich undeclared low-enriched uranium product diverted from Facility Y. The measures implemented at Facility Y therefore, would be focused on detecting the higher-than declared production scenario, and verifying the declared material flows, as efficiently as possible. The safeguards measures implemented at this Facility Y are likely to be relatively limited compared to the measures implemented at Facility X, which is located in a State without an additional protocol in force, and where the provision of safeguards-relevant information to the IAEA has been more limited. For Facility X, the excess production scenario is of high importance because the IAEA is not able to draw the broader conclusion regarding undeclared enrichment facilities. In Facility X, the data needed to draw safeguards conclusions (right side of fulcrum in Figure 2) will likely require a relatively 'heavy' suite of safeguards measures (left side of fulcrum).

Facilities X and Y are fictitious, created only to provide tangible examples of how the IAEA might define facility-specific safeguards measures under the State-level concept, using a flexible toolbox of unattended instruments and inspection authorities. In the remainder of this paper, more details and discussion about each of the individual unattended instruments are provided, along with more thorough descriptions of how the data streams from such instruments might be integrated at the facility level. Facility X is used as an illustrative example in these discussions.

3. Roles for Unattended Instrumentation at Facility X

The safeguards measures at Facility X include substantial utilization of unattended systems—load cell monitoring combined with OLEM, and UCVS. Consequently, this facility provides a convenient example for discussing how the data streams from these instruments could be integrated to allow the inspectorate to address the three relevant diversion scenarios: 1) diversion from declared, 2) excess production, and 3) higher-than-declared enrichment. It is assumed in this discussion that Facility X contains two Material Balance Areas (MBAs, see Figure 3). The Process MBA includes the cascades, feed and withdrawal stations, weighing and sampling areas, and scrap and waste recovery. The Process MBA in Facility X includes the cylinder blending stations, though it is possible that the blending area could be a separate MBA, or even within the Storage MBA, in facilities under IAEA safeguards.

The excess production scenario could be addressed by counting the cylinders introduced to the cascades to ensure that only declared cylinders are utilized, and via the continuous monitoring of the in-process UF_6 material balance ($MUF_{proc}(t)$ in Figure 3). This material balance would be based on the measured feed, product and tails mass flow rates (*F, P, T* respectively) in each enrichment unit (each of which might consist of 8-10 cascades), as determined from the sharing of operator load cell data from all of the feed and withdrawal stations in the unit. The time-dependent mass data, *M(t)* from the operator's load cells could be shared with the IAEA to determine the time periods during which specific cylinders are being filled (for product and tails stations) or are being withdrawn as plant feed. The material unaccounted for (*MUF*), would be calculated by the IAEA at time intervals negotiated with the operator, taking into consideration for example, the protection of operator's proprietary information. Under normal operation, the *MUF(t)* for total uranium calculated by the IAEA's sharing of the operator's load cells would be expected to be relatively small over short material balance periods, and consistent with mass decrements that are typical of normal operation for the plant (e.g. due to sampling, scrap, holdup). Unattended monitoring of the feed and withdrawal stations could also help to streamline inspection activities (e.g. to minimize cylinder switchover activities).

The OLEMs on each unit header pipe would continuously measure the time-dependent relative uranium enrichment, *E(t),* in weight percent ^{235}U, of the gas filling or the gas being withdrawn from the cylinders. *E(t)* could be used in several ways. First, it could be combined with the *F, P* and *T* total uranium mass flow rates recorded by feed and withdrawal station load cells, to calculate *MUF(t)* for ^{235}U. The IAEA then, could monitor for the excess production scenario using both the uranium and ^{235}U mass balances on the in-process gas.

OLEM data could also be used to calculate the average enrichment of the UF_6 in cylinders, E_{cyl}, by weighting the *E(t)* data for each cylinder time window by the *M(t)* for that same time window. By coupling the load cells and OLEMs in this way, a high-accuracy, independent measurement of E_{cyl} is produced. Alternatively, in cases where the sharing of load-cell signals is not acceptable or practicable, less-direct approaches to deriving mass-flow data could be considered. Such approaches may be viable, for example, in modern enrichment plants where the product enrichment level in each unit header is typically held as stable as possible for relatively long periods of time (e.g. 4.42% for several months). Under these assumptions, $E(t)$ = constant = E_{cyl}. *M(t)* could be assumed constant, or inferred from other plant variables.

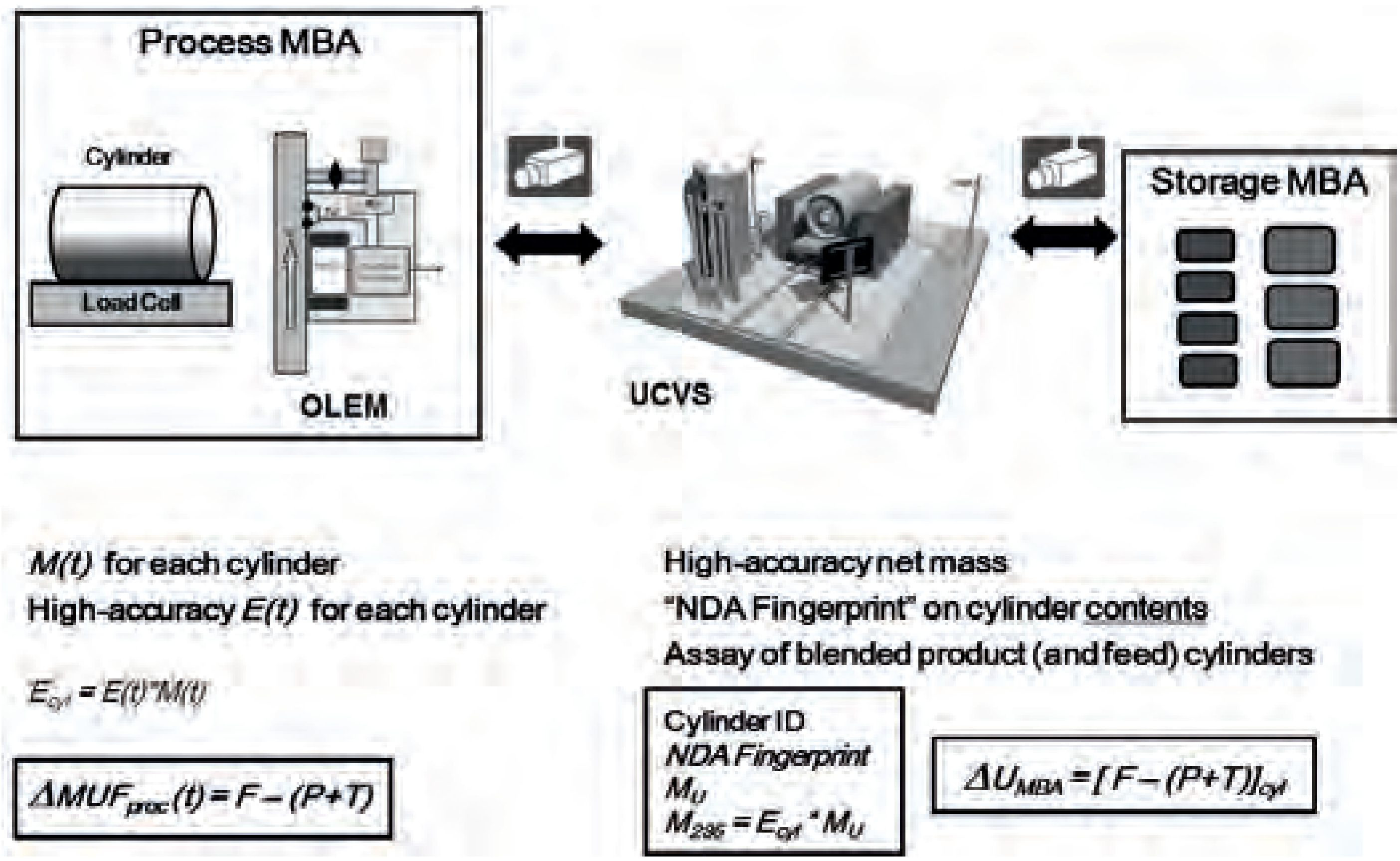


Figure 3: Schematic overview of how load-cell monitors, OLEM and UCVS might be integrated in a two-MBA plant similar to Facility X. Other containment and surveillance measures (e.g. cameras) in the facility would complement the unattended measurement systems.

Another important role of the OLEM units is the continuous monitoring of in-process gas for early detection of greater-than-declared enrichment levels. Because of the location of the OLEMs (see next section), a scenario involving cascade recycle and early takeoff inside the cascade halls is not precluded, but such a scenario is likely to require the operator to make undeclared facility modifications that would be prone to identification during unannounced inspections. Load-cell monitoring and other IAEA tools (e.g. environmental sampling during unannounced inspections) could also be used to address such early takeoff scenarios.

An extremely important piece of data for the facility-level instrumentation system at Facility X is the net uranium mass, M_U, in each cylinder. This mass would be based on the full and tare weights measured by the operator's accountancy scales, as reported through the sharing of the accountancy scale weight tickets. The UCVS, which would be built around the operator's accountancy scales in order to leverage the cylinder characterization opportunity presented by the facility's normal cylinder weighing operations, could be the interface for the collection and utilization of the scale weight tickets. Since $M_{235} = E_{cyl} \cdot M_U$, the combination of load cell, OLEM and UCVS data allows determination of ^{235}U mass for each unblended cylinder (blended cylinders are discussed later). Further, the accountancy scale weight values can be important as a confidence building measure for the less-accurate tare and full weights reported from the load cells at the feed and withdrawal stations. Direct, independent assay of M_U using UCVS radiation signatures might also be a confidence-building measure on the authenticity of accountancy scale and load-cell data.

Once the values of E_{cyl}, M_{235} and M_U are established for each cylinder, it would be ideal that continuity of knowledge (CoK) on that cylinder and its contents would be maintained as long as the cylinder remains at the facility. This is a particular challenge in gaseous centrifuge enrichment plants since the traditional tool for CoK on nuclear material containers, metal or electronic seals, would require very frequent inspector presence to either emplace or remove seals; there exists no practical mechanism for unattended placement and removal of such seals. (There is a precedent for operators to either emplace or remove seals, but not both.) A new concept is needed to address this CoK challenge, and for that purpose, the concept of an 'NDA Fingerprint' applied and verified by the UCVS is being investigated by the IAEA. This NDA Fingerprint is intended to compensate for the lack of traditional, continuous CoK on the verified cylinders, by providing a means to periodically confirm, in an unattended fashion, that the contents of the cylinder are unchanged.

The NDA Fingerprint is a collection of distinguishing attributes for the cylinder contents that could include, for example, total uranium mass, M_{235}, various isotopic ratios (e.g. M_{234} / M_{235} and M_{232} / M_{235}) and the spatial distribution of ^{235}U within the cylinder. The task of 'setting' and verifying the NDA.

Fingerprint would be performed by the UCVS. A UCVS scan would occur each time a cylinder crosses an MBA boundary, to provide periodic re-verification of the cylinder contents, until the time the cylinder is shipped offsite. The UCVS and NDA Fingerprint concept could also be extended to facilities preceding the enrichment plant (e.g. for feed cylinders from the uranium conversion facility) and following the enrichment plant (e.g. receipt of the product cylinders at fuel fabrication plants), as a part of a State-level verification approach.

The UCVS units could play other important roles in Facility X, for example in terms of cylinder identification and tracking, and for the verification of the UF_6 in blended cylinders for which there would be no associated OLEM-based measurement of E_{cyl}. Another potential benefit of the UCVS would be to ease and expedite the product cylinder release process for the operators. For example, product cylinders ready for shipment could be brought to the appropriate accountancy scale for final confirmation of M_U and verification, via the NDA Fingerprint collected by the UCVS, that the UF_6 inside the cylinder is unchanged since the cylinder was previously measured at the boundary of the Process MBA. A conceptual overview of how unblended product cylinders could be verified and released from the facility using unattended instrumentation is given in Figure 4 below.

4. Technology Development Status

Though many development challenges remain before field implementation of these technologies could be considered by the IAEA, there are encouraging results and indications coming from development efforts in the safeguards community. A brief summary of the development status for OLEM, UCVS and shared-use load cells is given here; a full discussion can be found in [6].

Modeling-based OLEM viability studies by the IAEA established the expected range of measurement uncertainties under representative plant conditions [7] and helped inform the IAEA's user requirements and performance targets for OLEM [8]. A collaborative field measurement campaign performed by Los Alamos National Laboratory (LANL) and Urenco at Urenco's Capenhurst (England) facility provided invaluable experience and empirical support for the viability of OLEM [9]. These field tests extended the community's understanding of how pressure transients can be used for wall-deposit calibration, and confirmed that measured uncertainties on product-gas enrichment are consistent with IAEA's modeling-based performance targets. Collectively, these simulation and empirical studies

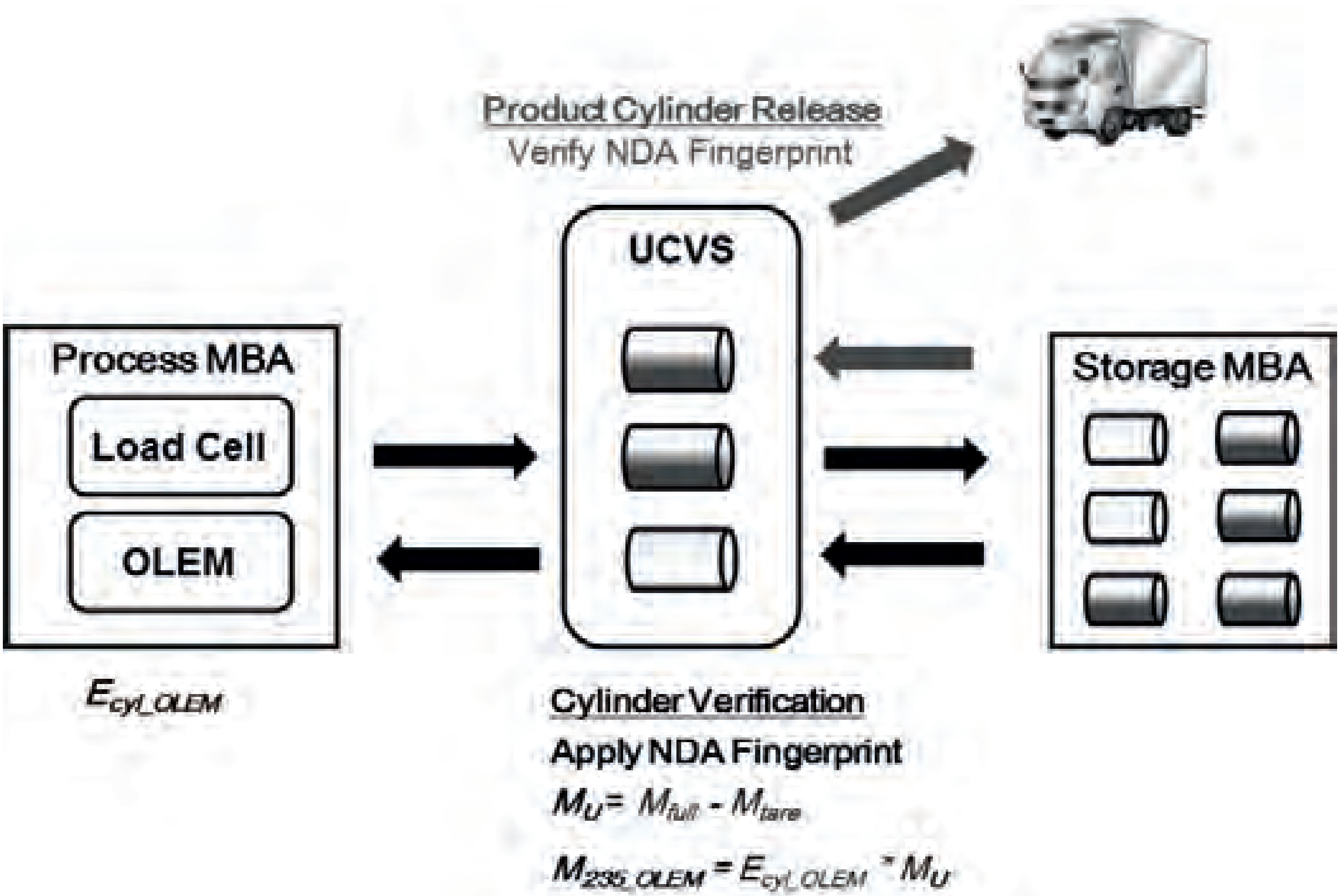


Figure 4: Conceptual overview of how an unblended product cylinder could be verified and released from the facility using a combination of load cell monitoring, OLEM and the UCVS. The empty cylinder would begin in the storage MBA at right, be characterized by the UCVS on its way into and out of the Process MBA. Data from load cells and OLEM (E_{cyl_OLEM}) would support high-accuracy calculation of M_{235_OLEM} in each cylinder. When the operator is ready to ship the cylinder off-site (grey arrows at top), the UCVS's NDA Fingerprint capability would be used to verify the constancy of the cylinder contents since production.

indicate that well-calibrated instruments on header pipes are capable of meeting OLEM performance targets: 1%, 2% and 3% (relative one-sigma) uncertainties for product, feed and tails gas streams, respectively. OLEM field prototypes are now being developed under the United States Support Program to the IAEA [10], in a collaboration between Oak Ridge National Laboratory (ORNL) and LANL.

Modeling-based viability studies for the NDA functions of the UCVS have been undertaken, and the strengths and limitations of two different cylinder assay methods are currently being studied. Pacific Northwest National Laboratory (PNNL) has developed a hybrid cylinder assay technique that utilizes an array of NaI(Tl) spectrometers to simultaneously measure the direct 186-keV signature from ^{235}U and via high-energy gamma rays induced by neutrons in ^{56}Fe and the NaI(Tl) itself, the total neutron emission rate from the cylinder. The 186-keV signature provides an unambiguous measure of E_{cyl}. Under assumptions of known $^{234}U/^{235}U$ behavior in the plant, the total neutron signal can be calibrated to total M_{235} in the cylinder [11][12]. Over several field campaigns using PNNL's Hybrid Enrichment Verification Array (HEVA) prototype for the assay of Type 30B cylinders with enrichments ranging from 2.0% to 5.0%, relative uncertainties of approximately 3% for E_{cyl} and 4% for M_{235} were reported. LANL's Passive Neutron Enrichment Monitor (PNEM) employs moderated 3He modules to measure the singles and doubles neutron emission rates from the cylinder [13][14]. The singles emissions come primarily from the ^{234}U, which under an assumption of known $^{234}U/^{235}U$ behavior allows determination of ^{235}U mass. The singles to doubles ratio allows calculation of the cylinder enrichment level. A field campaign using a PNEM prototype included the assay of Type 30B cylinders with enrichments ranging from 2.0% to 5.0%, and measurement times of approximately 20 minutes, but relative uncertainties for E_{cyl} and M_{235} over the measured cylinder population have not been published. The European Commission's Joint Research Centre (JRC) at Ispra provided both qualitative and quantitative assessments of the systematic and statistical uncertainties that arise when utilizing various radiation signatures to assay cylinder contents [15]. While this prior work on NDA methods for UCVS has been encouraging, the expected measurement uncertainties in realistic enrichment plant operation are not yet fully understood, nor has the viability of the NDA Fingerprint, or the direct assay of total uranium mass, been explored.

Though there are no new developments needed in terms of the operator's load cell systems themselves, there remain a number of unanswered questions about the statistical and systematic uncertainties associated with data streams from those load cells, how those uncertainties propagate through a facility-level mass balance, and the effectiveness for detecting excess production scenarios using a mass balance with those uncertainties [6][16]. Work is also underway to develop and assess hardware and software approaches for data sharing that meet IAEA requirements for data security. Ongoing studies by the European Commission's Joint Research Centre (JRC) at Ispra, in an operating enrichment plant in France, will aid the community's understanding of hardware, data collection methods, and operator tolerance for the sharing of near-continuously produced process control data that is often considered proprietary [17]. Innovative techniques for building confidence in the integrity and completeness of the load-cell data are being considered by ORNL [18].

5. Conclusions

Key themes and conclusions from discussed in [6] and summarized in this paper include:

Potential for unattended instruments to substantially improve effectiveness and efficiency: Creative integration of unattended instrumentation and coupling to unannounced inspections has the potential to achieve significant improvements in the timely detection and deterrence of enrichment- plant diversion scenarios. Significant improvements in cylinder assay accuracy offered by the integration of load-cell monitoring, OLEM and UCVS opens the possibility of near-real-time verification of the declared ^{235}U mass balance at the perimeter of the process MBA. This capability was never before available to the IAEA, due to the limited sampling of cylinders during interim inspections and the relatively poor measurement accuracy of the portable devices used for cylinder verification measurements. Such unattended instrumentation combinations would also lead to substantial efficiency improvements, for example the elimination or significant reduction of routine interim inspections, and a reduction in sampling of gas and cylinders during inspections.

Need to characterize and quantify instrument measurement uncertainties: A solid understanding of the achievable measurement uncertainties in realistic plant environs, and the corresponding uncertainty budgets (i.e. the relative contributions of random and systematic errors), for each of the candidate unattended technologies is invaluable to the IAEA to help guide and refine the development of user requirements, and also to support the analysis of facility-level diversion scenarios. These instrument-level uncertainty studies are more advanced for OLEM and UCVS than for load-cell monitoring, but further investigation is needed for all three unattended instruments.

Need to characterize potential vulnerabilities and data security challenges: Instrument development activities should address, at least in the preliminary sense, key vulnerabilities or spoofing possibilities, since vulnerabilities could ultimately define whether the technology could be adopted by the IAEA. The same could be said for data security measures and whether those measures are sufficient to meet IAEA's requirement to draw independent safeguards conclusions, while at the same time facilitating the sharing of instrument data with operators and other stakeholders.

Need to identify and pursue long-term field testing opportunities: In order to build confidence in the lifecycle viability of new unattended technologies, long-term field testing in representative facilities with field prototypes meeting IAEA's user requirements is needed. Developing flexible testing agreements that include tolerance for instrument 'learning periods' and down-time for revision or troubleshooting is critical. The IAEA will continue to engage Member States and facility operators to identify suitable testing opportunities.

Need to explore 'win-win' opportunities for IAEA and operators: Discussions between the IAEA and operators have suggested that IAEA's unattended instruments may have notable benefits for facility operators, for example for process control, criticality safety or to meet requirements from state authorities. Such opportunities should be identified and pursued as early as possible, so that the necessary hardware and software capabilities (e.g. sensor duplication, data branching methods and data security hardware/software) can be integrated efficiently, rather than as an afterthought.

The concepts presented in this paper should not be considered a comprehensive study of all implementation options being considered by the IAEA but rather, as a starting point for discussions regarding the potential and challenges associated with the use of unattended measurement systems at enrichment plants. It remains to be seen whether any of these technologies described in this paper, or combinations thereof, will be deployed in field operations. Ultimately, deployment decisions will be based on a combination of factors that include efficacy, lifecycle cost, and operator acceptance.

6. Acknowledgements

The authors are appreciative to Peter Friend from Urenco Limited, Kiril Ianakiev from Los Alamos National Laboratory and Jose March-Leuba from Oak Ridge National Laboratory for sharing their insights and experimental experience with on-line gas measurement techniques. On the topic of cylinder NDA methods, information sharing and discussion with David Jordan of Pacific Northwest

National Laboratory and Karen Miller of Los Alamos National Laboratory are appreciated. We would also like to thank Peter Schwalbach, who has provided helpful Euratom perspectives about enrichment plant safeguards objectives. The authors are grateful to Jill Cooley, Sergey Zykov, Cesare Liguori, and David Beddingfield of the IAEA for informative discussions and perspectives regarding the role of safeguards technologies, and emerging priorities under the State-level concept.

7. References

[1] Bush, W., et al. 2006."Model Safeguards Approach for Gas Centrifuge Enrichment Plants," IAEA Symposium on International Safeguards.

[2] Cooley, J.N. 2007. "Model Safeguards Approach and Innovative Techniques Implemented by the IAEA at Gas Centrifuge Enrichment Plants," INMM Annual Meeting Proceedings.

[3] International Atomic Energy Agency. 2011. "Research and Development Programme for Nuclear Verification 2012-2013, " IAEA Department of Safeguards.

[4] Lebrun, A.R., et al. 2009. "Improved Verification Methods for Safeguards Verifications at Enrichment Plants," Proceedings of the ANIMMA Conference.

[5] Zykov, S. 2012. "IAEA Instrumentation for the Future," INMM Annual Meeting Proceedings.

[6] Smith, L.E., A.R. Lebrun and R. Labella. 2013. "Potential Roles of Unattended Safeguards Instrumentation at Centrifuge Enrichment Plants," to appear in *Journal of Nuclear Materials Management*.

[7] Smith, L.E. 2012. "User Requirements: On-line Enrichment Monitor," IAEA SG-EQ-OLEM-UR- 0001, IAEA Department of Safeguards.

[8] Smith, L.E., and A.R. Lebrun. 2011. "Design, Modeling and Viability Analysis of an Online Uranium Enrichment Monitor," IEEE Nuclear Science Symposium Proceedings.

[9] Ianakiev, K.D. et al. 2012. "Field Trial of LANL On-Line Advanced Enrichment Monitor for UF_6 GCEP," INMM Annual Meeting Proceedings.

[10] Younkin J.R., J.R. Garner, N.C. Rowe, and L.E. Smith. 2012. "A Robust and Flexible Design for Gas Centrifuge Enrichment Plant Unattended Online Enrichment Monitoring," 9th International Conference on Facility Operations-Safeguards Interface.

[11] Smith, L.E., E.K. Mace, and A.C. Misner. 2010. "Signatures and Methods for the Automated Nondestructive Assay of UF_6 Cylinders at Uranium Enrichment Plants," *IEEE Transactions on Nuclear Science* (57).

[12] Jordan, D., C. Orton, E. Mace, B. McDonald, J. Kulisek, L.E. Smith. 2012. "Automated UF_6 Cylinder Enrichment Assay: Status of the Hybrid Enrichment Verification Array (HEVA) Project," PNNL-21263, Pacific Northwest National Laboratory.

[13] Menlove, H.O., M.T. Swinhoe, and K.A. Miller. 2010. "A More Accurate and Penetrating Method to Measure the Enrichment and Mass of UF_6 in Storage Cylinders Using Passive Neutron Self- Interrogation," INMM Annual Meeting Proceedings.

[14] Miller, K.A., H.O. Menlove, M.T. Swinhoe, and J.B. Marlow. 2011. "The Passive Neutron Enrichment Meter for Uranium Cylinder Assay," Proceedings of the ESARDA Symposium.

[15] Berndt, R., E. Franke, and P. Mortreau. 2010. "^{235}U enrichment or UF_6 Mass determination on UF_6 cylinders with nondestructive analysis methods," *Nucl. Inst. Meth. A* (612).

[16] Lebrun, A.R. 2009. "Sharing of the operator weighting data at enrichment plants," IAEA SG-PR- 7001, IAEA Department of Safeguards.

[17] Richir, P., P. Buchet, L. Dechamp, P. Dransart, Z. Dzbikowicz, G. Mercurio, 2013. "Process monitoring: Data acquisition and Data Analysis, Modeling and Integration of New Safeguards Technologies," European Commission - Joint Research Centre.

[18] Garner, J.R., et al. 2011. "New Measures to Safeguard Gas Centrifuge Enrichment Plants," Proceedings of the ESARDA Symposium.

Categorization of the Main Techniques of Neutron Coincidence/Multiplicity Analysis

Alan Michael Bolind

Integrated Support Center for Nuclear Nonproliferation and Nuclear Security Japan Atomic Energy Agency
Funaishikawa Eki Higashi, Tokai-mura, Naka-gun, Ibaraki-ken 319-1118, Japan
E-mail: alan.bolind@jaea.go.jp

Abstract:

Reactor noise analysis and neutron coincidence/multiplicity analysis for safeguards both examine the non-random clustering of neutrons in time, caused by the simultaneous emission of multiple neutrons from each fission event and by the correlation of successive fissions in the same fission chain. Despite these same physical origins, the various kinds of techniques are not often compared with each other on an intuitive level. This paper makes this comparison, primarily by examining whether a given technique relies on the joint probability of detecting neutrons or on the conditional probability. The techniques are compared in other ways, too, such as how they deal with fission chains. Subtleties are also addressed, such as the time origin of the Rossi-α diagram and the taking of moments. Specific instruments are not described in detail; the focus is the understanding of the physics and counting principles.

Keywords: neutron; coincidence; multiplicity; reactor; noise

1. Introduction

Neutron coincidence counting is based on the fact that several neutrons are emitted simultaneously from each fission event. The number of neutrons emitted from a single fission event is called the neutron *multiplicity*, ν, which should not be confused with neutron *multiplication*. The number of neutrons varies with each fission event according to a well-known probability histogram, P(ν), for each isotope. (See Figure 1.) (The term *neutron coincidence* will be used in this paper to refer to all orders of analysis, not just first-order analysis.)

The simplest and most ideal kind of measurement is a deterministic one, in which a small amount of a pure but unknown material that produces neutrons only by spontaneous fission is put into the center of a chamber that is surrounded by high-efficiency neutron detectors. The combined hardware of the chamber, the detectors, and other components will be called the "instrument" in the following discussion, with the specific exclusion of the sample chamber; the volume of the sample chamber is not part of the instrument. The amount of material put into the sample chamber is kept small so that the activity will also be small, such that most of the spontaneous fission events do not overlap, even though they occur randomly in time. The small amount of material also prevents the neutrons that are emitted from being reabsorbed in the sample due to neutron capture. As for neutron leakage, the high efficiency of the neutron detectors ensures that almost all of the neutrons from each spontaneous fission event are counted.

A histogram of the neutron counts of the fission events is made and is compared with the histograms in the literature (e.g., Figure 1). The radioactive isotope in the sample must be the isotope with the histogram that most closely matches the measured histogram. Because the literature histograms are normalized to a total area of one to make them probabilities, this comparison is a comparison of the shapes of the histograms, not of their scales. After the isotope has been identified, the next question is how much of the isotope is present in the sample; the sample might contain other, non-radioactive isotopes, such that a measurement of the sample's mass would not represent the mass of the radioactive, neutron-emitting isotope. The non-normalized, measured histogram represents a certain number of neutrons counted per unit time, and this absolute scale of the histogram can be correlated to the strength of the source, i.e., the spontaneously fissioning isotope's activity and mass. Thus, both the unknown neutron-emitting isotope and its unknown activity and mass can be determined by measuring the neutron multiplicity distribution coming from the sample.

In practice, such a simplistic measurement is rarely made, because many more unknowns exist, such as are in the following list:

Unknowns about the neutron sources in the material

- The sample may not be isotopically pure; more than one spontaneously fissioning isotope may be present in the sample. The measured histogram would then be a superposition of those of the various isotopes,weighted according to their activities in the sample.
- Fissile isotopes may be present in the sample, so that induced fissions might occur. Like spontaneous fissions, these induced fissions emit several neutrons at a time, so that, on an event-by-event basis, they cannot be distinguished from the spontaneous fissions except by their multiplicity histograms, as in Figure 1.

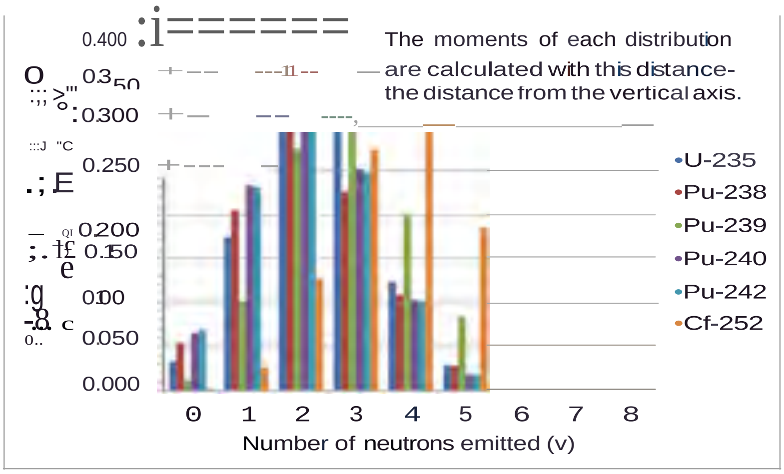


Figure 1: The neutron multiplicity histograms of several actinide isotopes. (The data are from Reference [1].)

- The probability or rate of induced fission depends not only on the amount and spatial distribution of the fissile isotopes.It also depends on the spatial and energy distributions of the neutron flux, which in turn, depend on the sample's geometry, composition, and density. It might also depend on the structure and composition of the instrument-specifically, the reflection of neutrons back into the sample by the instrument.
- Additional neutrons may be emitted by non-fission processes, such as by (a,n) reactions. These neutrons are emitted one at a time,which would ordinarily allow them to be distinguished from the spontaneous fissions,which are emitted several at a time. However, the intensity of the (a,n) neutron source is often high enough that these neutrons overlap with those from the fission events. Moreover, the singly emitted (a,n) neutrons can induce fission in fissile isotopes,which then emit several neutrons simultaneously. With sufficiently high multiplication in a sample, the fissions induced by the (a,n) neutrons can thus even be a more dominant concern than the detection of the (a,n) neutrons themselves.

Unknowns related to the inability to detect all of the neutrons

- Some neutrons may be captured in the sample or in non-sensitive parts of the instrument, such as in the polyethylene moderator surrounding a detector. Although this second possibility can be minimized or fixed by the design of the instrument,the first possibility-capture in the sample-depends on the composition of the sample,which is often unknown. It also depends on the geometry and density of the sample. Moderating material in the sample (i.e., lighter elements, especially hydrogen) has a major influence because it brings down the energy of the neutrons, making them more likely to be captured.
- Some of the neutrons may leak out of both the sample and the instrument without being detected.

Unknowns regarding the interpretation of the neutrons that are detected

- The activity of the sample may be high enough that the spontaneous fissions, induced fissions, and (α,n) reactions overlap.
- More specifically, the time between when the neutrons are emitted and when they are detected—that is, the physical detection time—is not instantaneous but has a finite duration that depends (1) on the geometry of the sample and the instrument and (2) on the moderation of the neutrons to low energy, at which they can be detected with high probability (high efficiency). In other words, there is a finite flight time between the position of the neutron- emitting event and the detectors, plus there is a finite moderation time that is a function of the kinds of scattering events that the neutrons encounter. (This moderation time also depends on the energy with which the neutrons are emitted, but often this variable can be ignored.) Even for a given sample and instrument, this physical detection time varies with each neutron, so that the detection of neutrons from one event can overlap with the detection of those from another event, even if the events did not actually occur simultaneously. In short, the physical detection time smears the chronology of the neutron-emitting events.
- From the point of view of the instrument, all the neutrons are indistinguishable from each other except insofar as the time at which they are detected. The overlapping of the detection of neutrons from separate events, due to high radioactivity and to the variance of the physical detection time, removes much of this chronological information. The information that remains is not sufficient for a deterministic analysis, such as the comparison of histograms that was mentioned above for the simplest case. Instead, the detected neutrons must be treated with a probabilistic analysis.

Both the production of neutrons and the detection of neutrons are mixtures of random processes and correlated processes. Primary neutrons are produced by spontaneous

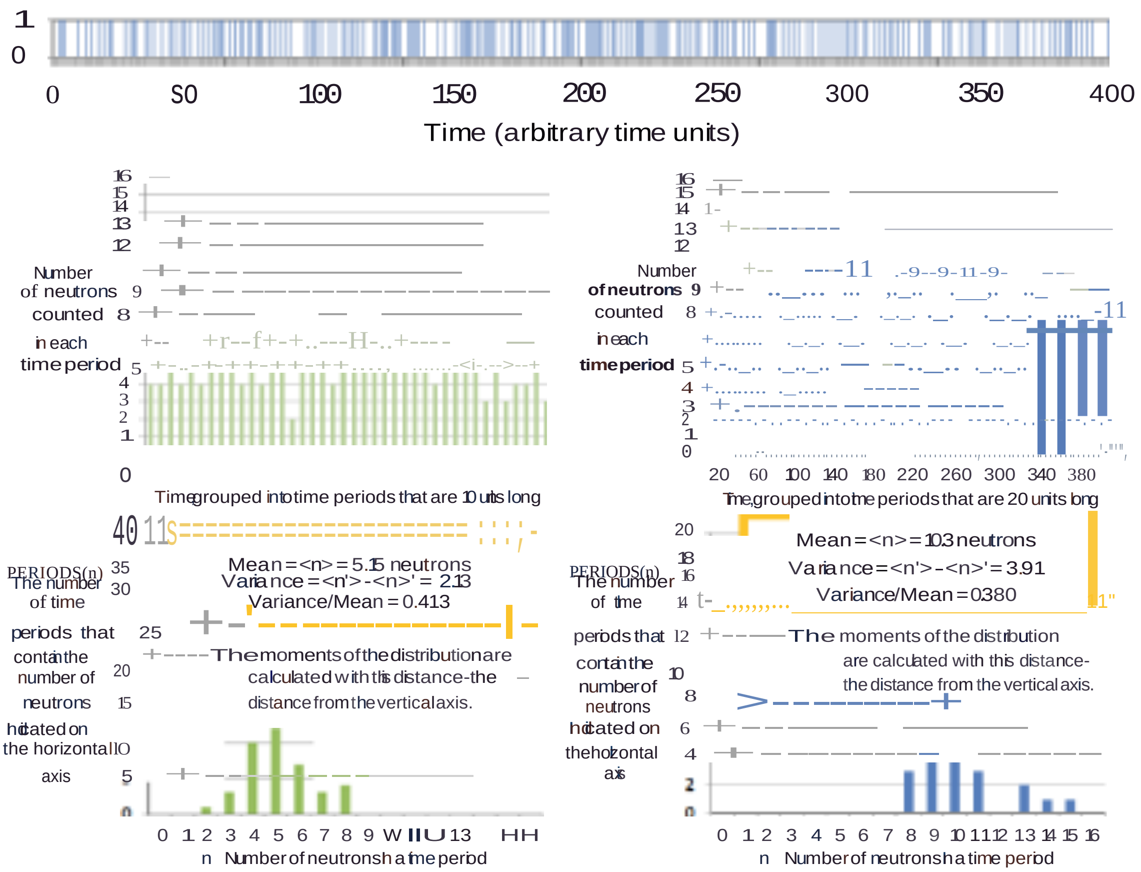


Figure 2: An arbitrary neutron pulse train (top); groupings of these neutrons into time periods of two different lengths (10 time units, middle left; 20 time units, middle right); histograms of those groupings (bottom left and right)[1]

fission and (α,n) reactions, which are both forms of radioactive decay and are therefore random processes. Induced fission, which produces secondary neutrons, can be a correlated process, because it requires incident neutrons. Therefore, an induced fission event is always somewhat correlated to the spontaneous fission, (α,n) reaction, or other induced fission that produced that incident neutron. (This correlation of induced fission events will be discussed in more detail below.)

The detection of neutrons is also a mixture of randomness and coincidence. Not only does the detection of neutrons reflect the randomness in their creation, but the variation in the physical detection time also contributes further randomness. On the other hand, each fission event releases several neutrons simultaneously, so that these neutrons are perfectly correlated with each other at the instant of their creation. Thus, even if the fission events themselves are random, the neutrons that each event produces are grouped together in time.

Probabilistic analysis deals with these randomizing influences by examining, within a small time period, either when the neutrons detected or how many neutrons are detected. This time period, which is often called a "gate," is small because it is on the same scale as the physical detection time or the die-away time of fission chains; it can vary approximately from one microsecond to many tens of microseconds. The measurement over this gate is repeated many, many times to produce values for averages and other statistical metrics. The gate width (i.e., the length of the time period) is varied over a range in some types of analyses. In this case, separate measurements of the neutron pulse train (i.e., the chronological detection of the neutrons) can be made with different gate widths, or the same neutron pulse train can be stored electronically and analyzed repeatedly with various gate widths.

There are two main categories of probabilistic analyses: those by joint probability and those by conditional probability. Joint-probability analyses examine how many neutrons are detected within a gate that is begun ("triggered") at random or periodic times. Figure 2 illustrates this process for two different gate widths. The key feature of joint-probability methods is that the starting times of this gate must be random with respect to both the emission of neutrons and their detection. So, the period for counting neutrons often begins in the "blank space" between the detections of neutrons. Conditional probability analyses,in contrast, examine only the subsequent neutrons that are detected after an initial neutron is detected. Before this first neutron is detected, the equipment (or data-analysis routine) merely waits,

[1] Figure 2 was created not by neutron detections but by the author tapping his finger randomly on his computer keyboard.This is why the variance-to-mean ratio of the 20-time-unit analysis is less than that of the 10-time-unit analysis,when it should be greater (Figure 3).

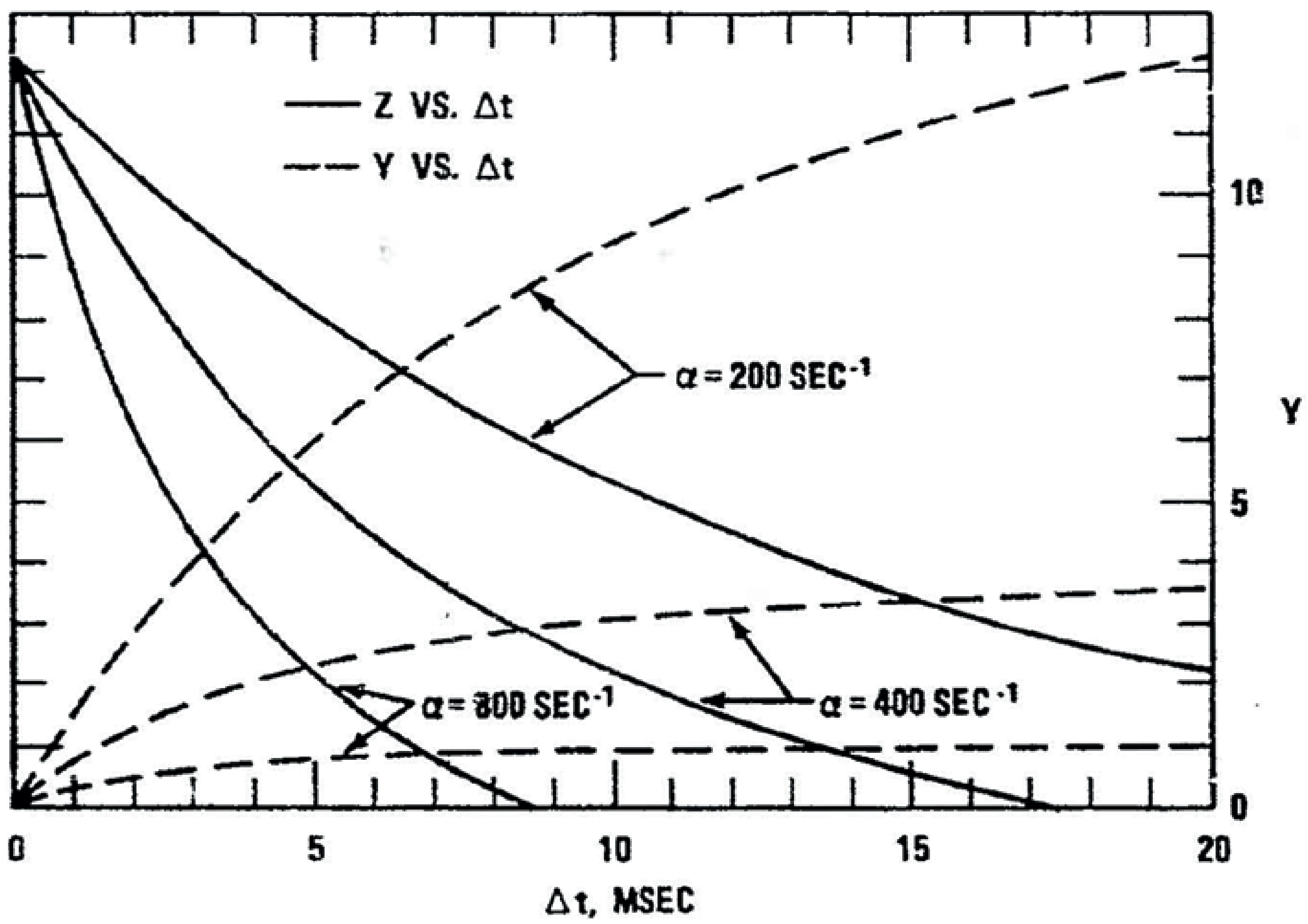


Figure 3: A comparison between Z (from the mean number of pairs in a time interval) and Y (from the ratio of the variance to the mean), as a function of gate width and for various values of α (the die-away time). The graph is for a specific set of experimental parameters. Copied from Reference [2].

doing nothing. If the neutron flux is purely random and without any correlation, then the average number of neutrons counted within a gate of a given width is the same for both types of analyses; but if there is correlation, then the conditional-probability analyses count more neutrons than the joint-probability analyses. These properties can be seen in the definition of conditional probability for two detections, at times t_1 and t_2:

$$P(t_2 \mid t_1) = \frac{P(t_1 \cap t_2)}{P(t_1)} \qquad \text{Equation 1}$$

If the detections are purely random and independent, then the following relations hold true:

$$P(t_1 \cap t_2) = P(t_1)\, P(t_2) \quad \text{for independent events}$$

$$P(t)\, P(t_2)$$

Equation 2

so, $P(t_2\ t_1) = P(ti) = P(t_2)$ for independent events

The crucial importance of this randomness in the triggering of joint-probability analyses demands further contemplation. There are three ways to achieve this randomness.

Firstly, the triggering source (i.e., whatever entity that decides when to start counting) could be external to both the instrument and the sample being measured. For example, the detection of photons from the radioactive decay of a separate cesium source in a neighboring building would be a suitable external, triggering source. Whenever a photon would be detected, then the NDA instrument would begin measuring neutrons and would continue to do so until the end of the gate, at which point it would stop and wait for another trigger from the photon source. Although it is theoretically satisfying, such an experimental setup is obviously excessively complicated in practice.

The second way to achieve randomness is much easier; it is simply to start the measurements at regular time intervals. An example is the starting of the next gate as soon as the previous gate finishes. Since the neutrons are originally created by radioactive decay (i.e., by spontaneous fissions and (α,n) reactions), and since radioactive decay is inherently random with respect to linear time, the starting of the gates at regular, periodic times is indeed random with respect to the neutrons. Because of its simplicity, most joint-probability analyses rely on this periodic triggering.

The third way to achieve random triggering is the most subtle one, but it is also an essential concept for understanding the shift-register method (Section 3). In this third way, the detection of a neutron from one fission chain serves as a random trigger for the detection of neutrons from other, separate fission chains. The independence of the fission chains makes this kind of triggering possible, and this independence is, in turn, caused by the randomness of the primary neutron sources. Specifically, the events that create the primary neutrons are not just random with respect to time, but they are also random *with respect to each other*. Thus, this third way of achieving randomness is almost identical to the first way, except that the random photon source in the neighboring building has been replaced by a random neutron source in the same sample. A complication, though, is that, although primary-neutron creation events are instantaneous, physical detection times and fission chains both have finite durations and so can overlap in time. Therefore, the only way to ensure that the triggering neutron and the measured neutrons are indeed from separate fission events and chains is to *wait* for a certain period of time after the triggering neutron, until the neutron population from the fission event and chain of which it was a member has most assuredly died away (terminated). Only then can the gate begin, with the confidence that the detected neutrons will have no correlation whatsoever with the neutron that triggered the gate. This third way of achieving randomness thus opens up the possibility of simultaneously performing both a joint-probability analysis and a conditional-probability analysis; the triggering neutron begins both a conditional-probability analysis in the short term and a delay that starts a joint-probability analysis in the long term. The shift-register method (described below), although it is fundamentally a conditional-probability method, partially incorporates this idea.

In the conditional-probability method, the gate is triggered by the detection of a neutron. In theory, the gate could be triggered by the fission itself, but in practice, it is usually impossible to detect the fission, since in most cases, doing so would require the detection of the prompt gamma rays or some other, super-fast particles (like anti-neutrinos). (The exception is discussed in the next paragraph.) It must be reiterated that the chronology of the fission events is smeared by the neutrons' physical detection time and the overlapping of events. Therefore, if the reader sees a graph in the literature that refers to the dying away of a neutron population with the time *after the fission event*, the reader must realize that such a graph *cannot* be determined directly by experiment, since the exact time of the fission event is always unknown. Instead, the conditional-probability method produces a graph of the probability that a neutron will be detected after the detection of the first neutron (Figure 4, for example). It is this first detection that defines the zero time ($t = 0$), thereby implying that the fission event that produced the neutron must have occurred at some unknown, negative time. This conditional-probability curve—or the non-normalized rate curve that corresponds to it—is known in the literature as the Rossi-α curve, named after Bruno Rossi, who suggested this kind of analysis.[2]

The exception mentioned above, in which a fission event can be directly detected, is when a fission chamber both is used as the neutron detector and is inherently part of the system being measured. A fission chamber located in the middle of a nuclear reactor satisfies this requirement. Any fission event in the fission chamber is detected by its fission fragments, while its neutrons proceed to perpetuate the fission chains in the system. It appears that perhaps de Hoffmann had this concept in mind when he implicitly defined his efficiency variable, ε, as being the efficiency for detecting fissions [3], although he, Feynman, and Serber actually used BF3 detectors in the experiments for their famous 1956 publication. [4] Williams made this definition explicit in his derivation (page 38 of Reference [5]). Mihalczo took this idea one step further and made a fission chamber out of ^{252}Cf; the spontaneous fissions of the ^{252}Cf were recorded in the chamber while their neutrons proceeded to start fission chains in the nearby nuclear system.[6, 7] Another, separate neutron detector then detected the neutrons produced by the nuclear system. Obviously, in Mihalczo's experiment, the starting time for the conditional-probability analysis really was the spontaneous fission event in the ^{252}Cf. In fact, his experiment was much like a differential-die-away (DDA) experiment, in which each spontaneous fission of ^{252}Cf served as a tiny neutron pulse to actively interrogate the fuel assembly. In common practice, though, and especially for NDA of fuel assemblies, the neutron detectors are outside the sample or system and are often not fission chambers. Therefore, the usual situation is that the time of the fission event is unknown, and the conditional-probability analysis begins with the detection of a neutron.

As was mentioned before, spontaneous fissions and (α,n) reactions do occur purely randomly, but induced fissions do not, because the neutrons produced by one fission event are the catalysts for the subsequent fission events in the fission chain. The average time between fission events, and the average length of the fission chains in a subcritical system are therefore both important characteristics of system with neutron multiplication. The effect of induced fission has traditionally been handled in either one of two ways.

(1) If the system is nearly critical and therefore has high multiplication (as in zero-power reactor noise analysis), the fission chains are long because they contain many fission events and (for thermal- neutron reactors) because the moderation time of the neutrons between fission events also lengthens the fission chains. In this case, the non-random spacing among the fission events of a fission chain contributes additional correlations to the Rossi-α curve, even to the point of dominating the correlation, over the correlation due to the

neutron multiplicity of each fission event. Thus, the induced fission lengthens the exponential portion of the Rossi-α curve and is simply measured directly.

(2) On the other hand, if the system is very subcritical and therefore has low multiplication, the fission chains are short and contain only few fission events. This case has two subcases, according to the reason why the system is subcritical.

(2a) If the system is subcritical because there is little moderation of neutrons, then the fast neutron spectrum also implies short physical detection times. In this subcase, the time between the spontaneous fission or (α,n) reaction that began the fission chain and the time of the last induced fission event of the fission chain is so short that all of the neutrons of the entire fission chain practically arrive at the detectors simultaneously, within the variation of the physical detection time. This fact led Böhnel to call these chains “superfissions,” since the chains are indistinguishable from single spontaneous fission events with large multiplicities.[8-10] This subcase is representative of measurements of cans of purified nuclear material (like MOX powder).

(2b) The other subcase is when moderation is present but the system is still subcritical because there is a low density of fissile material or much neutron capture or both. The number and length of fission chains are small because of the lack of fissile material, the time between the fission events in a chain is long because of the moderation, and the chance of detecting all the fission events of a chain is small because of the capture. Thus in this subcase, the correlation among the induced fission events can be lost, so that they appear to be random. NDA measurements on some spent fuel assemblies that are immersed in cooling water might fall into this subcategory.

It is important to clarify the way in which the sample or system (e.g., a fuel assembly) must be subcritical in order for the correlations to be able to be detected. In general, sub-criticality is an essential requirement for coincidence/multiplicity analysis, because if the fission chains never die out, then it becomes impossible to distinguish one chain from another. Succinctly put, if every fission event is correlated, then no fission event is correlated, in a practical sense. In such a system, only the correlation among the simultaneously emitted neutrons from each fission event would, in theory, remain distinct and able to be detected. In fact, though, it is possible to fully analyze a system that is critical on delayed neutrons but is subcritical on prompt neutrons (e.g., a reactor). In such a system, the relatively slow emission of the delayed neutrons causes them to appear more or less like a randomly generated, primary neutron source to the coincidence measurement. Also, the prompt fission chains do, in fact, die away. (If it is necessary, the effects of the delayed neutrons can somewhat be taken into account through more complicated analyses; see Pacilio, for example.[2])

Thus, coincidence/multiplicity analysis can be applied to critical nuclear reactors at zero or very low power levels at which the neutron flux does not overwhelm the detectors. Although this point is not of practical importance for the analysis of completely subcritical, single fuel assemblies, it is nevertheless of conceptual importance when adapting the methods from the reactor-noise-analysis literature to such an NDA application.

2. Coincidence analysis by the joint probability of detecting multiple neutrons in a random or periodically triggered time interval

The joint-probability method and the conditional-probability method will now be explained and related to each other. In the joint-probability method, many measurements are made of the number of neutrons that are detected within a gate. This number will be denoted by the letter *n*, and it varies, of course, from measurement to measurement. A histogram can be created from these measurements, showing the number of time periods (gates) that contain each number of neutrons. This number of time periods will be denoted symbolically by the capitalized word PERIODS. Figure 2 illustrates these concepts with an example, in which the same, arbitrary pulse train (top graph) is analyzed according to two different gate widths. Note that these gates are periodically triggered, with the next gate beginning as the previous gate ends. The net effect is to take the continuous time axis of the pulse train (top graph) and make its resolution poorer, by chopping it into consecutive but discrete time intervals.

The moments of the histograms (bottom of Figure 2) can be calculated as follows:

j^{th} moment about the origin = $E[n^j]$ or $\langle n^j \rangle$ or

$$n^1 = \frac{\Sigma_{n=1}^{oo} n^j \,\text{PERIODS}(n)}{\Sigma_{n=1}^{oo} \text{PERIODS}(n)} \qquad \text{Equation 3}$$

Mean = 1^{st} moment about the origin = $\langle n \rangle$

Variance = 2^{nd} moment about the mean = $\langle (n-\langle n \rangle)^2 \rangle$ = $\langle n^2 \rangle - \langle n \rangle^2$

The first moment about the origin is the average number of neutrons that are expected to be counted during a time interval (gate) of a particular length. Obviously, if the time interval is lengthened (the gate is widened), then more neutrons are expected to be counted. Also, dividing the number of counted neutrons by the duration of the counting is exactly the definition of the average neutron

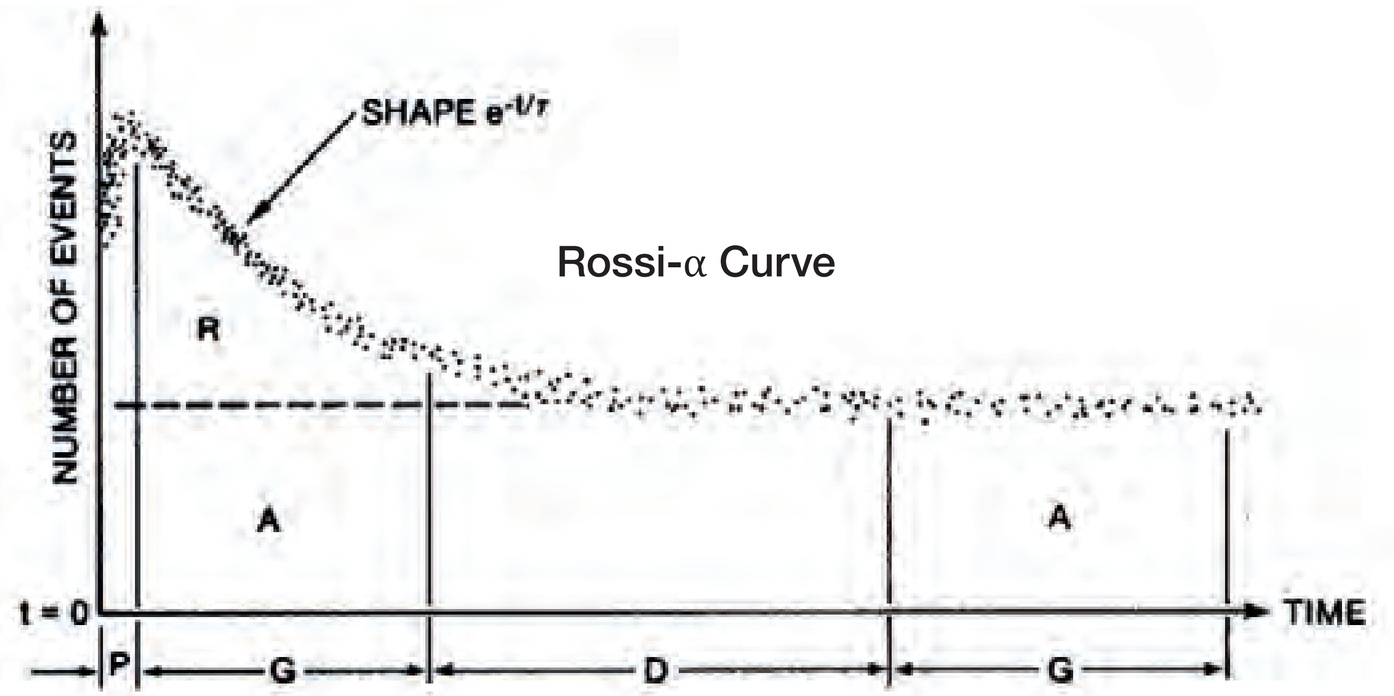


Figure 4: A sketch of a one-dimensional Rossi-α curve, which shows the rate at which second neutrons are detected as a function of the time after first neutrons are detected (which is the origin, *t* = 0). Note that the dots in the curve have no real meaning. Copied from Reference [1]

count rate. These concepts are expressed by the following proportionality:

$$\langle n \rangle \propto F(t_2 - t_1) \qquad \text{Equation 4}$$

where *F* is the production rate of neutrons (i.e., the rate of fission plus (α,n) reactions), *t1* is the starting time of the gate, and *t2* is the ending time. Note that the constant of proportionality would have to account for the average number of neutrons per fission or (α,n) reaction (i.e., $\bar{\nu}$) and for the probability that a neutron survives the journey to the detector and is detected (characterized by ε). Therefore, the product of $\bar{\nu}$ and ε is often used for this constant, but ambiguity exists in the literature.

If the arrival of the neutrons at the detector would be completely random, then the probability of detecting a certain number neutrons (say, *k* neutrons) within a specified time interval would be described by the Poisson distribution:

$$P(n=k)=\frac{11^k e^{-A}}{k!} \qquad \text{Equation 5}$$

Here, λ is a parameter that is equal to the mean, <*n*>; this fact can be verified by calculating the mean of this distribution (Equation 5), which will yield λ. Another interesting fact about the Poisson distribution is that the variance is also equal to λ; that is, the variance is equal to the mean. Thus, one way to verify that a process is completely random is to measure the mean and the variance of the output; if they are equal, then the process is random. Conversely, the extent to which the variance is *not* equal to the mean is a measure of the non-randomness of the process—that is, the coincidence among the outputs of the process.

These realizations led De Hoffmann, Feynman, and Serber to determine the ratio of the variance to the mean, of the neutrons counted in a time interval, as a function of physical, neutronic characteristics of the system that is producing the neutrons.[3, 4] Their equation has been derived by several authors and is as follows: [2, 3, 5, 11, 12]

$$\frac{\text{Variance}}{\text{Mean}} = \frac{\langle n^2 \rangle - \langle n \rangle^2}{\langle n \rangle}$$

$$= 1 + \frac{\varepsilon \langle \upsilon(\upsilon-1) \rangle}{a^2 \tau_f^2}\, 1 - \frac{1-e^{-\alpha \Delta t}}{\alpha \Delta t} \qquad \text{Equation 6}$$

$$=1+Y \text{ (explained below)} \qquad \text{Equation 7}$$

The time interval is Δ*t*, the average number of pairs of neutrons emitted per fission event is ⟨ν(ν - 1)⟩/ 2, the average time between fission events is τ*f*, and α is the die-away constant that describes how long it takes for the neutrons created by a fission event to disappear, by leakage or absorption. The characteristic lifetime of neutrons in the system is therefore 1/α. The factor ε represents a detection efficiency, but its meaning is ambiguous in the literature and will not be clarified here.

There are seven important features of Equation 6 to highlight:

1. The first term on the right-hand side is one, and it represents the Poisson randomness. The second term represents the extent to which the neutron pulse train is non-random and deviates from the Poisson distribution. This second term is often denoted by the capital letter *Y*, as in Equation 7.

2. The emission of several neutrons from each fission event (i.e., the neutron multiplicity) is represented by the factor $\langle \nu(\nu - 1) \rangle$.

3. The mean, the variance, and the variance-to-mean ratio depend upon the length of the time interval (width of the gate; Δt). See Figures 2 and 3.

4. As the gate becomes wider, the variance-to-mean ratio does *not* go to one. Only the term in parentheses goes to one, thus preserving the second term yet also saturating the variance-to- mean ratio.

5. As the gate becomes smaller, the second term goes to zero, reflecting the fact that the physical detection time (represented through α) and the time between fissions (represented by τf) smear the chronology of the neutrons and make it less likely to detect correlated neutrons within a gate that is too narrow.

6. As the time between fissions, τf, becomes longer, the second term becomes smaller and the variance-to-mean ratio becomes closer to one. This feature is partly a reflection of the physics mentioned earlier, that a long and varied time between induced fission events removes the correlation between those events. It is primarily caused, though, by the original purpose for which Equation 6 was derived—namely, for the detection of neutrons from *fission chains*, rather than for the detection of neutrons from individual fission events. The early authors were concerned about measuring the reactivity of nuclear reactors that were close to criticality.[2-4] In this view, the primary purpose of a fission event is to perpetuate the fission chain and thereby make it more likely that a neutron from that particular fission chain will be detected. This reason is why τf is multiplied by α in the denominator, because a short time between fissions counteracts a fast die-away time (a large value of α).

It should also be noted that delayed neutrons have been neglected in this equation, and only prompt neutrons have been considered.

The traditional way to use Equation 6 is to determine the variance-to-mean ratio for several values of Δt, which requires either several measurement runs or several re-analyses of one measurement run. The resulting values are plotted as a function of Δt and are fit with Equation 6 by least-squares fitting, to determine unknown quantities. In reactor noise analysis, the usual goal is to find the value of α for the reactor, because it can be related to its reactivity. The value of $\langle \nu(\nu - 1) \rangle$ is estimated or known. In contrast, the usual goal in safeguards NDA is to find the value of $\langle \nu(\nu - 1) \rangle$, because it is characteristic of the unknown isotopes in the sample (Figure 1). The die-away time (α) and the efficiency (ε) are controlled by the designs of the instrument and the sample and are determined by calibration.

The variance-to-mean ratio is directly related to the rate of counting two neutrons within Δt and can be derived algebraically from Equation 6: [5, 12]

$$\text{Mean number of pairs} = \langle \left(\frac{n}{2}\right) \rangle = \langle \frac{n(n-1)}{2} \rangle = \left(\frac{1}{2}\right)$$

$$- \frac{[F\varepsilon(t_2-t_1)]^2}{2} + F\varepsilon(t_2-t_1) \frac{\varepsilon_2}{\alpha^2 \tau_f} \frac{\langle \upsilon(\upsilon-1) \rangle}{2} \; 1 - \frac{1-e^{-a(t_2-t_1)}}{\alpha(t_2-t_1)}$$

Equation 8

$$= \frac{[F\varepsilon(t_2-t_1)]^2}{2} (1+Z) \text{ (explained below)}$$

Equation 9

The first term on the right-hand side of Equation 8 is the mean number of pairs to be expected from a Poisson distribution, as manipulations of Equations 4 and 5 can show:

$$\text{Variance} = \frac{\langle n^2 \rangle - \langle n \rangle^2}{\langle n \rangle}$$

Variance = Mean = 11 (for a Poisson distribution)

$$11^2 + 11 = \langle n^2 \rangle$$

Mean Number of Pairs (Poisson Distribution) =

$$\frac{11^2}{2} = \frac{[F\varepsilon(t_2-t_1)]^2}{2}$$

Equation 10

Since the Poisson distribution represents randomness, this first term in Equation 8 is often called the "uncorrelated pairs." The second term is therefore correspondingly called the "correlated pairs." Note that it is very similar to the second term on the right-hand side of Equation 6, with the time interval (Δt) being written out explicitly.

Furuhashi and Izumi chose to perform joint-probability analysis from this perspective. [13, 14] They subtracted off the first term of Equation 8 and then divided it by Equation 10, to form the ratio of the correlated pairs to the uncorrelated pairs in a joint-probability analysis. Following Feynman's choice of the letter *Y*, they denoted this ratio by the capital letter *Z*: [2]

$$\frac{\text{Average number of correlated pairs}}{\text{Average number of uncorrelated pairs}} =$$

$$\frac{\langle \binom{n}{2} \rangle - \frac{\langle n \rangle^2}{2}}{\frac{\langle n \rangle^2}{2}} = Z$$

$$Z = \frac{\varepsilon_2}{a^2 \tau_f^2} \frac{\langle \nu(\nu - 1) \rangle}{F\varepsilon\Delta t} \quad 1 - \frac{1 - e^{-ab.t}}{\alpha \Delta t}$$

Equation 11

(See also Equation 9.) As the length of the time interval goes to infinity, this ratio goes to zero, as can be seen mathematically by taking the limit. Physically, this fact occurs because, as the time interval increases, pairings are increasingly made among neutrons from random fission events and (α,n) reactions, rather than among the neutrons from just one fission event or short fission chain. Since pairings are a combinatorial quantity, the random pairings *among these unconnected fission events* rapidly swamp the correlated pairings within the set of neutrons of each of these fission events. The denominator of Equation 11 thus goes to infinity faster than the numerator, causing the ratio to go to zero.

(Note that this explanation is different from Pacilio's explanation on page 41 of his text, in which he says that the number of correlated pairs saturates within the interval as it is lengthened.[2] On the contrary, each extra fission event that is included does contribute more correlated pairs, since each fission event produces several neutrons simultaneously. The key is that these extra events contribute *even more uncorrelated pairings* than correlated ones, because the events themselves are uncorrelated with each other. Thus, the explanation here, rather than Pacilio's, is the correct one.)

One fact about Equation 11 that is essential to remember is that it is for *joint probability*, which means that these correlated and uncorrelated pairs are the pairs within *randomly or periodically triggered* time intervals. It is possible or even likely that any particular such time interval will contain zero neutrons. In contrast, conditional-probability analysis specifically excludes time periods that contain zero neutrons. The correlated and uncorrelated pairs in conditional-probability analysis are therefore different from those of joint-probability analysis, as presented in Equations 8 through 11.

3. Coincidence analysis by the conditional probability of detecting multiple neutrons as a function of the time after detecting one neutron

The fundamental expression of conditional probability is the Rossi-α curve (Figure 4). In its normalized form, it is the probability density function for a neutron to be detected after a first neutron has been detected. In its non-normalized form, it is the rate at which neutrons are detected after a first neutron has been detected, with units of counts per second. Figure 4 is not normalized, for example. The reader must be warned that almost all the literature uses the non-normalized form while simultaneously calling it a probability, which is obviously false.

The Rossi-α curve can be found either by an independent derivation or by manipulating the equation for the mean number of pairs in a randomly or periodically triggered time interval, Equation 6. This latter option has the advantage that the Rossi-α curve and the variance-to-mean ratio are thereby clearly proven to be related.

Taking the derivatives of Equation 6 with respect to the first and second detection times gives a kind of "joint" rate. By analogy with the definition of conditional probability, the average rate at which neutrons are detected (at time *t2*) after a first neutron (at time *t1*) is detected is as follows:

$$\mathrm{Rate}(t2|t1) = \frac{\mathrm{I}\,\frac{a}{at_1 at_2}\,\{\langle\binom{n}{2}\rangle\}\mathrm{I}}{FE} =$$

$$F\varepsilon + \frac{\varepsilon}{a\tau_f^2}\,\frac{\langle\nu(\nu-1)\rangle}{2} \qquad \text{Equation 12}$$

by analogy with conditional probability,

$$P(t_2 t_1) = \frac{P(t_1 Ç t_2)}{P(t_1)}$$

With *t1* set at zero and *t2* being variable, Equation 12 is the one-dimensional Rossi-α curve for prompt neutrons. [2, 5, 15] The rates are measured experimentally; and ε and τ*f* are assumed or separately measured. A least-squares fit of the *Rate*(*t2*|*t1*) data yields α; then Equation 12 is solved for ⟨ν(ν - 1)⟩, which is compared with the value from the literature to determine the isotopes in the sample.

There are two main ways to create a Rossi-α curve from measurements. (See Pacilio's report, page 13 [2], and Seifritz and Stegemann's paper, page 139 [7].) In both ways, the instrument waits until a neutron is detected and only then begins recording data. After the preset measurement time has elapsed, the instrument stops recording data associated with that first neutron and waits instead for another "first" neutron detection to trigger it again. The first way to make measurements is to not overlap measurement intervals. Even though several neutrons may be detected during the measurement period that was triggered by a first neutron, those several neutrons do not themselves start their own, separate measurement periods. Thus, this first way is wasteful of measurement time; because there is no physical distinction between one neutron and another, all neutrons can be considered as "first" neutrons. This fact leads to the second way to make measurements, which is indeed to start separate and overlapping measurement intervals after each and every neutron detection. This second way was actually the original way, used by Orndoff.[2, 7, 16] The two ways actually lead to different results. Babala [17, 18] explained it with reference to the Kolmogorov general theory of chain processes.

This difference between these two measurement methods leads to an important consideration of exactly how a Rossi-α curve comes to have its shape. The question is, "If every neutron can be a 'first' neutron—including the last neutrons to be detected from a fission event—then why is there a hump at the start of the curve? Why is the curve not flat, or why does it not have some random shape?"

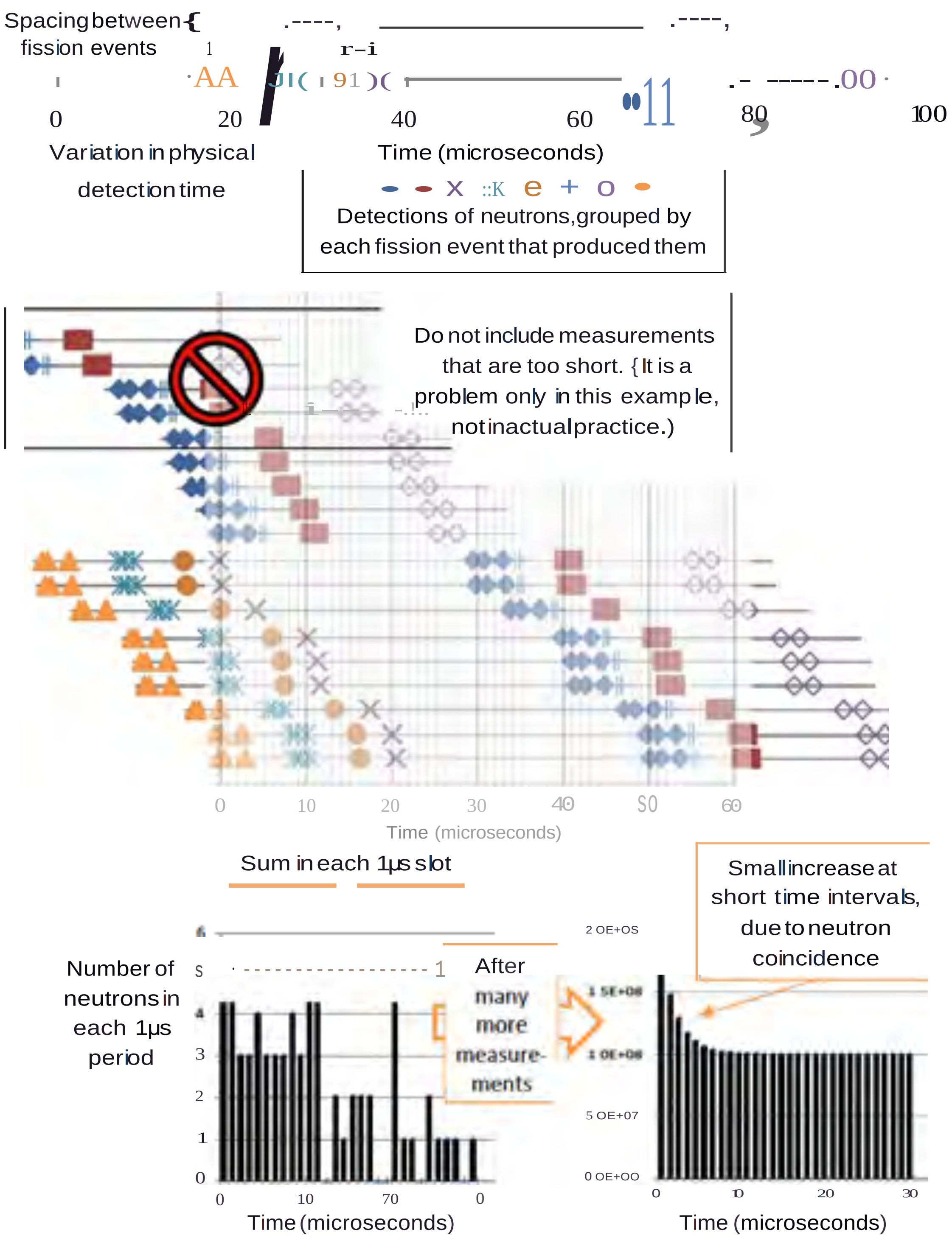


Figure 5: An example of creating a Rossi-a diagram from a time-sequence of neutron detections. Top: the time sequence. Middle: recording the data at each neutron detection, beginning with the first detection (bottom) and going to the last neutron detection (top). Bottom Left: summing the number of neutrons that fall into each 1 µs slot, from 0 µs to 30 µs. Bottom Right: a speculation about the final Rossi-a curve after measuring many more time-sequences (note the change in scale).

This question is related to the earlier warning about interpreting graphs that use the time of the fission event as the time origin (t = 0) of the graph.

The answer is most easily explained visually with a graph (Figure 5) of the creation of a Rossi-α curve by the second method mentioned above, that of starting a measurement interval with each and every detected neutron. As each neutron is detected, a type of gate is opened, to record the detections of all of the following neutrons within a specified time period. Because a separate gate is opened for each detected neutron, the subsequent neutrons are often being recorded in several gates simultaneously. This type of gate is not the same as the gates in the shift-register method of counting (described below), because those gates do not keep track of when the subsequent neutrons are detected, whereas this gate does. These time measurements of this gate are intentionally limited in their resolution, though, or else the resolution is worsened during the data analysis. In the example of Figure 5, the neutrons are put into time slots that are each 1 μs wide. The reason is simply that time is a continuous variable whereas neutrons are discrete entities; the discretization of time into time slots is therefore necessary in order to build up a histogram. This process of building up the histogram is illustrated in the middle and bottom-left parts of the figure. The separate gates associated with each detection are shown by stacking the time sequences.

It can be seen in Figure 5 that two kinds of time intervals are involved. The first kind is the differences in the physical detection times of the several neutrons emitted from each fission event. Although the physical detection time has some variation, the variation is nevertheless limited. The second kind is the time between fission events. This time interval is completely random for spontaneous fission events and (α,n) reactions but has some correlation for induced fission events, as mentioned before.

Consider first the presence of only the random events, that is, the spontaneous fissions and (α,n) reactions. During the recording of the data, the relatively close and consistent spacing of the physical detection time causes a buildup in the neutrons counted in the time slots closest to the origin. The random spacing between fission events, on the other hand, evens out the number of neutrons recorded at later times, farther from the origin. It is particularly important to recognize that this evening out occurs even though *clusters* of neutrons are indeed being recorded at these later times, because of the multiple neutrons released from each fission event. The fact that the neutrons are clustered has an effect only at the short time frames, when the several neutrons within each cluster cause a consistent and rapid succession of counts. Thus, the clustering of neutrons from each fission event implies correlation within each cluster but not from cluster to cluster. These principles remain true even when the fission events overlap with each other (which has not been done in Figure 5 for the sake of pedagogical clarity).

When induced fissions are included, the time between fission events has some correlation. This correlation appears in the Rossi-α diagram in the same way as the correlation among neutrons from the same fission event, except that the time scale over which the correlation is present is longer. For example, the exponential part of the histogram in the bottom right portion of Figure 5 would extend to later times when induced fission would be present. Indeed, what is happening is that there is a superposition of two die-away processes: the shorter-lived die-away caused by the variation in the physical detection time, and the longer-lived die-away caused by the subcritical decay of fission chains. If both die-away processes are exponential (as they are usually taken to be), then the superposition must be of the following form:

$$\mathrm{Rate}(t_2|t_1 = 0) = F\varepsilon + C_1 \exp(-a_{\text{physical detection time}} t_2) + C_2 \exp(-\alpha_{\text{fission chain}} t_2)$$

Equation 13

Here, *C1* and *C2* are constants. (Incidentally, the Differential Die-Away Self Interrogation (DDSI) method [19-21] attempts to distinguish between these two exponential terms.) The evening-out effect that was discussed in the previous paragraph still occurs when induced fission is present, but it can now be considered as being produced by the randomness among separate fission chains. In other words, the random spontaneous fission and (α,n) events, which produce the evening-out effect, now have fission chains attached to themselves.

The shift register is actually a piece of electronic hardware, used for counting neutrons.[1, 2, 7-9, 22, 23] The way that it counts the neutrons, though, is somewhat unique; and so the name for the hardware is often applied to the associated method of counting. The use of shift registers and the shift-register method of analysis is widespread in neutron coincidence and multiplicity analyses in the field of nuclear safeguards.

It is essential to recognize that the shift-register method is a conditional-probability method. Data— namely, the blank times between neutrons—are not recorded until one neutron is detected, thereby triggering the apparatus to record subsequent detections for a preset measurement period. This applies to the so-called “R+A” gate (Region 1 in Figure 6). The so-called “A” gate (Region 2 in Figure 6) is not conditional, since it is randomly triggered as explained in Section 1. Nevertheless, the coincidence information comes from the R+A gate and not the A gate, so the overall method is conditional.

The shift-register method of analysis essentially integrates Equation 12 over two separate regions of time: one for early times at which the exponential factor is still significant (Region 1), and one for later times at which it is practically zero (Region 2). (See Figure 6.) The difference between the regions thus corresponds to the second term and therefore to the multiplicity distribution. (See Equation 14.) With each triggering neutron (the “t/’ neutron), the number of neutrons within each region is tallied. Then for each region, a histogram can be made of the number of times it contains a certain number of neutrons, in an almost identical fashion as in Figure 2. (See Figure 7.) In other words, the gate width *l::::.t* is set to be long enough to span Region 1, but unlike in Figure 2, the time periods begin at each time that a neutron is detected, so that several time periods typically overlap at any given instant. For this reason, the PERIODS variable is given the subscr ipt “S.R.” (standing for “shift register”) to distinguish it. Moments can be taken of these histograms (Figure 7). Note that it appears

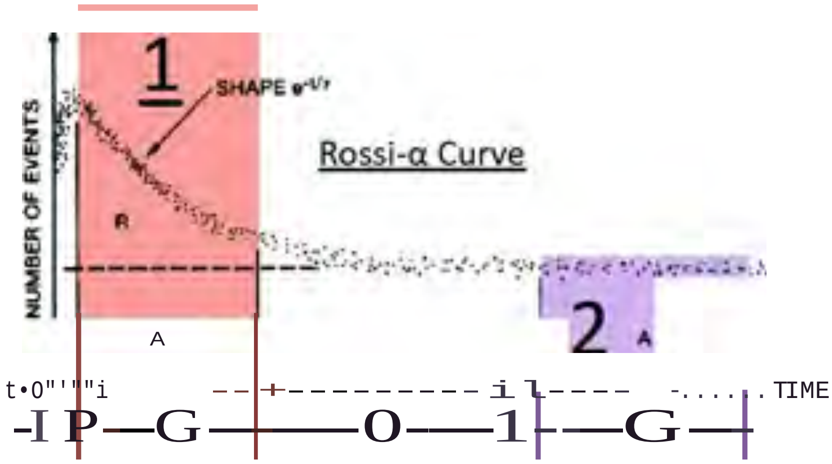


Figure 6: A modification of Figure 4, showing how the shift-register method is an integration of two regions of the Rossi-a curve

$$\textit{Region } 1 - \textit{Region } 2 = \int_{t=t_a}^{t=t_b} \textit{Rate } (t_2|t_1)dt - \int_{t=t_c}^{t=t_d} \textit{Rate } (t_2|t_1)dt$$

$$\cong \left(\frac{\varepsilon}{a^2\tau_f^2}\right)\left(\frac{\langle\nu(\nu-1)\rangle}{2}\right)\left(e^{-\alpha t_a} - e^{-\alpha t_b}\right) \qquad \text{Equation 14}$$

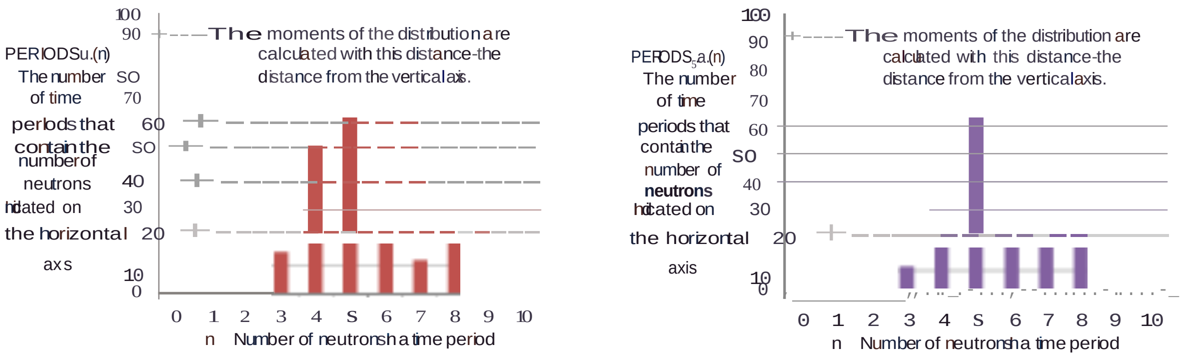


Figure 7: Histograms of the from a shift-register analysis of the neutron pulse train of Figure 2. The gate width is 10 time units long. Left: Region 1 (R+A gate). Right: Region 2 (A gate)

that more neutrons are counted in this figure than in Figure 2; the reason is that the time periods overlap, so many neutrons are counted several times each. The shift-register method is thus a hybrid between the "joint-probability" method of the variance-to-mean ratio and the "conditional-probability" method of the Rossi-a method.

The analysis by Dierckx & Hage [24] considered the differences in the moments of the two histograms for Regions 1 and 2 (e.g., Figure 7). The difference in the first moments (the means) represents the analysis of Equation 14. Dierckx & Hage said that the differences in the higher moments also represent the differences between correlated and uncorrelated multiplets. However, the histogram for Region 2, which Dierckx & Hage said is the "background" because it comes from random triggering, actually contains some correlation. If Region 2 is truly randomly triggered, then by the analysis of Feynman, De Hoffman, and Serber (Equations 3 through Equation 7), it must contain correlation, otherwise their analysis would not work. The reason that the first-order analysis (first moments) works is that the mean of the A gate is constant and represents the product of the average count rate and the gate width. It is therefore truly a background. For higher moments of the A gate, this is not the case, so that a simple subtraction cannot be done. It seems, therefore, that a multidimensional Rossi-α analysis, such as done by Bruggeman et al. [15, 25] may actually be needed.

4. Conclusion

This paper has discussed and compared joint-probability analyses and conditional-probability analyses. It has been shown in an intuitive way how they are related.

5. References

[1] Reilly, D, Ensslin, N, Smith, H, Jr., Kreiner, S (Eds.), *Passive Nondestructive Assay of Nuclear Materials*.

United States Nuclear Regulatory Commission, Washington, DC; 1991.

[2] Pacilio, N, *Reactor-Noise Analysis in the Time Domain*. U.S. Atomic Energy Commission, Washington, DC; 1969.

[3] de Hoffmann F, *Statistical Aspects of Pile Theory*, in: Goodman, C. (Ed.), *The Science and Engineering of Nuclear Power*. Vol. 2. Addison-Wesley Press, Inc., Cambridge; 1949. pp. 103-119.

[4] Feynman, RP, de Hoffmann, F, Serber, R, *Dispersion of the neutron emission in U-235 fission*. *Journal of Nuclear Energy (1954)*. 1956. 3, 64-69.

[5] Williams, MMR, *Random Processes in Nuclear Reactors*. Pergamon Press, Oxford, England; 1974.

[6] Mihalczo, JT, *Use of Californium-252 as a Randomly Pulsed Neutron Source for Prompt Neutron Decay Measurements*. *Nuclear Science and Engineering*. 1970. 41, 296.

[7] Seifritz, W, Stegemann, D, *Reactor-noise analysis*. *Atomic Energy Review*. 1971. 9, 129-176.

[8] Böhnel, K, *Die Plutoniumbestimmung in Kernbrennstoffen mit der Neutronenkoinzidenzmethode*. KFK2203. Kernforschungszentrum Karlsruhe, Karlsruhe, Germany; 1975.

[9] Böhnel, K, *Determination of plutonium in nuclear fuels using the neutron coincidence method*. H.M. Stationery Office, London; 1978.

[10] Böhnel, K, *The effect of multiplication on the quantitative determination of spontaneously fissioning isotopes by neutron correlation analysis*. *Nuclear Science and Engineering*. 1985. 90, 75-82.

[11] Albrecht, RW, *The Measurement of Dynamic Nuclear Reactor Parameters Using the Variance of the Number of Neutrons Detected*. *Nuclear Science and Engineering*. 1962. 14, 153-158.

[12] Keepin, GR, *Physics of Nuclear Kinetics*. Addison-Wesley Publishing Company, Reading, Massachusetts; 1965.

[13] Furuhashi, A, Izumi, S, *A proposal on data treatment in the Feynman-α experiment*. *Journal of Nuclear Science and Technology (Tokyo, Japan)*. 1967. 4, 99-101.

[14] Furuhashi, A, Izumi, A, *Third moment of the number of neutrons detected in short time intervals*. *Journal of Nuclear Science and Technology (Tokyo, Japan)*. 1968. 5, 48-59.

[15] Bruggeman, M, Baeten, P, De Boeck, W, Carchon, R, *Neutron coincidence counting based on time interval analysis with one- and two-dimensional Rossi-alpha distributions: an application for Qpassive neutron waste assay*. *Nuclear Instruments and Methods in Physics Research Section A*. 1996. 382, 511-518.

[16] Orndoff, JD, *Prompt Neutron Periods of Metal Critical Assemblies*. *Nuclear Science and Engineering*. 1957. 2, 450-460.

[17] Babala, D, *On the Theory of Rossi-Alpha Experiment in Reactor Noise Studies*. *Nuclear Science and Engineering*. 1966. 26, 418-419.

[18] Babala, D, *Theory of Rossi-α Experiment in Reactor Noise Analysis*. KR-105 (Nora-23). Institutt for Atomenergi, Kjeller Research Establishment, Kjeller, Norway; 1966.

[19] Menlove, HO, Menlove, SH, Tobin, SJ, *Fissile and fertile nuclear material measurements using a new differential die-away self-interrogation technique*. *Nuclear Instruments and Methods in Physics Research Section A*. 2009. 602, 588-593.

[20] Schear, MA, Menlove, HO, Tobin, SJ, Evans, LG, Croft, S, *Spent Fuel Characterization Using the Differential Die-Away Self-Interrogation Technique*. 52nd Annual Meeting of the Institute of Nuclear Materials Management (INMM), Palm Desert, California, July 17-21, 2011. Institute of Nuclear Materials Management (INMM), Deerfield, Illinois; 2011.

[21] Belian, A, Menlove, HO, Swinhoe, MT, Tobin, SJ, *New Design of the Differential Die-away Self- interrogation Instrument for Spent Fuel Assay*. *Journal of Nuclear Materials Management*. 2012. 40, 58-60.

[22] Edelmann, M, Externer Bericht INR-4/68-15. Kernforschungszentrum Karlsruhe, Karlsruhe, Germany; 1968.

[23] Ensslin, N, et al., *Application Guide to Neutron Multiplicity Counting*. LA-13422-M. Los Alamos National Laboratory (LANL), Los Alamos, New Mexico; 1998.

[24] Dierckx, R, Hage, W, *Neutron Signal Multiplet Analysis for the Mass Determination of Spontaneous Fission Isotopes*. *Nuclear Science and Engineering*. 1983. 85, 325-338.

[25] Bruggeman, M, Baeten, P, Paepen, J, Carchon, R, *Neutron Coincidence Counting with Time Interval Correlation Spectroscopy, luxury or necessity?* 20th Annual Meeting of the European Safeguards Research and Development Association (ESARDA), Sevilla, Spain, May 4-6, 1999. European Safeguards Research and Development Association (ESARDA), 1999.

"I agree that ESARDA may print my name, contact data, and article in the ESARDA Bulletin/Symposium proceedings."

Ontology-based semantic information technology for safeguards: Opportunities and challenges

Michael McDaniel

International Safeguards & Technical Systems Sandia National Laboratories[1]
Albuquerque, NM, USA mmcdani@sandia.gov

Abstract:

The challenge of efficiently handling large volumes of heterogeneous information is a barrier to more effective safeguards implementation. With the emergence of new technologies for generating and collecting information this is an issue common to many industries and problem domains. Several diverse information-intensive fields are developing and adopting ontology-based semantic information technology solutions to address issues of information integration, federation and interoperability. Ontology, in this context, refers to the formal specification of the content, structure, and logic of knowledge within a domain of interest. Ontology-based semantic information technologies have the potential to impact nearly every level of safeguards implementation, from information collection and integration, to personnel training and knowledge retention, to planning and analysis. However, substantial challenges remain before the full benefits of semantic technology can be realized. Perhaps the most significant challenge is the development of a nuclear fuel cycle ontology. For safeguards, existing knowledge resources such as the IAEA's Physical Model and established upper level ontologies can be used as starting points for ontology development, but a concerted effort must be taken by the safeguards community for such an activity to be successful. This paper provides a brief background of ontologies and semantic information technology, demonstrates how these technologies are used in other areas, offers examples of how ontologies can be applied to safeguards, and discusses the challenges of developing and implementing this technology as well as a possible path forward.

Keywords: safeguards; information; ontology; semantic technology; knowledge management

1. Introduction

The effective application of International Safeguards requires that the IAEA assess large volumes of information to come to high-confidence conclusions regarding States' uses of nuclear materials and technologies. Compiled from state declarations, inspection activities, material accountancy, laboratory analyses, sensors, open sources, and more, this information is heterogeneous in format, diverse in content and distributed in space [1]. To compound the challenge of handling such information, the emergence of the State Level Concept requires that the information analysis cycle be continuous and integrated; conducted within the context of all available information including existing knowledge in order to develop a complete picture of each State's nuclear fuel cycle activities.

The information challenges faced by the IAEA in carrying out its safeguards mandate, however, are by no means unique. Indeed these are the same problems faced by many industries whose main asset is information. The IAEA and its supporting organizations can look towards these industries and disciplines for best practices and technologies to make the handling of information more efficient.

Semantic technologies are among the solutions being developed to handle heterogeneous information. These technologies provide a structured means of describing information so that the information to be understood and processed by computers in meaningful ways. Often these technologies rely on ontologies which represent explicit specifications of knowledge within a domain. Semantic information technology has great potential to increase the efficiency of safeguards by helping to integrate, organize, and analyze heterogeneous information, but significant challenges remain for these benefits to be realized. This paper describes ontology-based semantic information technologies and their potential role in addressing the challenges of information management for International Safeguards.

2. Sematic information technologies

Information resources are largely designed and formatted for presentation to humans rather than for automated processing and manipulation by computers. While there are examples to the contrary, such as well-designed relational databases, these are inflexible and based on specific, often narrowly defined, data models. Semantic information technology attempts to shift this paradigm by allowing information to be encoded in such a way that computers can interpret and processes the information, thus taking some burden off the human consumer of information.

[1] Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND Number 2013-3943 C

The concept of semantic technology is not new. From the inception of the World Wide Web, Tim Berners-Lee envisioned a web of information that was meaningful to computers, rather than a web of documents meant primarily for human consumption [2]. However, by creating an information architecture that provides information that computers —understand|| it is possible to shift much of the analytic workload from humans to computers.

While semantic information technology encompasses a diverse collection of technologies such as natural language processing, data mining and artificial intelligence, this paper focuses on the technologies and specifications that serve as the foundation of the Semantic Web. Note, however, that Sematic Web technology does not pertain only to document exchange over the Internet; these concepts are equally applicable to all information systems.

One of the fundamental components of semantic technology is the concept of ontologies. Ontology comes from the metaphysics branch of philosophy and concerns the study of the nature of reality and its contents. Computer scientists have borrowed this concept to address the challenges of sharing information between systems based on an agreed upon understanding of reality. In computer science an ontology is a formal specification of knowledge within a given domain [3]. Ontologies explicitly encode concepts, their properties, relationships among concepts, and the logic for how these relationships are defined. Ontologies are defined using formal language in order to allow knowledge to be reliably reused. In a similar manner to object-oriented programming, once a concept is defined within an ontology as a Class it can be used to create specific instances, or individuals, based on this Class. For example, the Class <Country> may be used to instantiate the individual <Belgium>. The instance <Belgium> will inherit all the properties of class <Country> (e.g. having a population, spatial extent, etc.). These individuals can also be encoded into the ontology.

The development of ontologies for a given domain has several benefits including creating a shared conceptualization of knowledge that facilitates the sharing of information between systems and people. A well-developed ontology can serve as the basis of many advanced information management capabilities. Below, the fundamental building blocks of semantic information technology are described.

Ontologies can be encoded in any number of formal languages. The *Web Ontology Language* (OWL) is a family of formal language specifications and the W3C recommended specification for authoring ontologies. OWL provides formal semantics and vocabularies for defining classes, their properties and their relationships, for defining individuals based on these classes and asserting their properties, and the logic necessary to reason about classes and individuals [4]. In this way OWL can be understood as a modeling language capable of creating very specific, descriptive and complex models of the knowledge within a domain. These models are specified using standards that make the information —understandable|| to computers, allowing computers to manipulate the information described by the model in meaningful ways.

Figure 1 is an excerpt from the GeoNames Ontology [5], a widely used ontology for describing geographic places, and illustrates the graph structure common to OWL ontologies.

OWL itself it built upon another fundamental semantic web standard; the *Resource Description Framework* (RDF). RDF is the W3C recommendation for describing and exchanging information resources using Internet protocols. It also provides a flexible method for representing knowledge by decomposing knowledge into the smallest possible components, called statements. Statements consist of subject-predicate-object sets, or *triples*, that represent simple, distinct facts. Each statement relates a subject to an object. The predicate describes the nature of the relationship between the subject and the object (e.g. the triple <Light water reactor> <isType> <Nuclear reactor> represents the fact that a light water reactor is a class of nuclear reactors.) In order to make this method functional, it is necessary that subjects, predicates and objects (each potentially defined in OWL) be uniquely identified by a *uniform resource identifier* (URI). URIs are simply text strings that identify and provide the location of resources. Depending on the intended use of the resource identified by the URI, the URI can point to a location on the Web, in a file system, or on an internal server. Often, these URIs may refer to locations of classes or individuals in an OWL ontology. Specifying entities in this way allows for knowledge to be reused, shared and distributed across resources (for example, a subject may come from one location while an object and predicate come from another). In place of an object, predicates my relate subjects to a value. However, these values may belong to a class, as dictated by the predicate's logic.

Note that RDF is not a file format itself but is publishable in many different file formats, most commonly XML (other serializations such as N3 and Turtle also exist).

As mentioned previously, OWL is built upon RDF and allows for more expressive and meaningful descriptions and definitions of classes, properties and relationships than is provided by RDF itself. Additional specifications that are also RDF based such as the *Simple Knowledge Organization System* (SKOS) can be used within RDF documents to express additional information [6]. SKOS, for example, provides support for creating classification schema and thesaurus-type knowledge for resources.

Once ontologies have been developed and resources have been described using RDF, each can be queried using SPARQL, an RDF query language [7]. SPARQL is to RDF as SQL is to relational databases (RDF databases are referred to as *triplestores*). SPARQL, however, has many unique capabilities as compared to SQL that reflect the utility of RDF and semantic technology. For one, since RDF allows knowledge to be distributed, SPARQL can query across several repositories (i.e. it can conduct federated searches). In this way, a single query can draw information from multiple locations. Also, since semantic technology allows information to be integrated based on the meaningful descriptions encoded in RDF, SPARQL may potentially be used to generate complex queries for information from separate but interacting domains, given that each of these domains share a common ancestral schema.

Finally, there are several tools designed to reason over RDF data and OWL ontologies using the logic inherent in these specifications [8]. These reasoners compute logical consequences (e.g. if-then- therefore relations) from the statements contained within the triplestores or ontologies and allow for the development of sophisticated capabilities such as hypothesis testing or scenario generation based on the state of knowledge.

3. Examples of ontology-driven semantic technology adoption

Several diverse scientific disciplines and commercial industries have adopted semantic information technology in order to handle vast amounts of disparate and heterogeneous information and to create solutions to complex problems.

Perhaps the richest area of applied ontology work comes from the biomedical field. The problems of information management in clinical medicine are not entirely distinct from those of safeguards.

Biomedical professionals need to integrate large amounts of heterogeneous and distributed information in order to come to high-confidence conclusions regarding a patient's treatment. Medical records come in the form of imagery, laboratory results, unstructured text, and the like, and are decentralized, likely residing in individual doctors' offices. The need to unambiguously and reliably describe, communicate and exchange complex medical terminology is the primary driver behind this work [9]. The development of biomedical ontologies affords a solution to many of these problems by providing shared vocabularies and a standardized exchange mechanism for communicating terminology in a universal, reliable, and reusable manner.

Scientists in ecology are leveraging semantic information technology to synthesize knowledge from the volumes of existing information collected by individuals and institutions around the globe [10]. Because field research is difficult, costly and generally takes place over long time periods, scientists are looking at new ways to generate knowledge beyond collecting new data. Ecoinformatics has emerged as a subfield that is largely dedicated to integrating existing data to test new hypotheses, and to building tools to manage and share information based on semantic standards, e.g. [11]. Ontologies provide this community with a standard for publishing data so that it can be easily discovered and integrated with other resources that exist in various locations and in various formats as well as a new means of conducting science.

Not surprisingly, some of the largest and most conspicuous purveyors of information are adopting semantic technologies to help handle distributed, heterogeneous information. Within the past year

Google introduced the Knowledge Graph project that seeks to organize information resources and relationships among them in order to provide richer search results to its users by generating graphs based on search queries [12]. Facebook has developed the Open Graph Protocol, a simplistic metadata format based on RDF that allows web developers to describe their resources in a standardized way so that each information resource published on the web might be integrated into the social graph of Facebook [13].

For more information on the application of semantic information technology, W3C maintains a list of use cases that showcases the diversity of application spaces [14].

4. Semantic safeguards

There are several areas of safeguards for which the utility of semantic technology can be clearly recognized. Open-source information is one of these areas as it requires the collection and management of large amounts of heterogeneous, largely unstructured information. Given a well- developed nuclear fuel cycle ontology, open-source information could be semantically tagged with relevant concepts by natural language processors and stored with RDF metadata, greatly increasing the ability to integrate this information with other sources. Further, such a capability could be applied to existing resources, and information could be queried and combined regardless of where the information resides (similar to a federated information system).

Semantic technology also holds great potential for handling information in various languages by using internationalization standards that are already in place across the Web. For example, as the most common serialization of RDF is XML, any property can be modified by the xml:lang attribute to add additional translations to any resource. Once such a translation is added to a concept within the ontology, each resource referencing the concept can automatically inherit this translation and these resources can be seamlessly queried using any language encoded in the ontology.

The adoption of a nuclear fuel cycle ontology is consistent with the State-Level Approach. A nuclear fuel cycle ontology representing the general knowledge of all fuel cycle elements, materials, facilities and technologies can be instantiated for each state with a safeguards agreement.

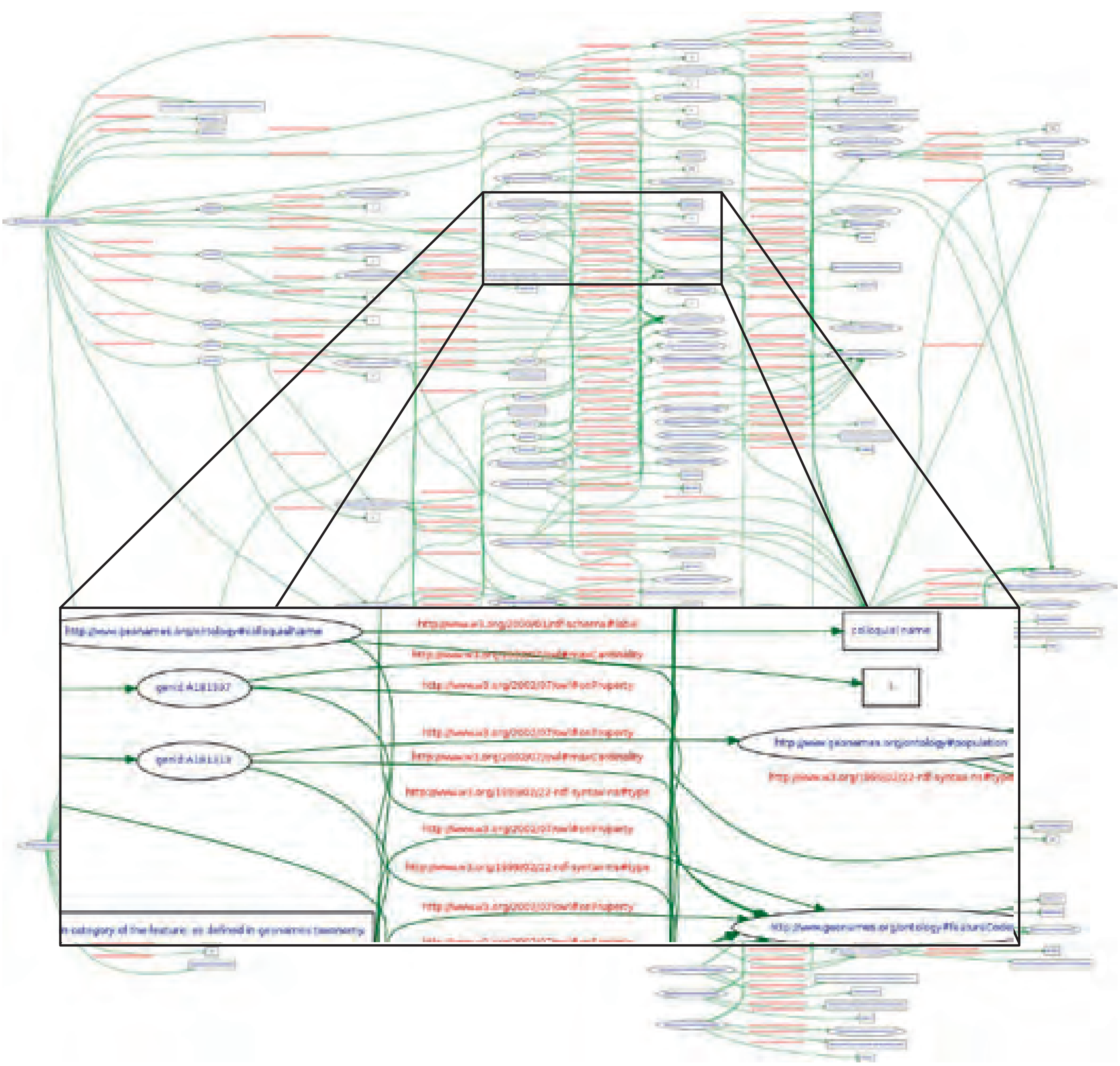


Figure 1: Graph structure of Classes and Attributes in the GeoNames Ontology, for illustrative purposes. Nodes represent subjects and objects while edges represent predicates. Note that nodes can be both subjects and objects.

State-specific knowledge (i.e. the states existing fuel cycle activities, declarations, etc.) could be added to each state-level ontology. This could serve as the platform for all state-level safeguard information to be stored, integrated and queried, thus facilitating the sharing of knowledge throughout the organization. Previously mentioned reasoning engines could then automatically analyze the consistency of declarations in light of existing knowledge, and highlight potential areas of concern for a given state (i.e. state X has technology Y and therefore may be doing Z). Such an ontology would inherently contain all possible proliferation pathways allowing for such capabilities as simulating diversion scenarios, and supporting future planning of safeguards activities by indicating to analysts and planners where to seek out potential noncompliance. This would represent an objective yet differentiating means of safeguards implementation.

Knowledge management at the enterprise scale would also be supported by the adoption of semantic information technologies. A standard, shared conceptualization of the nuclear fuel cycle, or of a particular state's fuel cycle as mentioned above, could serve as a valuable training tool for new staff. It could also be used as a tool to capture knowledge of departing staff. Moreover, semantic technology can standardize the exchange of information between departments, creating greater interoperability between systems which will be increasingly important under the State Level Concept.

5. A path forward

Ontology-based semantic information technology has the *potential* to impact every aspect of safeguards. While these benefits have already begun to be recognized with the use of named entity extraction and information harvesting tools, the full impact of semantic technologies may require the concerted, collaborative effort of the safeguards community.

Broadly speaking, it can be argued that the nuclear fuel cycle is the primary knowledge domain of interest for IAEA safeguards. By explicitly defining and describing existing knowledge of the nuclear fuel cycle—that is, by developing a nuclear fuel cycle ontology—the full potential of semantic information technology can begin to be reaped. However, the development of such a large and complex ontology is far from trivial. While the development of a complete fuel cycle ontology may be an ambitious undertaking it may be achievable by leverage the collective knowledge of the global community of safeguards experts, and by utilizing existing knowledge resources (such as the IAEA's Physical Model and various IAEA-maintained databases).

Ontology development must necessarily be a consensus activity. Creating an Ontology Working Group, perhaps under the auspice of the INMM-ESARDA (with input and guidance from the IAEA, of course), would provide the organizational platform and access to the expertise necessary to achieve this goal. This group could establish a collaborative engineering approach, breaking up the project into sub-tasks and sub-domains.

Noy and McGuiness [15] offer a sequential process for ontology development which includes: (1) Defining the domain and scope of the ontology; (2) Reusing existing ontologies and resources (for example, the Suggested Upper Merged Ontology [16] or some other upper-level ontology for high- level modeling); (3) Enumerating important terms in the domain; (4) Defining classes and class hierarchies; (5) Defining properties of classes (including cardinality, range, restrictions, etc.); and (6) Creating instances based on classes.

Following this model, the Working Group could make decisions regarding the first two tasks, while relying on subgroups with expertise in specific fuel cycle elements (e.g. enrichment, reactors, conversion, etc.) to carry out the third. Once the important domain terms are determined, the final steps could be —crowdsourced|| to experts around the globe who could contribute knowledge in their areas of expertise. To achieve this, a wiki-type site (with access controls) could be established with templates for specifying classes, properties and relationships. If done correctly, these wiki-pages could be easily converted into RDF/OWL documents. Such an effort would need to be curated to control quality, with editors volunteering for specified time periods to review additions and changes.

A parallel effort could involve IT specialists developing an information architecture capable of utilizing the ontologies generated by the group. This need not involve a complete re-engineering of the established architecture as semantic technologies may extend current systems rather than replace them.

6. Conclusions

Berners-Lee stated that —standards are the basis of emerging technologies|| [17]. Developing a nuclear fuel cycle ontology—a standard, shared knowledge representation of the nuclear fuel cycle—may be the key driver of innovation toward addressing the information management challenges of safeguards and making the safeguards regime significantly more efficient. While this is a difficult task, by leveraging the existing knowledge resources and the collective intelligence and effort of the global safeguards community, this can be achieved.

7. References

[1] M. Barletta, A. El Gebaly, W. Hammond, T. Lorenz, S. Robb, N. Zarimpas, and R. Zarucki, —Open Source Information Acquisition and Analysis in the IAEA Department of Safeguards,|| presented at the 33rd ESARDA Annual Meeting, Budapest, Hungary, 2011.

[2] T. Berners-Lee, J. Hendler, and O. Lassila, —The Semantic Web,|| *Scientific American*, vol. 284, no. 5, pp. 28–37, 17-May-2001.

[3] T. R. Gruber, —A translation approach to portable ontology specifications,|| *Knowl. Acquis.*, vol. 5, pp. 199–199, 1993.

[4] World Wide Web Consortium (W3C), —OWL 2 Web Ontology Language Document Overview (Second Edition),|| 11-Dec-2012. [Online]. Available: http://www.w3.org/TR/owl2-overview/. [Accessed: 07-Apr-2013].

[5] B. Vatant, —GeoNames Ontology - Geo Semantic Web.|| [Online]. Available: http://www.geonames.org/ontology/documentation.html. [Accessed: 06-Apr-2013].

[6] World Wide Web Consortium (W3C), —Introduction to SKOS - Simple Knowledge Organization System.|| [Online]. Available: http://www.w3.org/2004/02/skos/intro. [Accessed: 08-Apr-2013].

[7] World Wide Web Consortium (W3C), —SPARQL 1.1 Overview.|| [Online]. Available: http://www.w3.org/TR/sparql11-overview/. [Accessed: 08-Apr-2013].

[8] World Wide Web Consortium (W3C), —OWL Reasoner - Semantic Web Standards.|| [Online]. Available: http://www.w3.org/2001/sw/wiki/Category:OWL_Reasoner. [Accessed: 07-Apr-2013].

[9] D. M. Pisanelli, —OpenClinical: Ontologies.|| [Online]. Available: http://www.openclinical.org/ontologies.html. [Accessed: 07-Apr-2013].

[10] J. Madin, S. Bowers, M. Schildhauer, S. Krivov, D. Pennington, and F. Villa, —An ontology for describing and synthesizing ecological observation data,|| *Ecol. Informatics*, vol. 2, no. 3, pp. 279– 296, Oct. 2007.

[11] National Center for Ecological Analysis and Synthesis, —Semantic Tools for Data Management (Semtools).|| [Online]. Available: https://semtools.ecoinformatics.org/. [Accessed: 07-Apr-2013].

[12] A. Singhal, —Introducing the Knowledge Graph: things, not strings,|| *Official Google Blog*, 16-May- 2012.

[13] —Open Graph protocol.|| [Online]. Available: http://ogp.me/. [Accessed: 06-Apr-2013]

[14] World Wide Web Consortium (W3C), —Semantic Web Case Studies and Use Cases.|| [Online]. Available: http://www.w3.org/2001/sw/sweo/public/UseCases/. [Accessed: 08-Apr-2013].

[15] N. F. Noy and D. L. McGuiness, —What is an ontology and why we need it.|| Stanford University, 2000.

[16] A. Pease, —The Suggested Upper Merged Ontology (SUMO),|| 2013. [Online]. Available: http://www.ontologyportal.org/. [Accessed: 08-Apr-2013].

[17] T. Berners-Lee, —Opening Keynote - The Semantic Web,|| presented at the Technology Review - The Emerging Technologies Conference at MIT, Massachusetts Institute of Technology, 29-Sep- 2004.

Approaching acquisition path analysis formally - a comparison between AP and non-AP States

Clemens Listner[1], Morton J. Canty[1], Arnold Rezniczek[2], Gotthard Stein[3] and Irmgard Niemeyer[1]

[1]Forschungszentrum Jülich, Germany
[2]UBA GmbH, Herzogenrath, Germany
[3]Consultant, Bonn, Germany

Abstract:

In the past, the IAEA has planned its activities mainly based on the presence of nuclear material. However, resources should be spent where they are needed most. Therefore, a new risk model was developed to change the inspection system to a comprehensive, objective-driven approach where the State is considered as a whole, the so called State-level concept (SLC). Acquisition path analysis (APA) is a key element of the State-level concept. By considering the State's nuclear profile, the APA generates a list of acquisition paths ranked by their attractiveness for the State. Currently, this process is mainly based on expert judgment. However, the IAEA's requirements state that APA must be objective, reproducible, transparent, standardized, documented and as a result non-discriminatory.

A formal approach fulfilling the requirements was set up by the authors in the past [1]. This methodology is based on a three step approach. The process starts in the first step with the parametrization of the network. In the second step, the network is analyzed in order find all acquisition paths for a State. Finally, game theory is used in the third step to model the decisions made by the IAEA and the State.

In this paper, an advanced methodology will be presented. Improvements were made in the interface definition between the three stages. Also, the general network model was updated and the automatic visualization of acquisition paths was accomplished. Furthermore, a prototype implementation will be shown.

The advanced methodology was applied to two test non-nuclear weapon States under comprehensive safeguards agreements with the IAEA. Both States hold complex fuel cycles with only small technical differences. However,only one State is supposed to have the additional protocol (AP) in force. The example will show how the presence of the AP influences the detection probabilities of illegal behavior. As a consequence, these examples also indicate where to best focus safeguards efforts.

1. Introduction

Due to the experiences made in the past, the IAEA has developed a vision of a new verification model - the State-level concept (SLC). While the former approach has focused on declared nuclear material and facilities, the new concept concentrates on facts about a State. In order to increase effectiveness and efficiency, the IAEA wishes to migrate from a mechanistic verification procedure to a risk-based prioritization of its activities.

While differentiating between States due to different risk levels seems reasonable, one has to assure that no single State will be discriminated. Therefore, the State-level concept is to be objective, transparent, reproducible, standardized and documented (for details see Listner, Canty, Rezniczek, Stein, and Niemeyer [1]). Furthermore, the State-level concept should be applicable to all States with commitments regarding nuclear non-proliferation, item- or facility-specific safeguards agreements (INFCIRC/66), comprehensive safeguards agreements (CSA) with and without additional protocol (AP) as well as voluntary offer agreements (VOA) in nuclear weapon States (NWS).

According to Cooley [2], the State-level concept comprises three steps leading to a specific State-level safeguards approach:

1. Identification of plausible acquisition paths.
2. Specification and prioritization of State-specific technical objectives.
3. Identification of safeguards measures to address the technical objectives.

In the present paper, we will concentrate on the first step of the process, the acquisition path analysis (APA), as this is still a major difficulty when elaborating a State-level approach. According to IAEA [3], an acquisition path is defined as a sequence of activities which a State could consider in order to acquire weapons usable material. The APA analyzes all plausible acquisition paths, aiming to determine whether a proposed set of safeguards measures will be effective.

Up until now, the IAEA has implemented APA mainly based on expert judgment. This has led to a procedure that, although standardized, cannot fulfill the requirements mentioned above. Therefore, the IAEA is looking for a methodology and software tool that helps structuring the process of APA. The tool should provide for visualization of the acquisition paths in order to help the analyst maintain an overview of the situation in a State. It should automate

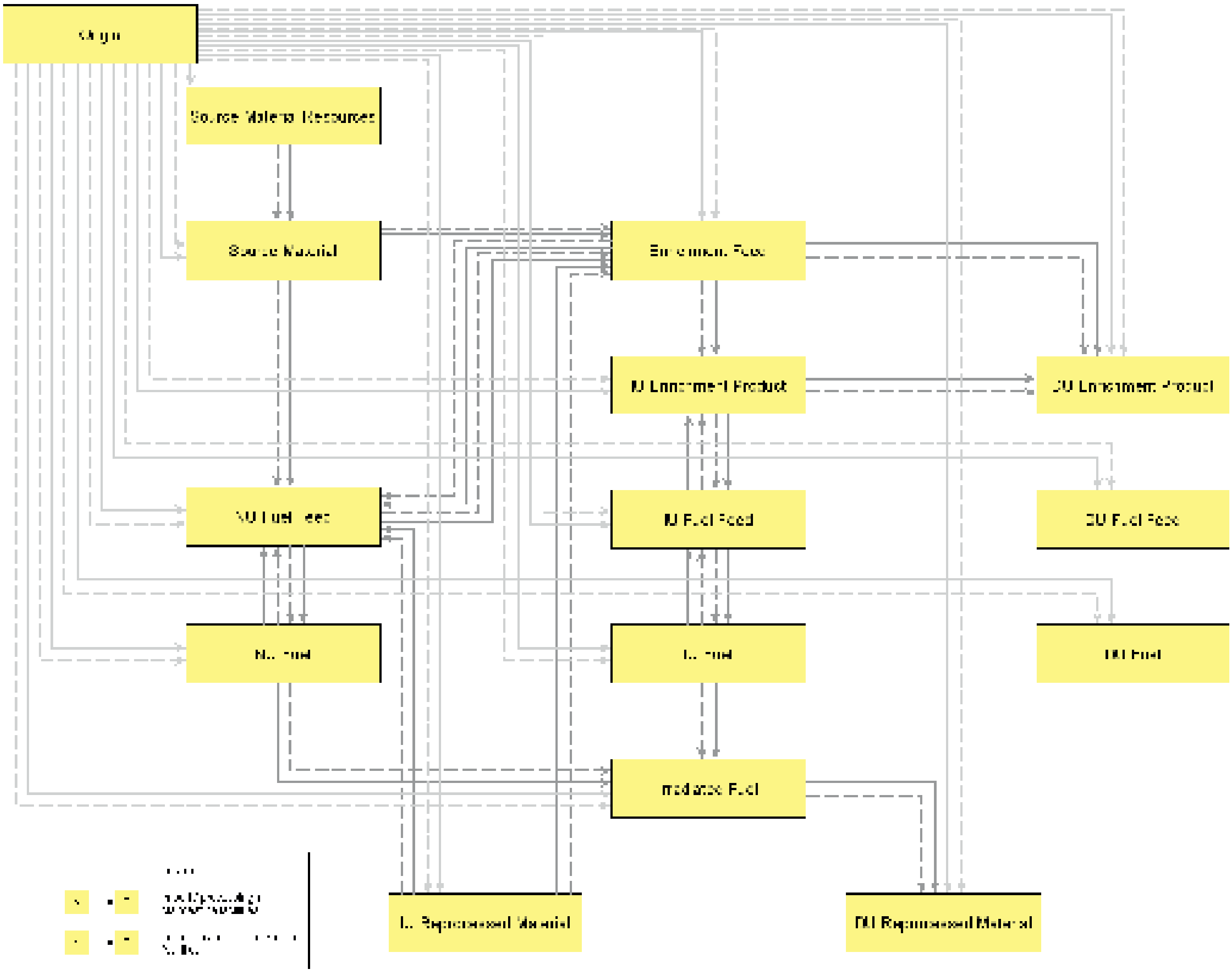


Figure 1: Generic physical model.

the process in order to be independent of subjective reasoning and thus guarantee reproducibility. Finally, a software tool assisting the analyst should integrate into existing systems and models at the IAEA.

In the following sections, we describe a new formalized procedure using network analysis techniques and game theory in order to assess proliferation risks and help distributing the inspectorate's resources in a reasonable way. In order to demonstrate the method, two case studies were carried out. Both cases were based on States with advanced fuel cycles. While the technical capabilities only slightly differ, they hold different safeguards agreements with the IAEA. The fi State has a CSA as well as an AP based on INFCIRC/540 (corrected) including a broader conclusion in force. The second State only holds a CSA with the IAEA.

2. Materials and Methods

As mentioned in the previous section, the IAEA's physical model serves as a basis for APA. It comprises an overview of all known relevant processes for converting nuclear source material to weapon usable material (see definition in IAEA [3]). In Figure 1, a generic version is depicted. The yellow boxes represent material forms which are transformed to other material forms by using specific processes symbolized by arrows in the model. In the fi the acronym "DU" stands for direct use, "IU" for indirect use and "NU" for natural uranium. Within the physical model, an acquisition path always starts at the "Origin" box followed by the diversion or undeclared import of the first material form. From there, consecutive process steps consisting either of misuse of declared facilities or of processing in undeclared facilities are needed in order to fi acquire weapons usable material, i.e. any material in the physical model with the prefi "DU".

From a mathematical point of view, the physical model can be considered as a directed graph. Therefore, it is possible to apply graph theory to the APA problem in order to fi all technically plausible paths.

In a directed graph, nodes can be connected by edges. To each edge a scalar number can be associated to measure the edge's length. Sequences of edges are called paths whose lengths are calculated by the sum of the edge weights. The concept of graph theory applied to acquisition path analysis implies a node being a material form in the physical model, an edge representing a process and a path standing for the acquisition path itself. Edge weights can be used to reflect the attractiveness of a process.

Using the model of a mathematical graph, acquisition paths can be found using several algorithms. The shortest path between two nodes can be found using e.g. the Dijkstra algorithm (see Dijkstra [4]). However, for a comprehensive analysis of a State's nuclear options, all paths from "Origin" to any of the "DU" material forms have to be assessed. This can be easily accomplished using enumeration techniques that prevent cycles contributing to an acquisition path.

Besides finding acquisition paths, APA ought to assess paths with respect to their suitability for a nuclear weapons program. As this comprises a strategic aspect, game theory is the appropriate tool to accomplish this task.

Game theory is a mathematical approach with the ability to model strategic situations between opposing players. By strategic situation, a choice between different decision alternatives is meant where decision making does not only depend on the protagonists' own courses of action but also on those of their opponents. Applied to APA, the inspectorate and the State are the opposing players. The strategies of the State are the acquisition paths themselves, as well as the strategy of compliant behavior. For the inspectorate, the different safeguards approaches, i.e. the inspection of a subset of all processes, can be considered as strategies. Each combination of the players' strategies may be associated with the players' utilities, thus leading to a bi-matrix representation of the game (for details see Canty [5]). Using this problem formulation, game theory provides a solution using the concept of Nash equilibrium. A Nash equilibrium in a two-person game is defined as a strategy combination for which neither of the players can deviate unilaterally in order to increase his or her utility. Thus, a relative scale is defined upon which different acquisition path configurations can be evaluated and compared. The effectiveness of a given inspection regime can be measured on the basis of the inspectorate's payoff. The most efficient strategy for the IAEA is that minimum effort strategy which is part of a Nash equilibrium in which the State behaves legally.

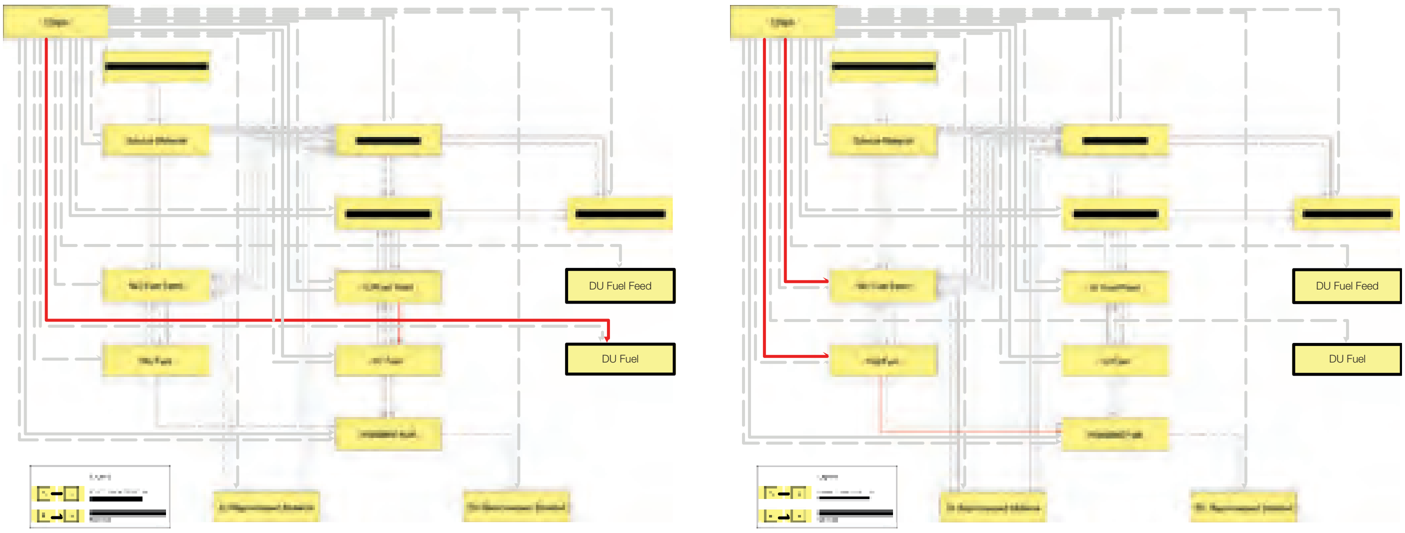
Using both graph theory and game theory, a new 3-step approach to acquisition path analysis was established. This approach is depicted in Figure 2.

The first step, network modeling, parameterizes the model. With respect to the edge weights, GIF PR/PP (see GEN IV International Forum [6]) proposes six measures for evaluating pro- liferation resistance which can also be used to model attractiveness in the case of APA. For this paper, three of these measures, technical difficulty (TD), proliferation time (PT) and proliferation cost (PC), are taken into account. Using these dimensions, the analyst is given the opportunity to rate each process based on a scale from 0 (very attractive), to 3 (very unattractive).

In the second stage of the process, the network analysis, all paths with their respective lengths are enumerated and sorted in decreasing order of attractiveness. Additionally, the paths are visualized using the GraphML format (see Brandes, Eiglsperger, and Lerner [7]) and yEd Editor (freely available at www.yworks.com). This step is carried out in a fully automatic way using a Python script including the NetworkX toolbox (see Hagberg, Schult, and Swart [8]).

Finally, in the third stage of the process, the strategic assessment, the strategic options of both the IAEA and the State are evaluated using the game theoretic approach described above. To accomplish this, actions of the inspectorate are associated with costs and pre- sumed detection probabilities. Based on a cost threshold *W*, it is

Figure 2: 3-step approach to acquisition path analysis.



State A. (b) State B.

Figure 3: Physical models for the two cases with diff highlighted in red.

possible to compute the Nash equilibria sequentially and thus to obtain the inspectorate's minimum effort strategy for inducing compliant behavior on behalf of the State.

3. Example Case Studies

In order to illustrate the methodology's workflow presented in Section 1, it was applied to two non-nuclear weapon States (NNWS) signatory to the non-proliferation treaty (NPT). Both States were modeled as having a CSA in force. However, for State A an additional protocol was assumed to be in force with the broader conclusion drawn. For State B no additional protocol was considered.

At fi the generic physical model in Figure 1 was adopted to the situation in the two countries leading to the removal of several edges: Both States were assumed to have no declared reprocessing, i.e. the edges representing the diversion of reprocessed material as well as the edge for the misuse of an existing reprocessing facility were deleted. Also, direct use material was only supposed to be present as direct use fuel in State A. Therefore, the edges representing diversion of those materials were removed except for direct use fuel diversion in the case of State A. Furthermore, no declared natural uranium fuel cycle was assumed in State A, thus the edges for natural uranium diversion and the misuse of a heavy water reactor were removed. On the other hand, in State B no reactor utilizing direct use fuel was modeled. Therefore, diversion of this type of fuel was not part of the physical model in the case of State B. The modifi physical models are shown in Figure 3.

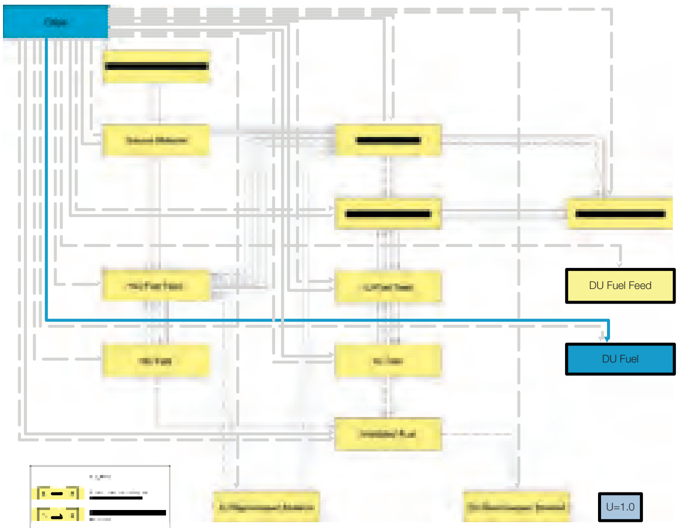
Both States were modeled to have a complex nuclear fuel cycle with a great deal of nuclear experience and know-how. Therefore, the attractiveness ratings were chosen similarly for State A and State B.

Regarding the inspectorate costs, the Safeguards Implementation Report (SIR) from 2011 served as a basis for estimation. For State A, the costs of all possible safeguards measures were assumed to be 5,900,000 EUR. Accordingly, for State B this amount was supposed to be 6,600,000 EUR. Based on the person-days of inspection, these costs were split and associated to particular areas of the physical model.

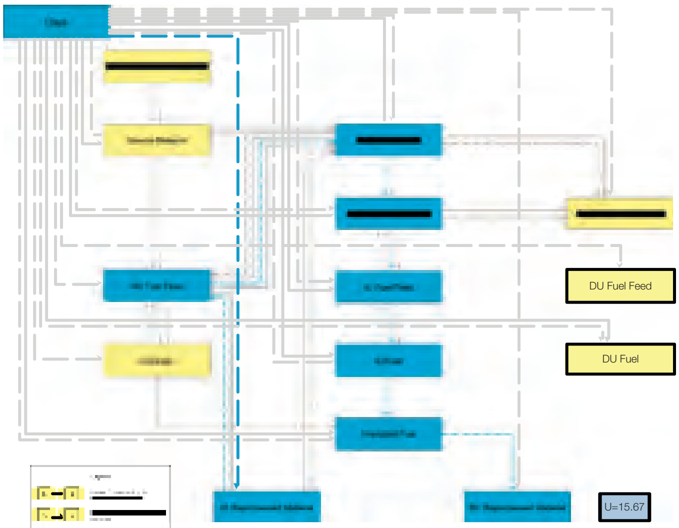
Expert judgment was applied to assess the attractiveness of each edge in the physical model. The IAEA's detection probability for clandestine processing was set to 95% in State A due to the presence of the AP and a broader conclusion. The figure of 95% detection probability is derived from the SIR statement saying that in a State with CSA, AP and broader con- clusion "'all nuclear material remained in peaceful activities"'. As there is always a chance to be wrong, a detection probability of 95% or equivalently a non-detection probability of 5% was assumed. In case of State B without the AP and the broader conclusion, the SIR statement is restricted to declared nuclear material implying that the IAEA is unable to draw a conclusion regarding undeclared activities. But there is always a certain chance of obtaining other kinds of information which is considered to be significantly higher than the non-detection probability for clandestine processing of 5% in case of State A. Therefore, the detection probability for clandestine processing was assumed to be 20% in State B.

After these steps, the adjacency matrix was available for further analysis. To accomplish the modeling, Microsoft Excel was used, allowing for an export of the relevant data.

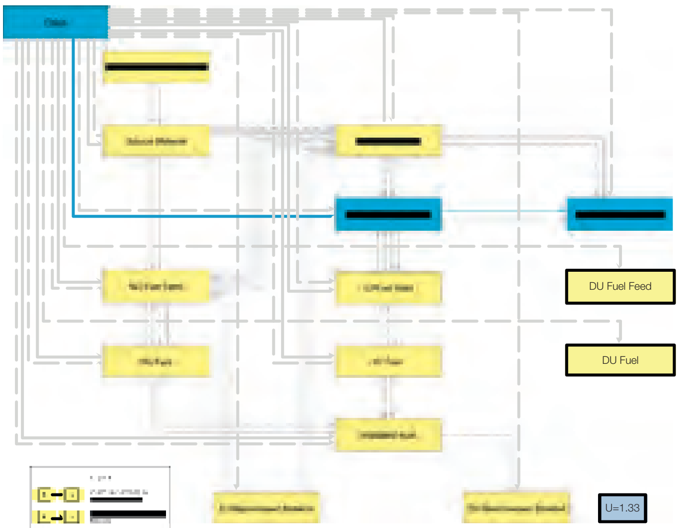
Based on the outcome of the fi step, all paths between the "Origin" node and any "DU" node were enumerated, visualized and sorted according to their attractiveness in the second step. This step uses the Python script mentioned



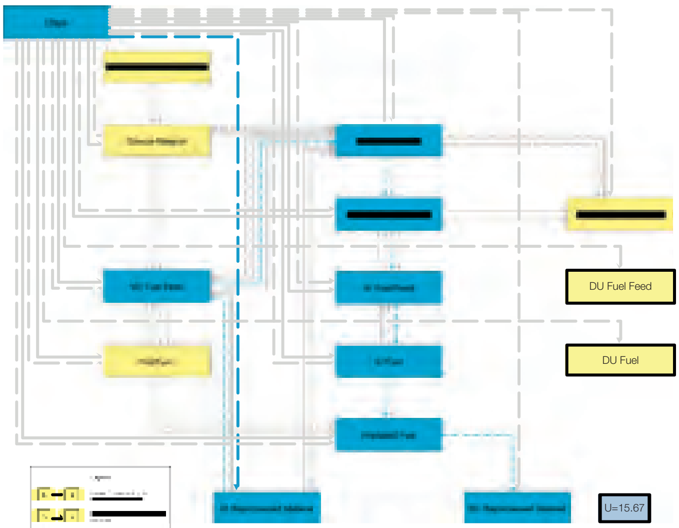
(a) Most attractive path for State A.



(b) Least attractive path for State A.



(c) Most attractive path for State B.



(d) Least attractive path for State B.

Figure 4: Two paths for each of the example cases.

in the previous section. Thus, a list of 1041 paths for State A was generated, while 814 paths resulted for State B. Moreover, for each path a separate chart was generated visualizing the respective acquisition path and its attractiveness (see examples in Figure 4).

In the third step, the acquisition paths together with compliant behavior were considered as the State's strategies. This led to a total number of 1042 strategies for State A and 815 strategies for State B. For the IAEA, any combination out of 16 distinct activities for State A and 18 distinct activities for State B were assumed to be a strategy. The costs for each combination of inspectorate activities were calculated based on the input from the SIR. By setting a limit on the inspectorate's costs, a set of strategies for the IAEA was determined. Then, the Nash equilibrium was calculated. If it did not comprise compliant behavior on behalf of the State, the threshold was increased by the amount of 100,000 EUR until the maximum amounts of 5,900,000 EUR or 6,600,000 EUR where reached. This approach led to the results in Figure 5.

Regarding the equilibrium strategies for a maximum budget of 800,000 EUR given State A, the inspectorate player chose a mixed strategy consisting of seven particular inspection strategies. The areas of the physical model that each strategy focused on are marked by an "'x"' in Table 1. The player representing the State, on the other hand, chooses compliant behavior in this situation.

According to the model, a budget of 800,000 EUR was sufficient to induce legal behavior in the case of State A. Further increasing *W* did not change this behavior. Following the comparison of the estimated with the actual budget of 5,700,000 EUR spent in State A, a significant increase in efficiency without losing effectiveness should be considered possible. In the equilibrium situation for the model of State B and *W* set to the maximum budget of

Strategy #	1	2	3	4	5	6	7
Probability	2%	5%	24%	32%	21%	6%	10%
Costs [kEUR]	793	785	727	689	794	741	741
DU Fuel Diversion	x	x	x	x	x		
IU Enrichment Product Diversion	x	x				x	
Enrichment Feed Diversion	x						x
Conversion I Misuse	x		x				
Irradiated Fuel Diversion		x					
Undeclared Import			x			x	x
Enrichment Misuse				x			
Undeclared Processing					x		

Table 1: Equilibrium strategy for the inspectorate in case of State A and W = 800, 000.

6,600,000 EUR, the inspectorate player chooses the strategy comprising all possible safeguards measures. The player representing State B, though, chooses an acquisition path leading to highly enriched uranium. This path is mainly based on processing in clandestine facilities.

This example turns out that deterrence cannot be achieved by the inspectorate in case of State B, as the detection probability for undeclared processing only amounts to 20% due to the absence of the additional protocol.

It should be noted that, in general, effectiveness values between 0 and 100% can arise when the State's Nash equilibrium strategy is illegal behavior given a fi chance of detection. This situation does not arise in the case of State A, however.

4. Conclusions and Outlook

Within this paper, an advanced 3-step methodology for acquisition path analysis was presented. The approach fulfils the IAEA's requirements regarding acquisition path

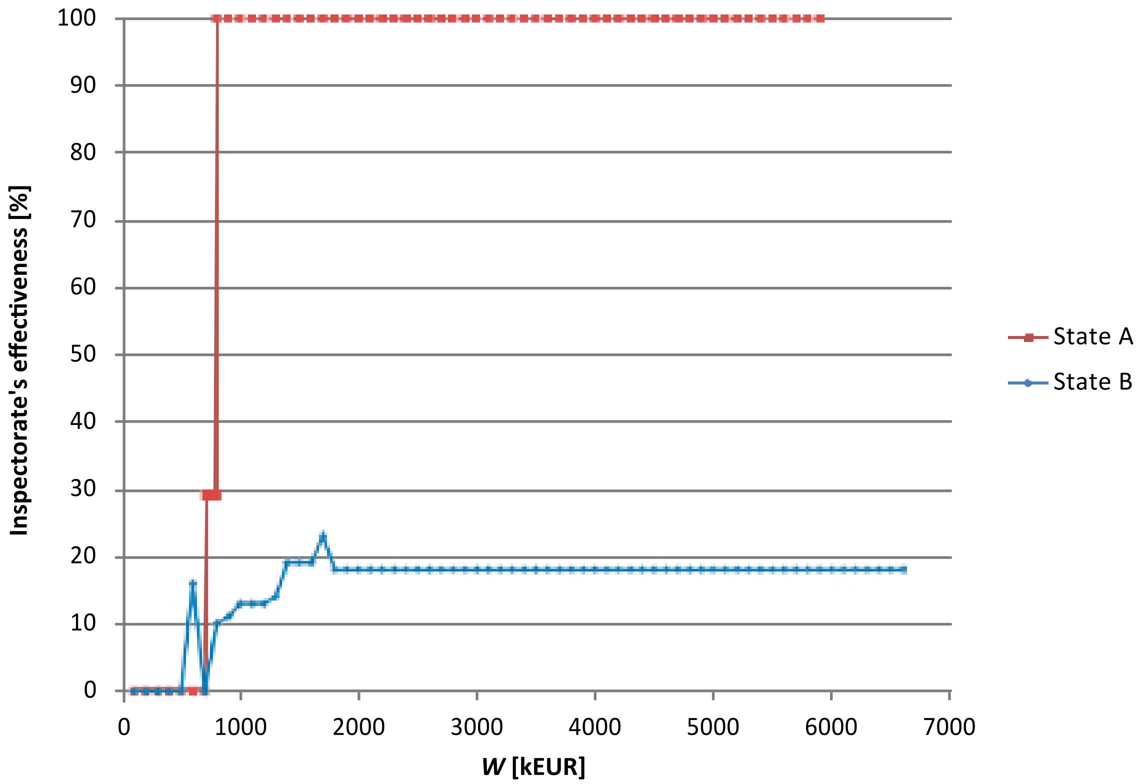


Figure 5: The inspectorate's effectiveness for the two States depending on the maximum budget.

analysis of being objective, reproducible, transparent, standardized and documented. As a result, the methodology accounts for differentiation between States without discrimination. Moreover, the procedure is modular and can be automatized. However to select the model's parameters, expert judgement is needed. But since the parameters values can be easily varied in the model, the effect of different assumptions on the outcome can be easily investigated and the analyst gets a clear feedback on the effect of different assumptions. Therefore, it should only be seen as a tool assisting but not replacing the analyst. A comparative example was presented showing that it is of utmost importance for the inspectorate to have the ability to detect undeclared processing.

Future work will, inter alia, comprise the enhancement of the cost model, the additional visualization of the game theory results and the operationalization as well as the integration into existing systems at the IAEA.

5. Acknowledgments

This paper was prepared as an account of work sponsored by the Government of the Fed- eral Republic of Germany within the Joint Programme on the Technical Development and Further Improvement of IAEA Safeguards between the Federal Republic of Germany and the IAEA.

6. References

[1] C. Listner, M.J. Canty, A. Rezniczek, G. Stein, and I. Niemeyer. "A Concept for Han- dling Acquisition Path Analysis in the Framework of IAEA's State-level Approach". In: *Proceedings of the INMM Annual Meeting*. INMM. 2012.

[2] J.N. Cooley. "Progress in Evolving the State-level Concept". In: *Seventh INMM/ESARDA Joint Workshop Future Directions for Nuclear Safeguards and Verification*. 2011.

[3] IAEA. "IAEA Safeguards Glossary". In: *international nuclear verification series No. 3* (2001).

[4] E.W. Dijkstra. "A note on two problems in connexion with graphs". In: *Numerische Mathematik* 1.1 (1959), pp. 269–271.

[5] M.J. Canty. *Resolving conflicts with Mathematica: algorithms for two-person games*. AP, 2003.

[6] GEN IV International Forum. *Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems*. 2006.

[7] U. Brandes, M. Eiglsperger, and J. Lerner. "GraphML primer". In: *Online available at http: // graphml. graphdrawing. org/ primer/ graphml- primer. html (accessed April 02, 2013)* (2011).

[8] A. Hagberg, D. Schult, and P. Swart. "NetworkX Library". In: *Code available at http:// networkx. github. com/* (2004).

7. Nomenclature

AP	additional protocol
APA	acquisition path analysis
CSA	comprehensive safeguards agreements
NNWS	non-nuclear weapon State
NPT	non-proliferation treaty
NWS	nuclear weapon State
PC	proliferation cost
PT	proliferation time
SIR	Safeguards Implementation Report
SLC	State-level concept
TD	technical difficulty
VOA	voluntary offer agreement

Preparation of Pu particle quality control materials

Cheolsu Kim, Takahiko Kitao, Ernesto Chinea Cano, Zsuzsanna Macsik, Stephan Vogt, Thippatai Tanpraphan, Olivier Pierre Bildstein, Laure Sangely, Jane Poths

International Atomic Energy Agency Department of Safeguards, Safeguards Analytical Services
IAEA Laboratories A-2444 Seibersdorf, Austria
E-mail: c.s.kim@iaea.org, kitao.takahiko@jaea.go.jp, e.chinea-cano@iaea.org, z.macsik@iaea.org, t.tanpraphan@iaea.org, o.bildstein@iaea.org, l.sangely@iaea.org, j.pohts@iaea.org

Abstract:

Plutonium particles were produced at the Technical Research Centre of Finland (VTT) from a well characterized solution of CRM 136 (Department of Energy, New Brunswick Laboratory, Chicago, U.S.A.) after chemical separation of americium (Am) and the plutonium (Pu). Different particle recovery methods were tested and individual Pu particles characterized for their size, Pu content and isotopic composition. Samples with known numbers of individual particles were produced for Pu/Am age dating analysis.

Keywords: particle analysis, CRM *136*, quality control particles

1. Introduction

The International Atomic Energy Agency's (IAEA) Environmental Sample Laboratory (ESL) carries out uranium (U) and plutonium (Pu) bulk and particle analysis of environmental samples collected during in-field safeguards activities. Environmental samples are typically swipe samples taken at nuclear facilities that are analysed to look for any indications of undeclared nuclear materialor activities carried out at these facilities. Analyses are performed by the ESL and are complemented by those of other laboratories from the IAEA's Network of Analytical Laboratories (NWAL).

Instrument calibration, method validation and quality control of the analytical processes require certified reference and well-characterized quality control (QC) materials. For U and Pu particle analytical techniques the availability of such materials is very limited.

Uranium, Pu and mixed U/Pu oxide particles were produced at the Technical Research Centre of Finland (VTT) using well-characterized solutions produced from different Certified Reference Materials (CRM) [1]. For Pu one set was produced from CRM 136 solution after chemical separation of Pu from americium (Am). Subsequently, individual PuO_2 particles were studied for their size distribution and other physical properties. Plutonium isotopic composition was characterized by analysing solutions produced from the dissolution of multiple particles [2].

In the particle production experiments carried out at VTT in Finland vacuum grease (Apiezon-L) was used to cover the aluminium (Al) impactor foils for better retention of the impacting particles. One technical challenge in handling the final product is the removal of particles from the Al impactor catcher foils for detailed studies and QC material production. Techniques to remove particles from the Al impactor foils and handling of individual particles for their analysis by a scanning electron microscope (SEM) and inductively-coupled plasma mass spectrometry (ICP-MS) after chemical dissolution, were tested.

The paper briefly presents the particle removal techniques, particle characterization and production of test samples for Pu/Am analysis using particle analytical techniques.

2. Experimental

For our particle removal tests we chose the Al impactor foil from stage 8, the same that was used in the initial characterization study by Shinonaga et al. [2]. A small section of about 1 cm was cut from the donut-shaped impactor foil and placed in a PFA (Perfluoroalkoxy, Savillex, U.S.A.) vial. After the addition of 2 mL of a solvent the vial was placed in an ultrasonic bath and sonerated for 10 minutes. Water, ethanol, isopropanol, heptane and acetone were tested in the experiment. After soneration the suspension was dried and the residue re-suspended in 0.2 mL of high purity water. A 1 µL aliquant of this suspension was applied onto the surface of a clean silicon wafer chip. The aliquant was dried and any organic residue decomposed by heating the silicon wafer to 400°C for 20 minutes. The effectiveness of the solvents was evaluated by visual inspection of the number of particles located on the silicon wafer.

Measurement of the Pu content and isotopic composition of the individual particles was performed by ICPMS (Element II, Thermo Scientific). Individual particles were handled using a particle manipulator (Suruga Seiki, M331) attached to the microscope. Particles were transferred from the Al impactor foil directly into a pre-cleaned cryo vial and dissolved using 0.2 mL 78% HNO_3 (Baseline®, SEASTAR Chemicals, Canada) and 0.2 mL 45% HF (Baseline®, SEASTAR Chemicals, Canada). The solution was diluted with 2 mL high purity water prior to the ICP-MS measurements. All chemical treatments and instrumental measurements were carried out in ISO class 5 clean rooms. Direct measurements of particle size were performed using a SEM (FEI XL30, Phillips).

3. Results and Discussion

Bulk removal of particles from the Al impactor foil and generation of a suspension of Pu particles was studied using water, isopropanol, heptane and acetone. Acetone has proven to be most effective in removing particles from the Al impactor foil and producing a suspension with a sizeable number of distinct particles. Direct particle manipulation from Al impactor foil sector using a stainless steel needle and a micromanipulator allows easy removal and handling of discrete particles.

Individual particles from these experiments were analyzed for their size, Pu contents and isotopic composition. Table 1 summarizes the results obtained for the isotopic composition of 27 discrete PuO_2 particles. The isotopic composition of the generated particles agrees well with the certified values. Very small particles exhibit a larger variability in the isotopic composition attributable to the lower counting statistics for the individual Pu isotopes. No attempt was made to measure the ^{238}Pu by alpha spectrometry and the ^{242}Pu count rates were at or below the detection limit. The Pu concentration in these particles varies by two orders of magnitude between 0.1 and 10 pg with an average Pu content 3 of about 2 pg. Using a density for PuO_2 of 11.5 g/cm [3] we estimated the size of the particles assuming spherical geometry. Figure 2 shows the estimated size distribution of the Pu particles based on their Pu assay. It suggests that most particles removed from the impactor stage have a size between 0.4 µm and 0.8 µm. Four particles were directly measured for their size using a SEM (Figure 3). The diameter of the particles assuming spherical geometry was determined to be between 0.6 µm and 0.8 µm. Both estimates are in good agreement with the distribution obtained by Shinonaga et al. The larger number of apparently smaller particles with an estimated diameter between 0.4 µm and 0.6 µm might indicate that a larger fraction of generated particles has a density lower than the nominal value of 11.5 g/cm^3. Shinonaga et al. also found that the density of the two particles analysed is considerably lower (5 g/cm^3 – 9 g/cm^3) than the nominal density of PuO^2.

A select number of particles were manipulated and transferred onto a graphite sample holder, either as distinct particles or particle doubles, for further studies of their Pu and Am isotopic contents and their nominal ^{241}Pu-^{241}Am age.

No.	^{240}Pu/^{239}Pu [at/at]	σ	^{241}Pu/^{239}Pu [at/at]	σ	Total Pu (pg)
1	0.145	0.002	0.008	0.000	5.42
2	0.146	0.001	0.008	0.000	10.32
3	0.145	0.003	0.008	0.001	2.39
4	0.141	0.003	0.007	0.001	2.94
5	0.142	0.003	0.007	0.001	2.52
6	0.146	0.003	0.008	0.001	2.96
7	0.144	0.003	0.007	0.001	2.30
8	0.149	0.003	0.008	0.001	2.06
9	0.140	0.003	0.007	0.001	2.27
10	0.145	0.003	0.008	0.001	2.30
11	0.145	0.005	0.008	0.001	0.98
12	0.135	0.014	0.005	0.004	0.11
13	0.144	0.005	0.008	0.001	0.86
14	0.147	0.014	0.009	0.003	0.11
15	0.145	0.014	0.008	0.003	0.12
16	0.151	0.014	0.011	0.004	0.11
17	0.145	0.014	0.010	0.005	0.11
18	0.146	0.005	0.007	0.001	0.98
19	0.143	0.005	0.008	0.001	0.99
20	0.143	0.005	0.008	0.001	1.05
21	0.142	0.005	0.007	0.001	1.01
22	0.143	0.007	0.007	0.002	0.48
23	0.143	0.010	0.008	0.002	0.89
24	0.152	0.008	0.008	0.002	1.26
25	0.147	0.011	0.008	0.002	0.70
26	0.141	0.007	0.008	0.002	1.63
27	0.148	0.011	0.009	0.002	0.79
Cerified. Value	0.145	0.0002	0.0067	0.00002	

Table 1: Pu isotopic ratios and total Pu content in single particles measured by ICP-MS.

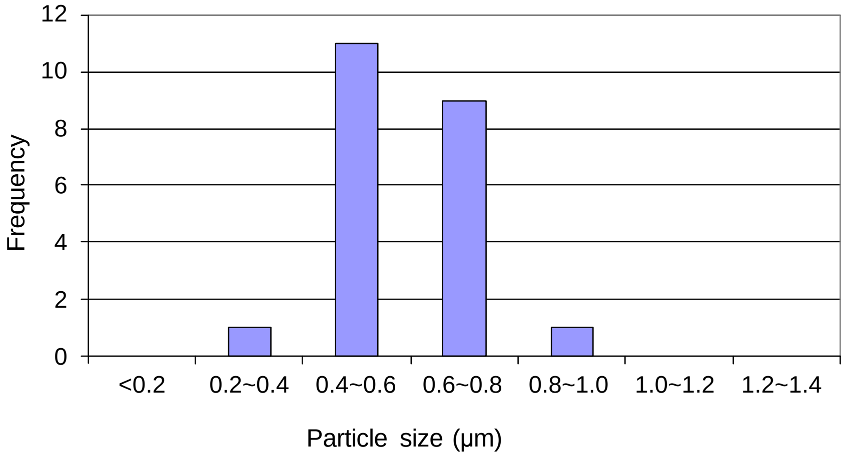


Figure 2: Size distribution of Pu particles.

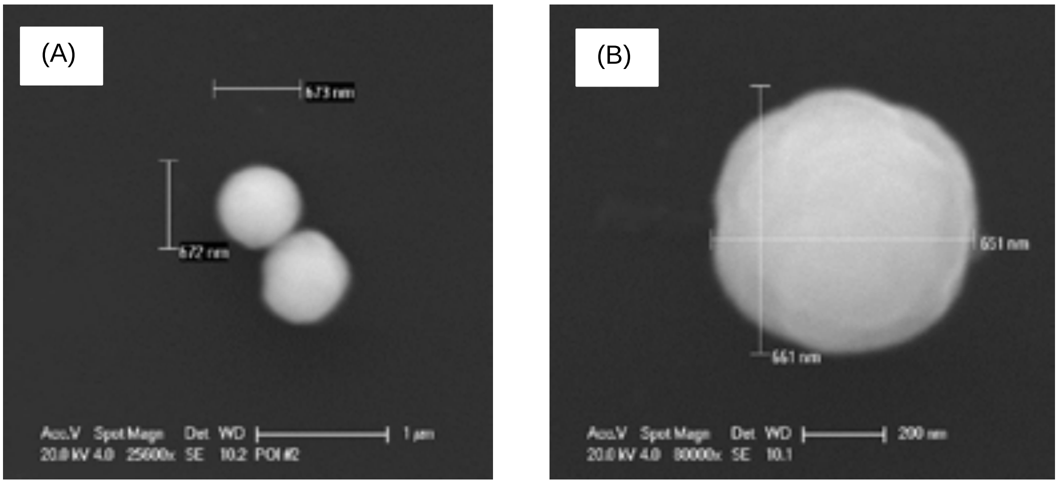


Figure 3: SEM images of a double Pu particles (A) and a single Pu particle (B).

4. Conclusions

Micrometer-sized Pu particles were produced in an aerosol generator (TSI 3076, TSI Inc.) and collected on Al impactor foils treated with Apiezon-L for efficient particle retention. An effective technique for particle removal from the Al impactor stage uses ultrasoneration in acetone and drying on an appropriate substrate such as a silicon wafer for further handling.

Individual particles from this experiment were handled using a micromanipulator in combination with a digital microscope and measured for their size, Pu content and isotopic composition.

The average size of particles determined from direct SEM measurements is 0.6 – 0.8 μm. The size of Pu particles calculated from their Pu assay (0.1 pg to 10 pg) and assuming spherical geometry and a 3 PuO_2 density of 11.5 g/cm ranges between 0.4 μm and 0.8 μm. This suggests that a larger fraction of the generated particles did not reach the nominal density of PuO_2 in agreement with the initial characterization. The isotopic ratios of $^{240}Pu/^{239}Pu$ and $^{241}Pu/^{239}Pu$ are in good agreement with previous measurements and the certified values from the certificate of CRM 136.

5. References

[1] Production of Plutonium Particles; VTT-R-03896-11; Helsinki; September; 2011.

[2] Shinonaga T; Donohue D; Aigner H; Bürger S; Klose D; Kärkelä T; Zilliacus R; Auvinen A; Marie O; Pointurier F; *Production and Characterization of Plutonium Dioxide Particles as Quality Control Material for Safeguards Purposes*; Anal Chem.; 84(6); 2012; p 2638~2646.

[3] Reshetnikov F G; Bibilashvili Yu K; Golovnin I S; Énergoatomizdat; Moscow; 250–265; 1973, p 38–40.

Conclusions of the ESARDA Joint meeting on IAEA's State-Level Concept

European Commission Joint Research Centre, ITU Ispra, Italy (November 12, 2013)

F. Sevini[1], A. Vincze[2], I. Niemeyer[3], K. van der Meer[4]

[1] Chair of the Export Control WG,
[2] Chair of the Implementation of Safeguards WG,
[3] Past Chair of the Verification Technologies and Methodologies WG,
[4] President of ESARDA

1. Introduction

The IS, VTM and EXP ESARDA Working Groups invited the IAEA, EURATOM and all interested safeguards actors to review and discuss on the State-Level Concept in the context of the Additional Protocol. The meeting took place at European Commission JRC ITU in Ispra, Italy on November 12, 2013. It followed the similar initiative of the 2012 INMM Workshop held at the University of Virginia with elaboration of case studies enabled participants to better understand several aspects of the SLC.

The SLC topic is grounded on the IAEA's combination of "classical" integrated safeguards inspections with the results of other sources of information and analyses, in order to draw conclusions on the absence of undeclared nuclear activities. These sources include satellite imagery, environmental analysis, acquisition pathway analysis, export declarations of Trigger List items (AP Annex II) and others.

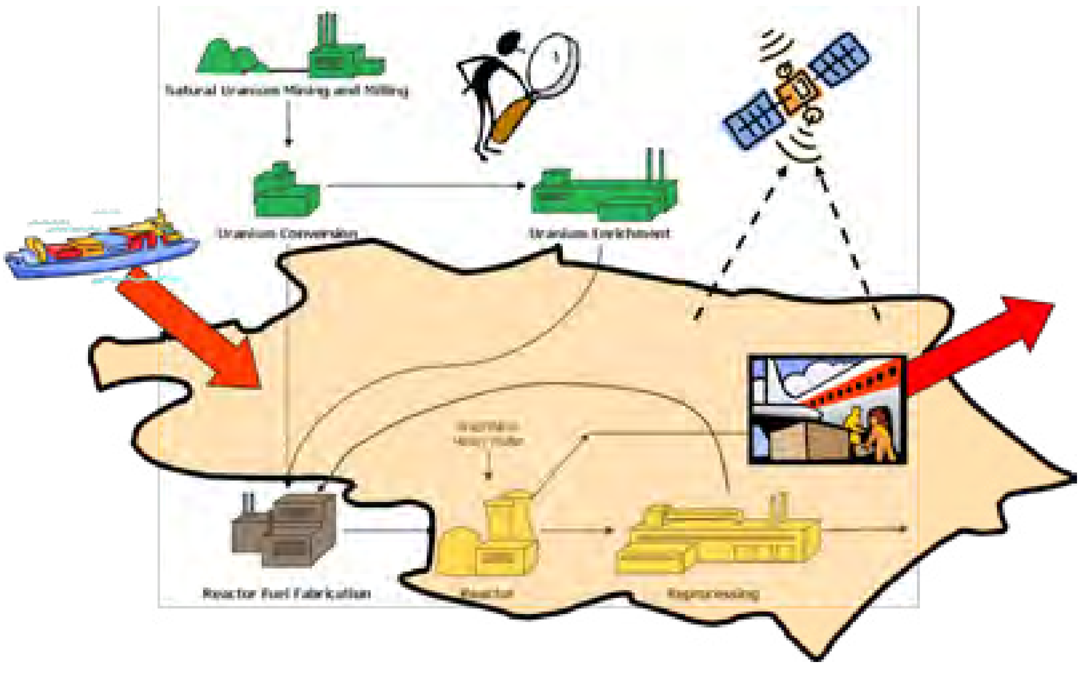
This synergy of inputs create a strong link among the three ESARDA research areas that organised the event; three dedicated topical sessions and a panel discussion tried to identify subjects meriting further attention and focus in the interest of improved and more effective conclusions on the absence of undeclared activities.

2. Contents

The IAEA, represented by J. Cooley, Director of Concepts and Planning division, Department of Safeguards, provided an extensive overview of the SLC motivations, framework and results.

EURATOM, represented by W. Kahnmeyer of Commission DG ENERGY, recalled the EU views and contributions to the IAEA SLC.

The Working Groups' technical sessions that followed underlined ESARDA's various research activities in support of



a better understanding and improvement of the State Level Concept.

The Integrated Safeguards session reported that a comparison of the inspection effort in nuclear facilities in the EC countries before and after the introduction of Integrated Safeguards showed a general decrease of the resources needed, although differences are observed per type of facility and per country. The role of a Regional System of Accountancy and Control in the SLC, and specifically the role of EURATOM being the most developed RSAC, will be subject for further research and discussion within ESARDA.

The export control session recalled that IAEA's safeguards do not impose export controls, but benefit from their existence. As required by AP Art. 2.a.IX, States are due to submit information to the IAEA about exports of nuclear Trigger List items (Annex II); ad-hoc confirmation of imports can be requested from recipient States, to match the figures. Additionally the IAEA has agreements with some States to exchange also information about refused export control licenses. This is possible thank to the compliance efforts made by nuclear exporters. The session debated about the AP Annex II list largely outdated in comparison to the continuous evolution of technical developments and Nuclear Suppliers Group control lists and the suggestions for possible improvements, including software, technology and nuclear dual-use controls.

The activities of the VTM Working Group focus on specific techniques, like geospatial information systems and mathematical models, in support of the SLC, but have also a more conceptual direction with substantial efforts in discussing and further elaboration of acquisition path analysis concepts and performance targets, which are indispensable for a State-specific approach. Case studies turned out to be a helpful tool to gain better understanding and confidence.

ESARDA has offered the IAEA to organise a similar workshop to explore this further in depth and plans also to organize again joint meetings on the topic.

3. References

The full paper is available on www.esarda.eu.

Report of the ESARDA Training and Knowledge Management (TKM) WG activities

P. Peerani

In 2014 the major achievement of the **Training and Knowledge Management** (TKM) working group has been the organization of the ESARDA Course on Nuclear Safeguards and Non-Proliferation. The 12th edition was held in Ispra on March 31st to April 4th 2014 and has been attended by 59 participants from universities, industry, national authorities and international organisations.

The course has then been duplicated, thanks to a funding provided by the EC's DG DEVCO, for the Asian region. The 13th ESARDA course was held in Bangkok on October 6th-10th with 41 participants from 11 countries of South-East Asia.

The TKM working group has also started the process of revision of the course syllabus. The syllabus, used mostly as textbook for the course, was published in his first edition in December 2008; after 8 years, it is maybe time for an update. During the 36th Annual Meeting in Luxemburg last May, the TKM has called publicly for the support of all the other working groups in the process of revision that will bring to the issue of a second edition within the next year. The scope of the revision is to update the existing parts, adding the new concepts and technologies introduced in the recent years and to complement with some topics that were missing in the first edition.

Moreover the TKM working group has started to go beyond the step of providing directly education in nuclear safeguards through the ESARDA course and fostering a sort of capacity building in the universities for teaching these topics. The idea is to prepare packages of teaching modules (including lectures in form of presentations, textbook and other support didactic material (such as reference documents, exercises, audiovisuals etc.). These modules could be made available to universities that wish to use it for its internal curricula. Once the material will be available, the transfer of knowledge will be done through train-the-trainer courses to form the professors. The concept of this process has been described in a strategic vision paper, developed by the Swedish members of the WG and endorsed by the entire WG, and is published hereafter in this Bulletin.

Reference: https://esarda.jrc.ec.europa.eu

Visions for the development of ESARDA and ESARDA TKM WG

Sophie Grape[1], Karin Persson[1] and Thomas Jonter[2]

[1] Uppsala University, Sweden
[1] Stockholm University, Sweden

1. Introduction

1.1 Background

The ESARDA Training and Knowledge Management Working Group (ESARDA TKM WG) is one of several working groups in the ESARDA organization. The primary objective of this group has been to offer the ESARDA nuclear safeguards and non-proliferation course to students and young professionals at least once per year. Each time, around 50 students and young professionals with both a technical and non-technical background are accepted to the course, which is free of cost for the participants. A dedicated text book, published in 2008, is given to the course participants.

1.2 Motivation for exploring new possibilities

At several occasions, the TKM WG has brought up several topics that are of relevance for the future development of ESARDA, such as:

- *How can we* collaborate with other institutions offering nuclear safeguards teaching?
- In order to reach out and attract attention to the nuclear safeguards and non-proliferation field we need to attract students and academia. *How do we* do that?
- *How can we* further develop the successful ESARDA nuclear safeguards and non-proliferation course?
- *How shall we* deal with knowledge management internally within ESARDA and how do we teach knowledge management?

We need to continue the discussion on these topics, with the goal in mind to come up with ideas on:

1. How to expose a larger fraction of nuclear engineering students to nuclear safeguards and nonproliferation? The goal is that all nuclear engineering students in Europe should be exposed to these subjects.
2. How to involve the TKM WG in practical knowledge management issues, not only (one) training (activity).
3. How to integrate the activities of the TKM WG with the other ESARDA working groups, in order to improve the sharing, learning and knowledge management of the ESARDA expertise.

This vision is about how the TKM WG could be developed to manage the ESARDA knowledge in a more effective way.

2. Presentation of the vision

In order to meet the wishes and needs mentioned in the introduction above, we suggest a new way for ESARDA to handle training and knowledge management within the nuclear safeguards and non-proliferation field. These ideas are presented in Figure 1.

2.1 Development and description of the module based training packages

Each module is meant to be a comprehensive collection of material sufficient to teach students about that particular subject. The subject could be of technical as well as non-technical nature, but should be of relevance to ESARDA or to a specific ESARDA working group such as e.g. non-destructive assay (NDA), destructive assay (DA) and knowledge management (KM) in practice.

Modules that do not correspond directly to the existing ESARDA WGs, but are related to ESARDA as a whole, could concern e.g. general information about non-proliferation (NP), safeguards for geological repositories, nuclear safeguards laboratories etc. The inclusion of additional modules which are not explicitly part of research on nuclear safeguards and non-proliferation such as e.g. nuclear security could be encouraged, assuming that the topic is considered to be of importance to ESARDA. Such topics could become part of the work within one existing WG or constitute a WG on its own, and the development of the module then becomes the responsibility of that particular WG.

As mentioned, the modules should be developed by primarily experts within the ESARDA working groups. It is however also possible for partners such as research institutes, universities etc to either collect material that they already have available and make it accessible to the TKM working group in the form of modules (as indicated by the single sided arrows in Figure 1) assuming that this partner has the interest, time and financial resources. In the more distant future, this could lead to an exchange of modules between several partners, and the latest research and "new" experts could be invited to present material at e.g. the ESARDA course (as indicated by the double sided arrows in Figure 1). If possible, resources earlier made available to publish the ESARDA course book could be made available to external authors.

Note that the job of ESARDA TKM WG should not be to develop modules on their own, but to *manage the knowledge within the ESARDA* organization as a whole and to coordinate, manage, select and quality control the content of the modules and as well to offer the ESARDA courses. The TKM WG should also define the minimum content necessary to label the course an "ESARDA course".

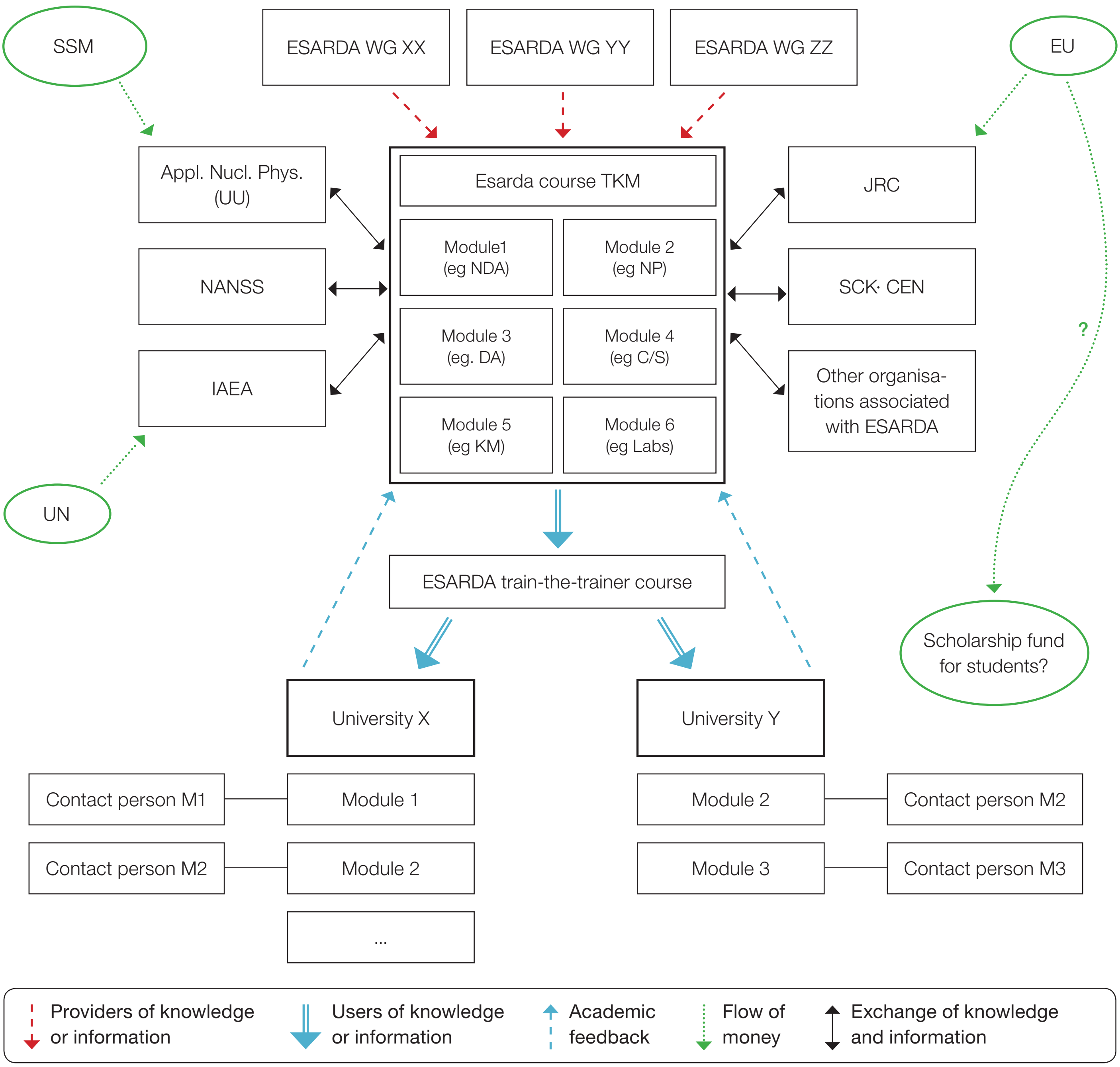
2.2 The use of the module based training packages

We suggest that a *module based training package* should be designed and made available by ESARDA. In this module based training package, a number of modules can be combined to suit different audiences with different needs.

The actual content of each module could be e.g. one or several texts, e-books, case studies, further references, video material etc. The course material should be kept in an electronic format which is easy to update, edit and "keep alive" and for each course opportunity, the course participants should be given access to the selected modules in order to be able to download them.

We have identified three possible uses for the module based training packages. They are:

1. To offer variations of the ESARDA course to (young) professionals
   A number of modules could be combined in order to*offer the ESARDA course, but with different "flavors"* depending on who is organizing it and who the target group is. Hence, one could select certain modules for



a less technical course, other modules for a more technical course and yet another mix of modules for a course with special emphasis on experimental safeguards activities etc.

2. To offer train-the-trainer courses
   We have identified a need to develop a *train-the-trainers course* in order to support university education in the basics of nuclear safeguards and non-proliferation (with an "ESARDA classified course"). We believe that the focus of this course should be to educate the lecturers about the technical content of the nuclear safeguards and nonproliferation subjects and not only present them with an overview. We leave it open for discussion to determine whether there should be only one train-the-trainer course, or whether we also here should define a "core course" with optional course to add on. There are several organizations that could deliver examples and best-practise guides on how to develop train-the-trainers courses in practice; this should be investigated further.

3. To access nuclear engineering students in academia
   Once the university teachers themselves have taken the ESARDA train-the-trainers course, *the modules can be made accessible to his/hers students*. The responsible teacher may in collaboration with the TKM WG select modules that are suitable for particular academic course. This bullet is further described in section 2.3 below.

2.3 Teaching nuclear safeguards at European universities

The lower part of Figure 1 is the most important one; it explains how the ESARDA TKM WG may reach the goal of spreading nuclear safeguards and non-proliferation knowledge and awareness to a much larger target group than today. We believe that the way to do this is through offering these modules to universities, where nuclear safeguard knowledge may be offered to a large selection of students in multiple countries at several occasions every year. In this case, we talk about an additional way for the ESARDA to offer teaching and mentoring and to attracting young people to the field. These people are active in academic universities and that is where we need to go.

In order to make it attractive for university teachers to teach nuclear safeguards (even if they are not themselves familiar with the subject), we need to reach out to universities currently teaching e.g. nuclear engineering programs or courses. In addition to inviting the teachers to take the ESARDA train-the-trainers course, we should make the training packages available to the teachers and in addition offer a personal contact who can aid the teachers with technical advice, additional information, clarifications etc. We suggest that one contact person or mentor is associated with each module. This mentor can, but must not necessarily, be the author of the module; another option is to use knowledgeable ESARDA WG members who are familiar with the content of the module. It is important to stress that this mentorship is meant to be time limited, associated with contact over email/phone/similar (but not necessarily in-person-contact) and that the work load should be distributed over several people in order not to constitute too much of a burden.

2.4 Keeping the motivation among students in the long run

In the long run, ESARDA wishes for more students to get professionally involved in nuclear safeguards and non-proliferation activities. We hope to achieve that through making the NuSaSET portal available to students who have participated in the ESARDA nuclear safeguards university module courses. Through this portal they come into contact with professionals in the field and companies actively working with these issues. This will be an excellent platform for advertising master thesis projects, project works, summer jobs etc to our target group, as well as to stay in contact with students who have undergone nuclear safeguards teaching as well as teachers who have undergone the train-the-trainer course via an "alumni group". We believe that this would be an excellent way to strengthen the connection to the lecturers and researchers at the universities and to the young promising and motivated students.

2.5 Scholarship fund

We also propose that ESARDA should create a scholarship fund (is it possible to create this from EU funds that go to the research center?) for students who have completed bachelor/master theses or project reports related to nuclear safeguards and non-proliferation, to enable participation and presentation of their work at ESARDA symposia. In this way, everyone who is engaged in ESARDA has the opportunity and responsibility to try and keep these people in our field also after their graduation.

3. Conclusion

In this document, we have described a vision of how the ESARDA WG could deal with both training and knowledge management in a more effective way by collaborating with other ESARDA working groups. We have also described how module based training package system could facilitate a larger spread of nuclear safeguards and non-proliferation knowledge to academia. This will, at the same time, make the ESARDA education more flexible and give possibilities to offer different courses depending on various needs and target groups for each individual course. We also suggest that a TKM should take steps to develop a train-the-trainer course in order to stimulate further interest in academia for teaching in the safeguards and nuclear non-proliferation field.

Reference: https://esarda.jrc.ec.europa.eu

Report on the ESARDA Implementation of Safeguards Working Group Activities

Arpad Vincze, IS WG Chair

The objective of the IS WG is to provide the Safeguards Community with proposals and expert advice on the implementation of safeguards concepts, methodologies and approaches aiming at enhancing the effectiveness and efficiency of safeguards on all levels and serve as a forum for exchange of information and experiences on safeguards implementation. One of the unique feature of the group is that its members and observers are coming from 19 countries (Austria, Belgium, Czech Republic, Estonia, Finland, France, Germany, Hungary, Italy, Lithuania, Netherlands, Norway, Poland, Slovak Republic, Spain, Sweden, Switzerland, UK, US), European Commission Directorate-General for Energy - "Nuclear Safeguards", research organizations and operators.

In 2013 the working group organized three well attended meetings with 20-30 participants. The first meeting was held in April in Bergen, Norway and the second in November in ISPRA, Italy, when the ESARDA Joint meeting on "IAEA State Level Concept" organized by ESARDA IS, EXP, VTM Working Groups was also included into the agenda.

A specific topic in all of our meetings is the information update on new developments and experiences of integrated safeguards implementation in the represented states and/or facilites. The information discussed in the course of these "round table updates" delivered by each member over many years in the WG meetings is of significant value, therefore the group decided already in 2012 to collect the information on history of and experiences during the implementation phases of the IAEA's Integrated Safeguards (IS) in a structured way, by means of specially developed State information sheets. In 2013 this information was used to compile a paper on the history of and experiences with the development and implementation of new concepts of Safeguards, in particular the IAEA's Integrated Safeguards (IS) in some European States represented in the IS WG. The resulting paper was presented during the 2013 ESARDA Symposium [1].

During the Bergen meeting in Norway representatives of the European Commission gave an overview of the Euratom and IAEA cooperation in the implementation of safeguards in the EU, whereby the actual state of the Subsidiary Arrangements and the Facility Attachments were discussed. The EC also presented the Euratom's approach to safeguarding final disposal facilities and the WG discussed its implementation aspects.

The group also had a session on Remote Data Transmission (RDT) implementation, where a presentation was made by the French representatives about RDT that is envisaged from AREVA NC La Hague reprocessing plant to Luxembourg and an overview was also given about the RDT implementation requirements in Germany. The representative of Sandia National Laboratories presented the details of the study conducted with JRC on the possibility of the implementation of secure branching in nuclear facilities and the related requirements for the different stakeholders. The working group gave feedback on the appropriateness of the high-level requirements for branching and gave its opinion about the most promising safeguards measurements and/or facilities where such a capability might best apply.

As a follow up on Safeguards Culture the WG agreed that training courses on safeguards at different levels of a facility would contribute to the safeguards culture of the facility. It was decided that a model training materials for the management, the general staff will be developed by a sub-working group.

During the second meeting in ISPRA the main activity of the working group was dedicated to the session of the Implementation of Safeguards WG as part of the ESARDA Joint meeting on "IAEA State Level Concept". The session highlighted that the IAEA's State Level Concept (IAEA SLC) is not new, but a result of a continuously evolving approach. It was also expressed that although there are many elements of the new IAEA SLC that can be identified in the IS-SLAs, this new concept can be regarded as a fundamental change from the "bottom-up" SLA based on facility level approaches, to the "top-down" SLA focusing primarily on the State as a whole. The driving force for the new approach is to have a more responsive system while maintaining or even increasing effectiveness and efficiency of the system. The problem of how to measure effectiveness and efficiency was also addressed in general and it was concluded that it would really be a difficult task to answer this question as far as the SLC is concerned. It is perhaps more appropriate to discuss the expectations for effectiveness and efficiency under the IAEA SLC. The most important expectations were proposed by one of the presentations. The main findings of the joint meeting are summarized separately in the present Bulletin [2] and the full report is available on the ESARDA website [3].

During the IPSRA meeting the chairmanships of the WG had to be changed, since the then vice-chair,Julie Oddou left the group due to her new appointment as IAEA Nuclear Counselor at the French Mission in Vienna. Mr. Romuald Bon Nguyen from IRSN was nominated and elected as the new vice-chair taking over the chairmanship of the group from 2015.

References

1. A. Vincze: "Experiences with the Development and Implementation of Integrated Safeguards (IS) in some European States", ESARDA Symposium 2013, 27-30 May, Brugge, Belgium

2. F. Sevini, A. Vincze, I. Niemeyer, K. van der Meer: Conclusions of the ESARDA Joint meeting on IAEA's State-Level Concept, ESARDA Bulletin.

3. www.esarda.eu

https://esarda.jrc.ec.europa.eu

Verification Technologies & Methodologies (VTM) WG

Activities 2013-2014

Irmgard Niemeyer, Former Chair VTM[1]
Erik Wolfart, Chair VTM, https://esarda.jrc.ec.europa.eu
[1] 07/2012-06/2014

The mission of the ESARDA Verification Technologies and Methodologies (VTM) Working Group is to provide the safeguards community with expert advice on modern verification technologies and methodologies The WG identifies, evaluates and promotes technologies and methodologies which may support nuclear or non-nuclear verification, identifies research areas for new verification technologies and methodologies and supports the establishment of research networks. The WG also acts as a forum for experts in different verification regimes for exchange of relevant information in this area on a regular basis.

The WG considers a wide variety of topics in principal. Topics range from general verification concepts, inspection models and the efficiency and effectiveness of verification regimes to information from open sources, geospatial information technologies, environmental monitoring and geophysical monitoring to surveillance and sealing systems and unattended monitoring. At the same time, the WG includes members and guests with various expertise and background from research centres and institutions (JRC ITU, SCK-CEN, Jülich, Fraunhofer INT, EU SatCen), US laboratories (SNL, LAN, LLNL, ORNL, PNNL), universities (Hamburg, Bonn, Uppsala, George Washington), international and regional organisations (IAEA, EURATOM, ABACC), national authorities and ministries (STUK, DoS, CNSC) and industry (Urenco, AWE, Sellafield Ltd., UBA GmbH, SDRI Consulting).

In the past two years, however, the WG focused on three topics: The State-level Concept, Arms Control and Disarmament Verification, and Geospatial Information Technologies, and a new book project.

1. State-level Concept (SLC)

VTM has worked on verification technologies and methodologies that can support the conceptualization and development of safeguards implementation at the State level. A number of examples were presented at the 2013 & 2014 ESARDA Annual Meetings, among others, on acquisition path analysis, GIS-based information management and integration, ontology-based semantic information technology, geology for the country report, societal verification, and the applicability of the State-level approaches (SLAs) to future arms control.

During the WG meetings in 2012-14, special focus was given to the acquisition path analysis (APA) methodology and the importance of case studies with regard to the development of State-level approaches.

Together with the IS and ExC WGs, an ESARDA Joint Meeting on the “IAEA State Level Concept” was held in November 2013 in Ispra.[1]

2. Arms Control and Disarmament Verification

Together with the German Network on Disarmament Verification[2] and ESARDA NA-NT WG, VTM has organised three special sessions at the ESARDA Annual Meeting in 2013 with reference to disarmament verification. First, a technical session including six papers from AWE, Universities of Darmstadt and Hamburg, LLNL, LANL and PNNL. The topics ranged from an introduction of concepts and measurements for plutonium mass determination to the development of the UKNI information barrier to the issue of transparency in simulations of measurements. Second, a panel discussion entitled “Disarmament Verification – A dialogue on technical and transparency challenges” was held with panellists from IFSH (Germany), VERTIC, LLNL, IFE (Norway), PRIF (Germany) and IAEA.[3]

3. Geospatial Information Technologies

Some VTM partners (Jülich, JRC ITU, CEA, EU SatCen) have contributed to the FP7 Collaborative Project GMES SEXTANT (Service Provision of Geospatial Intelligence in EU External Actions Support) from January 2013[4]. G-SEXTANT contains a work package entitled “Nuclear activities scenario”, led by Jülich, which aims at providing tools in support of monitoring nuclear-related sites and activities using satellite imagery. The activities of the work package are grouped into two sub-scenarios, namely “Monitoring

[1] See Report “Conclusions of the ESARDA Joint meeting on IAEA’s State-Level Concept on in this issue.
[2] See http://www.disarmament-verification.org
[3] See Report in ESARDA Bulletin 50 (2013), 124f.
[4] Niemeyer, I., Listner, C., Canty, M.J., Wolfart, E. & J.-M. Lagrange (2014): Integrated Analysis of Satellite Imagery for Nuclear Monitoring - Results from G-SEXTANT. In: Proc. INMM 55th Annual Meeting, Atlanta, 21-24 July 2014.

of nuclear decommissioning activities" and "Monitoring of nuclear activities in the context of the Nuclear Non-Proliferation Treaty (NPT)". IAEA/SGIM has joined G-SEXTANT as user.

The same VTM partners were founding members of the INMM WG Open Source/Geospatial Information (OSI) in 2012 and have contributed to OSI WG activities since then, e.g. by organising a special session (together with the INMM Technical Divisions "International Safeguards" and "Nonproliferation and Arms Control") at the INMM Annual Meeting 2013.

4. Book project

In the VTM WG meeting o in October 2012, a proposal was made by Nicholas Kyriakopoulos, The George Washington University, to work on a new book project, following the previous "VTM book" issued by Rudolf Avenhaus, Nicholas Kyriakopoulos, Michel Richard and Gotthard Stein in 2006.[5] This proposal has been further advanced by Mona Dreicer (LLNL), Gotthard Stein (Consultant) and Irmgard Niemeyer (Jülich). Based on two papers presented at ESARDA 2013 and INMM 2014 about the application of state-level approaches to arms control verification, the aim of the book is to further advance this concept from the methodological and technological perspectives and to show its applicability to (future) arms control agreements based on case studies.

The editors plan to hold two workshops on the application of the SLC to (future) (nuclear) non-proliferation and arms control. The first workshop will focus on SLC methods, such as pathway analysis, and their adaption to one or two simple non-safeguards verification cases. It has been scheduled in conjunction with the next VTM WG Meeting in Ispra on Nov 19/20, 2014.

5. Acknowledgements

The authors would like to thank all VTM members and guests for their interest, contributions and support.

Reference: https://esarda.jrc.ec.europa.eu

5 Avenhaus, R., Kyriakopoulos, N., Richard M. & G. Stein (Eds.) (2006): Verifying Treaty Compliance. Limiting Weapons of Mass Destruction and Monitoring Kyoto Protocol Provisions. Springer, Berlin.

Report on the ESARDA Novel Approaches and Novel Technologies (NA/NT) WG activities

Antonin Vacheret

1. Summary of NA/NT group

The NA/NT WG was established in 2010 to provide expert advice and assistance to international inspectorates on novel approaches and technologies in support of treaty verification implementation. It currently comprises over 90 members, including representatives from the IAEA, Euratom, the Comprehensive Test Ban Treaty Organization (CTBTO) and the Office for the Prevention of Chemical Weapons (OPCW). The NA/NT WG collaborates with other ESARDA WGs in joint scientific sessions on topics of common, or related, interest.

This year, the ESARDA working group for Novel Approaches and Novel Technologies (NA/NT) has identified several emerging technologies with potential use for safeguards. The technological readiness level of these technologies is low and considerable R&D are required before they are mature enough for routine inspections. Recently the working group has considered three scientific areas or applications in more detail: optics, antineutrinos and arms control verification technologies (ACVT).

2. Meeting 26th-27th March 2014 at the University of Oxford

The workshop covered various topics, inter alia, anti-neutrino detection systems, new neutron detectors, safeguards R&D programmes, non-proliferation, treaty verification, arms control and advances in simulations, nuclear data and novel measurement methods. Optical measurement didn't make it as part of the final agenda this time.

The antineutrino measurements have a close linkage to the development of new types of neutron detectors which are also the key technology in nuclear security. Therefore, regardless the application, it was natural to arrange a joint meeting with scientists working with neutron detection. It is envisaged that both groups will benefit from the understanding of the technological development in a broader scale.

Besides nuclear sciences, NA/NT often refers to other disciplines. The aim is to promote scientific research and development on methods and techniques for safeguards and nuclear security. Scientific meetings, such as the one in Oxford University, are important for information sharing and understanding the progress in the development of different detection technologies. The meeting in Oxford provided invaluable contacts and feedback to carry on scientific work towards various in-field applications.

3. ACVT activities

The sub-working group on Arms Control and Verification Technologies (ACVT) had a parallel meeting also in Oxford on the 26th March 2014. The meeting reviewed the current arms control research in the UK and the need for contributions from the wider community in order to achieve challenge of an effective weapon dismantlement verification regime. Current methods to detect the presence of fissile materials for dismantlement verification and the need for incorporating information barrier to balance secrecy and transparency was also presented. A compendium of technology is also being pursued to support the verification effort and its current status was also presented at the meeting. These data sheets would give the instrument capabilities and limitations for assumed typical scenario. Details of the work has been recently published in the ESARDA bulletin*.

**New Approaches and New Technologies for the Verification of Nuclear Disarmament*, D Keir, pp 106-115 ESARDA BULLETIN, No. 50, Dec. 2013

Presently, and also in the future, NA/NT will aim at providing expert advice and assistance to international nuclear inspectorates on novel approaches and technologies which have the potential to improve safeguards and nuclear security. Technical methods to verify international treaties, present or future, involving nuclear disarmament, arms control and non-proliferation are an important field of work.

Reference: https://esarda.jrc.ec.europa.eu

ESARDA Symposium 2015
37th Annual Meeting 19 - 21 May 2015, Manchester (UK)
on Safeguards and Nuclear Non-Proliferation

Registration opens 1 December 2014
http://esarda.jrc.ec.europa.eu/

ESARDA in partnership with National Nuclear Laboratory (NNL) would like to invite you to join them at the 37th ESARDA Annual Symposium, 19 - 21 May 2015, at the Midland Hotel, Peter Street, Manchester, United Kingdom.

The symposium will be an opportunity for research organisations, safeguards authorities and nuclear plant operators to exchange information on new aspects of international safeguards and non-proliferation, as well as recent developments in nuclear safeguards and non-proliferation related research activities and their implications for the safeguards community. The Symposium will be preceded by meetings of the ESARDA Working Groups, on 18 May 2015.

Further details about abstract submissions, registration and agenda can be found at http://esarda.jrc.ec.europa.eu/

LB-AB-14-051-EN-N

https://esarda.jrc.ec.europa.eu