# Passive Noise Analysis Studies on Tampering Indication

## INMM 56th Annual Meeting

Ben Baker, Jeff Sanders, Mark Schanfein, John Svoboda, James West

July 2015

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

56th Annual INMM Meeting

# Passive Noise Analysis Studies on Tampering Indication

Ben Baker[1], Jeff Sanders[1], Mark Schanfein[2], John Svoboda[3], James West[1]

[1]Idaho National Laboratory
P.O. Box 1625 Idaho Falls, Idaho 83415

[2]Pacific Northwest National Laboratory
902 Battelle Boulevard, Richland, WA 99354

[3]Private Contractor
Idaho Falls, Idaho

ABSTRACT - Idaho National Laboratory (INL) is part of a multi-laboratory research project tasked with investigating methods for detection of tampering on unattended/remotely monitored systems (UMS) in International Atomic Energy Agency (IAEA) installations. Ensuring that the detector signals received at the IAEA cabinet are authentic is central to the independence of IAEA's safeguards conclusions. INL is investigating a passive noise analysis technique in the frequency domain to detect tampering. Prior work performed by INL showed a proof-of-principle method in which changes in ambient conditions could be observed in the frequency spectrum. In this paper several new findings, as well as further investigation into prior findings used for tamper indication, will be presented. Information from various parts of the spectrum and the whole spectrum can be used to determine temperature changes, modifications made to a pre-amplifier/amplifier or the replacement, changes to the neutron detector, replacement of the transmission cable, tapping into the cable and teeing off the signal from the cable. Future work will investigate the viability of these indicators to detect tampering for normal operation, noisy environments and real world applications.

**Key Words**
Noise analysis; safeguards; tamper detection; transducer monitoring

## INTRODUCTION

Many of the facilities monitored by the International Atomic Energy Agency (IAEA) incorporate unattended/remotely monitored systems (UMS) using radiation sensors[1]. The cabling for these detection systems can have cable lengths of 50 m or more throughout a facility, thus making visual inspection and traditional data security measures, such as a tamper proof conduit, impractical. Further, some of the sensors are rarely inspected because these are located in places with high radiation environments. The data from these sensors are therefore at risk of tampering. INL is part of a multi-laboratory research project that aims at developing a solution to the cable and sensor vulnerabilities posed by these systems. Pacific Northwest National Laboratory (PNNL) is investigating Time-Domain Reflectometry and Los Alamos National Laboratory (LANL) is investigating pulse-by-pulse analysis and correction of signal integrity. The INL approach is a passive technique that observes the voltage on a cable, performs a Fourier Transform to obtain a frequency spectrum, and compares the obtained spectrum with a baseline spectrum for authentication. The voltage on the line can be separated to develop a spectrum due to the pulses and another spectrum for the noise. Besides the tampering event, the spectra can

[1] Of the 153 IAEA UMS operating in 2014, 128 were radiation based systems

also provide useful information such as environmental conditions [1]. This paper is a continuation of prior work and will explain the affects that can be observed on a spectrum when changes are made to the pre-amplifier/amplifier, neutron detector, switching of cables, tapping or teeing off the signal from the cable and temperature. This work was supported by the Department of Energy National Nuclear Security Administration (NNSA) Next Generation Safeguards Initiative (NGSI).

## EXPERIMENT EQUIPMENT

The findings presented for this paper were performed on the PRE-100A preamplifiers from BOT Engineering and use LND Inc. model #25288 $^3$He detectors. Two digitizer/data acquisition systems were used in this research. The first data acquisition was custom built by INL and generates a spectrum that is limited to the ~100-500kHz range. The second digitizer was an FPGA based bench top system from National Instruments that has a sampling frequency of 800MHz. Thus, the first digitizer was used to obtain high frequency resolution for lower frequencies and the second digitizer was used to observe a more broad view of the spectrum up to several hundred MHz. A flow diagram for the system is shown below in Figure 1.

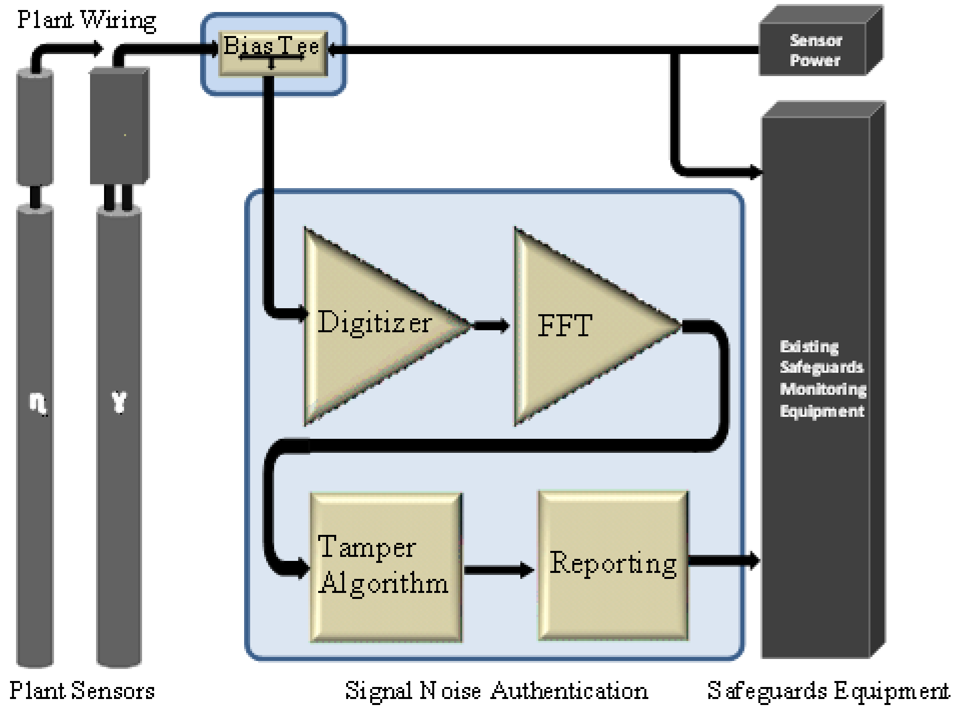

Figure 1: Passive Noise Analysis Flow Diagram

Further, experiments have been performed with the IRD-30A Si-PIN detector, IC-10 ion chamber (both from BOT Engineering), and the PDT 20A $^3$He detector. The BOT Engineering detectors were powered by the Next Generation Adam (NGAM); the PDT 20A was powered by the mini-GRAND module. The results from these systems were fairly similar to the PRE-100A system, and thus for the purpose of illustration, the PRE-100A will be the only sensor to be presented in depth in this paper. However, for the PDT 20A and IC-10 it was requisite to use a pci-U1071A digitizer from Keysight Technologies to obtain a better dynamic range than the National Instruments digitizer.

## RESEARCH STUDIES

Research studies were performed to determine if it was possible to detect tampering scenarios involving changes to the pre-amplifier, detector, swapping of cables, tapping into a cable and disconnecting a cable. As well, the root cause of the environmental changes observed from prior work was investigated further.

One way of establishing a metric for detecting differences in spectra was to measure the spectral energy and compare it with the baseline spectral energy. According to Parseval's Theorem, the energy of the signal can be calculated by summing the squares of magnitude of the Fourier Transform [2]. In other words, the energy contained in a frequency region is related to the sum of the spectral values. The energy figure of merit was used in each of the tampering scenarios to determine if the event could be detected. Further, the spectrum can be subdivided into zones and monitored for changes in the energy content. If any single zone produced results outside the typical energy range, a flag was raised indicating a tampering event.

### 1- Pre-amplifier

Two tests were performed on the PRE-100A pre-amplifier. The objective of the first test was to demonstrate the fact that no two pre-amplifiers can be completely identical, and the objective of the second was to adjust the gain on the pre-amplifier. The first tests obtained spectra from five PRE-100A pre-amplifiers; four pre-amplifiers came from the same batch and one came from a separate batch. Out of these five pre-amplifiers, three had fairly similar spectra, and two were very different. It was possible to detect the difference between the three pre-amplifiers with similar spectra by observing the energy in the spectrum and comparing it with a baseline. The most prominent differences between pre-amplifiers were peak shifts and changes in the noise floor. The graph below (Figure 2) shows two spectrums that were very similar in shape but have obvious differences.

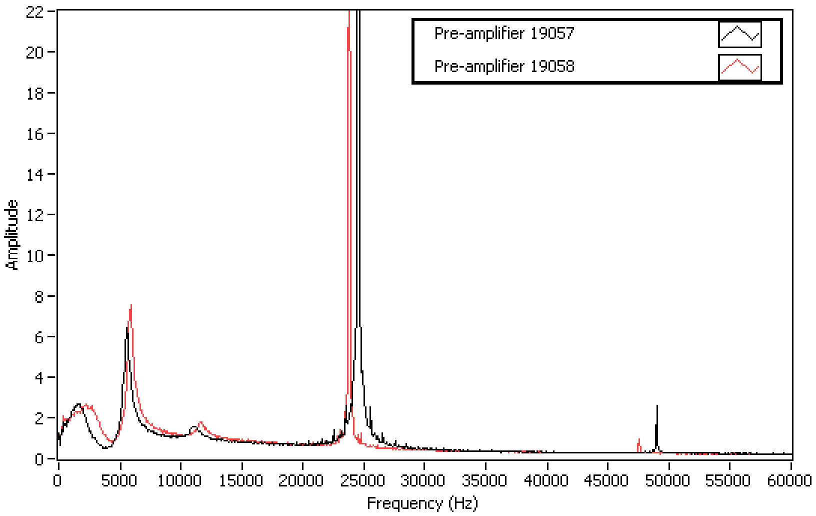

Figure 2: Two Pre-Amplifiers from the Same Manufacturing Batch

Figure 3 shows the absolute value of the change in energy of the entire spectrum from a reference when the pre-amplifier is switched with an identical pre-amplifier. Using the energy metric, it was also possible to show that one could detect a change to the gain of the pre-amplifier as well.

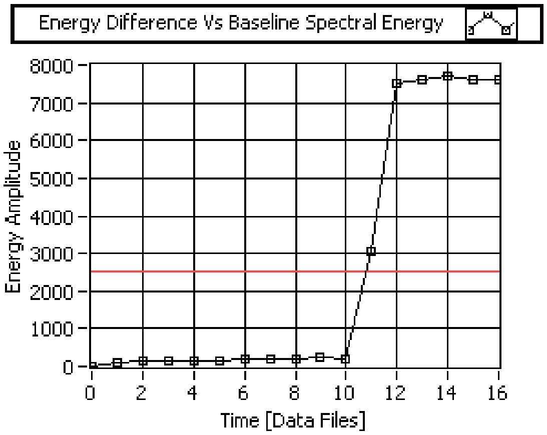

Figure 3: Typical Energy Difference Graph for Pre-Amplifier Swap

## 2- Detector

For the high speed digitizer, it was possible to differentiate the pulse spectrum from the noise spectrum. One study of swapping of the LND 25288 detector with the Reuter Stokes RS-P4-0812-124 detector displayed a major difference in the average pulse spectrum. The pulses from the Reuter Stokes detector tended to be smaller in amplitude and translated over to the frequency spectrum. Below is a graph (Figure 4) showing the spectra from both detectors. Further, it was possible to observe a change in the energy within the spectrum by ~2 times the baseline when the detector was simply removed. Unfortunately, for most experiments there was not much indication when a detector was swapped with an identical detector besides the time in which the detector was removed. There was one particular experiment when a detectable event occurred; however, it is believed that the detection energy was due to differences in radio-frequency (RF) pickup.

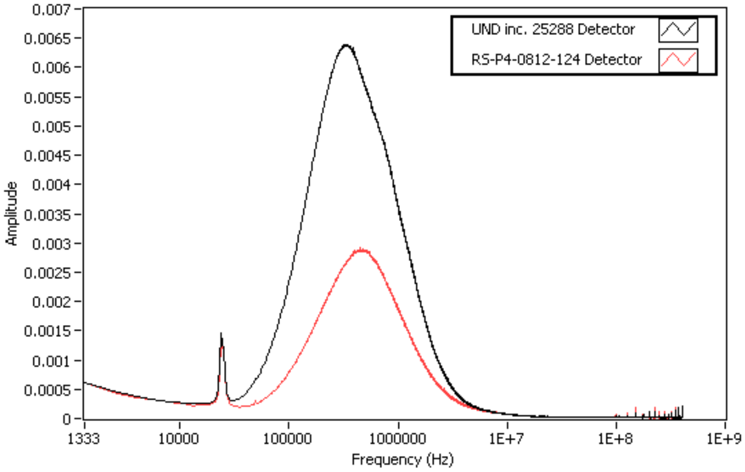

Figure 4: Spectral changes to the pulse spectrum when the detector is switched

## 3- Changing of Cables

Studies were performed to determine if modifications performed to the cables could be detected. These studies looked at identical cables, same cable type but lower attenuation factors, different cable types, and changes in cable length. It should be recognized that for any tampering event involving the changing of a cable, disconnect is required. For further details on disconnect, see section 5.

It was discovered that the key phenomenon for detecting a change to the cable was the attenuation coefficients. The attenuation to the energy on a cable is dependent on frequency, cable type (each has their own attenuation curve), and length. Thus, from observing the energy from a spectrum and comparing to a baseline, it was possible to detect many of the cable scenarios. Further, the detection was enhanced by subdividing the spectrum into zones and monitoring the energy fluctuation for each zone versus the baseline.

It was found that some identical cables had observable differences while others did not. It is believed that the observable differences were due to the cable responding slightly different to perturbing sources, such as radio waves or noise from electronics (i.e., RF pickup). Thus, one must conclude that identical cables might be detectable, but there is no guarantee.

To show that the attenuation coefficient had a major effect on the energy observed within a spectrum, a low loss cable for RG-174 was compared to a normal RG-174 cable. Thus, all other parameters, such as characteristic impedance, would be kept as constant as possible. This test showed that a change in the attenuation coefficient could be detected, but followed the attenuation verses frequency curve for the cable, with the general trend being little attenuation at low frequencies and a continual increase with frequency. For the two digitizers used (low and high frequencies), the energy within the spectra varied by 1.5 and 13.5 times the baseline energy value, respectively.

Further tests were performed by comparing the RG-174A/U cable against RG-62/U and RG-59/U cables. The results showed changes in the spectrum floor. The RG-62 and RG-59 cables have lower attenuation coefficients, and thus did not attenuate as much of the energy on the line as the RG-174 cable. Just like the low loss RG-174 cable, the energy differences between the RG-174, RG-62, and RG-59 cables followed their respective attenuation versus frequency curve. These differences were on the order of 28 to 34 times the baseline value for higher frequencies and from no detection to ~1.5 times the baseline region for low frequencies. Thus, the detectability is dependent on frequency and cable specifications.

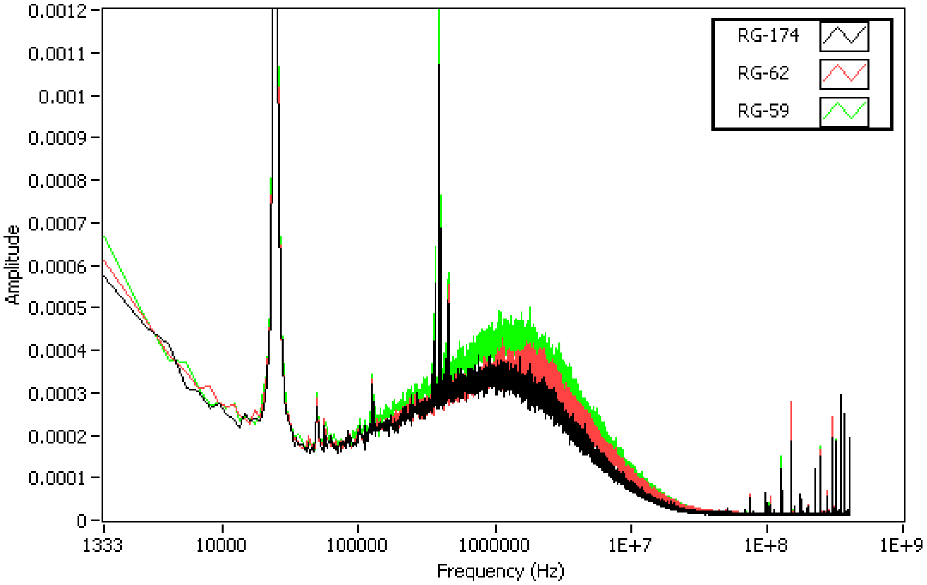

Figure 5: High frequency response for cables RG-174, RG-62, and RG-59 on 50 meter cables

Not only is the attenuation a function of frequency but it also is a function of length. The attenuation coefficients are often quoted in per unit length values. Thus, as the length increases so does the total attenuation (i.e., energy loss) to the signal. Two experiments were performed to determine the order of magnitude of attenuation that was required to be detected. For the high frequency data the absolute value of energy verses the baseline increased by 1.6 times with 1 meter of added length, which equates to 0.276 dB at 100MHz. However, this was not sufficient to trigger a tampering event. For the lower spectral frequencies, a detectable difference was observed with 22 meters of added length. For both of the cable addition scenarios, one must remember that while it may not be possible to detect the additional 1m cable, the adversary must first disconnect the cable which is a detectable event.

Each of these scenarios showed that it is possible to detect modifications to the cable type or length, independent of other affects such as disconnect that are prerequisite to these events.

## 4- Tapping into a cable (Cut in line & Tee connector)

The main scenario sequence for a tap/tee is for an adversary to cut into the cable or swap a barrel connector for a tee, and then attach a high impedance device to record the signal, and play it back with a low impedance signal generator. It is important to note that the data has not been compromised until the signal is played back on the line. Further, it is important to note that conventional techniques to play a signal back on a line require low impedance branching not high impedance.

For the experiments performed, none have been able to show that cutting into the cable have an inherent effect on the spectrum which is consistent with other references [3]. However, there was one experiment that was performed in which a noticeable change occurred, but it is believed to be due to extraneous effects, such as touching the shield and center wire at the same time or adding possible antennas by the use of metal tools to create the tap on the cable, since the detected event was not sustained over time. Further, there was no indication from any of the tests that could detect the difference between a barrel connector and a tee connector. However, one must account that disconnection of the cable must occur to make the switch (refer to section 5).

High frequency experiments showed that it was possible to detect a high impedance oscilloscope that might be listening to a cable. Another experiment was performed with a resister made to simulate a high impedance device to determine if the detection was due to the inherent impedance or the fact that the device has more components associated with it that might inject noise on the line. The individual resister was also detected but with less confidence than the addition of a device. Further testing will be performed with the component inside of an anechoic chamber to limit any antenna effects which might cause detection. Tests also showed that the addition of probes on the cable could be detected. The addition of a probe to the cable varied between 2.5 to 5 times the energy baseline values. Further, adding a high impedance device/component induced a change of an addition ~2.3 to 3.6 times the baseline, when the baseline includes the probe. These experiments were performed at 25m on a 50m cable. These values were also found to be dependent on the distance from the digitizer, with farther distances lowering the detectability. The baseline changes can be further increased by analyzing individual energy zones as illustrated below (Figure 6). From Figure 6 one can see the oscilloscope detection is ~9 times the baseline for energy zone 3 (12-156MHz) and 5.4 for the entire spectrum (0-400MHz). Further, there is no detection of the probe in zone 3, but is detected in other zones.

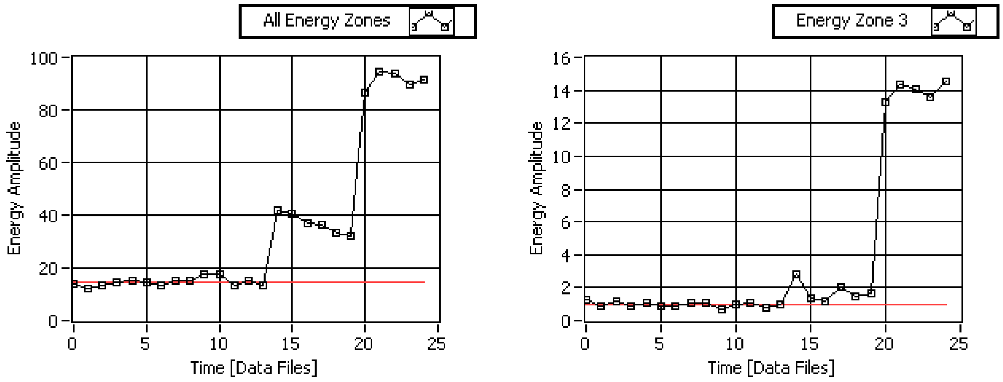

Figure 6: Attachment of a 10Mohms probe (Data File 14) and oscilloscope (Data File 20) at 25m on a 50m cable. (Left Graph: All Energy Zones, Right Graph: Energy Zone 3)

In order to play data back on a cable, a signal generator is normally used. Further, a majority of signal generators are low impedance devices (50 or 75 ohms) and differ from high impedance devices used to record signals (1x$10^7$ ohms). Tests were performed with adding a DC blocker on the cable so that cable terminators of 50-93 ohms could be added to the line (since the line is carrying 12V from the power supply and the added current trips the NGAM power supply). The DC blocker is merely a capacitor whose function is to decouple DC voltage (average voltage) from the AC signal or fluctuating parts of a signal. These cable terminators showed the inherent characteristics of low impedance devices. In every case it was possible to observe a distinct change in the signal energy for both low and high frequency regions. The variation was 2-4 times the baseline for low frequencies and 6-25 times the baseline for high frequencies. Further, it was possible to detect the addition of the DC blocker with the high frequency digitizer. The DC blocker would most likely be required by an adversary to playback the signal.

From these results, it is possible to detect an adversary listening to the signal on a cable and detect if the signal is being played back on the cable with several possible detection points along the path. Emphasis should be placed on detecting a signal being played back on the line, not detecting the signal being recorded, for the following reasons: 1) The data is never changed until the signal is played back; 2) A signal generator has a much higher chance of being detected; and 3) While it is possible to detect listening to a signal, it is not guaranteed, and for all intents and purposes, it is impossible to fully detect when there is listening on a line. If this were not true, encryption on secured networks in other industries would not be needed. In the case of UMS systems, it is not necessarily important to hide the signal contents from an adversary.

## 5- Disconnect

The majority of the cable tampering scenarios eventually involve a disconnection/full separation of the cable wire, if even for less than a second. Experiments were performed to determine how well and quickly a disconnection could be detected.

The results showed that a full disconnect changed the energy content by ~5 times the baseline for the low frequencies and ~50 times the baseline for high frequencies – more than enough of a change to detect any event. As for detection timing, the present systems were set at 0.2 seconds due to additional processing and wait times that were built into the program. However, the systems could be set to monitor continuously if a premium is applied to the detection of a disconnected cable.

It should be emphasized that disconnection of the cable is the most important tampering event because it is the single event that appears in almost every tampering scenario, and it is one of the most likely events to be detected.

## 6- Temperature

Aside from tampering scenarios, prior work showed that the environmental conditions had an effect on the noise spectrum [1]. It was believed that these environmental conditions could be used as indicators to validate that the data being received were authentic. Further tests were performed to clarify the source of the effects and the qualitative effect on a spectrum. An experiment was performed in which the noise spectrum was recorded over multiple days. Data from the air conditioning system were compared to the variation in the noise spectrum as compared to a baseline spectrum, and found to have the same variation. To determine if temperature or the mechanical system of the air conditioning system was the root cause, tests were performed in which the detector and pre-amplifier system were cooled by a refrigerator and heated with a heat gun. These tests showed that temperature caused the spectrum to shift frequencies in the region from 0 to ~1MHz with decreasing influence on the spectrum as frequencies increased. As the system was heated up, the frequencies would shift down and vice versa for cooling of the system. Frequencies above ~1MHz remained unaffected by temperature. The temperature effect is shown in the spectrum below in Figure 7.

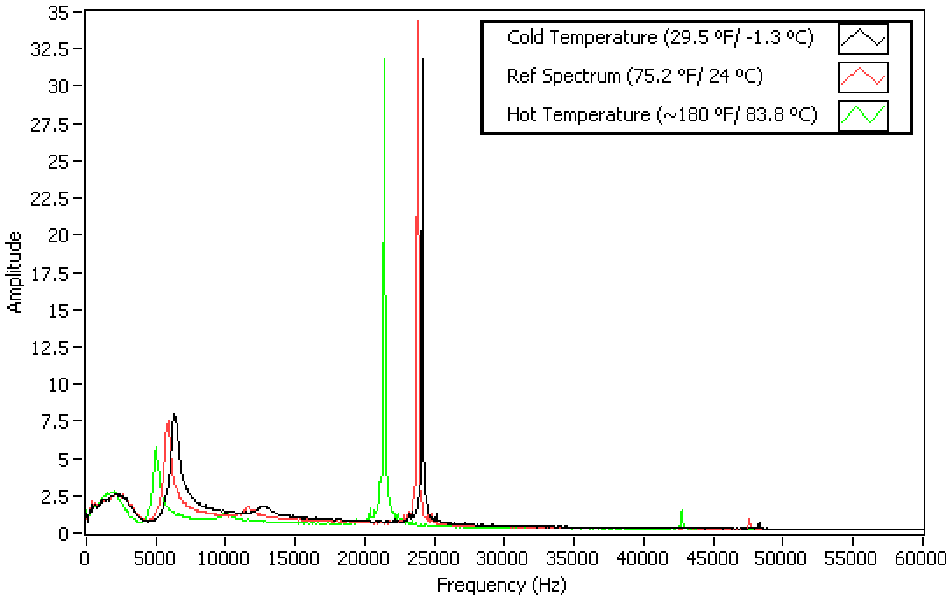

Figure 7: Temperature changes on a spectrum

## OTHER SYSTEMS and TEST CRITERIA

The IRD-30A (Si PIN), IC-10 (Ion Chamber), and PDT 20A ($^3$He) systems were also tested against the same scenarios as mentioned for the PRE-100A. Using the energy figure of merit, a program was devised to monitor the energy content with the spectrum broken up into zones. A fixed uncertainty was set for each zone based on a recording of the nominal variation. An event was considered detectable if the energy of the region fell outside the normal variation. A circular estimate of the uncertainty was used to allow the signal to slowly drift overtime to allow for temperature caused affects, such as the ventilation system turning on/off.

Each of these systems were fairly similar in outcome as the PRE-100A preamp. There were differences based on the functionality of the system, for instance the IC-10 and PDT 20A had much lower amounts of energy on the line than the IRD-30A and PRE-100A. The IC-10 and PDT 20A, on the other hand, had pulses that were invariant in shape and made the pulse spectrum more attractive than the IRD-30A and PRE-100A which produce pulses with a larger degree of variation in the shape. As a consequence of having lower energy on the line, the IC-10 and PDT 20A tampering events tended to produce results with lower changes from the baseline then those with more energy on the line.

In all, using either/or the noise and pulse spectra most of the tampering scenarios could be detected with the most critical (low impedance for playing a signal, disconnect, swapping of the preamplifier, and removal of the sensor) being detected. The only exception was the IC-10 and removal of the sensor. The IC-10 is unique in that it is converting the DC charge value from the detector into a pulse frequency proportional to the DC value. The arrangement makes it possible to remove the detector, and the IC-10 will continue to produce pulses every ½ second, indication it is on its lowest range (i.e., no charge on the line). However, a simple observation of the count rate would indicate the detector removal, since the chamber is meant to be in high radiation areas where a large change in count rate would be observed.

## CONCLUSIONS

The sensors and cables of unattended monitoring systems (UMS) in place by the IAEA continue to be at risk for data tampering. Experiments using spectral noise analysis, have been performed to demonstrate timely detection of tampering with sensor hardware and cabling. These experiments have shown that tampering with the sensor equipment and cables can be detected, with the most significant being a) removing/swapping the pre-amplifier and detector, b) recording and playing back a signal on a cable, and c) disconnecting the cable.

By monitoring the spectrum energy and energy within subdivisions of the spectrum for the pulse and noise spectra, it was possible to detect most of the tampering scenarios. The detected tampering events for hardware included swapping or removal of the pre-amplifier and sensor. The cable tampering scenarios showed that it was possible to detect differences in cable type, length, a high impedance device (i.e., recording the signal), low impedances (i.e., to playback the signal), other auxiliary attachments such as a DC block or probes, and the disconnection of the cable. Environmental effects were also shown to be caused by temperature and might have the possible application of further data authentication. It was shown that temperature causes fluctuations in the spectrum at frequencies less than ~1MHz with decreasing effect with increasing frequencies. The hardware and cable tampering experiments were also applied to four pre-amplifier systems and were found to have similar results.

Further work will focus on determining inherent system indication verses radio frequency (RF) pickup that lead to detection, assessing the thresholds necessary for real-world application and hardware requirements for a fully encompassing system. Additional tampering scenarios to be investigated may include the feasibility and detection of pulses placed on the cable through external electric, magnetic and RF fields which require no cuts to be made on the cable.

## REFERENCES

[1] Svoboda, J. and M. Schanfein, "Transducer Signal Noise Analysis for Sensor Authentication," INMM Proceedings, July 2012.
[2] Proakis J. and Manolakis D., Digital Signal Processing: Principles, Algorithms, and Applications, Pearson 4th Edition 2007.
[3] L. Griffiths, R. Parakh, C. Furse, B. Baker, "The Invisible Fray: A Critical Analysis of the Use of Reflectometry for Fray Location", IEEE Sensors Journal Vol 6., No. 3, June 2006.