INL/EXT-15-36437
Revision 0

Passive Noise Analysis for Advanced Tamper Indication: End of Year Report 2015

Benjamin Baker, Jeff Sanders, John Svoboda, James West

September 2015

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-15-36437
Revision 0

Passive Noise Analysis for Advanced Tamper Indication: End of Year Report 2015

**Benjamin Baker[1], Jeff Sanders[1],
John Svoboda[2] and James West[1]**

**1 – Idaho National Laboratory (Idaho Falls, ID USA)
2 – Contractor (Idaho Falls, ID USA)**

September 2015

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

http://www.inl.gov

**Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-94ID13223**

EXECUTIVE SUMMARY

Idaho National Laboratory (INL) is part of a multi-lab project assessing front-end electronics for unattended measurement (FEUM) being developed for the International Atomic Energy Agency (IAEA) unattended systems. The FEUM assessment project is funded by the Department of Energy (DOE)/National Nuclear Safeguards Administration (NNSA) Office of Nonproliferation and International Security and the Next Generation Safeguards Initiative (NGSI). The FEUM development activity provides an opportunity to address tampering detection between FEUM and the detector, signal integrity from FEUM to the data acquisition systems, and data validity – long-standing challenges for the IAEA. As part of the FEUM project, INL is investigating passive noise analysis as a tamper indicator based on proof-of-principle work performed by INL in prior years. This report summarizes the INL activities in Fiscal Year (FY) 2015 to characterize and test passive noise analysis as a potential tamper-indicating approach for implementation into FEUM or as a stand-alone method.

The project's primary objectives in FY-15 were to (1) determine detectable tamper scenarios, (2) perform tests of tampering scenarios with three common cable types used by the IAEA, (3) separate radio-frequency induced events from inherent effect by means of an anechoic chamber, and (4) perform tests at an industrial facility. Significant progress was achieved on each of these objectives, as summarized below:

1. Tampering experiments were performed using four pre-amplifier/detector systems. Each of the systems tested had a different ability to detect tampering, but tended to respond in a similar manner. Generally speaking, the systems could detect disconnect of the cable, presence of low impedance devices for playing back a signal, and the presence of high impedance devices for recording the signal. Many changes to cables including length, impedance, attenuation properties, and cable type could also be detected, as could removal of the detector and switching of the system hardware (i.e., pre-amplifier). The fundamental mechanism that changed the results between tested systems was the amount of energy in the signal.
2. Tampering experiments were performed for three cable types: RG-174, RG-62, and RG-71. These experiments included all four pre-amplifier/detector systems. The responses from these three cable types were fairly similar, with a few exceptions. The main difference between the cable types was the characteristic attenuation which is a function of frequency and length.
3. Anechoic chamber experiments were able to separate the tampering events based on the dominate effect being either inherent effects (i.e., physical attachment) or radio-frequency (RF) pickup. The majority of the tampering events were detected because of inherent effects. The experiments that were detected because of RF pickup differences were high impedance, identical cables, identical detectors, and supplemental hardware used in tampering events. Further, sources of peaks within the spectrum were identified.
4. Key tampering tests were performed in an industrial environment to determine if the detectability had changed.

From this testing, general conclusions were reached in several areas. Several key tampering scenarios could be detected in a laboratory setting (e.g., disconnect, record and playback of the signal, and hardware changes). The detectability of these events varied based on the system configuration but were primarily driven by the amount of energy on the cable. Further, some of the detections were a result of RF pickup, an important conclusion because it allows certain events that would otherwise be undetectable to become detectable. Unfortunately, RF pickup detection cannot be guaranteed and is subject to many variables. The results from the industrial environment were mixed and warrant further investigation. Several tests did show that it was possible to detect tampering scenarios such as disconnect, record and playback, and hardware changes with varying degrees of detectability.

It is recommended that the passive frequency analysis technique be coupled with the LiveWIRE spread spectrum time domain reflectometry (SSTDR) used by Pacific Northwest National Laboratory (PNNL) to take advantage of each technique's strengths and to supplement the weaknesses. The passive frequency analysis technique is weak when applied to systems with little energy on the cable. If supplemented by the SSTDR, a constant energy source will be provided by the SSTDR in the MHz range, thus increasing the frequency analysis technique detection limits. The SSTDR method most likely will not be able to detect pulses being placed on a line by means such as capacitive, inductive, and RF coupling that do not require cutting into the cable. These pulses, however, are likely to appear distorted when compared to normal pulses and would easily be picked up by the frequency analysis technique. The SSTDR also has the advantage of being able to determine the location of an impedance miss-match to a certain degree while the frequency analysis technique can detect equipment due to RF pickup that would not be detected by impedance miss-match. Additionally, using the combination of the SSTDR and frequency analysis technique will provide independent indication of tampering and could be applied to many safeguard systems at a reasonable price.

CONTENTS

FIGURES

TABLES

ACRONYMS

DOE	Department of Energy
INL	Idaho National Laboratory
PNNL	Pacific Northwest National Laboratory
LANL	Los Alamos National Laboratory
IAEA	International Atomic Energy Agency
FEUM	Front-End Electronics Package for Unattended Instrumentation
UNAP	Nondestructive Assay Data Acquisition Platform

UMS	Unattended Monitoring System
NGAM	Next Generation ADAM
MFC	Materials and Fuels Complex
ZCL	Zero Power Physics Reactor Counting Laboratory
RF	Radio Frequency
SSTDR	spread spectrum time domain reflectometry
StdEB	Standard Deviation Equivalent Bounds

1. INTRODUCTION

Idaho National Laboratory (INL) is part of a multi-lab project assessing front-end electronics for unattended instrumentation (FEUM) funded by the Department of Energy (DOE)/National Nuclear Safeguards Administration (NNSA) Office of Nonproliferation and International Security, Next Generation Safeguards Initiative (NGSI). As a part of its long-term technology development strategy, the International Atomic Energy Agency (IAEA) is in need of comprehensive testing and evaluation of a prototype FEUM package for its unattended instrumentation systems (UMS) and a viability study of candidate tamper-indicating measures that could be considered for integration into FEUM. The FEUM development activity provides an opportunity to address a long-standing challenge for the IAEA, by incorporating tamper-indicating measures between the detector and FEUM, and then from FEUM to the data acquisition systems (e.g., Next Generation ADAM [NGAM] or Universal Nondestructive Assay Data Acquisition Platform [UNAP] housed in the safeguards blue cabinet. See Figure 1.). Unfortunately, traditional data security measures such as tamper-indicating conduit are impractical for long separation distances (often 100m or more) between UMS components[1]. Further, some of the sensors are rarely inspected, because they are located in places with high radiation environments. The data from these sensors are therefore at risk of tampering, so more advanced tamper-indicating solutions are needed.

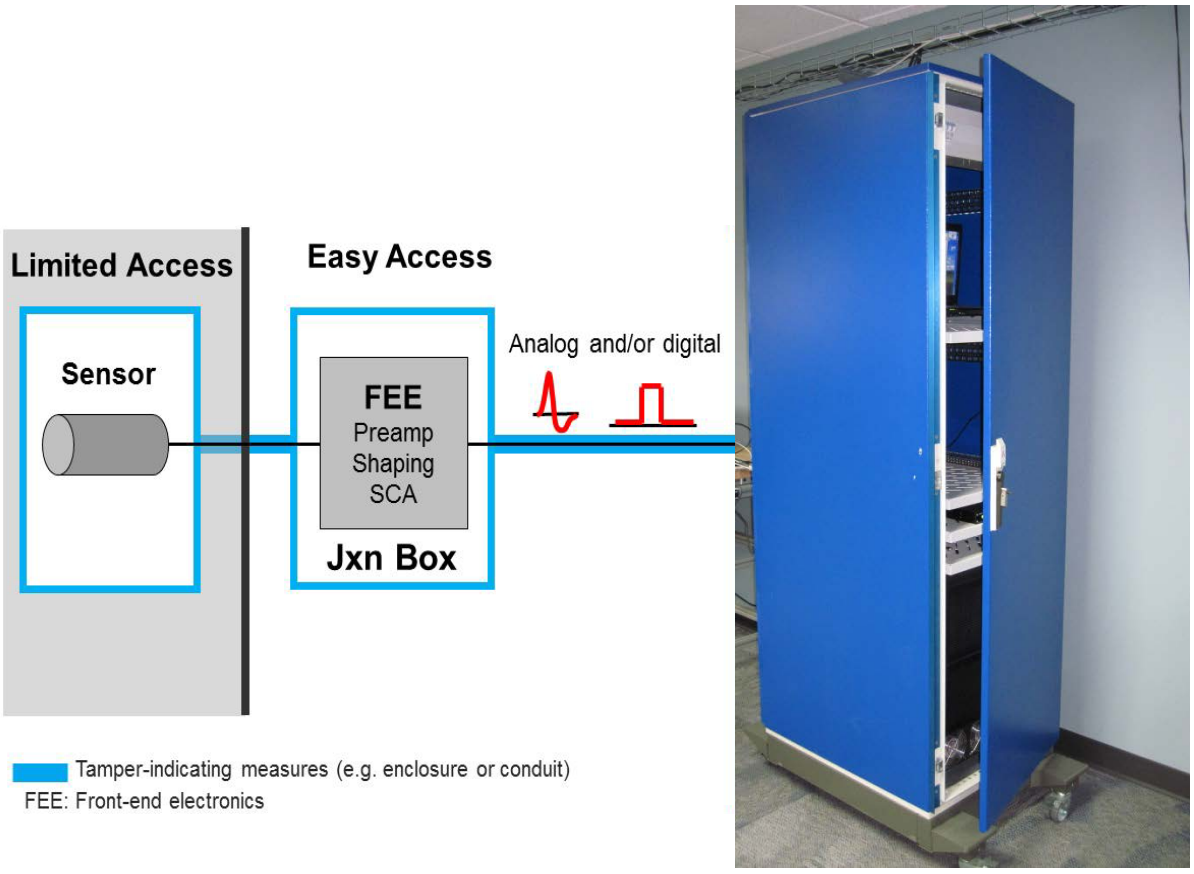

Figure 1. Overview of UMS system and FEUM[2]

As part of the FEUM project, INL is investigating an approach based on passive frequency analysis; Pacific Northwest National Laboratory (PNNL) has performed proof-of-principle experiments using time-domain reflectometry using a vector network analyzer and an application specific integrated circuit from LiveWire; and Los Alamos National Laboratory (LANL) is investigating pulse-by-pulse correction with

the coaxial shield as the electrode. This report summarizes the INL activities to characterize and test the passive frequency analysis approach as a potential tamper-indicating approach.

The concept of the passive frequency analysis approach is to separate signal from the sensor cable and pass it to a digitizer for processing. A bias-T is necessary if the cable has a DC voltage, such as the 12V on the NGAM system. The analysis could either be performed as part of the digitizer or it could be performed in software. The digitizer and signal separator tee would be placed in the safeguards cabinet for easy access and protection. The digitizer and tee do not need to be the exact same as those used in this study and can be purchased from commercial venders. A block diagram of a representative system is shown in Figure 2.

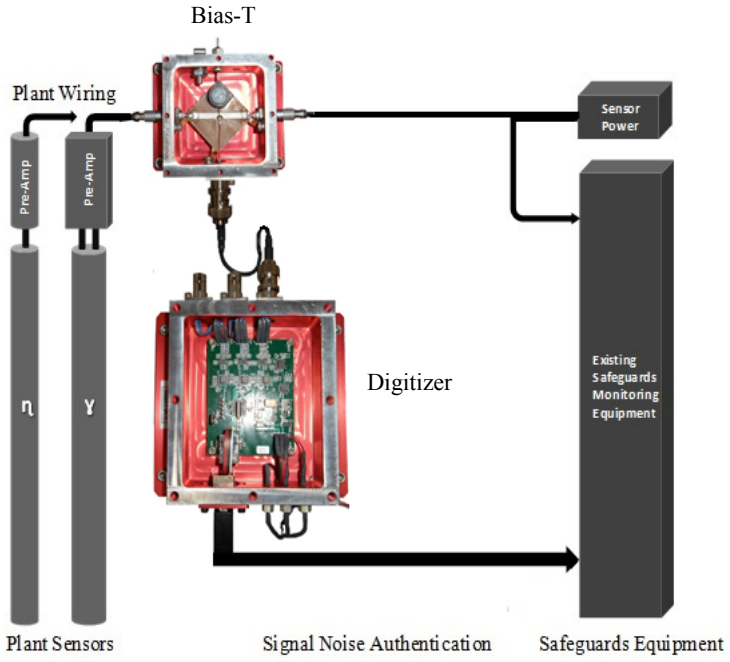

Figure 2. Noise Authentication System Block Diagram

The analysis starts after the digitizer separates the signal into either pulse or noise data in the time domain. These signals are then transformed into the frequency domain by the means of a Fourier Transform to create an amplitude spectrum. Examples of pulse and noise data in the time domain are given in Figures 3 and 4, and an amplitude spectrum is shown in Figure 5.

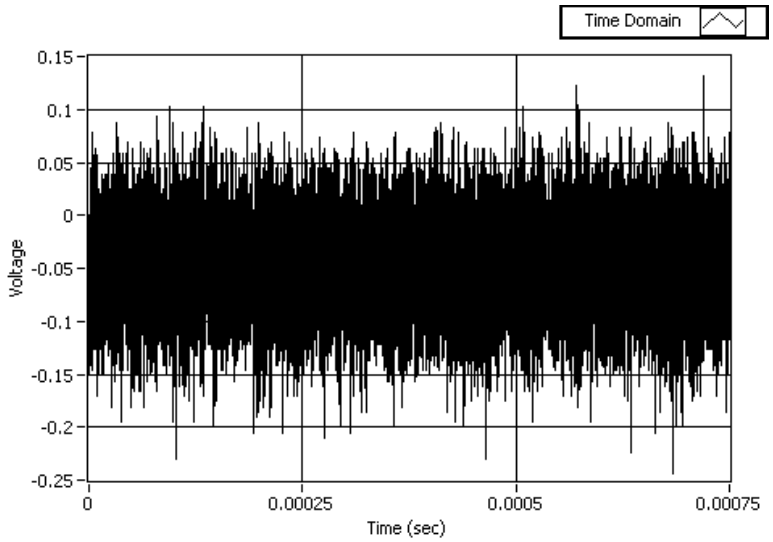

Figure 3. Noise Signal in the Time Domain

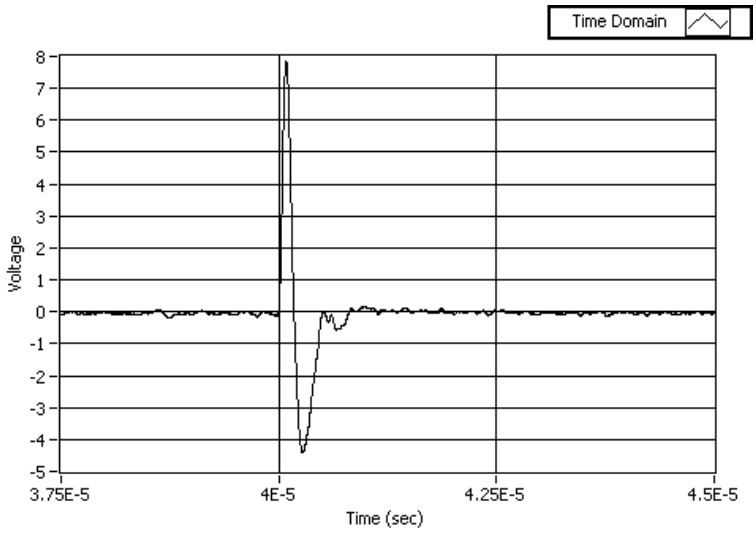

Figure 4. Pulse Signal in the Time Domain

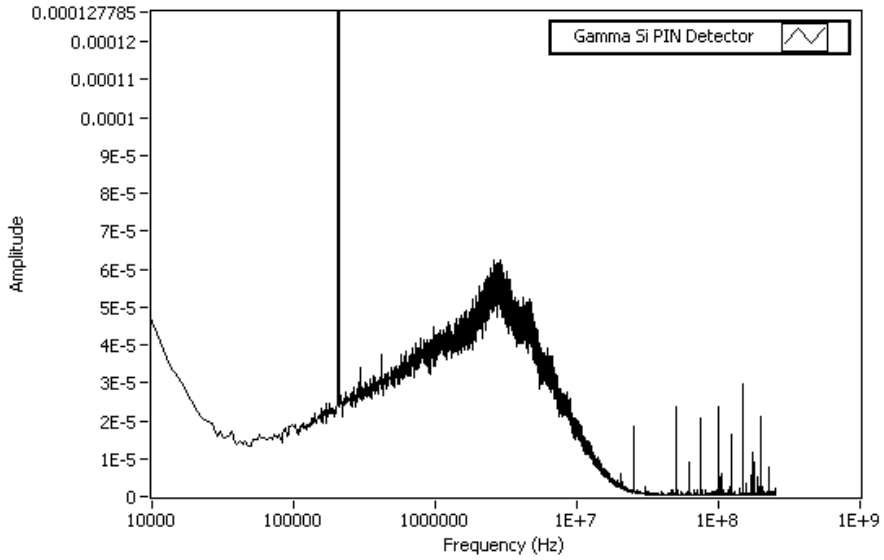

Figure 5. Example Amplitude Spectrum of the Noise Part of a Signal on a Gamma Si PIN Detector

After the signal (noise or pulse) has been transformed into the frequency domain, an average spectrum is obtained. Most experiments averaged 100 spectra over 30-90 seconds. The average spectrum is then divided up into several sub-sections or zones. A calculation is performed to derive a figure of merit for each zone and the entire spectrum. This figure of merit can be plotted over time. The figure of merit could be described as the integral or related to the electrical energy within the zone[3]. By dividing the spectrum up into zones tampering events that otherwise might not have been detected can be detected. Figure 6 shows a spectrum divided up into zones; Figure 7 shows the energy for 10 zones and entire spectrum over time.

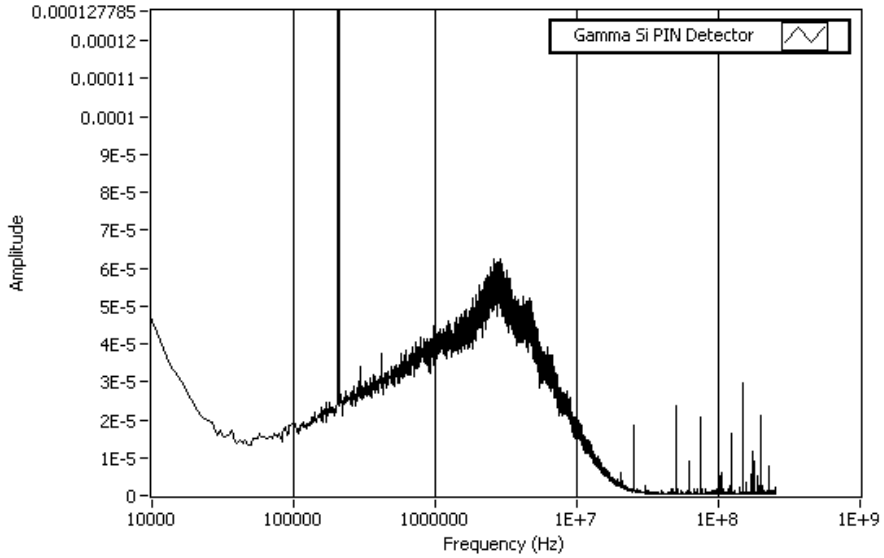

Figure 6. Example Amplitude Spectrum Broken-up into Several Sub-Sections/Zones

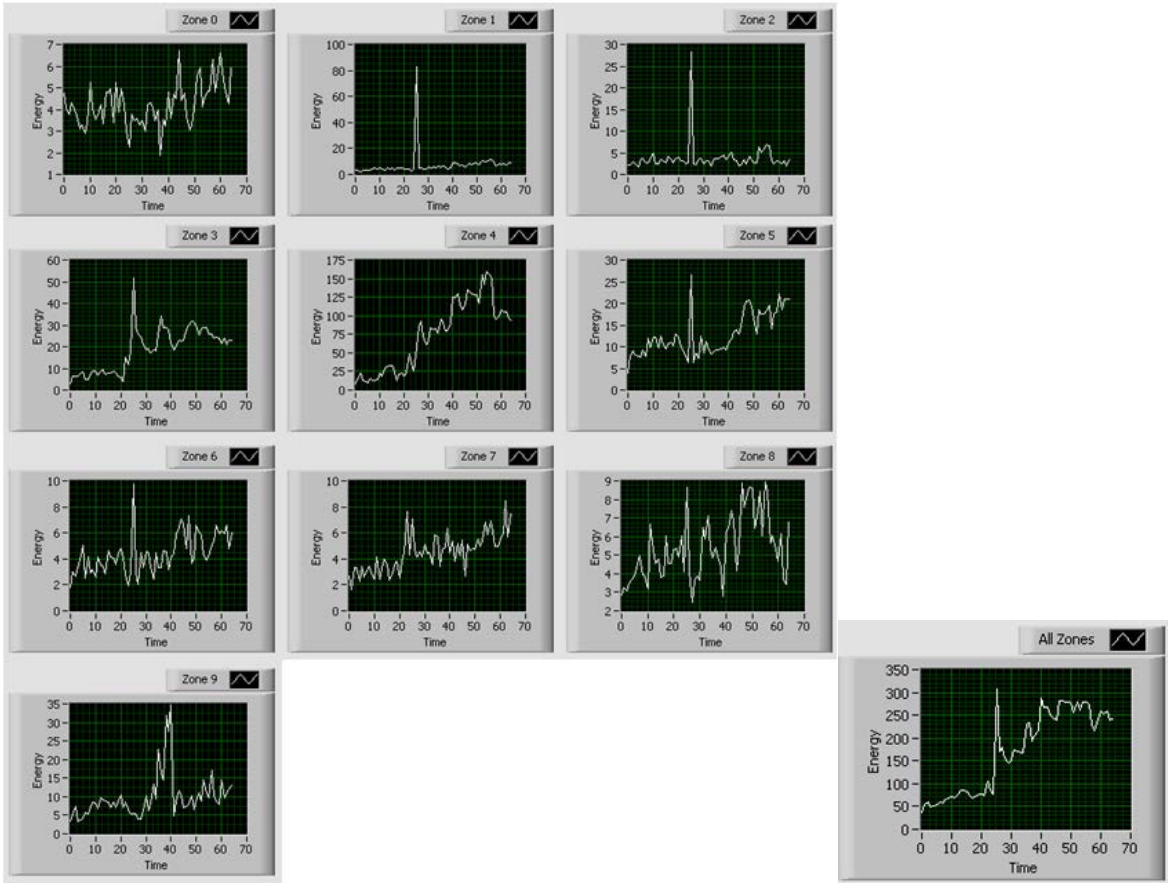

Figure 7. Graphs for Energy vs. Time for 10 Zones and Entire Spectrum (All Zones)

Bounds for fluctuations can be established for the energy within each zone as well as the entire spectrum for normal conditions. Bounds are established by determining the maximum number of standard deviations that occurred within each zone for normal operation. If the energy within a single zone or the entire spectrum exceeded the bounds a flag is raised indicating when the event occurred and which zone was affected. The algorithm is designed so that the mean value can fluctuate over time, which is why the bounds are based on the number of standard deviations from the mean (known in statistics as the z-score). Subsequently, the bounds are not a fixed amplitude but vary with the mean and standard deviation. Further, the mean and standard deviation are estimated using a revolving buffer so that the algorithm is dependent on nearby values and not all prior history, which is useful for large temperature changes. Figure 8 shows an example of the bounds on the energy verses time graph and a detector removal event.

The bounds for the tampering experiments were established by collecting data for a specific digitizer and hardware system over a period in which the most amount of fluctuation had been observed. This period was observed to be in the evening or morning when the facility would shut off or turn on the heating ventilation and air-conditioning systems. It was shown that temperature influenced the spectrum which is why the most drastic changes were seen during the shutdown and startup of each day, and the bounds took these sudden temperature changes into account. The temperature influence on the spectrum was shown to be most prevalent at lower frequencies and decreased above 1MHz.

The energy within a zone can be influenced by several factors. These can include components on the cable, the medium by which the signal propagates through (e.g., cable), reflections from impedance mismatch, and radio-frequency (RF) or electromagnetic pickup.

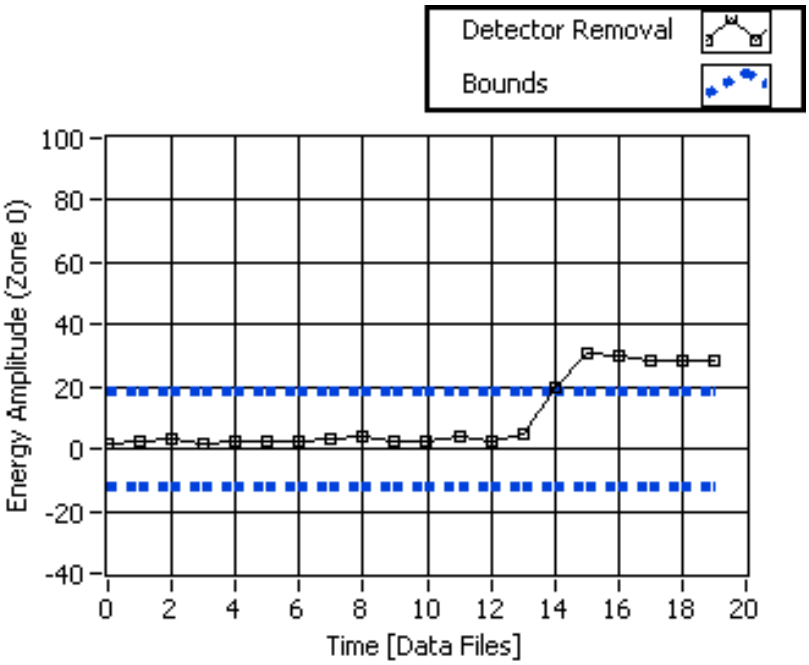

Figure 8. Example of Bounds for the Energy vs. Time Graph for Zone 0 (Detector Being Removed at File 14)

Other forms of analysis are also available besides energy monitoring, such as analysis of the signal peak resulting from a detection event. Some work was performed in peak analysis but was soon abandoned because the energy zone approach provided a clearer and more consistent indication when a tampering event occurred. Additional research into analysis approaches of the signal peak would be necessary to come to further conclusions on the ability of this approach to detect tampering.

Four pre-amplifier/detector systems were used for experiments and tampering scenarios. These pre-amplifier/detector systems were powered from two different, but common, UMS data acquisition systems used by the IAEA. The first power supply and data acquisition system was the Next Generation ADAM (NGAM) from BOT engineering used primarily for safeguard of CANDU reactors. The NGAM powered the PRE-100A, IRD-30A, and IC-10 pre-amplifier/detector systems. The second power supply used was the Mini-GRAND from Canberra and is used in many UMS systems. The Mini-GRAND was used to power the PDT20A pre-amplifier from Precision Data Technology, which provides a TTL signal pulse output as opposed to an analog pulse. Pictures of each of the systems are provided in Figures 9-12. The PRE-100A and PDT20A were used with ^{3}He neutron chambers, the IRD-30A is a Si PIN gamma detector (no pre-amplifier), and the IC-10 is a gamma ion chamber.


Figure 9. NGAM – Safeguards Data Acquisition System and Power Supply to PRE-100A, IRD-30A, and IC-10

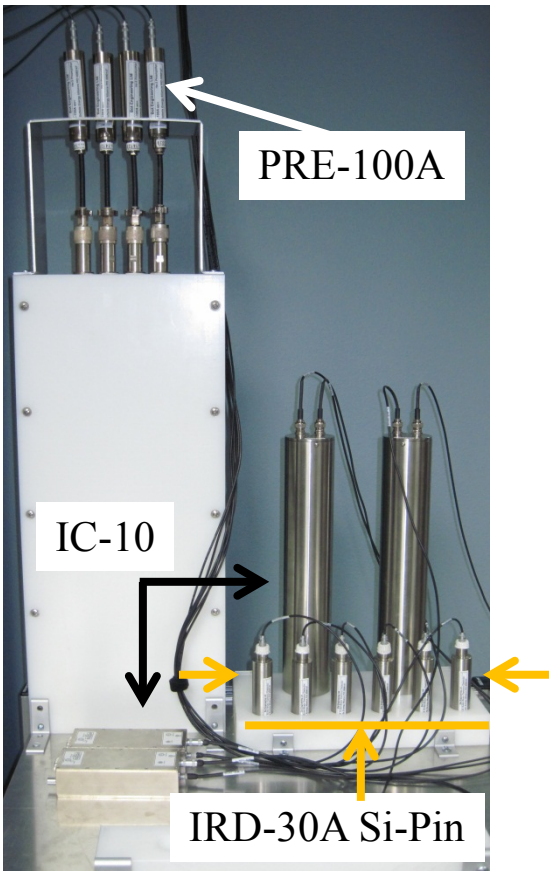

Figure 10. PRE-100A (white), IRD-30A (yellow), and IC-10 (black)


Figure 11. Mini-GRAND – Safeguards Data Acquisition System and Power Supply to PDT20A


Figure 12. PDT20A Pre-amplifier with ^{3}He Detector

While the digitizer represented in Figure 2 can be any commercial digitizer, three digitizers were used during the work performed in FY-15. The digitizers used were 1) A NGSI funded digitizer called the Development Board, 2) National Instruments PXI-5772 digitizer, and 3) A PCI-U1071A digitizer from

Keysight Technologies. These digitizers all perform the same function – digitize analog signals – however, trade-offs exist between each.

The development board uses a PIC32 microchip capable of a sampling 2MSamples/sec, 12-bit resolution with four amplifier gain options and 512kBytes of memory imposing limitations on waveform data length and creates dead time between data collections. For the experiments, the system collected 280kSamples/sec and 4096 samples/waveform. A trade-off exists between the waveform length and the sampling rate. The PXI-5772 uses an ADC with an FPGA adaptor capable of sampling 200MSamples/sec to 1.6GSamples/sec with step sizes of 200MSamples/sec. The PXI-5772 has a 12-bit resolution with a fixed amplification and is capable of continuous sampling, depending on the sampling frequency and limited by the computer hardware for memory limitations. For the experiments performed, the system used a sampling rate of 800MSamples/sec and collected 600kSamples/waveform and allowed for a dead time of 0.2 seconds between waveforms. The PCI-U1071A digitizer has various sampling options from 10MSamples/sec to 2GSamples/sec. The digitizer has an 8-bit resolution with seven amplifier options and enough memory for 128kSamples/waveform.

The development board was limited to lower frequencies (~140kHz) and could not obtain pulse signals, but had a better frequency resolution than the other digitizers. The PXI-5772 could observe much higher frequencies (0-400MHz), but had a poor dynamic range (voltage range/2^bit resolution) for the noise signals. It had a better dynamic range for pulse signals, but had a poor amplitude resolution for low frequencies. The PCI-U1071A digitizer could observe high frequencies (capable of 0-1 GHz) set to (0-250MHz for a better frequency resolution). It had a better dynamic range for noise signals, but a poorer dynamic range for pulse signals and a better low frequency amplitude resolution than the PXI-5772. Both high frequency digitizers have a poorer amplitude and frequency resolution and noise floor for low frequencies compared to the development board.

Because of these trade-offs the high frequency noise spectra for the IC-10 and PDT20A were collected using the PCI-U1071A digitizer, and the PXI-5772 digitizer was used with the PRE-100A and IRD-30A systems. All four of the systems were digitized with the development board for low frequencies.

It is worth mentioning that it is possible to take advantage of the hardware trade-offs. For example, it is impossible for an adversary to record the entire frequency spectrum and play it back with a single digitizer. Each device (digitizer for recording and signal generator for playback) will have limitations on the frequency range, frequency resolution, and amplitude resolution that can be recorded and played back. Thus, the recorded spectrum and playback spectrum would not matchup because of hardware differences between the digitizer and signal generator. By merely using two digitizers that have opposite qualities, it is possible to detect that part of the spectrum has changed on at least one of the digitizers.

The primary experiments for FY-15 work are outlined below:

1) Perform tampering scenarios and determine if they are detectable (applied to four pre-amplifier/detector systems)
    a. Cable tampering scenarios
        i. Disconnect
        ii. Tap and Splice (i.e., Record and Playback)
        iii. Cable Changes (length, impedance, attenuation properties, cable type)
    b. Hardware tampering scenarios
        i. Removal of detector
        ii. Switching of detector
        iii. Switching of pre-amplifier

2) Compare tampering scenario results between cables RG-174, RG-62, and RG-71 (applied to four pre-amplifier/detector systems)
3) Perform anechoic chamber experiments to segregate RF induced detection from inherent component detection
4) Perform tampering scenarios in an industrial environment

2. WORK PERFORMED/RESULTS

2.1 Tampering Scenarios

The tampering scenarios investigated can be grouped into two categories: cable and hardware tampering. The main focus of the project was on cable tampering. Hardware tampering was added because it took minimal time to perform and is a valuable benefit for the main goal of data authentication.

The criteria for detection were explained in the Introduction and were defined as the energy in any single zone surpassing the maximum number of standard deviations for normal operation. Since there are multiple detector systems that were investigated there needed to be a uniform means of reporting numerically "how well" a tampering event was detected. One method is to report the percent change in energy, which is an intuitive measure and will be reported only for the entire spectrum. However, this method does not take into account that the energy must first surpass the bounds before an event is detected.

A better method of reporting is to take the standard deviation from the mean for the tampering event and divide by the standard deviation used for the bounds. In this way, the reported value is a measure of how far above the bounds the event was, with '1' being equal to the bounds and anything above '1' indicating detection of a tampering event. This unit is called the standard deviation equivalent bounds (StdEB), and for the analysis used in this paper a StdEB was determined for each zone and the entire spectrum. For the analysis described in this paper, the StdEB is displayed for the entire spectrum and the zone with the highest StdEB. Additionally, the number of zones with an StdEB above 1 are reported. It should be noted that it is possible for an event to remain undetected by the entire spectrum energy change but actually be detected in a single zone. In this case, a 0 for the StdEB of the entire spectrum indicates non-detection in the entire spectrum. If the event was undetectable, 0's are used for all the StdEB values. Further, the experiments reported in the individual tampering sections are based on the RG-174 cable results. The one exception is the comparison between tampering results using cables RG-174, RG-62 and RG-71 which is covered in Section 2.1.3.

2.1.1 Disconnect

Disconnect can be considered one of the most important tampering scenarios because most tampering scenarios eventually lead to disconnect of the detector and the front-end electronics from the safeguards cabinet. Fortunately, this tampering scenario is one of the easiest to detect. The main distinguishing factor for disconnect detection between the pre-amplifier/detector systems is the amount of energy being carried on the line. The PRE-100A and IRD-30A preamplifiers output analog signals proportional to the radiation energy, and have much more fluctuation energy than the IC-10 and PDT-20A, which provide fixed energy TTL-type pulses for each event. For this reason, most of the tampering scenarios are better detected on the PRE-100A and IRD-30A.

The disconnect scenario consisted of disconnecting the cable from the pre-amplifier/detector or at the bias-T. The spectral results were fairly similar with some minor dependencies on location of the

disconnect on the cable. Several experiments were performed to assess the difference between an intermittent (<5sec) disconnect and a longer duration (>30 sec) disconnect. It was found that the methodology of observing the energy could detect a disconnected wire. However, if the disconnect time frame was very short in comparison with the time it took to obtain an average spectrum, the averaged spectrum could mask the fact that a disconnect had occurred. Therefore, the best practice is to let the algorithm look for a disconnect, or large change in energy, from each waveform collected as opposed to the averaged spectrum. Additionally, the disconnect is most manifest in zones where the highest energy content is present. For most systems, this zone is between 0-20MHz. Table 1 has the results for a disconnect scenario that was allowed to remain for the duration of five files (i.e., five spectra over time that are derived from averaging 100 spectra for each file). Recall that a StdEB is equivalent to the bounds at 1 and the reported value represents the multiple of those bounds, so a value above 1 indicates that a tampering event has been detected.

Table 1. Results for Disconnect

Disconnect						
		%Energy Change (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	6481	47.1	56.2	6	Detected
	IRD-30A	6004	113.3	210.1	9	Detected
	IC-10	107.8	0	1.3	1	Detected
	PDT20A	564.6	2.5	7	4	Detected
Low Freq. (Dev. Board)	PRE-100A	548.2	1.6	18.9	2	Detected
	IRD-30A	2082	30.4	30.4	8	Detected
	IC-10	736.5	4.1	32.8	4	Detected
	PDT20A	887.4	4.6	4.6	11	Detected

From Table 1 it can be seen that a disconnect scenario is far beyond the normal conditions (StdEB >> 1), with the exception of the IC-10 ion chamber at high frequencies (i.e., StdEB = 1.3 with 1 zone detecting the disconnect). However, in the low frequency region, the IC-10 performed comparable to the other systems. This shows that disconnect can be detected, but one needs to observe the best frequency region. Further, IC-10 and PDT20A have much lower amounts of energy on the line compared to PRE-100A and IRD-30A for high frequencies as seen by the orders of magnitude of the StdEB (56.2 to 210.1 compared to 1.3 to 7) and the percent change in Energy.

In conclusion, tests performed indicate that it is possible to detect disconnection for all pre-amplifier/detector systems. The frequency region is important; the more energy on the line, the better the results. It is recommended that the algorithm monitor each waveform for disconnect, so that intermittent disconnects do not go unnoticed.

2.1.2 Tap and Splice (Record and Playback)

The tap or splice scenarios are the type of intuitive scenarios that most people think of for an adversary spoofing the system. The main idea is that an adversary records the signal and plays back the signal while altering the system. Since the playback of the signal will increase the count rate, it is requisite to compromise the system in such a way so the count rate appears to be normal. Figure 13 shows four possible means of altering the system so that the count rate appears to remain the same. To avoid

detection, the removal/alteration of pulses must be performed unilaterally with the playback of the signal. The investigation of this section covers record and playback scenarios.

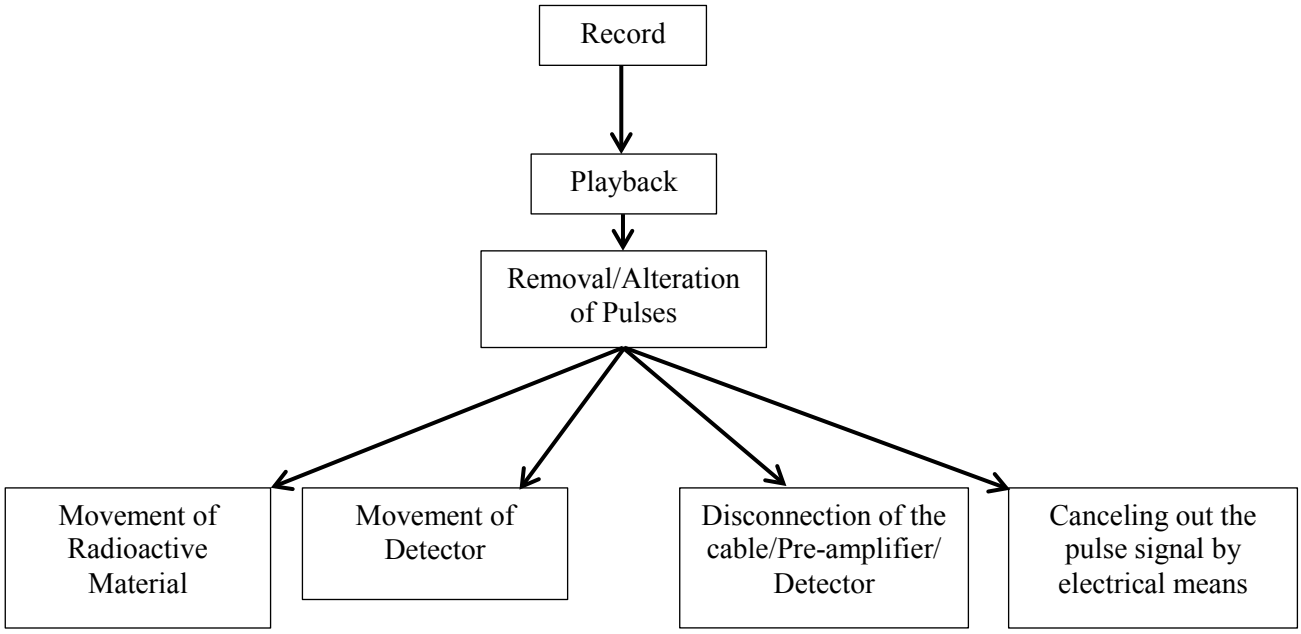

Figure 13. Steps for a Record and Playback Tampering Event

The tap scenario investigated for this project was defined as a cut into the cable while a splice is a tee connector. Both of these scenarios are nearly identical electrically, with the basic idea being that one must attach a probe to the center conductor and the outer braided shield. There is a slight difference between a tee connecter and a tap, in that the tap does not have a shield covering part of the dielectric. For the purposes of this report, the results are nearly identical and will be considered a record and playback scenario.

Several tests were performed to determine if it was possible to detect an adversary cutting into a cable and switching a barrel connector for a tee connector. The results showed that there was a detection for many of the cutting scenarios in real time. However, it was found that this detection was due to the bending of the cable and not the cutting event itself. It is believed that the triboelectric effect was the source of detection from cable bending. It was concluded that cutting into a cable could not be detected. Likewise, the replacement of a barrel connector for a tee connector could not be detected if one were forced to ignore the fact that a disconnect must occur for the exchange. In other words, the disconnection of the cable can be detected when switching a tee for a barrel connector, but the tee connector showed no change when the disconnect portion was ignored. These results were consistent with other investigations of cuts/frays on cables[4].

Given that the cut or tee cannot be detected, the next step in the record and playback scenario is the recording of a signal. A digitizer is normally used to record a signal. In order to avoid detection, one would use a high impedance (10Mohm or greater) digitizer. For this experiment, a probe or short cable was attached to the tap or tee, and then attached to an oscilloscope with an impedance of 10Mohms. Figure 14 is an example of energy verses time graph for the connection of a probe (file 14) and oscilloscope (file 20) at 25m and 50m on a 51m cable for the PRE-100A system.

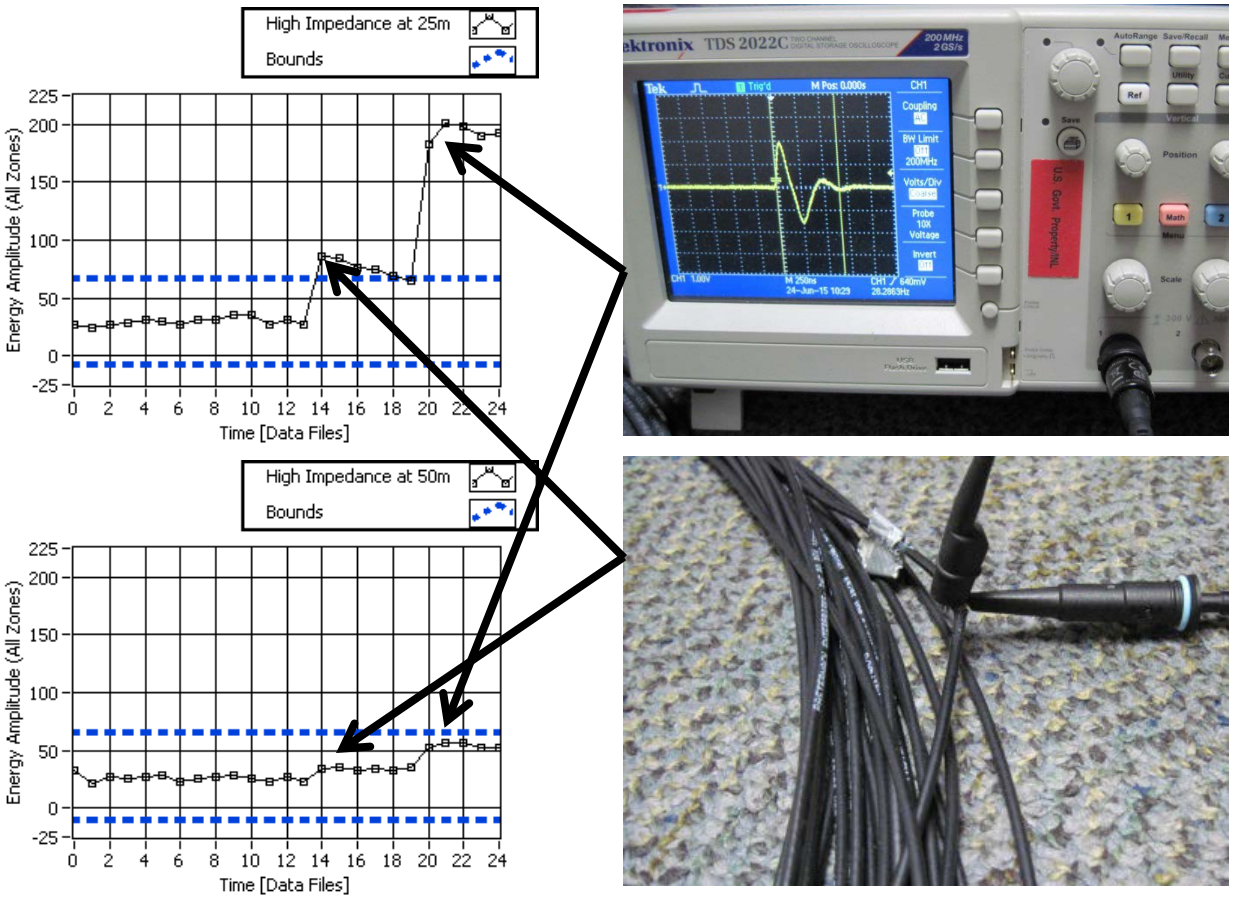

Figure 14. Attachment of High Impedance Device at 25 and 50m

Figure 14 indicates that detection is a function of location. The high impedance device was detected at 25m but goes under the detection limit at 50m. Supplemental equipment, such as a probe, also introduces a change and can be detected, such as in the 25m case. While it may be possible to detect a high impedance device, the detection cannot be guaranteed as illustrated with the 50m case. As described later in the paper, detection is not only reliant on location but on RF pickup as well.

After a signal has been recorded the next step is to playback a fake signal. Until this point, the data integrity has not been compromised, meaning that the recording of a signal does not modify the data. The modification of the data occurs when new signals are added to the line. The major challenge to adding this signal without detection is due to the fact that commercial signal generators are low impedance (typically 50-93 ohms), which is a very important concept. The reason why signal generators are low impedance is due to the requirements that the signal generator drive the line. For this purpose, low impedances are desirable. Additionally, the signal generator must be in parallel with the pre-amplifier/detector until the line is disconnected. Because the signal generator is usually low impedance several tests were performed to demonstrate the consequence of adding a low impedance device in

parallel (i.e., branched circuit). Figure 15 demonstrates the effect of a 50 ohm impedance attached in parallel at 25 and 50m for a 51m cable and the PRE-100A preamplifier.

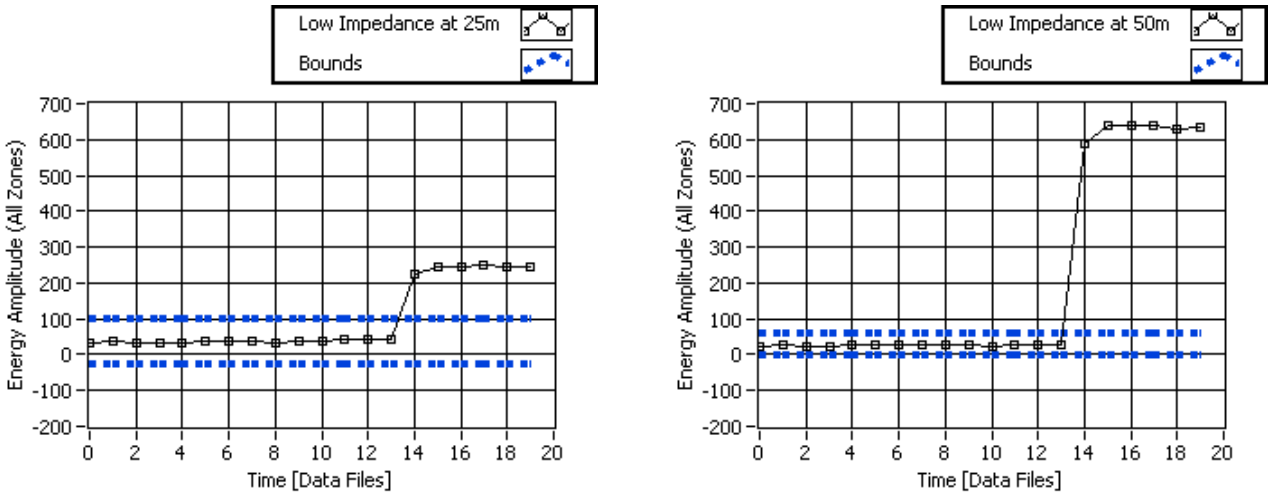

Figure 15. Low Impedance Branch (Representing a Signal Generator) at 25 and 50m

Figure 15 indicates that the detection ability is improved with distance, opposite that observed with high impedance devices – a result of the low impedance device absorbing more energy by being placed closer to the source (i.e., detector), thus causing a larger change. This effect was demonstrated in the PRE-100A and IRD-30A, but not the IC-10 and PDT20A which have little energy on the line.

While it is possible to construct a high impedance signal generator which would be more difficult to detect, increasing the impedance requires the generator to produce a high voltage in proportion to overcome the high impedance. By forcing the signal generator to proceed to high impedances, there is a higher chance that the signal generator will induce extra noise on the line and might trigger an event.

Representative results for the high and low impedance experiments can be found in Tables 2-5. Low impedance experiments were performed for impedances from 50ohms to 1.5kohms. Tables 4-5 show the 50ohm results. From these tables, it can be seen that the low frequency region analyzed by the development board is rarely able to detect the high impedance device, while the low impedance is detected for almost every case. In addition to the record or playback device, several additional pieces of hardware might be required to record or playback. For instance, to playback on the NGAM system a DC block is required because of the 12V on the line. It is possible for this supplemental hardware to cause a much larger change in spectral energy than the addition of the digitizer or signal generator. Tables 2-5 used a reference that already took into account the supplemental hardware. For the low impedance experiments, the addition of clips, conversion to BNC connector, and addition of a DC block would have raised flags before the low impedance was added.

The low impedance experiments tended to produce results with the best detectability at 50ohms that decreased as the impedance increased. An interesting phenomenon was observed for the PDT20A and IC-10 in that a higher impedance could be detected but a lower impedance could not. For instance, the PDT20A was able to detect both 50 and 93ohms at higher frequencies but failed to detect 75ohms. The 75ohms test did show a sizable change but was not enough to be detectable. These results demonstrate that the detectability can have some variation based on the reference data and it can fluctuate. For the case of higher frequencies PDT20A 75 and 93ohm tests, it is likely that both the 75 and 93ohms have the possibility of detection but cannot be guaranteed because they are within a region where the detectability bound fluctuates. The 50ohms, however, was sufficiently far enough away that it was always detected.

Table 2. Results for 10Mohms Impedance Device at 25m

High Impedance and Probe at 25m						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	555	1.4	7	6	Detected
	IRD-30A	599	2.3	2.3	3	Detected
	IC-10	2265	0	23.6	9	Detected
	PDT20A	1553	7.1	33.7	6	Detected
Low Freq. (Dev. Board)	PRE-100A	70.3	0	0	0	Not Detected
	IRD-30A	11.1	0	1.06	1	Detected
	IC-10	34.7	0	0	0	Not Detected
	PDT20A	50.7	0	0	0	Not Detected

Table 3. Results for 10Mohms Impedance Device at 50m

High Impedance and Probe at 50m						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	107	0	0	0	Not Detected
	IRD-30A	237	1.7	2.9	2	Detected
	IC-10	986	0	1.6	1	Detected
	PDT20A	255	1.2	2.6	3	Detected
Low Freq. (Dev. Board)	PRE-100A	0.2	0	0	0	Not Detected
	IRD-30A	35	0	0	0	Not Detected
	IC-10	8.4	0	1.2	1	Detected
	PDT20A	140	0	0	0	Not Detected

Table 4. Results for 50ohms Impedance at 25m

Low Impedance at 25m						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	696	4.5	7.5	4	Detected
	IRD-30A	576	6.9	23	2	Detected
	IC-10	235	1.4	12.4	3	Detected
	PDT20A	169	0	1.07	1	Detected
Low Freq. (Dev. Board)	PRE-100A	396	0	2.6	1	Detected
	IRD-30A	653	8.6	8.6	3	Detected
	IC-10	89	0	7.6	2	Detected

Low Impedance at 25m						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
	PDT20A	250	1.9	1.9	1	Detected

Table 5. Results for 50ohms Impedance at 50m

Low Impedance at 50m						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	2816	27	27	5	Detected
	IRD-30A	3350	74.9	125	5	Detected
	IC-10	137	0	0	0	Not Detected
	PDT20A	527	4	4	3	Detected
Low Freq. (Dev. Board)	PRE-100A	359	0	3.8	1	Detected
	IRD-30A	633	9.1	9.1	3	Detected
	IC-10	1.8	0	9	2	Detected
	PDT20A	147	0	1.6	2	Detected

The results presented here are for the case in which the conductors for the center wire and outer braded shield are in direct contact. There are, however, several other methods to inject signal into a system, such as by injecting pulses on a cable without tampering with the cable. For example, capacitive, inductive, and RF coupling could be used to induce pulses on a cable without cutting into it. Since the UMS systems generally look for a pulse that exceeds a certain voltage, a rather crude pulse could fool the system. Given the nature of capacitive, inductive, and RF coupling, the pulse would have a distorted shape and could easily be identified by the frequency noise analysis of the pulse.

In conclusion, the results of tests show that it is possible to detect a high and low impedance device that is used for recording and playing back a signal on a cable. The high impedance detectability decreases with length and cannot be guaranteed to be detected. The low impedances could be detected for every pre-amplifier/detector system in at least one frequency region.

2.1.3 Cable Changes

Several experiments were performed to determine detectability for various changes to cables. These changes included identical cable change out, length, attenuation properties, impedance, and cable type. In the majority of the scenarios, the dominate factor was found to be the attenuation properties for each cable. The scenarios are outlined below:

- Switch with identical cable
- Length additions
    a. 1m
    b. 22m
- Low loss RG-174 cable vs. regular RG-174 cable (Impedance remains the same attenuation properties change)

- Changes to characteristic impedance
    a. Compare RG-62 (93ohms) with RG-59 (75ohms)
- Changes based on cable type
    a. Compare spectral content for RG-174 with RG-62 and RG-59
    b. Compare tamper detection between RG-174, RG-62, and RG-71

The identical cable scenario consisted of switching a cable with an identical cable between the bias-T and preamplifier/detector. Tests were performed for RG-174A/U, RG-62, and RG-71 cables. The results ignored the fact that the cable must first be disconnected in order to switch the cables. The results showed that it was possible, at times, to detect the difference between the two cables. However, as explained in the RF vs. Inherent Component (Anechoic Chamber) section, the source of detection was the differences in RF pickup. In other words, the cables had different pickup from radio frequency sources. In the absence of RF sources, the cables could not be distinguished.

Tests were performed to determine if it was possible to distinguish a cable that came from the same manufacturer but was produced in a different batch. A cable from a different batch was purchased, tested, and found to have similar results as those tested that came from the same batch. The cable tested was the Pasternack model # RG-174A/U.

Tests were performed to determine the detectability of cable additions. Two tests were performed by adding 1m and 22m to the RG-174A/U cables. Tests were also performed for RG-62 and RG-71 cables. Again, in order to change the length of the cable, a disconnect must occur. The disconnect was ignored in data analysis. These tests showed that the major characteristic governing the detection of length changes was the attenuation properties. The attenuation is a function of frequency and length. Attenuations are usually quoted at certain frequencies and are listed in dB/length. The attenuation varies, with the majority of the effect at higher frequencies and drops to little attenuation at low frequencies. For this reason, it was easier to detect length changes at high frequencies for shorter cable lengths. However, as the cable length increased lower frequencies could start to detect the attenuation as well. The RG-174A/U cable has a higher attenuation verses frequency curve than most RG cables. The results for the RG-174A/U cable extension are shown in Tables 6-7.

Table 6. Addition of 1m

Add 1m Cable						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	63.2	0	0	0	Not Detected
	IRD-30A	97.9	1.5	3.2	2	Detected
	IC-10	227	0	3.3	4	Detected
	PDT20A	92.6	1.8	1.8	4	Detected
Low Freq. (Dev. Board)	PRE-100A	3.3	0	0	0	Not Detected
	IRD-30A	5.1	0	0	0	Not Detected
	IC-10	79.6	0	0	0	Not Detected
	PDT20A	99.4	0	0	0	Not Detected

Table 7. Addition of 22m

Add 22m Cable						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	1804	13	13	3	Detected
	IRD-30A	308	5.7	9.6	3	Detected
	IC-10	317	0	6.2	4	Detected
	PDT20A	232	0	1.2	2	Detected
Low Freq. (Dev. Board)	PRE-100A	29.8	0	1.7	1	Detected
	IRD-30A	84.5	0	0	0	Not Detected
	IC-10	27	0	0	0	Not Detected
	PDT20A	118	0	1.7	2	Detected

The low loss test and the comparison test between RG-62 and RG-59 were meant to try and separate the attenuation from characteristic impedance properties. It was easy to vary the attenuation property because many cables exist that have the same characteristic impedance but have different attenuation curves. To perform this test, an RG-174 low loss (Belden B7805R) cable was compared with the RG-174A/U (Pasternack) cable. However, to distinguish between characteristic impedance was very difficult. The problem with changing the characteristic impedance is that the attenuation properties usually change as well. To separate the two effects, it would be necessary to use two cables with different characteristic impedances but very similar attenuation curves – nearly impossible to do with real cables. Belden B8255 (RG-62) and Belden B9659 (RG-59) had fairly similar quoted attenuation data up to 50MHz as seen in Tables 8-9. However, the data only quoted one significant digit for several data points. With these two cables, the regions between DC to 50MHz could be used to separate the characteristic impedance from the attenuation property.

Table 8. Attenuation Data for RG-59 (B9659)

RG-59 B9659 75 ohm	
Freq. (MHz)	Attenuation (dB/100ft)
1	0.3
10	0.9
50	2.1
100	3
200	4.5
400	6.6

Table 9. Attenuation Data for RG-62B/U (B8255)

RG-62B/U B8255 93 ohm	
Freq. (MHz)	Attenuation (dB/100ft)
1	0.3
10	0.9
50	2

100	2.9
200	4.2
400	6.1

The results from the low loss cable showed that indeed changing the attenuation while maintaining the characteristic impedance changed that amount of energy within the signal. With a lower loss, more energy is preserved within the signal and the amplitude of the spectrum increases. Likewise, when the attenuation curve is increased the spectrum decreases and less energy is left in the signal for a fixed cable length. This is the same effect as was observed with cable changes – the longer the cable, the more attenuation.

The results from comparing RG62 with RG59 at low frequencies showed that there was a detectable change for one zone with a StdEB of 2.2. While the difference is detectable, it is not greatly different and could still be due to unaccounted changes. However, for high frequencies there was a change in the region between 100kHz to ~20MHz, as seen in Figure 16. What is interesting is that it is near the region in which the attenuation points for the two cables match. The natural conclusion would be that the characteristic impedance is causing a different amount of energy to be reflected at the cable connections and attenuated as it travels back through the cable in the opposite direction. The cable connections have little reflection at 50ohms and the energy within the reflections increases as the impedance deviates from 50ohms. The 93ohm cable's characteristic impedance lost more energy than the 75ohm cable.

However, it should be noted that changing cable impedances is not exactly the same thing as an impedances miss-match by branches along the cable. The difference is the location of the reflection in the signal and the magnitude. For the case of switching cables the reflections are occurring at the ends while a miss-match from a low impedance branch is somewhere between the ends and the reflection coefficient is based on the effective impedance from the cable and branch in parallel. The reflected signal travels in the opposite direction of its former trajectory and will slowly attenuated in the cable. Thus, impedance miss-match also influences the energy, but depends on the location of the miss-match.

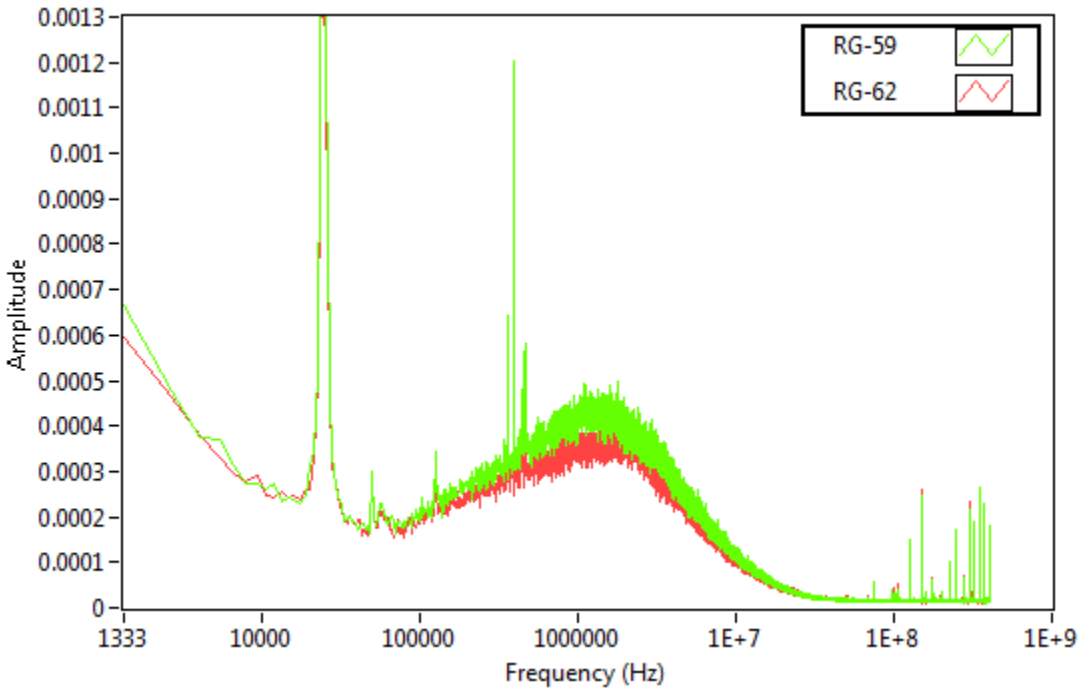

Figure 16. Spectral comparison between RG-59 and RG-62

Further cable tests were performed to determine changes based on differing cable types. The first set of tests simply compared the spectra content between cables RG-174, RG-62, and RG-59. A second set of experiments performed each of the tampering tests for cables and hardware on RG-174, RG-62, and RG-71.

The comparison between the RG-174, RG-62, and RG-59 cables showed amplitude changes at higher frequencies as was discussed in the characteristic impedances paragraph. Due to the significant changes between cable types, it is possible for most systems to detect differing cable types.

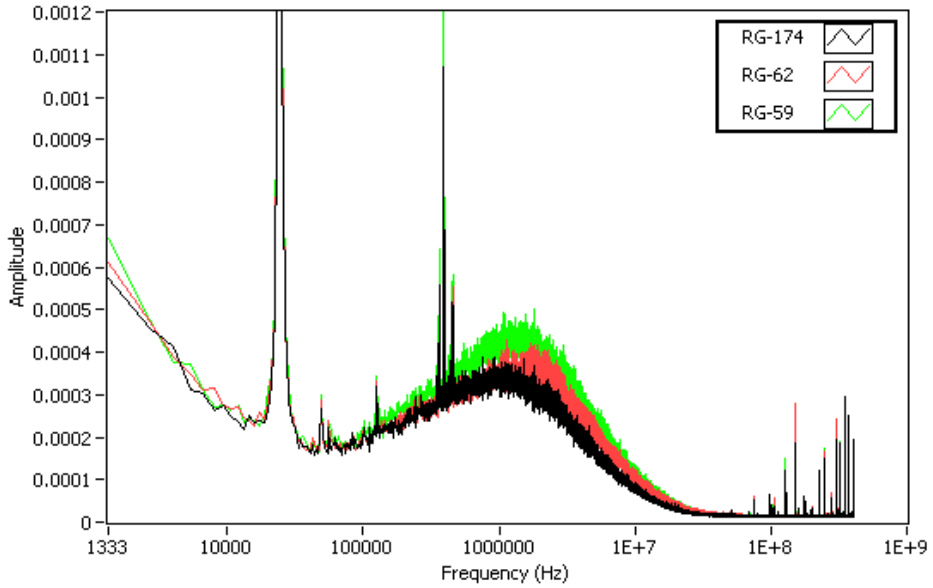

Figure 17. Comparison of spectra from 3 cable types.

The tampering tests with cables RG-174, RG-62, and RG-71 followed the same general trend with a few exceptions. There were detection changes for scenarios, such as the addition of cable length which depended heavily on the cable attenuation. RG-174 had the highest attenuation and it was possible for certain configurations to detect 1m of added cable. Detection was less likely with the lower attenuation per meter cables RG-62 and RG-71. Additionally, some of the changes could have been detected/undetected due to being near the detectability thresholds, as was discussed in Section 2.1.2.

The general conclusions from the comparison between cable types was that cable attenuation and characteristic impedance affects the spectral height and detection, and the majority of the tampering tests results are not dependent on cable type unless the cable attenuation is directly related to detection.

2.1.4 Removal of detector

The detector removal scenario consisted of the removal of the detector portion of the hardware. While the hardware may be protected by a seal, it is possible for an adversary to break the seal; it could be months to years before an inspector finds that tampering has occurred. It would be possible for an adversary to take control of the signal by removing the detector and fluctuating the voltage on the other side of the pre-amplifier to create fake signals while using the pre-amplifier to mask its intrusion. Before one takes control of the signal generation, one must remove the detector. Table 10 has the results for each of the pre-amplifier/detector systems. It should be noted that the IRD-30A does not have separate components for the detector and pre-amplifier, and removal of the detector is analogous to removal of the pre-amplifier or disconnect of the cable, which is why the detection of the IRD-30A for detector removal

is so large. Further, it should be noted that every system was detected with the high frequency digitizers. However, the detection was fairly close to the detection bounds and is therefore not guaranteed.

Table 10. Detection Results for Removal of the Detector

Removal of Detector						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	146	0	1.8	1	Detected
	IRD-30A	6004	113.3	210.1	9	Detected
	IC-10	137	0	1.5	4	Detected
	PDT20A	121	1.2	3.2	5	Detected
Low Freq. (Dev. Board)	PRE-100A	14	0	0	0	Not Detected
	IRD-30A	2082	30.4	30.4	8	Detected
	IC-10	34	0	0	0	Not Detected
	PDT20A	813	2	18.1	3	Transient-Detected

2.1.5 Switching of detector

The switching of the detector scenarios consisted of switching between identical detectors as well as switching a detector from a different manufacturer. For the second set of experiments, there were no alternative manufacture detectors available to test the IRD-30A and IC-10. The PRE-100A and PDT20A both used ^{3}He detectors and switched between LND 25288 and Reuter Stokes RS-P4-0812-124 detectors. For both of these experiments, it was necessary to ignore the detector removal that was required to switch the detectors.

Tables 11-12 show the results for switching between identical and different manufacture detectors. Since the IRD-30A does not have two separate components for the pre-amplifier and detector, the switching of the IRD-30A detector is analogous to switching of pre-amplifiers (see Section 2.1.6). The results suggest that it is very difficult to distinguish between identical and different manufacture detectors using the noise signal. The tampering events that did result in a detection have StdEB values that are very close to 1, and therefor may not be detected.

However, it is possible to have a strong indicator when the detector has been modified by observing the spectral results for pulses instead of noise. An example of the pulse spectrum from LND 25288 and Reuter Stokes RS-P4-0812-124 detectors on the PRE-100A pre-amplifier are shown in Figure 18.

Table 11. Switching of Identical Detectors

Switch Identical Detector (Noise Spectrum Results)						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	87.5	0	1.4	1	Detected
	IRD-30A	1165	21.9	43.3	3	Detected
	IC-10	27.9	0	0	0	Not Detected

	PDT20A	11.9	0	0	0	Not Detected
Low Freq. (Dev. Board)	PRE-100A	9.7	0	0	0	Not Detected
	IRD-30A	1412	27.3	66.3	7	Detected
	IC-10	440	2.4	2.4	3	Detected
	PDT20A	78	0	0	0	Not Detected

Table 12. Switching of Detectors from Different Manufactures

Switch Detector Manufacture (Noise Spectrum Results)						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	33.9	0	1.2	1	Detected
	IRD-30A	N/A	N/A	N/A	N/A	N/A
	IC-10	N/A	N/A	N/A	N/A	N/A
	PDT20A	123.6	0	1.6	1	Detected
Low Freq. (Dev. Board)	PRE-100A	64.2	0	0	0	Not Detected
	IRD-30A	N/A	N/A	N/A	N/A	N/A
	IC-10	N/A	N/A	N/A	N/A	N/A
	PDT20A	23.2	0	0	0	Not Detected

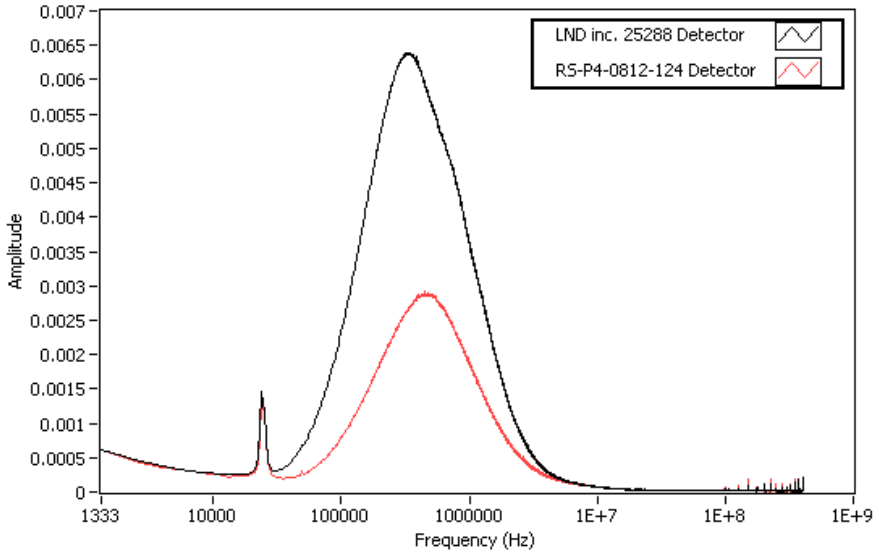

Figure 18. Pulse spectral differences for different manufactures

2.1.6 Switching of Pre-amplifier

Pre-amplifiers for each of the systems were switch with an identical pre-amplifier. Table 13 lists the serial numbers for the compared pre-amplifiers used in the experiments. It should be noted that the IRD-30A has the detector and pre-amplifier built into one component unlike the other systems that have separate pieces of hardware for the pre-amplifier and detector. The results for the IRD-30A are, therefore,

the same as those in the switching detector subsection. As before, the results ignore the disconnect that is required in order to switch a pre-amplifier.

From Table 14 it can be seen that for all of the systems, except for IC-10, pre-amplifier switching was detected. The IC-10 was detected in one particular case, but for the most part, it was not.

Table 13. Identical Pre-Amplifiers used for replacement

	Pre-Amplifier #1	Pre-Amplifier #2
PRE-100A	19059	19057
IRD-30A	14153	14151
IC-10	14159	14158
PDT20A	1127642	1127639

Table 14.Switch with Identical Pre-Amplifier

Switch Pre-Amplifier						
		%Δ Energy (Entire Spectrum)	StdEB (Entire Spectrum)	StdEB (Highest Zone)	# of Zones Detected	Notes:
High Freq.	PRE-100A	5267	12.5	13.6	4	Detected
	IRD-30A	1165	21.9	43.3	3	Detected
	IC-10	336	0	0	0	Not Detected
	PDT20A	456	2.2	9.4	8	Detected
Low Freq. (Dev. Board)	PRE-100A	1971	5.8	20.1	10	Detected
	IRD-30A	1412	27.3	66.3	7	Detected
	IC-10	300	0	0	0	Not Detected
	PDT20A	548	1.2	7.7	8	Detected

2.2 RF vs. Inherent Component (Anechoic Chamber)

Experiments were performed in an anechoic chamber to help discriminate between the sources that caused detectable events. It was suspected during several tests that the reason why certain tampering events were detected was because of regional changes that were coming from RF pickup. Some of the most common regions were in the 10-30 MHz region which was found to be caused by RF being emitted from the NGAM and 88-108 MHz from local radio stations. There were other sources of disturbances but these two where the most common. The anechoic chamber is designed to keep outside RF from penetrating into the chamber and dissipating internally produced RF once it reaches the walls which lowers the chance of reflection back towards the object being tested. In other words, it is the closest we can come to placing the internal objects in an electromagnetic vacuum. However, internally produced RF can still interfere with the object being tested. The goal of the anechoic chamber tests was to differentiate the mode of detection for the tampering scenarios between RF and inherent component caused events.

The tampering scenarios that were suspected of being detectable because of RF pickup were high impedance, identical cable replacement, removal of detector, and switching to an identical detector. It was also suspected that certain additional equipment used during tampering tests were inducing RF pickup such as clips and a BNC connecter used to attach to a cut cable or the DC block used to eliminate the 12V for a branched circuit. The tamper tests shown for this section were performed only on the PRE-100A

system due to time constraints. Baselines were, however, collected for every system for reference, with a few exceptions in the IC-10 chambers.

During the anechoic chamber tests it was discovered that the NGAM was the source for several RF induced peaks in the 10-30 MHz range. Additionally, the NGAM does produce several inherent peaks, which are a result of being attached on the same line, in the several hundred MHz range which are always present. The development boards were found to produce a small disturbance if the USB cable was attached in the 10 MHz range. Because the NGAM was a source of RF and needed to be placed inside the anechoic chamber, it was difficult to suppress the RF pickup by the cabling or object in question. However, the anechoic chamber and use of RF dissipating material made it possible to determine if the change in the spectrum was from RF pickup or the inherent component.

Two experiments were performed using a high impedance device. The first used an oscilloscope and the second used a 10Mohm resister. The 10Mohm resister was found to be very sensitive to RF pickup, and the attachment of the resister to the cable at 25m showed no proof that the detection was inherent. The attachment of the oscilloscope was still able to be detected within the anechoic chamber. However, after moving the oscilloscope around it was discovered that the oscilloscope was acting as an antenna for RF pickup, then putting that extra noise on the cable. This was shown by moving the oscilloscope to a cave built to keep out RF within the chamber where the cable was located. By moving the oscilloscope to this position, the induced noise from the oscilloscope disappeared, showing that the oscilloscope was not the source of detection but was picking up noise and putting it on the cable.

Identical cables were switched within the cave built to keep out the NGAM RF. The results showed that the only detectable difference between the identical cables was the RF pickup. Likewise, the switching of an identical detector was shown to cause RF pickup. However, it is suspected that for the PDT20A the detection of an identical detector is caused by a hysteresis effect when the detector is first removed. The removal of a detector, on the other hand, was shown to be inherently detectable. All other tampering tests were performed and confirmed to be due to inherent components and not RF pickup. Additionally, supplemental equipment such as probes used on the cut cable, a converter to BNC connector and the DC block were tested. This supplemental equipment was found to produce extra RF pickup. However, as in the DC block case, there is a capacitor which must have an inherent change besides the RF pickup but the dominate effect was the RF pickup. A summary of the RF verses inherent effects for each test are shown below.

Table 15. RF vs. Inherent Tamper Detection Mode

Tamper Event	RF	Inherent
Disconnect		X
High Impedance	X	
Low Impedance		X
Identical Cable	X	
Cable Length		X
Cable Characteristics		X
Cable Type		X
Detector Removal		X
Identical Detector	X	
Different Detector		X
Identical Pre-Amplifier		X
Supplemental Equipment (Probes, DC Block, etc.)	X	

In summary, the anechoic chamber tests were able to help discriminate RF from inherent effects that cause the tampering scenario to be detected. While the RF induced detection mode may not be very predictable, it is very beneficial because it allows for something that otherwise would be inherently undetectable to become detectable. The downside to RF pickup is that false alarms may be produced when RF sources are introduced in a location and exceed the normal variation conditions for the facility.

2.3 Industrial Facility

The equipment was moved to the Zero Power Physics Reactor Counting Laboratory (ZCL) on the Material and Fuels Complex (MFC) at INL. The ZCL was chosen as a good location to perform initial industrial facility testing because it is located next to emergency generators, the entire control system for the MFC complex, and could have sources being moved around at various points in time. Because of limited time, all of the system configurations could not be tested. The configurations listed in Table 16 were tested against the tampering scenarios listed in Table 17. The majority of the tampering scenarios were high and low impedance necessary for a record and playback event along with the necessary hardware such as a probe to attach to the cut cable, a converter to a BNC connection, and a DC Block for low impedances. The removal of the detector and disconnection of the cable were also performed.

Table 16. Configurations Tested

System	Cable	Digitizer
PRE-100A	RG-71	PXI-5772
IRD-30A	RG-71	PXI-5772
PDT20A	RG-62	PCI-U1071A
IC-10	RG-62	PCI-U1071A
IRD-30A	RG-62	PCI-U1071A
IRD-30A	RG-174	Dev. Board
PDT20A	RG-174	Dev. Board
PRE-100A	RG-174	Dev. Board

Table 17. Tampering Events

(At 25m cut)	(At 50m Tee)
Probe & Oscilloscope	3" cable & Oscilloscope
Supplemental Hardware	DC Block
50 ohms	50 ohms
75 ohms	75 ohms
93 ohms	93 ohms
330 ohms	330 ohms
1.5kohms	1.5kohms
Remove Detector	
Disconnect cable at pre-amplifier	

Table 18. Results for tampering scenarios in an industrial facility

System	PRE-100A	IRD-30A	PDT20A	IC-10	IRD-30A	IRD-30A	PDT20A	PRE-100A
Digitizer	PXI-5772	PXI-5772	PCI-U1071A	PCI-U1071A	PCI-U1071A	Dev. Board	Dev. Board	Dev. Board
(At 25m cut)								
Probe & Oscilloscope	Pass	Fail	Pass	Pass	Pass	Fail	Fail	Fail
Supplemental Hardware	Pass	Fail	Pass	Pass	Pass	Fail	Fail	Fail
50 ohms	Fail	Fail	Pass	Pass	Pass	Pass	Fail	Fail
75 ohms	Fail	Fail	Pass	Pass	Pass	Pass	Fail	Fail
93 ohms	Fail	Fail	Pass	Pass	Pass	Pass	Fail	Fail
330 ohms	Fail	Fail	Pass	Pass	Pass	Fail	Fail	Fail
1.5kohms	Fail	Fail	Pass	Pass	Pass	Fail	Fail	Fail
(At 50m Tee)								
3" cable & Oscilloscope	Fail	Fail	Pass	Fail	Pass	Fail	Fail	Fail
DC Block	Fail	Fail	Fail	Fail	Pass	Fail	Fail	Fail
50 ohms	Fail	Fail	Pass	Fail	Pass	Pass	Fail	Fail
75 ohms	Fail	Fail	Fail	Fail	Pass	Pass	Fail	Fail
93 ohms	Fail	Fail	Fail	Fail	Pass	Pass	Fail	Fail
330 ohms	Fail	Fail	Fail	Fail	Pass	Fail	Fail	Fail
1.5kohms	Fail	Fail	Fail	Fail	Pass	Fail	Fail	Fail
Detector Removal	Fail	Fail	Fail	Fail	Pass	Pass	Pass	Fail
Disconnect	Fail	Fail	Pass	Fail	Pass	Pass	Fail	Pass

In Table 18, a “pass” score means that the tampering event was detected, while a “fail” score means the event was undetected.

The results from Table 18 were not very encouraging considering that disconnect was not detected for several configurations. Further, it is rather odd that the PRE-100A on the PXI-5772 digitizer was able to detect the high impedance device but was not able to detect the low impedances. When the spectrum was observed visually it was obvious when the low impedances and disconnect had occurred. However, the approach to distinguish the event had failed to detect these large spectral changes even compared to the normal variations within the spectrum. Figures 19-20 show the PRE-100A spectra during the 50ohms and disconnect scenarios compared to the normal PRE-100A spectrum. The conclusions reached for the PRE-100A and PXI-5772 were found to also extend to the IRD-30A and PXI-5772 because easily identifiable changes in the spectrum could be observed as well but the software was unable to detect the event. It was believed that the method of determining a tampering event was to blame and was revisited because of the clear visual indicators. The IRD-30A and PCI-U1071A digitizer case was opposite to the results using the PXI-5772 digitizer and showed that high frequency information could detect every event but differed based on the digitizer.

The rest of the results were not entirely that surprising. It was expected that the performance of most systems would deteriorate because of added noise from the surrounding environment. The PDT20A and IC-10 were not expected to do well for either low or high frequencies, given that these two systems have little electrical energy within their spectra and the results from the laboratory experiments tended to be near the detection boundary. The IRD-30A at low frequencies performed just as expected, with detection of low impedances but no detection of high impedances. The low frequency results were very poor for the PDT20A and PRE-100A.

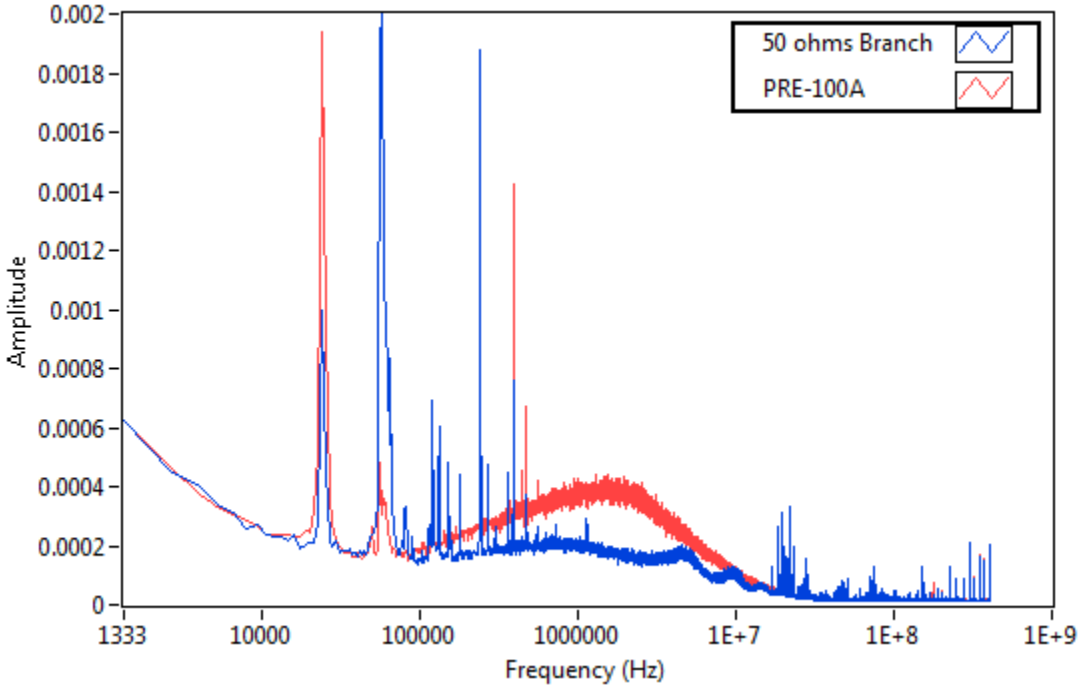

Figure 19. Comparison of the spectra between a 50 ohm branch and normal

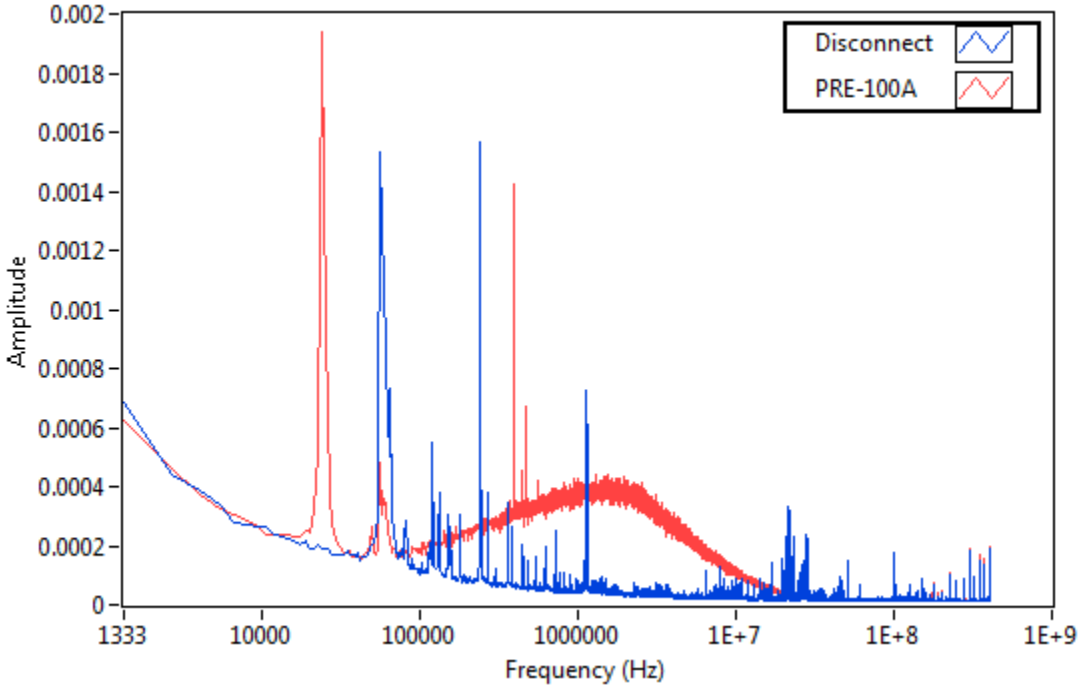

Figure 20. Comparison between disconnect and the normal spectrum

Modifications to the software were performed to determine if changes in the results would occur. The modifications included changing the number of zones from 10 to 20 and using logarithmically spaced zones for high frequencies. The development board does not lend itself to logarithmically spaced zones and a linear spacing was kept. Tables 19-20 show the results after the modifications were made to the software.

The high frequency spectra data showed an improvement using logarithmically spaced data compared to the linear spaced data. Comparison between Table 19 and Table 18 shows an added detectability for every system. The PDT-20A was the only system to lose detection of any event (oscilloscope at 50m) while gaining detection of other events. The major added improvement was that every system was able to detect low impedance branching and disconnect.

The low frequency analysis method changed the number of zones from 10 to 20, while keeping the zones linearly spaced. The changes between Table 20 and Table 18 showed improvement for the PRE-100A, detection of disconnect for the PDT20A, and no change for the IRD-30A.

Table 19. High Frequency, Logarithmically Spaced Zones (20 Zones)

System	PRE-100A	IRD-30A	PDT20A	IC-10	IRD-30A
Digitizer	PXI-5772	PXI-5772	PCI-U1071A	PCI-U1071A	PCI-U1071A
(At 25m cut)					
Probe & Oscilloscope	Pass	Fail	Pass	Pass	Pass
Supplemental Hardware	Pass	Fail	Pass	Pass	Pass
50 ohms	Pass	Pass	Pass	Pass	Pass
75 ohms	Pass	Pass	Pass	Pass	Pass
93 ohms	Pass	Pass	Pass	Pass	Pass
330 ohms	Fail	Fail	Pass	Pass	Pass
1.5kohms	Fail	Fail	Pass	Pass	Pass
(At 50m Tee)					
3" cable & Oscilloscope	Fail	Fail	Fail	Fail	Pass
DC Block	Fail	Fail	Fail	Fail	Pass
50 ohms	Pass	Pass	Pass	Fail	Pass
75 ohms	Pass	Pass	Pass	Fail	Pass
93 ohms	Pass	Pass	Pass	Fail	Pass
330 ohms	Pass	Fail	Fail	Pass	Pass
1.5kohms	Fail	Fail	Fail	Pass	Pass
Detector Removal	Fail	Fail	Fail	Fail	Pass
Disconnect	Pass	Pass	Pass	Pass	Pass

Table 20. Low Frequency, Linear Spaced Zones (20 Zones)

System	IRD-30A	PDT20A	PRE-100A
Digitizer	Dev. Board	Dev. Board	Dev. Board
(At 25m cut)			
Probe & Oscilloscope	Fail	Fail	Fail
Supplemental Hardware	Fail	Fail	Fail
50 ohms	Pass	Fail	Pass
75 ohms	Pass	Fail	Pass
93 ohms	Pass	Fail	Pass
330 ohms	Fail	Fail	Pass

System	IRD-30A	PDT20A	PRE-100A
Digitizer	Dev. Board	Dev. Board	Dev. Board
1.5kohms	Fail	Fail	Fail
(At 50m Tee)			
3" cable & Oscilloscope	Fail	Fail	Fail
DC Block	Fail	Fail	Fail
50 ohms	Pass	Fail	Pass
75 ohms	Pass	Fail	Pass
93 ohms	Pass	Fail	Pass
330 ohms	Fail	Fail	Fail
1.5kohms	Fail	Fail	Fail
Detector Removal	Pass	Pass	Fail
Disconnect	Pass	Pass	Pass

The industrial facility experiments were able to show a certain level of tamper detection with reduced quality as compared to laboratory experiments. The algorithm for detecting tamper events was called into question and was revisited since it was unable to detect clear changes to the spectral shape. The changes to the algorithm allowed several events to be detected that were not detected by the previous algorithm for analysis. The changes to the algorithm included increasing the number of zones and changing to logarithmic spacing for high frequency data. With the changes to the algorithm it was possible to detect low impedances for high frequencies in every system and disconnect was detected for every system and frequency region. The digitizer was also shown to have an effect on the tamper indication results.

3. CONCLUSIONS

The work performed for FY-15 consisted of performing various tampering scenarios, comparison of tampering scenarios with different cables, comparison of RF and inherent component effects, and testing in an industrial environment. These tests were performed with four different pre-amplifier/detector combinations which were powered by two different safeguards modules. The noise spectrum was primarily analyzed but some data included the pulse spectrum. The noise spectrum was obtained using three different digitizer types. Two digitizers were used for high frequencies and one was used for low frequencies.

The laboratory tampering tests showed that it was possible to detect a disconnect of a cable; both the recording and playback (i.e., high and low impedance) of the signal with varying detectability based on distance; various cable changes such as length, attenuation and cable type; the disconnection of a detector; and the switching of hardware such as the detector and pre-amplifier. The detectability of each scenario varied based on the safeguards equipment and the digitizer/frequency region being used. Comparison of tampering tests between three cable types (RG-174, RG-62, and RG-71) showed minimal difference in results unless the result was dependent on the cable attenuation properties.

The anechoic chamber tests were performed to determine whether a tampering event was detected because of inherent or RF effects. The tests showed that high impedances, switching of identical cables, switching of identical detectors, and various supplemental equipment used in a tampering event were detected because of RF induced effects.

Industrial facility tests showed a lowered level of detectability when compared to the laboratory testing due to increased fluctuations in the noise levels. Several systems were able to detect disconnection of the cable, high impedance devices used for recording of a signal, low impedances for playing back the signal, and the removal of the detector. The detectability varied based on the system and digitizer used. The only tampering event to be detected by every digitizer and system was disconnection of the cable, after modifications were made to the analysis software. It was clear from visual inspection of the spectrum that certain tampering events were present and should have been detected but were not, for this purpose the software was modified. The new analysis software allowed for an improvement in the detectability of tampering events.

No further work is expected to continue on this project for FY-16. However, in closing it should be important to summarize the major advantages and disadvantages of the frequency analysis technique for future projects.

Advantages

1) Perform noise and pulse authentication
    a. Useful to detect modifications to the pulse, such as RF, capacitive, and inductive induced pulses which do not require tampering with the cable
2) Observe changes to equipment
3) Observe deviations to equipment that are located beyond the pre-amplifier and are considered to be hidden electrically
4) Ability to detect electrically identical devices/parts because of differences in RF pickup
5) Ability to detect high impedance because of RF pickup from the device and the possibility to detect added noise from the device's internal hardware
6) Ability to detect changes to facility temperature and RF modifications

Disadvantages

1) Detection ability is limited by energy content within the spectrum
    a. Induced SSTDR or other active sources should improve results
2) RF pickup is not easily predicted and susceptible to varying industrial conditions

REFERENCES

1. L. E. Smith, P. Ramuhali, D. Sheen, J. Tedeschi, R. Conrad, K. Ianakiev, M. Brown, J. Svoboda, J. West, J.Sanders, "Detection of Physical Intrusion in the Cabling of Unattended Safeguards Instruments: Preliminary Requirements and Evaluation Scenarios," Sep 2014. (PNNL-SA-23749)

2. L.E. Smith, J. Svoboda, K. Ianakiev, R. Conrad, S. Morris, P. Ramuhalli, D. Sheen, J. Tedeschi, M. Schanfein, B. Baker, J. West, M. Iliev, M. Newell, M. Brown, "Front-end Electronics for Validation Measurements: Performance Evaluation and Viability of Advanced Tamper Indication Measures," Symposium on International Safeguards: Linking Strategy, Implementation and People. Vienna Austria, Oct 20-24, 2014. (INL/MIS-14-33231, Idaho National Laboratory, 2014)

3. Proakis J. and Manolakis D., Digital Signal Processing: Principles, Algorithms, and Applications, Pearson 4th Edition 2007.

4. 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.