Setting the Tuning Parameters

Application Note

Fiber SenSys, Inc. (FSI)
2925 NE Aloclek Dr.
Suite 120
Hillsboro, OR 97124
USA

Tel: 1-503-692-4430
Fax: 1-503-692-4410
info@fibersensys.com
www.fibersensys.com

Contents

Introduction

There are two crucial objectives in calibrating a Fiber SenSys Alarm Processing Unit (APU): detecting intruders and preventing nuisance alarms. To achieve these two objectives, Fiber SenSys has developed sophisticated digital signal processing algorithms that make it possible to calibrate an APU for nearly any situation.

This document provides detailed information about the parameters available for calibrating Fiber SenSys APUs, in addition to step-by-step instructions on how to calibrate a detection zone. This calibration process applies to chain link fence applications with the objective of capturing climb and cut intrusions, though the principals can be applied to other mediums. This process is intended for calibration of FD300 (excluding FD322) and FD500 series APUs, which utilize *SpectraView* and *500 Series Suite* software, respectively.

Though this document is intended to be comprehensive, some APUs may not support all the tuning parameters explored in this document. See the appropriate user's manual for a comprehensive list of the parameters supported by each APU.

This document assumes the user has a working knowledge of the appropriate software and Fiber SenSys products. Contact Fiber SenSys Technical Support at (503) 726-4455 or support@fibersensys.com for additional information.

1. Calibration Fundamentals

Timing: Calibration of the APU should occur after installation of the system and before the system is commissioned.

Resources: It is estimated that it will take a trained technician approximately one hour to calibrate each zone. Each sensing zone is calibrated individually. Calibration requires a minimum of two people, one to operate the software and another to simulate intrusions. Expect to simulate a minimum of ten intrusions of each classification (typically climb and cut) per detection zone.

Intruder Profiling: An intruder profile should be established prior to calibration. It is critical that intrusion simulations imitate the profiled intrusions, to the best of the tester's ability, to ensure optimal performance of the system. In all applications, this means selecting a climb tester who best models the profiled intruder (weight, height, agility, attire). For simulating intrusions on chain link fencing, intrusion simulations typically involve climbing to a height such that the tester's waist is level with the top of the fence mesh and jumping off to conclude the simulation.

Threshold: Threshold refers to the cumulative effect that all parameters have on detection. Threshold is *not* a parameter in and of itself. Properly defining the alarm threshold by following the process below is key to minimizing optimizing detection and minimizing nuisance alarms.

Safety: Measures should be taken to ensure the safety of the climb tester. Protective gloves should be worn and fall protection should be in place as per site rules, regulations, and fence height require. Some sites may require a safety spotter as a precaution. There is no alternative to climbing the fence for calibration of an APU.

2. Defining Parameters

Detection algorithms in Fiber SenSys APUs contain a variety of user-defined parameters that are analyzed using two signal processors (P1 and P2). Each of these processors is targeted at capturing one of the two following intrusion classifications:

Processor 1 (P1) - Long duration, low frequency, low amplitude (e.g., climb intrusion)
Processor 2 (P2) - Short duration, high frequency, high amplitude (e.g., cut intrusion)

By separating intrusion signals into two classifications and processing each individually, the system will have a reduced Nuisance Alarm Rate (NAR).

2.1. Signal Processing

2.1.1. Sensitivity

Sensitivity acts as a raw signal amplifier, increasing signal size incrementally with each point added. This is the *only* parameter that will produce a visible change in the *RealTime* signal. Figure 1 below displays the visual signal change with a variation in **Sensitivity**.

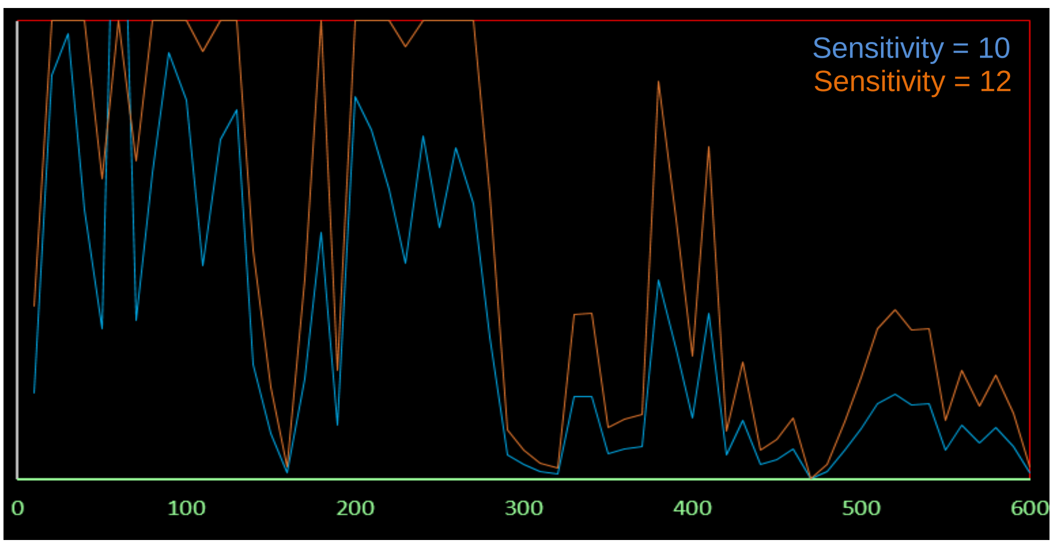

Figure 1 – Amplification of the signal by adjusting Sensitivity from 10 to 12

2.1.2. Lowest and Highest Frequency (Lo and Hi Freq)

Filters define the frequency range in which the signal will be processed. Any signal outside the defined range will be ignored during signal processing. For example, setting a **Low Frequency** of 200Hz and a **High Frequency** of 600Hz will cause the unit to process data only in the 200-600Hz range. Frequency filters help differentiate detection between P1 and P2 and aid in preventing nuisance alarms.

2.1.3. Duration of Signal (Duration)

Duration determines the length of time a signal must last to generate as an event. **Duration** helps distinguish intruders from nuisance signals and differentiates detection of the two intrusion classifications. Figure 2 displays the interaction between the threshold and **Duration**.

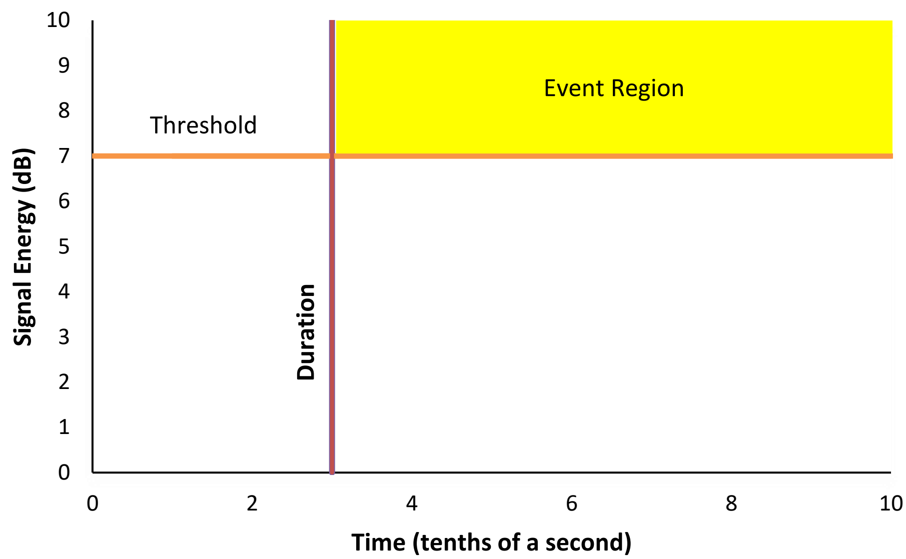

Figure 2 – Duration and threshold define event qualifying signals

2.1.4. Gain

Gain adjusts the threshold for both processors. Increasing **Gain** lowers the threshold and will make the processor more likely to generate an event. **Gain** affects both Processor 1 and Processor 2. **Gain** is inversely proportional to **Level of Signal**.

2.1.5. Level of Signal (Signal)

Level of Signal adjusts the threshold for each signal processor individually. Only the signal that exceeds the **Level of Signal** amplitude will contribute to creating an event and alarm. Lowering **Level of Signal** will make the system more likely to generate an alarm. **Level of Signal** affects each processor individually. **Level of Signal** is inversely proportional to Gain.

2.1.6. Low Level Tolerance (Tolerance)

The **Low Level Tolerance** parameter decreases the threshold at the expense of increasing the **Duration** required to generate an event. This parameter is primarily used for detection of stealthy intrusions (long duration and low amplitude climbs). If the signal is *lower* than the threshold by *more* than **Low Level Tolerance**, it cannot generate an event, regardless of how long it lasts. Figure 4 depicts the additional event region added by the relation between **Tolerance**, **Duration**, and threshold.

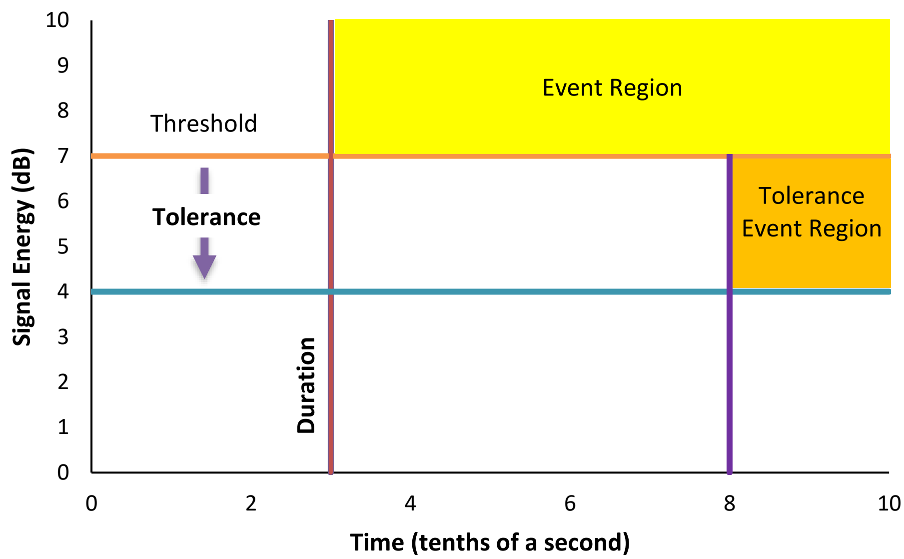

Figure 3 – Threshold, Duration, and Low Level Tolerance diagram

2.2. Alarm Processing

2.2.1. Event Count (Event Cnt)

Event Count defines the number of events required to generate an alarm. **Event Count** is one of the best ways to differentiate an intruder from nuisance sources. For example, an intruder cutting through a fence will create periodic signals as they cut through each chain link and generate events. This periodic signal characteristic is rarely present in nuisance sources.

2.2.2. Event Mask Time (Event Msk)

Event Mask Time defines a brief period of time (after an event) in which signal is rejected. This prevents multiple events from occurring from a single high-energy impact.

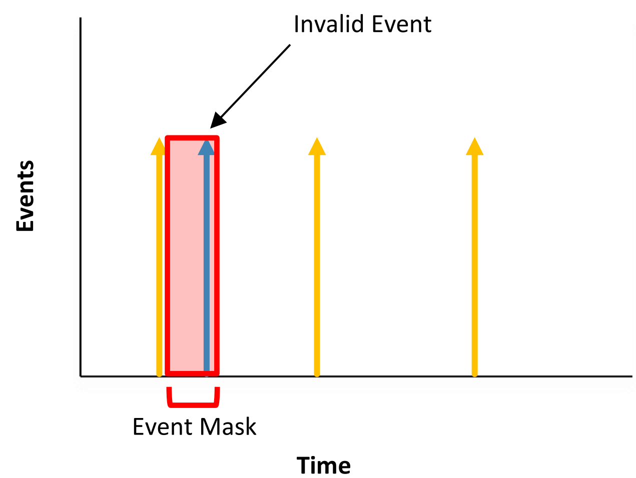

Figure 4 – Event mask time prevents excessive events from being generated

2.2.3. Event Window (Event Win)

Event Window is the maximum amount of time that can exist between events before the **Event Count** resets. When an event occurs, the **Event Window** timer is initialized. If another event occurs within the timer, the **Event Count** is incremented by one and the timer reinitiates. If an event does not occur within the window, the **Event Count** is reset to zero. If the number of events reaches **Event Count**, an alarm is generated. Figure 5 displays the interaction between **Event Window** and **Event Count** for the generation of alarms.

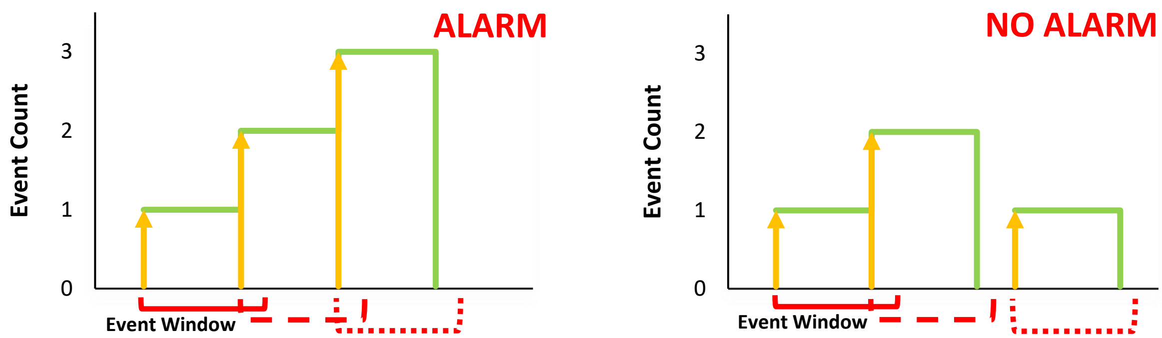

Figure 5 – Event Window interacting with Event Count

2.3. Nuisance Signal Processing

2.3.1. Wind Rejection (Wind Reject)

The **Wind Rejection** algorithm monitors the noise floor and dynamically adjusts **Gain** to prevent nuisance alarms. The **Wind Rejection** value defines the speed and amplitude at which the algorithm acts. Figure 6 shows a representation of **Gain** reduction in the presence of wind.

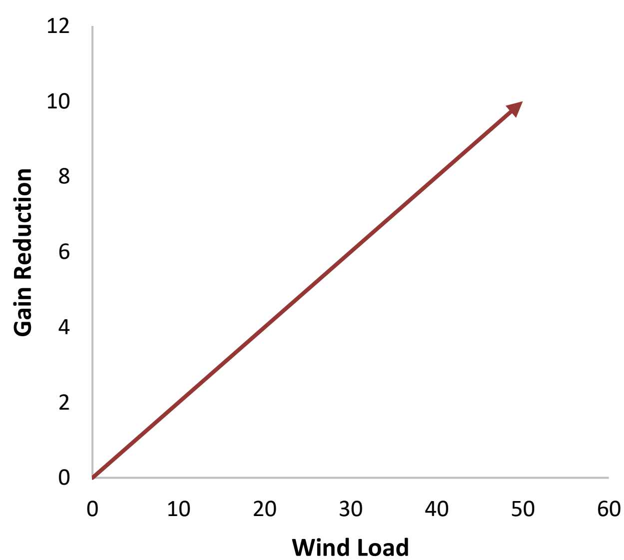

Figure 6 – Wind Rejection Software reduces Gain as Wind Load increases

2.3.2. Comb Reject (Filter)

The **Comb Reject** filter eliminates the user-defined frequency and all harmonics (multiples) of that frequency (+/-5Hz). For example, setting **Comb Reject** to 60Hz in *SpectraView* will filter out the signal at 55-65Hz, 115-125Hz, 175-185Hz, etc. In the *500 Series Suite,* the user can enter the *Filter* tab and select the individual harmonic frequencies to filter the signal out. This parameter is particularly helpful when a source generates specific frequencies, such as a fan, compressor, or power lines. This parameter will affect signal processing but will *not* visibly change the signal appearance on the screen. Figure 7 shows a sample nuisance source with a harmonic frequency response.

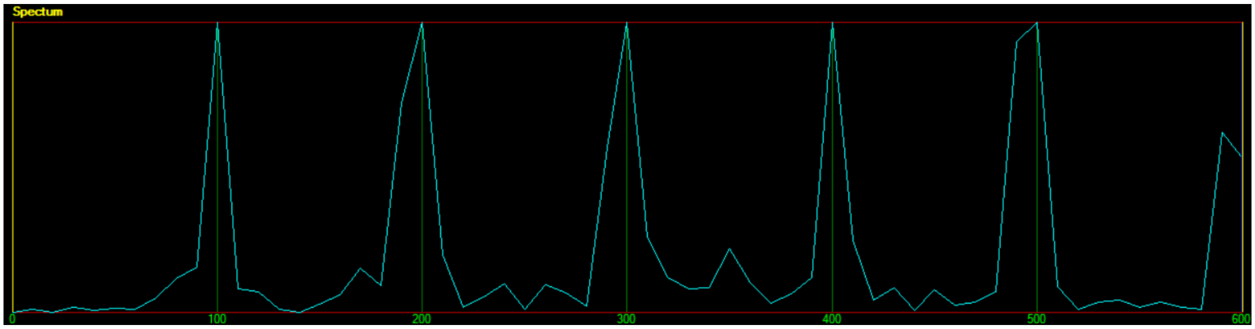

Figure 7 – Nuisance source generating harmonic frequencies of 100Hz

3. Calibration Procedure

This section provides detailed step-by-step instructions on how to calibrate an APU. This is a basic tuning guide and does not account for unique scenarios or in-depth calibration methods to reject nuisance alarms. This calibration process applies to chain link fence applications with the objective of capturing climb and cut intrusions, though the principals can be applied to other mediums. *The recommended process and settings are subject to variation caused by system response and parameter dependency.*

3.1. Adjust Signal Size

Objective: The objective in setting signal size is to receive an ideal amount of signal to allow for optimal processing. This is done with the **Sensitivity** parameter. If **Sensitivity** is too low or too high, the signal may become indiscernible from the baseline noise and nuisance sources. The target saturation point with an optimal **Sensitivity** setting is ~200Hz.

Process: In *RealTime*, watch and record the climb tester performing a simulated intrusion. Open the spectral recording in *Replay.* Drag the cursor control buttons together in the *Acoustic Power vs Time* graph. Right-click to drag both cursor control buttons at once and move them back and forth while looking for the *highest* frequency where the signal commonly saturates (full scale/reaches top of graph) in the *Spectrum* graph. Adjustments to **Sensitivity** should be made 1-2 points at a time to until the target average saturation point of ~200Hz is reached. **Sensitivity** should not be raised to a point where the noise floor is visible in calm weather.

Examples: Figure 8 displays signal with saturation up to ~270Hz. This signal is too large. **Sensitivity** should be decreased to bring the point of common saturation to the target value.

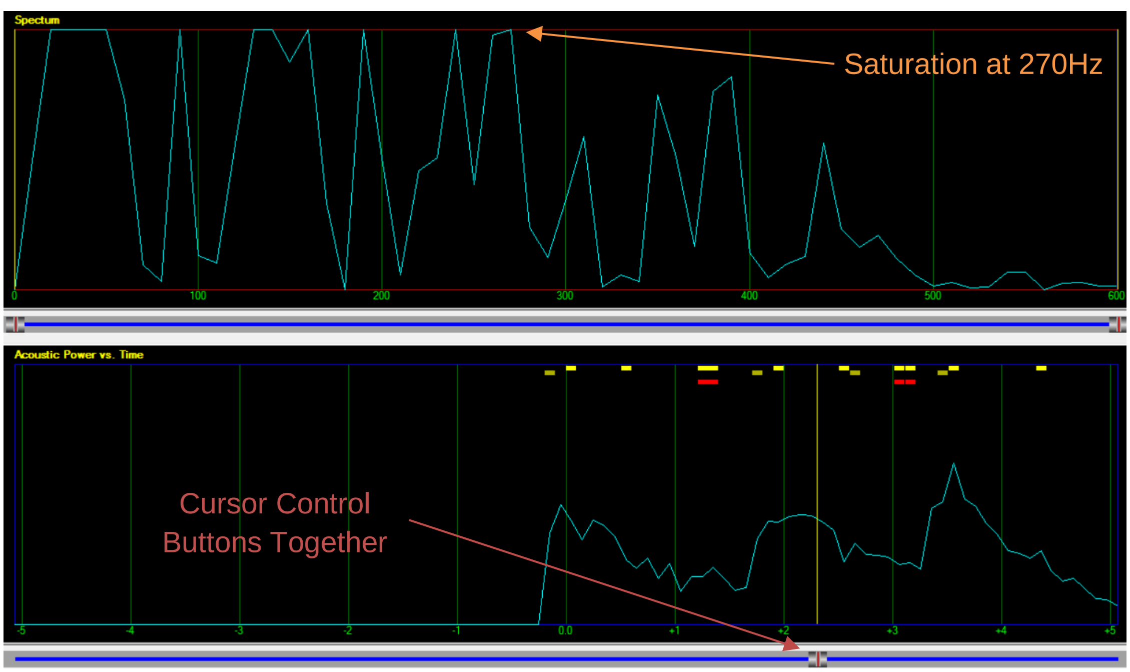

Figure 8 – Intrusion signal with saturation up to 270Hz

Figure 9 shows signal from a fence that is inherently insensitive. At the point of the largest signal, it reaches saturation up to only 140Hz. **Sensitivity** for this system needs to be increased to reach the target value of signal saturation.

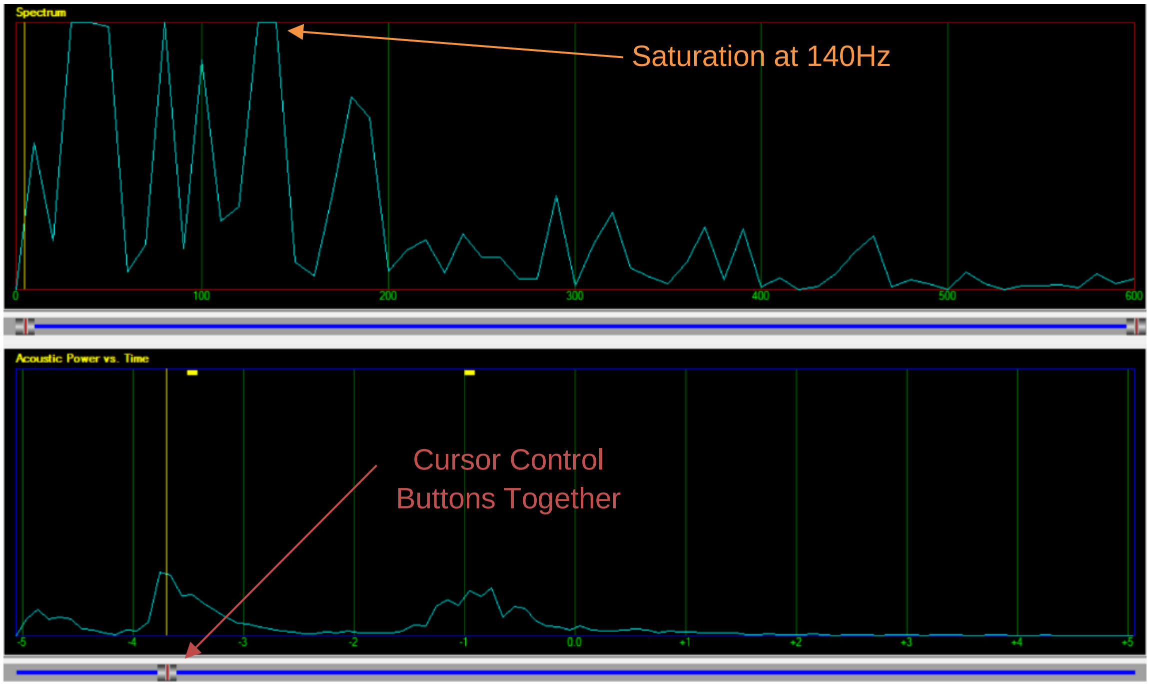

Figure 9 – Intrusion signal with saturation up to 140Hz

3.2. Frequency Filters

Objective: The objective in setting the frequency filters is to remove frequencies of common nuisance sources from signal processing. Nuisance sources typically exist between 0-200Hz whereas intrusion signals have a diverse frequency response. A typical **Low Frequency** setting is 200Hz for Processor 1 and 300Hz for Processor 2.

Highest Frequency should be left at the default value of 600 except in unique circumstances that require advanced tuning techniques. Nuisance sources rarely exist in the high-frequency range, and these frequencies are critical for capturing intruders.

Process: Perform a simulated climb intrusion and open the recording in *Replay* mode. Drag the cursor control buttons together in the *Acoustic Power vs Time* graph. Move the cursor control buttons back and forth and observe the *highest* frequency where the signal commonly saturates in the *Spectrum* graph (same process as in 3.1). This value will become the **Low Frequency** for Processor 1 and should be near the target value of 200Hz. If the value deviates significantly from the target value, **Sensitivity** may need to be adjusted.

Perform a simulated cut intrusion and open the recording in *Replay* mode. Drag the cursor control buttons together in the *Acoustic Power vs Time* graph. Move the cursor control buttons back and forth and observe the *highest* frequency where the signal commonly saturates in the *Spectrum* graph. This value will become the **Low Frequency** for Processor 2. Deviations from the target value for P2 are common since **Sensitivity** is set according to climb intrusions.

Examples: Figure 10 displays the spectral signal of a climb with saturation around 200Hz. This point of saturation should be compared to the remainder of the signal. Presuming the remainder of the signal has a similar response, an appropriate **Low Frequency** setting would be 200Hz.

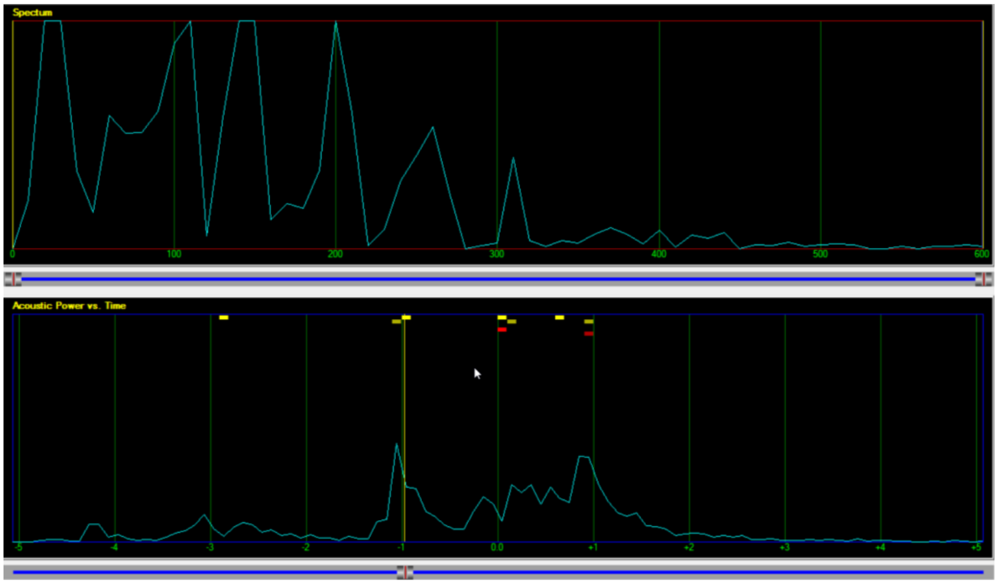

Figure 10 – Intrusion signal has saturation at ~200Hz

Figure 11 shows a cut file where the signal saturates at 400Hz. An appropriate **Low Frequency** setting would be 400Hz in this scenario.

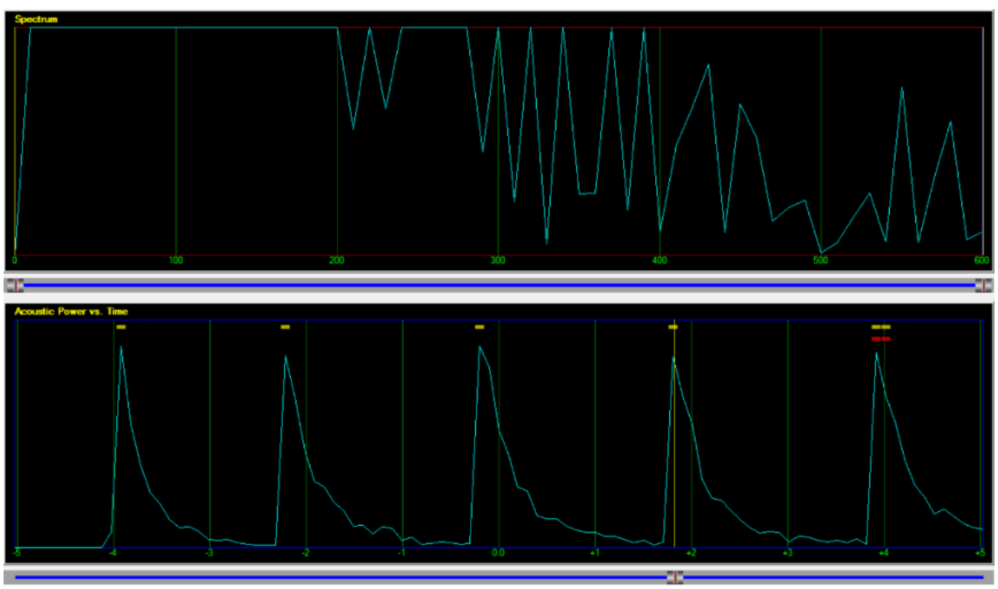

Figure 11 – Intrusion signal saturation at ~400Hz

3.3. Duration

Objective: The objective in setting the **Duration** is to reduce nuisance alarms by isolating the two different intrusion classifications on Processor 1 and Processor 2. Typical **Duration** values for Processor 1 are 3 to 5 (.3s to .5s respectively). Processor 2 **Duration** should always be set to the default value of 1 (.1s).

<u>Process</u>: Perform a simulated cut intrusion and open the recording in *Replay* mode. Drag the cursor control buttons to the start and end of the signal in the *Acoustic Power vs Time* and observe the time that the peak signal lasts. Add .1s to the value (this allows for filtering of the two intrusion classifications). This value will become the **Duration** for Processor 1.

<u>Examples</u>: Figure 12 shows a series of three cut simulations with an alarm on Processor 1 and Processor 2 (prior to **Duration** adjustment, both processors often receive an alarm from cut simulations). The cursor control buttons indicate a length from start to finish (signal decline) of ~.3s. An appropriate **Duration** value in this scenario is 4 (value is in tenths of a second).

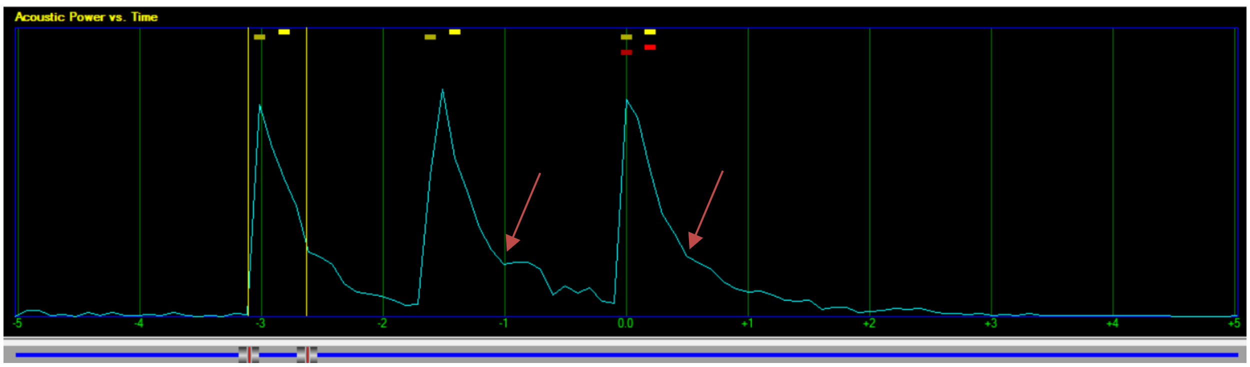

Figure 12 – Arrows indicate signal decline for measuring Duration

Figure 13 below shows a series of three cut simulations with an alarm only on Processor 2. The **Duration** on Processor 1 has caused it to filter out simulated cut intrusions.

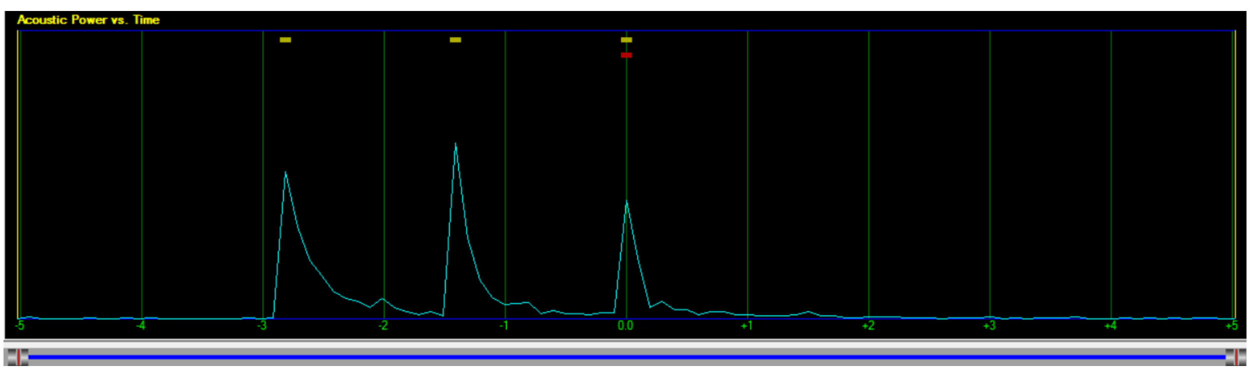

Figure 13 – Cut simulation generates alarm only on P2

3.4. Level of Signal and Gain

<u>Objective</u>: Prior to this point, each parameter adjustment has conditioned the signal for optimal signal processing. The objective in setting **Level of Signal** and/or **Gain** is detection – once set, the system should detect all simulated intrusions while being as minimally sensitive as possible to avoid nuisance alarms. This step is termed *GainLev* because **Gain** and **Level of Signal** settings are inversely proportional and together help define the threshold. *Appropriate*

parameter values may vary significantly because detection is highly dependent upon adjustments made in the previous steps and the system response.

For ease of use, it is recommended that **Gain** is left at default and adjustments be made only to **Level of Signal**. Unique scenarios in which Processor 1 and Processor 2 have very different signal amplitudes may require **Gain** *and* **Level of Signal** to be increased to allow for better threshold resolution. If the steps below are followed and **Level of Signal** reaches a value of 2 or lower, follow section 4.1 for adjusting **Gain** or contact Fiber SenSys Technical Support for assistance with this step of calibration.

Process: Perform a simulated climb intrusion and watch the *RealTime* mode for yellow (event) and red (alarm) flashes (or indicators at the top of the screen). If you received an alarm, the system is already detecting but may be too sensitive. **Level of Signal** should be increased by 1-2 points on Processor 1 incrementally until a simulated intrusion is *not* captured. Next, adjust **Level of Signal** back to the setting where the simulations were detected consistently. Continue testing in various locations to ensure detection throughout the sensing zone.

If an alarm was not received initially, the system is not sensitive enough and **Level of Signal** should be decreased by 1-2 points on Processor 1 incrementally until the simulated intrusions are captured consistently. Continue testing in various locations to ensure detection throughout the sensing zone.

Perform the same procedure for Processor 2 with simulated cut intrusions. Confirm detection throughout the sensing zone by testing in various locations.

Examples: Figure 14 shows a system that is overly sensitive and received two alarms on Processor 1 from a *single* simulated intrusion. **Level of Signal** should be increased until the system is consistently capturing with just one alarm on Processor 1 from the simulated intrusion (and minimal additional events).

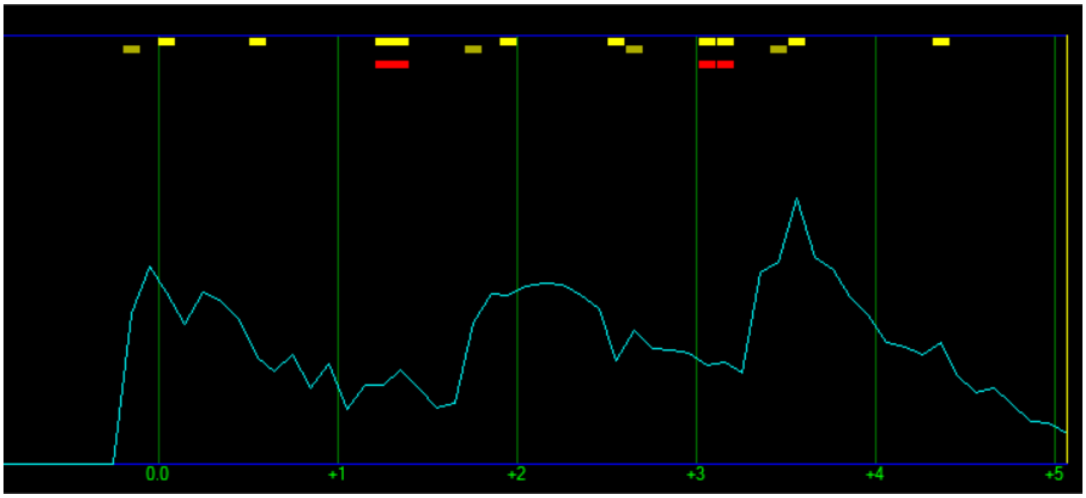

Figure 14 – Climb file of system that is overly sensitive

3.5. Wind Rejection Software

Wind Rejection is enabled by default with a value of 50 and should not be disabled unless using an anemometer (optional for FD331 and FD332 only). For locations experiencing high winds, it is recommended that **Wind Rejection** is set to 60 *prior* to intrusion testing. If nuisance alarms from wind persist, this value can be increased incrementally up to 65. It is not recommended this be set to a higher value without consulting FSI Technical Support.

3.6. Other Parameters

It is recommended that all parameters not outlined in the Calibration Procedure above be left at default for standard system calibration. Experienced and trained technicians can refer to Section 4, Advanced Calibration Methods, for additional calibration techniques. Contact FSI Technical Support for additional information.

3.7. Maintenance

Any adjustments made to the system (e.g., parameter change or fiber repair) warrant manual testing of the system to ensure detection. See document <u>PI-SM-516 Periodic Preventative Maintenance Tech Tip</u> for additional information on general system maintenance.

4. Advanced Calibration Methods

This section provides guidelines for the use of advanced tuning parameters not outlined in Section 3, Calibration Procedure, above. The methods below require in-depth knowledge of Fiber SenSys products and extensive calibration experience, in combination with well-educated decision making. It is strongly advised that new users not attempt to calibrate using the methods below. These methods are explored because they can positively influence the system performance when used properly. *The recommended applications and processes below are subject to variation caused by system response and parameter dependency.*

Many of the processes below are targeted at detection of stealthy intrusions. While it is well within the scope of the Fiber Defender® product line to detect stealthy intrusions, improperly calibrating a system to detect such signals may result in an excessively sensitive system with an elevated NAR. Failing to follow Fiber SenSys recommendations for intrusion simulations and calibration may also result in an elevated NAR. Contact FSI Technical Support for additional information.

4.1. Gain

Objective: The objective in adjusting **Gain** is to increase the resolution of the threshold during the *Level of Signal and Gain* phase of Section 3, Calibration Procedure, above.

Process: If the system requires a very low **Level of Signal** setting (2 or lower) for detection, there is a risk of making the system overly sensitive. Rather than just lowering **Level of Signal**, **Gain** should also be adjusted to improve the resolution of the threshold. Increase **Gain** by 5 points and **Level of Signal** on P1 and P2 by 5 points (**Gain** affects both processors whereas **Level of Signal** affects each individually). This modification causes no net threshold change and only serves to improve the resolution of the threshold. Once the adjustments have been made, continue adjusting **Level of Signal** according to the procedure in Section 3.4. If needed, perform the same **Gain** and **Level of Signal** increase until the desired results are obtained.

Examples: This adjustment typically occurs with fencing that is inherently insensitive or for detecting stealthy intrusions. The threshold must be refined in each of these scenarios to minimize nuisance alarms and optimize detection.

4.2. Low Level Tolerance

Objective: Effectively setting **Low Level Tolerance** may raise Probability of Detection (PD) for stealthy intruders. While optimal for detection of stealthy intrusions, raising the **Low Level Tolerance** excessively may negatively impact the NAR. It is recommended that **Low Level Tolerance** not be raised above a value of 7 without contacting Fiber SenSys Technical Support.

Process: Calibrate the system using **Level of Signal** for standard climb simulations by following the Calibration Procedure outlined above. Next, simulate stealthy climb intrusions and increase **Low Level Tolerance** in one point increments until simulated intrusions are consistently captured.

Examples: This parameter is typically adjusted when attempting to capture stealthy intrusions. This parameter decreases the threshold at the expense of a longer required signal duration, allowing for efficient capture of stealthy intrusions while minimizing impact of large amplitude nuisance sources on system performance.

4.3. Comb Reject

Objective: The objective in setting the **Comb Reject** is to eliminate nuisance alarms from sources with a harmonic frequency response.

Process: Observe the nuisance source's signal response in *RealTime* mode or a recorded file in *Replay* mode. Observe the frequency response and identify the fundamental frequency. Set **Comb Reject** to the fundamental frequency to also filter all harmonics. In the *500 Series Suite,* the user can enter the *Filter* tab and select the individual frequencies to filter the signal out.

Examples: This parameter is most commonly used with harmonic frequency responses from electrical equipment. Common culprits are AC power with harmonics of 50-60Hz and HVAC systems at 60Hz. The figure below shows harmonic frequencies at 100Hz intervals, so the fundamental frequency can be identified as 100Hz. The filter should be set to 100Hz to remove the signal from processing.

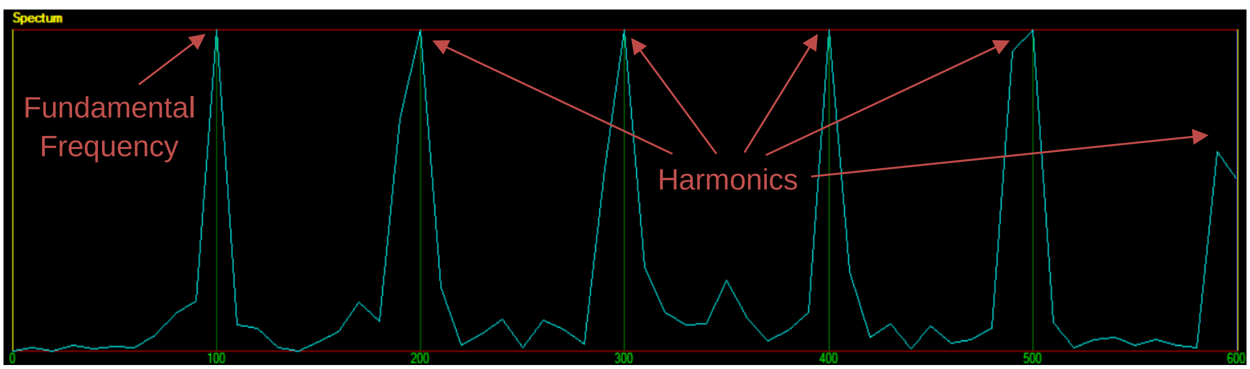

Figure 15 – 100Hz harmonic frequency response

4.4. High Frequency

Objective: The objective in modifying the **High Frequency** would typically be to eliminate nuisance sources or more effectively isolate the two intrusion classifications.

Process: For eliminating nuisance alarms, a high frequency nuisance signal should be observed in *RealTime* or *Replay* mode. Similar to setting the **Low Frequency** in the Calibration Procedure above (Section 3.2), the user should identify an appropriate frequency where the signal will be removed from processing. This value will become the **High Frequency**.

Alternatively, if the user is struggling with isolating the two intrusion classifications, this parameter can be used to select bands of frequency to process the signal. For example, the user may identify P1 to receive good signal between 200Hz and 320Hz and P2 between 350Hz and 450Hz. These values would become the **Low** and **High Frequency** on P1 and P2, respectively.

Examples: This technique is most commonly used with very sensitive installations prone to nuisance alarms caused by large signal responses. Use of this parameter in such a scenario may assist in eliminating overlap in signal processing and reduce nuisance alarms.

4.5. Event Count

Objective: The objective of changing the **Event Count** is to make the system alarm when variations to the recommended intrusion simulations are made. It is strongly recommended that users not change **Event Count** to a value below 3 as this will negatively influence the NAR.

Process: Adjust **Event Count** to the desired value. Confirm detection and continue calibration using the standard procedure above.

Examples: This value is typically only decreased on Processor 2 for high-security installations that require **Event Count** to be set at 3.

4.6. Event Window

Objective: Adjustments to the **Event Window** are made to ensure an intrusion signal is generating the appropriate number of events (on the correct processor) within the set time frame to generate an alarm.

Process: If a simulated intrusion signal contains the appropriate number of events but does not receive an alarm, increase **Event Window** in .5s increments until alarms are consistently generated from simulated intrusions with the appropriate quantity of events.

Examples: Typical climb intrusions last 3 to 5s, however tall fences requiring a longer climb or stealthy intrusions may generate signal upwards of 10s in length. Long duration signals in these scenarios may require an increased **Event Window** for optimal detection settings. High-security installations may also adjust this parameter to ensure that highly knowledgeable intruders do not wait out the **Event Window** to bypass the system.

4.7. Mask Time

Objective: The objective in changing the **Mask Time** would be to ensure only one event occurs per single high amplitude intrusion signal.

Process: **Mask Time** should be increased by .1s incrementally until a single high energy impact receives only a single event. Avoid increasing **Mask Time** by greater than .2s to avoid an impact on Probability of Detection.

Examples: This parameter is most often adjusted with very sensitive installations and fence types prone to oscillation, such as a chain link fence with minimally tensioned mesh. For example, a single simulated cut may generate two events consistently on a loose section of fencing, regardless of threshold settings. **Mask Time** could be used to prevent this.

For more information, please contact us at:
info@fibersensys.com
Tel: +1(503) 692-4430
Toll free (US) +1(800) 641-8150
www.fibersensys.com

High Performance - High Reliability - High Security