ATHENA POWER, INC.

Cyber Security Detection at the Edge of the Grid

Mel Gehrs, Principal Investigator

Athena Power Inc. | 1240 4th St. NE, Suite 416, Washington, DC, 20002

SBIR Phase I - Final Technical Report

Office of Cyber Security

Power Systems Settings Security – 1B

Table of Contents

Introduction

This SBIR Phase I project titled, "Cybersecurity at the Edge of the Grid" conducted by Athena Power, Inc. explored how grid-edge devices or modern Fault Circuit Indicators (FCI's), such as the Athena UFD (See Figure 2) could incorporate neural network/machine learning technology to better detect cyber-attacks/grid intrusion on critical infrastructure facilities. This project researched and implemented the most effective neural network algorithms that can discover deviations in electric load signatures into the Athena UFD firmware. The capabilities and success of this new technology in detecting grid intrusion (deviations) were researched and tested in (3) real-world scenarios deemed, 'critical facilities' by society. These critical facilities where real-world data was used in our testing included Municipal Streetlights, Electric Trains, and Schools.

The Athena/SBIR team worked with highly credible 3rd party organizations to validate results from Athena's internal testing. These third-party organizations include ComEd/Exelon and Pecan St. (through The Department of Energy PLATFORM Commercialization Program). The testing and final reports from the third-party organizations involved were consistent in proving this methodology was effective and could be utilized by grid-edge sensors (such as the Athena UFD).

I. **<u>Overview</u>**

There has been a significant amount of emphasis placed on the security of the BES, the Bulk Energy System (aka transmission grid), the "backbone" of the electric grid in the USA. However, with the advent of the 'Smart Grid' (smart-digital meters, reclosers, capacitor banks and switches) the potential for a cyber-attack on the electric grid has been increasing. There have been limited but successful attacks on

Figure 1

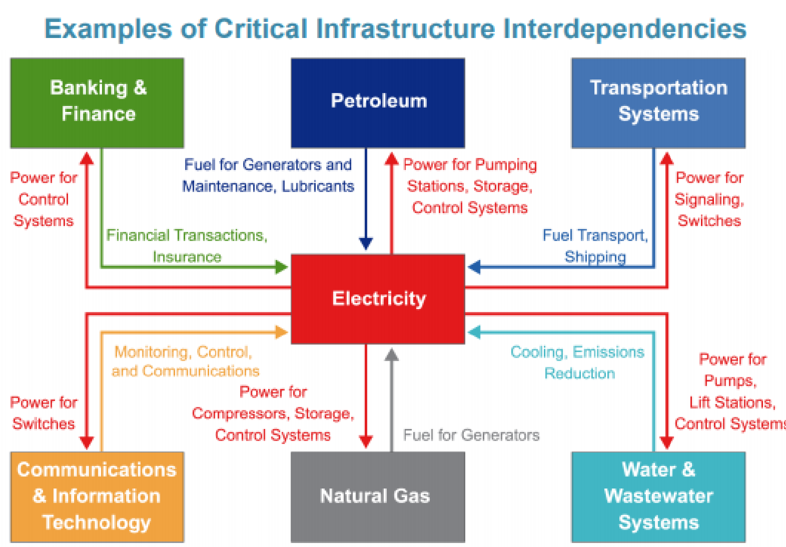


Figure 4.4: The interdependence of critical infrastructure systems increases the importance of electricity resilience, as disruptions to energy services are projected to affect other sectors. Shown above is a representative set of connections, and the complex relationships are analogous to other systems (Ch. 17: Complex Systems). A more complete listing of these linkages can be found at DOE.[2] Source: adapted from DOE 2017.[2]

foreign power grids (Ukraine 2016) and a March 2019 attack on a US power control center. Of even more concern are the critical infrastructures that society depends on for their daily lives (municipal systems – streetlights, water treatment, schools, mass transit) as well as systems that the electric grid depends on such as natural gas distribution centers, peaking plants, and communications centers. As depicted in the figure 1 above taken from the Fourth National Climate Change Report published by the US Global Change.

Research Program, there are numerous critical commercial and industrial systems that if compromised could significantly affect the performance of the electric grid and have a negative impact on the local community.

The question that this SBIR research attempts to answer is, "Can changes in the electrical usage patterns of critical infrastructure customers be an "early warning" system of a potential cyber-attack/grid intrusion?" To answer that question this research will use neural network technology to analyze interval data previously collected by smart meters to determine if the usage patterns of these customers are unique and repeatable. Once the patterns have been identified a small representative subset of those patterns, called an archetype(s) will be download to a grid edge device (In this case, we used our Athena Power Utility Fault Detector - UFD) and subsequently compared against the usage during the current day to identify deviations from historical usage patterns. Using an existing device such as the Athena UFD (See Figure 2) has numerous advantages. The current hardware has enough capabilities to monitor up to 6 electrical circuits (phases) simultaneously, includes power harvesting capability, wide area cellular communications and a "cloud" management/monitoring service. It can be connected to a feeder, transformer, customer service drops or even an individual circuit in a commercial facility. By merely updating the firmware, the additional functionality can be implemented without a major redesign of the entire system.

Figure 2

II. USE CASES – Business Cadence (Streetlights, Electric Trains, Schools, High speed Capture)

One of the results of this research was the discovery that business, schools, municipalities and other large commercial electric customers have a unique daily energy usage pattern, a kind of repeatable cadence that is directly tied to their business operations. Using a Kohonen Neural Network on smart meter data, one can see the unique patterns of each industry (See Figure 3 below). Note that High Schools have distinct evening activities that elementary schools do not have. For the Electric Train, the rush hour morning and afternoon load spikes uniquely identify train station loads in a major city. It is these explicit patterns that can be utilized to detect abnormal and potentially malicious activity should these patterns deviate from the norm.

Figure 3

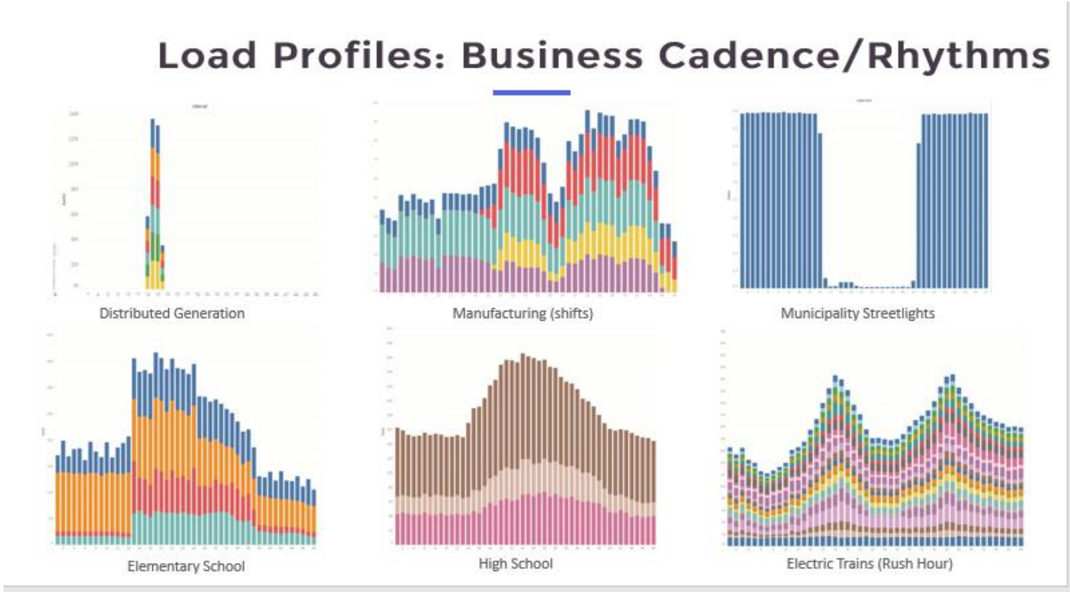
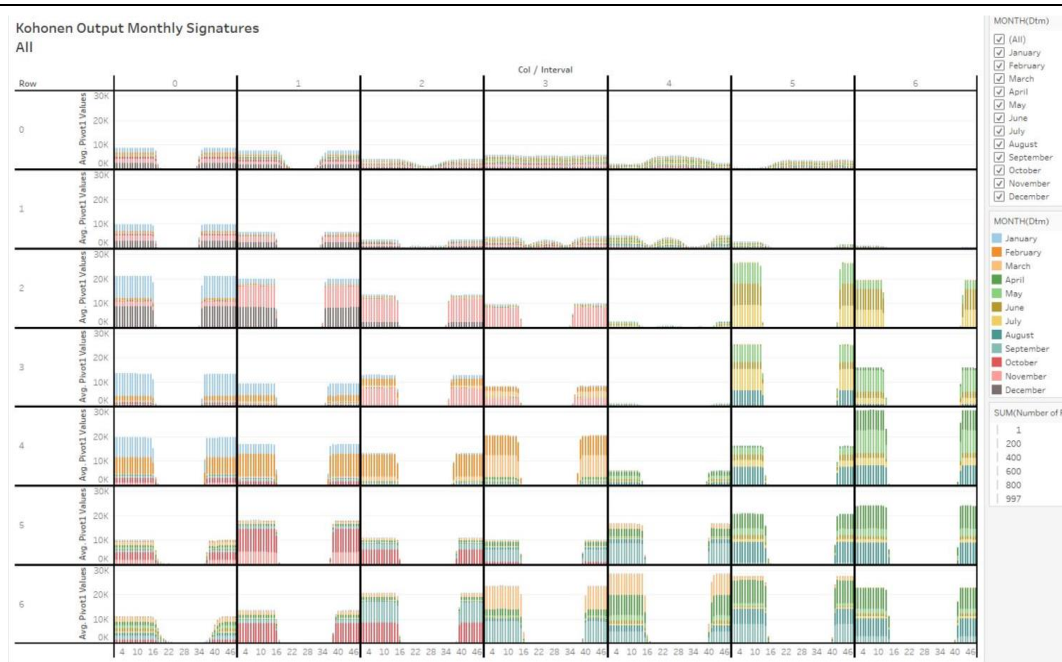


Figure 4

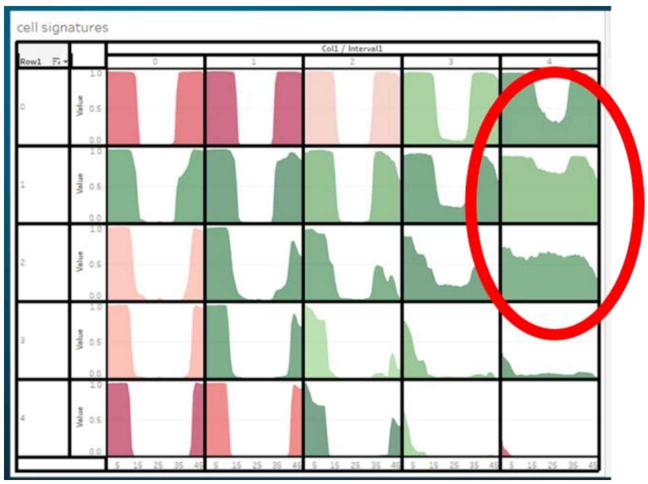


a. Streetlights

When developing 'Use-Cases' for testing, the key is to identify critical infrastructure targets for cyber-attacks/grid intrusion. Recently, municipal systems have become "hot targets" for ransomware and other malware attacks. There have been successful attacks on municipalities that have shutdown payroll systems and even compromised water treatment plants. In addition, Athena Power has repositories of actual streetlight load usage profiles from smart meters that have recorded malicious diversion of electricity by 3rd parties. Looking at Figure 4 above displays the results of running a Kohonen neural network on thousands of streetlight load profiles (48 intervals/day) for an entire year.

The "U" shaped load profile is the result of early morning and late-night darkness. The "bottom of the U" changes length depending on the time of year with shorter days in December and longer days in June. It is easy to see that one could choose a small representative sample of 6-7 signatures to use as an archetype (a recurrent pattern) to compare against the latest real-time interval readings. It is important to note that in the case of streetlights, the amplitude (total kwhr) is less important than the shape of the signature. Figure 5 shows two abnormal load profiles (upper right-hand corner of Kohonen), the top one is a failure of the streetlight photocell (day burner), and the second is a restaurant owner who has connected their store's signage to an adjacent streetlight. In the testing section of this report below, you will see various tests where the UFD successfully identified normal and abnormal streetlight signatures.

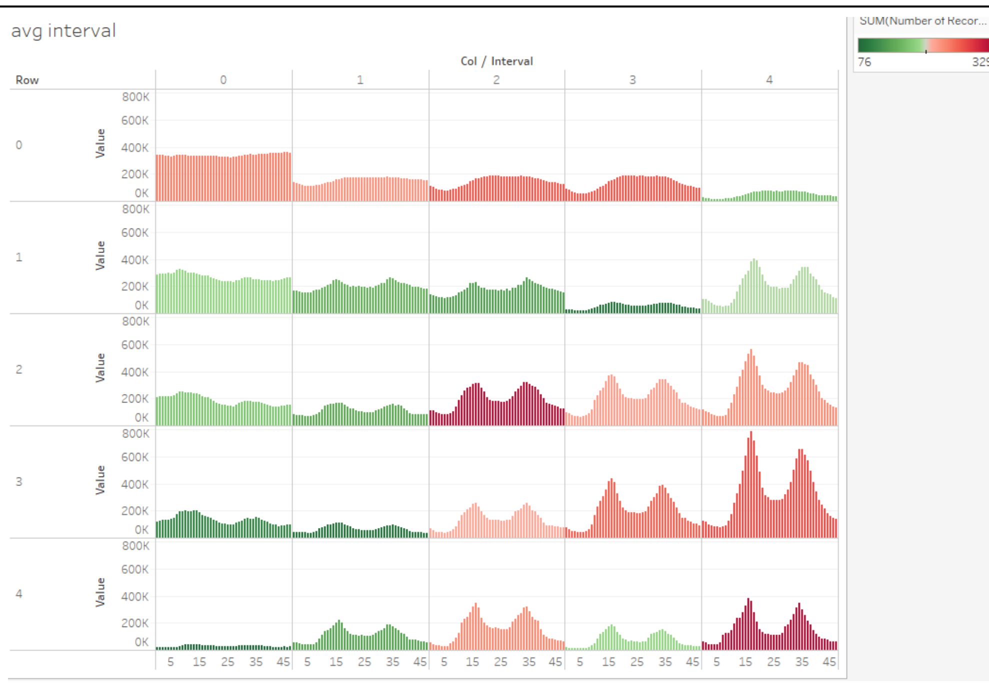
Figure 5



b. <u>Electric Trains</u>

There is considerable discussion in the industry about the vulnerability of the railway infrastructure and the potential for a cyber-attack/grid intrusion that could cripple a major mass transit railroad. As railroads implement new digital technologies such as positive

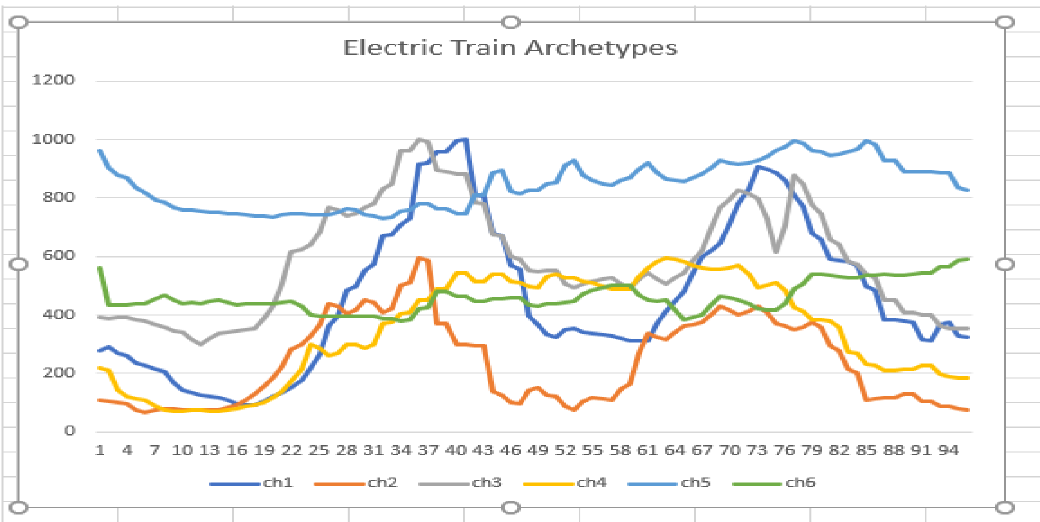
Figure 6



train control and SCADA systems, they become vulnerable and more attractive targets for cyber-attacks. Below in Figure 6 is a Kohonen neural network analysis of a years' worth of actual daily load profiles for a major city railroad (*the city will remain confidential throughout this report*). The variations across the Kohonen matrix are attributed to the seasonal changes (heating and cooling), frequency of trains through a station, rush-hour crowds, and railcar storage overnight.

Figure 7 shows seven examples of load signatures that represent the majority of load shapes encountered at various stations/yards. These "archetypes" will be used in the testing section to identify normal and abnormal electric train signatures

Figure 7



c. <u>Schools</u>

According to the news service Techradar, "2019 has seen more cyber-attacks than the two previous years combined" on school districts. Data breaches and malware consisted of >50% of the attacks, but over 10% of the attacks targeted the school's infrastructure. Recently, a school in Michigan had their HVAC system compromised. Students were told to stay home for several days until the heating and cooling systems were returned to normal. Figure 8 shows the results of running a Kohonen neural network on a years' worth of actual smart meter data for both elementary and secondary schools. It is easy to see the schools that have late night events vs. those that use most of their energy during daylight hours. Interestingly, the upper right-hand corner shows several small loads with a U-shaped signature similar to the streetlight signatures above. These are meters that are associated with the parking lot and path lights at the schools.

Figure 8

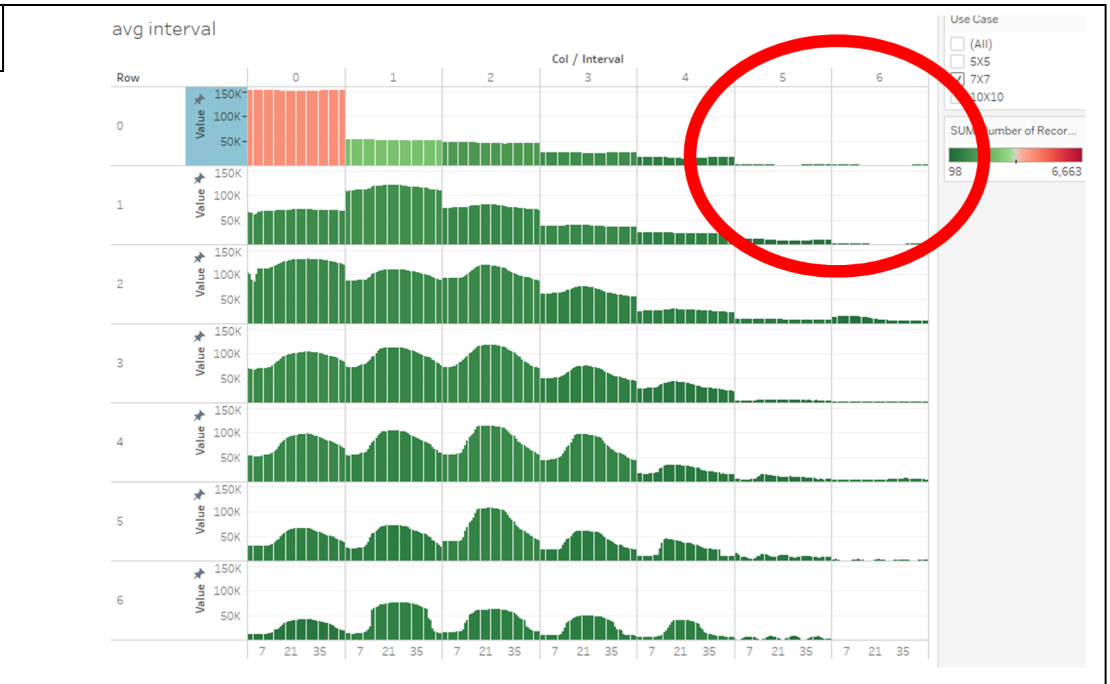
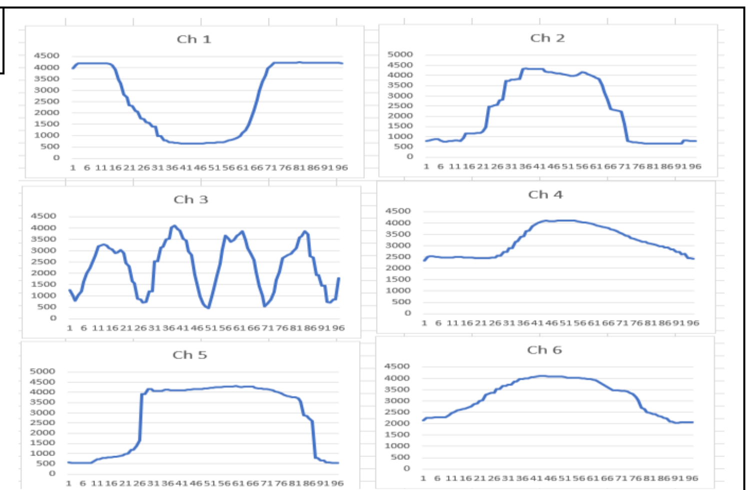


Figure 9 shows the six archetypes that will be used to identify normal vs. abnormal schools load signatures during the UFD testing.

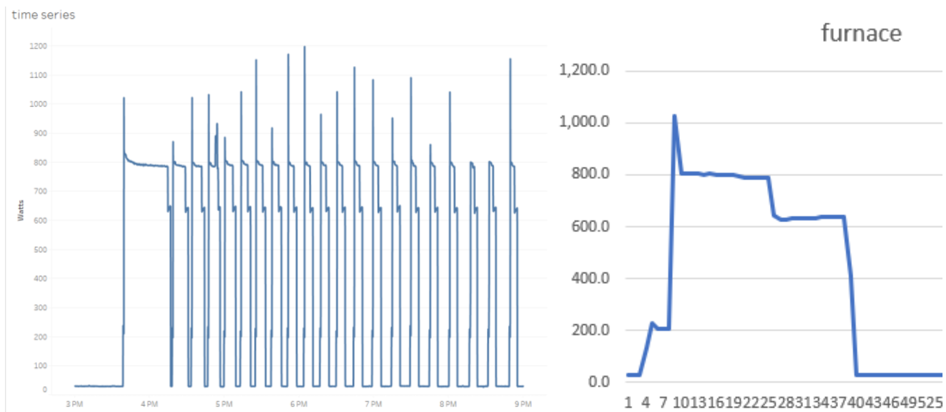
Figure 9



d. High-speed capture – Furnace signatures

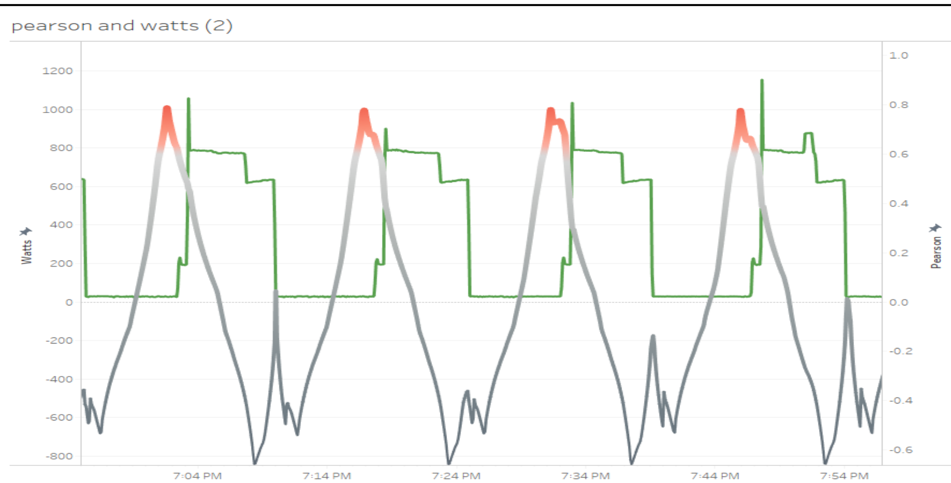
Typically, the UFD interval accumulation rate is 15 minutes per interval for a total of 96 intervals in a day. However, the UFD has the capability of increasing the number of intervals per day, thereby reducing the accumulation duration to as little as 5 seconds per interval. Below, figure 10 is a snapshot of the energy signature of a natural gas furnace sampled at a 5-second rate. (See Figure 10)

Figure 10



One can see from the figure on the left that the daily load signature is a series of on/off events whose duration and spacing is dictated by the outside air temperature, thermostat settings, insulation in the home, and several other variables. On the right is a typical individual furnace signature that shows the initial spike when the solenoid that controls the gas valve closes, the blower motor current spike, the duration of the fan cycle, and finally exhausting the plenum with the blower motor before shutting off. This poses the question of whether a Pearson Coefficient can be adapted to this more complex stream of individual load signatures. This can be done with high levels of certainty by creating a moving Pearson algorithm that compares all archetypes at EVERY interval where you can identify when the furnace cycle begins and ends. Figure 11 below shows several of the furnace cycles (green lines), and the red peak is the point at which one of the archetypes has the best Pearson match. This level of granular detail, a form of load disaggregation, provides much greater insight into the equipment operation, including frequency of use, energy efficiency, and duration of the operation. For C&I customers with critical infrastructure, it is possible to use the UFD Rogowski coils (load/current measurement sensors) on individual circuits/phases to monitor and asses the performance of the respective infrastructure in high levels of detail.

Figure 11



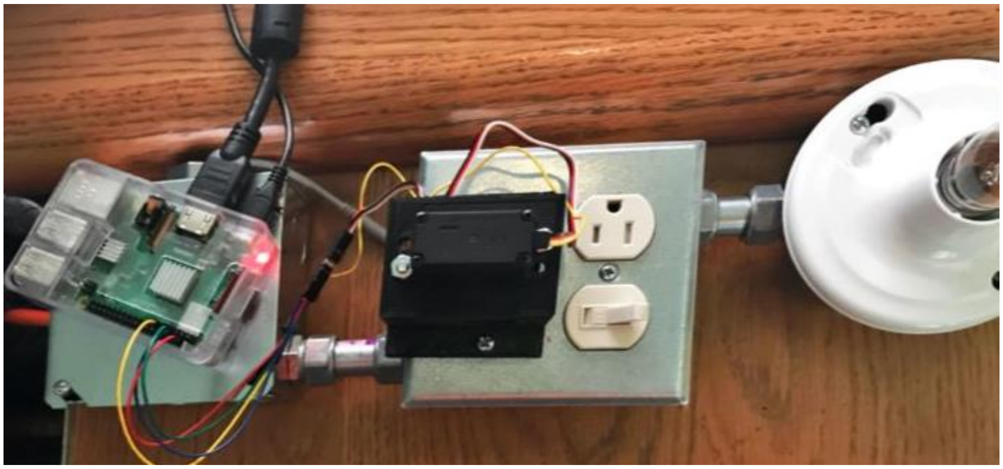
iii. Internal Testing/Algorithm Verifications

The goal of testing was twofold:

1) Validate that the Smart Meter interval accumulation and Pearson – archetype algorithms have been successfully developed and implemented in the UFD firmware
2) Verify that the entire architecture – hardware and firmware could successfully be used to identify normal and abnormal load signatures from a variety of Use Cases (within the realm of what would be considered critical infrastructure facilities for society)

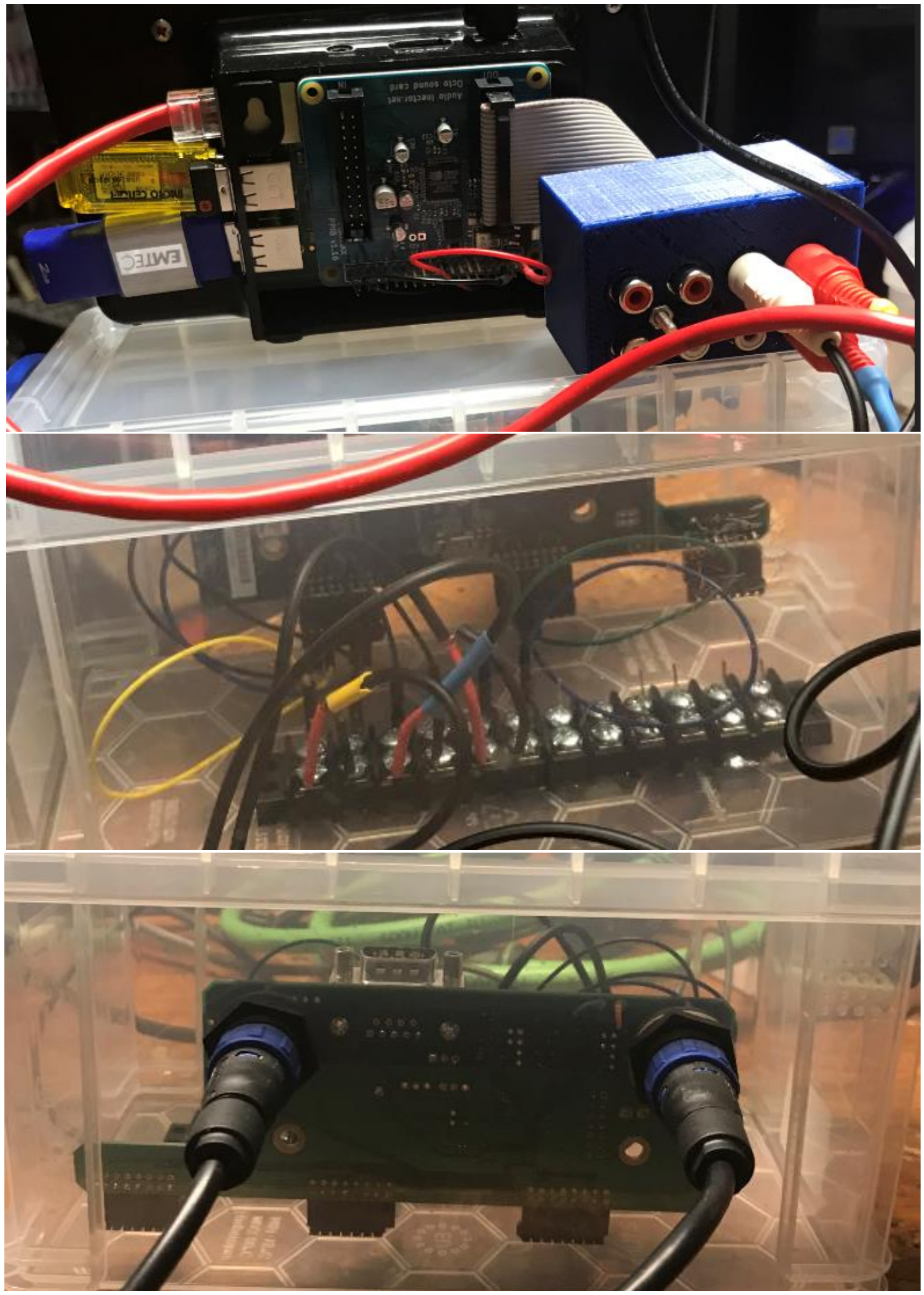
The Athena-Power UFD is a complex device to do testing on because of its broad array of functions within its platform that include applications such as fault detection, (6) channels of data acquisition, bi-directional power flow, 3-phase AC analytics/power quality, smart meter intervals and Pearson signature analysis. Initial testing was done using a single channel and a Raspberry Pi controlled servo "light dimmer" that would generate custom-built load signatures. (See Figure 12)

Figure 12



This approach was deemed to be too slow and inaccurate, so a novel approach was devised that used a commercially available (8)-channel soundboard to directly "inject" custom audio waveforms simultaneously into all (6)-channels of the UFD (See Figure 13). By accelerating the interval collection rate in the UFD, this allowed for (6) distinct load signatures to be "injected" into the UFD, simultaneously simulating an entire day's worth of load in just 8 minutes. (96 intervals * 5 seconds/interval / 60 seconds/ minute = 8 minutes)

Figure 13



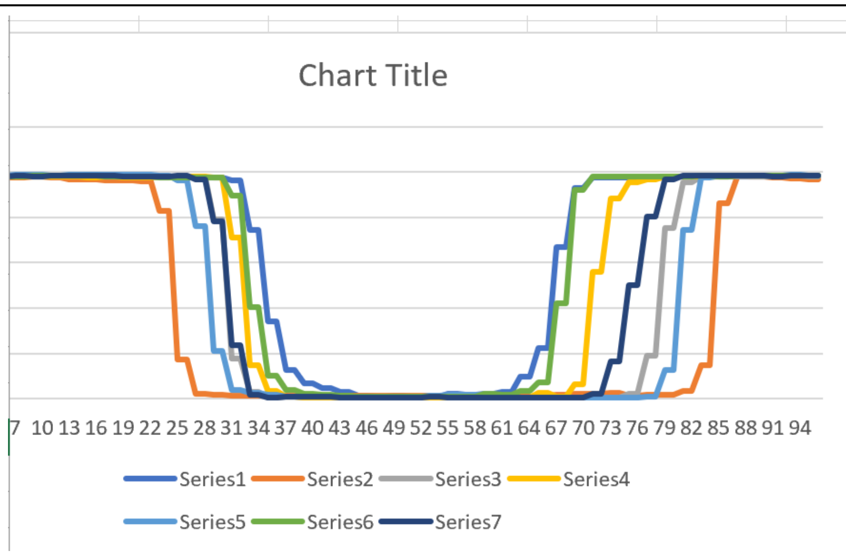
This approach proved to be very useful in testing the diverse array of UFD function by simulating the various waveforms in a custom-built sound (.wav) file. Figure 14 displays one example of a custom (6) channel wave file, in this case, (6) streetlight load signatures that are used to simulate actual 60 hertz AC waveforms whose amplitude represents an actual smart meter load profile. Once the entire waveform is played, the UFD calculates the best Pearson Coefficient from all the archetypes that were previously loaded into the UFD for each channel. More details describing this novel testing are approach in the Technology section below.

Figure 14

a. <u>Streetlight Load Signatures</u>

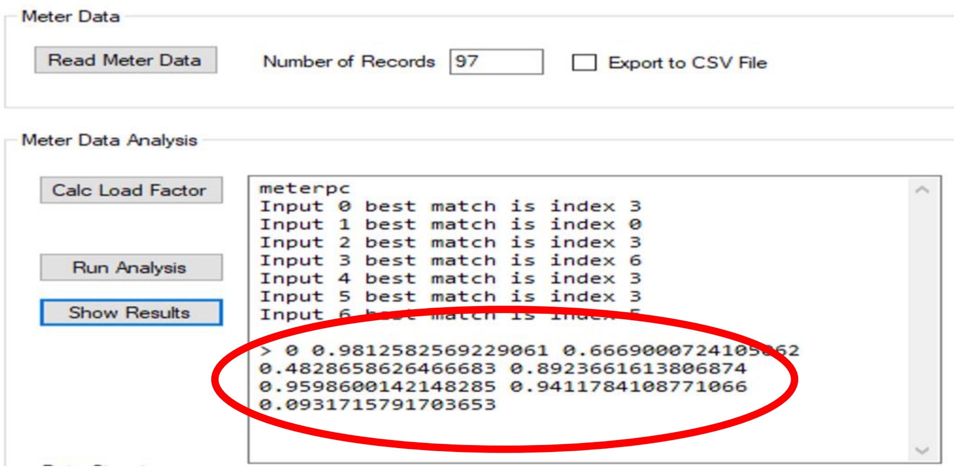
For testing of streetlights, (7) archetypes were chosen that represent the variety of seasonal changes throughout the year and their effects on the streetlight load signatures. (See Figure 15)

Figure 15



These archetypes were loaded into the UFD to be used for comparison to actual load signatures. Next, the waveforms above in Figure 14 were recorded by the UFD when "injected" into the UFD using the sound generator card. Waveforms channels 0,3,4,5 are all good while channels 1 and 2 contained anomalies. Once the waveforms were recorded, the Pearson Correlation Coefficient was calculated for all (6) of the channels. As you can see from below, (See Figure 16) channels 0,3,4,5 all had correlation coefficients of > 90%. While channel 1 had a 66% correlation and channel 2 and 48% correlation effectively demonstrating the

Figure 16



UFD's ability to distinguish between normal and abnormal streetlight load signatures while accommodating seasonal variations.

b. **Electric Train signatures**

As can be seen in the Kohonen results matrix below, figure 17, the electric train signatures can be reduced to a few fundamental archetypes (Figure 18) that represent the rush hour and inner-city load profiles.

Figure 17

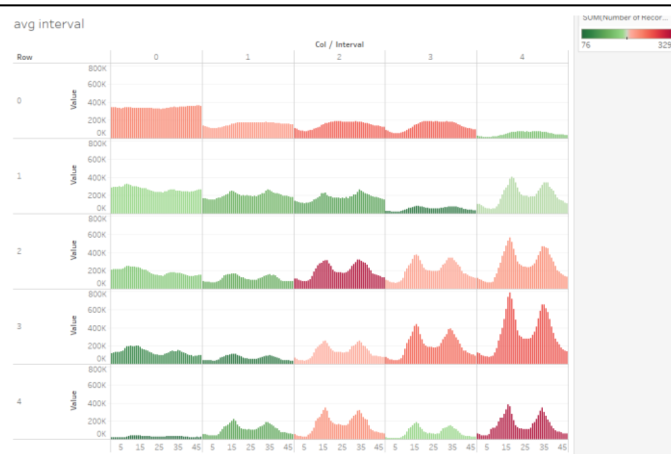
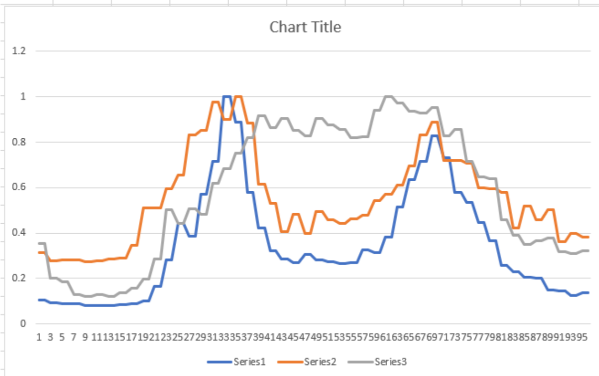
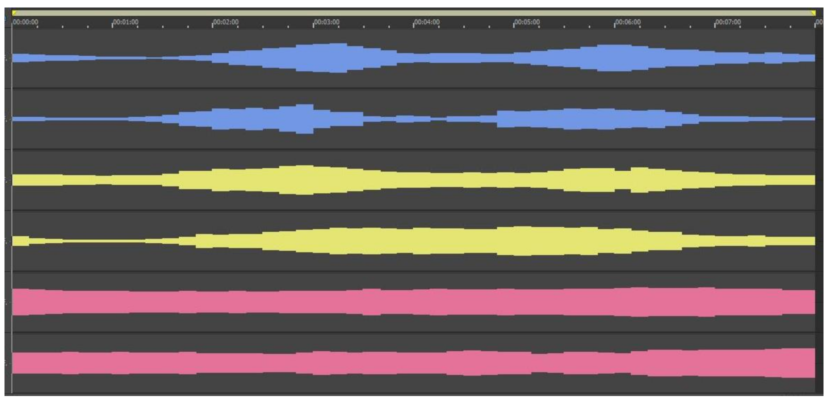


Figure 18



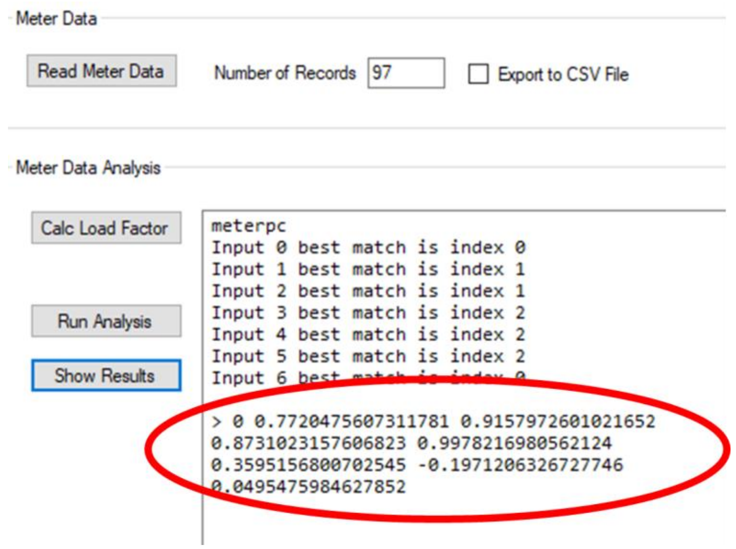
The actual waveforms "injected" into the UFD that simulated electric train load profiles consisted of 4 good signatures (1-4) and two abnormal signatures (5,6) Figure 19

Figure 19



In Figure 20, the UFD identified the first 4 signatures with scores of 77%, 92%, 87% and 99%. The last two abnormal signatures scored correlation coefficients of 36% and a -19%. This again demonstrates the UFD's capabilities to differentiate between good and abnormal electric train signatures.

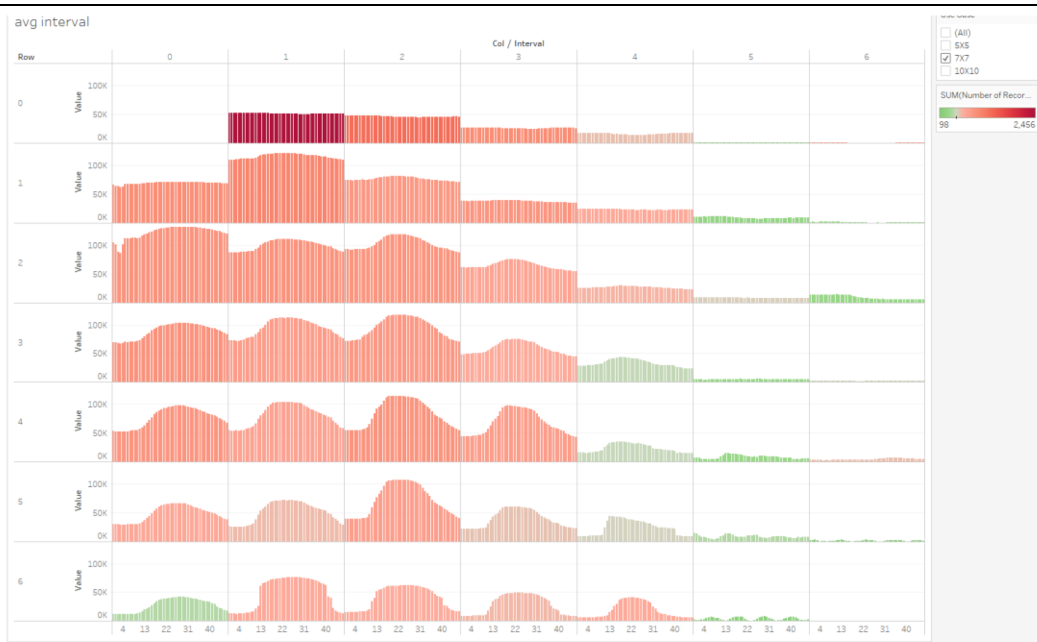
Figure 20



c. **<u>School signatures</u>**

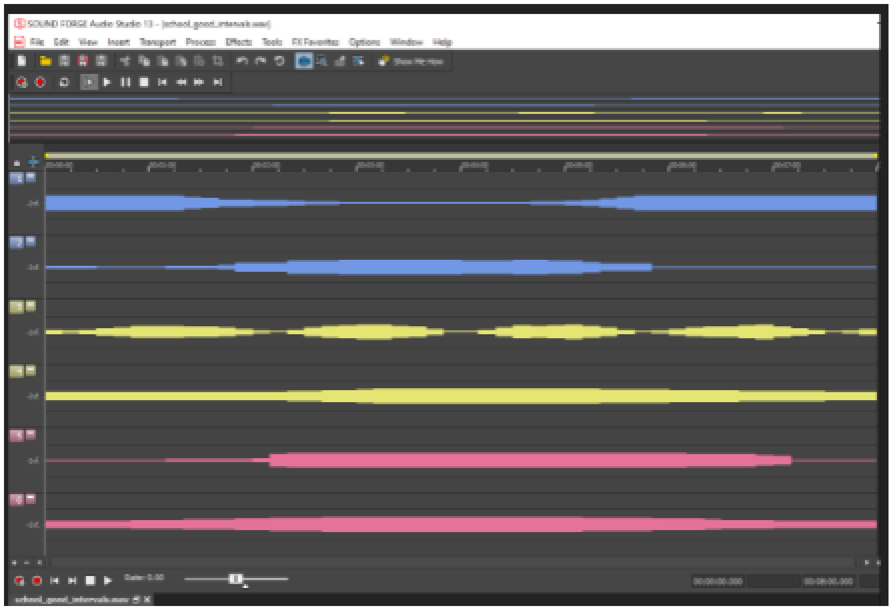
Of the three chosen Use-Cases in this project, schools are by far the most challenging to develop archetypes. As can be seen in the Kohonen matrix below (See Figure 21), the variety of shapes is quite large. From the high schools with evening usage to the repetitive cyclic loads during the day, developing archetypes can be challenging because of the multiple meters and loads on a school campus.

Figure 21



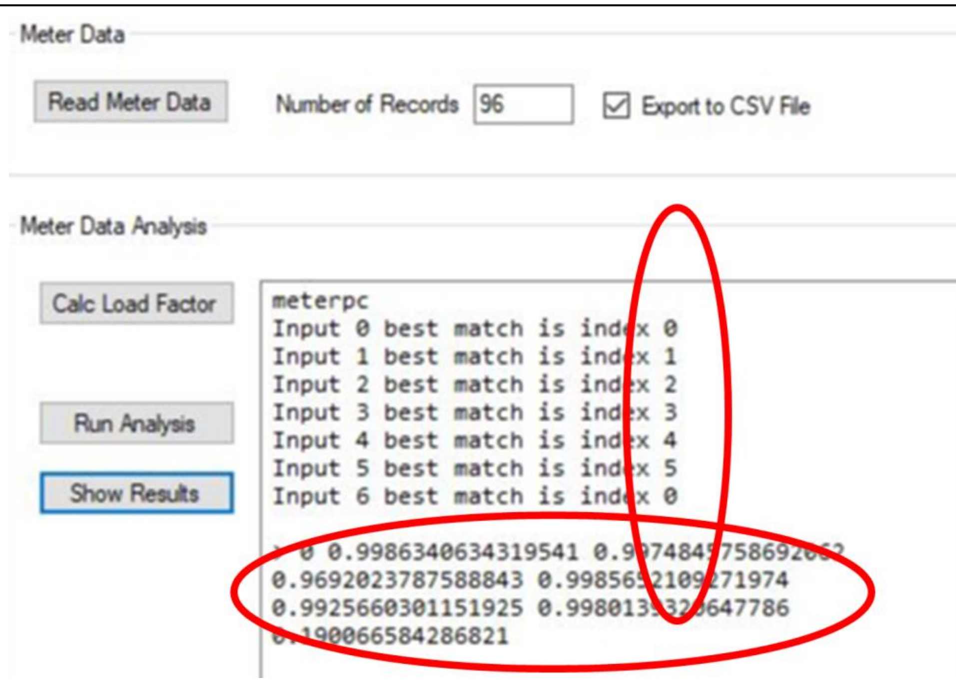
To prove that the Pearson algorithm can handle the variety of load signatures created by various types of schools/loads, (6) signatures were chosen that all represent good but diverse load shapes. (Figure 22)

Figure 22



After "injecting" the load signatures into the UFD and running the Pearson algorithm, seen below, Figure 23, that all (6) channels produce a Pearson Coefficient of > 96%. In addition, (6) different archetypes were selected to produce the "best fit" results.

Figure 23



IV. Supported 3rd Party Testing

a. ComEd Smart Cities lab

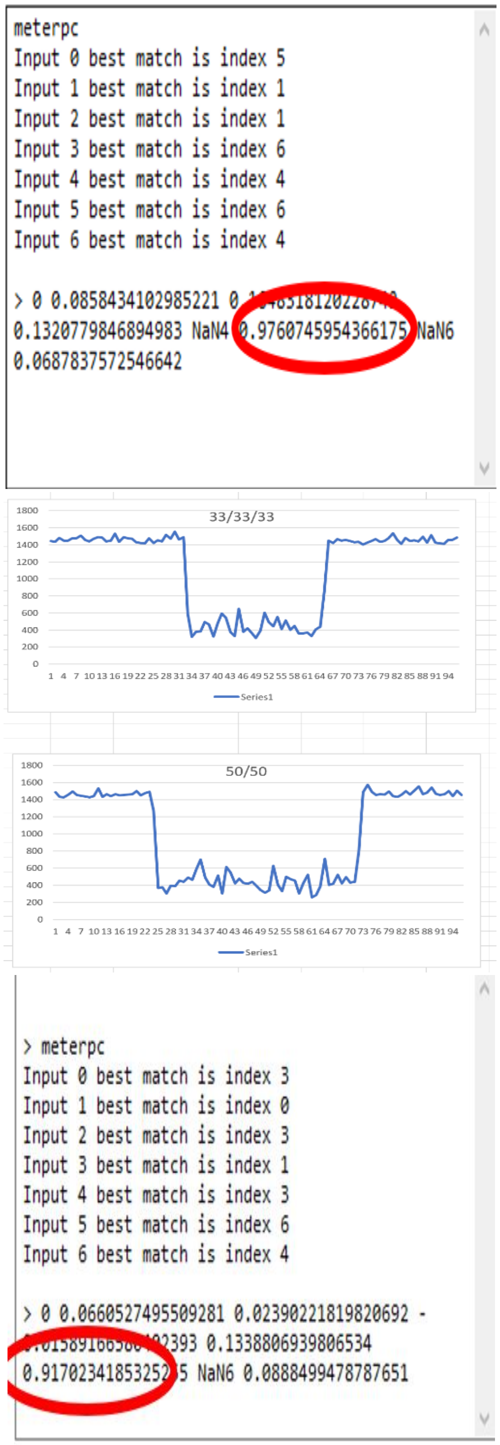
The ComEd Smart Cities lab is designed to test all aspects of Smart Metering and Smart Cities technologies. The test includes actual LED streetlights (See Figure 24) from several manufactures that have the SSN/ITRON RF NIC (Network Interface Card) installed. That allows for remote control of the streetlight and the ability to change the LED brightness

Figure 24

from 0-100% using a simple script.

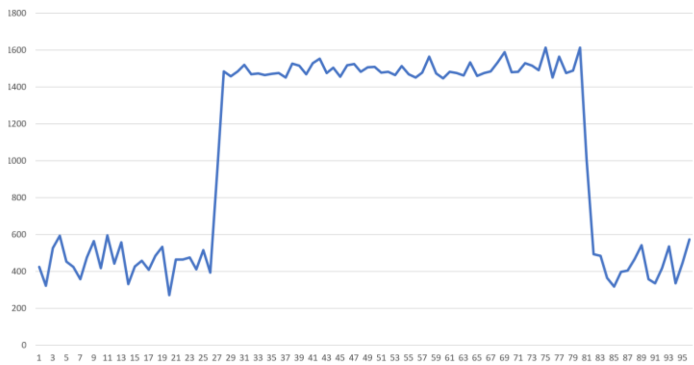
By connecting the UFD Rogowski coil (a current measurement sensor) to a streetlight circuit, various lighting patterns can be simulated and recorded by the UFD and exported to MS Excel for analysis. The first series of tests were conducted to simulate actual streetlight load profiles of the seasonal lighting extremes. (December = short days and June = long days). The first actual signature simulates December's patterns of 30% on, 30% off, and 30% on and June's 25% on, 50% off, 25% on. Below are the snapshots (See Figure 25) of the Pearson results from the UFD, in the December case, the signature was a 98% match with the previously loaded archetypes. In the June case, a 92% match was achieved, proving the effectiveness of the Pearson algorithm in the UFD.

Figure 25


meterpc
Input 0 best match is index 5
Input 1 best match is index 1
Input 2 best match is index 1
Input 3 best match is index 6
Input 4 best match is index 4
Input 5 best match is index 6
Input 6 best match is index 4
> 0 0.0858434102985221
0.1320779846894983 NaN4 0.9760745954366175 NaN6
0.0687837572546642
33/33/33
Series1
50/50
Series1
> meterpc
Input 0 best match is index 3
Input 1 best match is index 0
Input 2 best match is index 3
Input 3 best match is index 1
Input 4 best match is index 3
Input 5 best match is index 6
Input 6 best match is index 4
> 0 0.0660527495509281 0.02390221819820692 -
2393 0.1338806939806534
0.91702341853252 5 NaN6 0.0888499478787651

To demonstrate the opposite extreme, an inverted load signature of 25% off, 50% on, and 25% off was generated and analyzed. As can be seen from the snapshot below (See Figure 26) the Pearson generated a negative (inverted) correlation of a -64%

Figure 26




```
meterpc
Input 0 best match is index 5
Input 1 best match is index 6
Input 2 best match is index 4
Input 3 best match is index 6
Input 4 best match is index 0
Input 5 best match is index 6
Input 6 best match is index 4

> 0  0.05508265818923561  N2 0.1088901413452653
Na 4 -0.6488716579374715 Na 6 0.0888772342428334
```

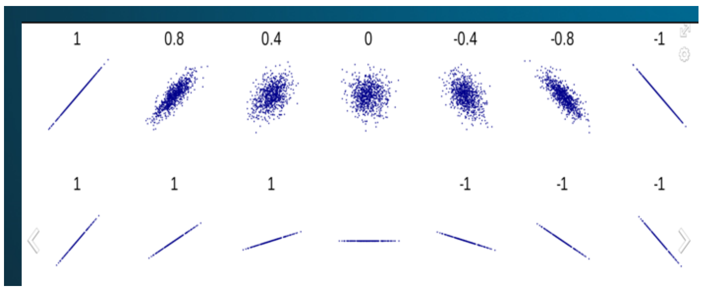
V. Technology

a. Pearson Correlation Coefficient

The Pearson Correlation coefficient (See Figure 27) is a key enabler for the technology. It compares two arbitrary length arrays and produces a number between -1.0 (inverse correlation) and 1.0 (perfect correlation) that represents the similarities between the two arrays. It is important to note that the magnitude of these curves is irrelevant; only the shapes are compared.

Figure 27

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad \text{(Eq.3)}$$



b. Sensor vs. DI platform

Technology continues to evolve and improve in performance over time. Whether it's memory capacity, disk storage, CPU capabilities, or VLSI densities, they all continually improve. Figure 28 shows this progression from a sensor to a DI (Distributed Intelligence) platform. The Athena-Power UFD was chosen for this project because of its memory capacity, high speed sample rates, compute capability and commercial availability. As can be seen in the Results/Conclusions section below, the recommendations include a new hardware platform for SBIR II that will allow more extensive computing and algorithms, such as neural networks (as discussed extensively on this report) to be executed "at the edge" of the grid.

Figure 28

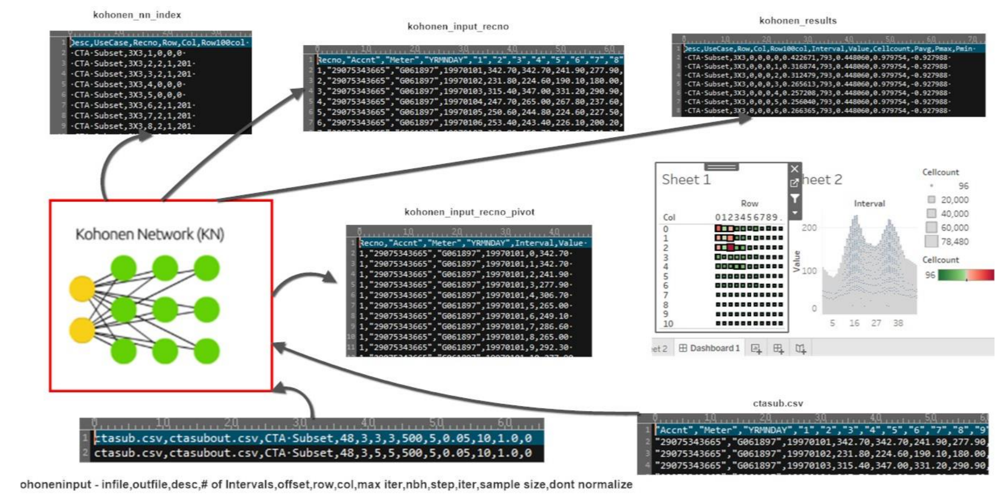
Deployment – Sensor vs DI Device

Sensor	DI Device
Single function	Multi Function
Minimal math capability	Special Hardware (FPU,DSP,NN)
Monolithic Code	Real Time OS – download apps
Limited Ram	RAM available for other apps
Limit Flash	Extensive SSD flash
Single Core CPU	Multi-core CPU
Compiled code single language	Multi language & Interpreted

c. Neural Networks

The other key technology in this SBIR is the Kohonen SOM/Neural Network https://en.wikipedia.org/wiki/Self-organizing_map. Initially, the "R" implementation of the Kohonen algorithm was used to process smart meter interval data, but the results were disappointing. Long convergence times, small sample sizes (<30,000 days) and unexplained execution aborts were experienced. To address this problem, a new Kohonen algorithm was written entirely "from scratch" in "C" with the following advanced capabilities. Support for up to 2,000,000 daily load profiles, dynamic convergence, statistical sampling, normalized/denormalized options, and export (See Figure 29) of various files that can be used directly in a data mining tool such as Tableau. To date, the results from this implementation have been impressive, including the process of hundreds of different USE CASES with data sets exceeding 1.6 million daily load profiles and a convergence time of less than 5 minutes.

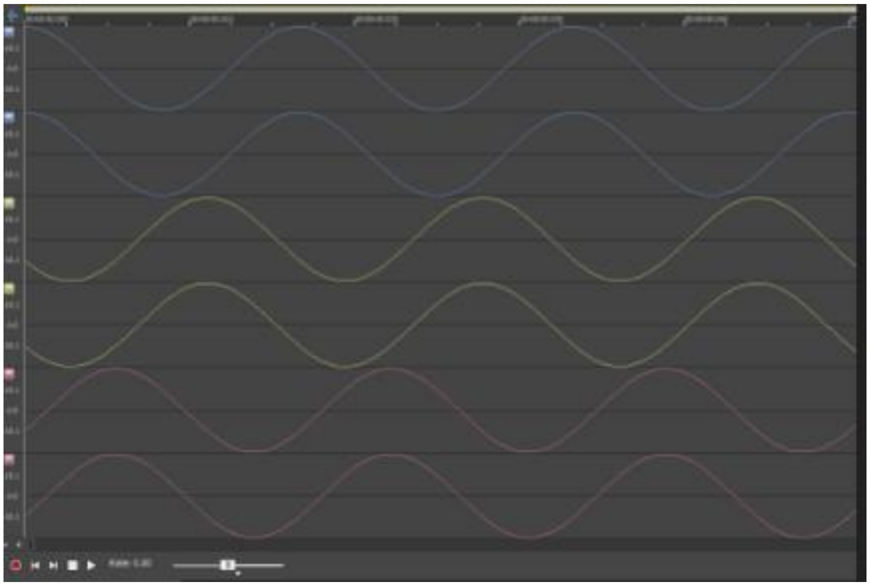
Figure 29



d. Wave file (*.wav) generations

The Wavefile (waveform audio file) or .WAV file, for short, is a popular audio file format developed by Microsoft and IBM. The Python language contains several libraries that can encode an array of multiple signal channels into a .WAV file. For example, Figure 30, is the results of a Python program creating a typical 3 phase AC, voltage, and current waveforms.

Figure 30



Various Use-Case load signatures (streetlights, electric trains, schools) were encoded into wavefiles and "played back" into the UFD to test the various features and algorithms of the UFD, using a variety of tools. One of the advantages of using an industry-standard file format is that programs like the audio editing/visualization tool Sound Forge can be used to visualize the results of the Python encoding. https://www.magix.com/us/music/sound-forge/sound-forge-audio-studio/

e. Smart Meter Emulation

In order to implement the Pearson algorithm, the UFD firmware was first modified to support intervals like those found in Smart Meters. Since the UFD scans all its sensors and does the AC calculations every second, it was relatively easy to include interval accumulations with a 1 second granularity. Like Smart Meters, 96 intervals per day (15 minutes per interval) was chosen as the standard daily load signature. In addition, the UFD stores 30 days' worth of intervals for all (6) input channels. To support accelerated lab testing, the interval duration can be changed manually to as little as 5 seconds per interval. This change allows for an entire 24-hour test to be completed in just 8 minutes.

VI. Results/Conclusions

The results/conclusions of this SBIR project include:

a. Critical infrastructure facilities such as municipalities/streetlights, schools, and electric trains exhibit repeatable unique electrical load signatures that correlate to their business processes. Deviations from these signatures can signal possible malicious attacks on their facilities, as was demonstrated by the diversion of streetlight energy to adjacent signage.
b. Kohonen neural networks can be successfully used to analyze smart meter data for these facilities and develop archetypes that represent these repeatable signatures.
c. The Pearson correlation coefficient can be used to compare these archetypes against current load profiles to detect abnormal load usages that could indicate a possible cyber-attack on their facilities.
d. The Pearson coefficient can be effectively implemented in a small microprocessor-based system/Grid-Edge device such as the Athena-Power UFD, without compromising the other functions that the UFD performs.
e. Based on all the results of this project, it is possible to deploy several UFD's on critical facilities and create an Energy Anomaly Dashboard to detect a coordinated cyber-attack/grid intrusion on one or multiple facilities.

VII. Next Steps/Additional Research

a. Implement Learning at the "Edge"

i. The current process of using Smart Meter data with a Kohonen neural network in the "back office" to learn the customer archetypes is not scalable to a large deployment of UFDs. The next generation of this technology will require a revision to the UFD hardware that will implement the ability to run a neural network analysis on-site/locally on historical and current load signatures. Once installed, this hardware will store daily load signatures and begin the process of developing a library of archetypes for the specific customer. Over time, the library will become more robust as it encounters the full spectrum of customer behaviors.

b. Expand the USE CASE library

i. As more critical infrastructure is identified as potential targets for cyber-attacks/grid intrusion, the library of 'Use-Case' archetypes will need to be expanded. Essential to the development of these 'Use-Cases' will be the "learning at the edge" capabilities described in the section above.

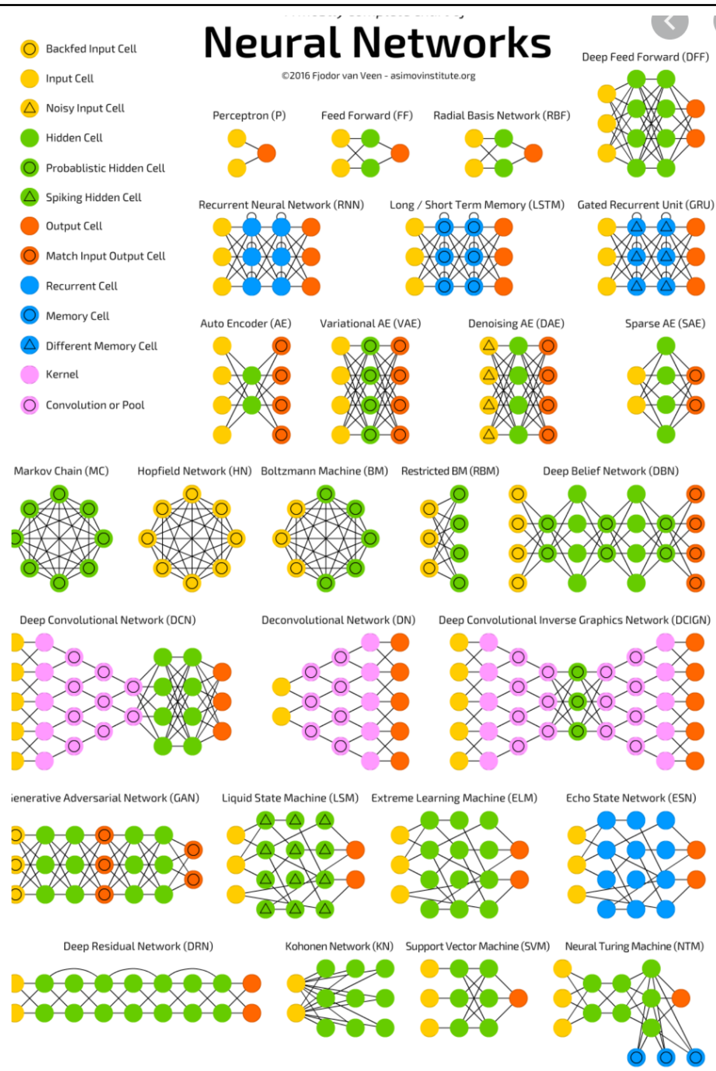
c. Real World deployment and testing

i. Using smart meter data to train neural networks is a great place to start when developing a prototype. However, field deployments on actual customer sites will yield much finer-grained sampling rates and real-time analysis/detection of customer abnormalities. Factors in selecting customer deployments include possibility/frequency of cyber-attacks, impact to the community and electric grid, of a successful cyber-attack, size of electrical load, relationship and interest demonstrated by potential customers and the number of additional similar sites.

d. Research alternative neural network technologies.

i. The Kohonen neural network is just one of many algorithms in the Neural Network Zoo, as documented by the Asimov Institute https://www.asimovinstitute.org/neural-network-zoo. (See Figure 31 below) While the Kohonen is excellent for classifying/clustering archetypes, other neural networks like the CNN/RNN algorithms could also be used for detecting anomalies.

Figure 31



e. Expand Aegis to include a cyber dashboard capability

i. As additional "cyber-enabled" UFDs are deployed using Aegis (Athena's Cloud-based Software Platform for the UFD), Aegis should be expanded to allow a geospatial display of the cyber status of multiple related customers (all schools, all trains, all municipal systems ...) In addition, critical customer facilities on the same utility feeder or geographic location should be highlighted to show potential coordinated attacks by a cyber or physical terrorist.

f. <u>Continue research on high-speed sensor recording/signature recognition</u>

i. As sensor and microprocessor technology evolves, it is now possible to sample electrical waveforms at higher sample rates. Sample rates of > 10khz can now be achieved with low-cost microprocessor-based systems. This finer-grained data will allow for a more detailed and accurate analysis of customer load signatures. Additional algorithms, such as the moving window Pearson algorithm, as described in section II above, should be implemented to perform load disaggregation of individual pieces of equipment.

g. <u>Integrate UFD functionality in Utility Transformers</u>

i. The more UFD's deployed, the greater the potential to detect a cyberattack during the initial infection. Ideally, embedding this technology in utility-grade transformers could significantly improve the deployment density/coverage. Athena-Power is pursuing partnerships with several utility transformer vendors to explore options for creating Smart Transformers with the Athena-Power technology embedded at the manufacturing level.

Attached References:

Pecan St. Platform Report – Athena Power, Inc.

SBIR Project Team

Athena Power, Inc. Team

- Mel Gehrs, SBIR Principal Investigator
- Raj Lakhiani, Project Manager
- David Sizemore, Firmware Engineer

ComEd Team

- Nick DePinto, Power Engineering/Lab Support
- David Doherty, Director of Smart Cities/AMI Department

Pecan Street (PLATFORM Program) Team

- Andrea Tosi, Power Engineer
- Elisa Gibson, Project Manager
- Scott Hinson, CTO