



Volume 29 Issue 2

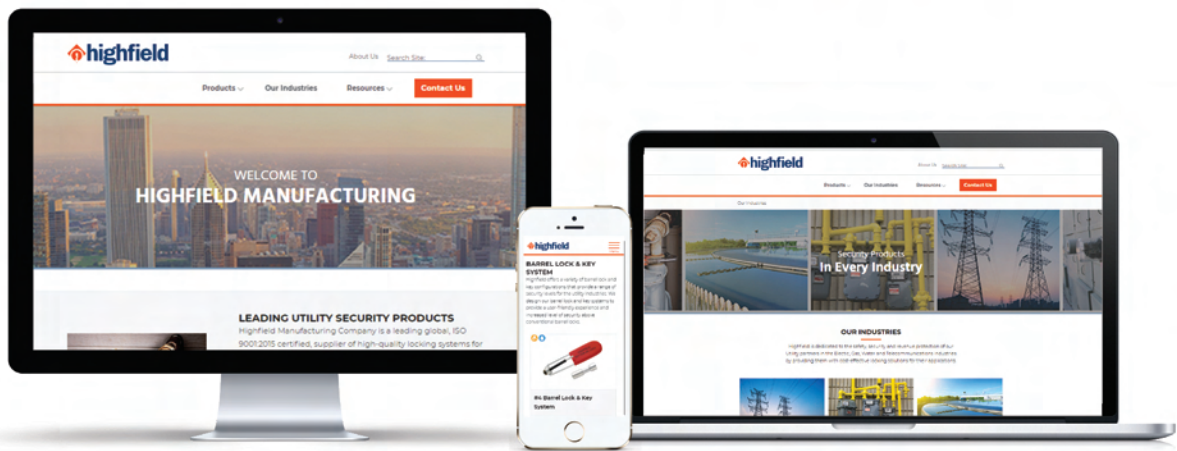
30th Anniversary Conference New Orleans

Fall 2019





HIGHFIELD-MFG.COM



SAME HIGH QUALITY. BRAND NEW LOOK.

Advancing safety, security and revenue protection. Products built to withstand the toughest conditions now available from any device on the new highfield-mfg.com.

Mobile-Friendly

Easily navigate through our products to find the right security solution from any device.

Helpful Tools

Resources at your fingertips focused on helping customers through any product question.

Customer Service

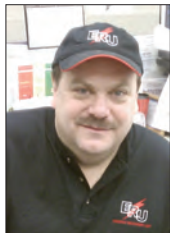
A friendly customer service team continuously working to answer any question as quickly as possible.

From the Chairperson

Revenue Protection at a Crossroads

It seems that things are changing in our world of Revenue Protection. As I have talked with many of you from utilities across the country and observed at my own utility, it doesn't seem quite as clear or cut and dry as it used to be. For as long as I can remember it seemed pretty clear that if someone is stealing power or doing anything that negatively impacts a utility, the utility would deal with the problem. Today I am talking with Revenue Protection specialists from across the country who are either fighting to start programs, or even to keep going the programs they have had for years. Even at my own utility—one that has been actively involved and considered one of the more proactive units in the country—I have found myself fighting for our very existence this year. As hard as it is to understand, some are being told to stand down and in some cases to even look the other way, often times in the name of safety or negative publicity. This crazy argument that I hear sometimes, that maybe it's better to look the other way than to risk employee safety, is just short sighted and ignorant. It is always much safer to have a trained Revenue Protection Employee or Unit dealing with theft than it is to have some unsuspecting employee or customer stumble into the hazard.

I just mentioned one possible cause for this new way of thinking, but there are more, such as the notion that new technology or smart meters will solve



Steve Sprague
IURPA Chairperson

If we are going to continue to be successful and to have support for our programs, we have to stay engaged and not just assume because it's obvious to us that management will get it also.

the theft problem for us, so there is no need to have a program any longer. There is also the age old problem we have always had about our utilities worrying about the negative image of busting customers for power theft. Lastly I will bring up a new cause, and one that has impacted my own utility—new management. Whether it's due to the passing of the torch from those people that knew the business to those who have yet to learn, or from the current trend of utilities hiring new managers from other industries, those of us knowledgeable and experienced find ourselves trying to defend the obvious. Assuming that this new wave of management gets it or understands how and why we do things is a big mistake and things could quickly and easily get away from you; don't take this for granted!

So after considering all these threats, how do we ensure Revenue Protection is recognized for the important work that it does, and the answer for keeping this new technology in line? We must be diligent in highlighting and emphasizing the benefits we bring to the our respective utilities. First, it's always been and always will be critical to report the revenue that is recovered and protected, but that's not enough anymore. Utilities just don't look at revenue like most other businesses do. Utilities are protected by line loss and PUC's, and afforded a guaranteed rate of return. Next, we all know that safety seems to be at the forefront. Be sure to emphasize to your upper management the benefits to safety a Revenue Protection Unit brings. Also, when you work large thefts and/or encounter services made hazardous due to tampering, be sure to document with photos and numbers to share with your management. I found from my own experience that when I actually showed the officers of my company the pictures we had taken of the walls being cut open or the underground wires dug up, it really made it personal for them as they experienced the emotions of having someone violate the utility in this manner.

If we are going to continue to be successful and to have support for our programs, we have to stay engaged and not just assume because it's obvious to

ON THE INSIDE

IURPA to hold their 30 th Anniversary Conference!	4
THE SHORT-COMINGS OF AMI RSS TECHNOLOGY	5
DETECTION OR PREVENTION?	7
LEGALITIES OF SELF DEFENSE	10
UK SMART METER ROLLOUT!	11
PARTNERS IN FIGHTING CRIME	12
Rogue Meters	13

us that management will get it also. I believe we are all stronger if we stay together. Let's be there to support each other, from the regional and international conferences, to always taking the time to assist another utility—one that may be less experienced or dealing with a management that isn't backing them as they once might have. As always, IURPA is committed to being there to help educate and support as needed. In fact, in May of 2020 IURPA will be hosting a conference of it's own in New Orleans to celebrate 30 years. The conference will highlight top speakers and industry leaders and will push to attract management from across the country, as we realize this is an audience we all have to make sure we get involved. We will make sure to have certification classes for

Revenue Protection specialists, and we will work hard to teach about what it takes to start and maintain effective programs. Start early planning to attend both your regional and our international conference, and reach out to your managers and officers to see if they would attend also. We still need many more IURPA members so please sign up, and we look forward to seeing you in New Orleans next year.

Steve Sprague
Chairman IURPA
Advisory Board WSUTA
Supervisor Portland General Electric



IURPA
NEWS



IURPA to hold their 30th Anniversary Conference!

Plans are underway for IURPA to host their 30th anniversary conference in the spring of 2020. There will be a host of presentations on a variety of subjects to include international speakers. Tentative information for this conference is as follows:

Date: May 18 – 21, 2020 PLEASE NOTE THE DATE CHANGE
Location: Drury Inn & Suites, New Orleans, LA
Room Rate: \$149/night
Conference Fee: \$400 for IURPA Members - \$500 for non-IURPA Members

Registration will take place from 1:00 – 5:00 on Monday, May 18th with a vendor reception to follow. A full breakfast will be provided for all attendees who stay at the hotel. Luncheons and breaks will be provided along with vendor receptions both Monday and Tuesday.

New Orleans has always been an exciting location to visit and we are very excited to host a conference to celebrate our 30th anniversary in this fascinating city.

For those interested in other regional conferences in 2020, please note that the Northeast Utilities Revenue Protection Association (NURPA), the Midwest Energy Theft Association (META) and the Southern States Revenue Protection Association (SSRPA) will **NOT** be holding conferences in 2020 in support of IURPA's 30th anniversary conference.

We hope you plan to join us in New Orleans in May!

THE SHORT-COMINGS OF AMI RSS TECHNOLOGY

BY CHRISTINE SMITH, META VICE PRESIDENT



Christine Smith

During a remote reconnect procedure Dec. 7 of last year, a We Energies field servicer witnessed an arc flash that caused serious damage to an electric service located in the basement of a multi-unit apartment building.

To identify the root cause of the arc flash, a “Significant Incident Investigation” was completed. The investigation determined that the remotely disconnected service had been bypassed in a configuration that could not be detected by the meter and would therefore not prevent the service switch from closing. In addition, the investigation determined that prior to requesting the remote reconnect, the field servicer had not completed the necessary on-site safety checks that would have identified the bypass and prevented the arc flash.

December is typically the start of We Energies “mass reconnect.” It is the time of year when the weather in Wisconsin turns colder, and we return to all disconnected residential premises to reconnect the service.

While on-site, the field servicer attempts to make contact with the customer. If the customer is home and answers the door, the field servicer inspects the socket, performs all the necessary voltage and safety checks, verifies that the main disconnect is open, and calls the office to have the meter reconnected via the remote service switch.

In this instance, the field servicer admittedly did not perform the voltage and safety checks. Consequently, he did not find the 12-gauge, solid-core copper wire strung between the line and load-side meter terminals on the right side of the meter. More importantly, he did not find the 12-gauge, solid-core copper wire connecting the load-side meter terminals, creating a short that, when the meter was remotely reconnected, resulted in an arc flash.

The servicer stated that when the arc flash occurred, he was standing inches from the meter, waiting to hear the familiar click signaling the service switch had closed and the meter was reconnected. Instead, he heard the click instantly followed by a loud bang, flames, sparks and smoke erupting from the meter socket.

Within the five-meter set, the arc flash destroyed the disconnected customer’s meter socket, as well as the neighboring socket. The entire service was deemed unsafe and had to be disconnected at the pole, leaving several customers without electricity for 11 days. Although he was surprised and alarmed, the field servicer was not injured.

The meter being remotely reconnected was a Form 2S advanced metering infrastructure (AMI) meter, equipped with a remote service switch (RSS). The meter was installed in a single phase, self-contained, 120/240-volt, three-wire service. At the time of the remote reconnect, the main disconnect was open, and the AMI RSS meter operated as intended.

Consistent with industrywide standards, in this type of metering circuit, the neutral passes through the socket and is not connected to the meter (Figure 1). Because the neutral is not connected to the meter, the AMI RSS meter cannot detect when both load-side meter terminals are connected to the same voltage source (Figure 2). As a result, the AMI RSS meter will not prevent the remote service switch from closing under these conditions, and closing the switch will result in an arc flash.

When an AMI RSS meter is checking for load-side voltage, often referred to as “backfeed,” prior to remotely reconnecting, the meter is verifying that there is no difference in voltage between the two load-side meter terminals. If the meter does not detect a difference in voltage, the remote service switch will close.

Although the AMI RSS meter can identify load-side voltage, it cannot detect the voltage if there is a short resulting in both load-side terminals being energized by the same voltage source. The short could be ahead of the main disconnect or after the main disconnect. Regardless of where the short is located, if no difference in voltage is detected on the load-side meter terminals, the switch will close and there will be an arc flash.

In this case, the bypass installed between the load-side meter terminals created a short that was energized by the single line-to-load bypass. Because both load-side meter terminals were energized by the same leg of the single-phase service (Figure 3) the customer was able to use all of their 120-volt lighting and equipment, but none of their 240-volt equipment.

This configuration also prevented the meter from sending a load-side voltage flag, reducing the likelihood that the bypass would be discovered through data analytics. Because neither the AMI RSS meter nor the on-site field servicer detected that both load-side meter terminals were connected to the same voltage source, the reconnect signal was sent, the remote service switch closed, and the load-to-load side short resulted in an arc flash.

By failing to complete the proper reconnect process, the field servicer serendipitously provided insight into what was thought to be a rare bypass configuration. The significant incident investigation brought awareness to all field personnel of this bypass configuration, the reasons a customer might choose to bypass in this manner, and the safety hazards associated with this type of bypass.

As a result, the revenue protection department has been made aware of several disconnected services that were bypassed in the same manner. Most of these bypasses were discovered and disassembled by servicers conducting on-site reconnections during the 2018 “mass reconnect.”

The electric field operations trouble group identified one bypass during the 2019 disconnect season where the remote reconnect resulted in an arc flash that blew the fuse at the pole top transformer, causing an outage at several neighboring homes. The troubleshooters traced the source of the outage back to a disconnected single-family home where they found the remnants of this same bypass configuration.

The suspect had used an 8-gauge stranded wire instead of a 12-gauge wire. The meter socket was destroyed in the arc flash (Figure 4). Instead of being reconnected, the service had to be disconnected at the pole and replaced prior to restoration.

At this point, we have been left to wonder how many additional arc flashes have occurred, but were not recognized or brought to our attention.

Unless an employee is sent to investigate a failed remote reconnect, or we are in the midst of our mass reconnect, we no longer have an employee on-site to verify the safety and condition of a service before it is reconnected. If a short exists somewhere in the service, and neither the AMI RSS meter nor a field employee is able to identify the presence of the short prior to reconnection, sending the remote reconnect signal will result in an arc flash. That arc flash has the potential to cause property damage and/or personal injury

If this method of bypassing after disconnection becomes a trend, using data analytics to identify and follow up on all power outages that occur after disconnection, not just those with a load-side voltage flag, will be a key component in minimizing the risk of arc flash. If the utility does not use data analytics and/or does not employ adequate resources to follow up on all of the identified power outages, the consequences could be significant.

This article represents information specific to the AMI RSS meters used by We Energies. To assess the capabilities of the AMI RSS meters used by a particular utility, contact the meter manufacturer.

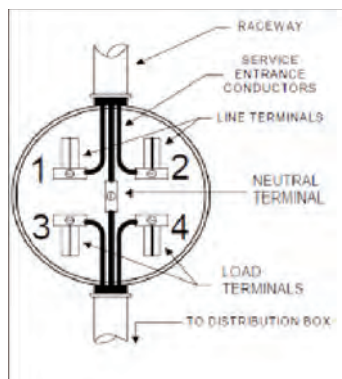


Figure 1: Form 2 meter socket.

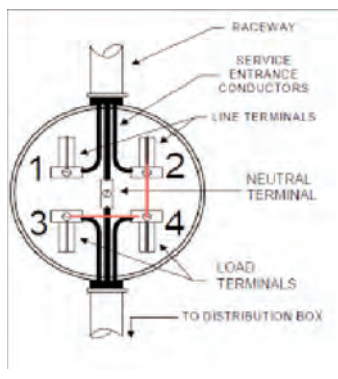


Figure 2: Example of the same voltage source (2-4) energizing both load-side terminals (3-4).



Figure 3: Bypass configuration on the back of a Form 2 meter. Both load-side terminals would be fed by the same voltage source



Figure 4: Remnants of a load-to-load short and socket damage discovered at a single-family home.

Detection or Prevention?

**By Kevin Lumsden
Supervisor, BGE Theft of Energy**



Kevin Lumsden
Supervisor, BGE
Theft of Energy

As I'm writing this article I can't help but recall a conversation with a vendor at a prior utility conference. The vendor had commented on how his product could solve my energy theft problem. My response was a bit direct: "Your product can only detect energy theft, not prevent it". It was not my intention to be rude but I could see from his expression he was not happy with my reply. I spent the next 10 minutes or so trying to soften my response by identifying the challenges of energy theft in the Baltimore area. I highlighted that energy theft had reached epidemic proportions (more work than resources) and damage to our equipment is so severe it's often unrecognizable. Every commercial theft product currently available had been defeated in some form or another. Baltimore is one of the most severe testing grounds for a theft product to survive. "Can your product prevent those issues" was my question to the vendor. His reply was a quiet and somber "No.....it can't".

The purpose of the story was to highlight an issue we all face regarding our energy theft challenges - what's the right balance between detection and prevention? Both elements are critical in any energy theft operation, but given certain circumstances, one may become more important and necessary than the other. The circumstances that exist in Baltimore have driven us to adopt a strategy heavy on prevention. We rely on detection devices and processes to highlight the magnitude of theft in ways we may not be able to otherwise quantify. As important as detection is, it does not fix energy theft - it only lets us know how bad it really is. Anyone that works a neighborhood/territory can intuitively tell you the extent of your theft issue without the investment of detection products.

Prevention is much harder to effectively incorporate. Much of what is commercially available is not tailored specifically for prevention (with some exceptions). Availability of preventive products simply does not exist for some theft challenges (high damage rates, overhead twin services, etc.). I know some will argue that a lock prevents theft. In some cases, that's true, but even the best locks get defeated in extreme environments. Our theft investigators have defeated every locking product available - and we do so to better understand the product's vulnerabilities and where it's most practical to deploy.

That's not meant to be a criticism of locking devices; we use them and will continue to do so. The preventive devices I'm referring to have a high success rate in even the most extreme environments. Preventive products must endure extremely harsh treatment, as they will be tested with very destructive methods. In many cases, a preventive product has not yet been conceived and manufactured. Many utilities (us included) adopt their theft strategies based solely on what is commercially available. We're changing that.

Detection or prevention is not an either/or proposition. Every utility needs to determine what the appropriate mix between the two should be. The challenge becomes the difference between what that balance is, vs. what it should be. I can identify what the balance of detection/prevention is within our business - but it's not the same as what that balance should be. We're constantly trying to move our organization to being more proactive (vs. reactive) in dealing with theft and that drives a need toward more preventive measures. We haven't found a solution to every problem, but by placing a heavy emphasis on prevention, we're moving in the right direction at a faster pace than before. Our Theft Sleeve is a good example. It's a unique solution to preventing an overhead service from being tampered with - and in our deployment in Baltimore's challenging areas, it's proven 100% successful so far. Our Innovation Central campaign is designed to allow creative ideas like our Theft Sleeve to progress from initial concept to reality. We fully leverage that campaign to develop new ideas relative to energy theft to prevent the theft we encounter in Baltimore - a concept we refer to as "Theft Hardening". As our efforts to develop new products advance, I'm hopeful to report out on those successes in future articles.

If you have not already done so, ask yourself the question about what level of prevention you should have in your area, and what you're doing about it. Discuss those challenges with your manufacturing partners to help force the industry to create new and more preventive products. Share those challenges within the NURPA community. Collectively we command a voice within the industry that can drive innovation and realize the birth of new products. Don't just be satisfied with what's available - be a driver of innovation in your business. The more requests manufacturers receive relative to an issue, the more likely they are to commit to a solution. To our manufacturing partners - we have ideas, and we'll be calling you!

THEFT STOPS HERE

INNER-TITE®

Serving Utilities Since 1932



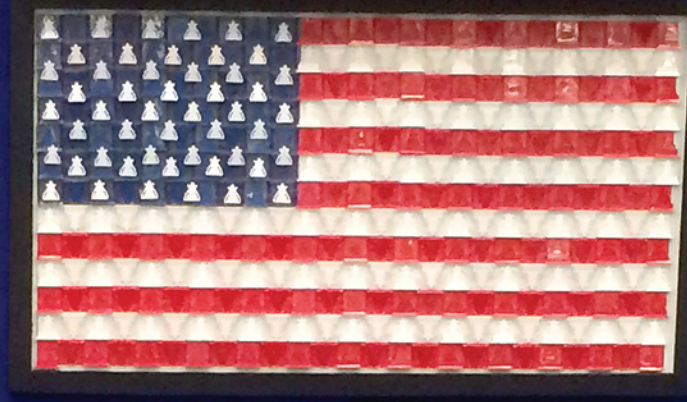
INNER-TITE
Water Meter Locking Devices

- Protect Metering Equipment
- Enhance Revenue Protection
- Effectively Disconnect Service

INNER-TITE
Gas Meter Locking Devices

- Protect Metering Equipment
- Comply with Federal Code
- Safely Disconnect Service

Barrel Locks and Keys



INNER-TITE
Electric Meter Locking Devices

- Protect Metering Equipment
- Enhance Revenue Protection
- Safely Disconnect Service



Agbay Barrel Lock & Key System

Fort Knox Lock

Smart Ring

Twist-Tite Wire Seal

Clearseal

INNER-TITE
Twist-Tite Wire Seal



INNER-TITE®

Congratulations IURPA
30 Years Protecting Revenues

IURPA! International Utilities Revenue Protection Association Inc.

1990 - 2020



EXPECT MORE...AND GET IT!
www.inner-tite.com • 508-829-6361 • security@inner-tite.com



Legalities of Self Defense
By Kevin Lumsden
Supervisor, BGE Theft of Energy
Co-Owner, Lumsden Martial Arts

What's a self defense article doing in an IURPA newsletter? The answer should be obvious; any utility that has employees working in the field will encounter situations that may warrant the employee defending themselves. This gets even more probable with Revenue Protection work. Anyone who spends time in the field in a utility position has encountered more than one irate individual intent on causing them harm. While all the aspects of a threatening encounter are beyond the scope of this short article, I'll focus on one that often gets overlooked and rarely explained correctly – legality of your actions in a self-defense scenario.

I am not a lawyer. My information comes from 47 years of experience training in and teaching several martial arts systems, coupled with a great deal of study on legalities of force on force encounter situations. It's also based on an understanding that any actions we take while in the field may present significant challenges for our employer. This article is not intended to displace any of the policies of your utility employer, so please be sure you follow whatever requirements may be established regarding your employment and their view of how you should handle threatening situations.

Disclaimer aside – let's get to the specifics. Every individual has an inherent right to self-defense. If your life is in jeopardy, you have the right to take an appropriate level of action to prevent harm to yourself or others. Many force on force experts will talk about the "fight after the fight" – that means dealing with the legal consequences after the physical encounter. Take the wrong actions in a confrontation and the legal battle could be much more difficult than the actual physical one. Being able to physically defend yourself is a good thing – but applying an MMA style beatdown on someone that cusses you out for disconnecting their service is entirely different and uncalled for. Even if you are physically capable of doing the above – it's almost certain to get you in hot water with both your employer, and possibly earn you a law suit. Deadly force encounters require you to prove 5 aspects to justify your actions. An under-

standing of these aspects is also directly applicable to the more common non-deadly self-defense situations utility field employees may encounter:

Innocence: How do you justify that you're not instigating an issue? Did you deliver the first strike? Being able to prove you're a neutral party is key. "I'm a utility employee responding to XXXX – I'm not looking for any trouble". Your employment status goes a long way in establishing your innocence.

Imminence: Your actions, at a specific time were necessary to avert a worse outcome. An imminent attack is one that can't be avoided in any other way than with force. "Had I not taken the action I did at the time I did, I would not be here today".

Proportionality: Did you use only a level of force equivalent to the level of force of your attacker? Continuing to pummel a downed opponent who's nearly unconscious does not demonstrate a proportional use of force (or a reasonable one). Proportionality follows the Use of Force Escalation (see graphic as an example).

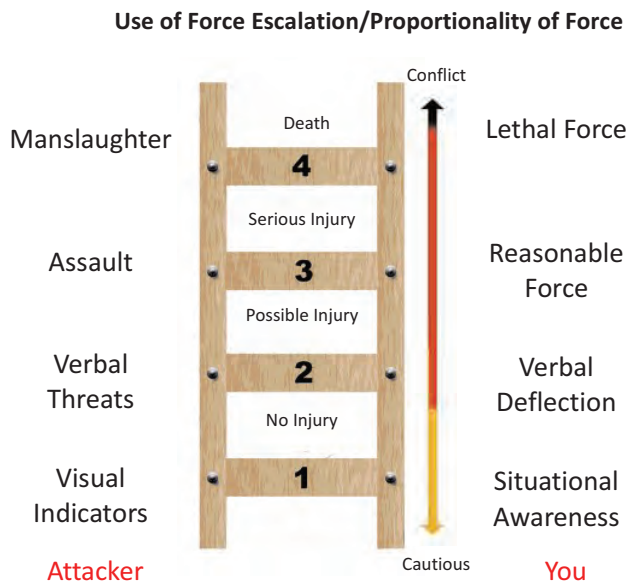
Avoidance: This is the difference between the aggressor or the defender. Did you attempt to not engage the situation in the first place? Retreating is an example of avoidance. A hand's up "I don't want any trouble" neutral posture goes a long way in visually showing bystanders you intended to avoid any trouble.

Reasonableness: Your actions must be the same as a reasonable and prudent person, in the same or similar circumstances and who possesses the same physical characteristics, specialized knowledge and mental characteristics as you did at the time you used defensive force. Would a jury of your peers find your actions responsible and justified? All this just because one of your employees gets in a confrontation with a customer? If this sounds complex, it can be. Defending yourself is never easy, physically or legally. Developing an understanding of the legalities of your actions can help assure you can be more successful if your actions wind you in court.

Continued on page 11

Use of Force Ladders are used worldwide by Police and Security agencies to gauge a corresponding level of force necessary to address a threat. Each action of the individual intent on harming you is met with a proportional action by you. The ladder escalates from non-contact, visual indicators to lethal force response for manslaughter threats. Use of Force escalation determines the proportionality of your response to a threat.

References: For a more thorough explanation of the legalities of Self Defense, I strongly encourage you to research Andrew Branca's "The Law of Self Defense" book and seminars. As a graduate of his seminar, I incorporated his 5 aspects in developing this article. I have only scratched the surface of his exhaustive and essential work on self-defense legalities. Additionally, there are many Use of Force ladders that have been developed. The graphic in this text is tailored more directly to civilian use and was adopted from one like Jim Wagner's Reality Based Self Defense (jimwagnerrealitybased.com).



UK SMART METER ROLLOUT!
MIKE WILKINSON, VICE CHAIRMAN UKRPA

The UK Government had mandated that all the gas and electricity supply companies had to fit up to 53 million Smart Meters to their customers by 2020 or face potential financial penalties. Issues have been well documented especially when the meter reading data doesn't get transferred when customers change to another supply company.



MIKE WILKINSON

OFGEM the energy government department has now delayed the end date to 2024, to allow issues to be sorted.

CANNABIS GROWS ON!!!
"Huge £4m Scunthorpe drugs factory is the biggest detective has seen in 30 years"

Humberside Police DI John Cram described the cannabis factory on Park Farm Road as a 'hugely significant find' on the 30th July 2019! A detective investigating a huge drugs factory discovered in Scunthorpe has said it is the biggest he has seen in 30 years of working with Humberside Police.

Officers raided a unit on the Foxhills Industrial Estate on Monday and found more than 15,000 cannabis plants in various stages of cultivation, with an estimated total street value of between £2.5 million and £4 million. Three men were arrested after a warrant was executed at the building and a further two are wanted by police, although officers believe the men could be modern-day slaves living in poor conditions at the Park Farm Road site.

The factory, described as a "very professional set-up", was uncovered following police enquiries and concerns raised by members of the public. Speaking to Scunthorpe Live, Humberside Police Detective Inspector John Cram said: "This is a hugely significant find. It is a very professional set-up which we believe to have been ongoing and operating for a period of months.

This find will greatly reduce the amount of the 'drug' getting onto the streets, and will more than likely put the price of a 'joint' up!



PARTNERS IN FIGHTING CRIME
A DAY IN THE LIFE OF AN INVESTIGATOR

While the excitement of being an investigator is great the job it comes with a lot of ups and downs. On one side you're out catching the bad guy stealing and then you come across the single mother with 3 kids who just did not have enough to make ends meet and made a poor decision to keep her kids comfortable. The day in the life of an investigator can be rewarding on one end by making a positive impact in lost revenues, and on the other dealing with hostile customers or individuals just trying to get by. Every day is an adventure and you never know what or who you are going to be dealing with.



JOSE ESTELA



JOSE ROMAN

together never leaves the element of surprise open because we are constantly watching over each other to make sure the other is safe and that no one is going to try to harm us while we are disassembling a tampered meter or pulling out jumpers from a meter base.

We have worked together to catch thieves on numerous occasions, in the past we have shared information with individuals identified to us as a Fixer (the hook up man). Jose Estela gave some information to Jose Roman and he investigated this individual which resulted in him catching the fixer red handed while installing jumpers into the meter base. With a video we were able to land him an easy conviction in court.

With Duke Energy and Piedmont Natural Gas merging, there were a lot of uncertainties. The transition of joining forces investigating both gas and electric came with a lot of benefits. While at Duke being a Revenue Assurance Investigator, I (Jose Roman) was just looking for electric theft. While at Piedmont being a Corporate Security Investigator, I (Jose Estela) was primarily looking for gas theft. As investigators in utilities, we worked together in keeping other utilities informed of our findings and learning from one another along the way. The attitude was if they are stealing from one utility they might be stealing from another. Learning best practices in both industries now we were one team and we are assisting each other to catch that "thief" checking each while at the premise.

Although we leave some residents in an uncomfortable and frustrating position, the feeling of knowing that we have left a premise safe from theft makes the job easier to handle and we can leave the location knowing that we have potentially stopped all the risks such as accidental shock, fire, explosion or even death.

Working together as a team has really benefited us both and now we are able to "kill 2 birds with 1 stone" while on a property and having each other's back. This also gives us an upper hand on the safety aspect of the whole job. Working

Teaming up also has resulted in the company recovering lost revenue through theft. As we all know our paying customers are virtually responsible for paying for our theft. We have been able to "stop the bleeding" and reduce the number of cases of theft by teamworking. We have worked with other departments, provided training within and outside the company and educated law enforcement. With of our efforts together we feel that we have made a big difference together. We will be always on the lookout for theft to keep our employees, our customers and our communities safe!

Rogue Meters

A new threat to Revenue Protection professionals in Southern Africa



Rens Bindeman

Utilities in Africa have for many years experienced the phenomena of meters being moved illegally from one Utilities area of responsibility to another for a number of different reasons by consumers and unscrupulous meter installers. This phenomena was labelled as “foreign meters” and were dealt with in the same way as tampered meters. These meters are post as well as prepaid meters and incidents are found to be definitely not linked to any organized crime entities and the only common factor that could be found was the fact that mostly Utility staff or Utility Contractors were involved.

However, during 2018 reports started flowing in to SARPA which indicated that there was a new phenomenon developing whereby prepaid meters foreign to the Utilities own meter fleet were now been used to replace the Utilities meters without their knowledge or permission. These meters were apparently not purchased nor installed by a Utility or a Utility agent and the revenue was not going to the Utility, but to a third party. It was also very difficult to detect these as field teams cannot easily verify which meters are on the data base while in the field. It was also reported that these meters looked identical to those already in use by the Utilities.

A probe was launched by SARPA to obtain further information regarding this possible threat. It was seen as crucial to determine what the modus operandi is of the entities performing such acts. There was also a need to determine what is the reason for this happening all of a sudden and what could the impact be on Utilities if this threat was not addressed immediately. It did not take long to realize that the processes of “sub metering” and “reselling of electricity” which was introduced a few years ago in the region, has created the perfect environment for certain individuals to find a nice loophole to exploit.

This concept of reselling of electricity could be summed up as follows: - A Utility installs a bulk meter at the consumers property on the incoming feed and the body corporation or an external reseller company installs their own meters in such complexes or flats, in order to monitor consumption of each tenant. However, it has been found that this concept has morphed into normal individual home owners also obtaining such meters and using it to monitor the consumption of their “back yard dwellers”.

Once SARPA started to examine the source of these meters, we became aware of the huge availability of such meters in the market place. We found that various kinds of meter were available either over the counter, in local hardware stores, through online vendors or via social media platforms, where entrepreneurs make business of selling electricity meters in an array of different prices and package deals. Some even vending companies even advertise “free meters”.

Several reports were followed up which included: individuals advertising on line that they could supply the cheapest metering installations, that their electricity is much cheaper than the Utilities, and that the consumer will never receive another Utility electricity bill. It was also determined that in some areas individuals were “walking the streets” selling electricity meters out of plastic bags.

During the SARPA 2018 Convention in August the concerns of the investigation group was raised to the forum. Everyone present recognised the imminent threat of this phenomena to all Utilities in the Southern African region and the forum requested that swift action should be taken to analyse what the extent of the problem is. It was therefore decided to select a pilot site, where more information could be obtained and the extent of the problem could be analysed. A specific Metro was chosen for this exercise and all further investigations were halted in other areas, in order not to interfere with the processes followed in the pilot project.

Inputs were requested at the Convention regarding the naming of this new threat and after deliberation between the key role players, it was decided to accept the proposal of “rogue meters” The Cambridge Dictionary definition of the word rogue is: - “explaining the process of something behaving in ways that are not expected or not normal, often in a way that causes damage.

The report from the pilot site was presented at a SARPA Branch meeting in Cape Town in February 2019 and together with reports from other sites, the following conclusions could be made.

There were three different types of rogue meter installations detected up to date namely:-

1. Installation of a rouge meter on the supply side of the original Utility meter,

2. Replacing the Utility meter with a rogue meter and then discarding the Utility meter,
3. Connecting a cable to the incoming supply before the utility meter and then feeding sub-housing units down stream of the meter.

It must be understood that the normal installation of a “sub meter” should be after the Utility meter and from the distribution board of the premises. The first method of installation are mostly been done by internal staff, who installs the rogue meter under the pretence of a “check meter” to monitor a possible faulty meter. The payments then goes to the installer’s bank account and the consumer is mostly oblivious of the fact that this is an illegal act. The second method are done also by an installer, either in collusion with the consumer or on his own accord and the money could go to either’s account. The third method is presumably done with the knowledge of the consumer, as the money paid by the sub tenant goes into his / her account after the vending company taking off their commission.

It was also noted that if an Utility has the processes, resources and technology to accurately monitor the purchasing patterns of each of its prepaid consumers, such fraudulent acts should be detected in a short period of time. However, if these don’t exist, these actions could go undetected for a very long period of time. It was also noted from the report that companies and associations involved in the vending process were not prepared to supply information regarding their customer base or allow anyone access to the money trail. Where at first they pledged their support, they were soon asking for court orders under the “Information Act”. In the pilot site this was however temporarily circumvented with an MOU between the Utility and the Service Provider.

The statement that consumers “will never again receive a Utility bill” opens up a whole new angle that has not even been addressed at this stage and that is the fact that post-paid meters could also be replaced with rogue meters. The current practice of meter readers finding a prepaid meter in the place of a post-paid meter in the field is usually for them to note it down and just to ignore it in following readings. In bigger Utilities this will be identified as a problem immediately, but in smaller Utilities this installation might go missing from the revenue stream.

The biggest danger is the fact that some of these actions are in fact very difficult to detect them,

as the sales on the reports are often not affected in such a way that it could be easily detected. In some cases where the utility meters were removed, the guilty parties were still vending in smaller amounts, in order to stay off the radar of revenue protection officials. Therefore, it was concluded that rogue meters could be accounting for the unexplained increase in electricity consumption in most of the utilities in the region and subsequently the increase in non-technical (commercial) losses. The only proven way to detect these meters is through performing sweeping meter audits, which is a costly and time consuming exercise.

If this threat is carefully considered, one must conclude that there should be mostly a measure of complicity between customers and rogue meter installers. Customers ought to suspect something is wrong, unless totally ignorant. This should be prompted by the fact that there is no change in their consumption, or they receive supply at a rate lower than the utilities tariffs, which is of course not possible. It is further ignorant to believe that a customer soliciting a meter installation via a social media platform has ethical motives.

It was therefore decided to establish a Task Team which would consider different ways on how to combat this threat. The most relevant role players from SARPA, Utilities, Judicial representatives, Resellers Association, STS Association and Corporate Governance (COGTA) were invited and an Action Plan was drawn up. It was also decided to take the legal aspects to the broader Legal fraternity, in order to get some legal opinions regarding the different ways to prosecute such offenders. It was also suggested to develop a guideline for all those involved in the investigation of such crimes, in order to understand the different steps to take. It will only take one badly prepared case to set a precedent for others to walk away freely in the future

Progress regarding all of this was reported at the recent 2019 SARPA Convention in August during a panel discussion. Stakeholders were asked to come forward with suggestions on how to address this threat. It was once again highlighted that the main challenge would be to find ways to prosecute those involved in these illegal actions and determine how to get government officials and politicians to fathom the size of this threat to state owned Utilities.

As part of this process all laws and bylaws have been scrutinized to determine which ones could be used or need to be revised in order to deal effectively with these types of crimes. One of such Laws is the new Criminal matters Amendment Act (CMA), which was initiated by SARPA. The goal of this Act is to counter the theft or damage of essential infrastructure in the country. A tampering clause was included into this Act by SARPA, in an effort to replace the “tampering clauses” that was excluded from the Electricity Act a few years ago. Since then only Municipal Bylaws could be used to act against those tampering with meters. It is however not easy to start prosecuting using the CMA, as the National Prosecuting Authority (NPA) are monitoring all the cases reported under this Act.

The challenge is to determine where does the essential infrastructure start and end with relation to electricity distribution services. The common feeling is that it starts at the generation point and ends at the meter. If that is the case, the rogue metering issue should be falling within this ambit. A positive legal opinion has been obtained from COGTA, the government department that championed the promulgation of the CMA. However, meetings with representatives from the NPA, Police Legal Department and Department of Justice has resulted in a “thumbs down” for this idea. It was concluded that this Act

could only be utilized if the essential service to a consumer was interrupted or taken away through the act of the perpetrator. However, tampering with a meter does not fit that description and the police legal team emphasized that the fact that this act does not allow bail, this could result in civil suits against the police and the Utilities for wrongful arrests. It was decided that seeing that there is an element of fraud in all these actions, this should be the main charge followed by tampering with electricity, miscellaneous damage to property and racketeering.

Taking all of this into consideration, the need to seek other avenues to deal with this challenge has left Revenue Protection, Police officials and Legal entities with the mutual understanding that we do not have the necessary answers at this stage to deal effectively with this new challenge.

Going forward, we have decided to keep the information about the threat of rouge meters out of the media for now, in order to prevent everyone jumping on the band wagon to also make a quick buck. We however are under no illusion regarding the extent of this threat and understand that smaller Utilities are really in danger to losing their entire customer base over a very short period of time. It is envisaged to present a paper on this phenomena at the 2020 IURPA Convention.

IURPA – 2020 ANNUAL MEMBERSHIP

PLEASE PRINT

Name: _____
 Company: _____ Title: _____
 Mailing Address: _____
 City: _____ State: _____ Country: _____ Zip: _____
 Telephone: _____ Fax: _____ E-Mail: _____
 Utility Type: Gas _____ Electric _____ Water _____ Cable _____ Other _____
 Payment Method: Check Enclosed _____ Credit Card _____

Credit Card Payments Information:

Name as it appears on the card: _____
 Billing Address: _____
 City: _____ Zip Code: _____
 ___ VISA ___ MC ___ / ___ / ___ / ___ Expires: ___ / ___

**Note: Credit card payments may be made directly from the IURPA website. Please go to: www.IURPA.org
 Annual dues are \$75 (US) per member.**

Payments may be made by check or credit card. Please send form along with your payment.

Make checks payable to IURPA and mail to: George A. Balsamo, c/o IURPA, 3 Elaine Drive, Seymour, CT 06483



IURPA Publishing Team
 Brody Printing Company
 265 Central Avenue
 Bridgeport, CT 06607







IURPA • 29 Years





The International Utilities Revenue Protection Association was founded in 1990 to protect member utility companies worldwide from revenue losses associated with unauthorized use of service. In twenty-four years, the organization has grown from a small regional group into an association that includes representatives of more than 400 utility companies around the world.

IURPA Officers



-  **Chairman**
Steve Sprague
 Portland General Electric Company
 Portland, OR 97202
 steve.spaugue@pgn.com
-  **Vice Chairman**
Paul Unruh
 ComEd
 Oakbrook, IL 60523
 Paul.Unruh@ComEd.com
-  **Secretary**
Jeff Kauf
 L.A. Dept. of Water & Power
 Van Nuys, CA 91405
 jeffrey.kauf@ladwp.com
-  **Treasurer**
Danny North
 GreyStone Power Corp
 4040 Bankhead Hwy
 Douglasville, Ga. 30134
 danny.north@greystonepower.com

IURPA Directors

-  **John L. Kratzinger**
 PECO Energy
-  **Patricia Uhlman**
 Eversource Energy
-  **Gary Signorelli**
 Duke Energy-FL
-  **Jeff Cornelius**
 Peace River Electric Co-op

-  **Cleve Freeman**
 Southern California Gas Co.
-  **Michael Szilvagy**
 DTE Energy
-  **Webmaster**
Kurt Roussel
 We Energies
-  **Finance Director**
George Balsamo
 Northeast Utilities/ United Illuminating

International Liaisons

-  **Mike Wilkinson**
 Vice Chairman UKRPA, RWE npower
 United Kingdom
-  **Itzick Michaeli**
 Israel Electric Corporation
 Afula, Isreal
-  **Rens Bindeman**
 SARPA
 South Africa

Please send all correspondence to:
 IURPA Publishing Team
 Brody Printing Company
 265 Central Avenue, Bridgeport, CT 06607
 phone 203 384-9313 • fax: 203 336-0871
 e-mail: perch@brodyprinting.com

For Application, please go to our website www.iurpa.org

No part of this newsletter may be transmitted or reproduced without the prior written consent of IURPA. Opinions expressed in this newsletter by the authors are their own and do not reflect those of the editors of the IURPA Newsletter Committee, or its Officers, or Board of Directors.