

Volume 14, Issue 2 October, 2004

GREAT NORTHEAST BLACKOUT, AUGUST 2003



REVENUE SECURITY



SIDEWINDER LOCKS

PROTECT AGAINST THEFT OF SERVICES



BULLSEYE RINGLESS METER-LOCKS











- ▼ USER-FRIENDLY MCGARD TRI-TOOL HEY OPERATES ALL THREE MCGARD METER LOCK STYLES
 - ▼ EXCLUSIVE OR MULTIPLE REGISTERED HEY PATTERNS AVAILABLE FOR CONTROLLED ACCESS USING MCGARD'S PATENTED HEYS
- ▼ PROPRIETARY ARMORGARD™ PLATING TO RESIST CORROSION—EXCEEDS ALL INDUSTRY STANDARDS
 - ▼ SIDEWINDERS & SNAP-RINGS EASILY INSTALL IN SECONDS WITHOUT TOOLS OR HEYS
 - **▼** ACCEPTS STANDARD SEALS
 - **▼** PATENT PENDING







THE SUM IS GREATER THAN THE TOTAL OF IT'S PARTS

ynergy, is the term commonly used when describing how as a group, when everyone works together, the end result is greater than its parts. While many people may not believe in that, I do. I see it all the time. And, what's really fantastic, is that I've been placed in a position in IURPA where I see it clearly. It's absolutely amazing. The RP Departments worldwide are synergistic, and they don't even know it. The profession keeps moving forward based upon the individual actions of our members.

This year, as Chairman, I've had the opportunity to attend and participate in most of the regional conferences, and this has allowed me to see what's going on in each region. It's easy to tell "what's going on" because the agendas presented by the regional groups are addressing the needs and wants of the RP professional in each region. This has allowed for the unprecedented sharing of information for strategies, processes, and methodologies that have worked somewhere else with measurable success.

That which grows slowly, endures. Participants of the conferences bring -Josia Gilbert Holland this information back to their individual utilities, tweak the ideas to work within their systems, and reap the benefits. Through networking with other RP professionals in the IURPA community, we learn from the best and implement. Our individual companies prosper because of it.

This year, I attended the conferences presented by SURPA/ SCURPA, META, and WSUTA/IURPA conferences. At each conference, I learned something. You name it, advanced metering, "Thinking Outside the Box" (which I admit caught me completely

On THE INSIDE

The Sum is Greater Than the Total of It's Parts Check Meters-A Valuable Tool in the Fight to Protect Revenue WSUTA/IURPA Conference

Hide and Seek

Internal Security - Is Your Barrel Lock & Key System Compromised?

Revenue Assurance with AMR The Good, The Bad, and The Possibilities

Stop - Look - Listen

T&D Crews Help Protect SCE Revenue



Kurt Roussell **IURPA** Chairman

Progress, however, of the best kind, is

comparatively slow. Great results cannot

be achieved at once; and we must be

step by step.

satisfied to advance in life as we walk,

There is no royal road to anything. One

thing at a time, all things in succession.

That which grows fast, withers as rapidly.

— Samuel Smiles

by surprise. I expected the "usual" corporate speak, but was I way off course. It was about data mining within your billing systems looking for abnormalities that have been impacting revenues) which is an area that I wish to address at my company.

The META conference was chock full of information on protecting revenues through data mining, the impact of e-commerce fraud, and performance benchmarking.

Personally, one of the highlights of this conference was the presentation on Gas Theft that was presented by Jeff Harris of Missouri Gas Company. It included video of an actual investigation, and news

> stories regarding their RP activities. If you haven't met Jeff Harris, you should.

> The joint conference with WSUTA and IURPA was truly an informative event. WSUTA was an excellent host, and we were fortunate to have David Brown from the United Kingdom and Itzick Michaeli from Israel to provide an international prospective.

> The two quotes highlighted in this article are "quotable quotes" regarding cumulative results. I believe they are

reflective of IURPA and our regional affiliates. Through the efforts of each of you individually and collectively, our regional groups, and our international presence, we are slowly marching along. We're getting better every day, and our companies are better for it.

I'm pleased to announce the Board of Directors has elected me to serve again in my capacity for 2005. I am honored to serve. For those of you that don't know, Timothy Hopper has left the industry and has resigned his position with IURPA. He has moved into another industry combating fraud, and I'm sure, knowing Tim, he will excel.

Jeff Cornelius has been extremely busy because of the double whammy of hurricanes in Florida. As I'm writing this article, Hurricane Ivan (the Terrible) is the next one coming his way. He's managed to save his home thus far (and his sanity...well, maybe that's questionable). Utilities nationwide are providing assistance in helping out by providing people and equipment to help restore power far outside of their normal service territories. It's synergy at work again.

The year 2005 should be an excellent year for revenue protection. It is my expectation for IURPA to continue moving forward. Please continue to support IURPA, refer a friend to the organization for membership, and continue to work safely.

If there is anything I can do, please let me know.



CHECK METERS -A VALUABLE TOOL IN THE FIGHT TO PROTECT REVENUE

REPRINTED WITH PERMISSION FROM METERING INTERNATIONAL



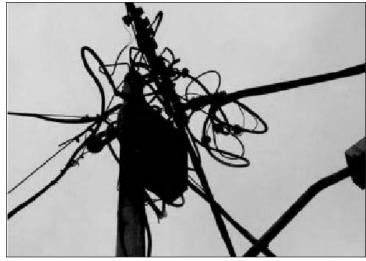
By Yitzhak Michaeli– Afula Regional Director, Israel Electric Corporation, Israel

Preventing the unauthorised use of electricity, as we call it at the Israel Electric Corporation (IEC), has gained significant momentum over the last three years. The decision made in 2000 by the former IEC director general to start addressing the phenomenon of electricity theft with the seriousness it deserves led to the formation of a pilot programme.

Tithin the scope of the programme, the largest operational region in the IEC's northern district, the Afula region –which serves over 100,000 customers – was entrusted with training and overseeing a group of employees who specialise in revenue protection. The pilot aimed to ascertain whether allocating employees and resources to pinpoint, verify and collect revenue is worthwhile. The group consisted of two knowledgeable employees who were experienced in reading meters and performing activities in the field, and an office worker who was trained to make the calculations to establish how much electricity had been stolen. This was necessary when conducting negotiations with customers regarding the refund that would be claimed from them. The results were above expectations. They led to management's decision to formalise the handling of the unauthorised use of electricity, and to set up specialised units in each of the IEC's administrative regions.

CALCULATING THE VALUE OF THE LOSS

The issue of calculating the scope of electricity theft is problematic, since in many cases it is based on an estimate of electricity consumption in the apartment, building or commercial entity. Electricity thieves have two main methods of operating: meter tampering or bypassing the grid, which results in the power used not being reflected in the consumption records. We calculate consumption during the theft period by checking past consumption data, or by recording the consumption for a certain period of time after the



The improvised check meter

theft is discovered and the meter has been changed or the bypass removed. Those who steal electricity are inclined to use it lavishly, which means that relying on previous consumption averages is far from realistic. We have come across many cases when we submitted an invoice and the customer paid it without batting an eyelid – in other words, he got a 'good deal'. We have often come across customers who continue to steal electricity after they have been caught doing so, because of the 'low invoice' they received. There have been quite a few instances where delinquent customers realised that they would be billed for future consumption, and did everything in their power–even at the price of relinquishing comfort by switching off air conditioning or heating–to prove to us that their consumption, both before and after the meter was changed, was similar.

During the course of our work, we often became suspicious that electricity was being stolen at a particular location, or we received information to that effect. Sometimes we conducted secret tests that did not reveal any suspicious findings, but we still felt the electrical consumption recorded on the meter did not appear reasonable, considering the size of the building or the equipment installed (air conditioners, swimming pool, lighting facilities and so forth).

VERIFYING SUSPICIONS

As a result, we were asked to find a method that would enable us to verify our suspicions before we submitted a claim to a customer. Moreover, caution and secrecy were necessary to prevent the suspicious customer from realising that we were on his track and disposing of any trace of electricity theft. We have learned that the safest way is by measuring and comparing the customer's meter readings to the amount of electricity supplied to him from the grid. Our employees designed an improvised 'check meter', which was hidden in a connection box placed at the top of the electricity pole supplying the customer's facility.

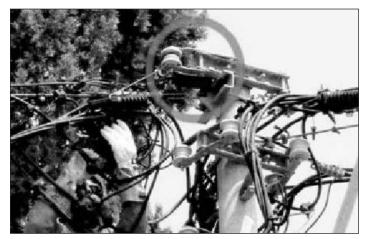
This 'check meter' quickly yielded impressive results. It demonstrated the true extent of the power used, and the refunded revenue grew. The drawbacks, however, were obvious – the device was awkward, cumbersome to install and stood out from a distance. Moreover, in order to read the meter, it was necessary to climb the pole and open the box in which it was installed.

During a visit I made to ComEd's meter system at the company's commercial headquarters in Oak Brook, Illinois, I was shown a new type of check meter which is being used by ComEd's revenue protection unit. Its small dimensions and the option of reading consumption by remote control make it unique. The meter can be installed on any type of electric pole, in connection boxes and meter cabinets. ComEd personnel's opinion was very positive.

Since equipment of this kind was not being used at the IEC, I recommended that its performance should be tested within the scope of the activities of the specialised unit in the region. In order to assist with decision-making, I conducted a survey among the members of the IURPA (International Utilities Revenue Protection Association). Through the good offices of Woody Woodward, who serves as the association's Webmaster, I asked members to respond to several questions:

REVENUE PROTECTION





The check meter on exposed grid

- Are check meters routinely being used, and how many units are used?
 - How frequently are check meters used and in which cases?
- What is the success rate in court as a result of presenting check meter data?
 - What are the customers' reactions to the meters' findings?

There were dozens of responses, and the results were unequivocal. Most of the organisations employing a check meter recommended it as an essential revenue protection tool. Respondents commented on its convenient use, the significant contribution it makes toward collecting revenue and, primarily, the ability it offers to present the customer with clear proof of the scope of electricity theft. This usually makes it possible to avoid the need to resort to the courts. The users pointed out that the cost of the check meter is recouped within a relatively short time. While opinions concerning the meters used by ComEd were very positive, several users said they also planned to test a check meter that is read by means of a cellular phone.

The specifications of the check meter and the results of the survey were presented to IEC decision-makers, who agreed that the meters should be tested. The IEC national meter department checked the technical specifications and their compatibility to the standards used in the State of Israel and at the IEC, and we purchased 12 meters that can be used for both single and polyphase metering.

THE PILOT BEGINS

The meters arrived in May 2003 and were delivered to the specialised unit in the Afula area for the pilot. We are pleased to say that within approximately four months, the greater part of the meters' cost has been recouped.

The team of investigators from the unit is licensed to implement grid-related tasks independently, enabling them to install the check meters without involving any other technical units. The meters were installed in all possible configurations, to enable the team to thoroughly test the method of connecting the meter's components to an exposed grid and to an insulated grid. In addition the quality of the meter's transmission and data reception by remote control was tested.

No problems in connecting the meter to an exposed upper grid or

to an accumulation strip in connection boxes or meter cabinets were identified. Problems arose – and have yet to be solved – when the meter was connected to an insulated grid (partial reading due to a faulty connection of a phase or two to the grid).

The decision regarding the need to set up a check meter is impacted by two key needs:

- 1. A strong likelihood of electricity theft. In this case, the meter will serve as a tool to measure the extent of the theft and the ensuing data will form a solid basis for calculating revenue reimbursement.
- 2. Suspected electricity thefts. Here the check meter will serve as a tool for verifying the suspicion, and of course for calculating the scope of the theft.

There are various types of check meter on the market, and the IEC intends to examine those that can be read from a distance by means of a cellular phone.

CUSTOMER REACTIONS

An interesting phenomenon that we have come across on several occasions is a sudden and unexplained increase in electricity consumption among customers suspected of stealing electricity, once the pole supplying their home had been equipped with a check meter. One assumes that such customers are more suspicious, and that if they identify unusual movement of IEC employees in the vicinity of their home, or if they spot a 'foreign body' on the pole, they will dispose of the evidence and begin to consume the full kWh.

To prevent this, check meters are installed when customers are not on the premises. Our assessment is that some of the wiring components connected to the check meter stand out from the grid and make it possible to identify the meter. In at least one case, the customer admitted that he sensed our increased presence. Nonetheless, he paid the bill we submitted without argument, as there were clear signs of his having tampered with the meter.

The process of setting up units specialising in handling the unauthorised use of electricity in each of the IEC regions has begun. Check meters will be provided to serve as standard tools for the purpose of verifying cases of electricity theft and determining its scope. It will be necessary to develop a methodical work procedure that will include clear directives with regard to the need to recalibrate the check meter after each use. This is essential to establish the check meter's reliability, in the event that a case reaches the courts.

The trial period in the Afula region is drawing to a close. The report to be forwarded to the IEC marketing department's management will recommend broadening the use of the check meters, ordering check meters measuring up to 600A, and purchasing check meters read by a cellular phone for trial purposes.

ABOUT THE AUTHOR:

Yitzhak Michaeli has been involved with IURPA activities for the past three years. After ten years in the HR department of the Israeli Electric Corp., he was promoted to manage the Afula region, where he ran a successful pilot programme that motivated senior management to allocate additional resources to revenue protection activities.

ABOUT THE UTILITY:

The Israel Electric Corporation (IEC) provides 2.2 million customers in Israel and the Palestinian Authority with electric power. Installed capacity exceeds 9,000 MV and total revenue in 2002 was \$2.7 billion. The IEC operates under the Public Utilities Authority – Electricity, which determines electricity rates and standards.



WSUTA/IURPA CONFERENCE-LAS VEGAS 3-4 NOVEMBER 2004

AN APPRECIATION BY: DAVID BOWN (UKRPA EXECUTIVE COMMITTEE MEMBER AND SIEMENS REVENUE SERVICES PRODUCT MANAGER UK)

have a passion. Many people do. For some it's art, for some it's food, for some it's women, for some it's sport, but for me it's Revenue Protection, which probably explains my sad and lonely existence!

Some of those that know me would call it an obsession. Anyway, I've been involved in RP since 1979, when the UK first really woke up to the challenge it faced from the power thieves. No, don't stop reading. I'm not going to give you a resume of everything that's happened in the last 25 years!

Suffice to say that this job has had me hooked for a long time. Occasionally I get away but it keeps coming back. And I guess that's the point, it's not an area of work in the energy/ utility industry that many warm to or find easy. There are times when it appears that everything is against you. Be it difficult customers, the regulator, consumers' groups, the legal process, budget restrictions or unappreciative bosses who sometimes see the activity as just a complaint generating pursuit and drain on resources who could otherwise be employed on 'core' work.

With de-regulation in the UK came the rush for customers with the energy supply companies falling over themselves with fancy offers to win market share. Every consumer is perceived as an honest prompt paying individual to be nurtured and to not be upset at any cost. Communication in the market has been designed on the assumption that nothing will go wrong, that everyone will act responsibly and without error. But oh shock horror! This is not the case. People are still stealing energy, billing errors have multiplied and bad debts have escalated, mainly caused by supply hopping and poor housekeeping. What is to be done? Who can save us? Well the good news is that there still exists in the UK a select band of highly motivated professional individuals who are dedicated to the survival of effective revenue protection. It was my immense honour to represent these wonderful people at the WSUTA/ IURPA conference held this August in Las Vegas. This was the second such conference I had attended, having been in Atlanta in 2002.

So what of the location? Atlanta was brilliant with hospitality second to none. But what of Las Vegas? Again, the American people took me to their hearts and demonstrated once more that there can not be anywhere else in the world that a visitor is made so welcome.

As for Las Vegas – this should be an entry (or entries) in the New Oxford English Dictionary to describe the indescribable. People who had visited Vegas had tried to give me an impression of what to expect but however well painted nothing can prepare one for the unbelievable experience that awaits. Some may call it sin city (and what's wrong with that!), some a gimmick in the desert but for me it was the most marvellous experience. Everything is done with such class, no expense is spared on pleasing the visitor and the customer service is second to none. Yet it isn't expensive. Due in part to the strong pound perhaps but I found everything to be of excellent value.

I found the conference very informative and it was a great opportunity to meet old friends and develop new relationships (especially with the lady I met in Rio!). The main impression I got and I'm sure that this won't come as a surprise to many is how similar the job and challenges are wherever you are in the world, particularly in regard to assessing losses (or to quote Ed Holmes, 'calculating' losses), difficulties in prosecuting, utility cause losses and the close link with energy theft and cannabis growing.

Many of you reading this article will have been at the conference

or seen the agenda or spoken with colleagues who attended but the highlights included an excellent presentation by Yitzhak Michaeli on RP in Israel, a very interesting development regarding 'presumptive evidence' by John Culwell and AMR theft issues from John Kratzinger and Jim Roscovich of Peco Energy. Then we had Ed Holmes getting down to the 'nitty gritty' with methods for calculating losses and losses at commercial/ industrial



David Bown

sites, which I found particularly relevant to what is going on in the UK at present.

My one over riding memory from the conference was of how everyone joined together as a family, all 'fighting' for the same cause, including the vendors who must not be forgotten and without whom the conference couldn't exist. Everyone was focused on the job and full of enthusiasm. My batteries have been recharged for a further twenty five years!

Finally, but by no means least, I wish to extend my personal thanks to Kurt Roussell, Wayne Wohler, Lynda Steyaert, Steve Ardito, 'Woody' Woodward and George Balsamo for their hospitality and for making me feel so welcome. Also (just in case any of them happen to read this) to the staff and management of the Palms Casino Resort Hotel for helping give me the experience of a lifetime.

I hope to see as many of you as possible at the UKRPA Conference, to be held on 3-4 November at the Hanover International Hotel, Bromsgrove, UK. For further details please email Gary Morris at the UKRPA on ukrpa@gemserv.co.uk or visit www.ukrpa.org.uk



Professional Training & Consulting Since 1973

The Current Diversion CD-ROM

Now Available - Includes

- 15 Minute Training Video
- Five Lesson Investigator Course
- Two Power Point Briefings
- Additional Case Study Images
- Current Diversion Documents File
- Excel Monthly Data Program Shipped in the U.S., \$295.00 Outside the U.S., \$320.00

Shipped within the U.S. on approval.

No prepayment required

To Order Contact Karl Seger:

Telephone 865.986.8026

Fax 865.988.5131

Email karl@accusa.com

Web Site: accusa.com



HIDE AND SEEK

By Karen Sweat

hat do you call an individual with a single service point and two (2) meters? Customer? Prepared? Creative? Thief? "Customer S" had the entire Kansas City Power & Light (KCP&L), Customer Revenue Management Team asking just that question. Luckily the team at KCP&L has a cadre of tools to assist in solving such riddles.

KCP&L has CellNet's automated meter reading (AMR) system installed in over 80% of its service territory. After deployment, KCP&L's IT department integrated daily CellNet reads with the CIS + billing system. Account activity that is consistent with either unauthorized or inadvertent usage such as vacant accounts with usage, reconnect self accounts and minimum bill accounts are identified and reported by the system.

Last summer a list of vacant premises reporting usage was generated and dispatched to the field. "Customer S's" residence was probably on that list. The meters were disconnected on June 26th, 2003.

On June 30th, "Customer S" sent KCP&L a lease with a July 1st move in date. August 9th, the newly installed meter at that residence went "stale", meaning it stopped transmitting AMR reads. On September 15th, Customer S was cut-off for non-payment. However, the meter we locked and booted was not the meter KCP&L installed on July 1st, but an "alien" meter that previously had been stolen. On September 18th, the "alien" meter was again registering usage. Because KCP&L receives daily reads the situa-

tion was quickly identified.

Back at KCP&L a Senior Billing Clerk and a Revenue Protection Representative started putting pieces of the puzzle in place. They documented proof from the CellNet readings that "Customer S" had been using the meter of record Mondays through Fridays and the "alien" meter throughout the weekends. KCP&L's Revenue Protection Representative investigated, took photos and removed the "alien" meter. The customer's account was



Karen Sweat

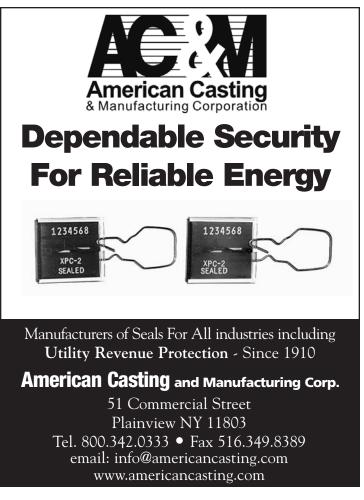
flagged in CIS+ with an alert that referred him to the Revenue Protection department.

When "Customer S" called he did not deny the meter switching. He was advised he owed \$645 in fees and charges and to turn over the meter of record. "Customer S" complied and his service was re-established on October 4th, 2003.

Billing Services calculated "Customer S" was responsible for an additional \$78.56 of usage from the "alien" meter. That amount was back-billed. All totaled "Customer S" paid an extra \$645 for his efforts.

KCP&L's experience shows AMR coupled with analysis tools and resources works in the ongoing Revenue Protection battle. Call "Customer S" caught!







Internal Security – Is Your Barrel Lock & Key System Compromised?

MARK GRAVELINE - GENERAL SALES MANAGER, INNER-TITE CORP.

well managed barrel lock and key system is vital to utility companies financial success. A proper locking system for meters, cabinets and other hardware, as well as enforcement and support through strict control over the distribution of the keys has proven to be of utmost importance as the competitive utility environment evolves. As utility companies grow and merge, it is imperative that the integrity of internal security systems be sustained and security assured through these transitions. For many years, utility companies have relied upon a barrel lock and key as the foundation for locking their field devices. This unique system, exclusive to utility companies, restricts unauthorized access to their meters, cabinets and appurtenances.

Security Concerns

But what about internal security within the utility company? Is the lock and key system truly secure? Concern is growing among many utility companies in regards to the integrity of these internal security systems. Many believe that their once secure barrel lock and key system, has been jeopardized. Personnel turnover rates, lost keys, stolen keys and a number of other outside effects have raised questions as to whether the barrel lock and key system has been compromised. Internal security audits have shown that an increasing number of barrel lock keys have gone unaccounted. Barrel lock keys can be broken, barrel lock keys can be lost, and barrel lock keys can be stolen. Control of these security systems can go astray by any one of these scenarios. With the rising costs of services, now is the time to regain control. More than ever, revenues must be protected. For utility companies, this means safeguarding the meter; the "cash register."

A barrel lock and key system is at the forefront of a utility compa-

ny's security system. The meters, current transformers, and enclosures must be properly locked to prevent unauthorized access and tampering. Barrel locks are used widespread to prevent would-be thieves from gaining illegal access. But how are these systems kept secure? As with all security systems, access must be given to those who need to help maintain it. With utility companies, this can include a large number of individuals. Meter read-



Mark Graveline

ers, independent contractors, supervisors and revenue protection officials can all have keys to these systems. In a large utility this can easily number in the hundreds. While utility personnel recognize the need to protect the security systems, they also acknowledge that maintaining a 100% secure system is a challenge. Many incorporate internal policies that assist in system maintenance. This can include proper documentation of key dispersal, records of key repairs, maintaining a key serial number database. Keeping track of these is paramount; and with proper documentation and enforcement, a system can be kept reliable. Without proper record keeping upon start-up, the integrity of any barrel lock and key system must be held in question.

Recent accounts suggest that increasing numbers of utility companies have serious concerns regarding the integrity of their current barrel lock and key system. In some cases lost, stolen, and missing keys have reached intolerable levels. One utility reported that they can only account for 10% of the keys purchased over a ten year period. Many now acknowledge that their current system is compromised to the

HIGHFIELD

Customer Needs = New Product Solutions = Higher Utility Revenues
Visit us on the Web at www.highfield-mfg.com



MULTI-BAR FOR GANGED SOCKETS BOTTOM MOUNT SPEEDY LOCK FR

FRONT ENTRY ECON-O-RING®

For information on these and other quality Highfield Security Products, call or fax our Sales Department

Our sales engineers are available to discuss security solutions for all requirements

The Highfield Mfg. Co.

SERVING THE UTILITY INDUSTRY FOR 70 YEARS
380 Mountain Grove Street
Bridgeport, CT 06605

Phone: 203-384-2281 Fax: 203-368-3906

point where drastic measures must be considered. It is at this point where proper assessment and decision-making are needed to reverse the situation.

System Upgrades

A quality barrel lock and key system can often offer what is known as an upgrade. These upgrades allow the utility to incorporate a new barrel lock into their current system without having to fully replace the system. The upgraded barrel lock can be used where instances of illegal access have occurred. The upgraded key will open both barrel lock types; but the old key will not open the new barrel lock. Incorporating an upgraded barrel lock and key into the current system allows the utility company to take some initial steps to increase security throughout the system. The utility now has a new lock that it can introduce into the system to secure areas where security has been breached without a complete system replacement. While an upgraded key system allows for a new system to be introduced, concerns still weigh regarding the original barrel locks in the field. By upgrading the barrel locks in trouble areas, initial problems can be addressed. But without replacing every barrel lock, overall security remains in question.

Exclusivity

Interest is growing among utility companies to increase security measures by acquiring barrel lock and key systems that are exclusive. Instances often exist where neighboring utility companies may very likely use the same barrel lock and key. This raises further concerns. Lost and stolen keys now can pose a threat to the security of neighboring utility companies' locking system. Upgrading the current system will help address some concerns but an upgraded lock and key system does not provide exclusivity. Certain systems are available in which there are geographical limitations. This means no other utility can purchase the same system within a certain region, thereby helping the utility retain a certain level of exclusivity within the region. The Next Level

Trends within the industry indicate that more and more utility com-

panies are looking for their "own" system. One that is exclusive and unique only to them. While plunger style barrel locks can offer security and variety of different lock mechanisms, design impediments exist which limit the number of possible configurations.

A barrel lock possessing its own unique combination has become an attractive solution. Given the limitations that the traditional plunger-style barrel locks pose, newer systems based upon rotating disks have evolved to a point where a quality system can solve these new demands. Known as "disk-style" barrel locks, these advanced barrel locks use internal rotating disks to establish a combination. The inner components of disk style barrel locks allow for much wider variety of configurations thereby allowing for thousands of unique combinations. The results allow utility companies to purchase and retain a much higher security barrel lock and key system that is truly exclusive. The inherent design of a disk style barrel lock also support building master key systems providing greater control options.

Conclusion

With the vast amount of changes happening within the utility industry, it is crucial, now more than ever, for utility companies to maintain control over internal security systems. Higher security barrel lock and key systems represent the latest advancements in the industry and can offer a utility company greater security and many more options than the traditional barrel locks and keys. Successful implementation of such a system can solve many of the security issues brought into question. By offering utility companies exclusive combinations, disk style barrel lock and key systems represent the next level in security. Proper procedures along with a tightly controlled barrel lock and key system will prove to be a valuable asset in the changing marketplace. A properly implemented and supervised barrel lock and key system furnishes the utility company with the inner foundations for the security they will need to succeed in this every changing industry.

Which of these four products solve a common problem?



Our complete line of solid brass tumbler-pin padlocks can be keyed alike, different, master, grand master or to most popular lock brands, and feature a unique bore hole to apply an indicative seal for extra security.



New Dual Channel™
Padlock Seal presents
clear evidence of
tampering. Stainless steel
hasp is configured to pass
through apertures with
a minimum 1/8-inch
diameter.



New Snap Ring[™] high security stainless steel locking device, with its one-piece, front-entry design, is an economical way to secure ring-style residential and gang meter sockets.



New Quik Lock™ high-security locking device in high-density plastic or steel for ringless-style meter sockets is fast and easy to apply, with no holes to punch or tools required.



2004 E.J.Brooks Company

UTILITY PRODUCTS GROUP

BROOKS SECURITY PRODUCTS

BROOKS EKSTROM BROOKS METER DEVICES

We Have Answers.™

8 Microlab Road, Livingston, NJ 07039 800.458.7325 Tel: 973.597.2900 Fax: 973.597.2919 brooksutility.com sales@ejbrooks.com

We Have Answeis.

Answer: All of the above, because at Brooks Utility Products Group, that's what we do.

IURPA

REVENUE ASSURANCE WITH AMR THE GOOD, THE BAD, AND THE POSSIBILITIES

By Ed Malemezian



Ed Malemezian

he pending installation of Automated Meter Reading (AMR) is often looked at as a mixed blessing by those touched by the project. Since many different groups will be affected by AMR, whether they realize it or not, the pending project frequently leads to much anxiety and ambivalent feelings about the changes brewing in the wind. Revenue Assurance professionals are often smack dab in the middle of this turmoil, and tend to get very concerned about what it really

means to them, especially as it relates to their ability to continue bringing value to the organization. This article will attempt to clear the air by describing The Good, The Bad, and The Possibilities of an AMR deployment as it applies to revenue assurance.

THEFT IS A COSTLY PROBLEM

The fact that you are reading IURPA News in the first place, means that I don't need to convince you that energy theft can be a problem just about everywhere. Studies by the Electric Power Research Institute (EPRI), the Edison Electric Institute (EEI), and many utilities report energy theft in terms of: 1% lost revenue annually, average losses at \$5 to \$20 million for a medium sized utility, total industry losses between \$1 and \$2 billion annually, 1% of customers with confirmed cases, and recovery of 0.5% to 1.0% in revenue. All of these reaffirm that theft is a big ticket item and a subject worthy of attention.

REASONS TO DO AMR

Tamper detection usually rates very high in business cases used to justify AMR. Chartwell's 2002 Report on AMR states: 20% of utilities use or plan to use AMR for tamper detection, 35% of utilities are considering using AMR for tamper detection, and tamper detection is the most popular benefit of AMR. Usually, the reduction in meter reading costs is the biggest single dollar saving benefit in an AMR business case. Dollars get saved by eliminating monthly meter reading visits to each customer, thereby presenting us with a dilemma: meter reading costs go down, but on the flip side, the monthly meter reading eyes looking for tampering also go away. AMR hardware and associated systems need to be clever enough to replace these lost "eyes."

TYPES OF TAMPERING

Tampering can be split up into three very broad categories:

- Internal to the meter
 - o Adjustment screws One Time (OT)
 - o Register tampering OT
 - o Magnetic circuit alteration OT
 - o Electrical alteration OT
 - o Dial tampering Recurring (RC)
 - o Program alteration OT
- External to the meter
 - o Magnets RC
 - o Hole in cover / disk pinning RC
 - o Upside-down meter RC
 - o Stolen meter OT or RC
- Installation tampering
 - o Line-side taps
 - Weather-head OT
 - Service entrance conductors OT

- Underground OT
- Switchgear / buswork / troughs OT
- o Bypass
 - Jumpers in meter socket OT
 - Close bypass device OT
- o Instrument transformer installations
 - Re-wiring OT
 - Shorting of current transformers OT

AMR TAMPER DETECTION

AMR tamper detection does a very effective job in identifying some of the types of tampering noted above, a mediocre job with other types, and a poor job with yet other types. In all cases, dedicated tamper detection sub-systems or external systems to "filter" accounts, coupled with external data and customer profiles, improve the effectiveness of detection tremendously. More on that later ...

REVERSE ENERGY flags do a great job in detecting meters that have been turned upside down. In addition to the flag, some meters capture the reverse energy in a separate register. Other meters simply add reverse energy to forward energy, thereby accumulating the total consumed. With this approach, however, the total energy register in the AMR module no longer matches the meter dials.

TILT SWITCHES are used to detect when the meter is tilted some amount, typically 50° to 70° from its normal position. Early tilt switches contained mercury. The switches used today are mercury-free. Tilt switches, taken alone, have a notorious reputation for providing false indications due to vibrations and shaking of the meter.

METER REMOVAL can be reliably inferred when the tilt switch is actuated at the same time a power outage is detected. Meter removal, however, does not directly translate to tampering. In order to be effective, one needs to "back out" legitimate reasons for meter removal: regular meter work, emergency work (trouble calls), disconnects (move outs), and acceptable customer work by an electrician or homeowner. All of this screams out for an automated "system" solution, with ties to work management and trouble call systems. Without such an automated approach, the volume of false alarms can be quite overwhelming. Even with a decent automated system, meter removal detection alone to detect any of the One Time types of tampering is hit or miss at best.

METER INVERSION can be reliably inferred when meter removal has been detected, the tilt switch stays closed, and power is restored. In addition, one would expect to set a reverse energy flag too. All these, taken together provide a very reliable indication that the meter is running upside down.

POWER OUTAGE COUNTERS can increment every time a power interruption is detected. Some AMR modules utilize industry standard definitions (IEEE / ITIC / CBEMA) in determining if the interruption is counted or not. Some modules don't use recognized standards, instead using their own "easy to implement" definition. Just be careful ... As was the case with meter removal, power outage counters require a system solution to be effective in order to "back out" normal power outages, storms, regular meter work, trouble work, etc. Ties to work management and outage management systems are a must. In addition, the smarter system solutions would include comparison of the outage count against those



experienced by neighbors, i.e. other customers on the same transformer.

MAGNETIC SENSORS have been provided in some AMR modules to detect the presence of large magnets customers have been known to use to slow down the meter disk. In general, magnetic sensors have created too many false alarms to be very effective.

METER AND SITE DIAGNOSTICS, as provided in solid state meters are both very effective in detecting problems internal to the meter, both malfunctions and tampering, and site problems such as meter wiring, instrument transformer, voltage and current balance problems.

RFID AND OTHER high tech approaches are beginning to appear that better tackle the installation integrity issue. RFID is a Radio Frequency Identification chip that is imbedded in a seal placed across the meter enclosure and meter, that communicates via RF with the AMR module. RFID is not commercially available for AMR today, but folks are working on it, as is seems to offer considerable promise for some situations.

SYSTEMS FOR FILTERING

To be truly effective, "hardware" based tamper detectors incorporated in AMR modules need to be evaluated against other information to be filtered properly. Power outage counts and outage flags must be compared against neighboring meters. Normal meter and trouble work, legitimate customer work, and related activities need to be backed out of the pile of suspected tampers. Without such filtering, hit rates in finding the true tampers in the big pile are often too low to make it worthwhile to roll an investigator to the site. To be practical, filtering and cross-checking need to take place in the background, completely automated without much, if any, operator intervention. The big problem is, that, today's AMR systems tend to lack much capability in this area. This leaves utilities with only a partial solution, unless they develop their own "custom" systems to do the filtering. AMR providers with systems to do this effectively will be the big winners. Vendors, are you listening ???

TRENDS, COMPARISONS AND PROFILES

Taking tamper detection and revenue assurance to the next level involves bringing in even more data for a proactive approach to spotting problems. AMR deployments typically can be configured to retrieve tremendous amounts of consumption data. Once you get past the paradigm of a once a month reading, you can get really creative in how to use more frequent data. A number of AMR systems provide daily or hourly usage data on some or all customers. With some clever thinking, this capability can be used to spot trends and abnormalities that are indicative of tampering, malfunctioning equipment, or usage when there shouldn't be any. To be most effective, customer's actual usage patterns should be compared against typical usage patterns for similar customers. This can be accomplished by having a library of usage profiles for the most common customer categories. These would be developed for each rate class, stratified by usage, broken out by type of premise (city residence, beach house, mountain condo, farm outbuilding, etc.) Profiles for the whole year and normalized by the actual weather, would provide the means to readily spot abnormal conditions. Again, the big problem is, that, today's AMR systems lack capability in this area. AMR providers with systems to do these comparisons effectively will be the big winners. Vendors, are you listening ???

VENDOR CAPABILITIES

Not all vendors are created equal. A utility needs to thoroughly investigate what they are getting with regard to tamper detection.

The following table demonstrates how these capabilities differ by vendor, and even by different models from the same vendor.

Vendor	Electro-Mechanical or Solid State Meter	Rev Energy Flag	Rev Energy Register	Meter Tilt Flag	Meter Inversion Flag	Pwr Outage Counter	Magnet Sensor	Meter & Site Diag	Other RFID	System - Trends
Α	EM	Х	fwd	Х	Х					
Α	SS	Х	fwd	Х	Х			Х	future	
В	EM	Х	fwd	old		Х	Х			
В	SS	Х	fwd	old		Х	Х	Х		
С	EM	Х	Х			Х				Х
С	SS	Х	Х			Х		Х		Х
D	SS	Х	Х					Х		
E	EM	Х	Х			Х				
Е	SS	Х	Х			Х		Х		
F	EM		fwd			Х				
F	SS		fwd			Х		Х		

REVENUE ASSURANCE

Revenue assurance is much more than just tamper detection. Revenue assurance is the effort to make sure that all the revenue owed the utility is collected by the utility. It includes: theft detection and follow up, metering mistakes, meter malfunctions, meter constant errors, billing errors, consumption on inactive accounts, and collection problems. AMR provides a wonderful tool to help utilities reduce lost revenues in each one of theses areas, but AMR is only a tool. AMR requires good people, knowledge, and systems to be effective.

HOW DID WE DO ???

AMR does a good job in helping with: Recurring tampers of upside-down meters and dial tampering, site and installation diagnostic problems, consumption on inactive accounts, and in providing detailed data for trends and comparisons. Plus, an AMR deployment provides the opportunity for a 100% clean sweep as each and every meter installation is visited.

AMR, by itself, provides little or no help with the One-Time tampers (adjustments, register tampering, magnetic circuit alteration, and electrical circuit alteration), tampering external to the meter (magnets, disk pinning, and stolen meters), and in finding taps and jumpers. However, detection of all of these conditions is enabled by AMR feeding data into the appropriate filtering or comparison system.

CONCLUSIONS

AMR provides great information for finding certain kinds of losses. AMR provides little help with others. To be truly effective, systems to filter, trend, and compare are required. Utilities need active Revenue Assurance programs and systems, staffed by knowledgeable people, even after AMR. The revenue assurance workload will not necessarily go down, it will simply shift to new areas, and recovery and "assurance" will both improve. Utilities must go into AMR with their eyes wide open. Consider all The Good, The Bad, and The Possibilities.

Ed Malemezian is the president and principal of **Ed Malemezian Consulting, Inc.**, where he serves the needs of clients requiring an in-depth understanding of the metering industry. In 2000, Ed retired after 30 years at Florida Power & Light (FPL). His 25 + years of metering experience cover all facets of the discipline from competitive services, to field metering, to meter shop, to meter engineering, and more.

IURPA

STOP - LOOK - LISTEN

BY JIM PETERSON, WSUTA - 1ST VICE PRESIDENT

Power theft does take on many faces. It can come from just a very simple customer self reconnect or be a very elaborate and very dangerous life threatening situation. With these safety issues, you want to wear all of you personal protective gear at all times while doing your investigation. Many of the more dangerous cases involve marijuana growers where electrical codes don't exist. Thieves don't care how dangerous a situation they leave for themselves or anyone else, including their own families. Also economic backgrounds have no boundaries either. You may find power theft or a grow operation in the more neglected part of your town or in the upper class neighborhoods. As utility workers we need to always be on the lookout for these dangerous situations.

You wouldn't run into a burning building without first "stopping" to see if you can safely enter. You do that by first looking and listening to what is going on around you. With that in mind, every utility job you go up to, you should be looking for what is out of the ordinary. "Stop" and "look" at everything before you touch anything and "Listen" to you customer if they are around because, if they have in fact tampered with anything, they are probably going to be very nervous and try to cover their tracks and play as dumb as possible.

You will want to look at all of the weather head connections for new tape or bare spots where connections may have been made or look for extra wires. Check all seals to see if they have been tampered with. Remember, your thief is going to try to make everything look as normal as they possibly can. Look at all screws on the outside of the meter base to see if they are in place and not tampered with. Many meter bases have external screws that hold the face of the meter base in place. If these screws are missing the meter can be pulled without disturbing the meter seals. Sometimes these screws are missing, so that when you pull the meter, the face of the meter base falls down against the energized jaws of the meter base and or meter resulting in an explosion. Also, look for holes drilled in the meter that would allow stoppage of the meter disk. These



lim Peterson

could be anywhere on the meter cover. Look for fresh dug dirt around the meter base where underground taps could have been made. If necessary or in doubt, use your "Tap Locator" to check for underground taps or in the wall taps. Remember, these conditions are not inspected, so anything is possible, and it will your pain and suffering if you are not paying attention and get injured.

Listen carefully to your customer. Many times a customer will tell on themselves. They will try to convince you how little they know about electricity. When this happens, the red light should come on to really look for something wrong and to be careful. Often neighbors will be willing to volunteer information. Also, sometimes even the customers own children or spouse may give you clues. Kids love to tell all they know, so all you need to do is ask questions that my lead to answers you are looking for. Remember, you are only looking and listening for clues and gathering evidence, so don't start accusing the customer of anything. This will put the customer on the defense and will usually result in a confrontation and or further cover up of what they don't want you to know or find. Also, remember you are not on a search warrant. You only have a legal right to investigate the utilities facilities.



T&D CREWS HELP PROTECT SCE REVENUE

BY JUDY ASMAN

That does \$17,765.71 mean to SCE? That's how much it cost the company to provide about a year's worth of 24-hour lighting to a Rialto resident's marijuana patch. And the customer didn't pay a dime.

How did he do it? By illegally tapping into SCE's distribution system.

This incident represents a fraction of what SCE rebills every year to residents who illegally connect to our electrical grid. Thanks to CSBU's Revenue Protection department, SCE is able to find



these residents and collect the millions of dollars every year it costs SCE to provide this power.

"In 2003 alone, we rebilled about \$2,900,000 to residents who illegally set up bypasses to our system," says Revenue Protection Investigator Supervisor John Giles. "We collected \$2,139,000, a total that includes rebills from previous years."

Some residents go for years using unauthorized bypasses before SCE and law enforcement officials catch up with them. One of SCE's biggest cases reached its breaking point in January.

In 1996, after a Foothill resident was delinquent on his electricity bill, SCE cut his power. But that didn't stop him from turning on his lights.

"We'd never seen anything like it," says Revenue Protection Investigator Terry Terkelsen. "We went through a series of investigations on this resident. And after each one, he still hadn't let up."

The first investigation was in 1998.

Terkelsen checked up on him periodically because he knew the resident's account had been idle since 1996. Terkelsen noticed the resident's Malibu lights were on. He approached the resident and asked if he could check his meter. The resident went into his house to "put the dogs away," the Malibu lights went off and Terkelsen didn't see the customer again.

The following investigation happened in 1999. Terkelsen discovered the same resident had full power using a 240-volt extension cord, which was buried four inches underground and plugged into an outlet in the neighbor's back porch. Terk-elsen again approached the resident and had him remove it.

The final investigation started in April 2003, when Revenue Protection received an external tip that this same resident was using "free" power. Two weeks later, Terkelsen was reassigned to

the case.



It came to a head in January, when the Rialto Police Department granted Terkelsen and Giles a search warrant to investigate the same home—with the help of T&D.

"John (Giles) and I went out there on Jan. 29 with the Rialto Police Department. We determined the customer was again engaging in unauthorized use of power but could not immediately determine the source of it," recounts Terkelsen. "That's when we dispatched Troublemen Greg Davis and Frank Felix."

Davis, Felix and two contractor crews eventually located the source of the Foothill resident's electrical connection. But it was no easy task.



Judy Asman

When Davis and Felix appeared on the scene, they examined the resident's backyard until they discovered wires coming out of one of the breakers, going through a pipe on the wall and plugged into a generator. But the generator wasn't on.

The troublemen lifted covers to see where the wires were going and saw they went right through the bottom of the generator and into the ground.

At this point, they called the Distribution Operations Center (DOC), who dispatched Underground (Upgraded) Foreman Ralph Mesa. Mesa called out two contractors, Weissker Inc. and UTI, who are equipped to detect underground electricity connections.

UTI found the underground conductors right away and used spray paint to mark the trail of the wires. Then the group started digging.

After locating the wires, they found two 10-gauge wires connected to each one of SCE's secondary conductors. These were buried about five feet underground. The wires were connected to

3 ways to stop electricity theft in a few seconds:

RF Interrogated Check Meters

Universal Meter 2W, 3W, 4W Y & \triangle , 120 - 480V. 0-6000 amps 50 or 60 Hz, read range to 500 ft.

Tap Detectors

Identify presence and location of Tap from 0 to 200 ft. in less than 10 seconds. Windows®-compatible software in Spanish, Portuguese, English & French, Metric & English.

Active Tamper Alarms Computer Surveillance Systems

Record meter reading in 5, 15, 30, 60-minute or daily intervals. Stores up to 3000 readings and 50 alarms. Data can be downloaded via modem or direct connect.

...and many more.

Universal Protection Corp.

6767 Peachtree Ind. Blvd., Suite L, Norcross, GA 30092 USA 800-635-5042 fax 770-453-9798 • upcx.com

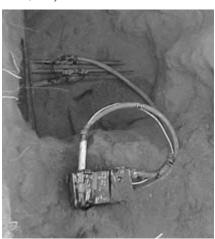
a homemade junction box, wrapped in plastic and stuffed in a large bucket.

Mesa removed the bypass and repaired the secondary conductor. Revenue Protection has since rebilled this customer for more than \$12,000. And this doesn't include the associated costs of about \$2,000 to conduct the investigation.

Revenue Protection relies on internal and external sources to find customers who are engaging in unauthorized use of electricity. All tips are anonymous.

"A majority of our tips come from our employees," explains Giles. "If an employee suspects energy theft, they can complete a tip card or call our toll free hotline. Then we'll start investigating."

If the Revenue Protection investigators determine there is a need, they'll ask the troublemen to install surveillance meters



Make checks payable to IURPA and mail to:

near the suspects' homes. These meters register the amount of electricity the residents use versus what is being billed.

If you suspect anyone of energy theft, contact the tip hotline at 800-227-3901.

H.J. Arnett Industries, LLC

Home of the White Knight Tap Locator with on unit graphical displays!





Featuring the new <u>Fiber Optic Scope</u> with a length up to 96" for near meter viewing in conduit!

Single and Poly Phase <u>Flagship</u> Check Meters Beats ANSI C.12.1 accuracy standard!





Arnett Consulting

The leader in Revenue Protection

7500 SW Tech Center Drive, Suite 130, Portland, Oregon 97223 Phone 503-684-9844 Fax 503-684-8360 www.arnettindustries.com

IURPA - 2004 ANNUAL MEMBERSHIP Name: Company: Mailing Address: _____State: _____Country: _____Zip: _____ City _____E-Mail: _____ Telephone: Electric Water Cable Other Utility Type: Payment Method: Check Enclosed Credit Card **Credit Card Payments Information:** Name as it appears on the card: Billing Address: _____Zip Code: ______ City: __VISA __MC ___ __/___/ Expires:____/ Note: Credit card payments may be made directly from the IURPA website. Please go to: www.IRUPA.org

George A. BalsamoThe United Illuminating Co.

157 Church Street, P.O. Box 1564, New Haven, CT 06506-0901 USA

Annual dues are \$50 (US) per member. Payments may be made by check or credit card. Please send form along with your payment.

INNOVATIONS

Make Us First





















INNER-TITE

Serving Utilities Since 1932

PH: 508-829-6361 ● FX 508-829-4469 www.inner-tite.com security@inner-tite.com



IURPA • 14 Years

IURPA Directors

Michael Szilvagyi

Detroit Edison

Jersey Central

Nevada Power

George Balsamo

Clifford Green

Ed Holmes

(Retired)

Southern California Gas Co.

Director of Web Services

United Illuminating Company

Director of Business Planning

Highfield Manufacturing

Richard Woodward

Director of Finances

Cleve Freeman

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 fourteen 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



Chairperson -Kurt Roussell Wisconsin Electric Power Co. Milwaukee, WI 53203 Phone: (414) 221-3634 (414) 221-2214 Fax: kurt.roussell@we-energies.com

1st Vice-Chairperson -

Southern California Edison

909-925-8325

Kent Manning

Fax:

Menifee, CA 92585

Manninkj@sce.com

Phone: 909-928-8225



Secretary -Jeff Cornelius Peace River Electric Co-op Wauchula, FL 33873 Phone: (941) 722-2729 (941) 722-5837 Fax: corneliusj@warner.edu



Treasurer **Raymond Croft** Pacificorp Portland, OR 97232 Phone: 503-813-6601 503-813-6200 Fax: Ray.Croft@Pacificorp.com

International Liaisons

David Bown - United Kingdom Seimans Energy Service Ltd. Bedford, England Luiz Fernando Arruda CEMIG, Brazil **Deon Louw** Capetown, South Africa

Vendor Representative Joseph Werner

Sterling Security Systems **Newsletter Committee Wayne Dickinson** LADWP

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: ernie@brodyprinting.com

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.



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