

ORIGINAL

Antonio Gill

From: Patricia
Sent: Tuesday
To: Mayo
Cc: Pierce
Subject: Fwd: I

Generic Smart Meter
Investigation
E-00000C-11-0328



00000139577

DOCKETED

ump-Web

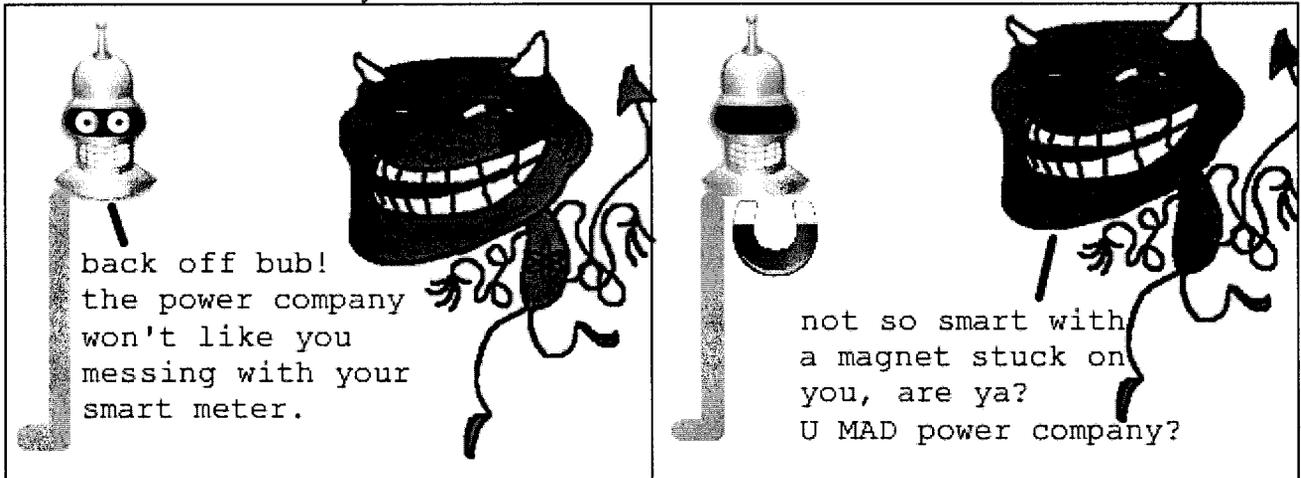
2012 SEP 18 10:41:20

Dear Mayor Evans,



With the FBI as witness for the magnetic simplicity depicted in the cartoon below, one wonders at the design flaws possible to sophisticated hackers interested in multiple sources of income from a secondary market arising from what APS now calls: *smart meters/automated meters*. Selling private information and sabotage are issues that are most often mentioned. Some wonder if the entire grid can be hacked.

smart meters: how do they work?



MONDAY, APRIL 9, 2012

http://www.secmeme.com/2012_04_01_archive.html

Quote from the forwarded article below relates to the magnet cartoon:

The bureau also said another method of attacking the meters involves **placing a strong magnet on the devices, which causes it to stop measuring usage, while still providing electricity to the customer.**

“This method is being used by some customers to disable the meter at night when air-conditioning units are operational. The magnets are removed during working hours when the customer is not home, and the meter might be inspected by a technician from the power company.”

“Each method causes the smart meter to report less than the actual amount of electricity used. The altered meter typically reduces a customer’s bill by 50 percent to 75 percent. Because the meter continues to report electricity usage, it appears be operating normally. Since the meter is read remotely, detection of the fraud is very difficult. A spot check of meters conducted by the utility found that approximately 10 percent of meters had been altered.”

Quoting Robert Former, in blue, from the same forwarded article, “What you’re hearing is the sound of [a] paradigm shifting without a clutch”.

Customers like ourselves and the Town of Payson, "have to be more enterprise security-aware. With these incidents at organizations of any size or age, the first reaction is to cover it up. The thinking is if we keep

this kind of thing secret, nobody will find it or exploit it. But for those of us who are inside the industry, and have been at this long enough, the only way we're going to fix a security problem is to expose it."

If the APS name change from *smart meters* to *automated meters* is any indication, it looks like APS is in a secretive/spin/cover up stage.

For security and safety reasons, I urge you to protect the Town of Payson and notify APS that the Town of Payson chooses to keep its analog/mechanical meters. As former CIA Director James Woolsey says in this video interview, **CIA Director calls Smart Grid "Stupid" due to Security problems**, "a so called Smart Grid that is as vulnerable as we've got, is not smart at all, it is a really really stupid grid." www.youtube.com/watch?v=MAid1bS8t9U

Please notify me about our progress maintaining The Town of Payson's safe analog meters.

Sincerely,
Patricia Ferre

Begin forwarded message:

From: Warren Woodward <w6345789@yahoo.com>
Subject: Fw: FBI: Smart Meter Hacks Likely to Spread
Date: September 2, 2012 1:04:11 PM MST
To: Pat Ferre <pferreact@mac.com>

Thanks for your email. FYI:

--- On Thu, 4/12/12, Warren Woodward <w6345789@yahoo.com> wrote:

From: Warren Woodward <w6345789@yahoo.com>
Subject: FBI: Smart Meter Hacks Likely to Spread
To: pierce-web@azcc.gov, newman-web@azcc.gov, burns-web@azcc.gov, stump-web@azcc.gov, kennedy-web@azcc.gov
Cc: paboud@azleg.gov, sallen@azleg.gov, fantenori@azleg.gov, nbarto@azleg.gov, abiggs@azleg.gov, jburgess@azleg.gov, ocajerobedford@azleg.gov, rcrandall@azleg.gov, adriggs@azleg.gov, sgallardo@azleg.gov, rgould@azleg.gov, lgray@azleg.gov, ggriffin@azleg.gov, jjackson@azleg.gov, lklein@azleg.gov, llandrum@azleg.gov, llopez@azleg.gov, jmccomish@azleg.gov, amelvin@azleg.gov, rmeza@azleg.gov, rmurphy@azleg.gov, jnelson@azleg.gov, jlewis@azleg.gov, spierce@azleg.gov, mreagan@azleg.gov, dschapira@azleg.gov, dshooter@azleg.gov, dluan@azleg.gov, stevesmith@azleg.gov, syarbrough@azleg.gov, eables@azleg.gov, lalston@azleg.gov, barredondo@azleg.gov, cash@azleg.gov, bbarton@azleg.gov, kbrophymcgee@azleg.gov, chcampbell@azleg.gov, hcarter@azleg.gov, tchabin@azleg.gov, scourt@azleg.gov, ccrandell@azleg.gov, jdial@azleg.gov, kfann@azleg.gov, sfarley@azleg.gov, efarnsworth@azleg.gov, jfillmore@azleg.gov, tforese@azleg.gov, rgallego@azleg.gov, sgonzales@azleg.gov, dgoodale@azleg.gov, dgowan@azleg.gov, rgray@azleg.gov, ahale@azleg.gov, jharper@azleg.gov, mhein@azleg.gov, khobbs@azleg.gov, rjones@azleg.gov, pjud@azleg.gov, jkavanagh@azleg.gov, dlesko@azleg.gov, ddavis@azleg.gov, nmclain@azleg.gov, jmesnard@azleg.gov, emeyer@azleg.gov, cmiranda@azleg.gov, rmiranda@azleg.gov, smontenegro@azleg.gov, jolson@azleg.gov, lpncrazi@azleg.gov, dpatterson@azleg.gov, jpierce@azleg.gov, fpratt@azleg.gov, tproud@azleg.gov, areeve@azleg.gov, brobson@azleg.gov, msaldate@azleg.gov, cseel@azleg.gov, dsmith@azleg.gov, dstevens@azleg.gov, atobin@azleg.gov, atovar@azleg.gov, mugenti@azleg.gov, surie@azleg.gov, tvogt@azleg.gov, jweiers@azleg.gov, jpweiers@azleg.gov, bwheeler@azleg.gov, vwilliams@azleg.gov,

kjee@azleg.gov, consumerinfo@azag.gov, cfraulob@azruco.gov, jjerich@azruco.gov,
Vicki.Gray@co.yavapai.az.us

Date: Thursday, April 12, 2012, 12:19 PM

Re: AZ Corp. Comm. Docket # E-00000C-11-0328

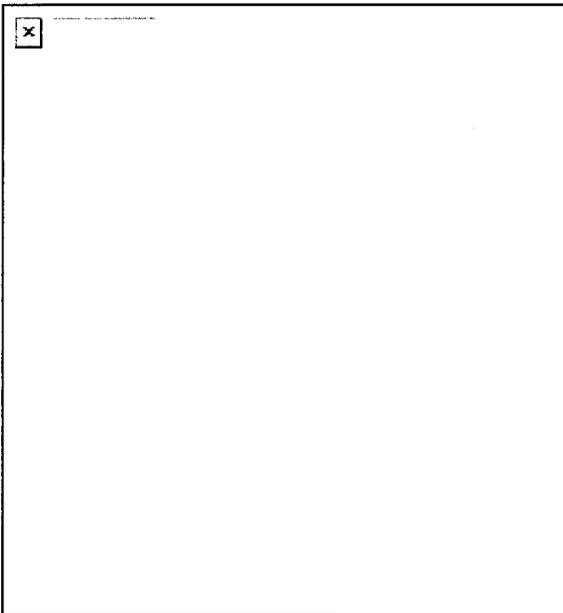
<http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/>



FBI: Smart Meter Hacks Likely to Spread

[564tweetsTOP1Kretweet](#)

A series of hacks perpetrated against so-called “smart meter” installations over the past several years may have cost a single U.S. electric utility hundreds of millions of dollars annually, the **FBI** said in a cyber intelligence bulletin obtained by KrebsOnSecurity. The law enforcement agency said this is the first known report of criminals compromising the hi-tech meters, and that it expects this type of fraud to spread across the country as more utilities deploy smart grid technology.



Part of an FBI alert about smart meter hacks.

Smart meters are intended to improve efficiency, reliability, and allow the electric utility to charge different rates for electricity at different times of day. Smart grid technology also holds the promise of improving a utility’s ability to remotely read meters to determine electric usage.

But it appears that some of these meters are smarter than others in their ability to deter hackers and block unauthorized modifications. The FBI warns that insiders and individuals with only a moderate level of computer knowledge are likely able to compromise meters with low-cost tools and software readily available on the Internet.

Sometime in 2009, an electric utility in Puerto Rico asked the FBI to help it investigate widespread incidents of power thefts that it believed was related to its smart meter deployment. In May 2010, the bureau distributed an intelligence alert about its findings to select industry personnel and law enforcement officials.

Citing confidential sources, the FBI said it believes former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash and training others to do so. “These individuals are charging \$300 to

\$1,000 to reprogram residential meters, and about \$3,000 to reprogram commercial meters," the alert states.

The FBI believes that miscreants hacked into the smart meters using an optical converter device — such as an infrared light — connected to a laptop that allows the smart meter to communicate with the computer. After making that connection, the thieves changed the settings for recording power consumption using software that can be downloaded from the Internet.

"The optical converter used in this scheme can be obtained on the Internet for about \$400," the alert reads. "The optical port on each meter is intended to allow technicians to diagnose problems in the field. This method does not require removal, alteration, or disassembly of the meter, and leaves the meter physically intact."

The bureau also said another method of attacking the meters involves placing a strong magnet on the devices, which causes it to stop measuring usage, while still providing electricity to the customer.

"This method is being used by some customers to disable the meter at night when air-conditioning units are operational. The magnets are removed during working hours when the customer is not home, and the meter might be inspected by a technician from the power company."

"Each method causes the smart meter to report less than the actual amount of electricity used. The altered meter typically reduces a customer's bill by 50 percent to 75 percent. Because the meter continues to report electricity usage, it appears to be operating normally. Since the meter is read remotely, detection of the fraud is very difficult. A spot check of meters conducted by the utility found that approximately 10 percent of meters had been altered."

"The FBI assesses with medium confidence that as Smart Grid use continues to spread throughout the country, this type of fraud will also spread because of the ease of intrusion and the economic benefit to both the hacker and the electric customer," the agency said in its bulletin.

The feds estimate that the Puerto Rican utility's losses from the smart meter fraud could reach \$400 million annually. The FBI didn't say which meter technology or utility was affected, but the only power company in Puerto Rico with anywhere near that volume of business is the publicly-owned Puerto Rican Electric Power Authority (PREPA). The company did not respond to requests for comment on this story.

The hacks described by the FBI do not work remotely, and require miscreants to have physical access to the devices. They succeed because many smart meter devices deployed today do little to obfuscate the credentials needed to change their settings, said according to **Tom Liston** and **Don Weber**, analysts with InGuardians Inc., a security consultancy based in Washington, D.C.

Liston and Weber have developed a prototype of a tool and software program that lets anyone access the memory of a vulnerable smart meter device and intercept the credentials used to administer it. Weber said the toolkit relies in part on a device called an optical probe, which can be made for about \$150 in parts, or purchased off the Internet for roughly \$300.

"This is a well-known and common issue, one that we've warning people about for three years now, where some of these smart meter devices implement unencrypted memory," Weber said. "If you know where and how to look for it, you can gather the security code from the device, because it passes them unencrypted from one component of the device to another."

The two researchers were slated to demo their smart meter hacking tools at the Shmocon security conference earlier this year, but agreed to pull the presentation at the last minute at the request of several vendors and utilities that they declined to name.

"It turns out that the vendor has a consortium of utility customers with whom they have regular conference calls," Weber said. "Several of the utilities in this group had a concern about the information becoming public. Luckily we have worked with several of the utilities in the group. We have been able to stem the fears of all but one utility. We hope to have them on board very soon."

Liston said utilities have become accustomed to deploying meters that can last 30 years before needing to be replaced, but that the advanced interactive components being built into modern smart meters requires a much more thoughtful and careful approach to security.

“Traditionally, metering technology has been very cost effective, because much of it is very resilient. But these older devices didn’t have a lot of technology in them, and they certainly didn’t have wireless connections and things like memory storage,” Liston said. “The utilities are still expecting the lifecycle of newer pieces of equipment to be 20 to 30 years, and they’re just coming to the realization that some of new stuff deployed is not going to last nearly that long.”

Robert Former, a security engineer at smart meter manufacturer Itron, said he hopes that researchers continue to push the industry toward adopting technologies that can withstand these and potentially other, as-yet-undiscovered attacks.

“What you’re hearing is the sound of [a] paradigm shifting without a clutch,” Former said. “Utilities have to be more enterprise security-aware. With these incidents at organizations of any size or age, the first reaction is to cover it up. The thinking is if we keep this kind of thing secret, nobody will find it or exploit it. But for those of us who are inside the industry, and have been at this long enough, the only way we’re going to fix a security problem is to expose it.”

Antonio Gill

From: Nancy Baer <redrockclass@msn.com>
Sent: Thursday, September 06, 2012 12:49 PM
To: Burns-Web; Kennedy-Web; Newman-Web; Pierce-Web; Stump-Web; 'Representative Fann'; 'Representative Pierce'; 'Representative Tobin'; 'Yavapai County Commissioner District 1'; 'Yavapai County Commissioner District 3'; 'Yavapai County District 2 Commissioner'
Cc: 'Tim Ernster'; 'Nicholas Gioello'; 'Barbara Litrell'; 'Dan McIlroy'; 'Jessica Williamson'; John Martinez; Mark DiNunzio; Mike Ward; Rob Adams
Subject: 'SMART' METER FIRES - Two perspectives
Attachments: Texas State Representative David Simpson on Smart Meters.pdf
Importance: High

Please read the attached first so that you understand the issues presented – the contents were protected and could not be copied and pasted into one document :

Curtis Bennett - Expert witness at Texas PUC hearing August 21, 2012 explains smart meter hazards *Chief Science Officer, Interprovincial Journeyman Electrician (Red Seal), Engineering Technologist*

The attached letter was sent to Texas State Representative David Simpson regarding Smart Meter Frequencies being "illegal as applied. Smart Devices can be wired. Wireless are dangerous across the board, especially with utilities not identifying the entire wireless access network(the wireless circuit) including routers, collectors. Collectors covering 125 sq. miles are a killing field and an unintentional frequency weapon against everything in the area covered."

The statement below was copied and pasted in its entirety from the url so noted.

From the IEEE 09/04/12

"We are seeing a spate of report from around the United States—and indeed around the world—of fires believed to have been caused by smart meters that were faulty, incorrectly installed, or connected to circuits where there were unfortunate and unforeseen effects. This appears to be not just a matter of freak incidents that may or may not have taken place here or there. In a compilation made by the EMF Safety Network, which specializes in EMF and RF precaution, there are at least a couple of dozen smart meter fire reports from Australia to Canada and virtually all regions of the United States, and some of those reports concern a couple of dozen fire incidents. In some cases fires appear to have originated in the meters themselves, in other cases in appliances like microwave ovens or refrigerators (as in the photo above), because of power surges.

To be sure, those reports are not necessarily going undisputed by local utilities and energy companies. In one instance, for example, California's PG&E and fire officials have taken issue with an initial report of meter induced fires in Santa Rosa; a short circuit in the distribution system blew out a number of meters, both conventional and two-way, the local fire chief said. On the other hand, just last week Commonwealth Edison of Illinois confirmed three smart meter fires in its operating area, and earlier last month its sibling company Peco Energy suspended smart meter installations in the Mid-Atlantic states after 15 reports of smart meter fires, one in Philadelphia.

Britain's Electrical Safety Council considers meters generally a fire hazard, as cables or fuses deteriorate with time, and it has warned electricity users against storing flammable items like rags or paper near electrical intake equipment.

Obviously all companies with smart meter programs, and all their suppliers and sub-contractors, are going to have to take a close look at the issue of fire hazards. This is just the beginning of a difficult story. Companies installing smart meters already have run into a lot of consumer push-back because of concerns about privacy, security, and--sometimes--higher rather lower electricity costs. The last thing the smart grid needs is meters causing fires.”

<http://spectrum.ieee.org/energywise/energy/the-smarter-grid/smart-meter-fire-reports>

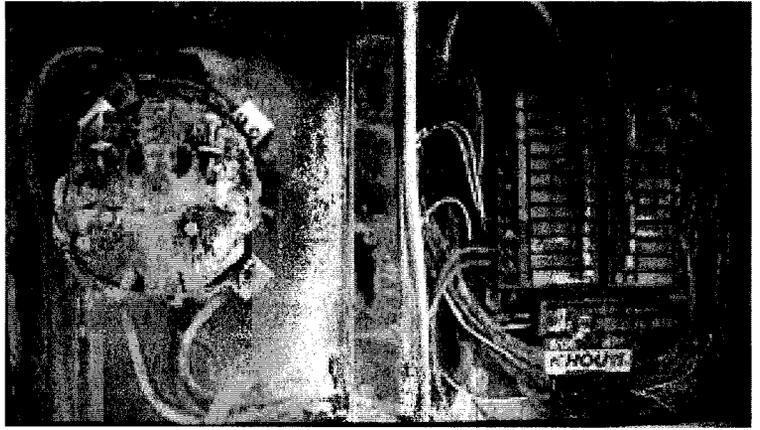
Antonio Gill

From: Monnie Ramsell <monnie@ramsell.net>
Sent: Friday, September 07, 2012 6:04 PM
To: Sedona City Council; Tim Ernster; Nicholas Gioello; Barbara Litrell; Dan McIlroy; Jessica Williamson; John Martinez; Mark DiNunzio; Mike Ward; Rob Adams; Sedona City Council; Burns-Web; Stump-Web; Pierce-Web; Newman-Web; Kennedy-Web; Andy Tobin; Gary Pierce; Cheryl Fraulob; Karen Fann; Andy Tobin; jpierce@azleg.gov
Cc: chip.davis@co.yavapai.az.us; web.bos.district1@co.yavapai.az.us; web.bos.district2@co.yavapai.az.us; web.bos.district3@co.yavapai.az.us; Vicki Gray; Thomas Thurman; Chip Cain; Elizabeth Kelley; Cheryl Fraulob
Subject: Smart meter safety?? AZCC Docket Number: E-00000C-11-0328

Dear Commissioners, Mayor of Sedona, Sedona City Council, Sedona City Manager,

All the utility companies have been assuring us that smart meters are safe and accurate. Looking at those photos, either they are lying or they just have a different idea of what safety is.

I have found a legal document concerning a Qui Tam Complaint filed by an engineer, Don Baker who worked for a smart meter manufacturer, Sensus for over 15 years. He discovered that the meters were **not properly tested** and **seriously flawed**. These meters have a tendency to **overheat and melt or burn**. When he raised the issue to management, he was told to keep quiet. He had direct personal knowledge that the utility company had installed these meters in a



million homes and at least two were burned as a result. He found out meters were not properly tested and over time, that the manufacturer continued to **change and substitute meter components, firmware and manufacturing processes without adequately testing their products.** Once the meters reached the utility company, **1% of the meters were tested - only for their accuracy.** They were **never tested "on the system"** to determine how they would react when actually connected to the power grid on the side of the home. Hundreds of thousands of these meters **had not undergone "performance" testing.** **25,000** installed that year **required replacement** and at a failure rate of **9%** (acceptable failure rate is **.5%**) or **150 meters failed per day.** Both the manufacturer and the utility companies were aware that these installed meters are materially deficient and unsafe and may fail dangerously in a sudden surge of electricity (a relatively common occurrence). Knowing that these meters were flawed, the manufacturer had not performed certain tests including the EFT test (Electrical Fast Transient) as required by ANSI standard. When the utility company demanded to manufacturer to test a sample of these meters, **they all failed.** Later they found **130,000 meters to contain "flux"** or loose solder residue that affected the proper functioning of the meter. After 400,000 meters had been delivered to the utility company, it was determined that the equipment used by the manufacturer to calibrate the meters was itself not properly designed, resulting in meters that produced **incorrect readings.** Don had personally investigated several instances of **over-reporting meters and found individual meters misreporting up to 700%.** They discovered that an electrical resistor was defective on at least **85,000 meters** delivered to the utility company



and at least 170,393 meters delivered to the utility company were discovered to contain faulty Epson "TCXO" components. Sensus also learned that 19,000 installed meters were reporting a "hot socket alarm" - that is, the meters' internal thermometers were registering and reporting temperatures in excess of 200 degree Fahrenheit. Then Don began receiving reports that the meters were **drastically overheating to the point of catastrophic failure, melting and burning**. He personally photographed numerous meters reduced to little more than piles of misshapen, blackened plastic - though another company engineer told him that the meter's plastic cover should not melt at a temperature lower than 500 degree Fahrenheit. Then should we assume that the temperature rose to over 500 degree Fahrenheit? If these meters burned and melted, they might never find out what were the exact causes of fire? Now, why would they build a cover of plastic which we all know will melt when heated? Glass resists flame while plastic burns and melts. The old style meters are solid state with thick glass casing built to last. According to a complaint filed with the Hawaiian PUC, in California alone, there were over 800 documented fires along started by improperly installed smart meters. Arizona is a dry desert and the fire risk is high. The last thing we want is loss of property and life due to something we suspect is unsafe but preventable. What about over-reporting meters? How many rate payers are notified to have their bill adjusted to reflect the over billing error of up to 700%? Why aren't there fines and penalties in place to prevent utility companies from over-charging customers?

This is the legal document I am quoting from. Please spend some time to read it in its entirety. <http://stopsmartmeters.org/wp-content/uploads/2012/01/Alabama-Baker-Sensus-Complaint.pdf>

Faulty meters were installed all over the nation. Arizona is no exception. An unknown number of the smart meters APS installed in the Tri-city area might have a flaw. The manufacturer told the utility that in a test group of 12,000 installed meters, as many as 6 percent of them might have a defect impacting the meter's remote capabilities. A source with knowledge of the problematic



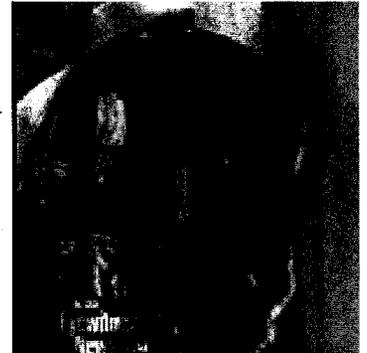
meters who didn't want to be identified claimed more than 4,200 residential and about 351 business meters have the flaw. The manufacturer, Lester Solutions, informed the utility that the flaw is potentially in 3 to 6 percent of the meters in the test group. I am wondering how many percent of the meters were in the test group. In the Sensus case, they tested 1%. Now talking about test group makes me really nervous. Does it mean only meters in the test group were tested, and tested for what exactly? Are the meters installed that were not tested? If so, how many? Are those tests done by outside independent firm or done by in house people? In the Sensus case, they were only tested for accuracy and not safety. Because the tests were done by the same manufacturer themselves, they do not have to disclose any of the test result to anybody. In fact, engineers involved were told to remain silent. If all these meters were UL certified, these kinds of problem would be discovered. If I

were a manufacturer, I would have the meters safety tested by outside independent firm. I just don't understand why it is okay to put a faulty piece of equipment in anybody's house without their consent and without fully testing its safety, reliability and accuracy. Is it "okay" to accept a failure rate? So who are the unfortunate ones whose meters are considered "acceptable" to fail? I guess they can keep doing it as long as rate payers are fully responsible for anything past the meter. And why didn't someone halt the program until they fixed the flaw if they already knew there was known flaw? What about flaws that are not yet known that will only show up in time? If the electronic components are not built to withstand overheating (not to the degree of burning and melting), will overheating affect the accuracy and safety of the meter? If it were automobiles or other consumer items, there would have been recalls. As we can see from the examples cited, not all meters exhibit the same flaws. This makes it even harder for the someone to believe those who

complained about their higher bills, interference with the appliances, damages of appliance due to power surge or meter fire. Didn't we keep hearing from utility companies and PUC that **most** of the meters are just fine? It is exactly with this kind of illogical reassurance that we need tougher regulation and protection from our PUC, city and county. It is NOT okay if a meter is not **independently tested as safe**, especially that was the one installed at you house.

<http://www.dcourier.com/main.asp?TypeID=1&ArticleID=98613&SectionID=1&SubSectionID=1086&Page=2>

In Sensus's case, there is a whistle-blower who had risked his job to tell the public of the truth. If he had not come forward, this information would be buried. We can't expect to find a whistle blower for every company and every utility. Even if such information exists, whoever has the knowledge would be silenced.



Are we asking too much when public safety is concerned that all meters installed should be UL certified? Peco has suspended its smart meter installations after the Bucks Fire. They have already installed 186,000 meters since March. Will they go back and test each and single one installed to insure they are safe? Well, they should. By the way, meters installed by Peco were manufactured by Sensus, but of a later model than the one cited by the lawsuit above. Since the fire, Peco has replaced more than 15,000 of the Sensus meters. The Pennsylvania PUC sent Peco a letter with 17 questions regarding its "advanced metering infrastructure" program, including failure rates of the smart meters, training issues, and Peco's research on manufacturers on August 24. Peco has 10 days to respond.

Read more: <http://www.tmcnet.com/usubmit/2012/08/28/6542154.htm#ixzz25p2NeUbB>

The issues of smart meter fires are not isolated incidents. On April 2, 2012, American Electric Power gave a presentation on "Temperature Monitoring for all AMI meters" at the Spring 2012 EEI Meeting. <http://www.eei.org/meetings/Meeting%20Documents/2012-04-01-TDM-Dimpfl.pdf> The IEEE Spectrum, the world's preeminent standard setting body had an article in their blog on smart meter fire dated September 5. <http://spectrum.ieee.org/energywise/energy/the-smarter-grid/smart-meter-fire-reports>

Even if some of the meters out there seem to be working fine, there is no guarantee that the next batch won't have substituted parts that are flawed. Looking at those photos, can we still trust anybody who insists that smart meters are safe? And yes, some are safer than others. But the biggest question is why utility companies still claim that smart meters are safe? Which **independent** lab or firm tested them and **certified** them safe? If such tests are done, please show us the results and the certificate. If not, wasn't such fraudulent claims unlawful?

Next time you hear from your utility company assuring you that smart meters are safe, just remind them that it really sounded familiar. You have heard that from the tobacco industry before. Radio frequencies penetrate through walls, much worse than second hand smoke. If your neighbor's house is on fire, yours is at risk. Just remind them of the San Bruno fire and the Palo Alto fire. For myself, unless there are **independent safety tests** done by third party, I am not convinced. Unless

installed Smart Meters are UL certified, homeowner's insurance will not even cover any loss or damage from them. Mine won't. Under Federal Regulations as defined by OSHA rule 29 CFT 1910, testing and safety approval is required for certain products, including smart meters. Smart meters have not been tested for OSHA safety. The Department of Energy waived the requirement of UL certification **by request of the manufacturers**, and only required testing for FCC specifications. Every appliance in our home requires UL testing, even Christmas lights have a UL label on them. Smart meters have not been tested and approved under OSHA regulations as required by Federal safety rules. Under this rule, electrical conductors or equipment are required to be tested and or approved for safety. Smart meters are not safety tested by either OSHA nor UL. If you are smart, you wouldn't allow any Smart Meters attached to our home.

Will the City of Sedona and the state of Arizona wise up and put public safety first after learning from all the mistakes from other states? 57 Cities and Counties in California had opposed the deployment of smart meters. The City of Capitola put a halt on the program when they found out that smart meters installed are not UL certified. Only fools rush in when angels fear to tread.

Sincerely,

Monnie Ramsell

Encl: UL testing for smart meters

Smart Meter Performance Testin

Your Global Access Partner for the Meter Market

UL (Underwriters Laboratories) is an independent standard laboratory and certification body with a mission to enhance commerce. Our solid expertise, established objectivity and and that enables us to help you obtain Smart Meter appro

UL certification services for smart meters

UL has more than 10 years' experience in evaluating energy meters, both in providing reliable certification services and in educating manufacturers on safety standards.



UL t
feat
Asia
eval

• A
• A
• I
• B
• U
UL's
• A
• F
A

Summary List of Tests for Electronic Meters (So

Test Item	IEC/AS 62052 Part 11	IEC/AS 6 Part 21
General Mechanical Requirement	•	•
Protection against Penetration of Dust and Water, Terminals - Terminal Block, Resistance to Heat and Fire, Marking of Meter, Spring Hammer Test	•	
Temperature Test: Dry Heat Test, Cold Test, Damp Heat Cyclic Test and Solar Radiation Test, Vibration and Shock Test	•	
Starting Current, Test of No Load Condition, Influence of Ambient Temperature Variation, Voltage Variation, Frequency Variation, Effect of External Power Frequency Magnetic Field, Influence of Short-time Overcurrent, Influence of Self-heating, Accuracy Measurement at Different Loads		•
Auxiliary Voltage Variation		•
Harmonic Component, DC and Even Harmonics, Odd Harmonics in the AC Current Circuit, Sub-harmonics in the AC Current Circuit, Reversed Phase Sequence, Voltage Unbalance, Interpretation of Test Results, Meter Constant, Operation of Accessories		•
Continuous Magnetic Induction of External Origin		•
Immunity to Earth Fault	•	
Power Consumption		•
Fast Transient Burst Test, Immunity to Electromagnetic RF Fields, AC Voltage Test	•	•
Immunity to RF-conducted Disturbances	•	•
Radio Interference Suppression	•	•