Public Inquiry for
Kentucky Public Service Commission
18-00005

Transparency:

- Other utility companies are leasing the unused wireless from RF meters for commercial traffic. Is this true of LGE, and is it required that they are transparent regarding all revenue streams?

Security:

- In October, 2014, Reuters reported that wireless smart meters were easily hacked.
    - How can we be sure our systems are completely secure?
    - If the computer code of the meter is hacked, who is responsible?

- Analog meters are designed to PROTECT the CUSTOMER from error and fraud.

Safety:

- In August 1999, it was reported that RF currents have risk of <u>shock and burn</u>. What is the risk of shock and burn?

- LGE has made three previous failed attempts at wireless meters. Of those failed attempts, how many wireless meters were audited for RF safety from the time they were installed in the field? How many RF meters are regularly tested to ensure they are operating within the legal RF limit? What is the audit record?

- Is LGE completing regular safety audits of the RF transmitters? If LGE is not doing the safety audits, how does LGE verify that the vendor is providing accurate assessment?

- LGE is responsible for maintaining the safety of the workforce and customers. What measures are in place to ensure all RF meters are operating in a safe manner at all times?

- If a baby's crib is located on a wall adjacent a bank of 20 RF meters, is the total physical RF capability of the entire meter bank within the legal SAR limit? More important, is that baby safe?

JENNIFER LOCKHART
4716 COFER 40258

[redacted]

Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields

OET BULLETIN 56

Fourth Edition

August 1999

Authors
Robert F. Cleveland, Jr.
Jerry L. Ulcek

Office of Engineering and Technology
Federal Communications Commission
Washington, D.C. 20554

P1 of 2

Time Averaging of Exposure

The NCRP and ANSI/IEEE exposure criteria and most other standards specify ***"time-averaged"*** MPE limits. This means that it is permissible to exceed the recommended limits for short periods of time as long as the ***average*** exposure (over the appropriate period specified) does not exceed the limit. For example, Table 1 shows that for a frequency of 100 MHz the recommended power density limit is 1 mW/cm^2 with an averaging time of six minutes (any six-minute period) for occupational/controlled exposure.

The time-averaging concept can be illustrated as follows for exposure in a workplace environment. The sum of the product (or products) of the actual exposure level(s) multiplied by the actual time(s) of exposure must not be greater than the allowed (average) exposure limit times the specified averaging time. Therefore, for 100 MHz, exposure at 2 mW/cm^2 would be permitted for three minutes in any six-minute period as long as during the remaining three minutes of the six-minute period the exposure was at or near "zero" level of exposure. Therefore, in this example:

$$\mathbf{(2\ mW/cm^2)\ X\ (3\ min.) + (0\ mW/cm^2)\ X\ (3\ min.) = (1\ mW/cm^2)\ X\ (6\ min.)}$$

Of course, other combinations of power density and time are possible. It is *very important* to remember that time averaging of exposure is only necessary or relevant for situations where temporary exposures might occur that are *in excess of* the absolute limits for power density or field strength. These situations usually only occur in workplace environments where exposure can be monitored and controlled. For general population/uncontrolled exposures, say in a residential neighborhood, it is seldom possible to have sufficient information or control regarding how long people are exposed, and averaging of exposure over the designated time period (30 minutes) is normally not appropriate. For such public exposure situations, the MPE limits normally apply for continuous exposure. In other words, as long as the absolute limits are not exceeded, indefinite exposure is allowed.

Induced and Contact Currents

In addition to limits on field strength, power density and SAR, some standards for RF exposure have incorporated limits for currents induced in the human body by RF fields. For example, the 1992 ANSI/IEEE standard (Reference 3), includes specific restrictions that apply to "induced" and "contact" currents (the latter, which applies to "grasping" contact, is more related to shock and burn hazards). The limits on RF currents are based on experimental data showing that excessive SAR levels can be created in the body due to the presence of these currents. In its 1996 Order adopting new RF exposure guidelines the FCC declined to adopt limits on induced and contact currents due primarily to the difficulty of reliably determining compliance, either by prediction methods or by direct measurement. However, the FCC may reconsider this decision in the future because of the development of new instrumentation and analytical techniques that may be more reliable indicators of exposure.

P2 of 2

INTEL OCTOBER 7, 2014 / 8:55 AM / 4 YEARS AGO

Popular electricity smart meters in Spain can be hacked, researchers say

Reuters Staff

6 MIN READ

* Researchers find security flaws in some smart meters

* Says weaknesses could lead to fraud, blackouts

* Spain one-third done with nationwide meter upgrade

By Eric Auchard

FRANKFURT, Oct 7 (Reuters) - Network-connected electricity meters installed in millions of homes across Spain lack essential security controls, according to two researchers who say the vulnerabilities leave room for hackers to carry out billing fraud or even cause blackouts.

Security experts Javier Vazquez Vidal and Alberto Garcia Illera said in an interview on Monday that so-called smart meters installed by a Spanish utility to meet government energy efficiency goals lack basic safeguards to thwart hackers.

The researchers said flawed code in reprogrammable memory chips enable them to remotely shut down power to individual households, switch meter readings to other customers and insert network "worms" that could cause widespread blackouts.

"You can just take over the hardware and inject your own stuff," Vazquez Vidal said, referring to the threat that hackers could insert malicious code into one box and use it to control nearby meters, and thereby cascade an attack across the network.

Traditionally, energy utilities have kept power plants and mechanical electricity meters safe from cyber attack by keeping them insulated from the open Internet.

Smart meters are connected over power line networks to give customers and utilities instant data about when, where and how much energy households use, enabling energy providers to monitor and adjust energy flows.

The European Union wants more than two thirds of Europe's electricity users to have smart meters by 2020, an initiative it hopes will reduce energy use by three percent.

Over the last decade, most countries in Europe have mandated that smart meters be installed in homes and businesses. But as nationwide deployments have taken place in Italy and Sweden and are now in motion across France, Spain and the United Kingdom, experts have begun to uncover cybersecurity threats posed by some meters.

The two researchers declined to identify the utility or European-based hardware manufacturer of the smart meters found to be vulnerable to attack. They will discuss their findings at the Black Hat Europe hacking conference in Amsterdam next week.

"We are not releasing the exact details; we are not going to say how we did this," Garcia Illera said. "This issue has to be fixed."

The top power utilities in Spain are Endesa, Iberdrola and E.ON. Collectively, 8 million smart meters have been installed, or 30 percent of households.

The researchers said they had identified security flaws only in boxes from one meter manufacturer. Vazquez Vidal said he believes the utility may be able to patch the problem remotely, without being forced to send repair staff to upgrade each box physically.

An expert with Spain's markets and competition regulator, which oversees the smart meter mandate, said the agency was finishing a study on the threat of meter hacking and had not found any evidence it was taking place or at risk of occurring.

LEAVING THE DOOR OPEN

The security impact of a vast array of connected devices from smart meters to automobile controls to wearables such as smartwatches and health monitors are only now being seriously considered by industry, despite their growing use in daily life.

The Spanish researchers said they hacked the meters by bypassing encryption that was designed to secure their communications.

Vazquez Vidal and Garcia Illera said the meters use relatively easy to crack symmetric AES-128 encryption. The limited security appeared to be designed largely to prevent tampering with billing systems by fraudsters, they said.

Once through this first level of security, they said they could take full control of the box, switching its unique ID to impersonate other customer boxes or turning the meter itself into a weapon for launching attacks against the power network.

"Oh wait? We can do this? We were really scared," Vazquez Vidal said. "We started thinking about the impact this could have. What happens if someone wants to attack an entire country?" he said.

They say they tested the devices in their own lab, where they were able to reproduce various attacks in miniature using several of the smart meters.

The same researchers last year uncovered weaknesses in computer chips found in many automobiles, which they said could boost performance or be used to hotwire a car or cause crashes.

Vazquez Vidal, who said he was "unemployed and bored" at home in Cadiz when he carried out the smart meter research, subsequently was hired by a major European automaker based on his earlier work on car security.

Garcia Illera works for a California-based software maker. The two asked that their employers not be identified because their research projects do not involve their employers.

Mike Davis, a top security researcher with cybersecurity consulting firm IOActive, identified similar threats in U.S. smart meter devices five years ago.

“It was strange. Pretty much none of the utilities deploying smart meters at the time were considering the meters themselves as part of their threat problem,” Davis said.

Disclosure of his findings was a wake-up call for U.S. utilities, leading to increased government scrutiny and industry action to better secure the devices against cyberattack.

Davis said the vulnerabilities described by the Spanish research team sounded feasible given the slow response by utilities and meter makers to overhaul their meters’ security.

“The industry is starting to be much more intelligent,” Davis said. “Although for something that is attached to the side of your house, it still has a ways to go.” (Editing by Mark Potter)

Our Standards: The Thomson Reuters Trust Principles.