

ORIGINAL



0000144556

April 24, 2013

Arizona Corporation Commission
Docket Control
1200 W. Washington St.
Phoenix, AZ 85007

RECEIVED
2013 APR 24 P 4: 02
AZ CORP COMMISSION
DOCKET CONTROL

Docket E-00000C-11-0328 Smart Meters

To Whom It May Concern:

This filing for the Smart meter docket #E-00000C-11-0328 contains an original filing plus 13 copies and is being filed on behalf of the Safer Utilities Network.

Sincerely,

Frank R. Mead
LoronaMead, PLC
Attorneys for Safer Utilities Network

Enl.: Certificate of Service

Arizona Corporation Commission
DOCKETED
APR 24 2013

DOCKETED BY MN

Certificate of Service

The enclosed letter, dated April 22, 2013, was **MAILED** this 24th day of April, 2013, to the following:

Arizona Public Service Company

Jeffrey Johnson
P.O. Box 53999, STA. 9905
Phoenix, Arizona 85072-3999

Arizona Public Service Company

Thomas Mumaw
P.O. Box 53999, Station 8695
Phoenix, Arizona 85072-3999

Arizona Public Service Company

Michael Curtis
501 East Thomas Road
Phoenix, Arizona 85012-3205

Arizona Public Service Company

William Sullivan
501 East Thomas Road
Phoenix, Arizona 85012-3205

Arizona Public Service Company

Charles Moore
1878 W. White Mountain Blvd.
Lakeside, Arizona 85929

Mohave Electric Cooperative, Inc.

Peggy Gillman
P.O. Box 1045
Bullhead City, Arizona 86430

Mohave Electric Cooperative, Inc.

Tyler Carlson
P.O. Box 1045
Bullhead City, Arizona 86430

Mohave Electric Cooperative, Inc.

M. Jo Smith
88 E. Broadway
Tucson, Arizona 85701

Mohave Electric Cooperative, Inc.

Bradley Carroll
88 E. Broadway Blvd. MS HQE910
P.O. Box 711
Tucson, Arizona 85702

Mohave Electric Cooperative, Inc.

Michael Patten
Roshka DeWulf & Patten, PLC
One Arizona Center
400 E. Van Buren St. - 800
Phoenix, Arizona 85004

Mohave Electric Cooperative, Inc.

John Wallace
120 N. 44th St. - 100
Phoenix, Arizona 85034

Mohave Electric Cooperative, Inc.

Janice Alward
1200 W. Washington
Phoenix, Arizona 85007

Mohave Electric Cooperative, Inc.

Steve Olea
1200 W. Washington St.
Phoenix, Arizona 85007

Arizona Corporation Commission

Lyn Farmer
1200 W. Washington
Phoenix, Arizona 85007-2927

April 22, 2013

Docket Control
Arizona Corporation Commission
1200 W. Washington St.
Phoenix, AZ 85007

Docket E-00000C-11-0328 Smart Meters

PLC Smart Meters Should not be Exempt from Encryption Requirement

On October 23, 2012, Steven Olea, Director of the Utilities Division, entered a draft of the guidelines for smart meters into this docket.

Guideline #3 requires that wireless transmissions be encrypted, while PLC transmissions are exempt. PLC should not be exempt, as they pose both privacy and security risks.

Outsiders could intercept PLC transmissions in three general ways:

- Monitoring voltage fluctuations from an ordinary wall socket
- Using a current transformer or coupler, clamped around an electrical wire
- Wireless reception of PLC signals radiating from the wires

The voltage fluctuations created by PLC can travel from house to house,¹ and are not limited to the path of the current (i.e. the straight path between meter and receiver).

There are people who enjoy the challenge of decoding “secret” signals, and also terrorists who may do it for their own purposes. Some helpful decoding information is already available on the web.²

Once someone has decoded a specific PLC system, they will likely boast about their feat by posting detailed information and software on the websites dedicated to these activities. Then others can use the information.

This is what happened when someone cracked the DVD copy protection. The movie industry thought their movie DVDs could not be copied, but today anyone can buy a DVD copy program from most computer and office supply stores.

The computer industry also had to learn the lesson that unencrypted signals traveling on wires are not secure. Believing that PLC signals are any different is not responsible.

Some PLC smart meters (such as TWACS) can report household electrical usage every 15 minutes. This level of detail can provide significant information about activities and habits of the people living in the house. This is private information that must be protected by encryption.

Also, hackers and terrorists may take advantage of the vulnerability of PLC smart meters to create blackouts.

Some PLC smart meters have built-in service disconnect switches and the ability to receive software upgrades. Both of these functions are controlled by signals carried by PLC. Without PLC encryption, hackers and terrorists could send their own signals to PLC smart meters, first instructing the meter to disconnect the power, then download new software to the meter so it locks up. Utility personnel would then have to manually reset and restore each smart meter. This will mean a black-out will last for several days, if not weeks, and there would be no prevention of repeat attacks.

It appears that Pacific Gas & Electric has already thought of this problem. They have disabled the disconnect switch in their PLC meters, while they kept that feature in their wireless meters, which do have encryption.³ We do not know for sure that the PG&E PLC meters lack encryption, but a thorough search of the websites of the two dominant PLC smart meter vendors⁴ did not find any references to PLC encryption capabilities. As such a feature is highly desirable, a vendor would very likely advertise it if available.

PLC is not limited to communication between the electrical meters and the utility. It can also be used to control appliances⁵ though this is not yet common.

Without encryption of PLC communication, it would be possible for hackers and terrorists to send bogus signals to appliances in people's homes. Many scenarios are possible, including turning off the heat in homes in northern Arizona during the winter, so the pipes freeze.

The Federal Government is starting to take these kinds of security threats seriously. Former Secretary of Defense Leon Panetta recently warned of a possible “cyber Pearl Harbor”.⁶

The Corporation Commission should not encourage the installation of outdated equipment with significant security and privacy risks. PLC should not be exempted from an encryption requirement.

Submitted on behalf of:
Safer Utilities Network
P.O. Box 1523
Snowflake, AZ 85937

References and Notes

- (1) National Institute of Standards and Technology Smart Grid Interoperability Panel, PAP-15.
<http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP15PLCForLowBitRates>
(Scroll down to “Why Is Coexistence Important”)
- (2) For the most commonly used smart meter PLC system in the USA, see: United States Patent 5,933,072 and *A TWACS System Alarm Function for Distribution Automation*, by Sioe T. Mak, IEEE Transactions on Power Delivery, April 1994.
- (3) *Security Pros Question Deployment of Smart Meters*, Kim Zetter, Wired Magazine, March 2012.
<http://wired.com/threatlevel/2010/03/smart-grids-done-smartly/>
- (4) Aclara: www.aclara.com, www.aclaratech.com
Landis + Gyr: www.landisgyr.com
- (5) Examples are the DRU (Demand Response Unit) and LCT (Load Control Transponder) from Aclara, which can control a wide range of appliances, such as furnaces, air conditioners and water heaters.
- (6) *Digital Danger*, Charles Choi, Scientific American, December 2012.