Advanced Metering Infrastructure

HEALTH, SAFETY, PRIVACY, AND OTHER CONCERNS RELATED TO ADVANCED METERS

THE CITY OF INDEPENDENCE, MO

JANUARY 12, 2018

Radio Frequency (RF) and Health Affects:

Installations of advanced meters have more than doubled since 2010, with almost half of all U.S. electricity customers' accounts having advanced meters according to the Energy Information Administration report released on December 6, 2017. Concerns have been raised about the safety of advanced meters and potential health effects from exposure to radio frequency (RF) transmission.

The City of Independence City Council has directed staff to pose several health-related questions to the City of Independence Advisory Board of Health (BOH). The BOH met on December 7, 2017 to discuss AMI health-related issues and develop responses to questions posed by the Independence City Council. The BOH questions and responses are provided below. City Council further directed staff to address other, non-health-related concerns, specifically those related to alleged fire hazards, privacy of customer data, and cyber security. These issues are discussed in subsequent sections of this report.

1. Do advanced meters pose a health threat because they communicate using wireless signals?
    a. Have qualified researchers confirmed that there is an increased health risk?
        i. BOH Response: "*No, researchers have not confirmed that there is an increased health risk. According to scientific reviews by the World Health Organization (WHO), there is no convincing evidence supporting short- or long-term adverse health effects caused by exposure to the low-level radio frequency energy of wireless signals from transmitters. It should be noted that additional studies are recommended by WHO."*
    b. Is the risk measurable and significant?
        i. BOH Response: *"Risk is measured in Specific Absorption Rate (SAR) which measures the rate the radio frequency energy is absorbed by the body. All wireless devices sold and operating in the United States are tested to ensure that they do not exceed the maximum allowable SAR when the device is operating at its highest possible power level. Thus, the SAR risk from advanced meters is within acceptable Federal Communication Commission (FCC) standards. The International Committee on Electromagnetic Safety (IEEE) and the National Council on Radiation Protection and Measurements (NCRP) developed the FCC SAR standards."*
    c. How does it compare in scope to other wireless signals prevalent in the world today?
        i. BOH Response: *"Acceptable standards set by FCC for radio frequencies limits and exposure amounts depend on the frequency of continuous whole body exposure and the source. AMI has a lower level frequency (0.0018 W/m^2) than regularly used household equipment such as microwaves (0.0043 W/m^2) or Wi-Fi base station (0.0021 W/m^2). The AMI frequency range is not considered harmful to an individual's health (FCC). The frequency and power of the radio frequency waves given off by a smart meter are similar to that of a typical cell phone or cordless phone, and is well within the safe range (American Cancer Society). Advanced meters transmit data up to six times a day, amounting to less than*

one second of transmission a day. A person would have to be exposed to the RF from a smart meter for 375 years to get a dose equivalent to that of one year of 15-minutes-per-day cell phone use."

2. Is there an increased risk to people who live near advanced metering telecommunications transmission facilities?

    a. Have qualified researchers confirmed that there is an increased health risk?

        i. BOH Response: *"No, qualified researchers have not confirmed that there is an increased health risk. Radiation is characterized as either ionizing or non-ionizing. Ionizing radiation, under certain circumstances, leads to cellular and/or DNA damage with prolonged exposure. Examples of ionizing radiation include ultraviolet light and x-rays. Radiation associated with transmission facilities is non-ionizing and is generally considered harmless due to its lack of potency (National Institute of Environmental Health Sciences, National Cancer Institute). The frequencies of energy emitted by broadcasting transmitters, power lines or electrical wiring, mobile phones, or other wireless communication devices are too weak to break a cell's chemical bonds (WHO). This type of exposure is not recognized as increasing health risks (International Agency for Research on Cancer)."*

    b. Is the risk measurable and significant?

        i. BOH Response: *"Researchers have evaluated the radio frequency radiation from wireless telecommunication devices and equipment, including cell phones, smart meters, and portable wireless devices to assess its effects on DNA from exposure. The epidemiologic studies do not show an increased risk (National Cancer Institute)."*

    c. How does it compare in scope to other wireless signals prevalent in the world today?

        i. BOH Response: *"The FCC currently determines the accepted standard of safety against known thermally induced health impacts of smart meters and other electronic devices in the same range of radio frequency emissions. Exposure levels from smart meters are well below the thresholds for negative health effects (California Council on Science and Technology)."*

Questions were posed to Sensus (supplier of the meters and telecommunication infrastructure) and their responses are listed below:

1. What is the risk for people living close to the cell towers?

    Sensus Response: *"Sensus Base Stations and meters meet all FCC certification requirements that govern the amount of RF emissions that a radio can transmit. The Sensus FlexNet system is based on a point to multipoint system. The average RF transmission duration for both the water and electric meters is approximately 50*

milliseconds (ms) per transmission. When configured to transmit 6 times per day (commonly used for water & electric utilities and planned for City of Independence) that would equate to 6 x 50ms = 0.3 seconds per day. The transmission duration is dependent upon the amount of configurable data points the City wants to capture and transmit. More data points requested would increase the duration."

2. What information can you provide that would aid in the understanding of RF Emissions?

   Sensus Response: *"The link below offers more information on RF emission management and safety."*

   https://sensus.com/resources/videos/fact-fiction-smart-meter-rf-emissions/

Fire Concerns Related to Advanced Meters:

Meter fires are an important and sensitive issue that has particularly come under public scrutiny during the widespread infrastructure upgrades of the last decade as utilities increasingly move to advanced meters.

In response to the fire concerns raised by City Council, several questions were developed for consideration. The questions are listed below.

1. Is there a fire hazard risk with the AMI meters proposed?

   Sensus Response: *"The industry has faced issues caused by installing a meter in a bad meter socket such as loose jaws, corrosion, unsealed meter enclosure and bad wiring. This situation often creates a poor connection between the meter and the socket resulting in higher resistance that generates a thermal heating condition that can cause melting or even a fire. Across the industry, thermal heating due to these conditions is rare, and even rarer in those situations where the sockets are inspected and issues addressed before installing the new advanced meter. The Sensus Stratus® electricity meter is UL certified and following a $5 million investment in the company's premier meter testing lab, is design hardened and tested to verify performance under normal operating conditions and those that go beyond industry standards."*

2. Are the advanced meters UL approved?

   Sensus Response: *"Sensus and other meter vendors meet or exceed the industry standards set by ANSI and the new requirements for being UL 2735 certified."*

3. What safety features will be provided by the meter manufacturer to detect overheating meter sockets?

   Sensus Response: *"The FlexNet microprocessor in the Sensus Stratus® electricity meter uses an embedded temperature sensor to measure the ambient temperature inside the meter enclosure. The temperature is sampled every ten seconds at the same time as the voltage is read from the meter. The electric meter will contain an automated disconnect switch that will disconnect power when the temperature threshold has been exceeded at*

either the meter socket or on the circuit board and provide immediate alarm notification to the City's trouble dispatch office."

4. What has been the meter fire experience with the AMI solution being proposed by our vendor?

   In 2014, Sensus provided meters to Lakeland Electric – a municipal utility in Florida. Lakeland Electric serves approximately 125,000 electric customers. During their meter deployment, they experienced overheating issues with 6 meters. Lakeland officials made the decision to replace approximately 10,500 remote-disconnect meters and upgrade to a newer model that offered high temperature detection technology and other design enhancements that would help prevent water and other contaminants, such as insects, from entering the meter. Testing of the 6 meters in question revealed that one was caused by an issue with a meter base attached to a home, three were caused by utility over-voltage, two were caused by water intrusion through the meter base, and one remained undetermined.

   Sensus provided the following response to the Lakeland incident:

   "Lakeland made a decision based on a few incidents and pressure from the media to pull out a small portion of their meter population related to remote disconnect meters. Sensus worked closely with Lakeland to determine root cause in each of those incidents and there was no evidence that the meter was the cause of the incident. Lakeland recently began deploying Sensus' Stratus remote disconnect meter, considered the industry's most robust meter platform.

   Sensus, and others in the industry, have confirmed that overheating issues at the junction box could be caused by many reasons, most of which are based on the junction box itself and other variables beyond their control. These included water intrusion due to holes in meter boxes, hot socket conditions in the meter box and over voltage in the distribution system. Poor installation procedures have also contributed to meter issues.

   Over the past four years, Sensus has spent more than $5M in testing equipment and processes to build the industry's premier meter testing facility. This facility features the simulation of conditions that an electric meter will be exposed to in its lifetime that are above and beyond ANSI and UL2735 requirements. Aside from our own testing, our electric meter is tested via third-party test houses, generally using Met Electrical Testing Company Laboratories and Underwriters Laboratories (UL), and can provide those reports upon request."

   These third party test houses help companies demonstrate safety, confirm compliance, enhance sustainability, manage transparency, deliver quality and performance, strengthen security, protect brand reputation, build workplace excellence, and advance societal wellbeing. These two companies are the main source of product safety testing and certification in the United States.

5. What has been the fire experience in KCMO and KCK?

a. Kansas City Power & Light is at the tail end of a two and a half year project to install more than 700,000 advanced meters across the metro. A handful of meters installed experienced overheating as part of this project. KCP&L did an internal investigation and made the following statements to the press:

   i. *"Out of the more than 700,000 meters KCP&L has installed, we are only aware of six meter malfunctions. At this point, we have found nothing that leads us to believe there is a problem or safety issue with the new meters."*

   ii. KCP&L said the type of advanced meters they are using have not been recalled.

   iii. The utility's statement also said the vast majority of house fires are caused by factors other than meters like outdated and overloaded wiring.

b. A spokesman for the Kansas City Board of Public Utilities, BPU, said that utility has installed 70,000 advanced meters in Wyandotte County and there have been no reports of advanced meter fires there.

6. What are the various possible fire hazards and how do we propose to mitigate each type?

   a. The issues and conditions that have created the concern are industry-wide concerns with all manufacturers and utility infrastructures. Many studies have been done concerning the cause of meter fires during AMI deployments. The results have shown that the meter is usually not the culprit but overheating of the meter socket itself, a condition referred to as “hot socket”, is the main issue.

   b. Several features or sources can cause hot sockets, but among the most prevalent are:

      - Mechanical breakdown of components
      - Excessive moisture
      - Environmental contaminants
      - Frequent meter changes outs (resulting in loss of jaw tension)
      - Excessive electrical load (overload or short circuit)
      - Loose or melted conductors
      - Vandalism
      - Ground settling
      - Storm damage

      When old meters are removed, an opportunity is created to inspect equipment that may have been covered up for years, perhaps even decades. By detecting signs of deterioration or damage at the meter site and acting to make repairs, The City can proactively ensure the safety of their meter infrastructure for years.

      As part of the advanced meter deployment, meter technicians will be trained to identify hazardous meter socket conditions. Safety protocols will be developed to anticipate and address safety issues for every element related to meter, site and socket. These protocols will ensure that every meter is fully assessed and problems acted on. The City

has set aside funds to address any meter socket replacements or repairs. All repairs will be made by IPL Journeyman Meter Technicians or certified electrical contractors.

Privacy Concerns Related to Advanced Meters

The City of Independence takes privacy of customer utility data very seriously. We've been securely handling confidential customer data for decades and will continue to do so utilizing proven industry practices. The proposed AMI system includes multiple layers of security controls designed to protect the privacy and security of customer data. Data transmitted across the AMI network does not include personally identifiable information, such as social security numbers or banking information. The City of Independence does not permit sharing of customer's personally identifiable information to any third party except by written authorization of the customer or the request by law enforcement or public agency. Third Parties is defined as any person or entity other than employees of the City of Independence Public Utilities – Electric, Water, Water Pollution Control, Finance Department, or Legal Department, or any other entity contractually bound to the City to provide Managed Services, billing or collection services for utility accounts. Independence employees in all other City of Independence Departments shall be considered third parties and usage data connected to personal information shall not be shared with them without City Management review.

Customers have expressed concern that the data collected via an advanced metering solution can tell when a customer is home or away and exactly what the customer is doing while at home. Usage data may show when a home is occupied, because energy consumption is typically higher during those times. The advanced meter cannot identify what activities are taking place or the specific appliance in use. Some customers have opined that advanced meters actually make the electric grid less secure by providing an avenue to hackers to break into systems through the advanced meter. While cyber bad actors continually attempt to break into electric systems, their focus is generally at higher levels in electric grid operations where adverse impact to a wider area of the grid could be achieved. Hacking a meter to procure personally identifiable information is unlikely for a variety of reasons. Cyber intruders like to work remotely via the Internet, and advanced meters do not offer that option. Radio-based advanced meters require the perpetrator to be nearby in order to commandeer the weak communication signal, break the proprietary communication protocol and to be there for extended periods to collect the short bursts of data sent (less than a second per day). The data transmitted is the meter identification number and the electric or water usage. Therefore, advanced meters are an unlikely and unprofitable target for hackers.

Comments from Sensus Regarding the FlexNet Telecommunication Network:

In response to the privacy concerns raised by City Council, several questions were developed and sent to Sensus for response. The questions are listed below.

1. Does the fact that the data resides in the "cloud" make it more vulnerable (to a cyber breach)?

   "The Sensus FlexNet network follows a "defense in depth" security strategy. The network head end will be housed in the Sensus Data Center ("the cloud" in this case). The Sensus Data Center is at least as secure as the City's own Data Center, and likely far more secure due to the extremely stringent security practices that Sensus follows. Sensus maintains a dedicated Security Operations team, along with a 24x7 SOC (Security Operations Center) where we monitor security

around the clock. We maintain best practices around patch and vulnerability management, monthly vulnerability scanning, along with 3rd party penetration tests. Ensuring the integrity of our customers' systems is our highest priority."

2. How many security breaches have occurred with Sensus?

   "Sensus has had zero security breaches for our US Software-as-a-Service (SaaS) customers. No major breaches have been reported to Sensus by non-SaaS customers."

3. What data will be collected?

   "The FlexNet network does not transmit any personally identifiable information over the network. The network transmits Meter IDs, AdvancedPoint IDs, interval data and alarm data. These data are matched to the customer account within the City's CIS billing application."

4. What additional data will be collected that is not collected now?

   "The Meter ID, the Advancedpoint ID, and any alarm that may have occurred."

5. Is there a risk of hacking with transmission or storage and how does Sensus mitigate this?

   "Risk mitigation is performed for the entire solution, including meter to head-end communications, the method of backhaul to the backend, as well as data storage. Different mitigations are applied for each risk identified at different levels, for example when securing the backhaul only necessary ports for communicating to the RNI (head end system) should be open with only one White List location available to speak. Use of a White List is the process of restricting everything other than the list of entities approved for authorized access or privileged membership to enter a specific area of computing.

   Security and confidentiality across the FlexNet transmission network is achieved by encrypting communications using 256-bit AES (Advance Encryption Standard) encryption. Each meter has a unique AES 256 key that is used to encrypt/decrypt communications. This provides protection and confidentiality for all communications between the meter and Head End System. The encryption uses National Institute of Standards and Technology (NIST) approved, Federal Information Processing Standard (FIPS) 140-2 compliant encryption algorithm with a strong key (256 bits), this ensures that communication cannot be intercepted during transmission. In addition, to prevent a replay attack (the recording and replay of a harmful but still-encrypted command like disconnect), all encrypted communications use a time quantum.

   All sensitive data within the system is stored in an encrypted format using FIPS-compliant algorithms or hashed using NIST standards. Sensitive data stored on the system is limited to cryptographic keys, and passwords. The Sensus FlexNet network follows a "defense in depth" security strategy. The network operates on secure, FCC license frequencies and can be encrypted end-to-end. The modulation used by the FlexNet system can not be decoded or interpreted by off-the-shelf RF equipment. All network connections are secured by a Virtual Private Network (VPN), and the network is monitored 24/7/365. Sensus routinely tests the network and data center against security threats, and conducts periodic third-party security assessments."

6. Does the AMI system create new security risks? How will the risks be mitigated?

"Sensus adheres to a risk based model for assessing risks and threats during the design, development, testing and implementation of our FlexNet AMI suite of products. This is consistent with the implementation of Sensus' Secure Development Lifecycle (SDL) program. This model extends through our entire end to end solution. From assessing risk at the physical and logical areas of the endpoints, to network related threats through the communication path, to the risks associated with the head end system located in a secure data center. Sensus breaks each of these areas up into individual domains and applies the same assessment criteria to them based on physical and logical security threats. Once risks and threats have been identified, Sensus will mitigate these through a layered security model. By providing security controls at each layer of the product, Sensus practices defense in depth throughout our entire product line. Using the CIA (Confidentiality, Integrity and Availability) model, Sensus applies security controls (authentication, authorization, encryption, auditing, logging, etc…) to each components of the system to address the CIA requirement with regard to the threats and risks. By applying specific security controls to address CIA requirements, Sensus can ensure that threats and risks are being mitigated at each layer (Endpoint, Network, and Head End System) of the system.

Based on the Risk analysis of the Sensus FlexNet AMI solution, and mitigations for risks identified, Sensus has built a secure end-to-end system architecture based on best practices and industry standards. In our security architecture, the various components are segmented into separate security domains, threats/risks analyzed, and the associated security controls for each component are applied. Through this architecture, we have built defense in depth through a combination of Sensus and third-party security controls. These controls provide the confidentiality (encryption), integrity (authentication), and availability (redundancy and resiliency) throughout the entire FlexNet solution. The diagram shown in the following figure illustrates the typical security architecture for the FlexNet solution."

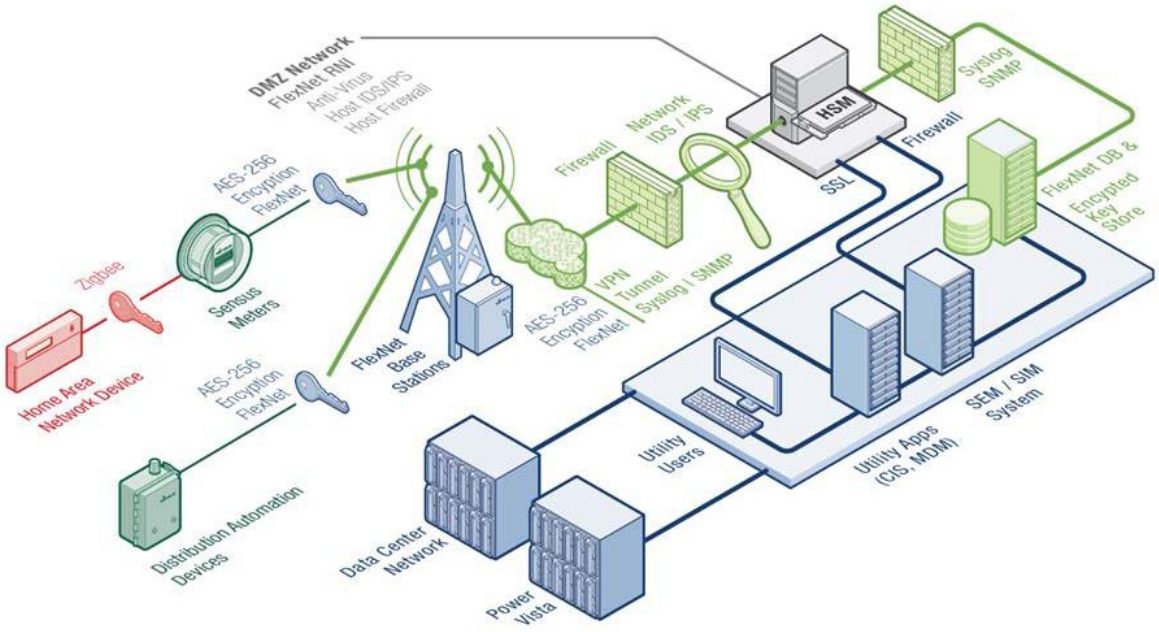

Figure 1: Security Architecture Domains

"In addition to the overall security architecture, the following table describes the detailed security controls provided by both Sensus and third parties. These controls are based on individual components in each security domain."

Functional Area	Sensus Component	Sensus Security Controls	Third Party Security Controls
Field Devices	Sensus Meters	Flexnet Security Architecture: • Physical locks and seals • Tamper alarms • Encryption AES-256 • AES-CCM message authentication • DSS Digital Signatures • ECDH Key exchange • Auditing and Logging – events pushed back to head end system • FCC Licenses Spectrum • Frequency Shifting Key (FSK)	• Third-Party Crypto Libraries
Communications	Flexnet Base Station	• Physical locks and seals • Tamper alarms • Weather-proof enclosures for external deployment • Locked down Linux kernel • IP-Tables host-based firewall (Sensus' pre-defined policy) • Authentication/authorization integrated with Radius or LDAP • OpenVPN/Stunnel used for secure backhaul communication • SSH used for encrypted administration of FlexNet Base Station remotely • SNMP and Syslog used for auditing and logging	• Third-Party, Host-Based Firewall
Head End System	Regional Network Interface (RNI)	• System segmentation to support DMZ deployments • Separation of duty through role-based Access Control • Integrated LDAP for Authentication/authorization • Support for integration with Microsoft Active Directory • Sensus provided system lockdown scripts • Sensus System Hardening Guidelines • OS-integrated firewall with Sensus-provided policies • SSL Encryption 1. User interface 2. Inter-process communication • Hardware Security Module for secure key generation, key storage and cryptographic functions	• Data Center Physical security control • Network-based firewall for DMZ segmentation • Network-based intrusion detection/prevention • Host-based malware/spyware protection • Support for Host integrity software (Tripwire) • Support for third-party multi-factor authentication mechanisms • Support for customer security policies and procedures
Back Office Application	N/A	• Sensus RNI provides authentication and authorization for API access • Sensus RNI provides SSL encryption for API access	• MultiSpeak Support

Table 1: Sensus and Third Party Security Controls

Meter Operational and Accuracy Concerns:

Just like traditional analog meters, digital advanced meters measure how much electricity and water you use. The main difference is that the new digital meters collect that information more times throughout the day. Consumption will be measured for electricity on 15-minute intervals and water consumption will be measured once an hour.

Once fully enabled, the new advanced metering infrastructure will provide access to online tools that can help you manage your electric and water bill, set up email or phone alerts to warn you of potential high bills and enhance IPL's power restoration process following storms.

The electric meters that Sensus will provide have a guaranteed meter accuracy of 0.2% for both residential meters and commercial/industrial meters. The water meter that the City has selected is the most accurate water meter available on the market today. It contains no moving parts and is guaranteed to maintain its accuracy over a 20-year lifetime.

The technology systems that support advanced meter systems have extensive data validation processes to protect the accuracy of billing records. In addition, advanced meters must meet rigorous requirements for accuracy, which were developed by the American National Standards Institute (ANSI). National Institute of Standards and Technology (NIST)-certified test equipment also is required to verify initial and continuing advanced meter accuracy.

Before the meters are shipped to the City, the manufacturer, Sensus, will perform accuracy testing on 100 percent of the meters to ensure that they meet the City's requirements for an accuracy variation of +/- 0.2 percent. Sensus will supply certified testing results to the City to demonstrate their meters passed all of the required tests for new meters.

In addition to this, the City will conduct sample tests periodically during the deployment period to verify that the meters being delivered match the certified test results from the manufacturer. If the sample test fails then the entire production run will be rejected.