EPRI | ELECTRIC POWER
RESEARCH INSTITUTE

A Case Study on the Revenue Protection Software: Sacramento Municipal Utility District Smart Grid Demonstration

December 2014

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICU-LAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCU-MENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUD-ING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTI-TUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Table of Contents

Overview

When it completed rollout of advanced meters in 2013, the Sacramento Municipal Utility District (SMUD) implemented data analytics software to identify instances when a meter had been tampered with, by-passed, or had simply malfunctioned. Traditionally, SMUD meter readers would identify such issues while reading the meters each month. In order to meet or exceed the standard set by this manual inspection process, SMUD installed revenue protection software provided by Detectent, Inc. This software generates leads for on-site investigation based on results from theft detection algorithms that process numerous datasets from different utility systems as well as external sources.

The primary purpose of this project is to replace physical inspections with data analytics in order to achieve numerous objectives, including:

- Protect the customer and SMUD employees from potentially unsafe conditions due to someone tampering with the meter.

- Reduce annual revenue loss from theft.

The revenue protection software compiles utility and third party datasets for evaluation. The utility data used by the software includes datasets from the advanced metering infrastructure (kWh, voltage, register, alarm, event, and other alert data), the customer information system (customer, premises, billing, and service notifications) and from the GIS (geospatial information system). External or third party datasets, such as county assessor property information, weather data, and demographic data, are also utilized. Almost all of the datasets are updated daily with the exception of the GIS and county assessor datasets which are updated weekly and quarterly, respectively. In addition, SMUD attempts to query the datasets monthly to identify and to fill gaps in the datasets missed by the daily updates.

The software identifies and prioritizes the most likely theft cases. The rich datasets enable SMUD's revenue protection analysts to generate leads for investigation, using 20+ theft detection algorithms. Simple leads, such as a "zero usage" that match disconnection orders, are usually viewed and closed without a field inspection. The leads requiring field inspection are prioritized based on weighting criteria defined by the analysts. The weighting criteria are continuously adjusted so that investigation and recovery activities are optimized.

Results

The revenue protection software permitted SMUD to move from a reactive response, relying on tips from the public and from SMUD employees, to a proactive response, using statistical analyses to make inferences of the data and identify possible theft.

SMUD has benefited from the technology and reduced revenue loss. However, the methodology that SMUD uses to track various types of leads makes it difficult to pinpoint the actual success rate of the generated theft leads. For example, the system assigns a new order each time an investigation is undertaken. If the original investigation determines that there is theft occurring and the meter is removed, all subsequent follow-ups to the premises are issued a new investigation order even though each one relates back to the original order.

Even though the precise theft detection success rate is elusive, SMUD does assign the following benefits to the detection software, and is starting to see trends, such as increases in the kWh billed and dollars collected, as shown in the table below. Benefits to the customer:

- Improves customer safety by better identifying meter tampering.

- Reduces revenue loss that would negatively impact customers by contributing to future rate increases.

Benefits to the utility:

- Improves employee safety.

- Prioritizes leads based on ones with the highest probability of theft.

- Provides efficient use of SMUD resources (labor, fuel, investigation costs, and software).

Table 1 illustrates the billed amount versus the collected amount associated with theft cases. The increases from 2011–12 to 2013 are largely driven from the use of the detection software to identify theft case and determine customers that are more likely to pay, such as commercial customers. This is shown in more detail in the last two columns that show a 12 month comparison between before and after the installation of the revenue protection software.

Table 1 – Summary of the Billed versus Collected Amounts with and without the Revenue Protection Software

	2011	2012	2013	12 Months Prior to Detectent	12 Months After Detectent
$ Billed	$1,752,820	$1,120,860	$2,953,334	$1.36M	$3.11M
kWh Billed	9,912,680	5,009,350	13,738,497	-	-
$ Collected	$138,020	$337,030	$653,418	$334k	$723k

Introduction and Background

The revenue protection software provided by Detectent, Inc. provides SMUD a solution to reduce revenue lost to theft each year by identifying instances of theft. SMUD estimates that approximately 1% of its annual revenues are lost to theft. For the 2007-2012 time period, SMUD back-billed $8.6 million from theft-related cases. As a result, the primary goal of the software solution is to utilize proven pattern recognition algorithms to detect probable cases of meter tampering, by-pass, and malfunctioning that tend to be signs of theft occurring. This is extremely important since the installation of advanced metering infrastructure (AMI) meters has eliminated monthly meter readings by trained staff that would have detected these issues in the past. Moving forward, the revenue protection and detection software now serves as the virtual "eyes in the field" for SMUD.

Figure 1 illustrates an example of attempted power theft. The revenue protection software flagged the account associated with this meter installation as having a probable case of tampering. The field investigation determined that someone attempted to steal power by drilling thru the meter cover to install a stick on a pushbutton used to place the meter in to a diagnostic mode. Although this was an attempt of power theft, the meter continued to register energy consumption as programmed.

The objectives of the software implementation were twofold: 1) SMUD moved from a reactive to a proactive approach for identifying theft. This was a natural outgrowth of the AMI project since the periodic visual inspections were abandoned along with the manual

Figure 1 – Example of Attempted Power Theft

meter reading activities. 2) The analytics software would serve as a platform to build future applications in billing, customer segmentation, and data-based decision making. Above all of these business-related objectives was the primary goal to ensure customer and employees safety by identifying meter tampering.

The revenue protection software is composed of two applications: an analytics platform called CustomerIP and a revenue protection application called RevEnhance. For Detectent, the software usually resides on their servers and the data from the utility is collected and supplied to them for processing and generation of possible theft leads that would then be sent to the utility for investigation. The uniqueness of the SMUD project was that the software is hosted on SMUD servers, although Detectent provides troubleshooting and technical support for SMUD. As a result, SMUD revenue protection analysts collect and process the data using the same core algorithms that Detectent would have used to generate leads for investigation. The data used by the software comes from both internal sources, such as the data from the customer information and AMI systems, and from external sources, such as weather and demographic data. The third party data resources enable the analysts to understand what is affecting the usage trends and to fortify the utility data for graphic display and for enhanced analytics.

Upon generating the leads for investigation, the revenue protection software has robust life-cycle tracking and reporting tools to trace theft cases from beginning to closeout. All evidence, such as notes and photos, gathered during an investigation is stored by the software. The software tracks the billed versus the collected amounts for each case and for an aggregate of cases. Additional reports can be configured to match utility reporting preferences.

Approach/Methodology

The revenue protection software was implemented over an 18 month time period to identify and prioritize cases of AMI meter tampering associated with power theft. The software performs data analytics on various data sets to rank probable theft cases. Table 2 and Table 3 show the most common data sets from internal and external sources. The data from the AMI meters provides key insights into the condition of each of SMUD's approximately 620,000 meters. The meters provide interval, register, voltage, and other data including events, alerts, and alarms. This meter data is pulled from the Itron Enterprise Edition meter data management system and from the suite of applications in the Silver Springs UtilityIQ platform. This data and the other data from customer related SMUD legacy systems are uploaded, in most cases, on a daily basis to the revenue protection software.

Table 2 – SMUD Data Sources Supplied to the Revenue Protection System

Data Category	Source	Frequency	Transfer Method
Customer Records	SAP	Daily	ETL (flat file)
Meter Records	SAP	Daily	ETL (flat file)
Billed Consumption	SAP	Daily	ETL (flat file)
Service Orders	SAP	Daily	ETL (flat file)
Meter Values	Itron Enterprise Edition (IEE) Meter Data Management System	Daily	Direct connection
Meter Events	Silver Spring UtilityIQ	Daily	ETL (flat file)
Device Location Notes	Revenue Protection System/Customer IP	On Demand	ESB
Past Investigations	SMUD Revenue Protection database	One time	Access Database

*Table 3 – External Data Sources used by Revenue Protection System*

Data Category	Source	Frequency	Transfer Method
Weather	Detectent (NOAA)	Daily	Web Service
County Assessor	DataQuick	Every 3 years	Manual Flat File
Customer Listings	SalesGenie (Yellow Pages)	Every 3 years	Manual Flat File

The revenue protection software processes the data to rank probable tamper and theft cases. The ranking relies on a combination of algorithms. The weight given to each algorithm result can be configured. This permits refinement of the total weighted score used to rank each case. Some of the algorithms utilized in the software are listed below.

- Consumption drop score – looks for decrease in consumption over past two years.

- Drop on tamper flag – looks for consumption drop immediately following a tamper or power down event.

- Frequent tamper alert – looks for a pattern of multiple tamper flags and a repeatable pattern.

- Load factor score – targets businesses with low consumption relative to their demand, a possible indication of intermittent tampering.

- Local chain business comparison – compares usage of customer to usage of similar customers.

- Max monthly usage – records the highest monthly energy consumption for comparison.

- Meter capacity score – finds businesses with CT services that have low consumption relative to their capacity.

- Meter set score – compares the seasonal interval consumption before and after the meter set.

- Minimum consumption score – assigns a score to the minimum energy use by the customer.

- Neighbor score – measures deviation from expected consumption based on nearby residences.

- Reverse power alert – records when power flow through the meter is from the customer to the utility.

- Slope percent – slope component of the linear regression over past 2 years.

- Total score – combines resultant scores of other algorithms to determine the likelihood of theft.

- Unauthorized use alert – records and flags energy consumption on an idle meter.

- YP score – identifies location of the customer based on phone number of customer.

- Zero use alert – registers zero energy consumption.

The revenue protection software analyzes the input data with the algorithms described above to identify and prioritize accounts that score the highest. This initial screening provides SMUD analysts a methodology to investigate and rank the accounts using the software so that the leads with the highest probability of having tampering and theft occurring are given to the field technicians to investigate first. Daily and weekly field investigations can be displayed geographically so that field investigations can be ordered to minimize travel time and fuel costs. Figure 2 shows an example graphical display used for daily field investigations. This prioritization ensures that the SMUD resources are used effectively throughout the process.

Figure 2 – Graphic Display of Investigation sites within the SMUD Service Territory
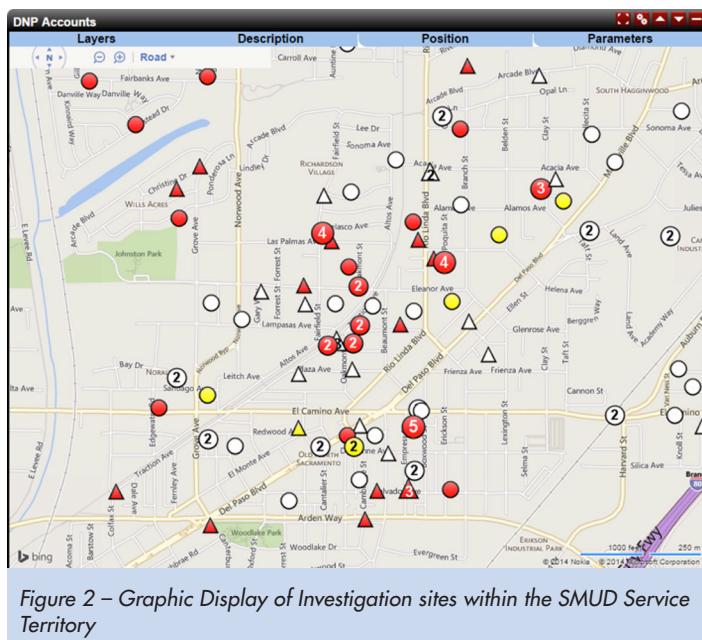
Modifications to the revenue protection software were made to optimally interface with SMUD systems and for reporting purposes. Different graphical views were created for SMUD staff to support the daily activities of identifying and investigating theft leads. Also, the detection algorithms were customized to facilitate better tracking and monitoring throughout the investigation process. All data and instigation material are stored in the revenue protection database to support on-going and future investigations.

In summary, the following are the main functions of the revenue protection software:

- Lead generation
  - Lists
  - Layer maps
  - Account detail
- Investigation tracking
- Reporting
- Database of Investigations

Results

As of May 2014, the revenue detection software was operational for one year. Thousands of leads have been generated with many of them leading to work orders for field technicians to investigate meter tampering and potential theft. The software has directly benefitted SMUD by ensuring employee and public safety through quick response to indications of meter tampering that could result in an unsafe condition associated with the meter and service installation of a customer. SMUD has been and will continue to prioritize investigations with the highest probability of theft and the greatest chance of collecting back payments. In addition, the software optimizes the screening and investigation process so that resources, such as fuel and labor, are utilized efficiently.

The benefits to the customers are improved neighborhood and personal safety. In addition, the reduced revenue loss lessens the impacts that could lead to a future rate increase for all customers.

Table 4 shows the impacts of the revenue protection software on both the amount billed and collected. In the first twelve months following the installation of the software, SMUD has billed 15.5 million additional kWh due to theft detection and investigation. This equates to more than $3 million in additional billing. The amount billed and collected has increased two- to threefold with the addition of the revenue protection software.

Table 4 – Summary of Monetary Effects of the Revenue Protection Software

	12 Months Prior to Detectent	12 Months After Detectent
$ Billed	$1.36M	$3.11M
$ Collected	$334k	$723k

SMUD has benefited from the technology and reduced revenue loss over the first year of operations. Trends in the amounts billed and collected from theft cases are evident. Secondarily, the measures of success of the algorithms are more qualitative than quantitative. This is largely due to the methodology SMUD uses to track various types of leads. SMUD's configuration of the software assigns a new order each time an investigation is undertaken even if the investigation is a follow-up investigation issue to the same premises. This makes it difficult to determine the success rate of the theft leads being generated; however, successful collection of back payments from theft illustrates the effectiveness of the software solution to detect and prioritize theft leads.

Lessons Learned and Key Recommendations

A number of lessons were learned by SMUD during 2013-2014 on use of the detection software:

- Some customization of the software may be needed so that it works well with utility processes, and increases the efficiency of the workforce. For example, at the beginning of the project, SMUD adjusted the standard software so that it operated efficiently with the SMUD systems and provided reports that closely matched the ones that SMUD employees were accustomed to working with. Also, algorithms were adjusted to increase the probability that each lead was a case of theft. At a minimum, SMUD recommends that a utility implementing a revenue protection data analytics program includes the following types of algorithms: kWh drop, meter set, minimum kWh usage, zero use, frequent tamper, load factor, meter capacity, max monthly usage, reverse power, high seasonal load, load factor deviation, similar customer comparison, and other demographic comparison algorithms.

- Purge non-essential data periodically to alleviate huge data storage. The data entered into the database daily provides a wealth of information but can be burdensome to store over time. The large set of data can be utilized to reduce the average estimated revenue loss to theft of 0.5%-1% that electric utilities experience each year. As the amount of data grows over time, SMUD has decided and would recommend purging non-essential data periodically. For SMUD, data is purged after two years. Essential data, such as investigation records, algorithm performance indices, and other important case data, is stored permanently.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass..

Together . . . Shaping the Future of Electricity

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com