IBM Global Business Services
White Paper

Advanced Approaches to Addressing Power Theft

By Adam Gersting and James Strapp

IBM

With the utility grid and its assets becoming more instrumented and interconnected, the long-standing challenge of power theft is being brought to light and becoming more addressable. Power theft – whether through tampering, diversion or other means – is of great concern for utility companies because it has a considerable impact on their bottom lines. Theft is also an area of concern from the safety, responsibility, and regulatory perspectives.

Utilities have faced power theft-related challenges of various types over the years, ranging from customer name-switching schemes to elaborate bypass systems. While certain types of theft appear to be increasing in North America, the larger change in the industry is the availability of new, more effective technologies and data analytics approaches to identifying instances of theft. The large-scale implementation of smart meters and smart grid technologies in North America has increased instrumentation that enables much richer data about energy use and tampering at the customer service point and along the network.

The application of advanced analytics techniques to this newly available data is expected to result in much greater efficacy of potential theft detection and be more cost-effective than previous, traditional techniques. IBM has defined advanced candidate detection approaches and overall framework for addressing power theft in today's utility environment.

Theft Areas and Impacts

Two of the major areas of power theft are meter-related tampering and diversion.

Meter-related tampering includes adjustment of the meter, replacing it with a mechanical meter, bypassing or jumping the reading portion, and other simple or more sophisticated tampering techniques.

Diversion is the practice of tapping into power sources prior to the power reaching the meter, so that the meter is not incremented based on this use. Smart meters and other instrumented assets provide more data, more rapidly, to help indicate cases of potential diversion.

The instrumentation of the meter and meter environment provides for the next wave of theft detection in the electrical world, in much the same way that video security cameras provided it for the physical world.

There are significant impacts – collectively – related to these two areas theft.

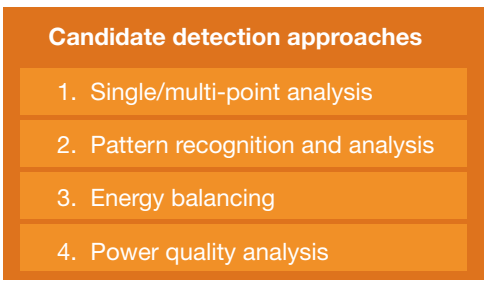
- **Revenue loss:** While not widely documented, it is thought that previous estimates of three to five percent revenue loss due to power theft in North America may be underestimated. Large-scale diversion of power in North America thought to be taking place by marijuana growing operations is another area of significant financial impact. One recent study estimates that the total annual value of missed billing revenue alone – in a single geography – due to marijuana growing operations to be in excess of $100 million dollars. That is nearly four percent of the utility's total domestic revenues lost to theft from marijuana growing operations alone.[1]
- **Damage:** With tampering and diversion, changes to the physical electrical infrastructure can potentially cause damage to the lines transformers and other assets.
- **Safety:** With modification to lines and assets – and with potential criminal activity taking place – there are safety implications for workers and the public.
- **Societal implications:** As the mechanisms and data to detect theft become more commonplace, there are societal impacts and potential obligations to address theft. Increasingly, regulators and the public expect that action be taken to reduce revenue loss versus factoring it into ratepayer increases. Taking action is also in keeping with the general and increasing public view of the need to conserve.

Advanced Detection and Analysis: Approaches and Challenges

In the past, utilities were dependent on limited information, and costly and sometimes dangerous approaches to identify theft. Reports from meter readers and other field workers were the only way to identify and report on tampered meters and diversions. Revenue protection departments relied on minimal consumption data and typically had to react long after the theft took place to recover unpaid revenue.

Now, there are a number of analytics approaches that can be taken to identify potential theft. Four categories of approaches are illustrated in the figure below and are described in turn. It is important to keep in mind that the outcome of all of these approaches is identification of cases for additional investigation and consideration, versus definitive indication of wrongdoing.

Detection and Analysis Approaches

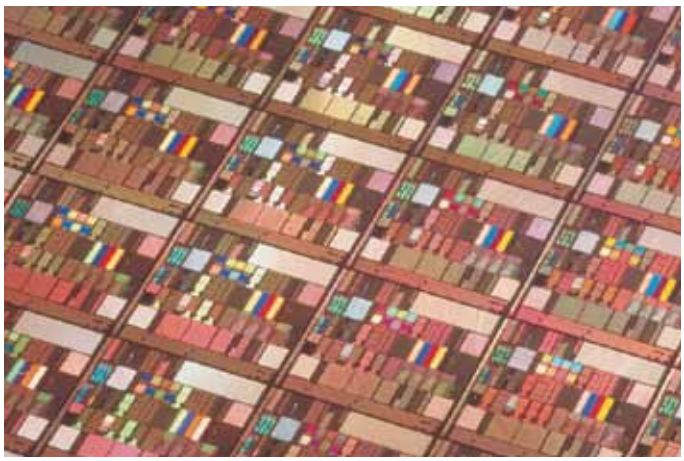


1 *"The Increasing Problem of Electrical Consumption in Indoor Marijuana Grow Operations in British Columbia"*. By Jordan Diplock and Darryl Plecas. University of Fraser Valley. Published on vancouversun.com.

- **Single / Multi-point Analysis:** This category involves looking at one or more data points at a given time to identify indicators or signals. As a single point analysis example, this includes capturing and examining meter event data points. Multi-point analysis includes the recognition that the indicator is a collection or sequence of data points (for example, power off / zero voltage flag followed by a negative flow flag).
- **Pattern Recognition and Analysis:** There are "straight" patterns that could indicate irregularity. For example, a pattern of 12 hours without power usage, followed by 12 hours of very high usage could indicate an unusual situation. Changes in patterns are also indicators: power consumption of one premise dropping significantly below previous levels while neighboring units remain the same; or a given inspector identifying fewer instances of theft in an area while others continue to identify previous amounts.
- **Energy Balancing:** Energy balancing is a form of "checks and balances" of the load across a portion of the network to identify unexpected losses. Feeder meters or transformer meters can measure aggregate load at a known point in the network. An unexpected delta between the aggregate load at the known point and the smart meter is in indication of unexpected loss along that portion of the line, potentially through diversion.
- **Power Quality Analysis:** Analysis of voltage, for example, can be used to identify potential power theft. Voltage analysis involves a comparison of the expected voltage drop at a load point against the actual voltage drop. The voltage of a network – with a configuration at a given point in time – drops in a known and predictable fashion. If the voltage drop is larger than expected, then this may be an indicator to investigate further.

With these approaches, there are a number of challenges to be considered. These and other approaches, along with the applicable considerations, should be examined by organizations as they take additional steps related to power theft and revenue attainment.

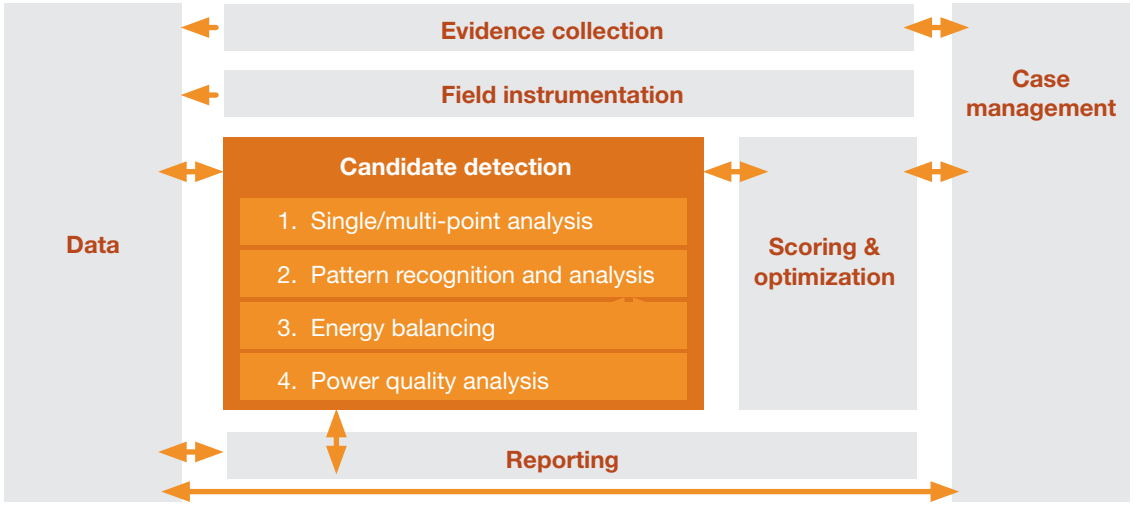
- **Data quality related to the state of the network:** Data needs to be captured and managed related to the environment in certain configurations. This, for example, will allow one to understand the degree to which the voltage drop is unexpected with the given network configurations.
- **Accuracy of sensors:** The accuracy of the assets – such as meters and feeder sensors – needs to be understood. The greater the accuracy of the meter relative to the deviation from the expected values, the more helpful and actionable the indicator will be.
- **Equipment required to obtain data:** Equipment and instrumentation is needed provide sensor data for capture and analysis. Additional investments required need to be balanced with the benefit obtained through revenue attainment and other areas.
- **Societal and privacy considerations:** As it relates to management and access of data, there are security and privacy requirements by law and expectations by society which differ between jurisdictions. Such requirements may influence the data that one can access for detecting and addressing potential anomalies.



Enabling Solution

These detection approaches and challenges should be addressed as part of an overall, end-to end revenue attainment process versus via point actions. The IBM Revenue Attainment Solution Framework for Power Theft supports an overall end-to-end process view. The seven elements of this Solution Framework are illustrated in the below figure and described in turn.

IBM Revenue Attainment Solution Framework for Power Theft



1. Field Instrumentation: The first aspect of the overall Solution Framework is the instrumentation in the field. This includes installation of smart meters, feeder meters, transformer meters, or SCADA devices.

2. Data Environment: The data environment supports the storage and management of data from field instrumentation, enterprise system data, GIS data, external weather, and law enforcement data, and actual case management data such as photographs, models, and actual versus expected comparative results.

3. Candidate Detection: This element encompasses detection approaches such as Pattern Recognition and Analysis and Energy Balancing as previously described.

4. Reporting: Performance and other reporting provide insights into the data itself, and the candidate detection results.

5. Scoring and Optimization: This element takes the results of detection and applies consolidated scoring, and optimization of dispatch of investigative crews.

6. Case Management: Formal case management approaches and techniques are applied to those items detected and determined to be a priority. This includes the needed case workflow, management of workforce dispatch to take additional steps, and any interactions with law enforcement, customers and other stakeholders.

7. Evidence Collection: This element follows from Case Management, involves investigative tools results and workforces, and coordination of the workforces and parties involved.

Through these seven inter-related elements of the Solution Framework, an overall and ongoing process of revenue assurance and theft detection can be enabled. IBM provides assets, software, services and hardware in support of this Framework.

Steps Organizations Can Take Today

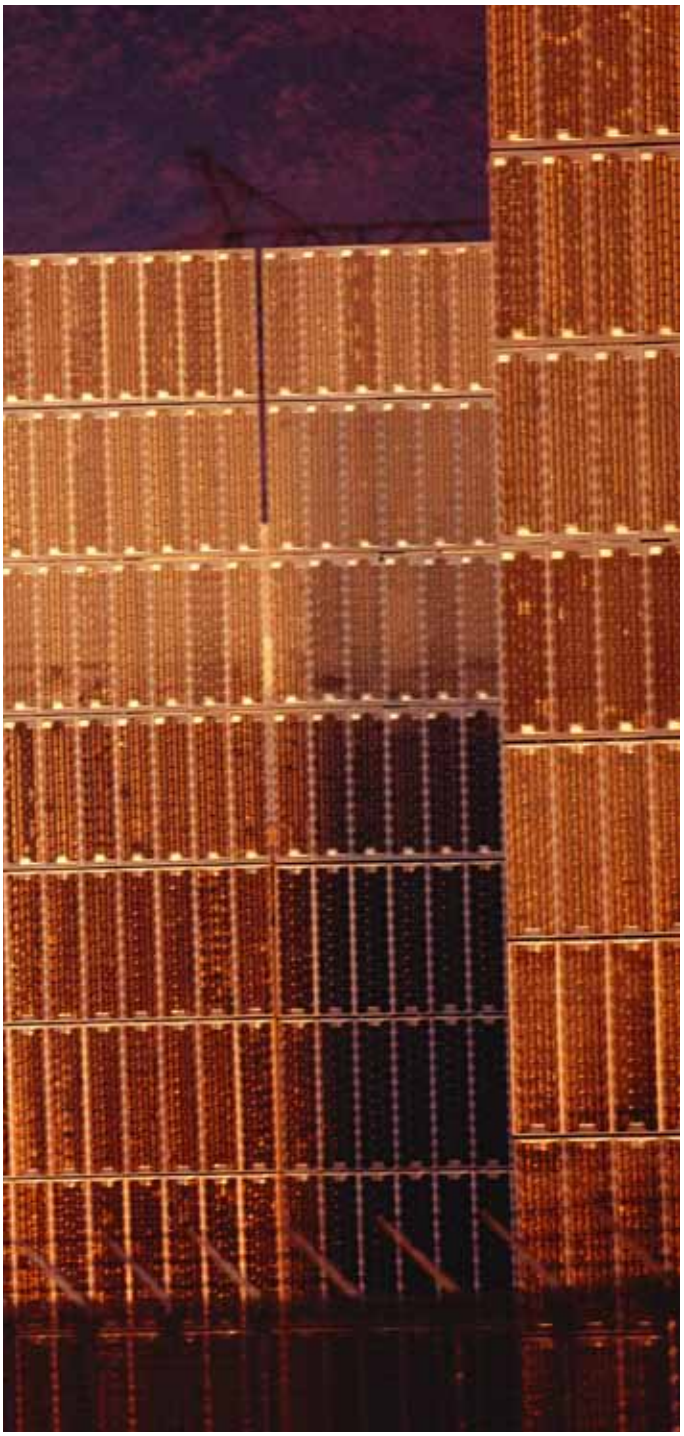
In tandem with establishing the proper solution environment for a given organization, there are steps that can be taken today to address potential power theft and revenue attainment.

1. Address the data environment. This includes understanding the data being captured today, ensuring that it is managed and of good quality.

2. Establish simple reports and alerts based on currently available data to begin to detect potential issues. Based on the quality of data that is available today, with enabling tools, initial models can be developed and applied to identify indicators of potential theft. Accurate identification of initial areas of investigation can enable effective truck rolls to further investigation and understanding.

3. Establish and plan the applicable elements of a Solution Framework. Together, the proper solution environment and detection approaches and revenue assurance process can be planned and implemented to address the challenges and abide by the regulations of a given jurisdiction.

In summary, power theft is a significant challenge in the utilities industry today in North America and beyond. With the growth of instrumentation, data management and the application of process and analytical models, there is opportunity for significant revenue attainment and additional benefits through enablement of an end-to-end process.



For more information

To learn more about smarter solutions for smarter energy, visit **ibm.com/**energy.

About the authors

Adam Gersting is a Partner leading IBM's focus on enabling Energy and Utilities companies through Business Analytics and Optimization. James Strapp is a Partner and the leader of IBM's Global Center of Competency for Energy and Utilities.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
August 2011

GBW03153-USEN-00