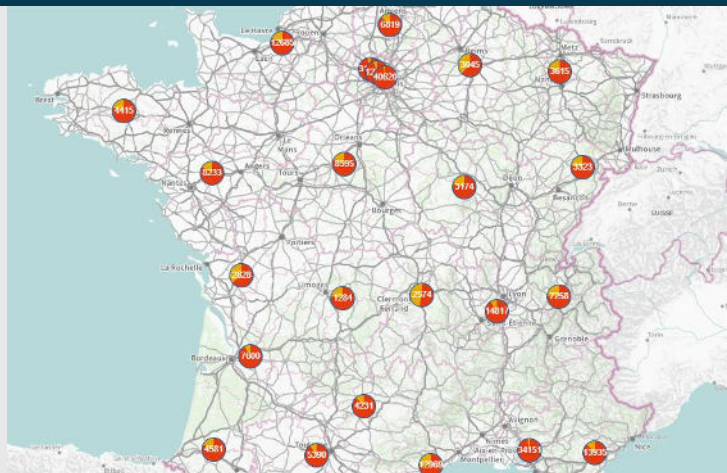


SUCCESS CASE 22.2025

Detection and Reduction of Non-Technical Losses

ALGORITHMS TO ENHANCE NETWORK SECURITY



THE CHALLENGE

Since the introduction of the Linky smart meter in 2014, overall network losses in France have decreased by 1 TWh by the end of 2021. On the network, **non-technical losses (NTL)** refer to the energy consumed but not measured or billed. Despite the reduction of NTLs achieved with the smart meters, Enedis has recorded an **increase in fraud linked to the rise in electricity prices**. In response to this issue, Enedis has set up a fraud detection system based on Linky meter data and characteristic drops in consumption. Since then, frauds have evolved from isolated incidents to more organised and sophisticated schemes. Thus, new methods must be developed to adapt to the fraudsters' evolving techniques and to detect new cases of potential fraud.

NTL detection schemes rely on data crunching across large datasets (measurements, network descriptions, etc.) and anomaly detection algorithms. These methods have made fraud detection easier and faster for Enedis.

THE SOLUTION

Enedis has developed and industrially implemented various **fraud detection algorithms** based on the analysis of **consumption data from smart meters**, cross-referenced with other customer characteristics. Currently, the French DSO is working on improving these algorithms through three types of innovative solutions:

- **Segmentation through sector-specific activity analysis.**
- **Data cross-referencing with external, non-energy datasets.**
- **Clustering algorithms**, which enable the identification of typical power consumption patterns or reference profiles. When a new data sample deviates significantly from these established patterns, it may indicate potential fraud.

Note: To respect confidentiality and proprietary processes, Enedis cannot elaborate further on the employed detection methods.



Detection of sudden consumption drops.

MAIN ACHIEVEMENTS

On the technical side, the algorithms have been optimised to reduce false positives (incorrect alerts) and to improve the prioritisation of alerts. This prioritisation enhances operational efficiency and shortens response times. Currently, Enedis' new data-driven approach significantly improves the accuracy of fraud detection, with some of the new algorithms achieving a **reliability rate up to 80%**. Overall, Enedis is transitioning towards a more **efficient and data-driven fraud detection model**, where the smart use of digital tools enhances both the performance and resilience of the electricity network.

KEY SUCCESS FACTORS

Enedis' digital fraud detection tools rely on several key success factors. The first is the **performance of the algorithms**, which can be assessed through metrics such as the accuracy of fraud suspicions, the reduction in analysis time, and the frequency of algorithm updates to adapt to new fraud techniques. Another key success factor is the **availability and effective use of data**. Furthermore, the **clarity and intuitiveness** of how the information is presented are essential for ensuring that detection outputs are actionable. Finally, the **strong involvement of business teams**, who maintain constant contact with field operations, plays a crucial role in transforming business insights into concrete detection algorithms.

