STAYING AHEAD OF PIPELINE THIEVES

Harry Smith, Sales and Senior Research Engineer, Atmos International, argues that theft detection hardware matters more than ever for pipeline operators.

Pipeline theft remains a serious global issue, with an estimated US$133 billion in crude oil and refined products lost annually to theft or adulteration worldwide.[1] While attention should be given to advanced software, the foundation of any effective detection system still lies in its hardware. Without high-resolution, real-time pressure and flow monitoring, particularly in hard to reach locations, many thefts will go unnoticed or unverified.

Figure 1. Metal spike embedded in a pipeline wall. These methods pose a high risk of leakage and environmental damage.

Figure 2. A tapping point discovered in Italy.

Figure 3. Motorcycle battery powering the circuit.

From 'slash and grab' to concealed tapping points

In some regions, particularly Latin America and Sub-Saharan Africa, theft remains crude and opportunistic. The 'slash and grab' method involves using tools such as metal spikes or grinders to breach a pipeline (Figure 1), often causing immediate leaks and posing significant safety risks. These are typically carried out to access small amounts of product quickly, sometimes for domestic use, and often result in poor sealing and structural damage.[2]

More refined techniques involve clamps and welded tapping points. These are frequently found on pipelines up to 20 in. in diameter and are associated with organised criminal groups seeking to remain undetected. Thieves' hardware can often be designed to allow slow valve openings and controlled withdrawals that stay below metering thresholds, reducing pressure transients and avoiding alarms. In Italy, a tapping point was detected by Atmos' technology only 147 m from its actual location (Figure 2), confirming the precision now achievable with modern theft detection systems.[2]

The rise of remote valves, tunnels, and night-time operations

Thieves are also becoming more technologically advanced. In Costa Rica for example, tapping points have been connected to relays powered by motorcycle batteries and remotely operated (Figure 3), significantly reducing the risk of on-site detection.[2] These methods blur the lines between physical and digital intrusion, with electronics enabling fast, low-profile product removal from pipelines.

Tunnel-based theft has also emerged in regions such as India and Costa Rica. In one case, a 40 m tunnel was used to extract fuel covertly, with the product routed to a private facility 300 m from the tapping point (Figure 4).[3] Despite the complexity, Atmos' detection systems identified the event with a sensitivity level of 0.2%, demonstrating how properly calibrated hardware can detect even long-distance, low-rate thefts.

Night-time theft is an increasingly common strategy, often involving skilled engineers, thermal imaging, and professional-grade welding kits. In one case in the Democratic Republic of Congo, battery-operated pressure sensors detected a theft event at approximately 00:30 with a +/- 150 m location error.[3] In the UK, repeated alarms triggered over five nights led to the discovery of a tapping point and confirmed the importance of continuous overnight monitoring, even during shut-in conditions.

The role of high-resolution detection hardware

Effective detection depends on more than simply having sensors in the right places. It requires sensors that can capture high frequency signals and detect subtle anomalies in real time. Atmos Eclipse is a non-intrusive device capable of acquiring flow, pressure, and temperature data even in environments without power or telecom infrastructure. It is designed for high-consequence areas where quick detection is critical.

Figure 4. The tunnel used by thieves in Costa Rica (top left) for their tapping point route (bottom left) which led to storage containers at a private property 300 m from the tapping point (right).

Atmos Odin complements this by offering a portable, battery-powered pressure logging solution capable of collecting data at 60 Hz for up to 40 days. Its low-profile design makes it difficult for thieves to detect and tamper with. Both systems have been instrumental in theft detection on legacy networks in Africa, where limited SCADA coverage made conventional monitoring impractical. Using these tools, engineers were able to locate multiple theft points with exceptional accuracy, even in remote or heavily forested terrain.[4]

Smart software for layered detection

Hardware provides the raw visibility, but software enables interpretation. Atmos combines negative pressure wave (NPW) and intelligent flow balance methods to identify a broad spectrum of theft scenarios. The NPW technique identifies the characteristic pressure drops caused by valve openings or closings at tapping points and offers near real-time detection with location triangulation. This method is especially effective in high-pressure, dynamic conditions and offers dual opportunities to detect both the start and stop of a theft event.

Intelligent flow balance, on the other hand, looks for discrepancies in volume across a pipeline segment. It accounts for operational conditions such as transients and packing/unpacking, providing an effective method for identifying slow withdrawals that fall below NPW sensitivity. Enhanced algorithms recently introduced by Atmos allow the system to detect changes between historical flow difference and real-time patterns, making it possible to identify theft rates as low as 0.1% of nominal flow.[2]

Human insight: offline analysis for low-flow and legacy systems

Not all thefts trigger automated alarms. In pipelines where flow variance is minimal or instrumentation has drifted, offline analysis by experienced engineers remains essential. This forensic-style review allows operators to review high-resolution datasets from both portable and fixed sensors, overlay algorithms, and compare historical operating conditions.

In Costa Rica, engineers used analog pressure data and three comprehensive algorithms to map a suspected theft event in 3D. This resulted in a confirmed theft alarm and law enforcement intercepting 12 containers of stolen fuel before they were moved.[5] In Belgium, engineers detected over a dozen thefts by analysing data that wasn't visible to the SCADA system. In one instance, the tapping point was located with an accuracy of 40 m across a 100 km network, negating the need for an expensive pig run.[2]

Integrated strategies for better outcomes

Atmos recommends a multilayered approach to theft detection. High quality hardware ensures high frequency, high resolution data acquisition. Smart software applies pressure wave detection, flow balance modelling and algorithmic filtering. Finally, human analysis bridges the gap, particularly in complex, low flow or legacy environments.

Atmos' experience across the world shows that theft detection cannot be solved with a single method. Different pipelines, different terrains and different criminal tactics require a modular but integrated strategy. In all cases, the combination of hardware, software and people has proven to be the most effective way to detect and respond to theft events.

Detect fast, locate precisely, adapt continuously

Theft techniques are becoming more organised, better concealed and technologically enabled. Operators need to match that evolution with theft detection systems that combine speed, precision and adaptability. Whether it's tunnel theft in Latin America or small-volume overnight siphoning in the UK, the solution begins with sensitive, real-time hardware, and supported by smart algorithms and expert review.

Investing in a high-resolution, multimodal detection system isn't just a defensive move, it's an operational necessity. With the right strategy, pipeline operators can reduce false positives, respond quickly and protect infrastructure and public safety in an increasingly uncertain world. WP

References

1. https://oilmanmagazine.com/article/oil-theft-a-frightening-international-perspective
2. https://www.atmosi.com/en/resources/technical-papers/ongoing-pipeline-theft-challenges-and-the-importance-of-hardware-for-theft-detection/
3. https://timesofindia.indiatimes.com/city/delhi/40-metre-tunnel-leads-police-to-underground-oil-theft-nexus/articleshow/104229398.cms
4. https://www.atmosi.com/en/resources/case-studies/sep-congo-opt-for-atmos-theft-net-as-an-effective-theft-detection-solution-for-its-legacy-pipelines
5. https://insightcrime.org/news/brief/costa-rica-oil-theft-record-high/