

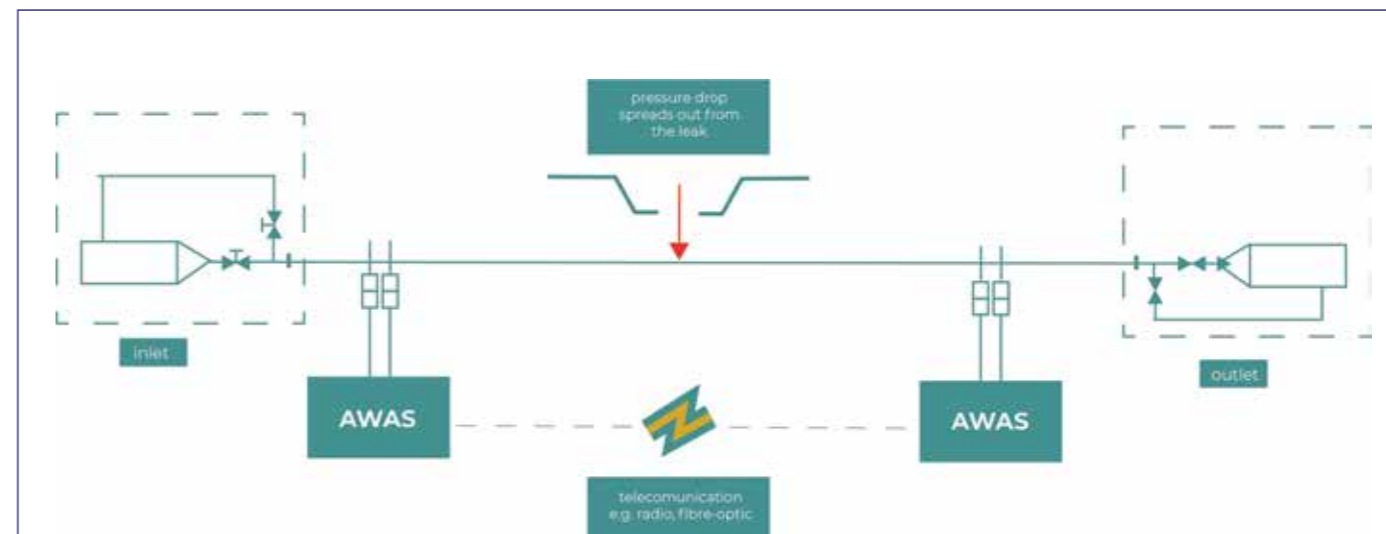
PROTECTING PIPELINES



Pipeline thefts are a global challenge. Harry Smith explains how smart technology can help to prevent them

Pipeline theft is a serious global problem and one that has been on the rise for the past few years. In terms of pipeline integrity, thefts are one of the largest risks that can be hard to prevent without strategic focus. The events in Mexico earlier this year demonstrated the risks thieves will take and the ultimate price some people will suffer as a result. However, pipeline theft is not restricted to Central and Latin America but extends worldwide, with occurrences in Nigeria, Indonesia and

China. In Europe, pipeline thefts have also risen, with incidences found in Eastern and Southern Europe and in the UK. Theft was designated so serious in the UK that the National Crime Agency became involved. The challenge to operators and law enforcement is that there is no single cause of thefts – a wide range of factors including social, economic, political and legal apply. Although some thefts are clearly organised for criminal gain, many are driven by often the most basic of needs, such as obtaining fuel for heating



ABOVE: Overview of the Negative Pressure Wave System with Atmos Wave Acquisition System (AWAS) units
LEFT: Thieves use a double tap to try and outwit pipeline operators. By using double taps, thieves try to 'fool' the system that product is not being removed from the pipeline

and cooking. It can be these small, *ad hoc* thefts that can have the worst consequences.

THE SOPHISTICATED THIEF

Thieves are becoming more sophisticated and organised, using specialist equipment such as commercial-grade welding machines, calibrated measuring instruments, night vision goggles and vans with modified suspension or exit holes built into the floor of the vehicles. Thieves will also sample product to decide if it is the right product to steal.

From a technical perspective thieves will deploy several tactics, including: pre-install the tapping point, hose,

associated valves and equipment before a pipeline is commissioned; select remote and well-hidden sites such as abandoned buildings such as farms and old factories; bury and cover the hosepipe and all other devices underground. Other tactics include opening the tapping point valves very slowly to generate small pressure change over a long time (known as the patient thieves), and maintaining the theft rate below flow meter repeatability level, e.g. 0.1% of pipeline throughput.

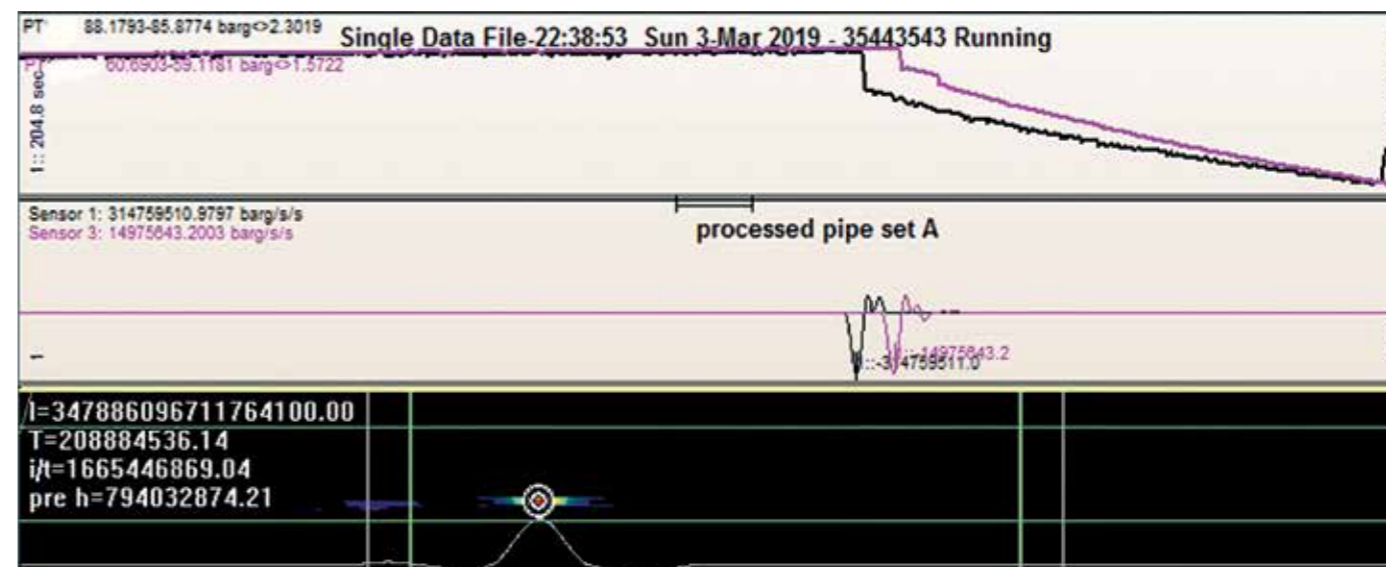
Adding to the challenging in detecting thieves is that they often carry out the activities at night. They frequently steal small volumes each time or inject water into the pipeline while

taking oil out. It's not uncommon for thieves to conduct thefts at multiple locations along the same pipeline.

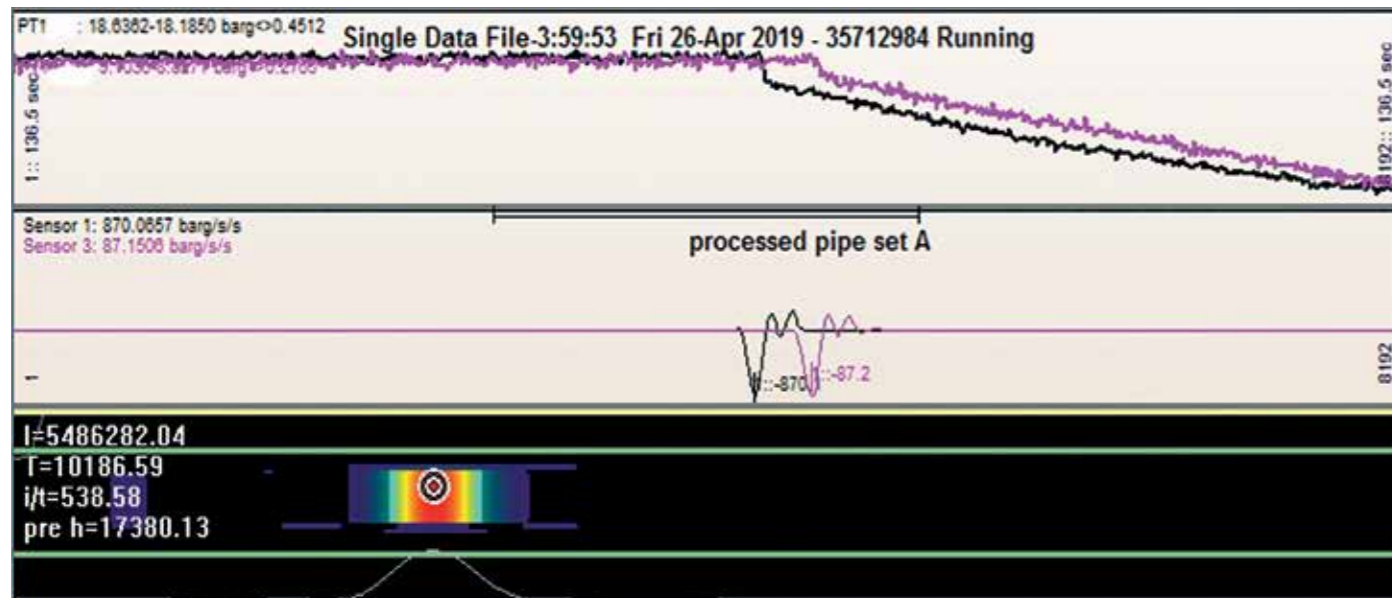
Thieves increasingly use dangerous techniques, including angle grinding and plastic equipment. At worst, thieves have driven stakes into pipelines and used rags to reduce the flow out of the pipeline.

All of these different tactics make it difficult for pipeline companies to detect and locate thefts quickly and accurately. Although leak detection methods have previously been used for theft detection, a more focused approach is required.

The application of the negative pressure wave, statistical volume balance



An example of a theft event generating 1.5 bar pressure drop



An example of a theft event generating 0.4 bar pressure drop only

methods is extremely beneficial for theft detection, with the use of offline analysis and further instrumentation.

As every pipeline is different, a 'one size fits all' approach is not suitable, however: each technology has its advantages and can often be combined to provide an integrated approach. Furthermore, non-intrusive pressure sensors with remote radio and cellular communications and battery-powered data logging can provide additional accuracy to support GPS location and offline analysis.

THEFT DETECTION SOLUTIONS

Avoiding detection is a key target when thieves are going to commence an operation to extract the product from a pipeline. This approach differs from pipeline leaks in several ways: a small amount of product is stolen (ranging from 10 to 3,000 litres); theft flow rate can be less than 0.1%; theft events last for less than one hour usually although occasionally a theft continues unchecked; and the changes in pressure are very small when the tapping point is opened/closed at the end of a long hosepipe.

With these unique characteristics the main requirements of theft detection are: sensitivity (detecting the small product withdrawal); accuracy (locating the tapping point as accurately as possible); and response time (detecting the product withdrawals as quickly as possible).

Different leak detection technologies can be adapted to meet the above requirements. The main theft detection

options are negative pressure wave, statistical volume balance and theft service approach.

NEGATIVE PRESSURE WAVE

This technology relies on high-speed analogue pressure sensor readings to identify whether a leak/theft has occurred on the pipeline. The system acquires and analyses the pressure data at a frequency much higher than the typical five-second SCADA rate, capturing data at 60 samples a second. Specialised equipment is thus needed to acquire data at such high frequency.

The main advantages of this system are: accurate leak location within metres of the actual location; short detection time for all leak sizes; and high sensitivity provided through the 60hz sample rate. These are the key features in effectively detecting theft events in all operational conditions.

STATISTICAL VOLUME BALANCE

This type of leak detection technology relies on the pressure and flow measurements taken from a pipeline. It uses the existing instrumentation and connects via existing SCADA, PLC or remote terminal unit (RTU) systems. This system monitors the difference between the inlet and outlet flow corrected by the inventory change. This is also referred to as the "corrected flow difference" to determine whether the pipeline is in a leak condition.

The statistical hypothesis testing method is known as the sequential

probability ratio test (SPRT). It is applied to the corrected flow difference to decide if the probability of a leak has increased.

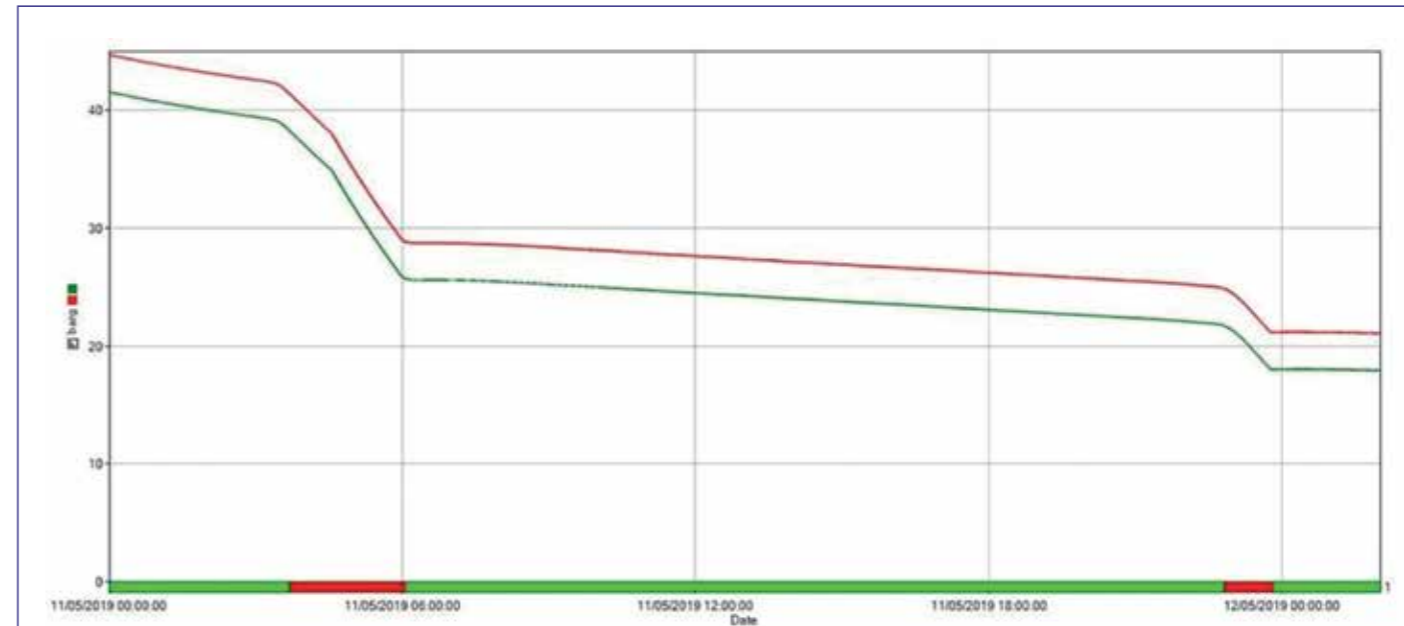
The main advantages of this system are a low false alarm rate, the ability to detect leaks under steady-state, transient and shut-in conditions, and accurate leak size estimate. Leak location accuracy is improved through higher data sample rates.

Since the theft rate is usually below the flow meter accuracy and repeatability level, it is difficult for this technology to detect small thefts under running conditions unless false alarms are accepted. The system includes an additional theft module for detecting thefts during shut-in conditions to maintain reliability for both leak and theft detection. The figure on the following page shows an example of it working.

Thefts are not a constant and can fluctuate. Tapping points are often left for years. In the UK a recent tapping point was located that was likely installed as far back as 2015 and left dormant until earlier this year.

When the volume of thefts along a pipeline reduce, it becomes necessary to lower the minimum leak size to be detected. However, in doing this, it can result in increased false alarms as the identified flow and pressure are mostly below the instrument repeatability and process noise level.

An offline service can be offered to pipeline firms. Combining technology with an offline service can provide



An additional module detects thefts during shut-in conditions

improved leak location accuracy and sensitivity without unnecessary false alarms.

Deployment of portable and fixed hardware with software solutions allows offline data analysis by an experienced engineer. Through this service, an engineer's ability to interpret data helps theft to be located down to a few metres, using pressure data collected at 60Hz sample rate and sent to a central location via a cloud-based service.

The data is then filtered to present only the relevant information required and the locations of the illicit tapping points

are reported to the pipeline operators.

It is well documented that online leak and theft detection systems must find a balance between sensitivity and false alarms. Some leak detection systems can detect leaks as small as 0.5% of nominal flow-rate without the issue of false alarms. However, this becomes an issue as most theft events are less than 0.3% of the nominal flow-rate. The capability to analyse the data offline has allowed the location and detection of theft to within 5m for thefts as small as 0.1% of the nominal flow-rate in static and running conditions.

Combining a detected theft service with a single or multiple online leak detection system allows for a more reliable leak detection system with the ability to effectively deal with all types of theft events. In the past two years, this combination of negative pressure wave, statistical volume balance and offline analysis has enabled one supplier to successfully detect and locate over 300 tapping points for its clients. ●

Harry Smith is with Atmos International. www.atmosi.com

EXAMPLES OF THEFTS DETECTED

The technologies discussed in this paper have been applied to theft detection on pipelines all over the world. The use of a dedicated theft service and leak detection systems has led to the detection and location of many illicit tapping points, such as an oil withdrawal through a 12mm hole that was attached to a 1.5km long underground hosepipe in Europe.

The theft detection systems have even detected the theft of

samples (taken before a full product withdrawal begins) between 10 and 20 litres of product from some pipelines during static conditions.

In the space of four months in 2019, two theft events were detected in the UK by both statistical volume balance and negative pressure wave systems. Both theft events had a leak location error of less than 50m. The thefts were found on a multi-product pipeline with varying

diameters of 6 to 14in with a total network length of 650km. The thieves stole quite small quantities of product during both events, around a total of 4m³ was removed before the tapping point was located. These events were detected in minutes of the tapping point being opened by the online leak detection systems but did take several days to locate due to the thieves hiding their activity very well. ●