Pipeline Evaluation Network for Protection from Third-Party Intrusion

M.F. Byl, M.B. Frish, R.T. Wainner, B.D. Green
Physical Sciences Inc, Andover, MA 01810

D. Davis, E. Kruft, K. Cowan
American Innovations, Austin, TX

G. Janega, D. D'Zurko
NYSEARCH/Northeast Gas Association, Parsippany, NJ

ABSTRACT

Third-party intrusion, i.e. unauthorized excavation that accidentally strikes and damages or ruptures a pipeline, is a primary cause of loss to gas pipeline integrity. The NYSEARCH/Northeast Gas Association, American Innovations and Physical Sciences Inc. are jointly developing an autonomous distributed sensor alarm and notification system that provides pipeline operators with a real-time warning of unauthorized right-of-way encroachment and excavation activity near a pipeline. Early warning provides pipeline owners the ability to respond to an intrusion in time to prevent pipeline damage, and preclude incurring the additional cost and risk of repairs. This intruder warning system consists of a network of discrete and unattended, geographically-distributed underground seismic sensor packages deployed along a pipeline right of way. Each sensor package continually processes seismic signals to distinguish threats or abnormal events from benign sounds. When activity is detected, several sensors acting collectively classify the activity as "safe" or a "pipeline threat". "Threat" events activate immediate notifications to pipeline operators via a wireless remote monitoring system. Notifications are communicated via text, email, and/or voice notification. This paper will present an overview of the intrusion warning system, including descriptions of the system hardware, performance specifications, operations, field test results and current development status.

Keywords: damage prevention, pipeline integrity, intrusion, excavation, remote monitoring

INTRODUCTION

A widely diverse and critical pipeline infrastructure system delivers gas and oil throughout the US with a high standard of safety. Third-party damage, i.e. unauthorized excavation that accidentally strikes and damages or ruptures a pipeline, is one of the leading causes of compromise to pipeline safety. Nationwide, the number of third party damage incidents reported for 2005 on gas pipelines was over 25,000; of that amount, over 30% were due to a failure of the operator to contact the “One-Call” notification center to properly locate the pipe before digging. Close to 20% of pipeline damage results from ‘excavator practices not sufficient’. Third party excavation damage to transmission pipelines has
resulted in over $500 million in property damage and resulted in 150 deaths between 1990 and 2009.\textsuperscript{1} Clearly, if gas operators had systems to detect and notify of encroachment or insufficient practices near their lines, they would take action to avoid damage incidents.

The pipeline intrusion warning system described herein addresses the need for pipeline protection by quickly warning pipeline owners and operators of unauthorized excavation within a pipeline right-of-way. Benefits of the intrusion warning system include: 1) increased safety, 2) reduced number of hits to pipe, 3) reduced system downtime and customer disruption, 4) reduced cost to customers and industry alike to address third party damage hits, 5) overall improvement in communication between the equipment operator and the utility operator, and 6) longer life and improved integrity of the pipeline infrastructure.

**DESCRIPTION OF THE SYSTEM**

The intruder warning system consists of an underground network of discrete and unattended, geographically-distributed smart sensor packages deployed around (but not in contact with) an underground pipeline or similar protected area (Figure 1). It uses low frequency (5 to 100 Hz) seismic/acoustic sensors to proactively detect and warn of right-of-way encroachment and unauthorized digging. The sensors continually listen to the environment. The firmware in each sensor package processes received signals to distinguish threats or abnormal events from benign sounds. The system capitalizes upon the unique characteristic seismic features of excavation equipment to distinguish threats from ambient noise. When any individual sensor detects an abnormal event, it activates its communications module and transmits information via radio within its local network. Using data from a minimum of three sensor nodes, the networked sensors collectively localize the event. If a threat is localized within the protected area and meets other criteria, the system transmits an alarm to an operations center.

![Seismic sensors and configuration of array installation.](image)

Each sensor consists of a low frequency seismic sensor packaged with a low-noise pre-amplifier, a digital signal processor (DSP), a power and communication adapter (PCA), and a wireless radio for communication between the individual sensor nodes and the network interface box (NIB). The current generation of the sensor node is packaged into a below ground unit consisting of the seismic sensor, pre-amp, and DSP (Figure 2.A) and an above ground unit containing the PCA, wireless radio, and the radio antennae (Figure 2.B). The sensor node is powered by a 12 V battery, which in the prototype
The system shown is capable of powering the sensor node for 10 days when the sensor is continuously streaming data back to the NIB. This same battery would be capable of powering the sensor node for up to 5 years when both data compression (radio duty cycle reduced by a factor of 10) and full sleep functionality are enabled (the sensor is expected to be in full sleep mode 90% of the time and in a low power state 9% of the time). The current generation of the network interface box (shown in Figure 3) consists of three components: a pole mounted antenna plus radio module, a laptop PC running the classification, localization, and alarm algorithms, and a communications module for client notification (e.g., American Innovations Bullhorn system, not shown).

**SYSTEM OPERATION**

The concept of operations (CONOPS) of the pipeline protection network is that seismic sensors are deployed along the right-of-way at a minimum spacing of 1 sensor per 100m of pipeline. The sensors are buried 45-60 cm below the surface with only an antenna for wireless communication located above ground. Individual sensors are grouped into local networks. Each network comprises approximately 10 sensor nodes: the actual number is dependent on the site-specific maximum range and bandwidth of the wireless transceivers. A single network interface box supports each wireless sensor network and the client notification module.
The sensor nodes have three operational states:

1. **Sleep**: Only the analog electronics and analog wake-up filter are in an active state (<10 mW).
2. **Low Power**: The sensor DSP and analog electronics are active but the radio is not powered (10’s mW).
3. **Full Power**: All elements are powered and active (~1 W).

The sensors are expected to be in the sleep state greater than 90% of the time, the low power state no more than 9% of the time, and the full power state no more than 1% of the time.

Once the system has been installed, the sensors operate in sleep mode except for periodic system checks from the network interface box. In sleep mode, the seismic sensor continuously monitors the seismic environment. The seismic signals are processed through a variable threshold analog wake-up filter. The threshold for the wake-up filter is updated every time that the sensor is awakened by either the periodic system checks or when a non-threat event exceeds the current threshold setting. Once a sensor is awakened, the seismic data is then passed through a band-pass filter and analyzed locally. The analysis algorithms implemented and demonstrated during field testing consists of a data compression process in which features such as average signal power are extracted from the filtered seismic data. In future versions of the sensor firmware, the individual sensors will make a preliminary evaluation of the signal source type based upon the features extracted during the data compression step. If a signal is classified as a threat, the sensor transmits a warning to the network interface box which awakens all of the sensors in the local network. The awakened sensors then each transmit time synchronous samples of the compressed data back to the network interface box.

At the network interface box, a second set of algorithms extracts a set of features from the data sent back from all of the sensors in the network. An example set of features is the average signal power from each of the three loudest sensors in the network. The extracted features are then passed to the alarm algorithm. The alarm algorithms evaluate the features to localize the event and classify it as a threat or not.

![Figure 4: Schematic of the pipeline protection network CONOPS.](image)
If an event meets the threat criteria, the network sounds an alarm identifying the threat location as well as an event time. Figure 4 shows a schematic drawing of this threat identification and alarm process. The time between a threat event occurrence and a network alarm is less than 5 minutes. The CONOPS timeline is roughly:

1. First sensor awakens and evaluates a seismic event (1 minute from event start).
2. First sensor alerts the network interface box to an event and the network is awakened (1-2 minutes from event start).
3. Network collects data and performs an alarm analysis (3-5 minutes from event start).
4. Alarm (5 minutes).

SYSTEM PERFORMANCE

The pipeline protection network has undergone significant field testing during the systems development process. Field tests include:

- NYSEARCH/NGA (Johnson City, New York), 2005-2006
- Private Property adjacent to the Kansas River (Lawrence, Kansas), 2007
- BP (Cushing, Oklahoma), 2009
- Public Service Electric and Gas Company (PSE&G) (Woodbridge, New Jersey), 2009

Figure 5 shows two satellite photos of the Woodbridge, NJ site. The site was chosen for its semi-urban location and moderate to high activity levels. This allowed operators to adjust and improve acoustical algorithms that would be able to distinguish between many different types of ambient seismic noise versus potentially dangerous seismic noise. The protected right-of-way is a 200 m x 40 m rectangle located within a utility right-of-way. The right-of-way contains a high pressure natural gas line, overhead power lines, and multiple buried telecommunications cable bundles. The site is bound on the south by a freight railway line with trains passing sporadically during both the day and night (about 6 trains per day). South of the railway line are several small factories which are most active during the 5 day workweek during daylight hours. North of the site is a commercial truck yard and suburban housing. Approximately 1 mile to the east is Interstate 95. The site is along the North/South flight corridor for Newark International Airport so low flying aircraft regularly overfly the site. There is daily vehicle traffic along the dirt road through the site as maintenance vehicles regularly visit the control station which houses the network interface. During the testing, the right-of-way was mowed twice. The network interface box was located in a permanent structure 150 m North of the protected area, and six sensors were used to protect the area.

Less than one day was required to install the pipeline protection network and it remained in place for a six week period in which data was continuously recorded. After installation, the system was subjected to scheduled, known threats for an initial performance evaluation and to collect data for algorithm development. The threat surrogate used for this testing was a "jack-rabbit" tamper. During the test phase system operated autonomously except for twice weekly maintenance to measure system functionality and perform battery changes. After 1 month, the NIB algorithms were updated and re-tested. The pipeline protection system had a mean localization accuracy of 10 m (i.e. the mean error between the actual threat position and the calculated position was 10 m).

Over 27,000 events known to be non-threatening were recorded and analyzed during the field test. These included all of the regular activity at the site, including train traffic, maintenance vehicles, several thunder and rain storms, and site mowing. Of these non-threatening events, 350 (0.1%) had seismic signatures detected at individual sensors that were classified as potential excavation threats and activated the NIB’s secondary analysis of synchronous information from multiple sensors. In all cases, the NIB algorithm successfully discriminated against activating client notification alarms when appropriate. Thus, the false alarm rate due to non-threatening events was zero.
Forty-four of the events were due to machinery known to be excavation threats operating within the right-of-way. These were actual threats warranting client notification. An additional 15 events were due to similar machinery operating outside the right-of-way: pipeline operators would not be notified of these events. Of the 44 actual threats, 40 were classified correctly as threat events. Of these 40 events, 38 were properly localized as occurring within the right-of-way and activated the client notification alarm. This resulted in an 86% overall probability of threat event detection. Of the 15 events that occurred outside the protected area, only 1 (when the threat was <10 m from the protected area) was incorrectly identified as occurring within the protected area, resulting in false client notification alarm.

**CONCLUSION AND STATUS**

We have described the configuration, operation, and results of testing an autonomous distributed sensor alarm and notification system that provides pipeline operators with a real-time warning of unauthorized right-of-way encroachment by excavation equipment near a pipeline. The system comprises a wireless network of discrete unattended smart seismic sensor nodes deployed along a pipeline right-of-way. Each sensor package, buried roughly 30 cm below ground, continually processes received signals to distinguish threats or abnormal events from benign sounds. When activity is detected, several sensors acting collectively classify the activity as benign or a pipeline threat. Threatening events activate client notifications. Table 1 summarizes the results of a six-week field test of this system operating in an active semi-urban environment.

Commercialization of this technology is currently in progress. Extensive testing of product prototypes is scheduled for 2011 with potential market introduction in 2012.
Table 1
Results Summary from the Woodbridge, NJ Field Test

<table>
<thead>
<tr>
<th>Property</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of detecting threat within protected area</td>
<td>86%</td>
</tr>
<tr>
<td>Probability of correctly classifying threat within protected area</td>
<td>91%</td>
</tr>
<tr>
<td>Localization error</td>
<td>&lt;10 m mean absolute error</td>
</tr>
<tr>
<td>False alarms</td>
<td>&lt;1 m rms variation for persistent threats</td>
</tr>
<tr>
<td></td>
<td>&lt;7% for threats slightly outside protected area</td>
</tr>
<tr>
<td></td>
<td>0% for non-threats</td>
</tr>
</tbody>
</table>

ACKNOWLEDGMENTS

The authors would like to thank BP (Bobby Roye in particular) for use of their Cushing OK facility, PSEG (George Ragula in particular) for use of their Woodbridge NJ facility, the NYSEARCH Member Companies and the PRCI member companies for their ongoing financial support of this project, the staff at Research Support Instruments, Inc. for their help supporting the NJ testing, and the technical staff at Physical Sciences Inc. including Will Stewart, Aram Faghfouri, Michael Hinds, and Phillip Mulhall. Lastly Physical Sciences Inc., American Innovations, and NYSEARCH/NGA would like to thank the Department of Transportation: Pipeline and Hazardous Material Safety Administration for their ongoing financial support.

REFERENCES