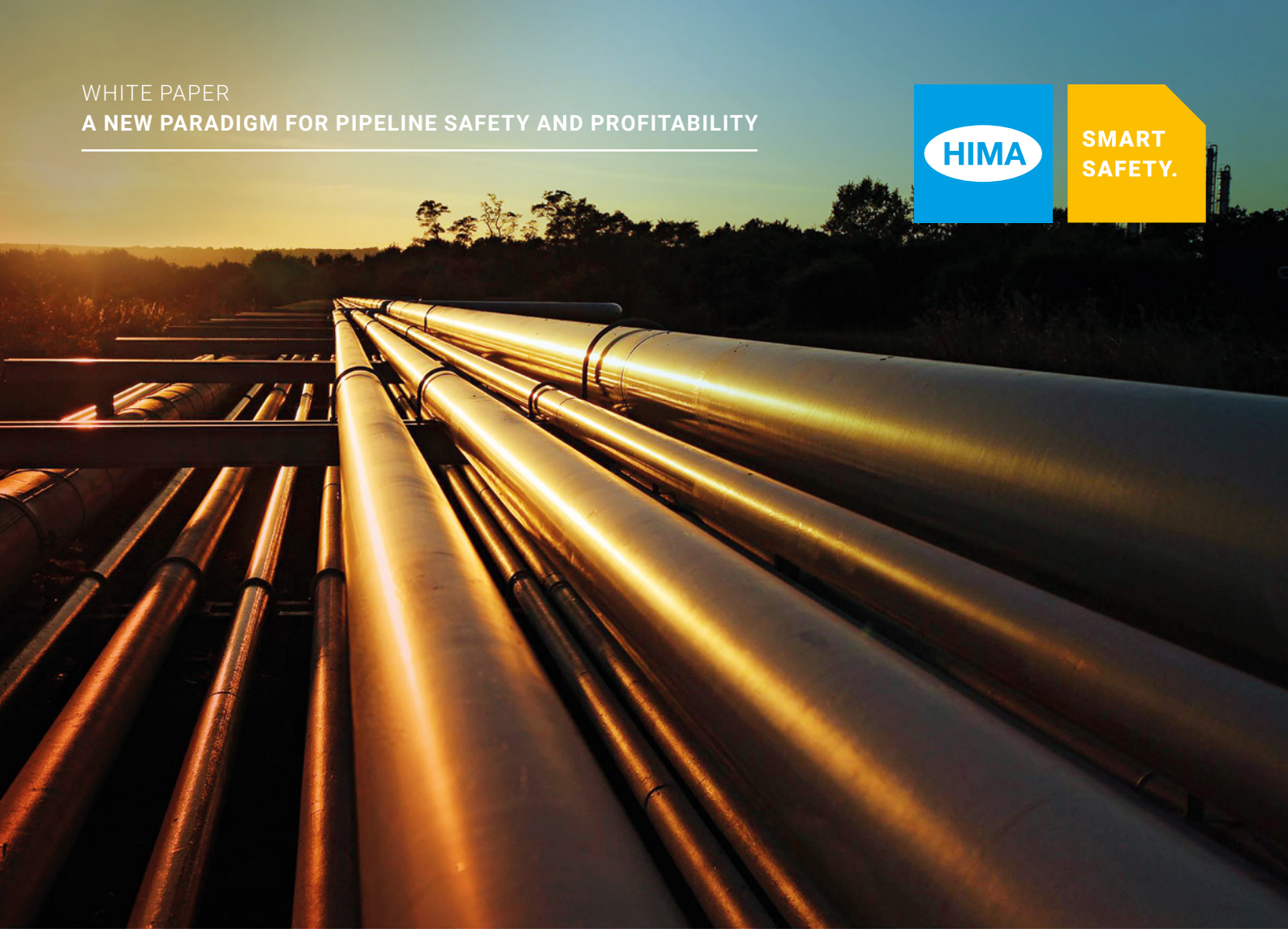
HIMA SMART SAFETY.



Pipeline Management 4.0

A new paradigm for pipeline Safety and Profitability

Sergej Arent, Director Applications

Pipelines offer the most dependable and cost-effective solution for transporting oil and gas, but they are not infallible. They can leak or rupture, they can be damaged accidentally or deliberately and they can be compromised to allow theft of the product they are transporting. Effective – and safe – management systems must provide pipeline operators with the tools they need to detect and localize these problems quickly and reliably, so that swift remedial action can be taken. And, in today's challenging world environment, management systems must not only be effective and safe, but also cybersecure. This paper introduces a new paradigm in pipeline management – Pipeline Management 4.0 – which integrates leak detection and safety systems to fully address these challenges. →

Pipeline management

Every day, millions of tons of liquids and gases are transported safely and securely by pipelines. Pipelines are exceptionally reliable, but given the large numbers in use and the huge distances they cover, it is inevitable that, from time to time, problems will occur. When they do, the environmental and financial impact can be enormous. In recent times, the situation has been further complicated by the growth in terrorism and cybercrime, both of which can have a devastating effect on pipeline operation and integrity. For these reasons, pipeline operators in almost every country of the world are now legally required to implement management systems that make it possible for them to meet strict safety, cybersecurity, and environmental requirements.

Leak detection: an essential element

An essential element of every pipeline management system is leak detection. It is of the utmost importance that leaks are detected and dealt with promptly, especially if the fluid that's being transported by the pipeline is flammable, toxic, corrosive, or otherwise damaging to the environment. Delays will not only lead to greater loss of product, but will also greatly increase the potential for consequential damage. The costs associated with the damage are often much greater than the cost of the lost product.

Figures from the United States Department of Transportation Pipelines and Hazardous Materials Safety Association (PHMSA) confirm that leak detection is at least as important today as it ever was. Since 2002, the number of pipeline incidents per year in the USA has remained above 600 and, in several years, it has approached 700.

Some of the resulting spills are large, as was demonstrated by the incident that occurred in South Dakota in November 2017 and affected the Keystone pipeline operated by TransCanada. The total volume of this spill has been estimated at 5,000 barrels (about 210,000 gallons) of crude oil, and aerial photography released by the news media dramatically confirmed that a large swathe of land was affected.

In recognition of the ever-present need for leak detection, the American Petroleum Institute (API) has produced a suite of standards to guide and help pipeline operators to reduce the occurrence of leaks and to minimize the impact of those leaks that still occur. The standards are:

- API 1160 – Overall standard to cover pipeline integrity management
- API 1130 – Design and implementation of leak detection systems
- API 1149 – Theoretical calculation of leak detection system performance
- API 1175 – Selection, operation, maintenance, and continuous improvement of leak detection systems.

Similar standards apply in most countries of the world; in Germany, for example, leak detection must comply with the Technical Rules for Pipelines (TRFL). While various standards differ somewhat in their approach and detail, all guide operators must consider the following when specifying or implementing a leak detection system:

- Sensitivity – A combination of the size of detectable leak and the time needed to detect it
- Reliability – A measure of the system's ability to accurately assess whether or not a leak exists
- Accuracy – The ability of a system to estimate key leak parameters such as leak flow rate, total volume lost, and leak location
- Resilience – The ability of a system to continue to function under unusual hydraulic conditions or when data is compromised

In addition, pipeline operators are now being expected to meet increasingly onerous safety, security and cybersecurity requirements. And it should be noted that these requirements apply not only to long-distance pipelines, but also to the much shorter pipelines found in chemical and petrochemical facilities.

Pipeline leakage is, of course, not a new problem and leak detection systems of various kinds have been in use for a very long time. It is instructive to examine the evolution of these systems to uncover the limitations of traditional approaches and to better understand how the latest advances help operators to meet today's increasingly stringent regulatory and commercial requirements. The first step is to look at the ways in which leaks can be detected.

External methods of leak detection

There are three principal external methods of leak detection: acoustic sensor, fiber-optic cable, and vapor sensor.

Acoustic sensors are installed along the pipeline to monitor internal noise levels. A leak produces low-frequency acoustic noise that the sensors detect. This method is sensitive to small leaks but it is liable to produce a large number of false alarms caused, for example, by vehicular traffic and the operation of pumps or valves. The efficiency and accuracy of this method depends on the skill of the operator. It is not well suited to long pipelines, as costs are too high.

Fiber-optic leak sensing uses a fiber-optic cable installed along the entire length of the pipeline. The cable looks continuously for the temperature changes produced by leaks. This method offers high leak location accuracy and is effective for identifying theft. However, installation cost is high, leak identification can be slow, stability over time is as yet unproven, and the entire pipeline must be excavated to install the cable. This method provides no information about the size of the leak.

Vapor sensing uses a sensing tube installed along the entire length of the pipeline. This carries air at a constant speed toward a sensor at the end of the pipeline. Scans are carried out periodically and, during a scan, a test peak of hydrogen is injected into the airflow. If vapor from a leak is detected, the system calculates the location of the leak based on the time difference between the arrival at the sensor of the vapor and hydrogen peak. This method gives good information about the size and location of the leak, but is costly to install. Also, scanning is usually carried out only once or twice a day, so leaks can become very large before they are detected.

Internal methods of leak detection

There are five principal internal methods of leak detection: statistical analysis of pressure and flow, real-time transient modelling, volume balance, pressure drop, and negative pressure wave.

Statistical analysis relies on pipeline pressure and flow profiles reacting to a leak in a specific way. The profile reactions are calculated using the correlations between inlet and outlet flow, and between inlet and outlet pressure. Unfortunately, this correlation only exists in steady state conditions, which means that statistical analysis doesn't work under transient conditions. This method has the advantage of using existing instrumentation, but leak location accuracy tends to be low.

Real time transient modelling (RTTM) uses basic physical laws to create mathematical models of flow within the pipeline. When the measured flow deviates from the model, this indicates a leak. RTTM is very good in transient conditions and can potentially use existing instrumentation. However, to minimize false alarms it is necessary to continuously monitor the noise level and modify the model accordingly. RTTM is expensive and sometimes difficult to program. The training cost for operators is high.

Volume balance is based on the principle of conservation of mass: What goes in must come out – unless there's a leak! The compensated volume balance variant is best for leakage detection, as this takes into account changes in pressure and temperature. This method uses proven technology and algorithms, it uses existing instrumentation with minimal programming, and it remains effective in transient conditions. It can, however, only estimate the location of the leak.

Pressure drop is a simple approach that uses existing instrumentation. During shutdown conditions, a pressure drop indicates a leak. This method can detect very small leaks (seepage), but it can only estimate the location of the leak.

Negative pressure wave leak detection works on the principle that when a leak occurs, it produces a negative pressure wave of known velocity both upstream and downstream of the leak. The leak location can be calculated by comparing the arrival times of the negative pressure wave at each sensor. This method uses existing instrumentation to provide extreme leak sensitivity and excellent location accuracy, combined with a low level of false alarms.

Leak Detection 1.0

The simplest of leak detection systems – which can be considered as Leak Detection 1.0 – use just one of the methods described above. This means that, although the system may seem simple to implement and, depending on the method, easy to operate, it necessarily suffers from all of the limitations associated with the chosen method.

Leak Detection 2.0

The next evolutionary step – Leak Detection 2.0 – uses multiple detection methods in combination; the benefits of each of the methods combine, and the weaknesses effectively cancel out. A successful approach to Leak Detection 2.0 has proved to be a combination of three internal leak detection methods: enhanced pressure wave, compensated volume balance, and pressure drop. The simultaneous application of these three methods means that system availability is assured for all pipeline operational phases, with a minimal level of false alarms. This approach also reduces programming costs, and the system requires little if any tuning to compensate for changes in the physical properties of the pipeline.

Leak Detection 3.0 – standalone rupture detection

While the approach and technologies of Leak Detection 2.0 are very effective in what they set out to do – detect leaks – they are designed only to warn operators of the problem rather than to initiate actions that will reduce the impact of the leak. Leak Detection 3.0 systems combine the concept of detection with automatic action, albeit only in the special case of a pipeline rupture, which is defined as a leak that reaches or exceeds around 30 percent of the pipeline flow rate.

These systems are designed for standalone operation, working independently of the leak detection implementation. They provide invaluable extra protection because they offer the immediate reaction to a rupture, which is essential to minimize spills and environmental damage, and these systems are, therefore, particularly appropriate for use on pipelines that traverse environmentally sensitive areas.

A typical Leak Detection 3.0 rupture control system incorporates a proven rupture detection algorithm that directly controls pipeline valves. When a rupture is detected, the system reacts immediately to initiate an emergency shut down (ESD) that isolates the affected pipeline segment.

Pipeline Management 4.0 – a hybrid solution

The most recent development is a logical progression that combines all of the key features of Leak Detection 2.0 with the ESD functionality of Leak Detection 3.0. The result is a hybrid solution that, because of its scope, exceeds the designation Leak Detection 4.0 and is more appropriately described as Pipeline Management 4.0.

Put simply, unlike traditional systems that detect leaks but take no action, Pipeline Management 4.0 is a complete automation system designed to help pipeline operators to improve safety and reliability. It can continuously monitor pipelines and shut them down automatically in hazardous situations, thereby significantly reducing or even eliminating direct and consequential damage.

A further important benefit is that sequences of automated actions to be carried out in response to specific events can be defined during the planning phase. This means that the behavior of the management system can be accurately matched to the needs of individual applications. In particular, shutting down the pipeline in response to a leak doesn't need to mean instantly closing all valves in the affected area.

In many cases, a smart multi-step shutdown sequence offers significant advantages. It might be useful to close one valve instantly, while delaying the closure of a second valve so that a section of the pipeline can be emptied to minimize the amount of leakage. Solutions of this type are particularly appropriate for inclined sections of pipeline.

Designing and implementing a system that can deliver on the promise of Pipeline Management 4.0 is not without its challenges. As the system performs key safety functions, it should conform with existing and, as far as possible, upcoming global safety standards. Because of this, most operators will require the system to comply with the requirements for Safety Integrity Level 3 (SIL 3) as defined by the IEC 61508 standard.

Pipeline Management 4.0 – a practical implementation

Devising and implementing practical, efficient, and effective Pipeline Management 4.0 solutions involves many challenges, but these have been successfully addressed and these solutions are now entering service and delivering important benefits for pipeline operators that have adopted them.

In an excellent example of such an implementation, flow rate monitoring is handled by SIL 3 capable safety hardware, with pressure and temperature data transmitted to the control center for visualization via a safety-compliant Ethernet protocol. The safety hardware at various locations along the pipeline is interconnected using the same protocol, so that each system knows the state of the overall pipeline. If a leak occurs, the controller implemented in the safety hardware automatically adjusts the flow, and shuts down the pipeline immediately in an emergency. This prevents or significantly reduces damage.

The software used for leak detection and localization also ensures that pipeline flow rates, pressures, and temperatures remain constantly visible to operators, and that anomalies are reliably recognized. As well as the main functions of leak detection and localization, the software supports batch and gauge tracking as well as data archiving and analysis. The system also accommodates pressure and temperature correction calculations.

In addition, the software can detect pipeline rupture and ensure that the damaged pipeline section is automatically and rapidly isolated, thereby minimizing the amount of product released.

Operators can adapt the detection algorithms to their specific needs. Unlimited changes, modifications, extensions, improvements and even prescribed verification tests during ongoing system operation, in line with the SIL 3 standard, are possible. In addition, the system can be easily integrated with almost any existing automation environment through open interfaces.

Even though it offers wide-ranging functionality and exceptional versatility, the system described makes no sacrifices in terms of performance. The SIL 3 capable leak localization system conforms to API 1130, TRFL and other relevant standards. To ensure continuous system availability, leaks are analyzed and localized using multiple methods. The enhanced pressure wave method, the volume balance, and the pressure drop method are used individually or in combination, depending on the nature of the leak and the operating state of the pipeline (static, transient, or shut down).

This approach ensures reliable detection of even the smallest leaks and minimizes false alarms. For example, the extended pressure wave method increases the detection sensitivity of the system, allowing detection of leaks that produce as little as 0.35 percent pressure change. Leaks can be localized accurately, and this method works in semi-static operating states. Its high accuracy eliminates over 80 percent of false alarms.

Cybersecurity

The discussion of the Pipeline Management 4.0 system so far demonstrates that it addresses many of the key challenges associated with pipeline operation, but there is one vital area that has not yet been mentioned: cybersecurity. Today's pipeline management solutions, as is the case with all modern automation and control systems, rely at their core on sophisticated software and networking. These are potentially vulnerable to cyberattacks by individuals and organizations intending to cause costly and potentially dangerous disruption.

Unfortunately, cyberattacks are a fast-growing risk. In the past, hacking was the domain of individuals and small groups with the primary aims of achieving notoriety or extorting money. Now however, there is increasing evidence that countries and states are involved, and their objective may well be to deliberately compromise key infrastructure – including oil pipelines – as a method of achieving political objectives. One of the most worrying aspects of this development is that countries and states have access to far greater resources than lone hackers or small groups of hackers, which means that they can be expected to mount much more sophisticated attacks.

In fact, an example of state-sponsored malware may have been seen already, in the form of the WannaCry ransomware cryptoworm, which is estimated to have affected around 300,000 computers in 150 countries. For those affected, the impact was substantial. Many were without IT facilities for hours or even days, and data loss was widespread. Admittedly, this attack targeted IT rather than automation systems but the well-known Stuxnet worm, which was deployed to derail Iran's nuclear program, confirms that automation systems are by no means immune.

It is almost certainly true that complete protection against the most skillful cyberattacks is impossible. Nevertheless, much can be done to protect systems against less determined attacks and also to make them less attractive targets for attack.

One very effective measure for enhancing cybersecurity in automation systems is to avoid the use of mainstream operating systems such as Microsoft Windows. Because these operating systems are so widely used, their vulnerabilities are quickly uncovered and exploited by hackers. A dedicated special-purpose operating system, as is used in state-of-the-art pipeline management solutions, is much less appealing to hackers as they will need to start almost from scratch to find ways in which it can be compromised, and there is no vast body of information they can draw on to help them achieve their nefarious ends.

The best pipeline management implementations are designed from the outset with cybersecurity very much in mind, using as guidance the IEC 62443 standard, which covers the security techniques necessary to prevent cyberattacks on facility networks and systems.
IEC 62443 requires the separation of key system elements and introduces the concepts of security zones and defined conduits to connect the zones. Crucially, it requires firewalls at every conduit that connects one security zone to another with different

requirements. This arrangement creates a tiered structure of defense mechanisms, a technique that is often described as 'defense in depth'.

But what precisely needs to be protected? According to the most recent version of IEC 61511, the standard that covers Safety Instrument Systems (SISs), the answer is that organizational demands and physical structures need to be given equal consideration.

The standard calls for these steps:

- Carry out a security risk assessment of the SIS
- Make the SIS sufficiently resilient against the identified security risks
- Safeguard the performance of the SIS, error detection and correction, protection against unwanted program alterations, protection of data for troubleshooting the safety instrumented function (SIF), and protection against bypassing restrictions to prevent the deactivation of alarms and manual shutdown
- Enable/disable read/write access via a sufficiently secure method

In terms of structural requirements, IEC 61511 instructs plant operators to conduct a further assessment of their SIS. The objectives are: to ensure independence between protection layers; establish diversity between protection layers; physically separate the protection layers; identify and avoid common-cause failures between protection layers.

There's no doubt that these requirements are complex and onerous, but this need not be a concern for pipeline operators that choose to adopt a modern pipeline solution. Leading suppliers of these solutions will have already taken steps to ensure that their products are cybersecure and compliant with the relevant standards. They will also be ready to offer advice about how their solutions should be deployed to maintain maximum protection against cyberattacks.

Conclusion

Pipeline operators are today offered a wider range of leak detection and pipeline management systems than ever before, which can make choosing the best system a challenging task. Before making a decision, however, operators should consider the benefits of the latest Pipeline Management 4.0 technology, which for the first time, integrates accurate and dependable leak detection with a SIL 3 compliant emergency shutdown system. The best systems have also been specifically engineered to provide robust protection against the growing threat of cyberattack.

This new hybrid pipeline management solution puts operators in full control of their pipelines whatever their operational status, and deals promptly and automatically with potentially hazardous occurrences such as major leaks and ruptures. The result is a reduced risk of product loss and environmental damage, both of which translate directly into consistent cost savings. Secure pipeline operation without disruption also contributes positively to the reputation and standing of the pipeline operator. Considered together, these factors make Pipeline Management 4.0 an exceptionally sound investment that will reliably minimize the effects of both intentional and accidental events in future.

For further information please contact:

HIMA Pipeline Competence Center
E-Mail: martin.snow@hima.com

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 6202 709-0
Fax: +49 6202 709-107
E-mail: info@hima.com

www.hima.com

Reference number: 96 9000666 0218 V01