Computational Pipeline Monitoring for Liquids

API RECOMMENDED PRACTICE 1130
SECOND EDITION, APRIL 2022

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed. The use of API publications is voluntary. In some cases, third parties or authorities having jurisdiction may choose to incorporate API standards by reference and may mandate compliance.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to ensure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be used. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

The verbal forms used to express the provisions in this document are as follows.

Shall: As used in a standard, “shall” denotes a minimum requirement to conform to the standard.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required to conform to the standard.

May: As used in a standard, “may” denotes a course of action permissible within the limits of a standard.

Can: As used in a standard, “can” denotes a statement of possibility or capability.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001.

Suggested revisions are invited and should be submitted to the Standards Department, API, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001, standards@api.org.

Contents

Figures

Computational Pipeline Monitoring for Liquids

1 Scope

This recommended practice (RP) focuses on the design, implementation, testing, and operation of CPM systems that use an algorithmic approach to detect hydraulic anomalies in liquid pipelines. The primary purpose of these systems is to provide tools that assist Pipeline Controllers in detecting commodity releases that are within the sensitivity of an algorithm. It is intended that the CPM system provide an alarm and display other related data to the Pipeline Controllers to aid in decision-making. The Pipeline Controllers would undertake an immediate investigation, confirm the reason for the alarm and initiate an operational response to the hydraulic anomaly when the alarm represents an irregular operating condition or abnormal operating condition or a commodity release.

The purpose of this recommended practice is to assist the Pipeline Operator in identifying issues relevant to the design, implementation, testing, and operation of a CPM system. This RP is intended for pipeline controllers and operators, CPM system developers and engineers, and others interested in CPM system design, implementation, and operation.

This RP includes definitions, source and reference documents, concepts of data acquisition, discussion of design and operation of a pipeline as related to CPM, field instrumentation for CPM purposes, alarm credibility, Pipeline Controller response, incident analysis, records retention, maintenance, system testing, training, considerations for setting alarm limits, trending, and recommendations for data presentation. The relationship between the Pipeline Controller and the CPM system is also discussed.

This recommended practice is written for liquid onshore or offshore trunkline systems. CPM systems have typically been applied to steel pipeline systems. CPM applicability and performance may be limited by the characteristics of non-steel pipelines.

This recommended practice was written considering single phase, liquid pipelines. Many of the principles apply to liquid pipelines in intermittent slack line flow or liquid pipelines that may have permanent slack line flow. This RP may not apply to the special case of determining leaks during shut-in conditions that occur when the line is shutdown (sometimes called static conditions) unless shut-in leak detection is part of the deployed CPM solution.

It is recognized that no single CPM methodology or technology is suitable for all pipelines because each pipeline system is unique in design and operation.

This recommended practice complements but does not replace other procedures for monitoring the integrity of the line. CPM systems are one part of an operator’s leak detection program. For further information on leak detection programs, see API RP 1175.

2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies (including any addenda/errata).

API RP 551, *Process Measurement Instrumentation*

API TR 1149, *Pipeline Variable Uncertainties and Their Effects on Leak Detectability*

API RP 1175, *Pipeline Leak Detection—Program Management*

Code of Federal Regulations, 49 CFR Part 195, *Transportation of Hazardous Liquids by Pipeline*

3 Terms, Definitions, Acronyms, and Abbreviations

3.1 Terms and Definitions

For the purposes of this document, the following definitions apply.

3.1.1
abnormal operating condition
A condition identified by the Operator that may indicate a malfunction of a component or deviation from normal operations that may:

a) Indicate a condition exceeding design limits; or

b) Result in a hazard(s) to persons, property, or the environment.

3.1.2
accumulator data
A SCADA data value that represents an accumulated quantity, usually volume in liquid pipeline service.

3.1.3
accumulator freeze
A feature of some SCADA protocols that allow all volumetric data to be captured at virtually the same time.

3.1.4
alarm
A visible and/or audible means of indicating to the controller an equipment malfunction, an analog or accumulation process deviation, or other condition requiring a controller's response.

3.1.5
alert algorithm
A part of a CPM system that evaluates the inferred measurements, compares against the thresholds, and issues a CPM alarm.

3.1.6
analog data
A SCADA data value that represents some measured quantity, such as temperature or pressure.

3.1.7
analog deadband
A parameter that defines the increment of change in a value that is significant.

NOTE See 5.2.3 for further information.

3.1.8
calibration
For this document, the activities in which instrumentation and measurement are proved.

3.1.9
communication failure
An interrupt in data exchange between the CPM system and the RTU, PLC, or Flow Computer.

3.1.10
commodity release
leak
An unintended loss of fluid from the pipeline.

3.1.11
computational pipeline monitoring
CPM
An algorithmic monitoring tool that alerts the Pipeline Controller to respond to a detectable pipeline hydraulic anomaly (perhaps both while the pipeline is operating or shut-in) which may be indicative of a commodity release and includes an Inference Engine and an Alert Algorithm.

3.1.12
conservation of mass
The principle as applied to liquid flow in pipelines, that states that the time rate of mass inflow to a pipe segment minus the time rate of mass outflow equals the time rate of mass increase (decrease is considered as a negative increase) in the pipe segment.

3.1.13
data archiving
A SCADA system feature that records data in an historical database under some pre-defined data management process.

3.1.14
data quality
A SCADA system feature that creates status bits that are attached to reflect the validity of process data.

3.1.15
drag reduction agent
DRA
An additive used in liquid pipelines to reduce friction loss.

3.1.16
event log
A SCADA system feature that creates a permanent record of changes to the pipeline and the system's state in chronological order.

3.1.17
false alarm
A commodity release alarm which, after investigation, was not caused by an actual commodity release.

3.1.18
filter
A device or algorithm to remove unwanted components from a process signal. Also called signal conditioning.

3.1.19
fluid properties
The characteristics of the fluid that describe its hydraulic behavior including density; viscosity, compressibility (or bulk modulus); coefficient of thermal expansion; thermal capacity.

3.1.20
historical data
Data that have been retained for later retrieval, typically maintained by a SCADA system's data archival subsystem.

3.1.21
hydraulic anomaly
An irregular operating condition on the pipeline or abnormal operating condition that is explainable through the systems hydraulics.

3.1.22
inference engine
A part of the CPM system that accumulates data, performs calculation, and provides outputs to the alert algorithm.

NOTE Additional description is offered in Annex B.

3.1.23
irregular operating condition
An infrequent event during which the pipeline may be operated in a way that is not normal and may require re-tuning the CPM.

3.1.24
leak declaration
The declaration that is made if a Pipeline Controller has reasons to suspect that a commodity release is occurring on the pipeline.

3.1.25
line balance
Comparison of the measured volume or mass entering the system to the measured volume or mass exiting the system or meter-to-meter reading comparison using conservation principles.

NOTE 1 Certain types of line balance are commonly referred to as mass balance or material balance.

NOTE 2 Additional description is offered in Annex B.

3.1.26
manual data override
When manual entries are input in lieu of actual field data values.

3.1.27
negative pressure wave CPM
A CPM system that senses the pressure wave signal that occurs when the pipe wall is compromised and the product escapes through the hole in the pipe.

3.1.28
noise
An unwanted component in a process signal.

3.1.29
pipeline controller
controller
A person who is responsible for the monitoring or monitoring and direct control of a pipeline.

3.1.30
pressure/flow monitoring CPM
A CPM system which examines the relationship between pressure and or flow changes and applies an algorithm to determine if they indicate an anomaly.

NOTE Additional description is offered in Annex B.

3.1.31
protocol
The specifications of the message structure between RTU or PLC and Control Center Computer are collectively referred to as the communications protocol.

3.1.32
rate of change
ROC
A calculated value that reflects the change in an analog data value per unit time.

3.1.33
real time transient model (RTTM) CPM
A CPM system which monitors instrument data and physical characteristics of the pipeline and fluids transported, then employs hydraulic calculations to determine the in/out balance, inventory, and instantaneous flow or pressure in segments of the pipeline, or both.

NOTE Additional description is offered in Annex B.

3.1.34
return to normal
The transition from alarm to normal state that signifies that an alarm condition has ended.

3.1.35
remote terminal unit
RTU
A SCADA system component, typically installed at a field site, that gathers process data from sensors for transmission to the Control Center Computer.

3.1.36
report-by-exception
A feature of some SCADA communication protocols that intends to improve communication efficiency by reporting only the data that has changed since the previous poll.

3.1.37
supervisory control and data acquisition
SCADA
The technology that makes it possible to remotely monitor and control pipeline facilities.

3.1.38
scan time
The time interval between two consecutive polls to Data Acquisition Devices on a SCADA communication channel.

3.1.39
segments
A shorter part of a pipeline section often bounded by instrumentation or other physical features of the pipeline.

3.1.40
sensitivity
A composite measure of the size of a leak that a CPM system is capable of detecting and the time required for the system to issue an alarm in the event that a commodity release of that size should occur.

NOTE This term is fully defined and discussed in Annex C.

3.1.41
shut-in
The pipeline hydraulic condition that exists when fluid is not entering or leaving the pipe but may be contained within.

3.1.42
single phase
A fluid state, either liquid or gaseous, based upon commodity, vapor pressure, pipeline pressure and temperature.

3.1.43
slack line
The condition where a pipeline segment is not entirely filled with liquid or is partly void. May also be called column separation.

3.1.44
statistical analysis CPM
A mathematical method of handling the CPM related instrument outputs from the pipeline. Statistical analysis CPM systems can use either Conservation of Mass techniques or Signature Recognition techniques or both techniques.

NOTE Additional description is offered in Annex B.

3.1.45
status data
A SCADA data value that represents the operational state of an item of field equipment.

3.1.46
steady state conditions
The pipeline hydraulic condition that exists when all the pipeline operating parameters remain nearly constant over a period.

3.1.47
system
An entire entity such as a complete pipeline. Segments are a subset of a system.

3.1.48
threshold
An upper or lower established value for a parameter which may be fixed or dynamic.

3.1.49
time skew
The variation in reporting times from one Data Acquisition Devices to another in a polled SCADA communications protocol.

3.1.50
time tag
A SCADA system feature that records the time that a measurement or event occurs along with the data.

3.1.51
transient conditions
transient
The pipeline hydraulic condition that exists when pipeline operating parameters change meaningfully over a period.

3.2 Abbreviations and Acronyms

For the purposes of this document, the following abbreviations and acronyms apply.

CPM	Computational Pipeline Monitoring
DRA	Drag Reduction Agent
PLC	Programmable Logic Controllers
ROC	Rate of Change
RTTM	Real-time Transient Model
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition

4 Technical Overview

This section discusses the generic types of CPM technologies and applications, provides a list of desirable CPM features, and mentions important issues concerning the fluids transported.

4.1 Selection Consideration

Each CPM methodology contains different combinations of features with varying degrees of capability and sophistication. Under appropriate circumstances, commodity release detection can benefit by employing multiple CPM techniques or applications for validation or redundancy. The independence of techniques used in some methodologies potentially allows for independent validation or redundancy.

CPM systems are installed to detect pipeline leaks. Before installing a CPM system, the following should be considered:

— instrumentation capabilities

— communications reliability

— pipeline operating condition

— pipeline physical constraints and characteristics

— product type

— commodity fluid/thermodynamic properties

— technical maturity level

4.2 CPM System Features

The following is a list of desirable CPM features and functionalities that improve performance or add utility, or both.

The CPM features listed below are not in any order nor is there any attempt to weight the importance of each. No one methodology or application possesses all these features and certain features may be more appropriate for specific pipeline systems.

The CPM system may:

— Be able to perform its CPM functions with existing sensors and instruments (or does not have special or additional requirements for instrumentation).

— Be minimally impacted by communication outages or by data failures, however, provide alarming based on a degraded mode of operation and during an abnormal operating condition (see 6.1.1).

— Accommodate complex operating conditions and be configurable to complex pipeline networks.

— Be available and reliable during transients.

— Perform an imbalance calculation on meters over a configurable set of time constants.

— Possess dynamic alarm thresholds.

— Possess dynamic liquid pack.

— Accommodate commodity blending.

— Account for heat transfer.

— Provide the pipeline system's real time hydraulic pressure profile, recognizing MAOP and elevation violations.

— Be able to handle slack line conditions.

— Be available during shut-ins

— Accommodate all liquid hydrocarbons.

— Can identify the location of a release.

— Can display pressure trends.

— Allow provisions to substitute manual override to specific status or values during periods when input data may be unavailable (e.g. communication outage, measurement failure, maintenance, etc.).

— Provide data attributes associated with supporting field inputs and calculated data.

— Identify the leak rate.

— Accommodate commodity measurement and inventory compensation for various correction factors (temperature, pressure, density, meter factor).

— Provide batch tracking including interface and anomaly markers. Compute bulk modulus and perform inventory compensation.

— Validate commodity release alarms using redundant analysis within the same method or redundant analysis between methods, or both.

— Account for effects of drag reducing additive.

— Provide the necessary documentation and training to support self-guided navigation, maintenance, alarm definition, and theory of operation.

— Vendor-provided technical support

— Provide tools to support a controller’s decision-making.

— Provide an interface to allow alarming of a stand-alone CPM application to be integrated into the Pipeline Controller’s primary alarm processing system.

— Provide audit trails of CPM actions taken by Pipeline Controllers and system developers.

— Allows self-testing without affecting performance while the test is underway.

— Allows for system health monitoring.

Different CPM systems have different features, not all of which are listed here. Operators are advised to do research and compare systems based on their needs.

4.2.1 Performance Metrics

Selection of a CPM system for a given pipeline involves evaluation of the required and expected (or estimated) performance of the system. Other aspects such as commercial considerations (e.g. use of a common system in

a Control Center with multiple pipelines) or economic criteria (e.g. capital and operating cost of the CPM) may be considered but these are not discussed herein.

The following categorizes and describes performance metrics for selection consideration. During the selection, the operator may place more weight or importance on one metric or another. A system should achieve a satisfactory balance between all four of these performance metrics. For a more complete description of these metrics please refer to Annex C.

— Reliability—The measure of the CPM's ability to render accurate decisions about the possible existence of a leak on the pipeline while operating within an envelope established by the CPM design. A system is considered more reliable if it consistently detects actual leaks without generating false alarms as defined by the operator's alarm management plan/program.

— Sensitivity—The composite measure of the size of a leak that a system can detect, and the time required for the system to issue an alarm if a leak of that size should occur.

— Accuracy—The validity of leak parameter estimates such as leak flow rate, total volume lost, type of fluid lost, and leak location are indications of CPM accuracy.

— Robustness—The measure of the CPM's ability to continue to function and provide useful information even under changing conditions of the pipeline (i.e. transients) or in conditions where data are lost or suspect. A system is considered robust if it continues to function under less than ideal conditions.

5 Infrastructure Supports for CPM

A CPM is not a stand-alone system. It depends upon field instrumentation, communications, and may be dependent on Supervisory Control and Data Acquisition (SCADA) infrastructure as a data source(s) and a vehicle to convey information to the controller (e.g. CPM data presentation and passing of CPM alarms). CPM systems use real-time data and may have other dependency interactions if the CPM is linked to a data historian.

5.1 Field Instrumentation and Measurement

This portion of the recommended practice discusses the selection, installation, calibration and maintenance of the field instrumentation and the measurement that is necessary to adequately support a CPM system.

Different CPM applications may require specific types of instrumentation or levels of performance. Some methodologies may need specialized instrumentation that is only used by the CPM. An operator may want to consider the best practices for equipment and instrument installation as they relate to CPM. Instrumentation requirements for a specific CPM application should be integrated into the CPM installation and maintenance programs.

5.1.1 Selection of Instrumentation and Measurement

Different CPM applications require specific types of instrumentation and measurement for levels of performance. Some methodologies may need specialized instrumentation and measurement that is only used by the CPM.

API Technical Report 1149, *Pipeline Variable Uncertainties and Their Effects on Leak Detectability*, outlines the importance of instrumentation and measurement to CPM performance. The calculations of API TR 1149 can demonstrate that additional and more accurate instrumentation and measurement increase CPM effectiveness and the calculations can be used to determine where the most cost-effective improvements can be made. Such analysis may be used repeatedly over the life of the pipeline system to achieve incremental performance improvement. The software developers or CPM providers may also be able to advise an operator on which instruments and measurements drive the CPM or influence the capabilities of the CPM applications as well as advise on what effects additional or upgraded instrumentation and measurement may have upon the CPM system.

The quality of instrument data can affect the CPM system. Instruments should be selected considering the required measurement accuracy. Ranges and specifications should be carefully matched to pipeline operating design, pressure, flow, temperature, density, viscosity, etc., to make best use of the instrumentation. Since instrumentation accuracy is generally stated in terms of percent of full range, the smallest available range greater than the desired range is preferable. There is no value in over specification of instrumentation and measurement accuracy if CPM performance is limited by the instrumentation or measurement loop accuracy, or repeatability and resolution of the SCADA system.

5.1.2 Installation of Instrumentation and Measurement

Instrumentation and measurement should be installed in accordance with the manufacturer's recommendations and consider stated accuracy and linearity. An operator may want to consider the industry best practices for instrumentation and measurement equipment and installation as it relates to CPM. For example:

— Using buried temperature probes to avoid ambient factors.

— Installing density or viscosity monitors, or both, at injection points where fluid properties are variable.

— Installing pressure sensors at intermediate locations along the pipeline system to improve leak location detection.

The placement of instrumentation in relation to the process equipment is important, and location should consider variations in operating conditions. Critical CPM instruments should be placed at locations where they will not be isolated during normal pipeline operations. For most CPM systems pressure, flow, and temperature are the most important data. Pressure should be measured where it best represents pipeline conditions and flow should be measured in an area where it can accurately be measured. For example, for inferential meters, at a location where there is a well-developed flow profile, temperature should be taken in a location that is representative of the process flow in the line or it may generate errors greater than results achieved without the input.

The design of the instrumentation process piping and the instruments should be located to include provision for convenient testing and calibration of instruments with minimum disruption of pipeline operations. Refer to API RP 551, *Process Measurement Instrumentation* for more information.

5.1.3 Calibration and Maintenance of CPM Instrumentation and Measurement

The quality of instrumentation and measurement data can affect the CPM system. A CPM system that has adequate instrumentation and measurement to achieve the desired commodity release sensitivity may be limited in its effectiveness if the CPM receives inaccurate data.

To maximize and maintain CPM performance, operators should prepare a CPM instrumentation list and a maintenance and calibration plan with procedures. This plan should recognize the importance of the CPM system to provide safe operation of the pipeline and provide for the priority repair of CPM critical instrumentation and measurement. The plan may result in instrumentation and measurement calibration practices that may exceed the requirements of applicable regulations. Some commonly used equipment and instrumentation does not require calibration, and this may be noted on the maintenance and calibration plan. In the CPM instrumentation and measurement calibration and maintenance plan, procedures should be developed to coordinate the test and re-calibration of field instrumentation with controllers and CPM system maintenance personnel since re-calibration may affect availability and performance of the system. The procedures should include the date, time, person's initials, and the events performed during the test. Instrumentation and measurement which requires calibration should be calibrated in accordance with the equipment manufacturer's recommendations or operator policy. Operating experience may provide the basis for determining an appropriate test and re-calibration interval. The CPM system itself may be the best indication of the necessity to test and re-calibrate an instrument or measurement.

5.1.4 Signal Conditioning

Noise is that part of the signal received that does not represent the quantity being measured. Noise exists to some degree in all measured data. Noise may reduce the performance of the CPM system.

Mechanical or electrical sources of noise should be reduced at the instrument. This may be accomplished by the installation of noise filters or reducing vibration at the installation site. Noise can also be reduced through software applications and other means.

5.2 Communications

This portion of the recommended practice discusses communication factors that can affect the quality and timeliness of the data required by the CPM system as well as the performance of the CPM system.

As all CPM systems require reliable communications, CPM systems should be implemented with an understanding of all aspects of the underlying communication infrastructure, including:

— the communication medium and error detection used;

— communication message structure and timing; and

— analog deadbands.

5.2.1 Communications Medium and Error Detection

All data communications media are subject to noise and interference that may cause data corruption. There is a varying degree of quality between the different forms of communication media used and operators should evaluate the quality of their communication medium infrastructure as it impacts CPM performance.

Most SCADA systems are designed to detect and reject communication corrupted messages. ‘Data quality bits,’ (sometimes called data attributes) that are available through the SCADA system can be useful to indicate lost messages and other information about the data (e.g. off-scan, manually entered, etc.). Ideally these status data should be used by the CPM system to identify missing, suspect, or conditional data.

5.2.2 Communications Message Structure, Data Collection, and Timing

SCADA systems gather data from field instrumentation using such Data Acquisition Devices known as Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), Field Data Acquisition Servers (FDA), or Flow Computers (FC), or a combination thereof. Each of these Data Acquisition Devices may be interchanged for specific applications on the pipeline system. In this recommended practice the term RTU is used to cover all of these Data Acquisition Devices. The specifications of the messages between these devices and the SCADA system or the Control Center Computers are collectively referred to as the communications protocol. The CPM system should be implemented with an understanding of the underlying communications protocol.

The communications is said to be ‘polled’ when the SCADA system or control center computer requests data from each field location in turn. The time interval required to poll all field locations and return to the first field location is referred to as ‘poll time’ or ‘scan time.’ To improve the scan time on slower communication channels and to gain efficiency on the communications channel, some protocols permit the field locations to respond with only the data that had changed since the previous poll. Such protocols are referred to as ‘Report-by-Exception.’ In polled systems the variation in reporting times from one field location to another is called ‘time skew.’ The software developers or CPM providers may also consider the impact of time skew in the data.

Communications may also be non-polled, meaning this protocol is a variation of Report-by-Exception. The approach may also be called ‘quiescent’ or ‘unsolicited.’ This protocol operation refers to Data Acquisition Devices which report without being polled either on a time scheduled basis or when field data changes. See 5.2.3 for a description of analog data change. For Report-by-Exception protocols that use this approach, have no defined scan time so the age of an item of data may be in question. To deal with this situation, some SCADA

systems generate ‘time tags,’ either in the RTU at the time data changes or in the control center computer at the time the data are received. Time tags may be used by CPM systems designed to analyze transient conditions in the pipeline.

Some SCADA systems can capture instantaneous volumetric measurement simultaneously at all locations. This feature is usually called accumulator freeze or data snapshot and effectively permits all volume data to be interrogated at one reference time. CPM systems not equipped to handle time tags may use this method to eliminate time skew.

5.2.3 Analog Deadband

Measured variables from process instrumentation are typically called SCADA “Analogs”. Report-by-Exception protocols or non-polled systems, or both, that report changed data may permit analog deadbands. When analog deadband is used, the value of the analog signal must change more than the deadband value before the new value is reported in the SCADA system. Such analog deadbands are generally used to reduce traffic on the communications channel or network, or both, as well as optimize disk space usage in the Historian/Logging system.

Flicker or step changes in the analog signal will appear to be a valid change in data Report-by-Exception (or Non-Polled) systems when analog deadband is not used. Such deadbands may be counterproductive for CPM methodologies that analyze the flicker for pattern changes.

When the precision of the SCADA system's analog-to-digital conversion hardware exceeds the repeatability of the sensor, the precision should be reduced using analog deadband. Care must be taken not to use an excessively large analog deadband since this technique effectively reduces the precision of the analog value.

5.3 SCADA

The SCADA system is a computer-based system. A SCADA system’s data acquisition function includes gathering real-time data through a communication network. A SCADA system’s control functions include controlling field devices. SCADA systems may archive data and provide warnings and alarms to the controller.

Generally, CPM systems use data gathered by the SCADA system, but some systems may gather data independently. Automated CPM systems may be interfaced bi-directionally with the SCADA system to receive pipeline data as it becomes available and to provide data back to SCADA or return alarm conditions to the SCADA system for alarm management utilities. Automatic transfer of the data makes it possible for the CPM system to analyze the data at a faster rate. Such automation requires that all necessary data are available from the SCADA system or other sources.

The data processing function in the SCADA system is responsible for converting the data to a format suitable for display and use by applications such as CPM systems. This section describes data processing features that affect CPM system as well as the performance of the CPM system.

5.3.1 Time Tagging

Time tags record when a data point was last updated. Some systems generate the time tags in the RTU, but it is more common for the SCADA system or control center computer to create the time tag at the time the data are either acquired or processed. Time tags, preferably originating at the RTU, can be used by the CPM system to reduce the effect of time skew, especially for accumulator values when a data freeze function is not available.

5.3.2 Data Quality

Data quality information may be stored with processed data. Typical data quality values that effect CPM systems include:

— ‘Non-updated’ or ‘old data’ caused by a RTU that is not responsive.

— ‘Off-scan,’ when a RTU has been taken off-line.

— ‘Manual data’ when manually entered data override interrogated values.

— ‘Range error’ when an analog value falls outside specified hardware limits.

— ‘Alarm inhibited,’ when the data are inhibited from alarming, even if out of tolerance (typically used during maintenance activities).

Data quality values may be used by the CPM system to help recognize and compensate for suspect data.

5.3.3 Analog Processing

Analog values typically represent measured variables such as pressure, temperature, density, viscosity, or flow rate, but can also represent items such as tank levels. The analog values are usually compared with predefined threshold values to detect when the values fall outside the desired range. The Rate of Change (ROC) is a calculated value, which is defined as the change of an engineering unit value per predefined time period. For Quiescent and Report-by-Exception systems, some type of smoothing algorithm, independent of the scan time, is usually needed to prevent the calculation of unrealistic ROC values for CPM approaches.

CPM systems generally rely on the scaled analog values and may also use sensor inputs that are external to the pipeline, including ground temperature.

5.3.4 Status Processing

Status data record the state of an item of field equipment.

CPM systems may need status information to determine pipeline configurations or if transient conditions are the result of changes in equipment state. An event log may be a good source of information when interpreting CPM alarms.

5.3.5 Accumulator Processing

Accumulator values represent an accumulated total of some process quantity since the start of the totalization process. In liquid pipeline SCADA service, accumulators are typically used to record volumetric or mass quantities passing a given point in the pipeline system.

5.3.6 Alarm Processing

Alarms are a special case of events that indicate a transition into an abnormal state. The return transition to the normal state is generally referred to as 'return to normal'. Alarms can be either transitory or continuous in nature. Transitory alarms have no return to normal state and are simply an indication that something has occurred such as a two-minute warning before a batch arrives or a ‘pig signal’ that a scraper has passed a station. Continuous alarms require a change to return to a normal state, such as a high-pressure alarm or a leak alarm.

5.4 Integration of CPM and SCADA

CPM systems may be closely integrated with the SCADA system. When CPM alarms and processed data are sent back to SCADA, they can be integrated into the standard SCADA displays. Maintaining a familiar method of data presentation can facilitate proper interpretation of the data by the controller.

All displays and data should be easily accessible by the controller to aid in operations of the CPM system along with the SCADA system. The hardware design should provide sufficient resources, either by organization of displays or providing enough displays to present needed information for analyzing alarms.

5.5 Data Historian

CPM system inputs and outputs can be stored in a historical database. Historical information retrieval is valuable for re-play of the CPM: to examine or analyze normal operation, irregular operating conditions, or abnormal operating conditions; for controller training; or to validate and sometimes improve sensitivity, accuracy, and robustness of CPM.

Alarm and event data should be retained per the operator's data retention policy.

A combination of historical and re-play data may provide the ability in some systems to recreate a series of events in a CPM system.

6 CPM Operation, Maintenance, and Testing

This section describes the operation, maintenance, testing, data retention, and documentation for a CPM system.

6.1 CPM Operations

CPM systems employ an inference engine and an alert algorithm that are defined for a given pipeline and its instrument and measurement data, configuration data, and product accounting data. The inference engine may use hydraulic calculations, or it may calculate data to infer the pipeline parameters. The alert algorithm considers inferred data or actual data, or both, and should issue an alarm if a limit is exceeded, for example, a mass conservation algorithm or a statistical algorithm's defined limits.

In the context of CPM, an alarm is a presentation of data concerning an abnormal or emergency event on the pipeline to the controller (via a SCADA system Pipeline Controller interface or a separate interface). An alarm could be triggered by many causes including equipment or data failure, an abnormal operating condition, or a commodity release.

6.1.1 Categorization of CPM Leak Alarms

CPM alarm causes can be subdivided into three broad categories, which are: possible commodity release, data failure, and irregular operating condition. Many CPM systems provide just one type of alarm and so in this case the determination of the cause and categorization of alarm should be made by the person who evaluates the alarm or by software that provides the cause or probability of cause.

The final determination of whether the alarm indicates a commodity release should be made by a Pipeline Controller who will use the CPM and SCADA system output to determine with a reasonable level of certainty the alarm's category.

Alarms should be considered as a possible commodity releases unless they are confirmed to be data failure or irregular operating condition alarms.

Other means of classifying alarms exist, and operators may use their own classification systems.

6.1.1.1 Possible Commodity Release

This category of alarm may be generated when the CPM system indicates a possible commodity release. In the case of closed loop control (which may be possible on some pipeline systems) the CPM system may automatically initiate action to shut down the pipeline.

The procedures that the controller should follow under this situation should be defined by the operator.

6.1.1.2 Data Failure

This category of alarm may be generated when critical CPM input data are missing or are determined to be incorrect. This class of alarms may also be called system impaired alarms. An example of missing input data would be a communication failure at a metering location. An example of incorrect data would be a pressure instrument that consistently reports values that have no hydraulic relation to other pressure and flow data on the pipeline. In this case the instrument may be out of calibration or locked at a fixed value. These incidents may be presented as types of data failure alarms. These data failure alarms could be automatically generated by the SCADA system, CPM system, or as manual entries in a controller's shift log. Some CPM systems indicate the impact the data failure has on continued CPM operation. The impact of this class of alarm could range from no effect to the disabling of the CPM system.

The procedures that the controller should follow under this situation should be defined by the operator.

6.1.1.2.1 CPM System Failure

This category of alarm may be generated when the CPM system has failed, and the impact would be total loss of this type of leak detection. The identified failure of one or a series of measured or calculated data points should not trigger a leak declaration. The internal CPM analysis utility should be able to identify data failures and alert the controller that this problem exists.

6.1.1.3 Irregular Operating Condition

This category of alarm may be generated when a pipeline is operating in a manner the CPM system has not been designed and configured to accommodate. For example, this type of alarm can occur during slack line or column separation on a pipeline which seldom experiences this condition.

The procedures that the Pipeline Controller should follow under this situation should be defined by the operator.

6.1.2 Alarm Response Considerations

The operator's procedures should require that all CPM alarms be evaluated. CPM alarms should be investigated to determine their cause and determine if action should be taken.

Many CPM systems provide just one type of alarm, a commodity release alarm. The operational responses to a CPM system alarm should consider these factors:

— All CPM alarms should be assumed to be valid until they are investigated.

— Other indications of a LOC should be considered.

— All CPM alarms have a cause.

— Past instances of alarm causes can be a useful guide in alarm evaluation, but every alarm should be evaluated individually, and assumptions of previous causes should not be readily made.

Operational response to a CPM system alarm would normally include an investigation and possibly remedial action.

Further information on alarm response can be found in API RP 1168 and API RP 1175.

6.1.2.1 Automated Pipeline Shutdown

Automatic closed-loop control response to alarm conditions that includes automatic valve closure requires a detailed transient analysis of the pipeline hydraulics prior to implementation. Automatic valve closures can potentially result in excessive surge pressure in liquid pipeline systems. If automatic valve closures are

implemented, then the controller should have the capability to override or disengage the automatic system for just cause.

6.1.3 CPM System Credibility and Review

A CPM system design goal is to maximize the system sensitivity to leaks or to find all leaks within the capabilities of the system and to minimize the occurrence of a leak declaration until the alert algorithm within the CPM indicates, with a high probability, the presence of an actual commodity release.

An excessive number of false alarms detracts from system credibility and may create complacency. It is suggested that the cause and number of CPM alarms should be reviewed on a periodic basis to attempt to reduce the number of false CPM alarms considering system sensitivity. There is a balanced relationship between the number of CPM alarms and the sensitivity of the CPM system.

For further information on KPIs, see API RP 1175.

6.2 System Testing

This section outlines testing methods and intervals to be considered for a CPM system. Testing of CPM systems is performed to establish a baseline of achieved performance for new CPM systems, or when there are changes to the CPM or the pipeline system that warrant re-evaluation of system performance, or for periodic evaluation of actual system performance.

The primary purpose of testing is to assure that the CPM system will alarm if a commodity release occurs. Another purpose of testing may be to assure that data failure alarms, system failure alarms, and irregular operating condition alarms function as expected.

Prior to testing, careful planning should be considered as to the reasons for the test and methods that will be employed and the process and procedures that will be followed. The test should be well managed to make sure it accomplishes objectives of the test plan.

Consideration should be given to the potential for a reduced level of pipeline monitoring during a CPM system test. The control center should be aware that an actual commodity release can occur simultaneously with the CPM system test and that an actual commodity release may be disguised or misdiagnosed during the test interval.

6.2.1 Testing Methods

CPM systems should be tested to alarm state with actual or simulated commodity removal. The test method and testing parameters should be chosen to be representative of line operating conditions.

Possible testing methods include:

— Fluid withdrawal tests

— Simulated leak tests

— Manipulating discrete instrument inputs of the SCADA or CPM system.

CPM tests may be ‘announced’ or ‘unannounced.’ An announced test is started with the awareness of the controller and tests only the CPM system. An unannounced test is started without the knowledge of the controller and tests the CPM system as well as the response of the controller. Generally, unannounced tests are used only if the performance of the CPM system has been established by previous successful announced tests.

The location of the test may be varied from one test to the next, so the CPM system experiences leak tests at various locations. This may increase the confidence in the capabilities of the CPM system. In addition, the test

may be performed at more than one withdrawal or simulated withdrawal rate or operating condition so the time and leak rate response of the CPM can be evaluated over a range of possible leak scenarios.

6.2.2 Initial Tests during CPM Commissioning

A CPM system should be tested to verify its functionality and performance. Throughout the installation and commissioning procedure, there may be a number and variety of tests. These tests ascertain the ability of the CPM system to function under varying operating conditions that are indicative of line operations. Initial tests may use simulated commodity releases. Consideration can be given to testing by actual removal of commodity from the pipeline for the final system test because the final test before acceptance will establish the baseline.

Subsequent CPM implementations on similar pipelines that employ the same CPM methodology may be able to use different initial test methods and may be able to take advantage of CPM work and testing on other pipelines.

Initial CPM tests should be rigorous and be planned and executed using good engineering and technical judgment on issues such as test methods employed, commodity loss rates, and situations to be simulated.

Testing, operating experience, offline modeling, or an API TR 1149 type analysis or other theoretical analysis of the CPM may establish the CPM baseline.

6.2.3 Periodic Retesting

CPM retesting of applications is necessary on a periodic basis to confirm the continued effectiveness of the CPM. Retesting should be documented in test records.

CPM applications should be tested on a 5-year interval to confirm the CPM system's continued effectiveness. It may not be necessary to test each pipeline system that uses the same CPM application, but consideration may be given to rotation of the tested pipeline and to varying the location of the test from one test to the next. Testing should be conducted in a manner consistent with producing results that are repeatable from test-to-test to assure that the leak threshold of detection does not vary widely or increase over time. The retest may use the same method employed in the initial tests or may use another test method.

Demonstrated performance of a CPM system, such as successful detection of a commodity release, may be an acceptable substitute for periodic retesting if it establishes the CPM's continued effectiveness. A successful identification of an actual commodity release, by an in-production CPM, shall be considered as sufficient for resetting of the retesting interval.

Subsequent tests may not be as rigorous as the initial tests. If no changes have been made to the pipeline or the CPM during the retest interval the re-test will be a confirmation test only.

6.2.4 Change-driven Testing

CPM systems should be retested following significant changes to ensure that their functionality is not adversely impacted. Operators should use discretion in deciding what constitutes a significant change. Examples of changes which might be significant can include, but are not limited to:

— Major changes to the pipeline configuration or physical characteristics.

— Major software configuration changes or addition of features.

— Major changes to pipeline operating conditions.

— New versions of the CPM software.

— Major instrument and measurement equipment additions or changes.

— Major SCADA system updates.

The decision to perform change-driven testing should be based upon individual analysis of the possible effect on performance and on a line-by-line basis. Consideration should be made as to how to document, if necessary, this analysis. In the case of pipeline configuration changes, testing similar to initial or periodic testing should be considered. Other changes may be tested using an actual commodity release data set, a data set from a leak test, a test simulation, or other off-line system testing.

The operator should determine which method is best suited to test the CPM system following significant changes.

When change-driven tests are documented in accordance with 6.2.5, such tests may be considered a periodic retest and set the start of a new testing interval.

6.2.5 Test Records

Records detailing the reasons for the tests, the test parameters and methodology, and the test results should be recorded and retained for initial tests and for retests. The details of at least two previous tests should be retained. Details of any actual commodity release, if that event is considered as a retest, should be retained as part of the two previous tests.

The operator determines the requirements for test documentation. Considerations for what information to include in the test records include:

— Date, time, and duration of the test.

— Technical reasons for the test that documents the reasons the test is to be performed and why the methodology and parameters have been chosen.

— Method, location, and description of the commodity withdrawal when used.

— Operating conditions at the time of the test.

— Details of any relevant alarms generated during the test.

— Summary of the performance of the CPM system during the test

Test results should be considered part of the ‘Check’ process identified in API RP 1175. Improvements to the CPM system made following a test should be considered part of the ‘Adjust’ process.

6.3 Operating Issues

For an operating CPM system, the following issues should be considered:

6.3.1 Security

Refer to API Standard 1164 for general cybersecurity provisions. Additional security privileges should be added for any CPM user interface device, parameter, alarm inhibit, and/or limit which could interfere with or degrade the performance of the CPM.

6.3.2 Parameter Changes

Provisions should be made against any alarm, parameter, and or sensor being inhibited without cause.

Parameter changes can be made in several ways. These changes should be coordinated or otherwise managed. Any changes should be logged.

A logging entry should include date, time, parameter, original setting, new setting, and person performing the change.

All CPM alarms and controller-initiated commands and events, which are part of data retention, may be stored in hard copy or “read only” format. All “read only” files should be protected from loss and unauthorized tampering.

The pipeline operating company should develop and implement a revision and release policy for software and firmware used within a CPM system.

Consideration may be given to allow the controller to make changes to parameters that are important in day-to-day or shift specific operation. The CPM system design may include provisions to allow the controller to modify and adjust parameters within fixed boundaries. Changes by the controller that affect the long-term operation of the CPM system should not be allowed.

The ability to make changes in the CPM system should only be accessible to authorized personnel and under the control of appropriate written procedures. Such changes should be recorded in an automatic log or in the shift log.

6.3.3 Pipeline System Maintenance Activities

The controller should be informed or have an indication whenever a CPM system sensor is inhibited and or disabled which causes the system to operate in a degraded mode. This may include the sensor’s calibration problems, communications problems, and software failures. This indication when identified could be provided by the SCADA system or other data gathering methodology if not integral to the CPM system.

Provisions should be made to minimize the effect of maintenance on the performance of the CPM system during periods of hardware, software, and field equipment maintenance and system upgrades.

System maintenance should be performed under the control of maintenance procedures, which address the effect of field and system maintenance on CPM performance. The procedure may also address the communications requirements between maintenance personnel and the controller

6.4 CPM System Data Retention

The retention of data and reports from a CPM system may be governed by several factors including the requirements of regulations, company policy, engineering and operations requirements and the controller training requirements. Careful consideration of what should be retained is recommended. The considerations should include what types of data and information may be useful or helpful in the future (e.g. a data set from a leak or leak test that can be used to verify CPM performance after changes have been made to the system).

All occurrences of a leak declaration should be historically documented including controller responses. Historical retention periods may vary between Operators.

6.5 CPM Documentation

Each CPM system employed on a pipeline system should be fully described and the documentation should be readily available for reference by the users and by those employees responsible for the maintenance and support of the CPM system. Documentation can include:

— A general description of the CPM outlining its principles of operation;

— A tabulation of the inputs used in the CPM procedure for each pipeline segment;

— A summary of how various products transported can affect the CPM system;

— An elevation profile;

— A list of special considerations or step-by-step procedures to be used in evaluating CPM results and for requesting assistance with alarm evaluation;

— Details of the expected performance of the leak detection system under normal and abnormal conditions; and the effects of system degradation on the leak detection results;

— CPM controller training manuals or information.

6.6 CPM Controller Training

The users of the CPM system and any CPM support staff require appropriate CPM training.

The following technical areas may be considered (only as they relate to the CPM system):

— Hydraulics. A Controller should be trained in the basic concepts of pipeline steady state hydraulics as they relate to the CPM system. The variances of hydraulic pressure due to elevation profiles, batches of differing density, temperature effects, and DRA. The Controller should also be trained in the basic relationship of pressure and temperature during shut-in conditions.

— A Controller should be trained to recognize the effects of pump start-ups/shutdowns, valve operation switch, pressure setpoints and other everyday activities, which cause transient conditions. Any of these will cause a system flow or pressure transient to appear potentially affecting CPM thresholds leading to non- leak alarming.

— Alarming/Performance. The Controller should be able to recognize and react to all CPM alarming, cognizant to indicators of CPM system performance.

— Data Presentation. A Controller should be trained in the recognition of the CPM notification or alarm and may be trained to research the cause of the alarm (data failure, irregular operating condition, or possible commodity release), or in methods of correlation of the alarm to independent data so the Controller will pursue the appropriate response. The presentation of CPM alarm data are a crucial component, such as the trend of the probability of a leak, or the description of the location for which the leak declaration has occurred. Other specifics to Data Presentation can be referred to in API RP 1165.

— Instrument Failure. The Controller should be able to qualitatively identify the impact of an instrument failure on the CPM system. The Controller should be trained to link the alarm event with the concept that the CPM system could be impaired.

— Validating CPM Alarms. An evaluation of the CPM system and operating conditions is necessary for validating or explaining the cause of a CPM alarm. The Controller should be trained to recognize and react to abnormal operating conditions and to take appropriate action. The training may be directed toward following procedures or calling upon and working with external resources for alarm evaluation.

— Line-pack Change (Online). A Controller should be trained to recognize CPM hydraulic pressure changes due to varying line-pack. A fundamental element in the spectrum of inventory control is the calculation of mass, or the comparison of barrels in versus barrels out. This training would include the ability to recognize the compressibility behavior of the liquid hydrocarbons that are transported.

— A Controller should be knowledgeable about sections of the pipeline that are susceptible to intermittent “slack line conditions.” The Controller should be knowledgeable about how this condition affects the CPM performance.

— Trending. A Controller should be able to recognize benefits provided by trending analysis of pipeline variables from SCADA and CPM. Trending data can be presented graphically or may be presented as a tabular display of historical data. A graphical output may provide the best visual history of CPM parameters. The Controller should be able to cross correlate CPM output with SCADA output wherever possible confirming CPM alarm evaluation.

— CPM System Operation. The Controller should be trained to understand the CPM system, and the concept/theory of its operation. A portion of Pipeline Controller training may include periodic review of the use of the

CPM system in a training environment. Training may cover all the various CPM systems in use within the Control Center and unique aspects of each application as they apply to individual pipeline segments.

— The Controller should be trained to interpret alarms correctly and in a timely manner or work with internal or external resources to evaluate the alarm. The CPM system should be implemented so the alarms are readily recognizable.

— Abnormal Functions. The Controller should be trained to recognize and react to the abnormal function of a CPM system as well as the abnormal function of the SCADA system. The loss of either should elicit certain predefined actions intended to preserve pipeline integrity. Targeted response actions should be thoroughly analyzed and scripted for prompt, efficient action.

— For example, if the CPM system becomes non-functional or severely degraded due to field equipment or SCADA failure, the Controller should be trained to employ other leak detection methods to compensate for the inadequacies of CPM. Alternatively, the Control Center may need to define what interval of time the CPM can be non-functional and what action needs to be taken. Short-term solutions may consider manual line balance and over-short and Pressure/Flow Monitoring. Actions might include tightening of pressure and flow alarm parameters.

— Other Leak Detection Techniques. The Controller should be trained in how to employ the results of other leak detection technique such as third party reports, SCADA deviation alarms, etc. so that a CPM system is not considered to be the only means of detecting leaks. The Controller should know what procedures to follow and reactions to make for other methods.

Annex A
(informative)

Discussion of CPM Thresholds

This annex discusses and illustrates that CPM is a pipeline tool designed to detect leaks within its capabilities. It may detect commodity releases or hydraulic anomalies that look like releases. Similar to any other tool, the CPM system is designed for a specific purpose and has its limitations. Limitations can be due to many reasons, which are discussed below.

Figure A.1 shows increasing sizes of commodity releases and which techniques can find leaks in the leak ranges:

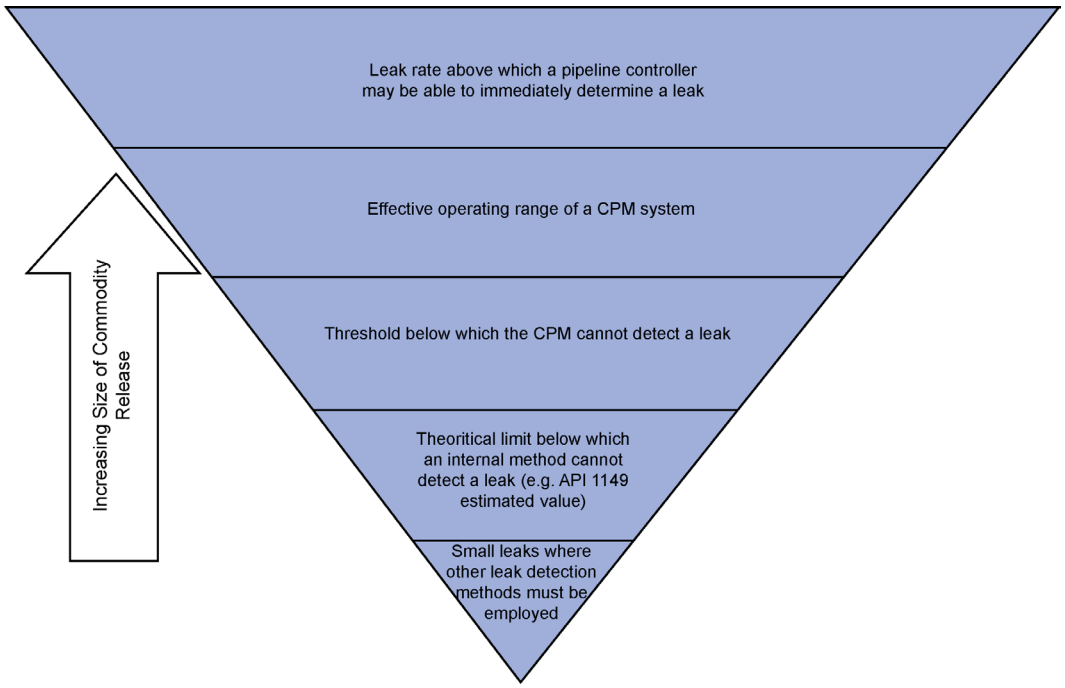

Figure A.1—CPM Releases and Techniques

Important concepts:

— The volume of product loss that occurs in any leak will be different for each individual pipeline. Therefore, it is impossible to specify the performance of a CPM system independent of the pipeline where it is applied.

— Steady-state or transient conditions of the pipeline influence the minimum size of commodity release that can be detected so CPM detection limits are not fixed. During transients the detectable limit may be higher. API TR 1149, for example, provides a method to calculate theoretical detection limits.

— CPM performance may be different when a pipeline is shut-in versus flowing.

— Performance of a CPM is governed by uncertainties in instruments, data scan rates and resolution, by knowledge of the physical details of the pipeline, and by the noise of the data used by the CPM. For example, less accurate data or instruments may affect threshold or detection time, or both.

— There will be a leak size limit below which the CPM is not capable of detecting a leak.

— Different CPM methods will find different sizes of leaks.

— Performance of Conservation of Mass CPM systems (the most common applications of a CPM) is influenced by the time over which the leak occurs and the magnitude of the leak. A commodity release at a high rate may exceed the CPM threshold quickly whereas a leak at a smaller rate will take longer to exceed the CPM threshold. Other factors that need to be considered for Conservation of Mass systems:

  — Slack line flow affects the volume in/out relationship.

  — The line pressure at the leak site affects the leak rate.

  — Transient events increase uncertainties.

  — Some applications are optimized to find small leaks over a long time window.

  — A slower instrument or SCADA scan rate provides CPM data more slowly and may increase time skew.

  — At lower flow rates the CPM may be less sensitive.

  — Line pack uncertainty is influenced by fluid temperature.

  — Longer balance sections have a greater uncertainty in the line pack and take longer to react to operational changes.

  — Fluid characteristics have a large impact on line pack uncertainties.

Annex B
(informative)

Description of Types of Internal Based CPM Systems

A CPM system is comprised of two parts, which are called: an Inference Engine and an Alert Algorithm. Figure B.1 shows the two parts.

The inference engine accepts data from instruments on the pipeline. For CPM systems the most common being: flow meters, pressure sensors, temperature sensors, densitometers, and equipment status . The data may be used in calculations to produce new values pertinent for leak detection purposes. The values are then passed to the alert algorithm.

The alert algorithm accepts values from the inference engine or data from field instruments, or both, and analyzes the values to determine if an alarm should be generated. It also determines what type of alarm should be generated.

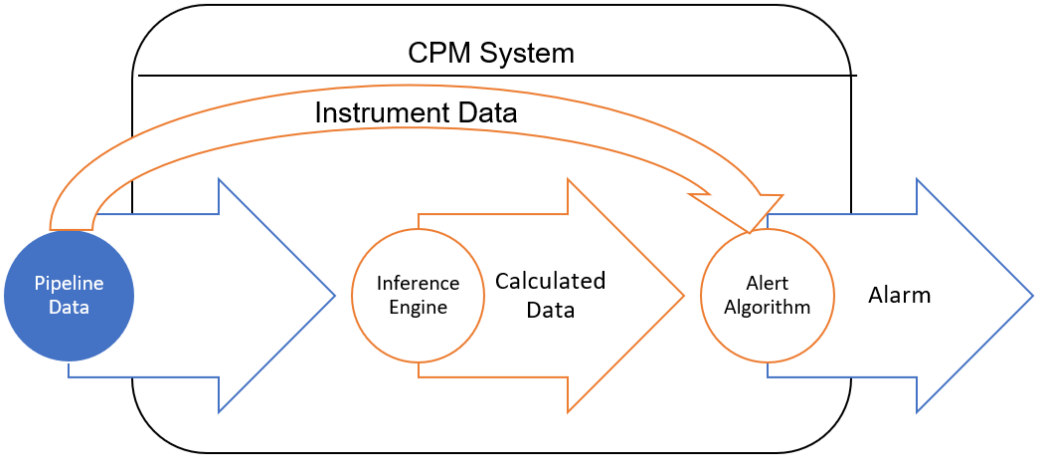

Figure B.1—CPM Systems

There are two primary technologies used in CPM systems: Conservation of Mass or Mass Balance methods; and Signature Recognition methods. Conservation of Mass methods work on the principle that whatever enters the pipeline should equal whatever exits the pipeline adjusted for change in inventory. Signature Recognition methods consider the relationships of system pressure or flow, or both, or recognize anomalies in sensor outputs on the pipeline.

Common names and types of CPM techniques are described below. These are included here to provide more vocabulary for the reader of this document and were outlined in the previous versions of this document.

B.1 Line Balance CPM Techniques

These meter-based methods determine the measurement imbalance between the incoming (receipt) and outgoing (delivery) volumes. The imbalance is compared against a predefined threshold for a select time interval. The imbalance is typically monitored over several time periods or windows (e.g. 15 minutes to 24 hours, also weekly and monthly) to detect commodity releases of different sizes.

The capabilities of the basic technique (i.e. simple meter in/meter out comparison) can be enhanced by correcting the meter readings to standard conditions and by compensation for changes in line-pack due to temperature or

pressure, or both, or commodity characteristics, or a combination thereof. Good engineering practice should be applied to determine the CPM's requirement for line-pack correction.

Names that are used for enhanced line balance techniques are volume balance, modified volume balance, and mass balance.

1) Volume Balance—Comparison of the corrected volume of fluid entering the system to the corrected volume exiting the system.

2) Modified Volume Balance—An enhancement of Volume Balance CPM that compares the measurement of corrected volume entering the system to the volume exiting the system and accounts for changes in the inventory of the pipe.

3) Mass Balance—A mathematical process that considers the fluid injected, delivered and the change in inventory of the pipeline so all the fluid is accounted for.

These systems use Conservation of Mass CPM techniques.

B.2 Real Time Transient Model (RTTM) CPM

A RTTM provides an enhanced view of pipeline conditions along the pipeline. Extensive configuration of physical pipeline parameters and commodity characteristics are required to design a pipeline specific RTTM. The application software executes a real-time transient hydraulic model with this configuration using field inputs such as flows, pressures, temperatures, and densities along the pipeline. Fluid dynamic characteristic values are modeled throughout the pipeline, even during system transients.

The advantage of an RTTM system is its ability to compute line pack more accurately than other line-balance system. The RTTM software may compare measured data for a segment of pipeline with its corresponding modeled conditions or it may use the modeled condition to calculate line pack. By comparing modeled process characteristics to measured ones, coupled with an understanding of the pipeline system physics, the RTTM can generate leak alarms. Some RTTM CPM techniques include Conservation of Mass and Signature Recognition.

B.3 Statistical Analysis CPM

The degree of statistical involvement varies widely with the different methods in this classification. A sophisticated statistical approach may calculate the probability of commodity release against the probability of no-commodity release. Pressure and flow inputs that define the perimeter of the pipeline are statistically evaluated in real-time for the presence of patterns associated with a leak. A probability value is assigned to whether the event is a commodity release. The analysis can, with suitable instrumentation, provide intelligent alarm processing which reduces the number of alarms requiring Operator analysis. This type of CPM methodology does not require an extensive database describing the pipeline.

The Statistical Process Control (SPC) approach includes statistical analysis on pressure or flow, or both. SPC techniques can be applied to generate sensitive CPM alarm thresholds from empirical data for a select time window. SPC may use line balance data from normal operations to establish historical mean and standard deviations. If the mean value of the volume imbalance for the evaluated time window increases statistically, the CPM system will give a warning. An alarm is generated if the statistical changes persist for a certain time period. SPC approaches can correlate the changes in one parameter with those in other parameters over time intervals to identify a hydraulic anomaly.

Statistical analysis CPM systems can utilize either Conservation of Mass techniques or Signature Recognition techniques or both techniques.

B.4 Pressure/Flow Monitoring CPM

Pressure/Flow Monitoring CPM examines the relationship between various sensors' outputs and applies an algorithm to determine if they indicate an anomaly.

Generally, more simplistic Pressure/Flow Monitoring techniques that alarm a single variable such as pressure/flow-rate deviation and pressure/flow-rate limit monitoring, although providing valuable information to the Controller, are not considered CPM systems.

CPM Pressure/Flow Monitoring techniques should make use of an inference engine and generally use multiple variables to alert the Controller of a possible leak.

Pressure/Flow Monitoring CPM usually utilizes Signature Recognition techniques.

B.5 Negative Pressure Wave

Negative Pressure Wave techniques take advantage of the rarefaction waves produced by the onset of the leak. The onset of the leak produces a sudden drop in pressure at the leak site. The leak generates two negative pressure or rarefaction waves, one traveling upstream and the other downstream.

For this CPM, sensors capable of detecting the pressure wave are installed on the pipeline. The transmitters continuously measure the fluctuation of the line pressure. A rapid pressure drop, and recovery is reported to the central facility. At the central facility, the data from all monitored sites should be used to determine whether to initiate a CPM alarm. Negative pressure wave techniques may use time of flight to assist with locating a leak.

Negative Pressure Wave CPM utilizes Signature Recognition techniques.

B.6 Acoustic

Acoustic techniques utilize the continuous pressure variations caused by a leak. The pressure differential between the inside of the pipe and its environment causes pressure instability within the fluid.

For this CPM, sensors capable of continuously measuring the fluctuation of the line pressure or direct monitoring of acoustic signal are installed on the pipeline. The transmitters continuously measure the fluctuation of the line pressure or acoustic signal.

Acoustic CPM utilizes Signature Recognition techniques.

Annex C
(informative)

Metrics and Other Pertinent Text from API Publication 1155

API Publication 1155, *Evaluation Methodology for Software Based Leak Detection Systems* was withdrawn. The Task Force charged with the development of this document decided to include the valuable definitions and discussion into an annex, so it is still available. The sections which were thought to be most pertinent are included below. A few minor modifications to the text have been made to make it consistent with the body of this document.

C.1 API 1155 Overview of Pipeline Leak Detection

Pipeline leak detection is treated herein as a classical problem in parameter estimation. In other words, the software-based leak detection system estimates parameters based upon measurement data. The leak parameter estimates are then examined to decide if they warrant the issuance of an alarm to indicate the likely presence of an actual leak. Note that the estimated parameters depend upon the nature of the leak detection system. These might include the leak flow-rate, amount of fluid lost, magnitude of pressure or flow disturbance at the leak site, most probable location of the leak, and so forth. Virtually all systems that make a statistical decision based upon a set of measurement data can be discussed within the framework of this model.

As represented in Figure C.1, the detection problem is a step-wise process that logically separates each of the system's components in terms of their relationship to the desired result. The software-based leak detection system relies on data values acquired from some reliable source, usually the real-time SCADA system, to provide a series of data sets representative of actual conditions at any given point in time. Once data for a given time period have been acquired, they are subjected to some pre-determined mathematical or statistical analysis process that generates additional data based on an assumed model of the pipeline and its associated parameters. Results from the analysis process are produced in the form of parameter estimates. These parameter estimates are in turn subjected to some probability law or decision criteria to determine if a leak does indeed exist. In the simplest case, a given set of data can represent one of two possible outcomes; the existence of a leak or the absence of one. Typically, the process requires an examination of many complex data interrelationships in order to provide acceptable results. Depending upon the nature of the leak detection system, this examination might be done over a small window in time, or it could involve periods of several minutes or even hours. In some cases, the time required to make a decision might also depend upon the size of the leak, if one should occur.

The phrase “model of the pipeline” is used in the most general sense. Some vendors and client companies tend to group software-based leak detection systems into the two categories “model-based” and “not model-based,” depending upon whether or not the system involves a fluid dynamics model. In fact, this is an incomplete characterization. Fluid dynamics models employ one or more of the basic equations of fluid mechanics, which include the equations of continuity, momentum, and energy. However, there are a number of software-based leak detection methods, all of which are based upon some set of rules or “model” describing the pipeline operation. It is this set of rules that determines how such systems use the measurement data to make decisions.

C.2 Leak Detection Performance

Determination of the presence or absence of a leak requires that the software-based leak detection system has prior knowledge of the problem to be solved and some pre-determined criteria upon which to base its decision. In the most general sense, there are four possible outcomes each time the leak hypothesis is tested:

1) The system correctly indicates that there is no leak,

2) The system correctly indicates that there is a leak,

3) The system incorrectly indicates that there is a leak, and

4) The system incorrectly indicates that there is no leak (failure to detect).

Outcomes 1 and 2 constitute proper operation of the leak detection system whereas outcomes 3 and 4 constitute failure of the system. In the ideal system outcomes 3 and 4 never occur.

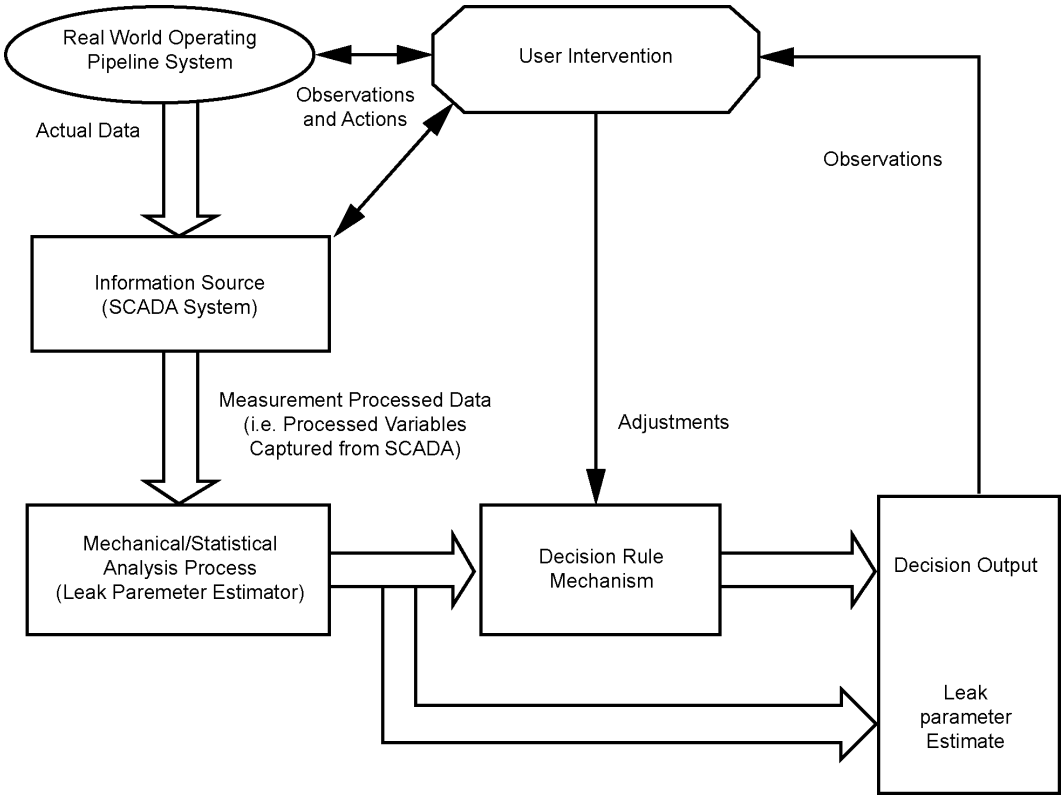

Figure C.1—Generalized Example of the Software-based Leak Detection Process

To further characterize an ideal leak detection system, one should recognize the importance of an accurate and timely response if a leak occurs. The characteristics of an “ideal leak detection system” are easily stated. Such an ideal system would always and immediately detect any leak that might occur, and it would never incorrectly declare a leak and would always and immediately provide an accurate estimate of the location and size of any leak. There are no known software-based leak detection systems that currently provide this ideal level of performance. Furthermore, certain characteristics of the “ideal leak detection system” impose conflicting requirements upon practical leak detection systems. It is not likely that such an ideal system can ever be achieved in practice.

The task of determining the best leak detection solution for a given pipeline always involves performance tradeoffs. These tradeoffs should be judged before the leak detection system is installed on the pipeline. In some cases, the leak detection system may be selected before the pipeline itself is placed into operation. Once installed, periodic adjustments of leak detection system parameters may be necessary to account for operational experience, configuration changes, and so forth.

C.3 Appraisal of Leak Detection System Performance

Determining the level of performance that can be expected from a software-based leak detection system is a process that involves several factors, some of which may not be within the control of the pipeline company or the leak detection vendor. Many implementations assume that a certain degree of error exists within the specification of the pipeline and with the measurements taken during operation and provide algorithms to compensate for such inconsistencies. Additionally, some vendors require that the system be subjected to a tuning period during the installation process, so that adjustments to the configuration and the corresponding compensation algorithms can be made using real-time pipeline measurement information. Although this can sometimes be a tedious and

time consuming process, it is generally accepted in the case of the more complex solutions, in that the ultimate outcome produces more accurate and reliable results.

Ideally, a vendor, given accurate information, could state exactly how their software-based leak detection system would perform on a given pipeline configuration, prior to its installation. In practice, this is sometimes difficult due to unavailable or incomplete information regarding the physical pipeline and its operation.

C.4 Output Data and Performance Metrics

Selection of a software-based leak detection system for a given application involves evaluation of the expected (or estimated) performance of the system, as well as operational features and functions that might add to the utility of the system but do not directly improve leak detection performance. The selection process for a specific pipeline system might also include commercial and economic criteria such as system cost, support, ease of maintenance, and so forth.

Any appraisal of leak detection system performance involves an assessment of the various tradeoffs that should be made when the system is installed. In order to establish appropriate performance criteria, the client pipeline company must perform their own assessment and understand the implications of that assessment with respect to the various categories of leak detection performance. In practice, real and potential costs are incurred for each incorrect alarm, missed alarm, late alarm, or any other deviation from ideal leak detection system performance, or a combination thereof. Any evaluation of costs and liabilities associated with improper alarming is beyond the scope of this annex.

Performance of a software-based leak detection system is tantamount to its ability to recognize leak conditions rapidly and without failure, to minimize fluid loss, property damage and the risk of personal injury. However, this definition of performance is too broad to be useful to determine projected performance of a leak detection system on a given pipeline or set of pipelines and needs to be defined more specifically by its components. With that goal in mind, a wide range of criteria used by pipeline companies and vendors in the specification of leak detection system performance has been examined. These performance criteria could be grouped into four categories, or metrics, that determine a system's reliability, sensitivity, accuracy, and robustness. A definition and discussion of each of these performance metrics follows.

C.5 Reliability

“Reliability” is defined as a measure of the ability of a leak detection system to render accurate decisions about the possible existence of a leak on the pipeline, while operating within an envelope established by the leak detection system design. It follows that reliability is directly related to the probability of detecting a leak, given that a leak does in fact exist, and the probability of incorrectly declaring a leak, given that no leak has occurred. A system is more reliable if it consistently detects actual leaks without generating incorrect declarations. Conversely, a system which tends to incorrectly declare leaks is often considered to be less reliable. This is particularly true in cases where it is difficult for the Pipeline Controller to distinguish between actual leaks and incorrect declarations. On the other hand, a high rate of incorrect leak declarations might be considered less significant if the Pipeline Operators have access to additional information that can be used to verify or disqualify a leak alarm.

Systems that limit or inhibit alarm generation in response to certain conditions of pipeline operation are not necessarily less reliable. Reliability pertains only to the functionality of the leak detection software without regard to SCADA system performance, availability of the pipeline instrumentation and communication equipment, or any other factor beyond the control of the leak detection system vendor. Such factors involve a separate category of performance, namely robustness.

The reliability of a leak detection system usually depends upon a number of parameter settings (e.g. decision thresholds, filter characteristics, and so forth) as well as all of the suitable leak detection techniques employed for the operational characteristics of the target pipeline system. In some cases, a Pipeline Operator should decide whether to use settings that cause frequent alarms during normal pipeline operations, or to use other settings

that are less likely to cause alarms but might delay or even fail to alarm when a leak is present. Many systems also make automatic adjustments to decision thresholds and other parameters in order to reduce the likelihood of generating alarms during defined operating conditions. When such adjustments are made, a corresponding penalty is normally incurred in some other aspect of performance. For example, decisions based on longer observation intervals might make a particular system less susceptible to random instrumentation errors or disturbances caused by normal pipeline operations, but this performance gain is achieved at the expense of longer response time and the risk of greater fluid loss if a leak should occur.

Reliability can be managed through the use of Pipeline Operator's response criteria and procedures. Such procedural methods, unless embodied within the leak detection software itself and performed automatically by the system, do not serve to discriminate between leak detection systems with regard to performance. On the other hand, if additional information is available from the leak detection, SCADA, or other systems, then reliability may be better managed.

C.6 Sensitivity

"Sensitivity" is defined as a composite measure of the size of leak that a system is capable of detecting, and the time required for the system to issue an alarm if a leak of that size should occur. The relation between leak size and response time is dependent upon the nature of the leak detection system. In some cases, as illustrated in Figure C.2, there is a wide variation in response time as a function of leak size. In other cases, the response time is relatively independent of leak size, as depicted in Figure C.3. However, there are no known systems that tend to detect small leaks more quickly than large leaks.

To further illustrate this definition of sensitivity, consider a hypothetical case involving four different leak detection systems (W, X, Y, Z) with the following projected levels of sensitivity on a given pipeline:

1) System W—This system can detect a small leak within 5 minutes of the start of the leak.

2) System X—This system can detect a small leak within 15 minutes of the start of the leak.

3) System Y—This system can detect a large leak within 5 minutes of the start of the leak.

4) System Z—This system can detect a large leak within 15 minutes of the start of the leak.

Based on these performance projections it is obvious that System W is the most sensitive and that the System Z is the least sensitive. However, comparison of the Systems X and Y is less apparent. It is possible that for one pipeline System X might be more appropriate, whereas for another pipeline System Y is more applicable. Since some leak detection systems manifest a strong correlation between leak size and response time, it is also possible that the two levels of sensitivity shown for the Systems X and Y could be manifested by the same leak detection system.

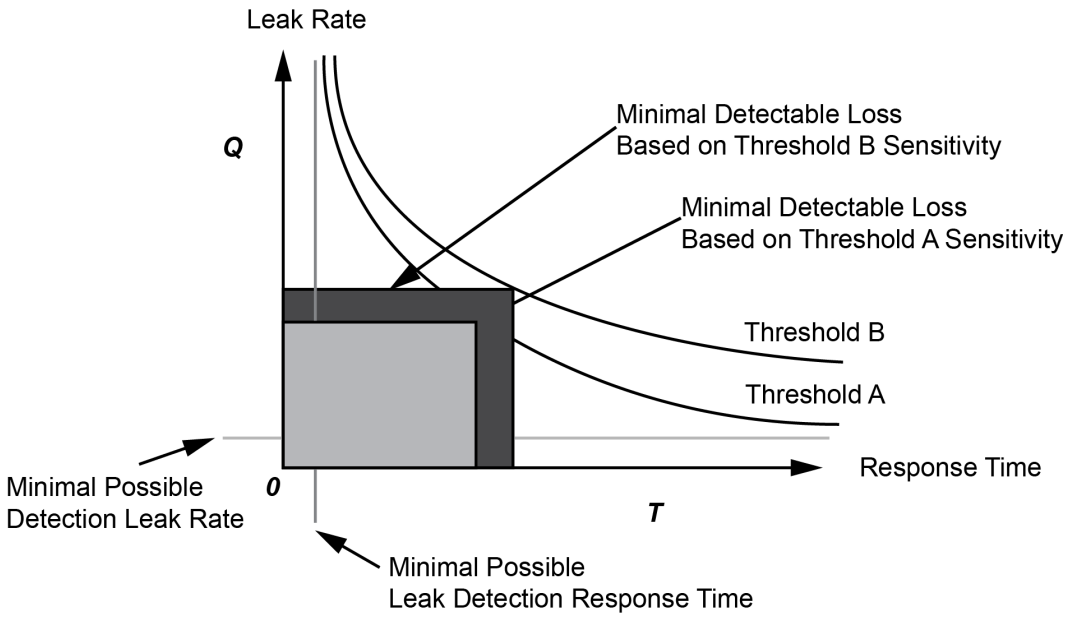

Figure C.2—Examples of Sensitivity Curves Based on Different Operating Thresholds. These Examples are Typical of Systems that Operate on Accumulated Parameter Errors (e.g. Volume Balance)

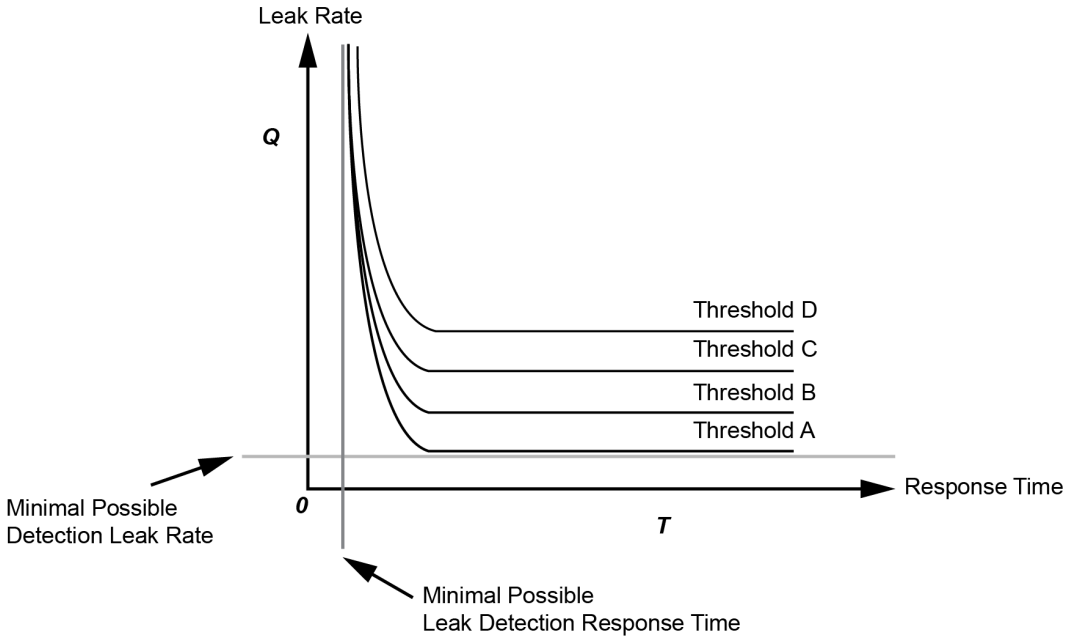

Figure C.3—Examples of Sensitivity Curves Typical of Event Oriented Systems. Such Systems Might Employ Pattern Recognition Techniques to Identify the Onset of a Leak

Frequently during the specification process, users attempt to define leak detection performance in terms of detecting a particular leak flow-rate within a specified minimum period of time. Although sensitivity expressed in such terms certainly represents one aspect of performance, its importance can vary depending on the nature of the leak detection system and the operating characteristics of the target pipeline system. As shown in Figure 2 and Figure 3, the correlation between leak size and response time can be highly dependent upon the leak detection techniques employed. It is also important to recognize that adjustments made in the interest of improving sensitivity can have a corresponding and not necessarily beneficial effect on other aspects of performance.

The examples shown in Figure C.2 and Figure C.3 also serve to illustrate the concept of minimum detectable leak size and minimum attainable response time on any given pipeline. In practice, most systems can be set up to achieve various levels of sensitivity, provided the minimum detectable leak size and minimum attainable

response time are not violated. The leak detection system vendor, and possibly the Pipeline Operator, can affect these characteristics by adjusting leak detection thresholds, filter characteristics or other parameters. Appropriate settings for these thresholds are usually dependent upon factors such as the SCADA system's scan time, instrument placement, fluid types, and so forth.

C.7 Accuracy

To this point, the focus has been upon the philosophy of detecting and announcing a leak but has not considered the additional information that might accompany a leak alarm. With reference to Figure C.1, this additional information is derived by the leak parameter estimation process and is made available to the user as ancillary data output from the software-based leak detection system. Although the amount and nature of such information varies between vendors, it typically includes estimates of leak parameters such as leak flow-rate, total volume lost, type of fluid lost, and leak location within the pipeline network at certain pipeline conditions. The validity of these leak parameter estimates constitutes a third measure of performance referred to as accuracy.

From a strictly mechanical point of view, leak rate depends upon the magnitude and shape of the perforation, pipe environment, fluid characteristics and pressure at the leak site. If the location of a leak is known, the leak flow-rate can be used to determine resultant disturbances in pressure, flow rate, and temperature at other points on the pipeline. Software-based leak detection systems, on the other hand, deal with quite the opposite situation. Although these systems approach their task in a wide variety of ways, the one thing they all have in common is that they should operate with no prior knowledge of the size or location of a leak, should one occur. Thus, a system might calculate a leak flow rate to compensate for a difference between observed and expected values of pressure or flow at certain points on the pipeline. This effective leak flow rate might then be used to estimate the location of the leak or the volume loss related to the leak, or both. Another system, operating on the same pipeline, might estimate total fluid volume lost based on metered volumes and calculated changes in line-pack, without ever attempting to directly estimate leak flow rate or location.

C.8 Robustness

Robustness is defined herein as a measure of the leak detection system's ability to continue to function and provide useful information, even under changing conditions of pipeline operation, or in conditions where data is lost or suspect. A system is robust if it continues to function under such less than ideal conditions. On the other hand, if the system disables certain functions, it might then achieve better reliability, but would be considered less robust.

The distinction between reliability and robustness is significant. Reliability is a measure of performance within a specified operational envelope. Robustness is a measure of the effective size of the operational envelope. For example, consider the following hypothetical leak detection systems:

1) System I—This system employs a sensitive leak detection algorithm. The system is normally reliable, frequently generates alarms during certain normal pipeline operations.

2) System II—This system employs an alternative algorithm which is somewhat less sensitive than that of System I but generates only a fraction of the alarms.

3) System III—This system employs the same sensitive leak detection algorithm as System I but inhibits leak detection during pipeline operations that can cause it to generate alarms.

4) System IV—This system normally employs the same sensitive leak detection algorithm as System I, but switches to the less sensitive algorithm of System II when it senses conditions that generate alarms.

In this example, the designers of System I have sacrificed a degree of reliability in order to maintain a high level of sensitivity, whereas the designers of System II have chosen to sacrifice a degree of sensitivity in order to achieve a high level of reliability. By simply disabling the leak detection function under certain conditions, the designers

of System III have sacrificed a degree of robustness in order to achieve higher levels of reliability and sensitivity. The example of System IV represents an attempt to selectively trade sensitivity or reliability, or both, in order to achieve a more robust system.

Although techniques vary between different software-based leak detection methodologies, most attempt to achieve an acceptable tradeoff between reliability, sensitivity, accuracy, and robustness by sensing conditions of pipeline operation that cause alarms and making temporary parameter adjustments or disabling certain functions as required. Prior to the selection of a methodology for a given pipeline system, it is important that the pipeline company understand the way all operating conditions are handled by that methodology. This understanding may help the pipeline company to determine if a solution is consistent with the target pipeline's operational characteristics, as well as the company's expectations.

The reliability of a pipeline's communication, SCADA, and instrumentation systems can also have a dramatic effect on the utility of a software-based leak detection system. A more robust system is one that is less likely to exhibit loss of functionality during periods of partial data outages caused by instrument failures, communication anomalies, routine maintenance, and so forth. Systems that continue to operate during outage periods or transient conditions on the pipeline might employ different settings for thresholds, filter characteristics, and other parameters. This usually results in some degradation of the system's sensitivity, accuracy, or reliability, or a combination thereof. In such cases, robustness is enhanced at the expense of other aspects of performance.

Consistent and reliable SCADA system performance is of critical importance to a software-based leak detection system, regardless of the methodology employed. If the quality of the data is bad, or if the data acquisition frequency is inadequate, the ability of the software to recognize a potential or actual leak condition is compromised. In addition to the physical description of the pipeline system, definition of the pipeline company's SCADA system, and its performance characteristics, are of critical importance to the leak detection vendor. This definition provides the vendor with background information necessary to determine if an existing SCADA system is adequate to support the needs of their software. SCADA performance characteristics that can have a negative effect on leak detection include slow or irregular update rates, time skew in acquired data from opposite ends of the pipeline, and communication system reliability. These, like many of the other factors, have different effects depending on the leak detection method under consideration, and therefore, should be discussed with each vendor to determine their impact on that method's functionality.

C.9 Specification and Prioritization of Performance Metrics

Within the framework of the proposed leak detection system evaluation methodology, each performance metric is evaluated in terms of a system's ability to satisfy a set of related criteria. Vendors should assist in the development of performance criteria that are relevant to their particular leak detection systems, but ultimately, it is the pipeline company that should establish specific criteria for a particular pipeline. In so doing, the company should first define their leak detection goals for the pipeline and then specify corresponding criteria relative to the performance metrics of reliability, sensitivity, accuracy, and robustness. These performance criteria constitute one set of information that the company would then provide to a potential vendor in order to determine if that vendor's system is an acceptable leak detection solution.

There are three steps involved in determining the appropriate leak detection performance criteria for a particular pipeline. The pipeline company should first identify any legal, contractual, or regulatory requirements relating to leak detection. A minimum set of performance criteria should be established to meet these obligations.

The next step is to characterize the pipeline in terms of its possible leak mechanisms and the likelihood that one of these may result in a leak. A number of diverse factors are involved in this characterization: see 49 *CFR* 195.452 (i)(3) and FAQ 9.5 for these factors.

The final step in developing performance criteria is to perform an assessment to definite potential costs associated with incorrectly declared leak alarms, missed alarms, late alarms, and any other deviation from ideal leak detection system performance. This assessment, when considered alongside the regulatory requirements and the leak potential characterization of the pipeline, could provide a basis from which the pipeline company could establish

a set of leak detection objectives. The task of defining the appropriate leak detection performance criteria could then be reduced to a process of prioritizing each performance metric in terms of its level of importance, and further defining a set of specific performance criteria that illustrate the desired objectives.

As an example, the format for presenting performance metrics and the related specific performance criteria to software-based leak detection vendors is divided into two tables as presented in Figure C.4. In the first table, each performance metric is ranked based on its level of importance to the pipeline company. Ranking of the four (4) performance metrics simply involves assignment of a numerical rank (1, 2, 3, or 4) to each, with the most important performance metric being assigned a rank of one (1).

The second table contains definitions of specific performance criteria related to each performance metric and may be optionally left blank or deferred to the vendor to complete. In this table, each performance metric may be characterized by a set of performance criteria to be evaluated under certain operating conditions on the pipeline. This criterion may be specified in either qualitative or quantitative terms. Pipeline companies are encouraged to provide qualitative specifications for performance criteria and quantitative specifications where possible. Even though many of the performance criteria are difficult, or even impossible, to completely separate from others, this mechanism provides the pipeline company with a means to identify and rank the specific elements of performance important to them and relevant to their operational needs and leak detection goals.

It should be noted that the performance criteria identified in Figure C.4 are specified in qualitative terms rather than quantitative terms and are only a representative sample of criteria that might be established under a given set circumstances. This is not an all-inclusive list that would apply to every pipeline, nor is it a recommended list with application to any particular pipeline. Since the needs of each pipeline company differ, it is only necessary to specify those performance criteria that are representative of the pipeline's specific needs.

Performance Metric	Level of Importance (Rank 1 – 4)
Sensitivity	
Reliability	
Robustness	
Accuracy	

Performance Metric	Qualitative Performance Criteria Specification
Sensitivity	Minimum detectable leak rate
	Minimum detectable leak volume
	Maximum volume loss prior to alarm
	Response time for a large leak
	Response time for a small leak
Reliability	Incorrect leak alarm declaration rate (overall)
	Incorrect leak alarm declaration rate (steady state flow)
	Incorrect leak alarm declaration rate (transient conditions)
	Incorrect leak alarm declaration rate (static conditions)
Robustness	Loss of function due to pressure outage(s)
	Loss of function due to temperature outage(s)
	Loss of function due to flow measurement outage(s)
	Loss of function due to pump state changes
	Loss of function due to valve state changes
	Loss of sensitivity due to pump state changes
	Loss of sensitivity due to valve state changes
	Startup stabilization period
Accuracy	Leak location error
	Leak flow rate error
	Leak volume error

Figure C.4—Tabular Format for the Ranking of the Level of Importance for Each Performance Metric, and an Optional Table for Qualitative or Quantitative Specification of Performance Criteria Related to Each Metric

Bibliography

[1] API 1164, *Pipeline SCADA Security*

[2] API 1165, *Recommended Practice for Pipeline SCADA Displays*

[3] API*Manual of Petroleum Measurement Standards* (sections on metering, calibration, and proving)

[4] CSA-Z662-03, [1] *Oil and Gas Pipeline Systems*

[1] CSA Group, 8501 East Pleasant Valley Road, Independence, OH 44131-5516, www.csagroup.org.

200 Massachusetts Avenue, NW
Suite 1100
Washington, DC 20001-5571
USA

202-682-8000

Additional copies are available online at www.api.org/pubs

Phone Orders: 1-800-854-7179 (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: 303-397-2740

Information about API publications, programs and services is available on the web at www.api.org.

Product No. D011302