PACIFIC GAS AND ELECTRIC COMPANY

ASSET AND RISK MANAGEMENT
DISTRIBUTION AND INTEGRITY MANAGEMENT

Attachment G

Rev 0

Monitoring for Potential Threats

3/14/2014

Contents

1.0 Purpose and Scope

The purpose of this document is to provide a process for monitoring potential threats in the Distribution Integrity Management Program. This process description includes instructions on how ongoing information from operations is gathered and reviewed. The risk evaluation and determination and threat categorization is detailed in Attachment I.

This Attachment is part of RMP-15 and PG&E's continuous effort to improve the safety and reliability of its gas facilities.

2.0 Introduction

In order to conform to the requirements in 49 CFR Part 192 Subpart P, PG&E has developed a program for monitoring data from operations to and to identify new threats and gain a greater understanding of its natural gas distribution . assets. The following sections describe the steps involved to effectively execute monitoring for new threats.

DIMP Engineering will be responsible for ongoing monitoring and logging for threats and provides a risk assessment to meet their business needs. DIMP Risk Management will utilize this information to classify the threats as known or potential and evaluate risk via the Issue Investigation Procedure outline in Attachment I.

3.0 Responsibility for Process

DIMP Engineering is responsible for the process of monitoring for new threats as described in this Attachment. DIMP Mitigation and Risk Management are responsible for the Issue Investigation Procedure (IIP), Attachment I. The IIP verifies the classification of the new threat as potential or known, evaluates its risk and determines mitigation actions.

4.0 Monitoring of Source Data

4.1 Source data is reviewed and screened for known threats. New threats and threats that DIMP Engineering deems necessary to track for their business needs will be recorded in the Identified Threat Log.

4.1.1 Examples of Known Threats to exclude from the Identified Threat Log include

Table 4.1.1 Threat Review Types for

Component	Type	Documentation	Exclusion Examples
Fittings	Asset	Multiple MPRs, existing PHMSA Reports	Aldyl-A Service Tees
Pipe	Asset	Multiple MPRs, existing PHMSA Reports	Aldyl-A Pipe

Late Maintenance	Operations	Gas CAP, Bi-Monthly CAP audits, CPUC audits	Late valve maintenance, leak survey
CP Down	Operations	Gas CAP, Bi-Monthly CAP audits, CPUC audits	Contacts, exhausted anodes

4.1.2 Other threats can be monitored via this process at DIMP Engineering or DIMP Risk Management's discretion.

5.0 Source Data to be monitored and Schedule

5.1 The following table lists the source data to be monitored and the minimum frequency of monitoring.

Data Base	Monitoring Interval	Group Responsible
PHMSA Bulletins	Annually	DIMP Engineering
NTSB/Accident Reports	Quarterly	DIMP Engineering
DIMP Field Review	As Performed	DIMP Risk Management
Material Problem Reports	Quarterly	DIMP Engineering
Gas CAP Reporting	Quarterly	DIMP Engineering
Potential Threat Log	Annually	DIMP Engineering

5.2 If additional data sources are identified prior to the next revision of this document they will be added to the monitoring process.

6.0 File Management

6.1 The monitoring log and the Identified threats log are maintained in an Excel file at this Share Point or its equivalent:
DIMP TEAM Project Tracking > Asset Engineering > Performance Trending - Asset Engineering > Process Monitoring Log

6.2 Monitoring activity is documented on the tab labeled "Process Monitoring Log" and new threats identified documented on the tab labeled " Identified Threat Log."

6.3 The file name is 'MonitoringLog Year-Month.xls." The file is to be appended with the current quarter at the time of each review and the previous version archived.

7.0 Process Monitoring Log

7.1 At minimum the required information identified in the headings in the Quarterly Process Monitoring Log.

7.2 The process or asset owner, or qualified alternative will be responsible for monitoring the data.

7.3 Source data - this identifies the source data to be monitored by the process or asset lead.

7.4 Quarter-Year column heading refers to the quarter and year of the source data. This is not the review date.

7.4.1 Lan ID - the LAN ID of the person conducting the source data review.

7.4.2 Date - the date that the review was conducted.

7.4.3 Issue #? - This corresponds to the issue number in the Identified Threat Log.

7.4.3.1 The reviewer will enter the existing issue ID for any previously identified threats that are observed in the current review of the source data

7.4.3.2 If a previously unidentified threat was observed, the reviewer will log the threat in the identified threat log and assign the next sequential ID number.

7.4.3.3 If no threats are observed in the review of the source data the reviewer will enter "N".

8.0 Identified Threat Log

8.1 At minimum the required information identified in the headings in the Identified Threat Log.

8.2 Issue ID – A sequential number assigned to threats as they are observed.

8.3 Threat Category – one of eight threat categories defined in 49CFR 192.1007(b).

8.3.1 Corrosion

8.3.2 Natural Forces

8.3.3 Excavation damage

8.3.4 Other Outside Force damage

8.3.5 Material or Weld

8.3.6 Equipment Failure

8.3.7 Incorrect Operation

8.3.8 Other

8.4 Process or Asset Lead Name

8.5 Threat description – Brief description of the threat. This section should identify the affected asset which the threat is related. For example: Threaded joints at customer meter sets increased leak rate due to deteriorated pipe dope.

8.6 Date Raised – Date the threat was recognized in the monitoring program

8.7 Date Reviewed- The date the threat was assigned for risk evaluation.

8.8 CAP Number – Gas CAP identification number from SAP, if the issue was identified via CAP.

8.9 Data Source – Where the threat was found. (MPRs, PHMSA bulletin etc)

8.10 Actions: (Date, LAN, Note) this field is used to capture follow-up actions on identified threats. The protocol for entering data is the date of entry, LAN ID of the person making the entry, the text of the action.

8.11 DIMP Risk Management – Documents the date, person performing the review and IIP tracking number if DIMP action is required.

9.0 Issue Investigation Process

9.1 The result of monitoring will be reviewed at minimum annually by DIMP Risk Management for the evaluation of risk and development of mitigation plans on an annual basis at minimum. Critical items requiring immediate action will be communicated as found.

9.2 DIMP Risk Mitigation will review the log file and follow the process outlined in Attachment I, Issue Investigation Procedure.

9.3 The result of DIMP's review will be made available to DIMP Engineering.

10.0 Archiving of Data Sources and Results

10.1 Copies of source data sets reviewed in the course of this procedure and the monitoring log will be saved in the DIMP team Project tracking SharePoint at the following link or its equivalent: DIMP TEAM Project Tracking > Asset Engineering > Performance Trending - Asset Engineering > Process Monitoring Log.

10.2 Each data source and log version will be downloaded and saved to the SharePoint during the review process, with the exception of SAP records. These records will be maintained for 10 years.