Evans Roger

From: rmooney[redacted]
Sent: Tuesday, October 16, 2018 1:23 PM
To: Evans Roger
Cc: [redacted]
Subject: Re: PLD18MR003 -- Merrimack -- Questions related to Risk Assessment

Roger, please find the answers to your questions below. In additions to reviewing the answers to the specific questions, I suggest you review CMA's Distribution Integrity Management Plan "DIMP which is on the Accellion Site in the Pipeline Integrity folder, and the "South Union St Project Work flow Data request" document, which is in the operations folder and the Work order approval flow subfolder. These documents provide a good overview of CMA's risk assessment and capital engineering / construction processes.

1(a). First, Jeff C told us that there are annual risk assessments of the regulators themselves and that specific risk scenarios are presented for each regulator (master/worker). Are the annual risk assessments in the M&R group shared with the engineering group? Yes.
1(b). Also, we understand the spreadsheet was supplied, can you assist with the file name so that we can retrieve the document? There are four documents related to regulator risk modeling on the Accellion Site in the "Pipeline Integrity" folder. The document labeled "Columbia Gas Regulator Risk Model" provides an overview of the process. The other three documents labeled risk model show the 2016 results, 2017 results and the year over year change. Please review the segment level risk assessment within CMA's DIMP plan as well.

2(a). When engineering packages are produced, such as a package for pipelines that are to be abandoned, does Columbia use a management of change system/modification procedure to manage the modification to the gas main? Yes. The scope of the modification procedures depends on the modifications being made. Please refer for instance, to the document labeled "South Union St Project Work Flow Data Request" on the Accellion Site. As shown in that document, Columbia Gas has a formal capital project close-out process to ensure that proper documents are included in the project package and that the systems of record (i.e. Work Management and GIS systems) are updated with as-built information.
2(b). Do you conduct risk assessments as part of your management of change, such as when modifications are made to your distribution system? Yes. Once again the scope of the risk assessment depends on the modifications being made. For instance, within CMA's DIMP, risk assessments are performed at a segment and system level. These levels are explained within CMA's Distribution Integrity Management Plan ("DIMP"), which can be found on the Accellion Site in the Pipeline Integrity folder. As it relates to mains and services, risk is assessed at the segment and system level taking into consideration probability of failure and consequence of failure. There are several risk profile factors that, if changed during a system modification, are incorporated into the risk model. These risk profile factors are discussed in CMA's DIMP. In addition, please refer to the document labeled "South Union St Project Work Flow Data Request," as mentioned earlier, which walks through CMA's life cycle of a project from concept to close out.

3. If a change management/mod package is used, are these packages shared with the M&R group? Yes. Depending on the nature and scope of the work involved the package would be shared with the M&R department.

4. When a pipe replacement/ abandonment project is created, is a risk assessment done? Yes. As risk relates to the CMA's DIMP, a risk assessment is done to help prioritize pipe replacement / abandonment projects. With regard to risk assessment as part of the management of change (i.e. modifications to our distribution system) refer to the response to question 2. In additional to DIMP, during the pipe replacement / abandonment project creation process, risk assessments are performed to ensure system reliability, operability, and safety.

5. When CMA performs risk assessments, do they have common mode failure/common cause failure scenarios (A common cause failure occurs when several failures have the same origin)? If yes, please provide examples and documentation to that effect.

Common failure mode explanation (how we view this terminology)
A common cause failure occurs when several failures have the same origin. Common cause failures are either common event failures, where the cause is a single external event, or common mode failures, where two systems fail in the same way for the same

reason. Common mode failures can occur at different times because of a design defect or a repeated external event. Common event failures reduce the reliability of on-line redundant systems but not of systems using off-line spare parts. Common mode failures reduce the dependability of systems using off-line spare parts and on-line redundancy.

The CMA risk analysis method is based on a data driven, SME validated approach. Risk is classified by asset and threat. This system-level process, primarily based on leak reports, provides a high level assessment of the risk profile associated with each threat category and asset group, regardless of whether the failures involved share geographical context. This evaluation considers all threat categories and all distribution facilities. The results of the evaluation will enable the Company to focus efforts on those asset groups and threats posing the greatest risk. Please refer to the CMA's DIMP on how risk is quantified and prioritized.

An example of a common mode failure scenario is leakage on bare steel pipe due to corrosion. These failures can occur at different times, in different areas, and involving different vintages of pipe. The asset and threat associated with these failures are common, and the risk analysis method can aggregate the data to determine risk.

An example of a common cause failure scenario would be other outside force damage on customer meter sets. This threat may occur when the Company's gas facilities are damaged by motorized vehicles or equipment not engaged in excavation. An example of such an occurrence would be damage to a meter set caused by vehicle impact. Such a failure could lead to several failures simultaneously to the meter set, riser, service line, etc.

The Company uses two risk evaluation processes, a system-level and a segment-level process. The system-level process is described above in this response. The segment-level process takes those system level risks and within that asset and threat combination, helps to prioritize the segments/areas of that specific system level risk. These two processes are assessed in parallel, and the results of each are used to add value to each other.

Please let me know if you have any additional questions or would like to discuss.

Rob Mooney
VP, Engineering and Pipeline Safety
NiSource, Inc.
[redacted]

From: [redacted]

[redacted] CAUTION: This email was sent from an external source. Think before you click links or open attachments. If suspicious, please forward to [redacted] for review.

Rob,

This is yet another one of those rare situations that requires a quick turnaround. **Can we have a response by 1:00 pm tomorrow?**

During the interviews of Louie R and Jeffrey C, we learned that pipe replacement packages are prepared that impact regulators and sensing lines.

1. First, Jeff C told us that there are annual risk assessments of the regulators themselves and that specific risk scenarios are presented for each regulator (master/worker). Are the annual risk assessments in the M&R group shared with the engineering group? Also, we understand the spreadsheet was supplied, can you assist with the file name so that we can retrieve the document?

2. When engineering packages are produced, such as a package for pipelines that are to be abandoned, does Columbia use a management of change system/modification procedure to manage the modification to the gas main? Do you conduct risk assessments as part of your management of change, such as when modifications are made to your distribution system?
3. If a change management/mod package is used, are these packages shared with the M&R group?
4. When a pipe replacement/ abandonment project is created, is a risk assessment done?
5. When CMA performs risk assessments, do they have common mode failure/common cause failure scenarios (A common cause failure occurs when several failures have the same origin)? If yes, please provide examples and documentation to that effect.

Common failure mode explanation (how we view this terminology)

A common cause failure occurs when several failures have the same origin. Common cause failures are either common event failures, where the cause is a single external event, or common mode failures, where two systems fail in the same way for the same reason. Common mode failures can occur at different times because of a design defect or a repeated external event. Common event failures reduce the reliability of on-line redundant systems but not of systems using off-line spare parts. Common mode failures reduce the dependability of systems using off-line spare parts and on-line redundancy.

Thank you.
Roger

Roger D. Evans
Senior Pipeline Incident Investigator
National Transportation Safety Board
Office of Railroad, Pipeline, and Hazardous Materials Investigations
[redacted]