The Case for Continuous Reassessment of Risk in Managing Pipeline Integrity

A Dynamic Risk White Paper Document

July 29, 2009
The practice of employing risk assessment as a tool for developing assessment plans has been universally accepted by gas pipeline operators in the United States with the adoption of Subpart O in Part 192, and by liquids pipeline operators by the adoption of 195.452. Now that baseline assessment plans have been developed, however, some operators may question the merit in conducting ongoing risk assessments. This white paper endeavours to address this concern by identifying and discussing the rational basis for this practice.

As outlined in Clause 5.3 of ASME B31.8S, there are six main objectives for risk assessment in pipelines and related facilities. These are:

1. Prioritization of pipelines / segments for scheduling integrity assessments and mitigating action;
2. Assessment of the benefits derived from mitigating action;
3. Determination of the most effective mitigation measures for the identified threats;
4. Assessment of the integrity impact from modified inspection intervals;
5. Assessment of the use of or need for alternative inspection methodologies; and,
6. More effective resource allocation

The overriding functional benefit of managing integrity through risk assessment is that it provides a basis for evaluating both the potential impact of different incident types and the likelihood that such events may occur. Furthermore, it does this in a manner that is rational, defendable and consistent. The following principals justify reassessment of risk on an ongoing basis and are an inherent part of an effective risk assessment strategy:

Accommodation of Continuous Improvement

In a dynamic environment such as a transmission pipeline, change is not only necessary, it is sought after in the pursuit of continuous improvement. Therefore, risk assessment should not be thought of as a one-time event. Rather, it is a tool that needs to be repeatedly deployed in a dynamic environment in order to stay abreast of the following:

- Changes in data quality and accuracy;
- Creation of new HCAs, reclassification of HCAs, or changes in HCA boundaries;
Changes in operating conditions (operating pressures, product stream composition, emergency response procedures, operating procedures, etc.);

Acquisition of new assessment data;

Changes in assessment effectiveness or reassessment interval;

Changes in physical plant (coatings, replacements, repairs, valves, etc.); and,

Refinement of knowledge (types of threats, magnitudes of threats, growth rates for time-dependent threats, locations, types and magnitudes of consequences, assessment and mitigation effectiveness, etc.)

Companies typically go to great lengths to ensure that the data attributes of risk are maintained in a database that can be updated on a regular basis. It is in the pursuit of the goal of continuous improvement that this is done, and it is with a view to supporting the continuous re-evaluation of risk. If risk assessment was a one-time event, such measures would not be necessary.

Identification of Effective Strategies Through Risk Trending

The risk assessment cycle provides a vehicle through which changes in operational risk with time can be tracked. This fosters an understanding of the cause and effect relationship that exists between specific integrity management strategies relative to the overall goal of continuous improvement through risk reduction. By undertaking such trending analysis, best-practice assessment and mitigation approaches can be identified on the basis of cost benefit. This can be done by identifying specific strategies that are most effective in achieving the greatest risk mitigation for a given expenditure of resources.

Refinement of Risk Algorithm

One of the most important steps in an effective risk analysis, and one that is often overlooked is the recalibration of the risk model through feedback. A risk assessment algorithm is essentially the basis of a logical model that estimates risk through the assimilation of risk attributes. Such models should never be considered to replicate real-life conditions perfectly, but are at best, approximations of reality. With the passage of time, and the accumulation of feedback, data, and experience, risk algorithms should be fine-tuned and recalibrated so that they provide greater levels of predictive capability and resolution among segments. Effective feedback is an essential process component in continuous risk model validation. In addition, the model must be adaptable and changeable to accommodate new threats.
Assessment and Risk Mitigation Program Refinement

As new information becomes available that may impact an understanding of risk along a system, it may at times be prudent to re-evaluate assessment and mitigation plans in terms of the order of priority and/or the most effective assessment or mitigation measure to be employed. This may be justified by the identification of new threats, changes in the understanding of the magnitude of a given threat, or changes in consequences. Further refinements may be made through what-if analysis through which the effects of changes over time and the risk reduction benefits from maintenance or remedial actions are investigated. Assessment and risk mitigation plans should never be considered static, or as an ever-repeating cycle year-over-year. A regular re-evaluation of new data and refinement of approach is necessary to ensure that the goal of continuous improvement through risk reduction is met.

As seen below, the Integrity Management Plan Process Flow Diagram, shown as Figure 2 in ASME B31.8S conveys a continuous process in which the re-evaluation of risk is an essential element.

Without the basic tenet of continuous re-evaluation of risk, the above principals of effective integrity management would be violated. From this necessity, risk assessment must be considered a process – not an event!