

## BIOGRAPHICAL INFORMATION

Ron Brush  
President  
New Century Software, Inc.

### Specific Responsibilities

Founded New Century Software ten years ago to provide GIS consulting, data conversion and software development services to the oil and gas pipeline industry. Responsibilities include management of company operations, strategic planning, GIS consulting, business development and project management. Recently founded New Century Field Services, Inc. to provide integrity management field mapping services for pipeline operators.

Mr. Brush has 13 years experience implementing GIS on more than 100,000 pipeline miles in North America including the development of enterprise GIS maintenance and mapping software, GIS data conversion and data integration. Areas of expertise include enterprise GIS implementation consulting, GIS database modeling, integrity management, data and application integration and software design. Mr. Brush helped develop a core database model that is currently in use by many major national pipeline companies to spatially enable corporate enterprise-wide facility database and GIS systems.

In 1998, Mr. Brush helped initiate the PODS Association, Inc. ([www.pods.org](http://www.pods.org)), serving as president in 2001 and is currently serving as Treasurer. As an active member of the association, he has contributed to the technical design and currently leads advanced PODS training workshops.

### Past Experience

Various positions with M. J. Harden Associates

### Educational Information

B.S. - Mathematics, Colorado State University, concentration computer graphics

### Professional Memberships

GITA, NACE, Common Ground Alliance, PODS Association

# A NEW THREAT CATEGORIZATION SYSTEM FOR RISK ASSESSMENT

**Presented by Ron Brush**

President

New Century Software, Inc.  
2627 Redwing Road, Suite 100  
Fort Collins, CO 80526  
970-267-2000

[www.newcenturysoftware.com](http://www.newcenturysoftware.com)

[ronb@newcenturysoftware.com](mailto:ronb@newcenturysoftware.com)

## ABSTRACT

This presentation will focus on an improved technique for categorizing pipeline threats and consequences for pipeline risk assessment. Building on the threats identified in ASME B31.8S, API 1160 and other sources, the benefits of a new standardized risk categorization system will be demonstrated through the use of an example case study. This presentation will include a discussion on database modeling of risk evaluation segments with regard to quantifying threats and consequences and their relationship to pipeline attributes and spatial data. The value of this system will be demonstrated by extending its use to monitor pipeline anomalies and track leaks as well as aid in pipeline reroute location selection, risk mitigation and new pipeline route identification using GIS. This system will also aid in risk management as pipeline assets are transferred between operators. This presentation will benefit pipeline personnel who are responsible for managing pipeline integrity and those who are responsible for managing the pipeline data that is used in risk assessment.

## **INTRODUCTION**

The Pipeline Industry is facing sweeping new data management and data integration challenges as a direct result of recent integrity management rules. These rules are causing gas and liquid pipeline operators to rethink data management practices and to consider new methods for tracking pipeline threats, consequences, leaks and anomalies, as well how this data is stored.

This paper presents a new method for identifying and tracking threats and consequences for pipeline segments. This method is referred to as the Standard Integrity Classification System (SICS).

### **WHAT IS RISK ASSESSMENT?**

Kent Muhlbaier defines risk assessment as “an analytical process by which an operator determines the types of adverse events or conditions that might impact pipeline integrity. It also determines the likelihood or probability of those events or conditions that will lead to a loss of integrity and the nature and severity of the consequences that might occur following a failure.”<sup>i</sup> He adds, “Risk is increased when either the probability of the event increases or when the magnitude of the potential loss increases.”<sup>i</sup> While this definition implies that the pipeline threats and the consequences of a release are measurable and quantifiable, it also promotes the notion that these threats and consequences are consistently defined across the pipeline system across varying types of operating environments and engineering design conditions.

ASME B31.8S states, “Information integration is a key component for managing system integrity. A key element of the integrity management framework is the integration of all pertinent information when performing risk assessments. Information that can impact an operator’s understanding of the important risks to a pipeline system comes from a variety of sources.”<sup>ii</sup>

### **COMMON REFERENCES FOR PIPELINE THREATS**

In recent years there have been many standards and papers published that list and describe various pipeline threats and consequences. ASME B31.8S-2001, Appendix A lists nine (9) primary threats. Dr. Kiefner lists 21 threats<sup>iii</sup>. API 1160 lists approximately 15 threats and other documents describe variations of these in varying detail.<sup>iv</sup> These threats and causes are also listed on the DOT Gas Incident Form RSPA F 7100.2, under part F – Apparent Cause<sup>v</sup> as well as Liquid Incident Form RSPA F 7000-1, part H – Apparent Cause<sup>vi</sup>. Other sources for these threats include API Pipeline Performance Tracking System<sup>vii</sup>, NACE, Common Ground Alliance and many other technical articles and papers.

An important key to integrating data for the purpose of assessing pipeline threats is the normalization of the threats and causes – the ability to relate them to actual physical and location data and the ability to clearly communicate, articulate, defend and define them at the appropriate level of abstraction for a given purpose.

The somewhat subjective nature of threats and consequences itself is a challenge to normalize. When less information is known, it is important to indicate that lack of knowledge; likewise when more specific information is known this knowledge should be retained and used to further characterize threats and actual discovered occurrences of anomalies and leaks. Because of this, a hierarchical (tree view) approach to normalizing these data is appropriate. Parent nodes indicate a broader scope with less specific knowledge. Child/Leaf nodes indicate detailed and specific knowledge. The more granular and detailed nodes more closely correspond with physical pipeline and environmental attributes.

## **THE SICS IDEA**

The Standard Integrity Classification System (SICS) was designed to provide an exact qualitative means of describing, storing and organizing pipeline integrity threats and consequences.

Following are some of the important features of SICS:

- Based on Existing Pipeline Integrity Standards  
SICS is based on multiple combined pipeline standards including ASME B31.8S, API 1160 and many other industry reference documents
- Hierarchical – moving from less to more detail as you drill down  
SICS is hierarchical allowing the user to indicate the exact type of information that is known about the threat or consequence. The further down the hierarchy one goes, the more detailed and specific knowledge can be recorded.
- Numeric – specific, quantifiable, well-defined  
Each SICS code is well-defined based on existing standards. This provides the ability for different operators to know exactly which threat or consequence has been recorded, avoiding differences in nomenclature arising from different standards and contexts.
- Multi-purpose
  - Threat Index  
When used as a threat index, SICS codes describe specific pipeline threats. These threats can be directly assigned to ILI anomalies, assigned during routine inspections or assigned based on existing pipeline data or environmental conditions.
  - Actual Cause – primary and contributing factors  
When used as a cause index, SICS codes describe specific causes of pipeline leaks or anomalies. This allows actual leaks to be directly compared with predicted threats.
  - Risk weighting  
Each item can be assigned an appropriate risk weighting factor.
  - New Pipeline Site Selection  
SICS codes can also be used to describe risk conditions related to planned pipeline construction – providing the ability to mitigate risk during the route planning phase for new construction or route planning for pipe reroutes.

- Standard Exchange between Operators as pipelines are bought and sold – consistency between threat/cause analysis

As pipeline assets are bought and sold, specific integrity threats and consequences, stored as a SICS code can be transmitted along with the database to ensure that vital pipeline integrity information is not lost in translation.

### EXAMPLE USAGE

Figure 1 illustrates the SICS hierarchy tree for time dependent threats/causes. While the other threats in this tree are not shown this illustrates the idea that if External Corrosion is a known threat, then the operator can indicate so by describing it using SICS code 1. If “Disbonded Coating” is a known threat because of the operating environment, type of coating, soil type and other special knowledge, then this knowledge can be indicated by using the SICS code 1.1.1.2. Likewise after investigating an anomaly, a cause described by SICS code 1.2.2 would describe this cause as External Corrosion resulting from Stray Current caused by Foreign DC current. This is useful information that can be used in the future to better integrate data using prior knowledge and experience to improve the ability to describe and predict potential increased threat. Therefore, each segment has the ability to be associated with one or more threats.

In addition, when reporting on pipeline threats, detailed threats can be easily summarized into higher-level categories, providing drill-down capabilities when needed. Thus the operator can report on only the high-level threats for the entire pipeline system, but drill-down to specific threats on a particular segment.

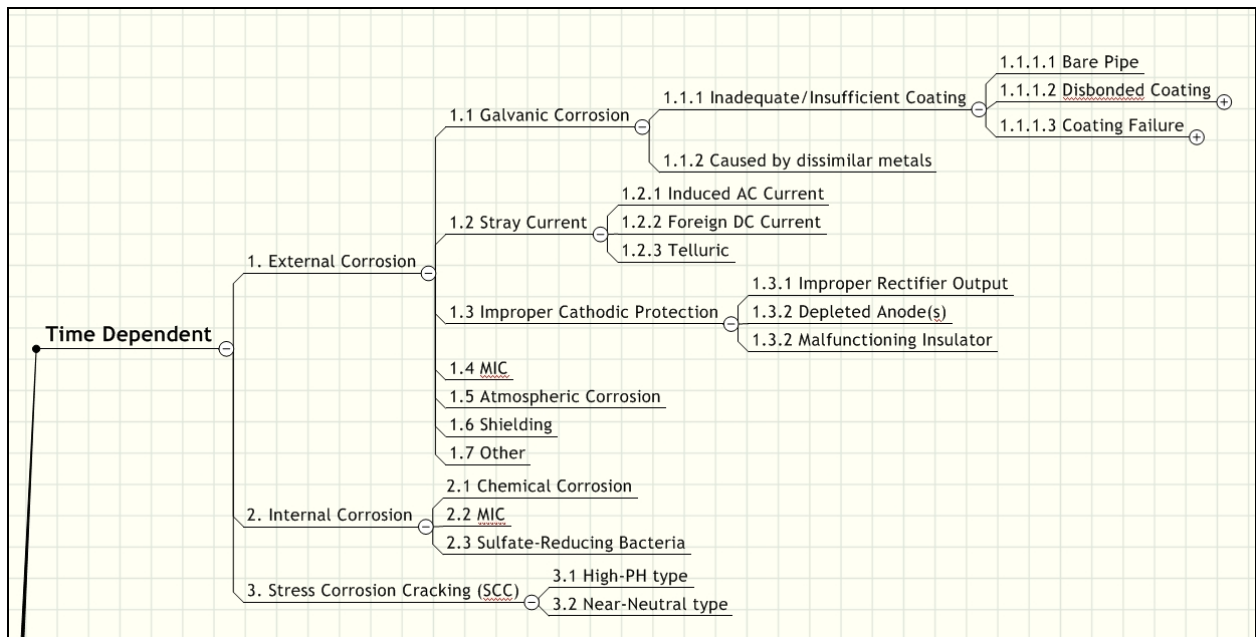


Figure 1. Example of SICS Time Dependent Threats

## **ALIAS**

The idea for SICS traces back to the ALIAS<sup>viii</sup> (Anomaly Library for Inspection Assurance Standards) convention for classifying pipeline anomalies. The ALIAS indexing methodology uses ten (10) categories that provide more than 200 different anomaly and feature types at varying levels of detail. This three-tier indexing system provides each feature with the following:

- Classification – general or characteristic or function
- Category – specific function, characteristics, or degradation mode/cause
- Type – specific feature or anomaly

Rather than a three-tier notation, the SICS convention uses a dot notation, providing for many hierarchy levels with many features on each level.

The genesis of the idea came during a Pipeline Geohazards conference in London, where myriad geohazards were discussed at great length. Combining the hierarchical approach used by ALIAS with existing standards resulted in a SICS method of identifying pipeline threats. This idea was expanded to pipeline consequences later.

## **CASE STUDY**

The SICS approach described in this paper has been successfully implemented on a PODS database through a web-based tracking system for pipeline risk assessment and leak tracking for a large gathering pipeline system. Using the SICS codes, threats for individual segments of pipe are evaluated by using a hierarchical tree view as illustrated in Figure 2 below. This diagram illustrates three threats that have been identified for a given pipeline segment, each at a different level of the SICS hierarchy:

Segment Threats:

- 1.1.1 Inadequate/insufficient coating
- 1.3 Improper Cathodic Protection
- 4 Manufacturing Threat

Note that when selecting 1.1.1, the user does not need to select checkboxes for 1 and 1.1.

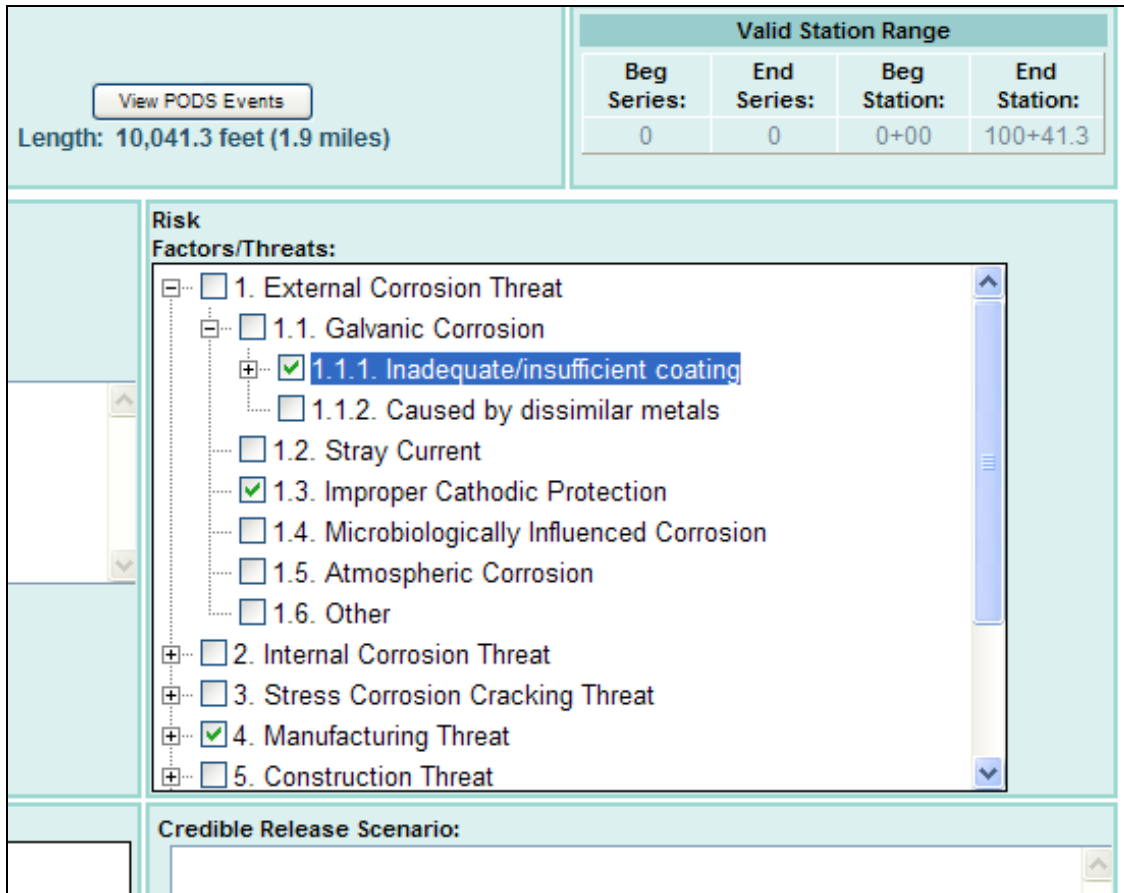


Figure 2. Example Web Page Screen

When tracking causes of leaks, the user is required to select only one primary cause and is given the same selection tree view to indicate contributing causes. The user may enter several causes suspected for newly identified anomalies. This natural linkage of threat and cause will, over time, provide an improved means of determining threats by comparing similar attributes on the pipeline with actual causes vs. predicted threats.

### CONSEQUENCES

Similarly, consequences as described in API 1160, ASME B31.8S and other standards documents have been indexed using the SICS methodology. Like threats, these well-defined codes can be used to describe the level of knowledge about particular consequences of release events at a detailed or higher level.

### PIPELINE ROUTING AND GIS

The SICS approach can also be applied when performing site selection for new pipeline construction or larger reroutes. Using GIS base map data to describe threats (e.g. third-party damage) or consequences (e.g. proximity to higher population), SICS values can be assigned geographically to regions that are used for pipeline route selection optimization. This is particularly useful for outside force threats and geotechnical hazards. Each of

these hazards can be weight-ranked and used to create a risk cost surface for pipeline site selection.

### **FUTURE DIRECTIONS**

While the standards documentation might lead one to believe that all of the known pipeline threats have been identified, the reality is that SICS must continue to evolve and mature as new threats and consequences are identified. Using a hierarchical system provides a well-ordered mechanism for organizing data, but would have limitations if certain threats defy this type of organization. As described in this presentation, SICS is at version 1.0.

Looking forward, it is the hope of the author that a standards group(s) would adopt this indexing scheme for incident reporting, threat documentation and recommended data management practices. Obvious benefits would be reduced reliance on high-level descriptions (such as “Third-party Damage”) and preferred use of detailed code values that explicitly describe each condition.

### **CONCLUSION**

The Standard Integrity Classification System (SICS) system provides pipeline operators and service providers a well-defined methodology for describing, storing and classifying threat and consequence conditions along the pipeline that together are used to quantify pipeline integrity risk.

Pipeline operators will benefit by using a standardized comprehensive list of threats that can be easily shared as pipelines are bought and sold. In addition, service providers can consistently categorize identified threats between their customers.

This system has been successfully used in a PODS database and implemented on a web-based application so that authorized personnel can evaluate and more accurately describe threats on individual sections of pipeline.

## ***REFERENCES***

---

- <sup>i</sup> Muhlbauer, W.K., “Pipeline Risk Management Manual,” Third Edition, Gulf Publishing Co. 2004
- <sup>ii</sup> American Society of Mechanical Engineers, ASME B31.8S-2001, “Managing System Integrity of Gas Pipelines”, 2001, Supplement to ASME B31.8
- <sup>iii</sup> Kiefner, John F., Trench, Cheryl J., “Oil Pipeline Characteristics and Risk Factors: Illustrations from the Decade of Construction”, American Petroleum Institute, 2001
- <sup>iv</sup> American Petroleum Institute, API Standard 1160, “Managing System Integrity for Hazardous Liquid Pipelines”, First Edition, November 2001
- <sup>v</sup> Incident Report – Gas Transmission and Gathering Systems, US DOT, Form RSPA F 7100.2 ( 01-2002 )
- <sup>vi</sup> Accident Report – Hazardous Liquid Pipeline Systems, US DOT, Form RSPA F 7000-1 (01-2001)
- <sup>vii</sup> PPTS – Pipeline Performance Tracking System
- <sup>viii</sup> ALIAS, “Anomaly Library for Inspection Assurance Standards” – [www.pipelinealias.com](http://www.pipelinealias.com)
- <sup>9</sup> “Safety Performance and Integrity of the Natural Gas Distribution Infrastructure”, January 2005, American Gas Foundation, Prepared by URS Corporation