

Make the Most Out of Process Safety and Operability Information

When information is organized and accessible, more people will use it and thus be better informed. Better information means better decisions, which results in safer facilities and more efficient operations.

V. ANTHONY CILIBERTI, P.E.
RELIABILITY DYNAMICS

TODAY, THE CHEMICAL PROCESS INDUSTRIES (CPI) have a wealth of process safety and operability information (PSOI) at their disposal. Unfortunately, this information is not being fully utilized due to inefficiencies in data management. PSOI is typically kept in a variety of media and data formats and is difficult to access, correlate and maintain. Many electronic PSOI data sets do not contain discrete parameters for correlating them with other information. HAZOP studies, for example, use a nodal analysis method that fails to explicitly identify process equipment items and safeguards and their roles in fault, event and consequence sequences. As a result, it is rare that all applicable PSOI is pulled together for decision-making purposes because doing so would require a herculean manual effort. The good news, however, is that current information technology can make this information readily available.

This article will discuss the use of a hierarchical functional location structure to represent an enterprise in its entirety and identify risk levels at any point within that enterprise. Also covered will be: methods for efficiently converting legacy PSOI into relational data sets and for dynamically interfacing multiple relational PSOI data sets with each other and with enterprise data; the advantages of using a universal risk matrix as one standard of measure for different risk assessment methodologies and data sets; and how to measure and determine the criticality of safeguards and use these data to prioritize operations and maintenance activities.

Defining common reference points

An enterprise should have a common system of reference for identifying all of its assets. This is done by creating unique master records for each technical object. As defined in the popular SAP R/3 plant maintenance module, technical objects are either functional components of process systems (functional locations) or individual physical objects that execute process functions (equipment). They are organized in hierarchical structures, with one functional location hierarchy comprising the primary structure that represents asset functionality. Equipment hierarchies (equipment and sub-equipment) are installed within the function location hierarchy at the points at which they execute their respective functions.

To make it usable as described in this article, the functional location structure must be configured so it captures all facets and components of a corporate business unit in a hierarchical manner, including administrative areas, processing areas, utilities, etc. (Figure 1). Top-level functional locations identify facility areas, or functional area locations (FALs), while bottom-level functional locations identify individual equipment functions, or functional equipment locations (FELs).

It is important to distinguish between FELs and equipment. FEL identifies the process function, whereas equipment identifies the physical asset performing that function. Equipment items are installed in FELs. The data relationship between FELs and equipment can have one-to-many cardinality, but if done rigorously, has one-to-one cardinality. Cardinality is a structural constraint in a database that specifies how many of

one record type relate to the other and vice versa. A typical workplace is an example of one-to-one cardinality — one employer, many employees. By contrast, engineering contractors have many-to-many cardinality with clients — one contractor can work with one or more companies and vice versa.

A hierarchical technical object structure allows a stakeholder to review data associated with any bottom-level FEL or to sum attribute data at higher-level “parent” functional locations. Parent functional locations contain all of the data applicable to each of their respective “child” functional locations, while the child functional locations inherit data applicable to their respective parent functional locations.

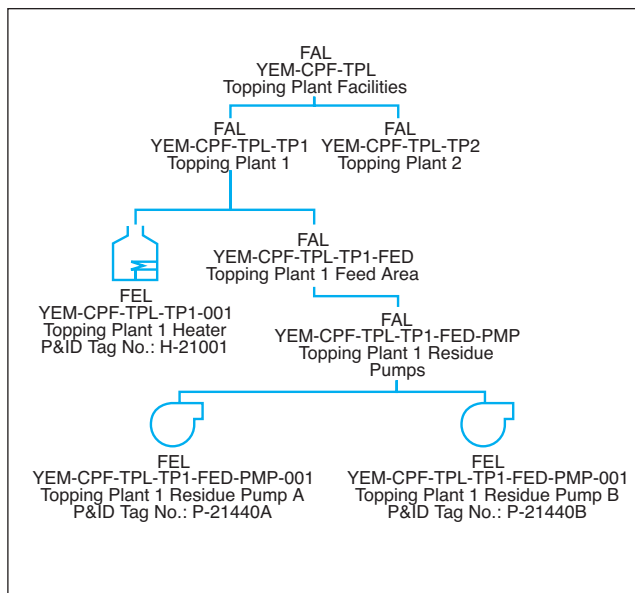
Classifying technical objects

Logic to store and classify data associated with technical objects is necessary to make the data readily accessible, retrievable and comparable between similar technical objects. Such logic, called taxonomy, is structured hierarchically and based on the characteristics of technical objects (1). Characteristics are grouped together into unique taxonomy identifiers, or classifications, within a taxonomy hierarchy. The data relationship between technical objects and classifications has cardinality of many-to-many as does the relationship between classifications and characteristics.

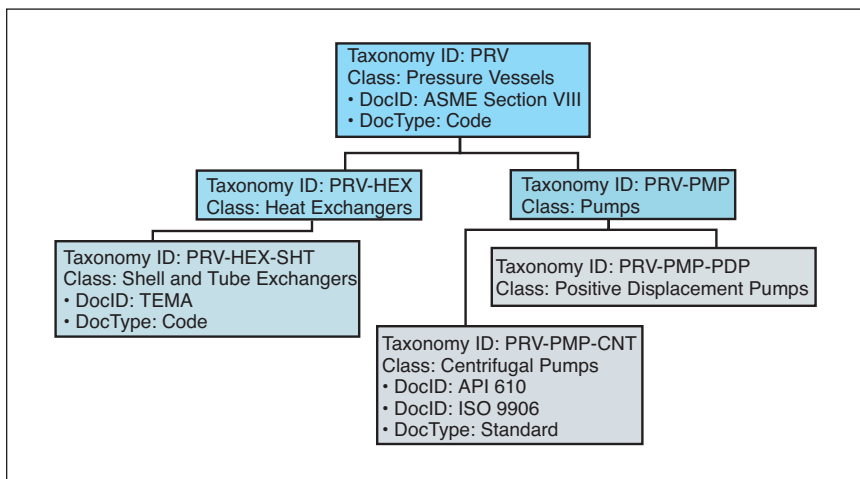
One or more characteristic values can be assigned either as tabular relationships at the classification level or at the characteristic level. Tabular relationships can be represented by entity relationship (ER) diagrams, which are essentially blueprints of the database (2). A simplified ER diagram showing technical object relationships can be found on www.cepmagazine.org.

Characteristic values assigned at the classification level in a taxonomy should be inherited by the lower-level classifications and roll up to the higher-level classifications. Figure 2 illustrates inheritance and roll-up of documents assigned at the classification level, in this case codes, standards, and recommended practices. The pressure vessel code, ASME Section VIII, is assigned at the top level of taxonomy (Taxonomy ID: PRV) and is inherited by all child branches (all pressure vessels). All assigned and child attributes (ASME Section VIII, TEMA, API 610, and ISO 9906 in the example) are part of the roll-up for Taxonomy ID: PRV, which gives a complete listing of all codes, standards, and recommended practices applicable to pressure vessels for this simplified example. Assignment of Taxonomy ID PRV-PMP-CNT to the functional location YEM-CPF-TPL-TP1-FED-PMP in Figure 1 makes two standards and one code (API STD 610, ISO 9906 and ASME Section VIII in Figure 2) all applicable to Pumps P-21440A/B in Figure 1.

Characteristics assigned at the classification level in a taxonomy should be inherited by the lower-level child identifiers,



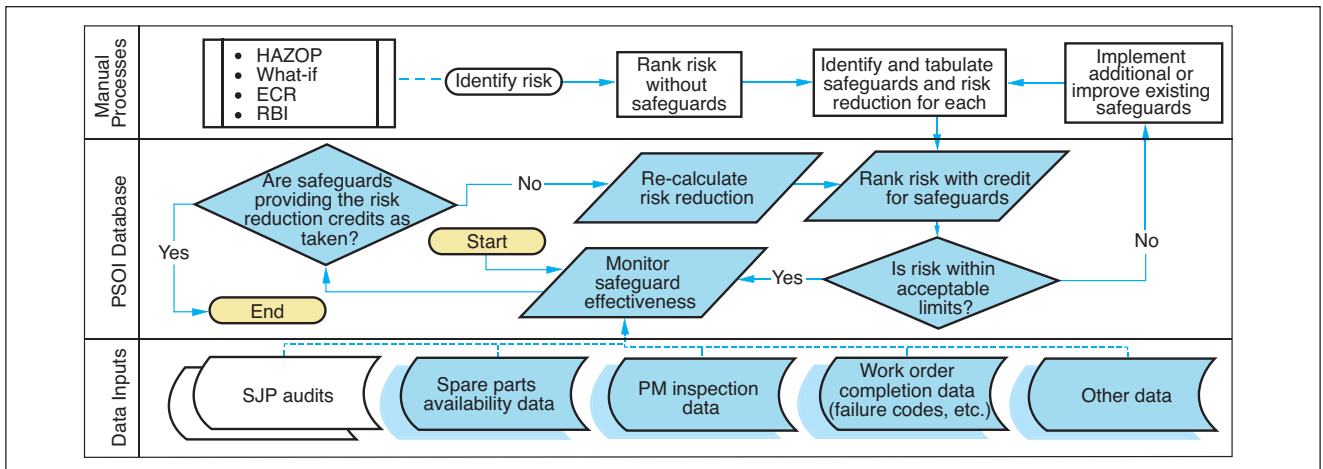
■ Figure 1 (above). Example of a functional location structure.
 ■ Figure 2 (below). Simplified example of a technical object taxonomy.



but characteristic values assigned to characteristics should not be inherited. For instance, the characteristic MAWP assigned to Taxonomy ID PRV in Figure 2 is inherited by all lower branch Taxonomy IDs, but the MAWP values, which can be different for each technical object, are not inherited. A complete example of a taxonomy structure is given in “Guidelines for Process Equipment Reliability Data with Data Tables” (1).

Preparing and interfacing data

PSOI is maintained in most facilities in a variety of media, which can be categorized as hardcopy files, non-relational electronic data (e.g., scanned images and free-formatted text files) and database applications (e.g., enterprise applications or single-user products). Hardcopy and non-relational files should be reformatted where practical into relational data tables. It is important to note that while non-relational data files can be accessed from within a structured database, the infor-



■ Figure 4. The real-time risk ranking process. Shaded boxes represent automated processes that are executed daily.

of risk level for a given functional location

- all initiating events related to specific equipment type failures in a facility, the unique ID of each equipment item involved in those events, and all safeguards in place to prevent such events
- all consequences related to specified events.

Making risk scenarios relational

The CPI use a wide variety of risk assessment methodologies to identify potential risks associated with the operation of their facilities. Examples include:

- equipment criticality ranking (ECR)
- hazard and operability (HAZOP) studies
- risk-based inspection (RBI) assessments
- reliability-centered maintenance (RCM) assessments
- pressure relief system assessments
- failure modes and effects analysis (FMEA)
- what-if checklists
- layer of protection analysis (LOPA)
- quantitative risk analysis (QRA).

While methodologies can vary significantly in complexity and type of approach, the end product is similar in that each produces a set of failure scenarios. A scenario includes, at a minimum, an initiating event and one consequence. It may also include subsequent events resulting from the initiating event (event tree), faults leading up to the initiating event (fault tree), identification of safeguards, additional consequences, and risk-ranking.

Each scenario has functional locations associated with it in one or more of the following roles — fault, event or safeguard. Each associated functional location and its role(s) should be explicitly identified as being part of its parent scenario. The associations are built with many-to-many relationships (Figure 3). The PSOI sets related to the child functional locations form combined data sets from which applicable items are identified and related to the parent scenario, as shown in the discussion on safeguards below.

Safeguards can be divided into equipment and non-equipment categories. Equipment safeguards are assets with equipment numbers that are installed in functional locations. Non-equipment safeguards, such as procedures and inspections, make equipment more reliable or otherwise reduce

risks associated with scenarios. Typically, only a subset of the total non-equipment safeguards linked to a given scenario via associated functional locations are applicable to that scenario. For example, a warehouse spare thrust bearing for Equipment No. 3021990, which is installed in functional equipment location YEM-CPF-TPL-TP1-DES-002 (Topping Plant Residue “A” Pump, Tag No. P-21441A), is a safeguard for this functional location, but it does not reduce risk for Scenario 1758, which is built on the initiating event “The Topping Plant 1 Desalter Water Pump trips interrupting the flow of water to the Residue Pump seal flush.” Each safeguard that is linked to a scenario and reduces risk should be associated via a many-to-many relationship with the respective consequence(s) and thereby the scenario for which risk is reduced.

Real-time risk ranking

Risk assessment data sets are typically maintained as static documents. HAZOP studies, for example, are reviewed and updated once every five years per OSHA requirements. Risk assessment concerns are frequently alleviated with the implementation of safeguards, which in many cases depend on proper execution of inspections or procedures. If these are not done or are improperly executed, risk levels go back up, possibly even to pre-risk assessment amounts. The risk-based inspection recommended practice in Ref. 4 states that “Risk mitigation achieved through inspection presumes that the organization will act on the results of the inspection in a timely manner. Risk mitigation is not achieved if inspection data that are gathered are not properly analyzed and acted upon where needed. The quality of the inspection data and the analysis or interpretation will greatly affect the level of risk mitigation. Proper inspection methods and data analysis tools are therefore critical.” The same logic also applies to risk reduction measures other than inspections, such as craft training/certification, spare parts inventory, and procedures.

Facilities need to be aware of fluctuations in risk levels so appropriate remedial action can be taken when required. A PSOI database can generate real-time risk data once numerical associations have been made between reliability, safeguard effectiveness, and safeguard support activities. The following discussion outlines this process.

Process Safety/Information Technology

Risk can be defined as a function of probability or frequency and consequence of a particular scenario with (3):

$$Risk = F(s, c, f) \quad (1)$$

where s = hypothetical scenario; c = estimated consequence(s); and f = estimated frequency. The estimated frequency of consequence occurrence is a function of the individual failure rates for equipment and safeguards that are part of a scenario.

Process equipment failure rate data typically are generic and do not factor in a number of process influences. Generic data can be adjusted to account for such influences with (3):

$$\lambda_A = \lambda_g \prod_i^n f_i \quad (2)$$

where λ_A = adjusted equipment failure rate; λ_g = generic equipment failure rate; f_i = adjustment factor i ($i = 1$ to n); and n = number of adjustment factors that apply.

Ref. 3 gives examples only of adjustments that increase failure rates, where $f_i > 1$, such as corrosion or vibration. Eq. 2 can also be used to consider the increased reliability given by safeguards, where $f_i < 1$. Adjustment factors for safeguards are, in many cases, values derived from expert opinion or judgment and are based on assumed levels of safeguard effectiveness. When the level of effectiveness for a specific safeguard is not achieved, credit for that safeguard needs to be correspondingly reduced. For example, a properly maintained relief valve has a probability of failure on demand (PFD) of 0.01 (5). If the adjustment factor for timely execution of the PM inspection is conservatively set at $f = 0.02$ and one preventive maintenance testing interval for testing and inspection of a relief valve is not executed, the PFD for that valve increases to 0.5 (the properly maintained case, $\lambda_A = 0.01$, and Eq. 2 is solved for the non-maintained case, λ_g). The logic proposed by Eq. 2 can also be used to make adjustments to consequence severity levels.

Risk reduction for installed equipment safeguards is treated in a similar manner. The LOPA methodology shows that risk reduction for independent protection layers is represented by the following equation (5):

$$f_i^C = f_i^I \prod_{j=1}^J PFD_{ij} \quad (3)$$

Literature Cited

1. **American Institute of Chemical Engineers**, "Guidelines for Process Equipment Reliability Data with Data Tables," Center for Chemical Process Safety, AIChE, New York, NY (1989).
2. **Bagui S. and R. Earp**, "Database Design Using Entity-Relationship Diagrams," CCR Press LLC, Boca Raton, FL (2003).
3. **American Institute of Chemical Engineers**, "Guidelines for Chemical Process Quantitative Risk Analysis," 2nd ed., Center for Chemical Process Safety, AIChE, New York, NY (2000).
4. **American Petroleum Institute**, "Risk-Based Inspection, API Recommended Practice 580," 1st ed., API, Washington, D.C. (2002).
5. **American Institute of Chemical Engineers**, "Layer of Protection Analysis: Simplified Process Risk Assessment," Center for Chemical Process Safety, AIChE, New York, NY (2001).
6. **American Institute of Chemical Engineers**, "Tools for Making Acute Risk Decisions with Chemical Process Safety Applications," Center for Chemical Process Safety, AIChE, New York, NY (1995).

where: f_i^C = the frequency for consequence for initiating event; f_i^I = the initiating event frequency for initiating event; and PFD_{ij} = is the probability of failure on demand of the i^{th} independent protection layer (IPL) that protects against consequence for initiating event. The values of PFD_{ij} and f_i^I in Eq. 3 are functions of maintenance inspections and other safeguards, which can be factored in by use of Eq. 2.

A similar process for reducing risk can be used with qualitative risk analysis. A review team typically will take safeguard credits for a particular scenario and reduce the likelihood and/or consequence severity categories correspondingly. Credits are assigned for each safeguard as a multiplier of a risk category increment and may range in value from a fraction to a multiple of unity.

Normalizing risk ranking

Combining data from multiple risk-ranking methodologies requires a standard unit of measure. Risk ranking is done using either qualitative or quantitative methods or both. Qualitative results are generally in matrix form, displayed as consequence severity categories vs. likelihood of occurrence categories. Risk matrices vary with different risk assessment and ranking methodologies, so it is not unusual for stakeholders to have multiple risk data sets presented in more than one matrix format. Consequently, the different matrix formats are often neither comparable with each other nor with quantitative data.

A universal risk matrix should be used to represent both qualitative and quantitative data. Consequence and likelihood categories should be assigned numerical value ranges that form a grid onto which quantitative values are plotted. Data cross-reference tables should be used to convert qualitative data in different matrix formats into a universal matrix format. A universal matrix requires assigning numerical values to both hazard (health, safety and environmental) and process-related consequence severity categories. Although assigning numerical values to death or injury of people is controversial, it is necessary for risk reduction purposes (6). Developing the matrix is best done by first developing consequence severity categories for process-related consequences, which are more-easily quantified, and subsequently developing hazard consequence severity categories by order-of-magnitude comparisons.

Conclusion

PSOI is much more accessible and versatile when it is relational and when stakeholders use common systems of reference. This is true not only for individual business units or companies, but for the CPI as a whole. We should develop industry standards for classification systems similar to the taxonomy proposed in Ref. 1.

CEP

V. ANTHONY CILIBERTI, P.E., is the principal engineer at Reliability Dynamics, a Houston-based oil, gas, and petrochemical consulting firm (E-mail: vciliberti@reliabilitydynamics.com; Website: www.reliabilitydynamics.com). Ciliberti specializes in equipment safety and reliability engineering, maintenance engineering, and information management. He has provided related services for domestic and international operations, including Aristech, Lubrizol, Exxon-HPO, Marathon-Ashland, Methanex, and Canadian Nexen Petroleum Yemen. He holds a BS in chemical engineering from Texas A&M University.