Integrating Risk Assessment Into Management Systems

Steven R. Trammell
Ronald D. Wright
Motorola, Austin, TX.

Presented at:
24th International Electronics Manufacturing Symposium
October 18-20, 1999
Austin, Texas

Abstract.

There is a move within regulatory agencies and standards making bodies towards incorporating the concepts of risk assessment into rule making. This follows a more generalized trend within many local jurisdictions and public and private corporations to utilize risk assessment in process risk management decision making. Most risk assessment language and proposed standards are subjective by definition, lending a perception that these efforts covet junk science and statistical manipulation as they are applied to risk management decisions. Environmental, Health and Safety (EHS) professionals have always been challenged with maintaining compliance to prescriptive standards, and now face additional challenges in determining effective methods of organizing and implementing risk management programs driven by risk assessment requirements.

This paper will present several methods that are being used to successfully meet the challenges of these regulations and standards relative to their risk assessment requirements. Also presented is a discussion on the integration of risk assessment into the design and development phase of complex equipment and systems.

Introduction.

In all aspects of our personal and professional lives we deal with risk decisions constantly. In fact, most of the risk decisions we make are without awareness that we have just made a choice between two or more competing alternatives. This does not necessarily mean that we are blatantly ignoring risk, but are choosing to view the potential consequences as acceptable or, are assuming a perceived lesser risk due to a lack of knowledge. Accepting risks unknowingly is the most common alternative we choose. There are so many risks facing us on a daily basis that careful study and evaluation of every risk situation we encounter is impossible. Situations which yield higher degrees of perceived risk are the ones which occupy more time for conscious assessment. The key is to gain knowledge of risks which are relevant to our situations, and to make informed and resourceful decisions.

Why Risk Assessment?

The desire and need to assess risk is not a new concept. Some of the earliest known instances of risk taking involved games of chance which were recorded on Egyptian tomb paintings and pictures formed on Greek vases. After the invention of printing, card games and their associated games of chance became popular in Europe. But the serious study of risk began during the Renaissance, when people broke loose from the constraints of the past and subjected long-held beliefs to open challenge. It was the challenge of a several hundred year old mathematics puzzle poised to Blaise Pascal and Pierre de Fermat, that provided the first breakthrough in the discovery and understanding probability theory, the mathematical heart of the concept of risk.[1] Since that time, entire professions and industries have evolved with their charters and goals aimed at identifying, quantifying, managing and reducing risk.

For industries, risk assessment and management have been a long-standing avenue for determination of business opportunities. Companies spend vast resources on market research and evaluation of market competitors to determine their course of investment and action. Large risks with small returns are typically avoided, and conversely situations with perceived low or manageable risks and large gains are developed and added to the portfolio. As in our life choices, the key to successfully navigating business risks lies in knowledge of the system of interest.

Regulatory and Standards Based Drivers.

For EHS professionals, evaluation of system risk also requires knowledge of the system. It also requires

[1] Bernstein, Peter L., *Against the Gods, The Remarkable Story of Risk*, John Wiley & Sons, Inc., New York. (1996): p. 3.

0-7803-5502-4/99 $10.00 ©1999 IEEE

knowledge of risk acceptance criteria and an understanding of the interaction of pertinent regulations and standards. Governmental control of risks is not a recent phenomenon. Every civilized country has adopted some form of government regulation to reduce societal risk. The oldest recorded governmental laws and regulations that reflect a collective approach to risk assessment and risk management were adopted to protect the food and drug supply.[2] Today's EHS professionals face dozens of laws and regulations, not to mentions internal company standards, which drive risk decision-making. Some of these regulations and standards are truly prescriptive in nature, and direct certain actions and behaviors based on pre-defined risk acceptance criteria. Over the past 25 years, Congress has enacted numerous laws that address health, safety and environmental quality. Most of these laws fall under one of three categories:

Health-based standards. For health-based standards, the mandate requires hazards to be regulated without regard to cost factors or the current availability of suitable control technology. For example, Section 109 of the 1970 Clean air Act directed EPA to establish standards for certain air pollutants that provided an "ample margin of safety" for the "most sensitive" groups. The standards were to be set based only on whether health risks existed and regardless of new costs imposed or technological limitations.

Technology-based standards. In this case, the mandate requires the adoption of "best practicable control technology", "best available technology", or other similar kinds of pollution controls or treatments. Here, the overriding considerations are not risk reduction but the cost and efficacy of a control measure in reducing pollutant or contaminant concerns. An example is the Safe Drinking Water Act, where maximum contaminant level goals are specified based solely on health considerations, but the actual standards are developed on technological feasibility and cost grounds.

Risk-balancing standards. Here, the balance of the benefits of risk reduction against the costs incurred is considered in setting risk management goals. Under the Federal Insecticide, Fungicide, and Rodenticide Act, EPA's regulation of pesticides must seek to balance the health and environmental impact of a chemical, the costs of regulation, benefits, and other societal concerns.[3]

Conversely, there is a trend towards less prescriptive language in many regulations. Several major corporations are rolling back non-regulatory based internal prescriptive standards in favor of system performance standards. These new performance standards rely heavily on risk assessment for identification of system hazards and associated controls to reduce the hazards to an acceptable level. The EHS professional is now not only faced with understanding the vast numbers of laws and regulations dictating prescriptive actions and behaviors, but must also understand the intricacies of risk management, risk acceptance and the associated methodologies by which the assessments are conducted.

Management Systems.

Decision Charts. There are numerous methodologies available for conducting risk assessments, and the decision to utilize a specific method will depend upon the type and complexity of the system, depth of study desired and available resources. Some organizations will specify the study methodology to be used, however it is generally accepted that no one method is best for every system. For manufacturing operations for which a number of different types of hazards can occur, and where systems are of varying complexity, a set of analysis tools is recommended to allow the EHS professional greater flexibility in matching methodology to the system. Within Motorola, a decision chart is used to assist the analysis in determining which method to use. This chart is loosely based on the comprehensive hazard evaluation technique selection chart presented in CCPS publication Guidelines for Hazard Evaluation Procedures.[4] The Motorola decision chart has also been developed to provide semiconductor industry specific guidance. (Figure 1)

Community Risk Standards. Community risk standards are becoming prevalent in most larger population areas. Regional requirements dictate transportation logistics, such as directing hazardous cargo onto specific highways as an example. In Austin, Texas, the local authority having jurisdiction requires a risk assessment for new hazardous chemical installations. Since the Uniform Fire Code (UFC) does not prescribe system design requirements for every conceivable system or potentially hazardous installation, an "alternate to code" evaluation must be performed. This risk assessment protocol requires a comparison of the proposed system against either a code model, or against a previous actual undesirable occurrence. Threshold

[2] Molak, Vlasta., *Fundamentals of Risk Analysis and Risk Management*, Lewis Publishers, Boca Raton, Florida. (1997): p. 293.
[3] *Understanding Risk Analysis*, American Chemical Society, Washington D.C., 1998.
[4] *Guidelines for Hazard Evaluation Procedures, Second Edition*, Center for Chemical Process Safety, AIChE, New York, (1992): p. 86.

0-7803-5502-4/99 $10.00 ©1999 IEEE

levels for damage and injury derived from actual event models are compared to estimated damage/injury potential from the proposed system. Proposed system damage/injury potential equal or less than that established by the code or actual model is given favorable consideration. The methodology used by the AFD is quantitative fault tree analysis (FTA). This analytical methods provides a quick, graphical method for determining complex system interactions, allows for quantifying system reliability, and identifies weak components or subsystems in the proposed design. Challenges with the methodology include consistent application of component failure rates and consistent construction of the model (tree) between analysts. Much of these challenges are being met though constant communication with the AFD, which includes sharing of system model templates and coordination of the component failure rate database.

In addition to the "alternate to code" evaluations, both the AFD and Motorola requires the use and application of the Semi S2 and S8 equipment design guidelines. The Semi S2 provides a set of industry derived EHS design criteria for semiconductor equipment, and the Semi S8 provides ergonomic design criteria. Equipment design to these Semi standards is required through language in Motorola's equipment purchase agreements, and is contractually enforced. The AFD requires that a semiconductor tool containing or using hazardous production materials be built in conformance to the Semi S2 prior to allowing the equipment to be placed in production.

Risk Assessment and Engineering Design.

It is well known that the most effective EHS systems are institutionalized when assessment efforts are applied at the design and development phase of equipment and systems. World class product safety programs begin with early investigation and integration of EHS criteria. A key challenge for EHS and product design professionals is determining what methodologies are appropriate for conducting effective risk assessments. Significant guidance is given by the decision charts as described in Figure 1, however truly effective risk assessments may utilize a combination of techniques. For example, Failure Modes and Effects Analysis (FMEA) is a traditional technique utilized for investigating failure modes of complex systems. FMEA is a "bottom up" approach, where a wide variety of potential failure modes are investigated and their risks to the overall system determined. This methodology is particularly thorough and effective when assessing system design for known and unknown hazards, and is widely used for assessing electronic, computer and complex hardware systems. A closely related methodology, Hazards and Operability Studies (HAZOP), is performed in a similar manner, and is typically used for complex interacting process systems and for systems where human interaction could be an important risk factor. Neither of these methods are particularly effective in evaluating combinations of failures which may lead to significant event.

Conversely, Fault Tree Analysis (FTA) is a deductive "top down" methodology which keys on a singular accident scenario or system failure mode. It is an excellent tool for investigating the root causes (especially combinational causes) of accidents or equipment failures. FTA can effectively evaluate human interactions and failures as part of the accident/failure chain of events. It is also utilized to conduct probabilistic risk assessments, although a more typical usage is qualitative or semi-qualitative.

In many cases, the most effective risk assessment methodology conducted in a design phase may be a combination of FMEA/HAZOP and FTA. For a typical complex system, where failure modes may not be well defined, the FMEA approach may be used. An exhaustive list of failure modes would be generated, and the associated risks assessed and prioritized. For higher level risks, corrective actions are developed and implemented. However, if the corrective actions are only applied to the singular failure mode identified in the FMEA, the true root cause(s) may not be fully addressed or even completely overlooked. Hence the risk to the system has potentially not been reduced to the level indicated by application of the corrective action.

For the higher level identified risks and associated failure modes, application of a FTA would be beneficial in fully understanding ALL primary and secondary failure modes, their interactions, the system rate of failure (quantitative or qualitative), and effective corrective action which address the root causes of the failure mode(s). The FTA will also graphically represent the failure scenario for the failure mode of interest, and becomes an effective presentation and training tool. Representation of key system failure scenarios using a fault tree is also conducive to effective management of change. As engineering and process improvements are investigated, timely evaluation of changes to system risk can be conducted by modification of the fault tree.

Conclusion.

After-the-fact assessment of risk is an unacceptable approach to managing our products and processes. The "second shot" is a luxury that no longer exists in many businesses. You get only one chance – after that, you will be talking only to attorneys, insurance

0-7803-5502-4/99 $10.00 ©1999 IEEE

agents, or the bankers.[5] Relatively simplistic yet effective risk assessment methodologies exist for evaluation of risk, and application of robust controls that truly address root causes of failure modes. The key is implementation. If these risk management programs and efforts are instituted early in the design and development process, maximum effectiveness in risk reduction will be realized.

[5] Grose, Vernon L., *Managing Risk, Systematic Loss Prevention for Executives*, Prentice Hall, Englewood Cliffs, New Jersey (1987): p. 50.

0-7803-5502-4/99 $10.00 ©1999 IEEE