Mary Kay O'Connor Process Safety Center
2006 International Symposium
http://process-safety.tamu.edu

Using a Risk-Based Process to Design Inherently Safer and More Reliable Technological Systems

David A. Jones, CSHO
AcuTech Consulting Group
2500 CityWest Blvd., Suite 300
Houston, Texas 77042
djones@acutech-consulting.com
Tel: 713-267-2293
Fax: 832-553-7560

Abstract

Over the past 15 years or so, numerous organizations worldwide have adopted the International Standard for Quality Management Systems ISO 9001 for delivering quality products and services. While one may think of a product in the process industries as the chemicals that are produced, this standard applies equally to the process design itself and the resultant engineered system as a product in its own right. One of the key elements of the standard is a set of requirements for the Design and Development process, which includes the following sub-processes:

- Design and Development Planning
- Design and Development Inputs
- Design and Development Outputs
- Design and Development Review
- Design and Development Verification
- Design and Development Validation
- Control of Design and Development Changes

Although the standard does not prescribe how a product should be designed to incorporate safety and reliability, it does require that the process outputs "specify the characteristics of the product that are essential for its safe and proper use." Therefore, it is up to the organization to determine what safety and reliability aspects are desired of the product, and in turn to "build in" these aspects or characteristics; for example:

- Functionality: What function is it expected to perform?
- Integrity: At what level of integrity (reliability, availability) is it expected to perform?
- Survivability: What accident effects is it expected to survive against in order to perform?

In practice, process safety and reliability activities in many situations are managed separately from the quality of the product, with design reviews often used as the only means to "check" the design. Even rigorous design reviews such as formal safety

assessments (including Hazard Identification (HAZID) studies, Hazard and Operability (HAZOP) studies, Failure Modes, Effects and Criticality Analyses (FMECA), etc.) are often carried out after the design has matured, resulting in missed opportunities to cost-effectively reduce risks by providing additional safety and reliability features, safeguards, etc.

Because of the severity of certain hazards, some industries (e.g. nuclear power, aerospace, offshore oil and gas exploration and production) over the past few decades have either developed or adopted formal process risk management methodologies to ensure that health, safety and environmental (HSE) hazards and their associated risks are properly considered and managed. These methodologies include the following steps: Hazard Identification, Risk Estimation, Risk Evaluation, and Risk Reduction. For example, best industry practices for selecting and using such hazard identification and risk assessment methodologies throughout the life cycle of a oil and gas processing facility have been summarized in the guidelines of the recently published International Standard ISO 17776.

To improve the process of managing hazards and risks, an integrated approach to designing complex technological systems is presented in the paper which combines the principles of quality management with those of HSE risk management. Through proper planning and control, such systems can be assured of having safety and reliability aspects designed into the system, thereby reducing risks before they are used for their intended operation or service. In this manner, inherently safer designs can be achieved from the start.

The policies, procedures and work instructions for this risk-based design process can then be integrated into an overall health, safety and environmental quality (HSEQ) management system for the entire life cycle of the product (i.e. the engineered technological system). To demonstrate the practical application of this risk-based design process, this paper will present the upper level structure of the management system process based on the applicable requirements of the following International Standards, as well as examples of the applicable design documents used throughout the design process:

- ISO 9001:2000 “Quality Management Systems – Requirements”

- ISO 17776:2000 “Petroleum and Natural Gas Industries – Offshore Production Installations – Guidelines on Tools and Techniques for Hazard Identification and Risk Assessment”

Objectives:

1. Describe the process for design and development of quality products;
2. Describe the process for hazard identification and risk assessment at the design stage;
3. Present a model for integrating these two processes into a single risk-based design control process;
4. Demonstrate the steps of the risk-based design process, with an emphasis on safety and reliability as quality aspects of the design of any engineered technological system; and
5. Present an example application of this process for a complex engineering design of an oil and gas production facility; specifically a summary of major hazards and corresponding risk reduction measures for safety-critical systems and equipment.

Learning Outcomes:

• To understand the steps for designing inherent safety and reliability characteristics into a complex technological system as a quality product;
• To understand the steps and methodologies for identifying hazards and assessing

risks at the design stage;

• To understand how to apply formal quality management standards to designing safe and reliable complex technological systems;

• To understand how to integrate the risk-based design process into an HSEQ management system; and

• To understand how to “build safety and reliability into a product” as a means to cost-effectively prevent

accidents through risk reduction at the design stage, rather than through costly engineering controls and

administrative controls after it is put into operation.