SAND2013-2645P

March 2013

Construction News Sense

What is Engineered Safety and How Does It Affect Me?

Engineered Safety is the next step in Sandia's work planning and control process. We want to ensure both the complex and simple operations are assessed properly and documented on a graded approach. As contractors, we have been conducting this exercise for years; however, in the old system we documented how we defined the scope of work, then analyzed the hazards that lead to the development of controls. After these steps were completed, we performed the work and gave feedback to improve the process.

Now when using Engineered Safety, the technical complexity and variation of this hazardous work can require a high degree of analytical and critical thinking skills to achieve mission-performance objectives. The purpose of this document is to make the application of these inherent skills more integral to achieving mission-performance objectives safely. We have historically used addendums, permits, and lift plans to address these issues.

Critical thinking requires a thorough understanding of the technical basis of the work. It requires seeking out failure modes that can cause accidents to occur. Fundamental to this approach is an understanding that safety is an attribute of a "system" of interconnected elements - people, procedures, facilities, equipment and the hazards inherent in them and that to which they are applied. In the context of this document, the term "design" means the purposeful design of this "system" to minimize the potential for accident consequences. Our younger workforce may not have the experience to do this without tolls.

There are distinctive decision points in Engineered Safety. The criteria will be addressed as applicable to the three formally documented decisions by line management on activity-level work, as follows:

- The first decision point is to accept or reject new work or re-evaluate and make a decision on on-going work if deemed necessary.
- The second decision point is approval of the "safety case" that explains how the system design addresses the criteria.
- The third decision point is "authorization" to begin work after all necessary verification activities have been performed on the final system design.

Sandia is responsible for flowing down the requirements for activity-level work performed on a DOE site by its subcontractors, as well as for ensuring appropriate planning for mission safety at work locations.

If one element of the system is changed, the system must be re-examined in that context. All the elements must remain seamlessly tied together from the design phase through the execution phase. Where different organizations are integral to the system, particular attention must be paid to early involvement and reliable communication across the organizational interfaces during execution. Poor communication of safety-related information across organizational interfaces is a frequent contributor to accidents.

Typically human performance is an integral part of the system and is often overlooked in planning because of trust and respect of each other's competence. However, human performance is a common source of error. Accident pathways resulting from human error must be identified upfront and removed or blocked by design intent. Further, robustness should be built into the design of the system to compensate for uncertainties in human performance.

Continued on Page 2

SAND xxxx

Publisher: Linda Sells, Org. 04844

Content Owner: Greg Kirsch, Org. 04844

In this approach we must define unacceptable consequences in light of Sandia's risk tolerance and not the individual. This can only be achieved by communication. Many factors contribute to the risk assessment approach:

- Often, there are little or no failure data to make a meaningful estimate of a specific accident probability; therefore, if the accident scenario has not occurred yet or it is not in a person's experience base, the probability must be low.
- Even when there are success and failure data that enable a statistically valid estimate, the uncertainty bounds or confidence limits on the estimate tend to be overlooked.
- Skill-of-the-worker or skill-of-craft, combined with judgments about complexity of the work, can be another way to presume low probability and not pay enough attention to the severity of accident consequences.
- A presumption of low probability can enable the belief that the accident is more likely to occur near the last trial than during the equally probable first trial.
- Mission success, cost, and schedule pressures can influence the presumption of low probability; the need for controls may add to these pressures.

The first priority is to eliminate a hazard rather than attempt to control it. When this is not feasible, the next priority is to eliminate single-point failures that can cause unacceptable consequences. For years in construction we have accepted single-point failures and we must remove as many as reasonable and practical. The remaining single-point failures that can cause unacceptable consequences dictate a natural priority for the development of engineered and administrative controls. Selection of personnel protective equipment is the last line of defense.

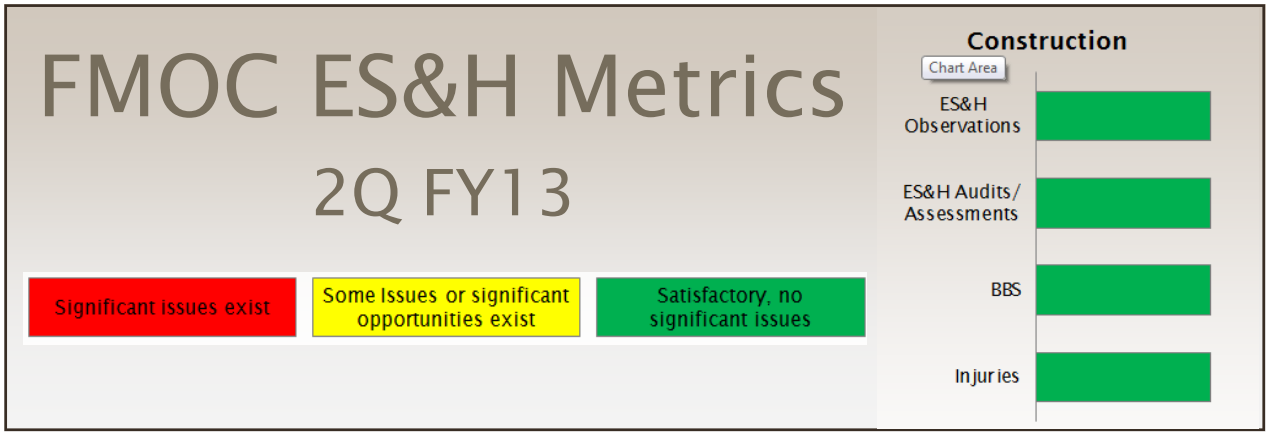
Engineered and administrative controls are described in broad context as follows:

- Engineered controls are physical or engineered features that provide active or passive protection to prevent or mitigate accident consequences. Traditionally, these were hardware controls; however, software controls also play an important role in assuring safety and their role needs to be carefully considered and evaluated.
- Administrative controls are processes and procedures utilized to control any exposure and assure appropriate safety discipline is used to conduct hazardous work. Based on potential accident consequences, a graded approach shall be used in regard to operating procedures, critical steps in procedures, team training and qualification, and hazard analysis.

During the upcoming Quarterly Construction Safety Seminar on April 24th we will be reviewing this in depth and asking for contractor input. Please be ready to talk about Engineered Safety and answer the following questions:

- What operations are most dangerous in your eyes?
- Who authorizes hazardous operations in your company?
- How do we ensure critical thinking in low rigor activities?
- How do you address change in condition and change in operations?
- Information from this article was taken from the Work Planning and Control Criteria for Safe Design and Operations.

Greg Kirsch, FESH Lead 4844



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000