FACILITIES MANAGEMENT AND OPERATIONS CENTER

Sandia National Laboratories

SAND2014-3572P

April 2014

Construction News Sense

Engineered Safety for Construction

At first glance, the definition of "engineered safety" seems like a planning process that is linked solely to engineering principals; however, this is not the case. Historically, Sandia Construction Teams have understood and worked under solid work planning and controls; however, time has revealed some holes in the process. In the past, we would define work, analyze and control hazards, prepare and perform work, and finally provide feedback and improve processes. While we saw a reduction in events and injuries using this method, we still had events occur. Now it is clear that with improved work planning, there is room for improvement. Although change is difficult, and some people may be reluctant to engage in continuous improvement, the bottom line is that we do not want to see anyone get injured.

While the core function of how Sandia operates is not changing, we are asking that everyone think through the six principals of engineered safety, which include a solid understanding of the work, ensuring operations are safe by design intent, understanding the technical basis, and identifying and controlling all energy sources, both potential and kinetic. Ultimately, we must get better at defining unacceptable consequences, using a risk assessment approach, and applying positive verification.

Principles of Engineered Safety

In general, the construction industry does not do a good job of defining unacceptable consequences, especially as we look at the upcoming year or even the next project. While our target is and always will be Target Zero, there needs to be a baseline to work from that triggers extensive engineering controls. The Sandia Facilities Management and Operations Center (FMOC) defines this as:

- Accidents that result in a serious occupational injury (per ESH100.4.RPT.3, *Report Occurrences*)
- Significant violation of environmental regulations
- Unplanned facility outages or interruptions that significantly impact critical mission work

The unacceptable and unmitigated consequences serve as a reference point for beginning the design of a new system or reviewing the design of an existing system.

The concept of "safe by design intent" looks at the interconnected elements of trades personnel, safety plans, pre-task plans, structures, equipment, and materials. If one element of the system changes or is changed, the overall system is changed and must, therefore, be re-evaluated. Particular attention must be paid to early involvement and reliable communication across organizational interfaces during execution, particularly where different organizations or contractors play a role in the system. Poor communication of safety -related information across organizational interfaces is a frequent contributor to accidents. Human performance, which we talk a great deal about, is an integral part of engineered safety and is often overlooked in planning because of many reasons. These reasons include previous bad responses to questions, trust and respect in others' competence, and even complacency. 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. Safety is most effectively and efficiently achieved by designing it into the system at the conceptual or initial planning stages. The Sandia design manual will be updated to reflect these changes.

Continued on Page 2

SAND xxx P

Publisher: Linda Sells, Org. 04878

Content Owner: Greg Kirsch, Org. 04878

Understanding the technical basis is also vital to safe operations. For mission safety, it is important to understand how the system design can fail and cause an accident. Failure mode analysis appropriate to the technical complexity of an activity will inform decision-making on the number and type of controls necessary to reduce the probability of occurrence. While this can be relatively straightforward for a new hazardous activity, it can be problematic for older facilities and operations. The technical basis of an existing hazardous activity must be reconstructed sufficiently to ensure continued safe operations. This effort will be prioritized according to the severity of potential accident consequences.

Overall, we are good at identifying and controlling electrical energy sources; however, as a group, we have been weak in recognizing and controlling potential and kinetic energy. This is apparent with the recent finger and hand injuries at SNL. Stored energy in all of its forms and disguises must be identified and controlled with appropriate engineered and administrative controls to prevent or mitigate the consequences of accidental release. Kinetic, potential, electrical, electromechanical, thermal, pressure, and chemical are all energy sources that can be released directly or in another form of energy, which can result in an accident. In most cases, the concern will be stored energy in a system, but it can also be lack of energy if continuous energized controls are necessary to ensure safe operations. Many tasks appear to be low rigor; however the risk, consequence, and severity can be high if a good "what if scenario" is not conducted. We need to focus on the weight of objects and line-of-fire conditions if we are to get to the next level of safety.

We all know that standard hazard assessments require making a judgment on the probability that a particular accident consequence will occur, and we often forget that we are biased with our own experience. While this is the basis by which people make risk decisions every day, this practice is problematic for early decision-making when determining appropriate controls for hazardous work. If an estimate of low probability of occurrence dominates early decision-making, which needs to go beyond OSHA standards, human nature and external pressures tend to minimize the use of what would otherwise be a sensible set of controls based on the severity of accident consequences. 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. In addition, the skill of the worker or the skill of craft, combined with judgments about the complexity of the work, can be another way we presume low probability without paying enough attention to the severity of accident consequences.

Conducting positive verification can be misunderstood and is often not conducted at the correct time. Accidents frequently occur as a result of little or no communication during the execution phase, especially across contracting interfaces. Many times, one person is relied upon to ensure a safe operation; however, the activity hazard evaluation process can assist with complex team evaluations. Positive verification means that each team member must affirm to the person in charge that their part of the system is in the state intended for safe operation. The pre-task analysis is the perfect time for this communication for less complex operations. If the team does not have concurrence, it should be assumed by the person in charge that it is not safe to proceed. The AHA process should be used for more complex operations. An example of this is a supervisor's walk down of a site to ensure that the sequencing of work is being executed on schedule to ensure minimal overhead work and that incompatible chemicals and hot work are being conducted in the same space.

In closing, all workers and supervisors should actively look for stronger engineering controls in all operations. All workers and supervisors need to increase awareness for tasks/activities that are low rigor and high consequence and severity. Typical examples include ladder operations, pinch points, and industrial ergonomics. If something abnormal occurs, pause and re-evaluate. Owners of contracting companies should ensure that updates to their CSSP properly reflect engineered safety. Owners and supervisors also need to verify data from their employees and subcontractors. Everyone should challenge answers respectfully and all workers should evaluate their "circle of safety" (i.e., their work area prior to work for potential hazards). All workers and supervisors must maintain a questioning attitude and use critical thinking skills.

Greg Kirsch, FESH 4878

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