Engineered Safety at Sandia National Laboratories

SAND2012-1972P

Sandia National Laboratories

Beginner's Guide: A Starting Point for Engineered Safety

Overview

As you begin learning the discipline of engineered safety, consider this to be your starting point. Here are five questions that start the engineered safety process. Answer these and you are well on your way to achieving technical mastery.

1. Who is the decision maker?

Who is the manager who will make a decision that the quality and safety of the project have been sufficiently addressed? Who is the responsible engineer for this work? Who will be held accountable by the decision maker to have a system understanding and deliver the working product?

2. What are the unacceptable outcomes?

Criteria for success is usually well known in a project. What about failure? What quality and safety performance would be unacceptable? The decision maker usually has a role in specifying this.

3. How can the system fail to perform as intended?

Perform a failure modes analysis to understand how the system can fail to perform as intended. Prioritize the failures you address:1) single point failures that lead to the unacceptable outcomes, 2) other failures that lead to unacceptable outcomes, 3) other failures. Use engineered controls first. Focus on defense in depth.

4. What if the system fails anyway?

Although the failure modes may be eliminated or mitigated, what if the system fails anyway? What is the planned response to a serious failure?

5. How do you know it will work?

How will the responsible engineer assure that the system is in its intended configuration before it is operated? This will be one of the last major opportunities to prevent a failure.

Goal: Technical Mastery

- Demonstrate a system understanding of the hazards and failure modes.
- Design and validate the system to eliminate and control identified hazards and failure modes.

Principles of Engineered Safety

Safety is an attribute of an operational system achieved by intent

Use technical expertise to systematically and critically analyze ways in which the system can fail to perform as intended.

Engineering design of the system prevents identified potential failures or mitigates their consequences.

Questions?

Mike R. Lopez, PhD
R&D Technical Manager
Z Pulsed Power Facility
Tel: 505.845.7582
Email: mrlope@sandia.gov

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. SAND No. 2011-XXXXP

NNSA U.S. Department of Energy