THE PENTAGON-S PROCESS:

A systematic approach for achieving high confidence in high-consequence products

Authors

Perry E. D'Antonio, 505-844-7956, pedanto@sandia.gov

John M. Covan, 505-845-8733, jmcovan@sandia.gov

Mark E. Ekman, 505-844-1771, meekman@sandia.gov

Sandia National Laboratories[1] (Energy Sector)

Albuquerque, NM 87185-0491

Abstract

Sandia National Laboratories has developed a systematic approach for achieving high confidence in major products requiring high reliability for use in high-consequence applications. A high-consequence application is one in which product failure could result in significant loss of life, damage to major systems or to the environment, financial loss, or political repercussions. The application of this process has proven to be of significant benefit in the early identification, verification, and correction of potential product design and manufacturing process failure modes. Early identification and correction of these failure modes and the corresponding controls placed on safety-critical features, ensures product adherence to safety-critical design requirements, and enhances product quality, reliability, and the cost effectiveness of delivered products. Safety-critical features include design features such as materials and dimensions, as well as manufacturing features such as assembly processes, inspections, and testing.

Keywords

High consequence, safety, surety, Pentagon-S, manufacturing controls, production controls, change control, product documentation, system safety, best practices, /S/

[1] *Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.*

Pentagon-S Overview

The Pentagon-S process is a multi-organizational team approach that includes the designer, customer, supplier and safety engineer working in concert to define the safety-critical features and determine how those features will perform in accident and operational environments the product may encounter. The purposes of the process are to identify safety-critical design features of a product, use a graded approach to control these features during production, implement a system of change control, and to provide an auditable, pedigreed trail of documentation from requirements to final product. Systems analysis tools (e.g., fault tree, FMEA) are used to determine safety critical features and their failure modes. Pentagon-S helps the customer weigh safety requirements against other system requirements and understand the consequences of not implementing certain manufacturing controls. The process, with its supporting information archival and retrieval system, received two *Best Practices* awards from the Navy Best Manufacturing Practices Office.

Introduction

Pentagon-S, or /S/, implementation is a systematic process that analyzes product design features in the context of their environments and operations to identify safety-critical features. Safety-critical features include materials, dimensions, processes, testing, etc. On production control drawings, /S/ markings identify safety-critical features that if changed or deviated from could degrade the safety function of piece parts or subsequent assemblies. Changes to /S/ features require review and management approval by both the design and safety organizations.

DISCLAIMER

Safety critical features must be identified and controlled in high-consequence applications. /S/ ensures that safety-critical features will not be changed without recognizing the effect such changes could have on the safety of the component or system as a whole.

Properly identifying, documenting, and controlling safety-critical features ensures that components and systems are built as designed and respond in a predictably safe manner. Documentation provides an auditable, traceable path between safety requirements and the product, and provides a record for future designers and producers.

Significant improvements in production yield have also been demonstrated with /S/ because of the enhanced manufacturing screens and defect controls the process provides.

Background

The Pentagon-S process was created during the development of a modern US nuclear weapon program. Pentagon-S was created to augment traditional quality controls that were in place at the manufacturing site. At that time no controls specific to safety-critical products or processes were in place and it was judged to be an inappropriate "weak link" in the product life-cycle of a high-consequence system. As we shall show, /S/ increased both the authority level and broadened the review body for change control, as well as strengthened Sandia National Laboratories' system safety methodology for assuring nuclear weapon detonation safety.

The Need for Control

Sandia's system safety engineering methodology–briefly described below– promotes high confidence in the product's safety performance only if it is manufactured by an equally robust process. Production must be controlled appropriately to ensure safety-critical features conform to their design requirements and are properly integrated into the system. Only then will the system meet its design requirements for high levels of safety in both operational and accident conditions.

The Scope of Control and Documentation

In general, the scope of control and documentation cuts across the entire safety process–from requirements development to design to manufacturing to operations to system shutdown and disposition. The most intense effort, however, occurs during the design phase after a *safety theme* has been developed. The safety theme describes the philosophy and implementation plan the designer will use to engineer a safe product and meet safety requirements. The safety theme describes the ideal safety performance of the system when exposed to normal operational and accident conditions. However, in practice, there is a tendency for safety performance to decrease with the realities of engineering trade-offs and manufacturing difficulties. As Figure 1 shows, the role of Pentagon-S is to maintain safety performance at a high and acceptable level. It maintains performance by *identifying safety-critical features of components that are most critical to safety and then controlling their manufacture and documentation.*

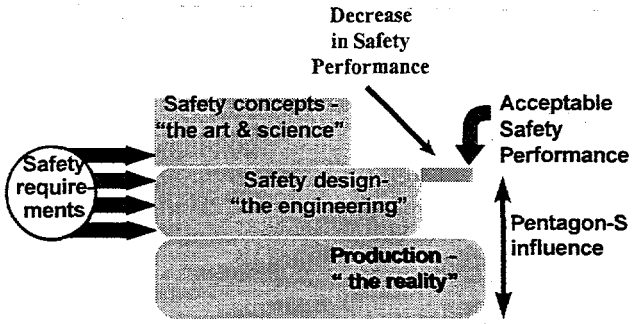

Figure 1. Pentagon-S maintains the designed-in safety performance.

How /S/ fits into Sandia's System Safety Engineering Methodology

Modern nuclear weapon detonation safety is the result of decades of analysis, testing, and experience that has led to the development of a design methodology for keeping the weapon *predictably* safe under a variety of stresses, both

operational (expected) and accident-based (unexpected). The methodology relies on mutually supportive safety design principles that are integrated through the proper implementation of fundamental physical principles known as *first-principles*. This integration is provided by a *safety theme* and its a-priori development avoids "Rube Goldberg" inventions that hinder the achievement of acceptable system safety.

The safety theme is implemented by partitioning safety requirements among multiple safety subsystems whose elements are essential to maintaining the safe state of the entire system. These elements are referred to as 'safety critical' because their failure, either singly (first order failure) or in combination (lower order failure), will result in system failure and the realization of (negative) high consequences. Safety critical elements utilize engineered features that are identifiable, analyzable, and controllable. The goal is to minimize the number of system components that are safety-critical in accident environments. Because the safety assurance then hinges on a relatively small subset of overall system design, limited design and verification resources can be better focused to improve confidence that predictable safety will result.

The /S/ process

The essential elements of the Pentagon-S process are: identify and rank safety critical elements, selection of controls, analysis of control measures, documentation, and change control.

Identify and rank safety critical elements

Fault trees are created having basic nodes (Basic Events) identifying possible failures of safety critical elements. Each failure in the fault tree can be identified either as "first order" or "lower order". A first order failure can singly cause a component, subsystem, or system not to perform its intended function, thus reducing or eliminating safety protection from that element. A lower order failure must occur in combination with one or more separate failures to cause a component, subsystem or system not to perform its intended function. This difference is significant because separate controls are implemented depending on the order of a fault.

Selection of controls

Because first order safety critical elements are more significant, more stringent controls are employed, typically involving 100% verification; lower order faults require less stringent controls.

Analysis of control measures

Control measures must be analyzed to ensure changes are not made without first knowing the effect those changes have on the safety functions. This evaluation must determine if any new hazards are introduced or if existing controls will be bypassed if the change is implemented. Management approval by the systems organization, the affected component organization(s), and the safety organization is required before the change is implemented.

Documentation

Safety critical features are documented using a formally defined template to capture the significant information about a safety-critical feature. A safety critical feature can be traced by using the unique basic event identifier from the fault tree and recording this same identifier on all product related documentation. Top level system or subsystem safety requirements contained are referenced in the safety documentation to tie safety requirements to the final product.

Figure 2, an example of this documentation, illustrates essential features of the Pentagon-S process.

Basic Event Identifier: E034

a. Title: Web Not in Contact with Shell
b. Parent Event: Web/Shell Interface Fails
c. Failure Order: 1
d. Control Requirement: CD413275, CD413354
e. Implementation Rationale and Background: The LAC must have an electrical breakdown from one or more contacts to an internal web through a dielectric arc-stimulation material if high enough potential develops across the contact-to-web gap. The LAC then conducts high current from the contacts to the web, through the arc established by the voltage breakdown to the connector shell, and finally to the metal bulkhead where the LAC is mounted. An assured continuous conduction path, free from insulating impurities or contamination, must exist within the LAC to provide a suitable margin of safety with respect to the minimum assured holdoff voltage of the stronglink switches. The web must be seated in a planar fashion to assure proper contact with the shell. There must be no insulating impurities between the web and the shell lip. Refer also to Basic Events E010, E012, E016, and E024. Failure to maintain a conduction path will compromise the nuclear safety critical function of the LAC.
f. Analysis and Test Reports: SAND94-1513, Lightning Arrestor Connectors, 1969-1994
g. Product Drawings: 398527 and 398529, Unit Assembly, Note 1.6.3, Note 1.6.4
h. Production Certification: 100% certification of good electrical contact between web and shell (FRB test), including certification required by Basic Events E010, E012, and E024.

Figure 2. Safety critical feature example documentation.

In order of their appearance in the figure, the entries are:

Basic Event Identifier- references the unique fault tree event affecting the specific safety critical feature

a) *Title*- specific Basic Event title found on the fault tree
b) *Parent Event*- records with entry a) the higher level event from which the safety critical basic event is derived (helps to locate the Basic Event in the fault tree)
c) *Failure Order*- as derived from fault tree analysis
d) *Control Requirement*- records specific safety requirement documents that are the source for control of this feature
e) *Implementation Rationale And Background*- provides a history and knowledge of why a feature is safety critical (especially useful when considering a change to the feature)
f) *Analysis And Test Reports*- supporting documentation demonstrating safety performance or contains pertinent safety-related information
g) *Product Drawings*- location of where the Basic Event identifier appears on production drawings with /S/ notation
h) *Product Certification*- lists what verifications are done to ensure the product meets design requirements

Change Control

Another formal documentation template was developed to document design changes to safety-critical features or to establish the disposition of product containing nonconforming safety critical features. This template includes the following information:

- *Background* - describes issue or problem with /S/ item.
- *Change Request* - describes the requested change to the /S/ feature
- *Impact of Change* - describes both the impact of not changing and implementing the change
- *Management Approval* - component, system and safety managers sign

Summary

Sandia National Laboratories has integrated a robust manufacturing process, known as Pentagon S, into their system surety engineering methodology to deliver an end-to-end safety process for high consequence systems. The overall process is depicted in Figure 3. This process will ensure safety-critical features are identified and appropriately controlled to ensure their safety performance throughout the system life-cycle in both normal and accident conditions.

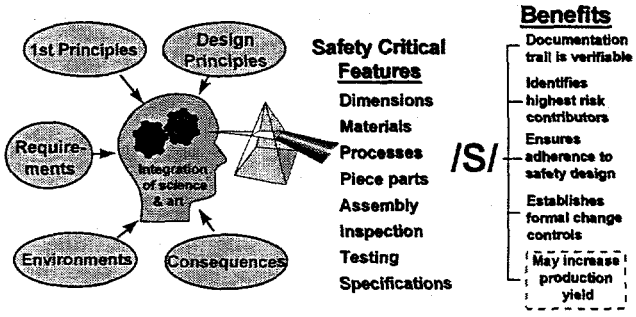

Figure 3. Pentagon-S as a part of the system safety process.

Author Biographies

Mr. Perry E. D'Antonio is currently on a special one-year assignment at the Department of Energy's (DOE) Office of Weapons Surety. Prior to this assignment, he managed the System Surety Engineering department at Sandia National Laboratories (SNL). The department develops system safety engineering solutions for nuclear weapons and other industrial high-consequence operations. He holds a Masters Degree in Electrical Engineering from Stanford University. In seventeen years at SNL he has held staff and management positions in weapon systems engineering design and safety assessment, and managed a research program to improve safety technology. He is the SNL representative to the Lockheed-Martin Engineering Process Improvement Center's System Safety Subcouncil. He is a weapons safety expert in the DOE Accident Response Group. Mr. D'Antonio is currently serving as President of the System Safety Society.

Dr. John M. Covan is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a PhD in Nuclear Physics from the University of Arizona and an ME in Industrial Engineering from Texas A&M University. He has held a number of positions cutting across surety engineering at Sandia Laboratories. In the use-control arena, he has evaluated related weapon subsystems and has developed new concepts involving use control. In the detonation safety arena he has modeled new safety concepts, done experiments on electromagnetic sensitivities to premature detonation and proposed procedures for investing detonation safety directly into new systems. He has also been involved in efforts to transport detonation safety-based concepts beyond this arena to more general commercial applications. He is a member of the System Safety Society and is currently serving on their Standards Committee.

Dr. Mark E. Ekman is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a Ph.D. in Chemical Engineering from Iowa State University. He has led the incorporation of the Pentagon S process for most of the nuclear weapon safety components in production at multiple DOE production agencies since 1992. He led a DOE multi-agency team to ensure consistency in process implementation throughout the Nuclear Weapons Complex (NWC) and is a co-author of the NWC Technical Business Practices defining the Pentagon S process. Dr. Ekman is a member of the American Institute of Chemical Engineers and American Chemical Society.