A Thematic Approach to System Safety

Mark E. Ekman, Paul W. Werner, John M. Covan, and Perry E. D'Antonio

Sandia National Laboratories[1]
P. O. Box 5800, MS 0490
Albuquerque, NM 87111-0490

Abstract

Sandia National Laboratories has refined a process for developing inherently safer system designs, based on methods used by the Laboratories to design detonation safety into nuclear weapons. The process was created when the Laboratories realized that standard engineering practices did not provide the level of safety assurance necessary for nuclear weapon operations, with their potential for catastrophic accidents. A systematic approach, which relies on mutually supportive design principles integrated through fundamental physical principles, was developed to ensure a predictably safe system response under a variety of operational and accident-based stresses. Robust, safe system designs result from this thematic approach to safety, minimizing the number of safety critical features. This safety assurance process has two profound benefits: the process avoids the need to understand or limit the ultimate intensity of off-normal environments and it avoids the requirement to analyze and test a bewildering and virtually infinite array of accident environment scenarios (*e.g.*, directional threats, sequencing of environments, time races, *etc.*) to demonstrate conformance to all safety requirements.

Introduction

Many domestic and foreign systems are subject to catastrophic loss due to accidental or malevolent causes. These systems can be considered as *high-consequence* systems. High consequences range over numerous categories. These can include loss of life, health or earning power; loss of property or economic opportunity; environmental damage; loss of public confidence and other negative political repercussions; or other catastrophic effects. There is no universally accepted threshold for high consequence; typically, it is defined by the owner of the system. However, nuclear weapons and many chemical plants definitely fall into the realm of high-consequence systems. In addition to high consequences, nuclear weapons and chemical plants face similar technological challenges with regard to safety, such as equipment aging, component replacement, surveillance, and development of predictive tools.

These high consequence systems ensure national security and provide for improved quality of life. Failure of these systems could result in unacceptable loss. Therefore, they

[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.

DISCLAIMER

require ultra-high levels of assurance that they will perform as intended under all circumstances. We define this high level of confidence as *system surety*. Surety is defined here as incorporating elements of safety, security, and reliability to ultimately achieve ultra-high quality.

System surety engineering is the systematic process used at Sandia National Laboratories to ensure the system will perform in a predictable and acceptable ways under normal (operational), abnormal (accidental), and malevolent (intelligent attack) environments. These environments are threats to the intended safe, secure, and reliable operation of high consequence systems. This paper focuses on the safety aspects of surety, and describes the approach developed at Sandia National Laboratories to ensure a predictably safe system response in a variety of operational and accident-based environments.

System Surety History

Modern nuclear weapon detonation safety is the result of decades of analysis, testing, and experience that has led to the revolutionary, as compared to evolutionary, development of a methodology for assuring that the weapon is *predictably* safe under a variety of stresses, both operational and accident-based. Prior to the development of this methodology in the early 1970s, nuclear weapon safety assurance relied on traditional engineering practices, such as designing "black boxes" that met the functional and interface requirements in normal operating environments. Probabilistic risk analysis and other conventional approaches were used to demonstrate compliance to safety requirements.

Analyses relied largely on plausibility arguments that accident-induced changes in the system would make it less reliable—and as a result—safer. For example, it was assumed for critical weapon circuitry that an accident causing an electrical fault to ground will predictably "dud" the system. Using this and many other assumed system responses, large probability matrices were developed for various accident environments. Elaborate computer models and fault trees were generated to calculate the probability of an accidental nuclear detonation.

However, a critical self-examination of these standard engineering practices revealed that *there was no technical basis for many of the assumptions made*, and that many of these assumptions were in fact grossly misleading. For example, an electrical fault to ground may not dud a system but actually cause additional propagating damage.

An extensive experimental program was established to demonstrate these concerns and to obtain an engineering understanding of the influence of electrical, thermal, mechanical and other types of energy on systems, components, and interconnections. A repeated lesson learned was that the uncertainties of accident-induced responses in a complex system could defeat the assumed "safe" responses in numerous, surprising ways.

A fundamental problem to the traditional engineering approach was the expectation that the accident would create a safe response when it often would do just the opposite. For

example, unpredictable charring of insulation would often make an unsafe connection to unexpected electrical paths rather than safely dudding the weapon. Such approaches simply could not result in the high levels of assured safety required for the design of new nuclear weapons and their attendant operations.

Inherent Safety in the Chemical Process Industry

An analogous revolutionary change in the approach to safety in the chemical process industry (CPI) was first published in 1978 (Kletz, 1978). Interest in this approach, known as *inherent safety* within the CPI, has grown rapidly in recent years (Kletz, 1996). A chemical manufacturing process is described as inherently safer if it reduces or eliminates the hazards associated with materials and operations used in the process, and this reduction or elimination is permanent and inseparable (CCPS, 1996). A *hazard* is defined as a physical or chemical characteristic, intrinsic to the material or to its conditions of storage or use, that has the *potential* for causing harm to people, the environment, or property (adapted from CCPS, 1996 and CCPS, 1992).

Prior to the inherent safety approach, CPI safety focused on controlling chemical process and plant hazards through updated procedures, supplementary safety interlocks, additional safety systems, and improved emergency response (CCPS, 1996). Kletz proposed that processes should be changed to completely eliminate hazards, or to reduce their magnitude to levels which would not require elaborate safety controls or procedures. Design strategies for achieving inherently safer plants have been defined by Kletz (1984, 1991) and IChemE and IPSG (1995) as four inherent safety principles:

1. Intensification/Minimization	Minimize the quantity of hazardous substances
2. Substitution	Replace a material with a less hazardous one
3. Moderation	Use less hazardous conditions, less hazardous form of a material, or facilities which minimize the impact of a release of hazardous material or energy (also called Attenuation or Limitation of Effects)
4. Simplification	Design facilities to eliminate unnecessary complexity , which are more forgiving of equipment, control, and human errors (also called Error Tolerance).

Despite the advantages and benefits associated with designing and operating inherently safer chemical plants, there have been few recognized examples of its application in

modern chemical plant design (Mansfield, 1996). Two commonly asked questions from industry regarding the principles of inherent safety are (Gowland, 1996):

> *"How do I know if my process is designed according to inherently safe principles?"*, and
>
> *"Can the influence of a process change on the inherent safety of a plant be measured?"*

The process used to design predictably safe responses for nuclear weapons not only achieves the concept of inherent safety, but goes a step further by providing the safety confidence demanded by these types of questions, and to extend the concept of inherent safety beyond its current state as practiced by the CPI.

A Different Approach to System Safety

The conventional engineering approach to achieve safety for a high-consequence system focuses on three major elements. The first element is *preventive*: to reduce or eliminate the hazard directly. Where the hazard cannot be eliminated or further reduced, the second element is *protective*: to reduce the likelihood that some initiating event can act upon the hazard, resulting in the undesired consequence. This is accomplished through the use of passive, active, or procedural risk control factors, such as choice of material properties, additional safety hardware, and increased regulations, respectively. The third element is *mitigative*: to provide for a means to mitigate the high consequences and minimize their effects should the other elements fail. This element includes emergency response and management methods. Demonstrating compliance to safety requirements using this approach relies on probabilistic risk analyses and related techniques. Adequate safety is achieved when the risk, which is the product of the accident likelihood and the magnitude of the high consequence, is acceptably low.

The system surety engineering approach to achieve safety for a high-consequence system incorporates the three elements described above to the greatest extent possible. However, this approach, derived from the practices used to assure the safety of nuclear weapons, includes a fourth, unique element (Trauth, 1997). This element is *interruptive* or *eliminative*: to design the system such that there exists no initiating event that can act upon the hazard to lead to the undesired consequence. Demonstrating compliance to safety requirements using this approach relies on mutually supportive design principles that are integrated through the proper implementation of fundamental physical principles, known as *first principles*. *Assured safety*, which avoids reliance on probabilistic or other estimates of risk, is achieved when the high consequence simply cannot occur.

As an example of these two approaches, consider a hypothetical catalytic reactor, where the catalyst, to be effective, requires a high surface area substrate. The high consequence to be avoided is reactor failure, which could release large quantities of hazardous materials to the environment and threaten worker health. If the reactor experiences a large

temperature increase, the reaction rate increases to the point where a runaway reaction could occur, increasing reactor pressure, causing the reactor to fail. The hazards have been eliminated or reduced to the lowest extent possible while still being able to produce the desired product.

The conventional safety engineering approach may consider a protective solution of constructing the reactor such that it can safely contain the highest possible pressure that could be generated by a runaway reaction, with a suitable margin of safety included. Acceptable safety has been sought by reducing the likelihood that the increased temperature will ultimately cause the reactor to fail; however, there is residual risk because the reactor can fail throughout its life due to defects, corrosion, physical damage, or other causes.

The system surety engineering approach is eliminative. A substrate is chosen to support the catalyst that has material properties such that in normal operating temperatures the catalyst is active, but for higher temperatures, the substrate decomposes, resulting in the catalyst becoming ineffective and stopping the reaction before high pressures can be produced. Assured safety has thus been achieved by eliminating temperature as an initiating event for causing the reactor to fail.

This example illustrates that controls over initiating events are of two types: those that lessen the probability that the initiating event will lead to the undesired consequences (conventional approach), and those that eliminate the initiating event as a causative factor for the undesired consequences (system surety approach) (Trauth, 1997). *Fundamentally assured safety is possible only with the latter approach.*

System Surety Engineering Process

The system surety engineering process was developed at Sandia National Laboratories in the course of its work in high-consequence (nuclear weapon) engineering. The process development was motivated by the realization that standard engineering practices did not provide the level of safety assurance necessary for its operations with nuclear weapons and their potential for catastrophic accidents. Using the system surety engineering process ensures a systems engineering approach incorporating basic system safety concepts, resulting in assured system safety.

The system surety engineering process consists of several steps, illustrated in Figure 1. Some of the major steps, with an emphasis on the safety element of surety, are described briefly in the following sections.

Identify system boundaries

A clear understanding of what constitutes the system is required. A system typically is an integration of people, procedures, equipment, and facilities that perform a specific operational task within a specific environment. The system boundaries include the

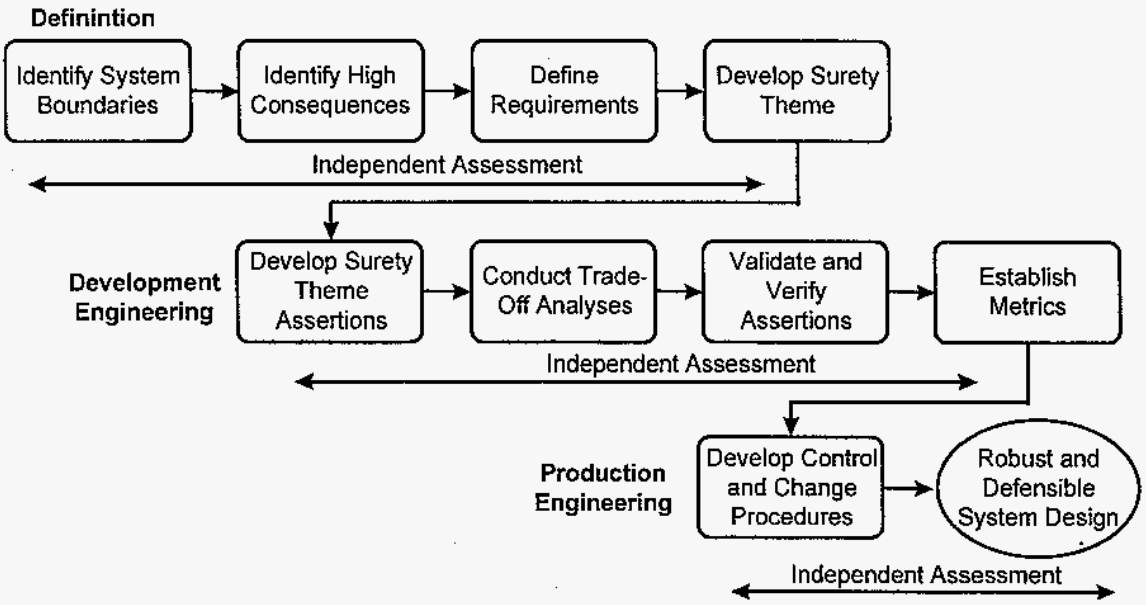

Figure 1. System surety engineering process.

interaction of this set that may contribute to the formation of hazards during the life-cycle of a system. System boundaries and interfaces are specific to the individual system and its life-cycle states. Of special importance are normal and off-normal flows of energy and information across boundaries.

Identify high consequences

The definition and threshold of high consequence varies with the operation and the system owner, but is judged to be severe, *e.g.*, resulting in significant loss of investment or loss of life. This is what the system design must inherently avoid.

Define requirements

Traceable system safety requirements are developed for both operating (normal) as well as accident (off-normal) environments. Defining requirements for system response in accident environments is often overlooked in conventional safety engineering approaches. Often, the most severe environment is not necessarily the most hazardous environment. Requirements should consider how the system is to perform with respect to operations, surety elements, regulations, and potential consequences. Requirements may define hazards to be avoided, credible operating and accident environments, span of operations for all life cycle stages, and system boundaries and interfaces. If there are many consequences and subsequent requirements, requirements may be divided into logical groups for prioritization, such as safety, operational, security, regulatory, *etc.* A good test of an organization's safety culture is where safety is prioritized with respect to other requirements. In a strong safety culture, safety should be the first priority in a high-consequence system.

Develop safety theme

The safety theme describes in a unified fashion the goals and measures that will be used to assure safety under all expected environments The theme broadly defines the philosophy and approach which will eliminate or reduce the hazards, decrease the likelihood or completely eliminate the possibility of initiating events exploiting the hazard, and mitigate the effects of the negative high consequences. The theme establishes the focal point for design and development efforts for meeting safety requirements and provides a framework in which to communicate various design implementations.

Consider again the example of the catalytic reactor. Its safety theme could be to assure predictable safety using the approaches of prevention and protection. The materials in the reactor walls can be engineered to reduce the likelihood of failure when exposed to temperature-induced high pressure, effectively "isolating" the reactor. The system surety engineering theme may add interruption or elimination to the theme. This could be implemented through the use of a catalyst support material with material properties designed to irreversibly fail in a specified thermal environment, interrupting catalytic activity and stopping the reaction before isolation by the reactor is lost.

The safety theme defines those elements of system design which, by association with first principles, become safety critical. The goal is to minimize the number of system components that are safety-critical in off-normal environments. When this is achieved, system safety hinges on a relatively small subset of the overall system design. Limited design and verification resources can then be better focused to increase confidence that predictable safety will result.

Safety theme implementation

The safety theme is implemented through product design and production. The implementation of safety critical elements, defined by the theme, must be first principles based; that is, it must include some characteristic inherent in the physics or chemistry of the element. These safety critical elements are engineered with features that are identifiable, analyzable, and controllable, to provide predictable, assured safe responses. Successful safety theme implementation ensures that that there exists no initiating event that can act upon the hazard to lead to the undesired consequence, resulting in fundamentally assured system safety.

Control of safety critical elements

Once specific safety critical implementations have been selected, they must be controlled when produced, or otherwise realized, to validate and maintain their enduring high standards. There must also be a process to assess any proposed design changes and their impact on the total system safety theme and system safety design. This assessment must determine if any new hazards will be introduced or if existing controls will be bypassed if the change is implemented. This level of change control can be extended to any aspect of the system, including, for example, such things as requirements, specific design features, material characteristics, manufacturing procedures, and acceptance tests.

System safety assessment/design validation

For assured safety, it is important that all system vulnerabilities be recognized. Assertions of safe system performance based on the safety theme can be readily assessed, thereby validating the system safety design characteristics. Validation of these assertions relies on scientific and engineering methods that are supported by testing. The importance of testing is to validate predicted failure mechanisms, and to validate simulation models and understand the uncertainties in these models. Validation of abnormal environment analyses must be particularly scrutinized to ensure conclusions formed are based on sound engineering principles and take into account any simplifying assumptions.

For the example of the catalytic reactor, the safety theme makes two assertions which can be tested to validate the safety design. One assertion is that the reactor can safely contain the pressure generated by a runaway reaction. This can be tested directly, or modeled if the system response is well understood. However, a safety assessment still relies on probability analyses of how likely the reactor is to contain the high pressure. Precise definition of what pressures can be reached in a runaway reaction, based on a definition of the intensity of the thermal environment are needed for this assessment. In the other case, the assertion is that the catalyst will be rendered inoperable before a runaway reaction condition is reached, preventing the possibility of reactor failure. Again, this can be tested directly or modeled. Once this is validated, the safety assessment no longer relies on a precise definition of the high temperature initiating event to determine conformance to requirements. The initiating event can be of any intensity and from any source, since an assured safe response is engineered into the system to eliminate high temperature as an initiating event leading to the negative high consequences. *This is a profound benefit from the sound implementation of the safety theme*—it avoids the need to limit the ultimate intensity of abnormal environments and it avoids the requirement to analyze and test a bewildering array of accident environment scenarios (*e.g.*, directional threats, sequencing of environments, time races) that would threaten the standard ad hoc design.

In the system surety engineering approach, safety assessments are performed according to safety-conservative principles. These principles include the following:

1. "Safety credit" does not accrue for elements not specifically defined by the safety theme, or non safety-critical elements. These elements cannot be relied upon to maintain the system in a safe state. Therefore, a safety assessment assumes such elements will always contribute in the worst way to system failure, even if this is not guaranteed or even expected to be the case.

2. Safety analysis must address external events (*e.g.*, natural phenomena, transportation, accidents at neighboring facilities), internal events (*e.g.*, fires, floods), human errors (*e.g.*, errors of omission or commission), and institutional controls (*e.g.*, staffing, utilities, emergency response).

3. The role of non-engineered hazard controls, such as procedures, personnel training, and warning systems, is minimized in the safety assessment.

4. Energy sources, internal and external to the system, that may trigger failure modes in safety critical elements, in either normal and abnormal environments, are postulated and characterized. These failure mechanisms are analyzed from first principles, for which the knowledge base is relatively stable. Failure modes are not discarded until it is understood that they cannot be manifested, or if they can, the risk is deemed acceptable. Failure modes are not removed *a priori* by appealing to low likelihood of manifestation based on historical data or estimates of accident frequencies, for which the knowledge database is relatively unstable. Understanding system response to low likelihood but high consequence accidents makes the system safety assessment more robust than conventional approaches to system safety assemsements.

5. The use of analytical tools to increase confidence that a design has met its requirements or to guide remedial efforts is acceptable, when appropriate. The tools employed depend on the level of understanding of failure characteristics and initiating events and environments. For failures that are well understood to be stochastic in nature and are supported by a large database, standard probabilistic risk analysis methods may be appropriate. In other instances, different analytical approaches, such as fuzzy logic methods, should be employed (Cooper, 1994). In either case, analysis should focus on safety critical elements. Safety conservatism should be incorporated into all analytical methods.

Other Surety Engineering Elements

There are several other components to a system surety engineering approach that contribute to the overall assured safety program. The following sections summarize some of these important elements.

Operations

High consequence systems should have a plan to continue evaluating the performance of the safety features during the operational phase. This ensures the system will maintain its predictable, safe response throughout the life-cycle. For nuclear weapon systems, this continuing evaluation plan is called a stockpile surveillance plan. Planned refurbishment to improve safety should be consistent with development times to ensure the retrofit is implemented before unacceptable loss of safety occurs.

Lessons Learned

Knowledge of safety related problems on past and related systems can increase the possibility of finding latent failure modes leading to more predictive safety assessments and future advances in system safety as designers become more aware of incomplete

implementations of first-principles. Also, attention to incidents can lead to early detection of safety problems before they become accidents that may result in catastrophic consequences.

Continuous Review Cycle

A periodic and systematic review process that incorporates the appropriate level of peer, management, customer, and independent assessment of the system product and processes is necessary to reduce the possibility of oversights that may negatively impact system safety and to ensure safety requirements continue to be met. Safety reviews will occur for any significant system changes and at regular minimum time intervals. These reviews are known as *clean sheet* reviews because they will reevaluate all known shortcomings and decisions as well as any lessons learned from related systems to determine the current system safety performance. These periodic reviews also serve to take into account the changing technological and societal environment to revalidate the acceptance of the residual risk.

Emergency Response

At times designs and products will fail, people will make mistakes, sequences will be out of control, and unexpected environments will occur. With these considerations in mind, products can be better designed to prevent catastrophic failures, mitigate the effects of a failure, and incorporate appropriate damage control to recover the lost safety as quickly as possible—all in a proactive designed-in approach. Personnel must periodically train, both in the class room and in the field, on how to handle emergency conditions. Drills and practice may bring out needed changes that will enhance recovery of lost system safety.

Nuclear Weapon Example

An example illustrating how system surety engineering is applied to a nuclear weapon is provided below to illustrate some of the key features of the system surety engineering process. While the implementations described are specific to nuclear weapons, the theory and general approach is applicable to a wide range of high-consequence systems.

The focus of the system surety engineering process is on achieving integrated intrinsically safe designs as opposed to tacking on individual elements of safety to an otherwise already-committed-to system design. The term *system* is defined in a broad sense in that it encompasses the entire life-cycle (manufacture to dismantlement) operations of the nuclear weapon.

As described, the process relies on mutually supportive safety design principles that are integrated through the proper implementation of fundamental physical principles, known as first-principles. The design principles of isolation, inoperability, and incompatibility form the philosophical basis for the nuclear weapon safety theme. The appropriate use of first-principles in the implementation of this theme provides the assured predictably-safe behavior required for nuclear weapons.

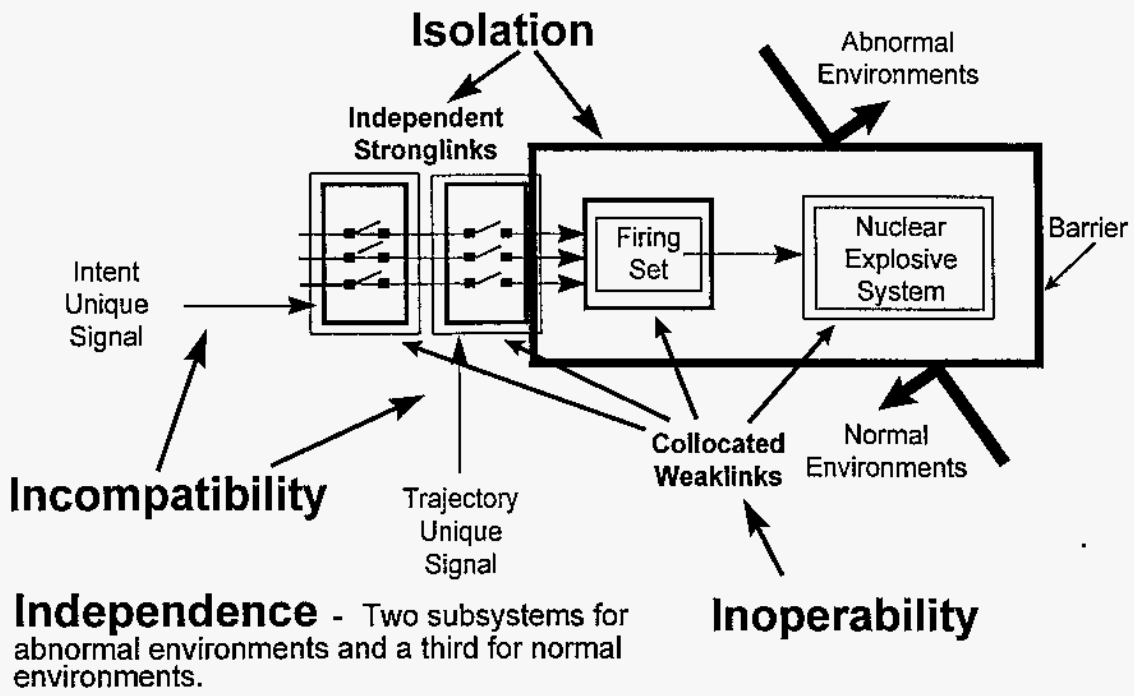

Figure 2. Safety theme and implementation for a nuclear weapon.

The safety theme seeks to prevent unintended nuclear detonation, and allow the system to meet operability requirements without unduly compromising safety. In developing this theme, three design principles are integrated into multiple independent safety subsystems.

The following sections describe the importance of this integration and the key role that independence plays in developing this safety theme. Figure 2 illustrates the key features discussed below.

Isolation

The design principle of isolation is first among equals in the nuclear weapon safety theme. Isolation means to protect elements necessary for producing a nuclear detonation from inadvertent activation until weapon use is authorized. In modern stockpiled weapons, isolation prevents premature operation of the firing system caused by inadvertent flow of energy or information. In the case of unintended energy flow, it blocks or diverts energy from exclusion regions— robust physical barriers that encompass components essential to causing a nuclear detonation.

In the weapon, *stronglinks* control the transfer of energy into the exclusion region. Because stronglinks act as an extension of the exclusion region barrier, these devices must be designed with as equally robust materials as those used in the barriers to ensure energy isolation between input and output is maintained in accident environments. Stronglinks prevent energy transfer when in the safe position and allow energy transfer when in the enabled position. This change of state between safe and enable positions is

controlled by a *unique signal*. The design intent for the stronglink is that it be the only pathway into an exclusion region; for all other circumstances, it and the rest of the exclusion region barrier remain impervious to all unwanted energy sources. In practice, however, isolation is maintained in all operational (normal) environments and in low-to-moderate intensity off-normal (abnormal) environments, such as a fuel fire. However, in high-intensity environments, such as a propellant fire, the exclusion region may eventually fail. Because of this potential failure, an adjunct, fail-safe design principle, known as inoperability, is invoked to make the weapon inoperable before isolation is lost.

Inoperability

Inoperability is the fail-safe criterion. It relies on inherent or designed-in fragility to permanently safe the weapon before isolation is lost. These fragile elements, called *weaklinks*, use a chemical or physical property in their design that will allow proper operation in normal environments and will predictably and irreversible fail when exposed to specified abnormal environments. This combining of functions is an important concept for weaklink designs. Weaklinks are necessary to successful weapon detonation and are located in close proximity to the stronglinks and the isolating barrier to experience essentially the same environments potentially threatening to bypass the isolation features. The design intent for these weaklinks is to fail irreversibly prior to the isolation features, permanently dudding the weapon. Multiple weaklinks may be necessary to cover various types of environments (thermal, crush, *etc.*) or geometric considerations that could threaten isolation.

Incompatibility

The incompatibility principle uses signals or energy forms designed to be highly unlikely to be inadvertently duplicated in normal and in accident environments. Nuclear weapon safety uses this principle in two ways: 1) to prevent accidental loss of isolation by inadvertent stronglink closure; and 2) to communicate intended operation to the stronglink thereby completing the nuclear detonation pathway into the exclusion region. Both these functions are achieved simultaneously via design of the enabling stimuli for a stronglink. Again, the concept of combining functions is key to minimizing the number of safety-critical parts. The stimuli are chosen during weapon development and given unique characteristics that are highly incompatible with the threat they are designed to protect against. Because stronglinks may take several forms, the enabling stimuli may also take on several forms. One form used in nuclear weapons is a sequence of long and short voltage pulses leading to the stronglink. This pulse sequence is the only one that will transform the stronglink from the safe state to the enabled state. Any other pattern will cause the stronglink to remain in the safe state.

Another type of stronglink may be enabled via environmental information. This stimulus is usually derived from some combination of time and acceleration to indicate to the stronglink that the weapon is experiencing its intended use environment, such as missile trajectory. Great care must be taken to engineer the stronglink to discriminate intended time and acceleration information from accident-caused environmental information.

The balanced combination of these three design principles forms the best system safety solution, for nuclear weapons, while maintaining system operability requirements.

Independence

Because requirements to assure nuclear detonation safety in operational and accident environments are very stringent, multiple safety subsystems have been incorporated into modern nuclear weapon systems to avoid total dependence on a single safety subsystem. The use of multiple safety subsystems is not specifically dictated by requirements; such use, rather, reflects engineering judgment about how best to achieve required levels of safety. The choice to use two or more safety subsystems allows simplifying the individual subsystem's design so that the isolation barrier-weaklink strategy has higher confidence in being ultimately successful.

These advantages come at a price, however. The safety subsystems, whether considered collectively or in pairs, must not be subject to chain-of-events coupling between subsystems or common mode failures in which both subsystems are damaged or bypassed by the same event. Thus each subsystem must provide its safety function independently of the others; that is, each must serve its purpose even if the other subsystems are defeated, damaged, or fail.

Independence is required if two or more safety subsystems are employed, and as such, must be ranked as a supporting theme to the safety design principles. As a practical matter, however, multiple safety subsystems are the norm and independence thus becomes critically important. Because its correct implementation requires great care, independence is a very important part of the overall safety theme.

Passive Design Approach

Nuclear weapon safety theme implementation allows a passive design approach. This means that no active response is required to place the weapon into a safe state—it starts out in a safe state and will stay safe until either the environment abates or the weapon becomes permanently inoperable. Safety devices are designed to be in an inoperable state until proper authorization is received. This is how modern stronglinks are designed. They remain in a passive, safe position until the enabling unique signal is received.

One might consider that an active approach is used in the design of weaklinks. For example, a weaklink may be required to change state (*e.g.*, melt) to render a system inoperable. However, a key concept is that this change-of-state is based on first-principles. Since first principles employs the fundamental laws of nature in the chemical or physical properties of materials to assure predictable response of a designed or engineered device, the probability of the state change occurring is one. Because the weaklink has used first-principles to implement its safety function, it can be viewed as taking a passive approach.

Benefits of the System Surety Engineering Approach

There are several benefits to using the system surety engineering process to designing high consequence systems. These benefits include:

1. An assured, predictable, and validated safe response of the system in normal and in a broad range of accident (off-normal) environments.
2. No need to limit the ultimate intensity of abnormal environments nor to analyze and test a bewildering array of accident environment scenarios.
3. A designed-in safety assurance approach for increasingly complex system designs and operations.
4. An integrated system of positive measures to meet safety requirements and standards.
5. A method for recognizing non-safety functions of safety-related hardware and making design tradeoffs.
6. A clear understanding of residual risk can be obtained associated with the tradeoffs.
7. A controllable and traceable design and production path to the requirements.
8. A predictive capability for determining the onset of safety degradation.
9. A method for identifying measurable safety improvements.
10. A method for optimizing system safety.
11. A method for identifying priorities for remedial action, if needed.

Conclusions

The application of the system surety engineering process, developed for assuring the safety of nuclear weapons, results in robust, safe system designs. Predictable safe system response in normal and off-normal conditions and environments is assured through the integration of mutually supportive design principles and fundamental first principles, based on the laws of chemistry and physics. Although developed for nuclear weapon design applications, the system surety engineering theory and approach has broad application to a wide variety of other high-consequence systems and industries.

Acknowledgements

The thematic approach to system safety was conceived and developed at Sandia National Laboratories over the course of several decades. Many individuals have contributed to its development over the years and to its refinement as the current system surety engineering process. Our recognition and thanks go to those who have "been there" before us.

References Cited

Center for Chemical Process Safety (CCPS) (1992). *Guidelines for Hazard Evaluation Procedures, Second Edition With Worked Examples*. New York: American Institute of Chemical Engineers.

Center for Chemical Process Safety (CCPS) (1996). *Inherently Safer Chemical Processes: A Life Cycle Approach*. New York: American Institute of Chemical Engineers.

Cooper, J. A. (1994). *Fuzzy-Algebra Uncertainty Analysis for Abnormal-Environment Safety Assessment*. SAND93-2665, Albuquerque: Sandia National Laboratories.

Gowland, R. T. (1996). "Putting Numbers on Inherent Safety." *Chemical Engineering* 103, 3 (March), 82-86.

The Institution of Chemical Engineers (IChemE), and The International Process Safety Group (IPSG) (1995). *Inherently Safer Process Design*. Rugby, England: The Institution of Chemical Engineers.

Kletz, T. A. (1978). "What You Don't Have, Can't Leak." *Chemistry and Industry* (6 May), 287-92.

Kletz, T. A. (1984). *Cheaper, Safer Plants, or Wealth and Safety at Work*. Rugby, Warwickshire, England: The Institution of Chemical Engineers.

Kletz, T. A. (1991). *Plant Design for Safety*. New York: Hemisphere.

Kletz, T. A. (1996). "Inherently Safer Design—The Growth of an Idea." *Process Safety Progress* 15, 1 (Spring), 5-8.

Mansfield, D. P. (1996). "Viewpoints on Implementing Inherent Safety." *Chemical Engineering* 103, 3 (March), 78-80.

Trauth, C. A., Jr. (1997). Personal communication, Sandia National Laboratories, Albuquerque.

Report Number (14) SAND--97-3099C
CONF-980318--

Publ. Date (11) 199712
Sponsor Code (18) DOE/MA, XF
UC Category (19) UC-900, DOE/ER

DOE