SAND2014-4182C

Exceptional service in the national interest

Sandia National Laboratories

Nuclear Safety Design Principles & the Concept of Independence: Insights from Nuclear Weapon Safety for Other High-Consequence Applications

SAND2014-????C

Jeffrey D. Brewer / Sandia National Laboratories

PSAM 12, June 2014 505-845-0494 jdbrewe@sandia.gov

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

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. 2014-????C

Outline

- Assured Nuclear Weapon (NW) Safety
  - Energy Scenarios: Front, Side, & Back Doors
  - Nuclear Safety Design Principles (NSDPs)
  - Four Step Process of Implementing NSDPs
- The Concept of Independence
  - Independence, Common-Cause Failure, Common-Mode Failure
  - Functional Independence
  - Temporal Independence
  - Physical Independence
  - Practical Tools for Generating / Identifying Independence Features
- Summary

Goal: Prevent Catastrophic Consequences

- **Problem:** Prevent inadvertent nuclear detonation (**IND**) & special nuclear material **dispersal**
  - Probability of IND must be < 1E-9 per weapon lifetime
  - Probability of IND must be < 1E-6 per credible accident
- **Solution – Assured NW Safety:** An approach to provide a robust technical basis for asserting that a NW system can meet safety requirements in the widest context of possible adverse or accident environments, using the most concise arrangement of safety design features and the fewest number of specific environment assumptions.

  *Rigor in understanding and applying the concept of **independence** is crucial for the success of the approach.*

Notional Nuclear Weapon

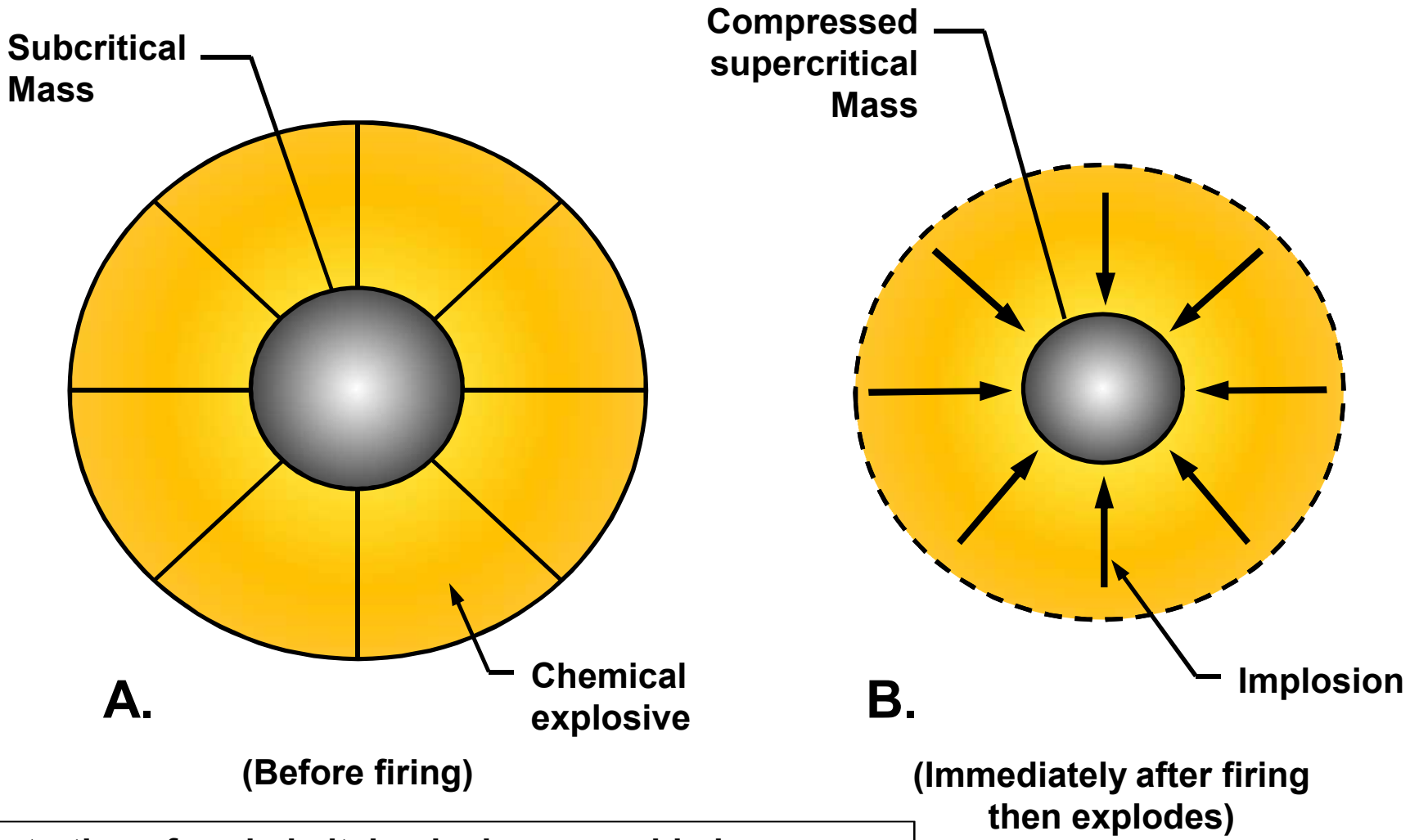


Illustration of sealed pit, implosion assembled weapon.

Sandia National Laboratories

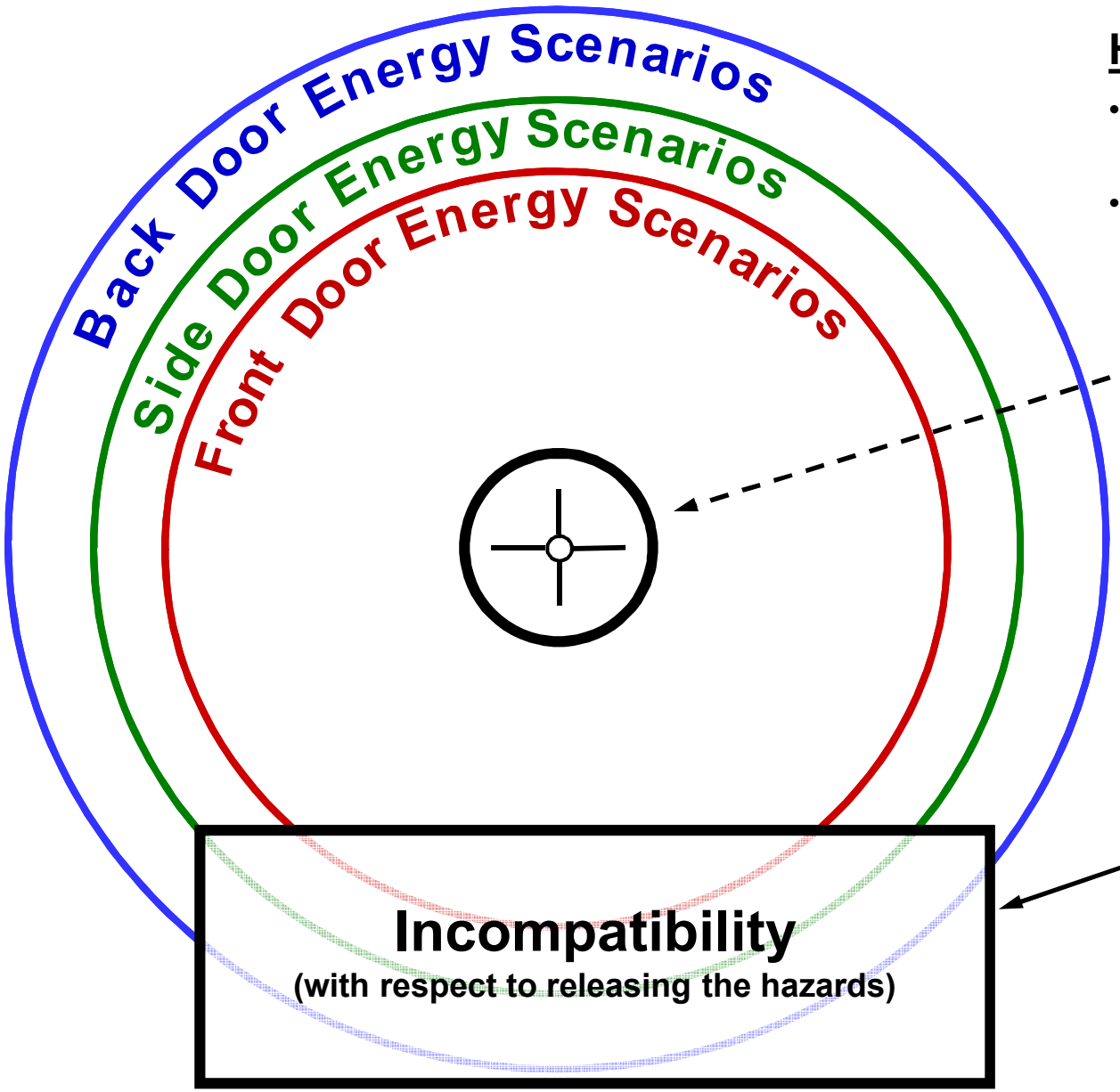
Types of Energy Scenarios

- **Front Door Energy Scenarios —** operating the high explosive (HE) detonation system using the intended energy storage/production devices designed to operate the HE detonation system or another internal energy storage/production device that is compatible with operating the HE detonation system.
- **Side Door Energy Scenarios —** operating the HE detonation system in any way that does not involve the intended energy storage/production devices or another internal energy storage/production device.
- **Back Door Energy Scenarios —** direct initiation of the high explosive material required to achieve a nuclear detonation; the HE detonation system is either irrelevant or simply plays a secondary role in achieving a nuclear detonation.

Back Door: High Explosives (HE) Surrounding Fissile Material

Back & Side Door: HE Detonation System Included

Back, Side & Front Door: Intended Energy Source(s) for Operating HE Detonation System



Hazards to Safety

- Inadvertent / Premature Nuclear Detonation
- Dispersal of Special Nuclear Material

= **Intended Use**

- Human Intent
- Correct Time & Place
- Compatible Energy

Incompatibility between intended use & all other energy and stimuli **provides the context for everything else. It tells you what type of *isolation* is needed and when *inoperability* is achieved.**

Sandia National Laboratories

Nuclear Safety Design Principles

- Incompatibility – the use of energy or information that will not be duplicated inadvertently
- Isolation – the predictable separation of detonation-critical elements from compatible energy
- Inoperability – the predictable inability of detonation-critical elements to function

Safety Theme – a high-level, concise expression of what will be isolated, inoperable and/or incompatible.

Sandia National Laboratories

Four Step Process of Implementing NSDPs

1. Develop a nuclear weapon that is **incompatible** with all forms & levels of energy except the correct sequence of intended, authorized, and unambiguous energy and stimuli.

2. For any part of the system that is compatible with unintended energy or stimuli, provide **isolation** from that energy or stimulus that could lead to an accidental explosion of any kind, and/or provide a **reversible inoperability** feature to eliminate or minimize exposure to safety hazards. The inoperability feature must be **incompatible** with all forms and levels of unintended energy and stimuli.

3. For any isolation feature that also blocks intended energy , provide a **reversible isolation** feature (a.k.a., a stronglink) to allow only intended energies to propagate to the HE detonation system. The stronglink must be **incompatible** with all forms and levels of energy and stimuli except the correct sequence of intended, authorized, and unambiguous energy and stimuli.

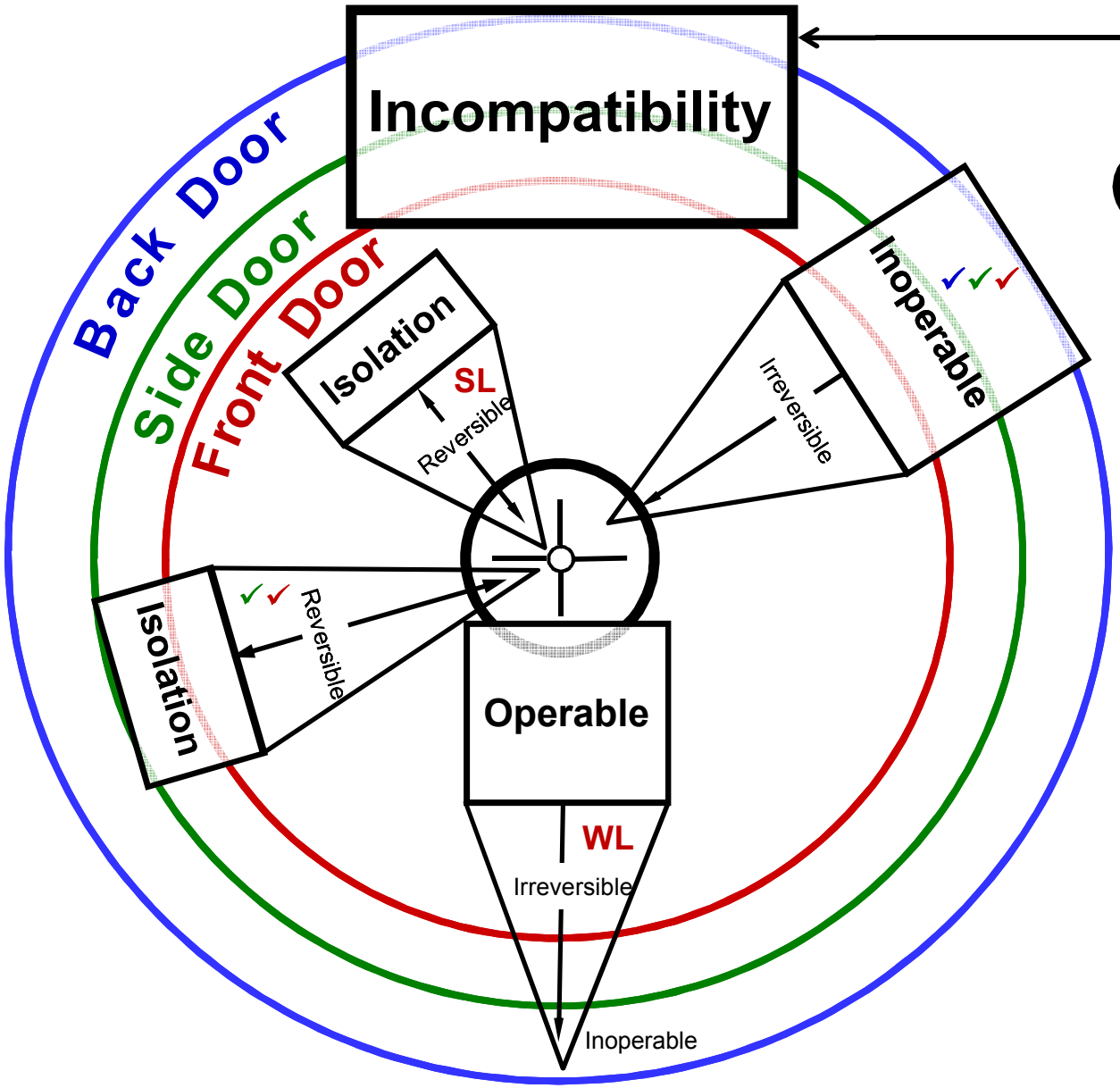
4. For any of these stronglinks, isolation features, reversible inoperability features, or incompatibilities that are subject to failure, provide an **irreversible inoperability** feature (a.k.a., a *weaklink*) that passively renders the nuclear weapon **inoperable** and incapable of producing an accidental explosion of any kind before such failure.

High Explosives

HE Detonation System

Intended Energy Source(s)

Nuclear Safety Design Principles (NSDPs)



Provides the context for everything else

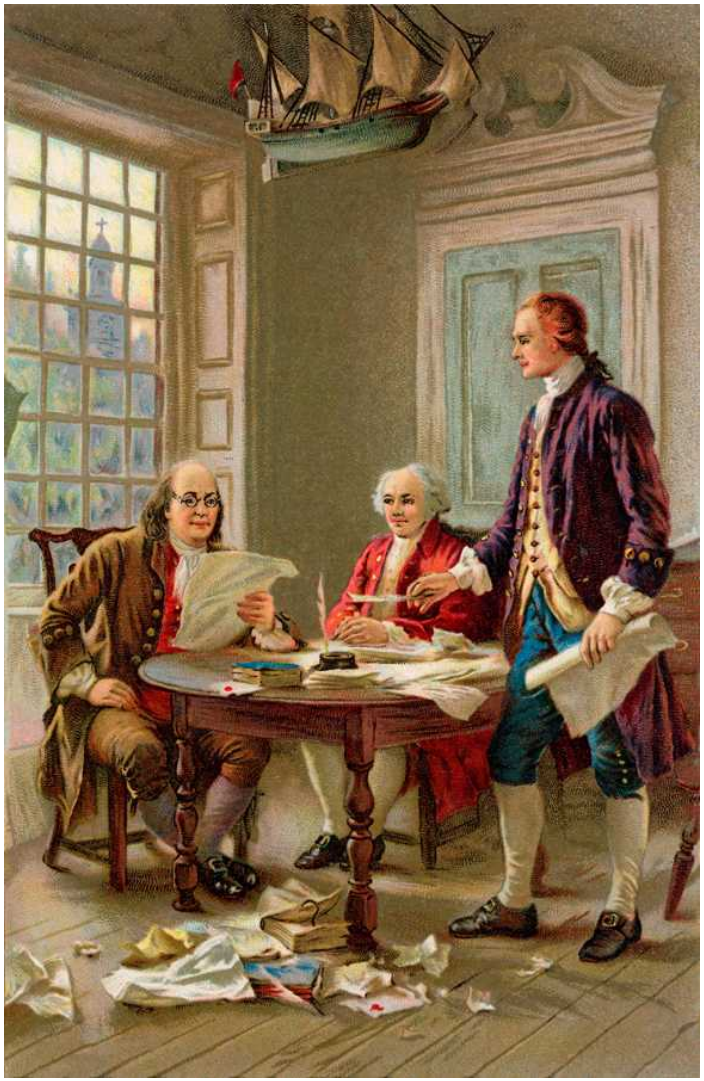
⊕ = **Intended Use**

- Human Intent
- Time & Place
- Compatible Energy

- Predictable Safe Response (essential)
- First Principles of Physics & Chemistry (FPPC)
- Inherent Safety (best)
- Passive Safety (good if FPPC solid for relevant environments)
- Active (fine if FPPC solid for relevant environments)
- Independence of Safety Features (often essential)

The Concept of Independence

No, It's Not That kind of Independence Talk!



What is Independence? New Definition

Independence – The occurrence of a state of one or more things does not provide any information regarding the likelihood of occurrence of another state of one or more things, or sequences thereof.

The concept of independence provides meaning only when describing the attributes of the relationship between two or more states, or sequences of states, of one or more things.

State – a mode or condition of being (Merriam-Webster 2010).

Thing – an item ranging from ideas and concepts to physical objects or processes (Merriam-Webster 2010).

It is important to realize that independence is defined by the *absence* of information.

Typical Definitions & Applications of Independence

- Event (A) and event (B) are independent events if $P(A|B) = P(A)$ and $P(B|A) = P(B)$, thus $P(A \cap B) = P(A)P(B)$. Recall that in general, $P(A \cap B) = P(A) \cdot P(B|A) = P(B) \cdot P(A|B)$, given $P(A) \neq 0$, $P(B) \neq 0$.
- Two events are independent if the outcome of one event does not influence the other event; i.e., knowing the outcome of a flip of a fair coin provides no additional insight about whether the next coin toss will reveal a head or tail.
- Beware not to confuse *independent* with *mutually exclusive*
- In the domain of formal experimentation, most common statistical tests require independence between events.
  - Independence forms the basis of hypothesis testing
  - To detect dependence between selected/manipulated factors, it is necessary to minimize the effect of sources of dependence which may not be controlled
- Typical examples: fair coin flips, cards from well-shuffled decks, fair die rolls, balls from a well-mixed urn, casino & lottery games

All involve well-defined and fixed boundary conditions or rules—unlike inadvertent nuclear detonation where many uncertainties regarding AEs exist





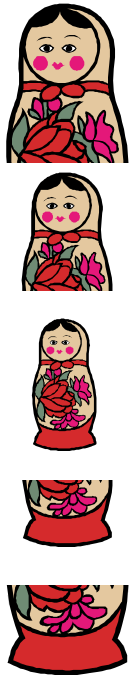

Independence Assumptions & Assertions

- Formal definitions of independence encountered during academic training are founded upon verification using a sufficient amount of observed data for all relevant contexts. They do not provide much assistance for verification in situations where data are sparse or non-existent (Brewer 2009).

- "***Declaring*** events independent for reasons other than those prescribed in (the formal definition) is a necessarily subjective endeavor. In practice, all we can do is look at each situation on an individual basis and try to make a ***reasonable judgment*** (emphasis added) as to whether the occurrence of one event is likely to influence the outcome of another" (Larsen and Marx 2001), p. 74).

- In the nuclear weapon safety domain, it is essential for analysts to resist the temptation of over-relying on the concept without providing a rigorous technical basis to justify independence assumptions relative to a decomposition of normal environments and abnormal environments (Brewer 2009).

New Definitions & Terminology



Independent Subsystems – design of subsystems to prevent common-mode and common-cause failures such that the failure of one subsystem does not affect the failure of another subsystem.

1 for Normal & 2 for Abnormal Environments

(< 1E-3) x (< 1E-3) x (< 1E-3) = < 1E-9

Common-Cause Failure – Failures involving multiple design attributes of a system that fail as a result of the same causal event or the same type of causal event. The mode of failure across the design attributes may be different.

Common-Mode Failure – Failures involving multiple design attributes of a system that fail in a similar manner as a result of the same causal event or the same type of causal event.

New Definitions & Terminology

Sandia National Laboratories

In many cases the distinction between Common-Cause & Common-Mode Failure is not necessary, sometimes it is:

Example 1: Maintenance worker uses faulty procedure, leaves 3 identical valves in the open state when they should be closed.

Example 2: Lightning strikes a system, one part fails due to a minor electrical short, one part deflagrates, one part melts, another part with a solenoid actuates to an unsafe state.

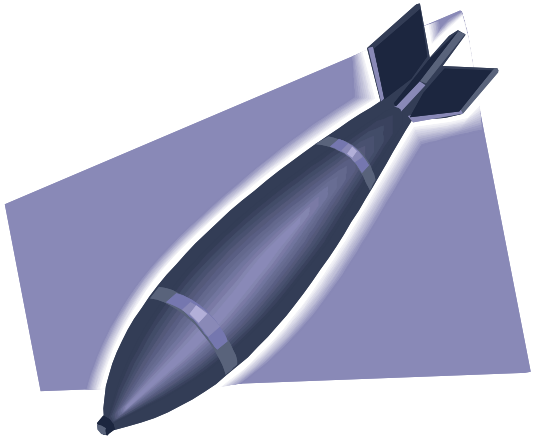
The distinction makes it easy to conceptually separate the modes of failure across multiple parts of a system given exposure to the same cause.

Technical Basis for Independence Assertions

How can one develop a rigorous, defensible technical basis justifying independence assertions in situations where data are sparse or non-existent?

Independence assertions can be founded upon the distinctions of ***functional***, ***temporal***, and ***physical*** differences.

Ideally, a technical basis for assuring independence between events would be established that is not greatly affected by all three factors of function, time, and physical properties, but achieving such a technical basis is difficult for a system that is designed to execute specific goal-directed behaviors.



Technical Basis for Independence Assertions

Sandia National Laboratories

Function, **Time**, **Physical Isolation**,

—while not providing mutually exclusive sources of "dependence," they are proposed as helpful concepts in the search for tendencies toward independence (both with respect to "energy" and "information")

Functional independence between two or more states of one or more things is increased when the states are achieved by functions that use different types of energy, logical relationships, materials, mechanisms, and/or methods of operation. Thus, phenomena best described as function variant are able to introduce independent effects during exposure to unintended environments.

Temporal independence between two or more states of one or more things is increased by manipulating the time when states may be achieved. Thus, phenomena best described as time variant are able to introduce independent effects during unintended environments.

Physical independence between two or more states of one or more things is increased when the states must be achieved on different sides of one or more barriers or there are significant intervening structures. Thus, phenomena best described as involving physical segregation are able to introduce independent effects during unintended environments.

Temporal Independence

Temporal independence may be increased by minimizing the time of exposure of energy or information to the system, or maximizing the time separation of packets of energy, enabling stimuli, or packets of information provided to the system, or some combination of each given the environmental context.

Time-related differences:

- Limiting times of mechanical operation
- Timer-based functions
- Manipulating speeds for digital communication of information
- Enforce single-sequential operations

Example of temporal differences between Subsystem 1 and Subsystem 2 with respect to energy isolation:

- Viscous damped interlock in subsystem 1 requires 10 sec to actuate
- Spring pin interlock in subsystem 2 re-latches if not operated within 300 msec
- Subsystem 1 interlock must operate before subsystem 2 interlock

Practical Tools for Generating / Identifying Independent Features

Sandia National Laboratories

The process of testing independence assertions should include **specific propositions**, framed both in **positive** and **negative frames of reference**, explicitly addressing **functional**, **temporal**, & **physical** attributes, which are supported using theoretical, analytical, and experimental models.

Positive frame:
Energy isolation features of safety subsystem 1 are independent of the isolation features of safety subsystem 2 with respect to exposure to a high voltage electrical environment.

Negative frame with open ended responses for justification:
Inadvertent generation of the _____ does not provide information aiding in removing isolation provided by _____ due to the following attributes of independence: _____, _____, _____.

Functional, Temporal, & Physical Attributes:
Attributes of independence between the _____ and the _____ with respect to _____ which are best described as **functional** include:
_____, _____, _____.

Checking for Independence

Sandia National Laboratories

"If the electrical enabling energy or information stimuli where changed, would one or both of the safety features need to be modified to accommodate the change to maintain a safe response in a predictable manner?"

– if both safety features must be changed then it may represent a lack of independence between the features.

This same type of question can be adapted to investigate independence-related impacts of any change involving the key elements of the safety theme that implement any of the Nuclear Safety Design Principles.

Checking for Independence

Sandia National Laboratories

"If the mechanical enabling energy or information stimuli where changed, what design features need to be modified to accommodate the change to maintain a safe response in a predictable manner?"

– If any design features must be changed, then it may indicate pre-storage of some portion of enabling stimuli information that should only originate from the intended human actions, or only from the physical stimuli experienced by the weapon during normal anticipated operations; thus it is information or energy that should never be pre-stored in the system

Summary

- Assured Nuclear Weapon (NW) Safety
  - Energy Scenarios: Front, Side, & Back Doors
  - Nuclear Safety Design Principles (NSDPs)
- The Concept of Independence
  - Independence, Common-Cause Failure, Common-Mode Failure
  - Functional, Temporal, Physical Independence
    - Need for all 3 is increased where data are sparse and possible consequences are high.

The ***assured nuclear weapon safety*** approach:

- Achieves a robust technical basis for asserting that a system is safe in the widest context of environments
- Using the most concise arrangement of safety design features and,
- The fewest number of specific adverse or accident environment assumptions

In essence, this approach claims to be an efficient approach for engineering bounded system safety-related responses.