SAND2018-8451C

Modern U.S. Nuclear Weapon System Safety Design Process and Q&A with NW Experts

Nuclear Safety Assessment
Sandia National Laboratories

Jeffrey D. Brewer

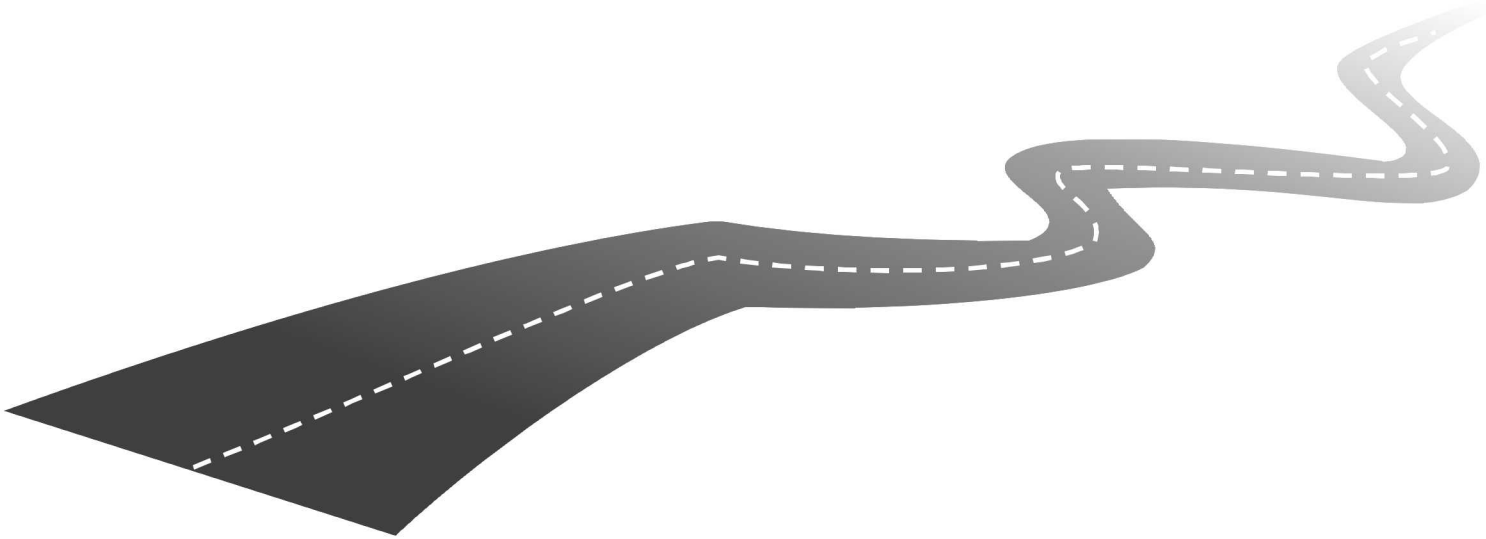
Foundational Innovators of U.S. Nuclear Weapon Safety Include:
W. L. Stevens, S. D. Spray, J. A. Cooper

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND NO. 2018-xxxx C

SAND2018-xxxx C

Road Map

- Overview of nuclear weapon system safety design process
- Overview of nuclear weapon system safety life-cycle assurance process
- Address questions

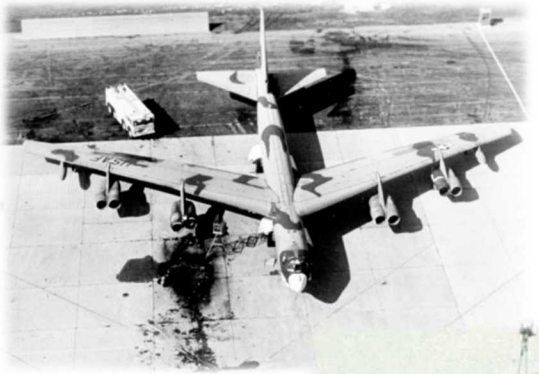


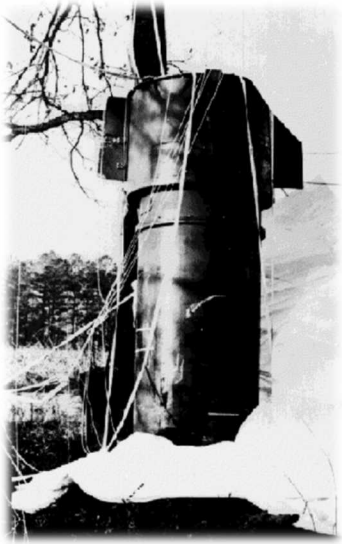
Sandia's Role

- The engineering arm of the nation's nuclear weapons enterprise
- Responsible for the non-nuclear components of U.S. nuclear weapons.
- Sandia integrates these components with the nuclear explosives package to maintain a militarily effective and sustainable U.S. nuclear deterrent.
- Ensure Always/Never…
  - They must *always* work if authorized by the president of the United States.
  - They must *never* work if not authorized.

Four Accidents Leading to Change

- 1961 - Goldsboro, NC
- 1964 - Bunker Hill, IN
- 1966 - Palomares Spain
- 1968 - Thule Greenland





Weapon Safety Design

Sandia National Laboratories

"We are trying to accomplish a design which will have a vanishingly small risk of a nuclear detonation given exposure to any credible abnormal environments."
--Morgan Sparks, President, Sandia Laboratories, 1977

Requirements to preclude these Unsafe States:

Unintended nuclear detonation (UND) & special nuclear material dispersal

- Probability of UND must be < 1E-9 per weapon lifetime
- Probability of UND must be < 1E-6 per credible accident
- Probability of UND must be < 1E-3 (bomb) or < 1E-4 (warhead) until arming firing set, as close to the target as reliably achievable

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 multiple safety design features, engineered to have independent failure causes, and which require the fewest specific environment assumptions in order to ensure that safe responses occur in a *predictable manner*.

Independent Safety Assessment throughout the weapon lifecycle.

Sandia's Assured Safety Approach

Fundamental Nuclear Safety Requirements:

1. Use the 3 I's to Provide Assured Safety
    - **Incompatibility**, **Isolation**, **Inoperability**
2. Develop a Nuclear Safety Theme and Theme Implementation Details (e.g., specific components and features)
    - **Independent failure causes** among layers
    - **Predictable safe response** throughout
3. Implement the theme by flowing down requirements
4. Document in Nuclear Safety Specification (NS)

And

5. Independent Assessments Throughout Entire Life-Cycle:

> **Design** — at multiple stages allowing for iteration, **Production**, **Annual Assessment of Stockpile**, …, **Dismantlement**;
> *Separate Funding and Management Chain for Assessors*

Nuclear Safety Design Principles

Sandia National Laboratories

Incompatibility – the use of energy and/or information that will not be duplicated inadvertently. This includes energy required for detonation to occur and energy and information associated with safety features.

Isolation – the separation of weapon elements from compatible energy. Barriers and exclusion regions are employed to predictably prevent uncontrolled access to detonation-critical components by energy sufficient to cause a nuclear detonation.

Inoperability – The inability of weapon elements to function. This is often accomplished in the form of predictably achieving irreversible inoperability of one or more detonation critical elements prior to loss of isolation features. However, it may also involve a reversible or controlled inoperability feature that must function to allow the weapon to operate as intended.

Multiple layers or "safety subsystems" with **independent causes of failure** in all **relevant environments**.

All 3 principles must be implemented such that they accomplish their intended function in a **highly predictable manner** in all **relevant environments**.

Basic Nuclear Weapon Design Considerations

Notional Nuclear Weapon

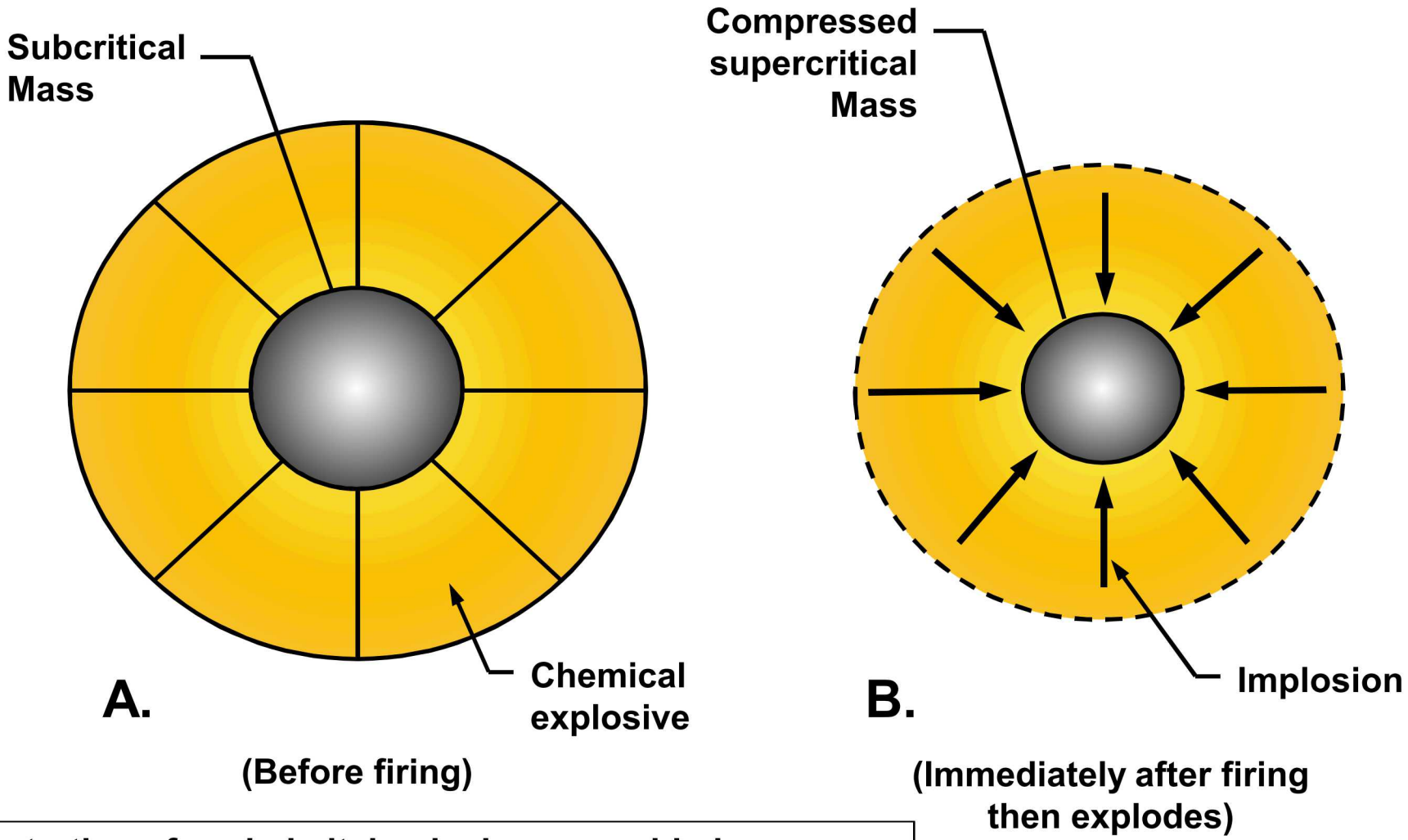


Illustration of sealed pit, implosion assembled weapon.

Sandia National Laboratories

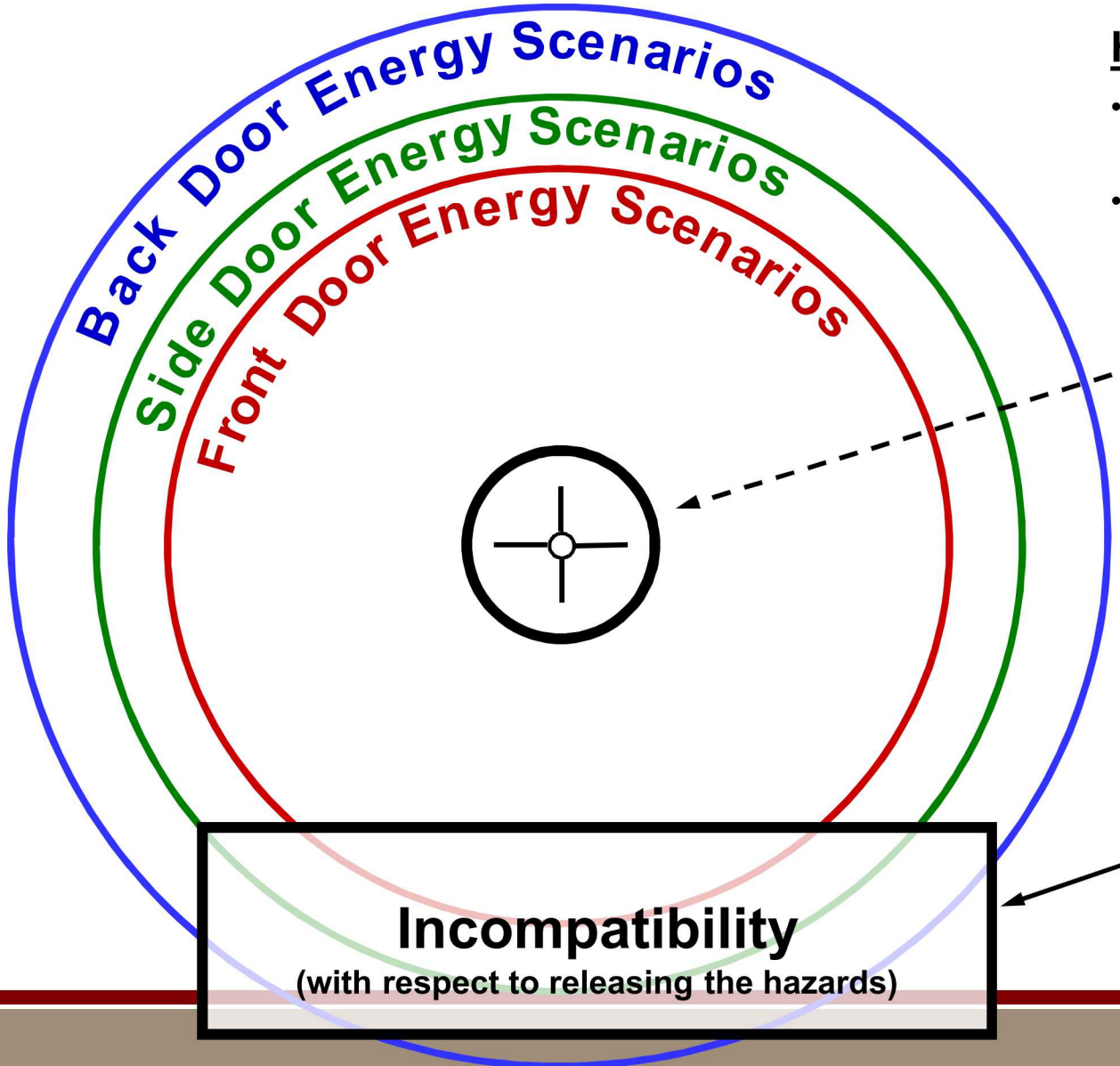
Types of Energy Scenarios

- **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.

Incompatibility
(with respect to releasing the hazards)

Inside Out Approach

The 5 step process of applying the Inside Out Approach:

1. Identify the simplest configuration of system elements that present a safety hazard of concern.
2. Evaluate all hazards to safety and the possible energy types, energy sources, energy pathways, and information that may facilitate unsafe consequences.
3. Add the next design feature to the simplest configuration.
4. Evaluate hazards, energy, and information as in step 2.
5. Repeat the process until the full system design configuration has been analyzed.

Inside Out Approach

Sandia National Laboratories

The inside out (IO) approach, when repeated at various times in the system design process, is an excellent means of identifying hazards and incorporating an arguably complete set of features to control the hazards throughout the lifecycle of the system.

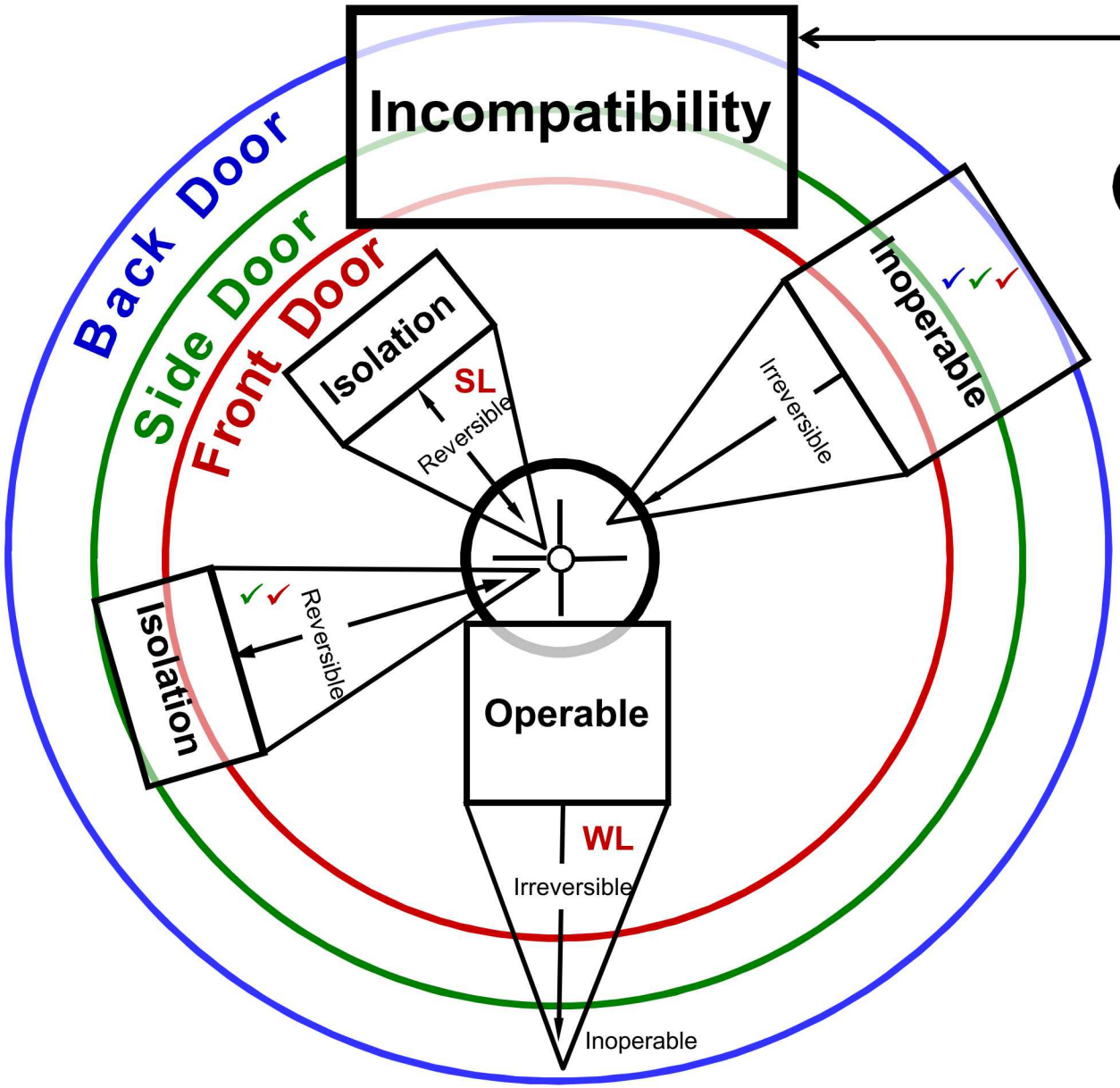
The IO approach proves beneficial for deciding how to manage hazards during the production process of a weapon system, as well as assessing levels of safety when the weapon system is fully assembled or partially assembled either due to adverse or accident environment exposure or due to assembly or dismantlement actions.

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)

Safety Theme & Safety Theme Implementation

Safety Theme – for a specific system, a high-level, concise expression of what will be isolated, inoperable and/or incompatible to provide assured safety

Safety theme Implementation – a detailed explanation of how independent safety subsystems and associated safety design features are integrated into a system to provide assured safety. The safety design features should provide their safety function in an inherently safe or passively safe manner.

Active and Passive Safety Concepts

- **Active Safety Feature** – **Do Something!**
  - A feature that relies on a change of state or some kind of action (i.e., “open” to “close,” “off” to “on”) in order to make the system safe
  - Example: air bag (release must be triggered)

- **Passive Safety Feature** – **Do Nothing!**
  - A feature that is already in a safe state and does not rely on a change of state in order to make the system safe (i.e. it is “born / built safe”)
  - Example: physical barrier

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.

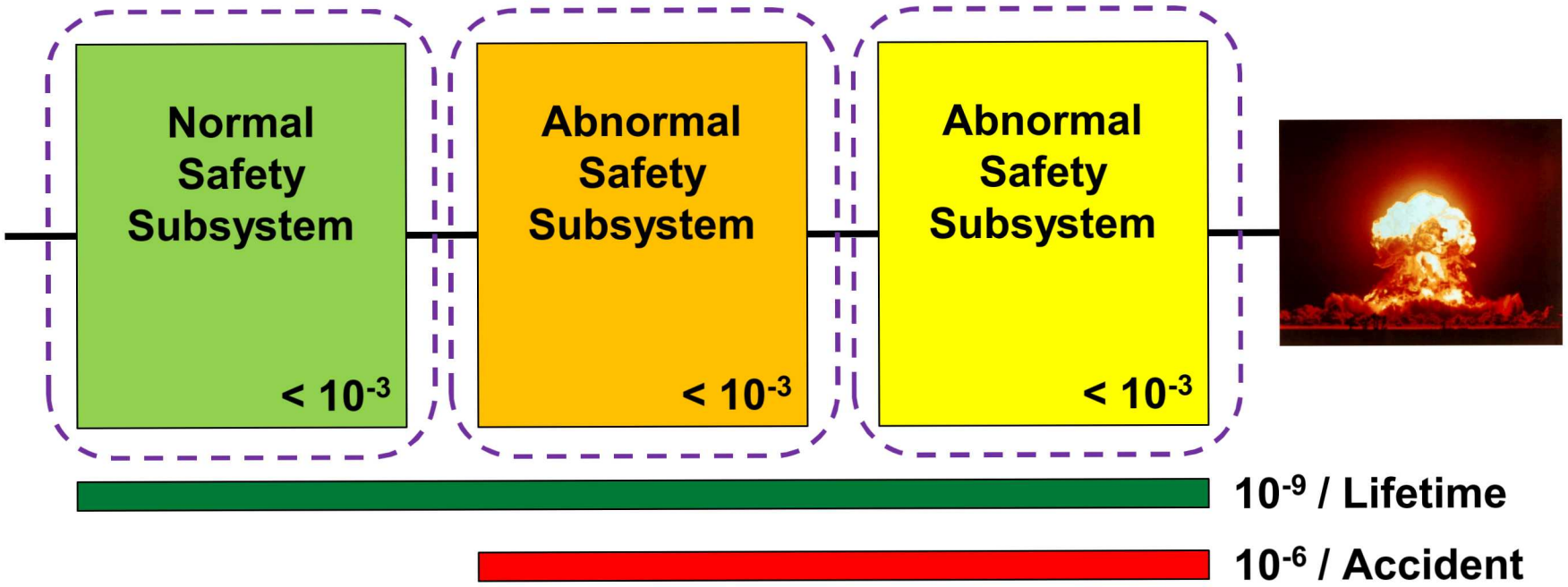
2. For any part of the system that is compatible with unintended energy or stimuli, provide **isolation** from that energy or stimulus that could lead to an accidental explosion of any kind, and/or provide a **reversible inoperability** feature to eliminate or minimize exposure to safety hazards. The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

Independent Safety "Layers" in Weapon Design

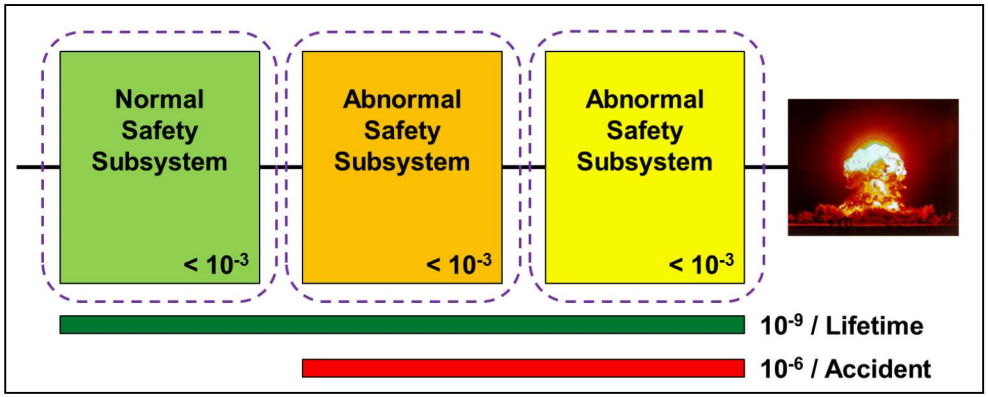
Independent Subsystems – Design of subsystems to prevent common-mode and common-cause failures such that the failure of one subsystem does not affect the failure of another subsystem



Independence

Independence of **failure cause** concept – *practical strategy* for defensible assertions that safety requirements have been met both within and between safety layers / subsystems.

First strategy = multiple layers of safety with independent failure causes



Second strategy = independent failure causes for elements within single subsystem, thus, all must fail to compromise safety critical function.

Third strategy = independent failure causes for safety critical & reliability critical functions.

For example, a stronglink design where failures of piece parts X, Y, and Z are independent of the failure of the shutter to isolate abnormal electrical energy.

Focus on independence of failure causes between safety and reliability critical functions can lead to simplified designs with stronger tech basis for accomplishing safety functions.

Encouraging Independence Between Failure Causes

Sandia National Laboratories

• Spatial separation	• Different method of operation per first principles of physics & chemistry	• Different design teams
• Geometric differences	• Different orientations of otherwise similar components	• Independent verification and vulnerability review teams searching for dependencies between the designs
• Temporal spacing of sequential functions	• Different energy types of operation	
• Different materials	• Geometric homogeneity of energy isolation features (e.g., spherical)	
• Different energy levels	• Different chemical processes / phases	
• Different information for intended use	• Different logic structures/algorithms/protocols	• Different human actions for intended use
• Different locations for redundant functions	• No pre-storage of human intent information	• Sense different environments

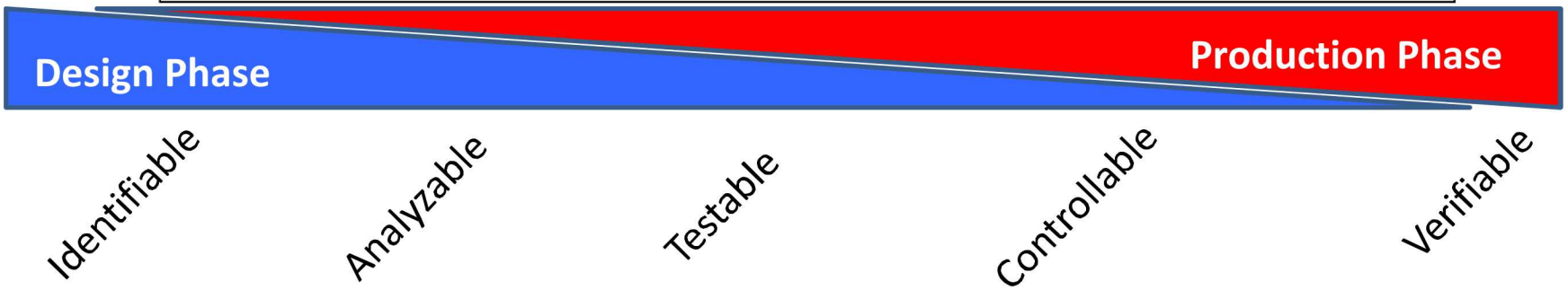
- Independent assessments: Design — at multiple stages allowing for iteration, Production, ... Dismantlement; Separate Funding and Management Chain

Predictability

The Safe Responses must be <u>Predictable</u>

We must know why / how / when / where design features will remain safe or fail safe

Predictability Attribute	Attribute Description
Identifiable	Can point to the critical parameters of the safety features in the theme
Analyzable	Amenable to analysis techniques available
Testable	Can be demonstrated by physical testing
Controllable	Can be produced in a repeatable fashion
Verifiable	Critical parameters can be shown to have met their requirements



Nuclear Safety Realities

- **Sandia Contractual Requirements**
  - DOE Order 452.1E: Nuclear Explosive and Weapon Surety (NEWS) Program
  - Military Characteristics (MCs)
  - Stockpile to Target Sequence (STS)
- **Sandia Implementation**
  - Nuclear Explosive and Weapon Surety (NEWS) Policy
  - RPP: Nuclear Weapon Safety Throughout All Design Phases
  - Derived Requirement (subassembly) Documents

Nuclear Safety is *Asserted*

- **Nuclear safety is *asserted* to be achieved through the robust use of three independent safety subsystems**
  - One normal environment subsystem
  - Two abnormal environment subsystems
  - Each subsystem is asserted to assure safety to 1E-03
- **Numerical nuclear safety requirements (Walske) can NOT be proved through a standard qualification and test program;**
  - Approximately 700 tests (with no failures) must be conducted to demonstrate 50% confidence that one (1) nuclear safety subsystem meets its nuclear safety requirements of 1E-03 for one particular subset of conditions

Nuclear safety requirements are ASSERTED to be met through robust engineering design based on 1st principles, limited testing, quality control, and expert judgment

Sandia's Assured Safety Approach

Fundamental Nuclear Safety Requirements:

1. Use the 3 I's to Provide Assured Safety
    - **Incompatibility**, **Isolation**, **Inoperability**
2. Develop a Nuclear Safety Theme and Theme Implementation Details (e.g., specific components and features)
    - **Independent failure causes** among layers
    - **Predictable safe response** throughout
3. Implement the theme by flowing down requirements
4. Document in Nuclear Safety Specification (NS)

And

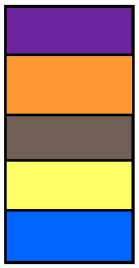
5. Independent Assessments Throughout Entire Life-Cycle:

> **Design** — at multiple stages allowing for iteration, **Production**, **Annual Assessment of Stockpile**, …, **Dismantlement**; *Separate Funding and Management Chain for Assessors*

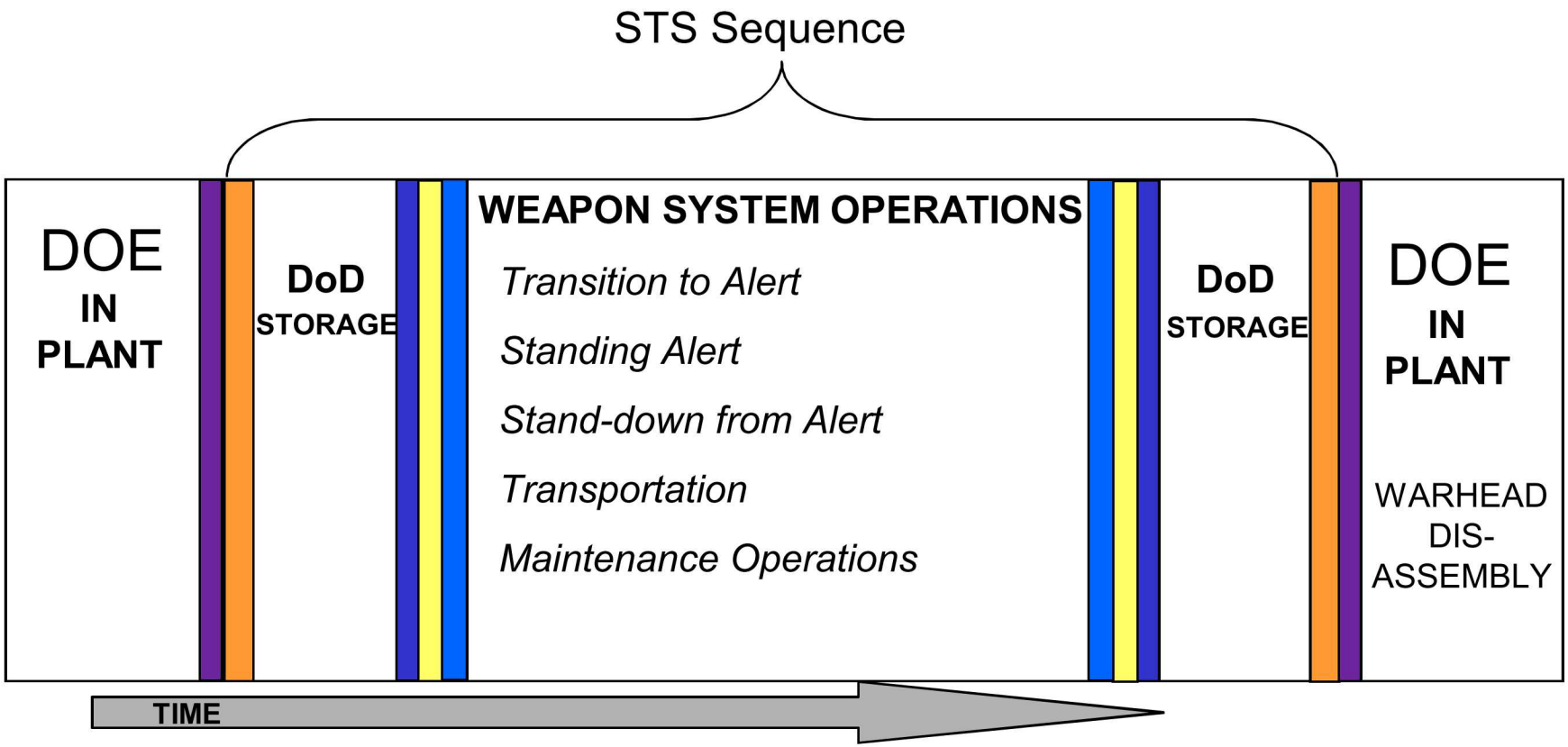
Nuclear Safety is *Challenged*

- **Nuclear Safety Assessment conducts independent and unbiased technical assessments of US nuclear weapon safety and of related nuclear explosive operations**
  - The department was established at Sandia in 1968 following the Palomares and Thule accidents
  - Organizationally independent of the design organizations
  - Operates under independent funding
  - Reports directly to Sandia Executive Management
  - Reviews and comments on the design organization's *Assertions* during the weapon's lifecycle
  - Can challenge any aspect of nuclear safety throughout a weapon's lifecycle
  - Participate on DOE and DoD safety studies

Stockpile-to-Target Sequence (STS) and Weapon Manufacture to Retirement Sequence (MRS)



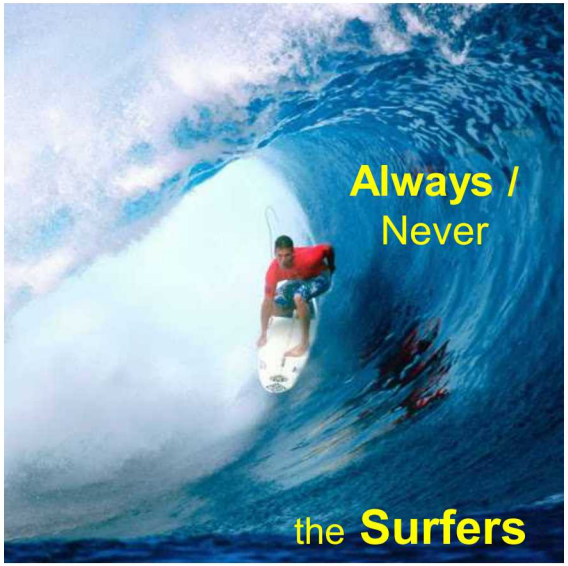
DOE Storage (temporary)
Transport between DOE and DoD
DoD Transport to/from Operating Bases/Sites
Storage at Operating Base
Weapon Buildup, Mating, Disassembly, De-mating



Independent Assessments, by those who are Knowledgeable, Objective, & Tactful

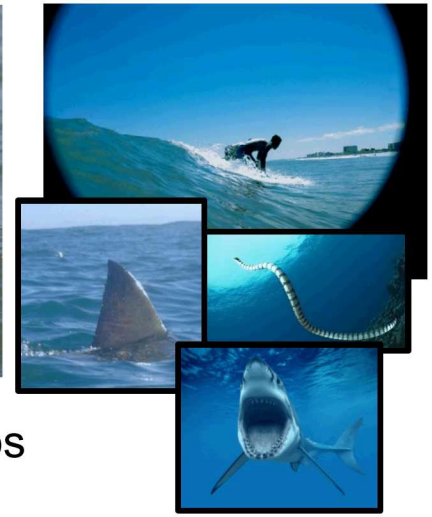
Sandia National Laboratories

Riding the fast moving wave...



- Strategic Needs of the Nation
- Strategic Plans – STRATCOM
- US Navy and Air Force Op. Units – providing nuclear weapon system readiness
- US Navy and Air Force POGs
- NNSA Design and Production Team – providing nuclear weapon readiness

Hanging back, searching for trouble...



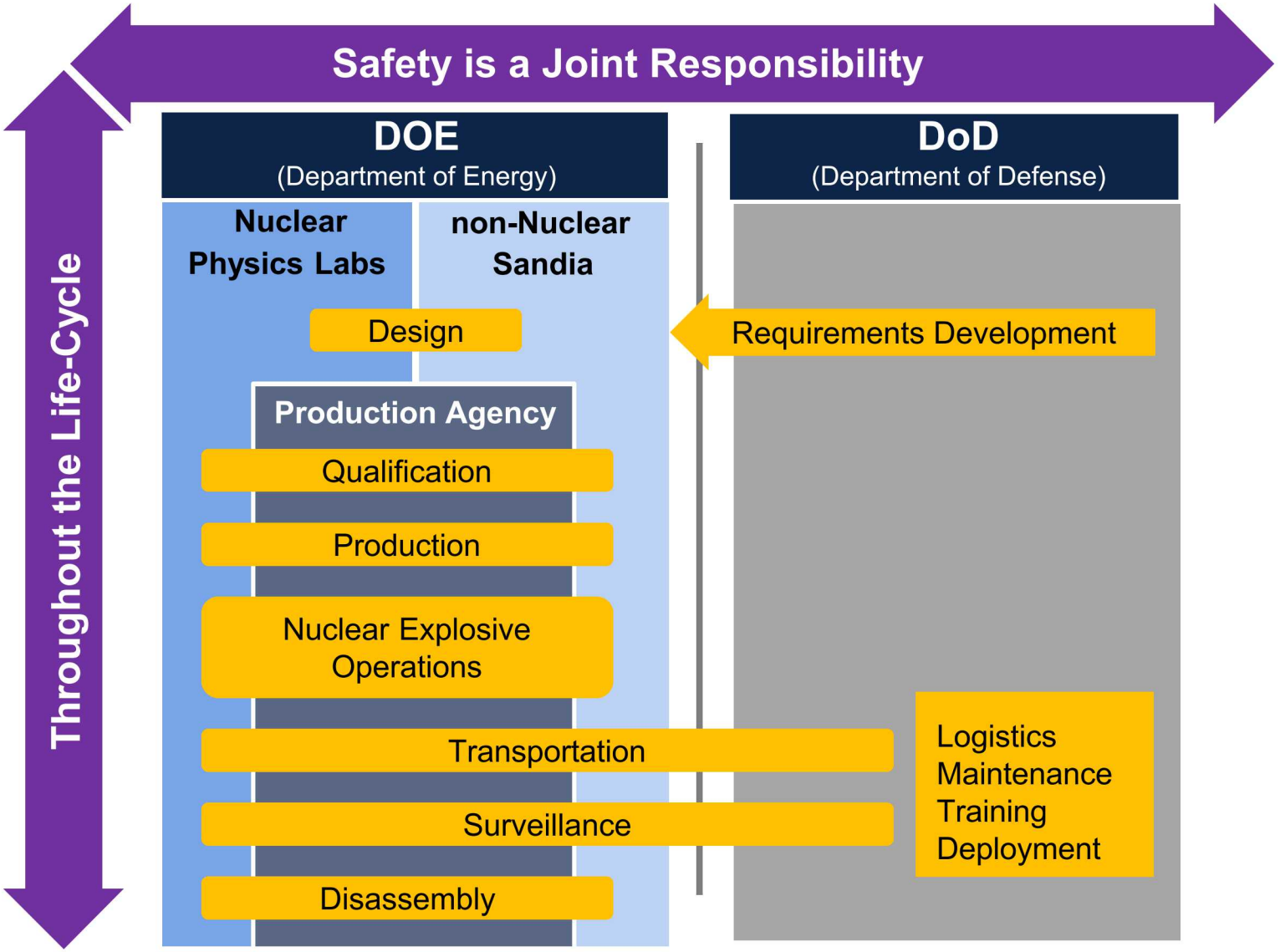
- NW System Safety Groups
- Red Teams, IVANs
- Independent Assessment Depts. / Teams

- Objective Criteria – *can mitigate "my baby" issue*
- Cross-System Knowledge Breadth, Deep Expertise
- **Independent Funding**
- **Independent Managers** & **Performance Appraisal**
- **Independent of Assessed Item** – *not your baby*
- Time to focus on selected items, probe for risk
- Be tactful, never question intent, nothing personal
- Steady nerves, thick skin, let emotional spikes pass

Nuclear Safety is *Concluded*

- **Major Assembly Release (MAR)**
  - A statement that War Reserve (WR) weapon material is satisfactory for release on a designated effective date to the DoD for specified capabilities and uses that may be qualified by limitations and exceptions

Nuclear Weapon Safety



always/Never

"We are trying to accomplish a design which will have a vanishingly small risk of a nuclear detonation given exposure to any credible abnormal environments."

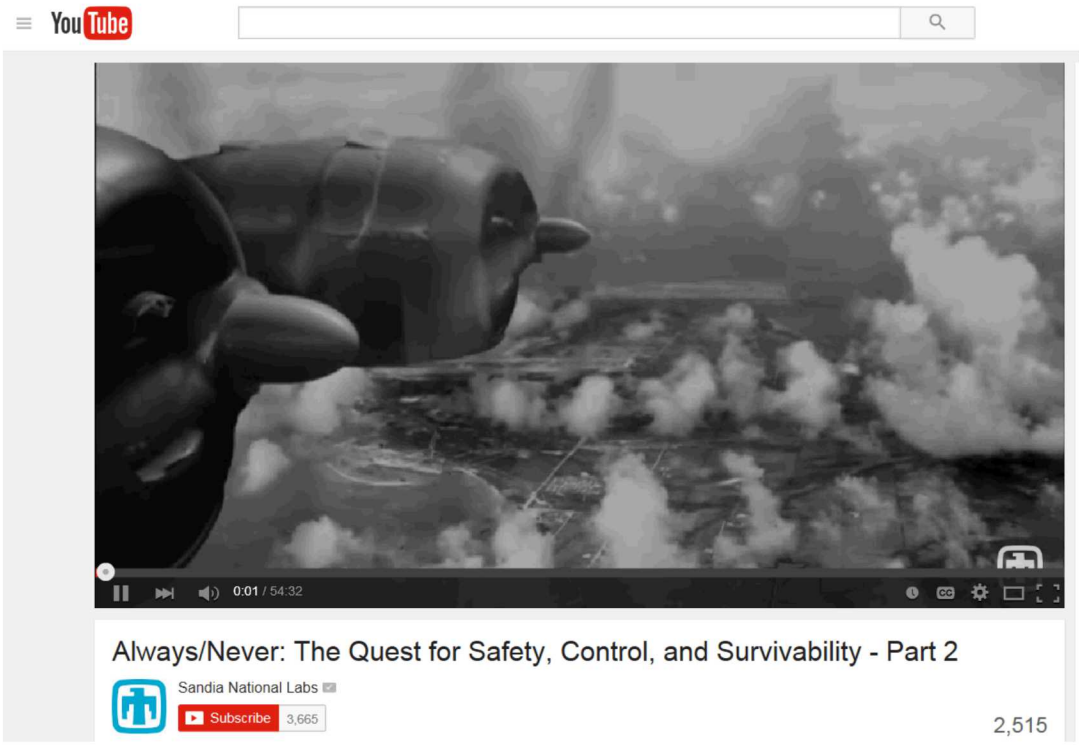
--Morgan Sparks, President, Sandia Laboratories, 1977

Ensure Always/Never…

They must *always* work if authorized by the president of the United States.

They must *never* work if not authorized.

Always/Never: The Quest for Safety, Control, and Survivability



Always / Never

Additional Details

This paper was presented at the Probabilistic Safety Assessment and Management Conference, Honolulu, HI, June 22-27, 2014. [SAND2014-1832C]

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

Jeffrey D. Brewer*
Sandia National Laboratories, Albuquerque, NM, USA

Abstract: Insights developed within the U.S. nuclear weapon system safety community may benefit system safety design, assessment, and management activities in other high consequence domains. The approach of *assured nuclear weapon safety* has been developed that uses the Nuclear Safety Design Principles (NSDPs) of *incompatibility*, *isolation*, and *inoperability* to design safety features, organized into subsystems such that each subsystem contributes to safe system responses in *independent* and *predictable* ways given a wide range of environmental contexts. The central aim of the approach is to provide a robust technical basis for asserting that a system can meet quantitative safety requirements in the widest context of possible adverse or accident environments, while using the most concise arrangement of safety design features and the fewest number of specific adverse or accident environment assumptions. Rigor in understanding and applying the concept of independence is crucial for the success of the approach. This paper provides a basic description of the *assured nuclear weapon safety* approach, in a manner that illustrates potential application to other domains. There is also a strong emphasis on describing the process for developing a defensible technical basis for the independence assertions between integrated safety subsystems.

Keywords: System Safety Design, Safety Assessment, Independence, Nuclear Weapon Safety.

1. INTRODUCTION

Insights developed within the U.S. nuclear weapon system safety community may benefit system safety design, assessment, and management activities in other high consequence domains. The approach of *assured nuclear weapon safety* has been developed that uses the Nuclear Safety Design Principles (NSDPs) of *incompatibility*, *isolation*, and *inoperability* to design safety features, organized into subsystems such that each subsystem contributes to safe system responses in *independent* and *predictable* ways given a wide range of environmental contexts. The *assured nuclear weapon safety* approach strives toward use of a concise arrangement of safety design features and a limited number of specific adverse or accident environment assumptions. Simplicity of safety features, passive safe responses, and a systematic allocation of basic features among engineered features and human actions[1] are emphasized in the implementation, and an innovative *inside out* process for hazard identification, which is described in this paper, is also applied throughout iterative system design phases to support the process of NSDP integration. In essence, this approach claims to be an efficient method for engineering bounded system safety-related responses.

Appropriate independence assertions are essential given that multiple safety subsystems, each providing safe responses for all relevant environments in independent and predictable ways must be integrated into the system to form a basis for meeting stringent qualitative and quantitative safety requirements. Overreliance on the concept of independence for asserting levels of safety without providing a sufficient technical basis is tempting, and must be avoided. In addition, it is recognized that humans do a poor job both of conceiving the many ways things may fail and estimating

* 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. This paper is designated as SAND2014-1832C at Sandia National Laboratories. The author may be contacted at: jdbrewe@sandia.gov.

[1] The primary human actions to consider are those designed to provide an unambiguous indication of intent to achieve a nuclear detonation. Other human actions include those related to ensuring safety during weapon production, assembly, testing, transportation, maintenance, and disassembly.

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

J. D. Brewer
SAND2014-1832C

Paper presented at:

Probabilistic Safety Assessment and Management Conference, Honolulu, HI, June 22-27, 2014

Sandia National Laboratories

Questions?